INNOVATIONS FROM THE UNDERGROUND:
TOWARDS A THEORY OF PARASITIC INNOVATION

By

Ethan Mollick

AB in Science, Technology, and Policy, Harvard University, 1997

SUBMITTED TO THE ALFRED P. SLOAN SCHOOL OF MANAGEMENT IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTERS OF SCIENCE

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June, 2004

Signature of Author _____
Ethan Mollick
Sloan School of Management

Certified by _____
Prof. Eric Von Hippel
Thesis Advisor

Accepted by _____
Margaret Andrews, MS Program Director
MIT Sloan School of Management

Innovations from the Underground:
Towards a Theory of Parasitic Innovation

by

Ethan Mollick

Submitted to the Alfred P. Sloan School of Management in partial fulfillment of the requirements for the degree of Masters of Science in Management.

Abstract:
For almost every complex, proprietary system there is a group of users trying to change, modify, or break it. These users have no regard for the carefully constructed business models that manufacturers use to justify their closed architectures. Instead, driven by utility, curiosity, or, occasionally, anger, these user communities innovate within the manufacturers' systems, bypassing both legal and technical safeguards. These communities exist in many diverse markets, most often as a hunted underground, but occasionally as valued partners of legitimate industry. In the computer industry, for example, they are called "hackers," while in the world of telephony they are referred to as "phreakers." Sometimes undermining systems and sometimes expanding them, these parasitic innovation communities have a deep and complex relationship with the companies whose systems they modify.

This thesis presents an examination of the phenomenon of parasitic innovation, developing explanations for how and why parasitic communities operate. It demonstrates that parasitic innovation is an ongoing phenomenon that has developed significant innovations over the last forty years. The paper then presents a model for how parasitic communities and firms interact, and offers a new strategic approach for how industry can better develop the positive effects of parasitic innovators while reducing negative impacts.

Thesis Adviser: Eric Von Hippel
Title: Professor, Sloan School of Management, MIT

Innovations from the Underground:
Towards a Theory of Parasitic Innovation

by

Ethan Mollick

Submitted to the Alfred P. Sloan School of Management in partial fulfillment of the requirements for the degree of Masters of Science in Management.

Abstract:
For almost every complex, proprietary system there is a group of users trying to change, modify, or break it. These users have no regard for the carefully constructed business models that manufacturers use to justify their closed architectures. Instead, driven by utility, curiosity, or, occasionally, anger, these user communities innovate within the manufacturers' systems, bypassing both legal and technical safeguards. These communities exist in many diverse markets, most often as a hunted underground, but occasionally as valued partners of legitimate industry. In the computer industry, for example, they are called "hackers," while in the world of telephony they are referred to as "phreakers." Sometimes undermining systems and sometimes expanding them, these parasitic innovation communities have a deep and complex relationship with the companies whose systems they modify.

This thesis presents an examination of the phenomenon of parasitic innovation, developing explanations for how and why parasitic communities operate. It demonstrates that parasitic innovation is an ongoing phenomenon that has developed significant innovations over the last forty years. The paper then presents a model for how parasitic communities and firms interact, and offers a new strategic approach for how industry can better develop the positive effects of parasitic innovators while reducing negative impacts.

Thesis Adviser: Eric Von Hippel
Title: Professor, Sloan School of Management, MIT

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

A great number of people were willing to share their knowledge, time, and assistance so that I could write this thesis. Laura Koetzle, "Dildog", Thomas Douglas, Jason Scott, and Chris Wysopol were all willing to take time out of their schedules to share their expertise with me. I would also like to thank Prof. Peter Buck, Prof. Eric Von Hippel, Andy Grant, Karim Lakhani, Jason Robar, Hugo Liu, and Prof. Lee Fleming for helping me work through various ideas and helping me fill in some gaps in my own knowledge. The errors in this thesis are mine alone, but without the insightful comments of Johanna Klein and Linda Mollick it would never have been seen this final form.

Finally, I would like to thank my wonderful wife, Lilach, who provided many key insights and encouragement thorough many late nights of work. This thesis is dedicated to her.

INTRODUCTION:
THE CHALLENGE OF PARASITIC INNOVATION

We work in the dark
We give what we have
Our doubt is our passion
and our passion is our task
The rest is the madness of art.
-- Henry James (Quoted by many parasitic innovators)

Parasitic innovators, be they illegal hackers or phone phreaks, are a challenge to established firms and their economic assumptions. They represent an alternative economic culture, brought to the mainstream as open source, and an alternative view of the economic nature of information and secrets, which they believe should not be held exclusively. More than presenting an intellectual challenge, these innovators are actors, working within established technical systems driven by their own motivations, communicating using their own methods, and interacting with other innovators as they see fit. The result is a profoundly deep divide between firm and innovator, a divide that, if mishandled, can become an all-out conflict, one which has already resulted in billions in damages and hundreds of people in prison. Even as parasitic innovation can lead to war, it can also lead to cooperation between innovators and firms, creating new business models and novel products.

The goal of this paper is to explore how parasitic innovators and firms interact, and develop approaches for innovators that result in cooperation, as opposed to conflict. By studying historic parasitic communities, and examining how and why they work, it is

possible to draw some conclusions about the role parasitic innovators play in innovating within closed systems. Additionally, by using the concepts developed to study user innovation, it is possible to relate parasitic innovation to the larger issues of innovation as a whole.

User innovation is a well-established phenomenon, responsible for the creation of many new products and services. What happens when a firm objects to communities of innovating users? In some cases, where the community is fragile or small, it disappears. In many cases, however, the community survives, and even flourishes, underground. I propose that systems-based user innovation communities as currently studied are like an iceberg – only part of the communities are obviously visible and contributing to firms in a legitimate way. These legitimate communities are the ones that no one objects to, or at least no one objects to strongly enough to force them to disappear. However, a large and ever-shifting community operates just below the surface, innovating despite, or sometimes as a result of, official censure. This phenomenon is especially prevalent in complex, proprietary systems tightly controlled by firms, such as networks and operating systems, which, due to their ubiquity, complexity, and closed nature become tempting targets for exploration.

For almost every complex, proprietary system there is a group of users trying to change, modify, or break it. These users have no regard for the carefully constructed business models that manufacturers use to justify their closed architectures. Instead, driven by utility, curiosity, or, occasionally, anger, these user communities innovate within the

manufacturers' systems, bypassing both legal and technical safeguards. These communities exist in many diverse markets. In the computer industry, for example, they are called "hackers,"[1] while in the world of telephony they are referred to as "phreakers." Sometimes undermining systems and sometimes expanding them, these innovation communities have a deep and complex relationship with the companies whose systems they modify.

The danger of this sort of innovation is familiar, and carries a real impact in the business world. For example, AT&T lost over $10 million a year in the 1970s due to "phone phreakers," while software piracy is currently estimated to cost $11 billion a year. Similar evidence of the increasing importance of this sort of user innovation is evident in the ongoing music and movie sharing, games system modification, and DVD copy protection – all of which are considered issues of paramount importance in their respective industries.

Industry complaints about piracy and theft are common, but countermeasures, whether legal or technical, often seem counterproductive, leaving open the question of how best to discourage negative user innovation. Some industries and firms have progressed further in their attempts at discouraging unwanted innovation and have in fact successfully harnessed negative user communities to significant effect. Computer game companies (Valve and id Software in particular) have successfully co-opted large segments of the

[1] The use of the term "hackers" to describe people who break into computer systems is controversial, with some authorities preferring the term "cracker." This paper will use the term hacker, however, as within the computer underground, this is the accepted name for the community. Further, among hackers of this sort, cracker has another, specific meaning of someone who overcomes copy protection on software.

previously rebellious innovation community attached to their industry. The community now develops product extensions for free, while discouraging unwanted software piracy. Similarly, companies such as TiVo have managed to gain industry leadership and acceptance over rivals by channeling or morphing potentially negative innovators into acceptable "unofficial" discussion boards and non-destructive innovation. Some firms are even harnessing these sorts of user innovation communities as important sources of highly qualified potential employees.

In this paper, I will demonstrate that this sort of innovation is an important, ongoing, and inevitable source of change in many complex industries, and that the relationship between firms and user-innovators must be carefully managed to avoid pitfalls and maximize gains. I will argue that, coexisting with most proprietary systems there exists a shadowy analogue to the standard user innovation community: the underground innovators, the pirate innovators, and the parasitic innovators.

Defining the Communities

Though the phrase "the underground innovators; the pirate innovators; and the parasitic innovators" may be dramatic, for the purposes of this paper each term will have a specific meaning as defined areas of study. The three terms are new coinages in the literature of the study of innovations, and each represents an exception to the standard user innovation community. All definitions are therefore subsets of the wider user innovation community; all three defined groups are non-commercial innovators; and the three groups occasionally, but not always, overlap, for particular user innovation communities. By

using three terms, we can clarify the way that non-traditional user innovation communities relate to both their innovations and established firms (See Figure 1).

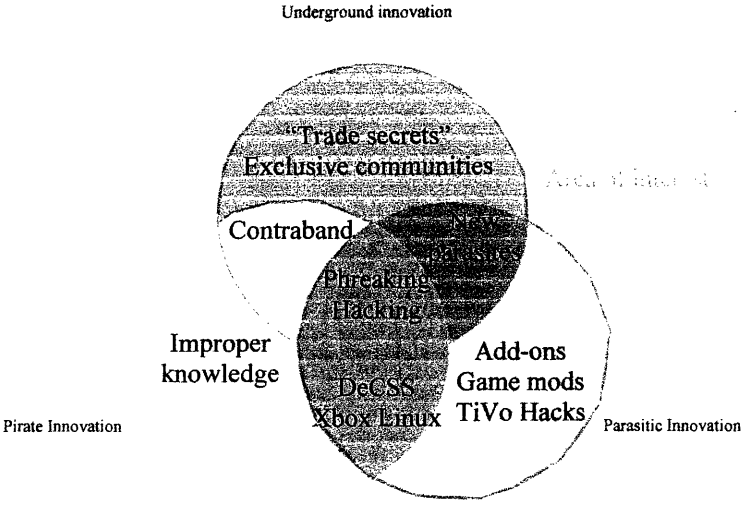

Figure 1: Parasitic, Pirate, and Underground Innovation

Underground innovators are user-innovators who intend for their discoveries and innovations to be kept secret within a small community for non-commercial reasons. Underground innovators may desire secrecy because what they are doing is discouraged or criminal; or just because they value the thrill of secret communities. Underground innovators thus do not intend to "freely reveal" to those outside of their community, and may define that community loosely or tightly, as they see fit.

The next group, the parasitic innovators, are user-innovators who create their innovations within a proprietary technical system. That is, they are users who are limited to the exploration and exploitation of an existing technology system, whether it be a network (telephone or computer), software (operating system), or hardware (AV equipment,

computers, cars). To meet the definition, this proprietary system must be closed, or, at least the portions within which the innovations are occurring must be closed. Thus, someone who discovers how to use undocumented proprietary software interfaces (APIs) to manipulate an operating system would be a parasite, while someone who uses documented methods to create a new application as the manufacturer intended would not be. Parasitic innovations cannot exist independently of the proprietary system upon which they innovate, and parasitic innovators do not create their own systems. Their innovations take the form of tools or extensions: tools that assist in the exploration and exploitation of their host system, and extensions that expand the capabilities of such systems.

This means that the definition does not include seeming parasitic innovators, such as virus writers, who write code for open systems, like Linux. Socially discouraged ideas are not the prerequisite for parasitic innovation, though many of the examples of parasitic innovation may be seen as discouraged, especially by firms. Instead, it is the interplay between proprietary systems and the innovators themselves that makes parasitic innovation different from other types of user innovation. It is also worth separating out systems form technologies to further clarify this definition – open software like Linux can be used as the underlying technology for closed systems, like computer or telephone networks. The networks are still closed, and still subject to parasitic innovation, even though some of the elements of the system are based on open source methods.

Pirate innovators are different from parasitic innovators, in that pirate innovation describes a user-innovator's official relationship to a firm, not to a particular type of system. Pirate innovators produce user innovations that are specifically or legally forbidden by the company whose products serve as the basis for the innovation[2]. Pirate innovation requires intent, so the definition includes those who expect their innovations would be forbidden, even if they are a part of an underground innovation community and their work is secret. Pirate innovators are therefore aware of the forbidden nature of their work, but carry on in any case, for either curiosity or some sort of alternate utility.

These three groups: pirate innovators, parasitic innovators, and underground innovators, occur in different situations, sometimes overlapping, sometimes not. Parasitic innovators, for example, form a common type of user innovation community, especially given the prevalence of large, proprietary electronic systems in recent decades. Parasitic innovators need be neither underground, nor pirates, as examples such as the overt computer game "modding" community and company-sanctioned alterations of TiVo video recorders would show. In Chapter 1, we will examine more closely the nature of these overt parasitic communities.

Pirate innovators, similarly, do not need to be parasitic, or even underground. Parasitic pirate innovators are innovating within a forbidden, closed system, and therefore are most often pirate innovators because of intellectual property violations, or, at worst, damage or

[2] Note that "pirate" is not a synonym for "illegal." The work done by pirate innovators is sometimes illegal, or becomes illegal at some point during the lifetime of the innovation community, though the legal system rarely keeps up with the nature of pirate innovation (see, for example, the recent DeCSS DVD decrypting cases.) Pirate innovation is also not synonymous with theft or immorality – most pirate innovators see themselves as striking blows against immoral or exploitative proprietary systems.

theft of data. Non-parasitic pirate innovators, on the other hand, trade in forbidden knowledge with potential criminal impact, such as illegal contraband like drug formulations, or legal but dubious information like methods of building explosives.

For the purpose of this paper, I am specifically interested in relationships between parasitic (and also underground or pirate) innovators and firms. Further, I am interested in parasitic innovation communities that transform into underground communities, and I will also examine the non-parasitic underground innovation community. The non-parasitic pirate community is generally unrelated to the area of study, and so will not be addressed in detail. Before trying to develop a framework to examine these communities in more detail, it is first worth examining the existing literature.

Previous Research

Literature on parasitic innovation as a whole.

As previously mentioned, parasitic innovation is not usually studied holistically, and, when studied in parts is most often approached from a particular perspective; the most common studies of parasitic innovators are adversarial and written from either a legal or technical angle, essentially ultimately posing the question "how do we stop these people?" A second type of literature on the subject mythologizes the parasitic innovator, especially the hacker, viewing him or her as "enacting technology" or seeing them through the lens of some other form of cultural criticism. Even works that attempt a more holistic approach to parasitic innovators, such as Gordon Meyer's "The Social Organization of the Computer Underground," which covers both hackers and phreakers,

focus on just the underground movements. Further, Meyer's work and others like it are papers written from a criminology perspective, an approach which I would argue is not ultimately conducive to studying what is an innovative, rather than a criminal, endeavor.

Efforts to approach the field quantitatively have proven especially problematic. Underground parasitic innovators have proven quite resistant to study, with their emphasis on privacy, paranoia, and desire to "hack the system." Surveys such as the Laurentian University Hackersurvey, published as *The Hacking of America*, are reduced to jokes inside the community. One typical response to this survey is provided Brian Martin, a hacker, who writes, among other, more vitriol-filled comments:

> ... let's consider 500 people responding to this survey. The notion that 500 self- proclaimed hackers could adequately represent the hacker population is absurd. Thinking back to the simple fact that the term *hacker* has not even been defined for this survey or anything else is amusing. So now we have 500 people professing to be something that we can't define, representing tens or hundreds of thousands of people around the world... Oops. There goes the science again.[3]

Perhaps it was these sorts of responses, along with threatened gaming of the survey, which prompted the Hackersurvey to refuse to release its results to peer review.

Better surveys of related communities, such the Boston Consulting Group Hacker Survey, do not truly cover the core underground communities themselves. They instead deal with legitimate communities like open source, which, by virtue of factors like the population's average of 11 years of programming experience in the BCG survey, clearly are not good proxies for the younger parasitic communities.[4]

---

[3] Brian Martin, "The Not So Scientific Process," http://www.attrition.org/security/rant/z/jericho.004.html, August 22, 2000.

[4].Lakhani, K. and R. Wolf , "Does Free Software Mean Free Labor? Characteristics

Parasitic innovation in the management of technology and innovation

Parasitic innovation as a separate phenomenon seems to be a relatively new field in the literature of management of technology and innovation. The closest area of research is the literature of end-user innovation, some of which even touches on user innovation enabled by electronic information exchange, as well as on the open source movement, which shares many characteristics with parasitic communities. The user innovation literature is fairly deep[5], but it makes two major assumptions that are not true of parasitic innovators.

The first of these assumptions is that users are driven to innovate by the need to customize products that do not currently exist. In the case of parasitic innovation, this is rarely true, with users much more likely to be motivated by curiosity, desire for status, or even destructive urges. While curiosity and desire to discover have been identified as elements in user innovation before, there is always the assumption that this is a contributing factor – only in parasitic innovation is it often the sum total of the motivation for a user-innovator[6]. There is also an assumption in the user innovation literature that innovation communities form because the needs of the user are generally in line with the needs of the market represented by the users. This is also not true in parasitic innovation, where the users often have entirely divergent tasks to which they

---

of Participants in Open Source Communities," BCG Survey Report, Boston, MA: Boston Consulting Group. 2000. [online: web] URL: http://www.osdn.com/bcg/.

[5] See, for example, von Hippel, E. *The Sources of Innovation.* New York: Oxford University Press. 1988.

[6] Franke, Nikolaus and Sonali Shaw. "How Communities Support Innovative Activities," Accepted for publication in *Research Policy*. January, 2002. [online: Web] URL: http://userinnovation.mit.edu/papers/9.pdf

apply the technology or products being modified, and are only united by their desire to perform such modifications.

A second similar area of research is represented by the literature on open source development. Many people have pointed out that open source innovation is motivated by a gift culture of status, similar to that of parasitic communities.[7] Once again, however, the nature of parasitic communities as motivated by things other than actual need, and the potentially destructive nature of such communities, sets them apart from standard open source users.

While both of these research areas offer insights into parasitic innovation, neither serves as an entirely satisfactory explanation for the unique nature of these communities. Even more importantly, I could not locate any studies in the literature dealing with firm strategies when faced with parasitic innovation. Where it is even discussed, co-option in user innovation is usually thought of as harnessing already useful innovation for commercial needs, rather than the parasitic innovation challenge of turning communities from negative to positive, or at least neutral, purpose. Thus, I believe this study could be of use both practically, and in the wider study of user innovation.

Research Methods

The major issue with gathering data concerning parasitic communities, is that many of them are underground, which poses a broad range of challenges. Even those

[7] Raymond, E. *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary.* Cambridge, England: O'Reilly. 1999

communities that are not underground tend to have shifting membership bases and use semi-anonymous forms of communication, such as computer bulletin boards. The result is that surveys, population analyses, and other quantitative sociological tools are often difficult to apply, and all quantitative approaches to studying parasitic communities have been severely flawed, as discussed in the literature review above. Despite these issues,, I attempted to conduct direct quantitative investigations of a number of underground parasitic communities. The results were not entirely fruitful, and a description of the methods used and their results are available in Appendix A.

Although a exclusively quantitative view was not appropriate, I also did not want to engage in full ethnography. Ethnographies of the hacker community already exist, but they are limited to studying how individual hackers or groups work, rather than the larger relationship of these communities to parasitic innovation as a phenomenon. Instead, pursuing a small-sample, case-based study seemed most appropriate.

Despite the trouble in surveying, parasitic communities are extraordinarily data-rich. Since at least the 1980s, almost all of the communication between parasitic community members has been electronic, leaving a preserved record of the internal communication between parasitic users, pseudo-journals that record findings, and computer discussion forums in which most regular interaction between users takes places. There is even a peer-reviewed print journal, *2600*[8], which is written by hackers for hackers. Even the archives of the pre-internet phreaker communities have been preserved online, either

[8] As an example of the continuity between parasitic communities, the title "2600" comes from the 2600 KHz tone emitted by the devices used by phone phreakers in the 1960s to get free phone calls.

through old electronic files, or, in some cases, by scanning old documents. In fact, since information exchange is a primary feature of the parasitic innovation community, these archives of data are remarkably well maintained. Indeed, the data-gathering of these communities borders on the obsessive, with almost every piece of minutia recorded, including details of individual meetings, reprinting of articles in popular journals, and other similar pieces of information. I found two weekly radio shows devoted to parasitic innovation, both with archives online, one having shows available since 1989. Documentaries and interviews are available for download, hacker conferences publish minutes, and generally the problem is not too little data but too much.

In addition to primary data and secondary sources, I found individual parasitic innovators only too happy to talk one-on-one, even if they would not answer surveys. The result is a rich data source that supported a deep analysis of the chosen cases, and which grants some authority to the results discussed in this study.

For the study itself, I have selected for analysis five parasitic user innovation communities over the past fifty years (Figure 2). These groups were selected because they are all relatively well documented cases of parasitic user innovation, cases in which the host industry reacted strongly and publicly to its parasitic communities, and cases in which the user communities themselves have left substantial documentation. Most importantly, in each of these cases, there was some ambiguity as to the true impact of parasitic innovation, making it valuable to examine how industry and user innovators interacted. I also wanted to defend against the possibility of selection bias, so while these

groups are the easiest about which to gather information, they are also sufficiently diverse as to provide a cross-section of types of parasitic innovation.

Figure 2.

Proprietary System	**Type of parasitic innovative community**
Telephone system from 1963-1985	Phone phreaks
Networked computer systems from 1980-2004	Traditional "hackers"
Computer games from 1985-2004	Game modders (Also includes a discussion of mod chips)
DVDs from 1998-2004	DeCSS
AV Hardware from 1998-2004	TiVo modifications

I would also argue that each of these cases represents an example of a common phenomenon. There are at least two arguments for why this would be the case. First, there is a direct linkage between these communities. The original phreakers (the earliest parasitic innovators in the study) moved directly from exploring the phone system to exploring computer software and then to modifying hardware, for example. This transition was quite seamless: early hackers used the exact same computer bulletin board systems (BBS) to share information as the phreakers before them, and inherited the phreaker language, which they still use today.

Beyond direct continuity, there is also continuity of methods and approaches. The communications systems, social structure, and methods of "attacking" proprietary systems are all substantially the same. Certainly, in the more recent internet era, these problems are all grouped under the "security" rubric, and are viewed to be outgrowths of a single type of hacker activity. To start, we will examine these communities.

CHAPTER TWO:
FIVE PARASITIC COMMUNITIES

The five communities below are described in roughly chronological order. The goal of each case is to provide both an overview of the nature of the community and its interaction with the firms that provide the technology upon which it is a parasite. Before detailing the communities, it is worth detailing some conventions used in this paper. Given the underground nature of many of these communities, individual innovators often use "handles" instead of names. Handles range from computer terms like Control-C to the fanciful, such as Deth Vegetable. These handles, as well as original, and often idiosyncratic, spelling have been preserved in the quotes throughout this paper. Where there are multiple possible terms for a single concept – such as the case of underground documents often called textfiles, filez, or philes – the author has selected a single consistent term to use.

Community One: "Phone Phreaks"

Phreakers make up the oldest of the communities studied in this paper, dating from the mid-1960s. Phreakers are also the easiest of the communities to classify according to the taxonomy of outlaw innovation – they were always an underground, pirate, parasitic community. They were among the first parasitic communities, if not the original community itself. There is no doubt that the community was always parasitic, operating within the bounds of the phone system by definition. Additionally, because the first rite

of passage for any phreaker was to learn to make free phone calls before manipulating the phone system in more sophisticated ways, they were always a pirate community as well, acting in constant danger of discovery by the monolithic AT&T. The forbidden nature of the phreaker's activities, as well as the drama that the community seemed to like to cultivate, also ensured that the community was underground in nature from the very beginning. This first group of outlaw innovators would therefore set the tone for other types of user-innovators to follow.

Description and history of the innovation community

The goal of phreakers, over the course of their three decades of active work, has been to explore and exploit the tremendous complexities of the national phone system. These phreakers, "without the help of Bell Systems Practices, circuit descriptions, Boolean algebra, [and] sequential circuit theory" managed to not just understand the phone system, but also to, in the words of one Bell scientist, "make it do things its designers had never anticipated."[9] In order for this type of deep innovation within a system to occur, however, the phone network had to reach a high level of complexity and automation. This finally happened in the 1950s and early 1960s with the advent of crucial modifications to the national phone network.

It was then that operators were eliminated from the long-distance system, allowing customers to place calls through Direct Distance Dialing (DDD). Bell had two options as to how to implement DDD since the rotary pulse method of calling used in local lines would not work for long-distance. One choice was to have out-of-channel signaling, in

[9] Staff, *Business Communications Review*, 1995, p. 22

which a separate line carries the call routing data, such as to whom the call was placed. The other option was to carry all of the information on one line. Bell chose the second, cheaper alternative implementing multi-frequency signaling (MF). MF was AT&T's control system for its long-distance service. The company decided to route long-distance calls along a single line by using a series of twelve combinations of six different tones. These combinations represented numbers, and were simply two different frequencies played together. In 1960, the *Bell System Technical Journal* published an article called "Signaling Systems for Control of Telephone switching" which listed all of the tonal combinations. This magazine was distributed to college universities around the nation, and it was not long before someone discovered how they could be used to manipulate the phone system.[10]

In 1961, AT&T became aware of a device called a "blue box"[11,12]. Blue boxes were relatively simple pieces of equipment that could produce all twelve tone combinations. To use a blue box, a phreak would call a toll-free line, making a connection between his local switch and the switching office serving the toll-free number. Before it rang, the user would press a button causing the box to emit a 2600 hertz tone. This tone is the same one continually emitted by an idle, unconnected switch. When the toll-free switching station detected this tone from the phreaker's switch it assumed the caller has hung up, even though the phreaker's line was still active. As soon as the tone ended, however, the toll-free switch once again registered the line as activated, and so it waited

---

[10] Bioc Agent 003, "Basic Telecommunications, Part IV," June 15, 1984. [online: Web] URL: http://www.textfiles.com/phreak/BIOCAGENT/basicom4.phk

[11] These boxes are rarely blue, but are named that way after the color of the first copy made.

[12] Kleinfeld, Sonny. *The Biggest Company on Earth.* Holt Rinehart & Winston, 1983. p 251

for a new number to be dialed. The phreaker entered this number with the blue box keypad, and the new call was made by the toll-free switch. Even though the switch servicing the toll-free number had made a new call, the phreaker's line remained connected to the free number, and was not billed for the call.

The exact inventor of the blue box is not known, but its invention was merely the automation of a process that had been developed several years earlier by a number of people around the country. What drove them all was curiosity about the phone system, and an almost obsessive desire to discover how it worked. Some of these original phreakers were blind, and played with the phone system as children. Others accidentally discovered unusual numbers, such as loop-around pairs, which are toll-free numbers that allow a caller to speak to the person who called the other number, and became curious about how the system worked. Regardless of how they became interested, one by one, these people learned how the phone system could be manipulated by using MF tones. They did this with methods ranging from physically whistling to blowing a free Cap'n Crunch cereal whistle that happened to produce a 2600 hertz tone. Even before the invention of the blue box, a small group of individual innovators were actively experimenting with phreaking.[13]

By the 1970s, blue box use began to skyrocket for several reasons. First, publicity about boxing increased, especially after a famous, and extremely detailed, article was published on the subject in a 1971 issue of *Esquire* magazine. Secondly, technical details became more available, as activist Abbie Hoffman and a person calling himself 'Al Bell' started

[13] Rosenbaum, Ron. *Esquire*, "Secrets of the Little Blue Box," October, 1971, p. 124

the *Youth International Party Line* (*YIPL*) in 1971, which published a quasi-underground magazine containing technical information on the phone system.[14] Adding to the increased visibility of phreaking was a number of prominent arrests, including one of the millionaire financier Bernard Cornfeld. [15]

As the popularity caught on, phreakers went beyond the blue box, inventing new devices, some of which were fairly esoteric. Among them were the red box, which fooled payphones into believing that coins had been inserted; the cheese box, which diverted calls; and the acrylic box, which gave the user call waiting and call forwarding. Some of the great innovators in the computer world, among them Steve Jobs and Steve Wozniak, founders of Apple, got their start in the phreaking community[16].

Corporate Response

AT&T, from the early days of the phreaker movement, saw these pirate users as a danger, and devoted substantial resources to tracking down and punishing all potential system abusers. The history of AT&T's counterattacks against phreakers started soon after the company first discovered the blue box in 1961. Originally, Bell attempted to crack down on blue box calls by looking for anomalies in calling records. If, for example, as in one court case, an individual was to make several thousand phone calls to information in a short period of time, than the billing computers would turn this information over to an investigator. The investigator would then attempt to determine if the individual was a

---

[14] Hafner, Katie and Markoff, John.*Cyberpunk.* (Simon and Schuster:New York), 1981, p. 20.
[15] Staff, *Washington Post*, June 14, 1978. p. D11.
[16] The blue boxes sold by the two for $150 a piece were partially used to fund their education, and, indirectly, the founding of Apple several years later.

blue box user by looking for risk factors. If the investigator suspected that a blue box was being used, (if, as in the court case, the suspicious line was owned by a bookie) than the phone company would monitor the line for blue box use.[17] This method was effective, but very slow. Additionally, it tended to catch only amateur blue box users, as only the ill-informed would make mistakes that would tip off the primitive accounting computers, such as calling information for hours at a time.

AT&T realized that this method was not particularly useful for catching the more dedicated phone phreaks. By 1965, it had come up with a better solution. New equipment from Bell Labs randomly scanned the phone lines looking for MF tones that could come from a blue box. If tones were found, the call was recorded and sent to security experts for evaluation. Between 1965 and 1970 about 30 million calls were searched, and 1.5 million recorded, a process which caught about 500 phone phreaks.[18] This approach, too, had its problems. It yielded relatively few arrests, and caused a large amount of resentment among civil libertarians.

With the increasing prominence of phreaking, AT&T stepped up efforts to control the problem. In fact, some analysts believe that Bell spent far more on trying to stamp out the problem than it was worth. In the late 1970s, for example, fraud cost AT&T only $10 million out of revenues of $32 billion, yet it was spending many hundreds of thousands of dollars and tremendous resources to hunt down the criminals. AT&T defended its practices by stating, in the words of the director of corporate security, "without the

[17] People v. Garber
[18] Silver, Roy. "Blue Box is Linked to Fraud," *New York Times* May 5, 1973

deterrent of knowing we are taking countermeasures, the use of these devices would be much more widespread."[19] Regardless, by 1977, AT&T had begun to change its systems, especially in urban areas, to make blue box use impossible.[20]

Even after three decades of cracking down on the phone enthusiast community, AT&T has never succeeded in containing the phreaker movement, which still exists today. Indeed, it can be argued that the company actually made the situation worse through its "get tough" stance. Not only did Bell encourage phreakers by the illicitness of the act, but they also further tightened the community through constant persecution. This view was demonstrated in a warning by "The Jedi": "Those of you that are new to phreaking and stuff like it, educate yourselves BEFORE you dive into it. Remember, we're all in this together, if you get busted calling a pirate/ hack/ phreak/ anarchy bbs [electronic Bulletin Board System]. They'll get a hold of the user list and posts and bust everyone on the system. Don't ever rat on anyone!!!"[21]

Another negative effect from AT&T was that the constant persecution by the company ensured that the systems attacked would be the most valuable. Phreakers are drawn to the most secure systems, since those systems are the ones that most increase that can most increase a phreaker's reputation. Thus, phreaks tend to attack those areas of the telephone network that the phone companies most want to protect. The result is that the telephone companies inadvertently encouraged phreakers through their own security measures to

---

[19] Kleinfeld, N. R.., "The Myriad Faces of Fraud on the Phone," *New York Times*, June, 1977
[20] Staff, "ATT Monitored Millions of Calls," *Wall Street Journal*, May 6, 1977. p. 40.
[21] Jedi, P/HUN Newsletter #1, phile 1.9, March 30, 1988

concentrate their attentions on the most sophisticated and vulnerable sections of the system.

The gradual reduction of blue boxing was not the end of phreaking, however, which continued apace through the mid-1980s and exists in some limited forms today[22]. The real cause for a reduction in phreaking through the 1980s was that something more interesting came along. Instead of being confined to a single network, phreakers had a much larger world to play with, the world of connected computers.

Enter the hacker.

Community Two: "Hackers"

Probably the most famous of the parasitic innovation communities, the hacking community, is also the broadest and the one most open to misinterpretation. For the purpose of this paper, I intend to define hacking rather narrowly, instead of becoming involved in the numerous arguments, both legal and academic, about "who a hacker is." Hackers, for innovation purposes, are underground, pirate, parasitic innovators who are primarily interested in computer and network security, just as phreakers, ultimately, focused on the security of the phone system. Therefore, users who attempt to break into secured computers to find secret information; who find "back doors" in operating systems; and who write applications that take advantage of security flaws, are all hackers. Other communities sometimes included as hackers – people who distribute illegal copies

[22] From "Phreak2K" : "Lack of recent information on the internet in relations to phreaking has been a real problem lately. This simple fact has lead many to believe that phreaking itself is dead. Of course this is untrue Therefore, in writing this tutorial, I am giving you, the reader, the chance to try out phreaking as it is today." The article goes on to describe a number of new phreaking techniques.

of software, for example – are less interesting from an innovation perspective and can be safely separated from the larger community in this case. The overview below will be relatively brief compared to some of the other communities studied in this paper. This does not diminish the importance of hackers as a parasitic community, but rather reflects the fact that there is substantial documentation on hackers in both the academic and popular press, making a full history unnecessary.

Description and history of the innovation community

The hacker community grew fluidly at the same time as the late phreaker community. It does not appear, however, as some have argued, that phreakers turned to hacking in order to penetrate the new computerized phone system.[23] Instead, it seems that as phreaking grew more restrictive and less interesting, hacking became a primary activity for already technically minded phreakers.[24] In addition to the underground world of phreakers, hacking had a parent in the Home Brew Computer Club, and other early hobbyist communities that developed hardware and software in the late 1970s and early 1980s.

More than any other parasitic community, hackers seem to feed on their own mythology, much of it of dubious veracity. The early underground pirate hacking community took a large portion of its inspiration from a movie starring Matthew Broderick as hacker who has to stop World War III, called *WarGames* and released in 1983. Many of the most famous hackers of the 1980s claim this film as inspiration, and, if not starting the hacking

[23] Meyer, Gordon, "The Social Organization of the Computer Underground," unpublished thesis, 1989. Available at http://bak.spc.org/dms/archive/hackorg.html.
[24] As late as November, 1989, *Phrack* magazine was still referring to hackers in general as phreakers/hackers.

movement, it certainly galvanized it.[25] Other works of fiction soon took up the hacker theme, most famously *Neuromancer* in 1984. The popularity of the idea of the hacker resulted in a parasitic community that both captured and reacted to the public imagination, though hackers, like cowboys, were never as glamorous in reality as they were on page and screen. Still, this image insured that hackers would remain an underground, pirate community.

What hackers actually did was take advantage of the growing connectedness of computers, first through dial-up modems, and later through the Internet. Hackers essentially seek lapses in security, whether these security flaws caused by errors in an operating system or human error. Once hackers get access to forbidden information, what they do with it varies – some "black hat" hackers use it for gain or destructive purposes, while "white hat" hackers notify companies of the security flaws they found. Either way, the impact of their activity is often overstated. A 2003 estimate puts worldwide yearly loses from hackers at $1 billion, as opposed to $8.4 billion from viruses and worms and $10.4 billion from unwanted email.[26] Further, the majority of the hacking damage comes from insiders within the wronged firms, rather than outside pirate innovators, further reducing the financial impact of hacking.

These relatively low damages in reality, as opposed to the perception of the danger posed by hackers, stem from the fact that the majority of hackers are primarily interested in exploration, not exploitation. Like phreakers before them, they are not specifically out to

---

[25] Thomas, Douglas. *Hacker Culture*,. pp 26-28
[26] Lemke, Tom. "Spam Harmed Economy." *Washington Times.* November 9, 2003.

cause destruction, but at the same time do not feel bound by the needs of firms or by laws that they do not feel are relevant to their greater interests. Many of the online beginning guides to hacking start with messages similar to this one:

> I am encouraging you to break laws, but in the quest for knowledge. In my mind, if hacking is done with the right intentions it is not all that criminal. The media likes to make us out to be psychotic sociopaths bent on causing armageddon with our PCs. Not likely.... The one thing a hacker must never do is maliciously hack(also known as crash, trash, etc..) a system. Deleting and modifying files unnecessary is BAD. It serves no purpose but to send the sysadmins on a warhunt for your head, and to take away your account. Lame. Don't do it.[27]

Hackers, like all parasitic communities, are highly innovative within their field. In their quest for interesting information, they created both novel forms of identifying and exploiting security weaknesses, as well as hundreds of software applications dealing with security topics. Many of the concepts currently used in security, such as black box testing and attack testing, came from the hacker community. Perhaps even more importantly, hacking serves as a training ground for many legitimate programmers, in the words of one hacker, "Most people who write code go through a hacking phase."[28]

Corporate Response to Pirate Innovations

Hacking is viewed as a serious threat by computer software and hardware manufacturers. Some companies have chosen to embrace "white hat" hackers, but the vast majority continue to treat the entire community with suspicion. The corporate response to hackers will be discussed in more detail in Chapter 3.

---

[27] Deicide, "The Neophytes Guide to Hacking," August 8, 1993. Available at http://www.textfiles.com/hacking/guidehak.txt

[28] Dildog, Interview with author, February 18, 2004.

Community Three: "Game Modders"

Though the game mod community started in a very similar way to communities of both hackers and phreakers – as an underground, pirate community - its member were later embraced by the firms upon which they acted as parasites. This case, then, gives an example of how an underground community can be made legitimate.

Description and history of the innovation community

Parasitic innovation in the world of games takes the form of optional extensions or modifications to existing computer game code, or "mods" in community parlance. Modding, through its relatively short history, has traveled from a nuisance and potential intellectual property issue to a key positive factor in computer game design.

There had been some limited modification of computer games as early as 1983, near the beginning of the home PC era. These first modifications to games were made by organizations with names like The Crew and Cult of the Dead Cow in order to overcome anti-copying protection built into the early games of that time. Calling themselves software pirates, these individuals and groups were often fluid parts of the larger hacker community previously discussed.

These early hackers soon turned their creative energies to modifying the games that they were playing. Often considered the first true "mod," in 1983, a parody of the popular

WWII adventure, Castle Wolfenstein, was released. Castle Smurfenstein was available free on the same BBS systems that the hackers and phreakers used.[29]

Figure 3: The Castle Smurfenstein Mod

The same mod efforts that went into creating Castle Smurfenstein were more generally applied to negative purposes. Almost every major game was "cracked" by groups of pirates who would often modify the game to feature their name, or offer cheat options. The technical skill required for these cracks was considerable, much more so than mods, and generally considered quite challenging. Take, for example, this piece from Krackowicz's Kraking Korner, a document which runs over 23,000 words in an original text file distributed electronically in the 1980s, dealing with how to mod games to make them easy to copy:

> The big thing about copy protection is that it doesn't. A year's effort by a crackerjack military cryptograpy team can usually be undone in fifteen minutes, between Klingon zappings, by your average fourteen- year-old. And, morality and economics aside, one fact stands out... undoing copy protection is fun! Not only is it fun, but cracking the uncopyable is about

[29] http://evlweb.eecs.uic.edu/aej/smurf.html

> the most challenging and rewarding thing that you can possibly do with your Apple. And, the things you learn along the way are exactly the skills that you will need to become a really great programmer. So, i guess we should all be thankful for the copy-protection people since they are giving us all this fascinating entertainment and superb training at an unbeatable price.[30]

Positive modding was non-existent from Smurfenstein until the mid 1990s, when the sequel to Castle Wolfenstein, Wolfenstein3D was released. Users created hundreds of additional maps, levels, songs, and characters as mods for Wolfenstein3D, significantly increasing the playability of the game and extending its shelf life. Not only did these modders create new content, but they actually developed entire toolkits making modding the game easier for future enthusiasts.

Game developers, often former hackers and phreakers themselves, quickly took notice. The next major Wolfenstein-like game release was Doom, and, with it, the developers had a new philosophy on modding: "we really wanted to enable the user to make their own content, to make that easy as possible. [we've] always had the Berkeley-like 'Information should be free' mantra."[31] This philosophy appealed to the modding community, which, in large part, abided by the request of Doom's developers to only develop mods to be used by people who bought the software, as opposed to those who had the free demonstration version.

---

[30] Krackowicz, Krackowicz's Kraking Korner, date unknown (probably 1982-1983). Available at textfiles.com

[31] Au, Wagner. Salon, April 16, 2002. p. 2.

These mods were surprisingly professional, and once again custom toolkits were created to make future modding easier. The quality of the end product was so good that Doom's developers later sold an "Ultimate Doom Kit" at retail stores containing the best of these free mods. Beyond just extending the game, these modders created real innovation, pushing the game industry in new and successful directions

> "Many were really cool and innovative," Hall [a Doom developer] says. Justin Fisher's "Aliens Total Conversion" for "Doom" and "Doom II," says Rich Carlson, an independent developer and veteran level designer, changed the way "Doom" was played "by focusing on stealth rather than frontal assaults ... [It] presaged the kinds of 3D action games and mods we play now -- by about eight years!"[32]

From that point forward, game designers considered modders an essential partner in developing games with long shelf-lives. Future game releases included sophisticated user toolkits, and official sites included libraries where mods could be downloaded, as well as mod contests. By any measure, this has been a fantastically successful partnership between the game developers and the once underground mod community. Some mods of games have sold over a million copies, and one or two good mods can extend the lifetime of otherwise aging games for years.

Corporate Response to Pirate Innovations

The response of game companies to modding was not pre-ordained. In fact, it was a potentially high-risk decision taken by one company, rather than an industry-wide approach. The tradition of modified games did not begin with Smurfenstein, but rather with software pirates cracking games for illegal distribution. Because game developers

[32] Salon, p 2.

were quick to see the potential upside of parasitic innovation, they recognized an opportunity. Game developers thus realized that while they could not stop pirate innovation, they could still harness other aspects of the parasitic community.[33]

While the PC game industry has accepted modding, however, the antagonistic Bell/phreaker scenario is beginning to play out in another section of the gaming market, the consoles. There, Nintendo, Sony, and Microsoft are fighting the introduction of "mod chips," pieces of hardware that can be attached to gaming systems to modify how they work, allowing custom software to be run on these proprietary machines. Already, the three companies have launched a flurry of lawsuits against individuals and small companies that make mod chips, including Lik Sang, the major Hong Kong producer.

As in the case of all parasitic innovations, mod chips have multiple potential uses, making it difficult to distinguish between the curious and the criminal. In the words of Anthony Jarrett, a leading Xbox expert:

> The Xbox mod chips can be used by homebrew (software) enthusiasts to do great things with the awesome power of the Xbox," said Jarrett. "But the mods also have a downside by allowing piraters to make money from the illegal selling of copied retail games. The problem is, both scenes require the same thing: to be able to run (recordable CDs or DVDs) using unsigned code. At present, this is not possible without the use of Xbox mods. [34]

---

[33] For an economic analysis of the failure of software protection to stop piracy, see Conner and Rummelt (1991), "Software Piracy: An Analysis of Protection Strategies", Management Science, 37, pp. 125-139.
[34] Becker, David.CNET News, May 22, 2002.

In response, the mod chip community has begun to retreat into the grey world of the phreakers, with secret sites, clandestine meetings, and the other hallmarks of a pirate community. It remains to be seen whether mod chips will follow the phreaker or PC game modder model of development.

Community Four: "DeCSS"

If game modding shows how an underground, pirate community can be turned legitimate, the case of DeCSS is an example of how a legitimate parasitic community reacts to a new classification of pirate status without ever going underground. Like all of these electronic parasitic communities, it can be hard to tell where another community, like hacking, ends and where the more specialized DeCSS community begins. Whether or not DeCSS is a product of the traditional hacking community (and I would argue it is much closer to the aboveground open source tradition than underground hacking), as a case itself it provides a valuable insight into how parasitic communities react to challenge.

Description and history of the innovation community

DeCSS is a program that decodes CSS, the Content Scrambling System, an encrypted key that prevents DVDs from being played back in an unauthorized manner or otherwise copied (DeCSS means "Decodes CSS"). Under the 1998 Digital Millennium Copyright Act (DMCA), firms gained legal protection of rights management schemes designed to protect content, like CSS. Suddenly, decoding DVDs became a violation of the law, making DeCSS, developed by a fifteen-year old-Norwegian and two anonymous open

source programmers so that they could make a DVD player that could run on Linux, the subject of a legal debate.[35]

When *2600*, the hacker magazine, published the DeCSS code on its website, the Motion Picture Association of America sued under the DMCA. In a series of court cases, the MPAA won. The result was that not only did the judge ban printing the code to DeCSS, but also banned links to the DeCSS code on grounds that it was "too easy" to follow a link. The reaction from the legal and civil liberties communities was swift, starting debates that continue to today over whether DeCSS violates the DMCA, whether the DMCA violates the constitution, and whether source code is protected speech.

From the perspective of the parasitic innovators, however, it was clear that the MPAA was wrong, and that banning source code and linking was a terrible wrong. The community thus reacted in a way presciently stated by the attorney representing the DeCSS defendants, "I presume what this is going to do immediately is lead to a massive protest. The decision doesn't matter, not because it shouldn't matter, but because those people who want the code have it, and those people who don't can still get it . . . You can't put the genie back in the bottle."[36]

---

[35] There remains controversy over whether DeCSS was created, as its authors and many sources claim, to create an open source DVD player. At the same time as the DeCSS algorithm was being developed for a Linux release, a Microsoft Windows version of the decoder, also called DeCSS, was released. Source: Warren, Rob. "Openlaw DVD/DeCSS Faq," Berkman Center for Cyberlaw, Harvard University. Updated May 3, 2000.

[36] Pegorano, Rob. "Hollywood to Viewers," *Washington Post.* August 25, 2000.

The issue of access to DeCSS for hackers was never in doubt, as copies were spread across the web. Additionally, this otherwise fairly pedestrian piece of code quickly became a focus of substantial innovative work, as teams of innovators refined, revised, and played with it precisely because it was banned. Clever responses abounded, including Mr. Bad, who wrote and widely distributed a piece of software called DeCSS that had nothing to do with DVDs, but instead was designed to make it nearly impossible for MPAA employees to identify the real software. Mr. Bad's plea for the distribution of DeCSS provides an eloquent view of the threatened parasitic community:

> I encourage you to distribute DeCSS on your Web site, if you have one.... I think of this as kind of an "I am Spartacus" type thing. If lots of people distribute DeCSS on their Web sites, on Usenet newsgroups, by email, or whatever, it'll provide a convenient layer of fog over the OTHER DeCSS. I figure if we waste just FIVE MINUTES of some DVD-CCA Web flunkey's time looking for DeCSS, we've done some small service for The Cause.
>
> [And a brief note for said Web flunkey: d00d, what are you DOING? How can you *possibly* be doing this job of searching around the Web and pointing fingers at people for trying to distribute free software? What is the matter with you? Have you no respect for the many hackers that have come before you, who built up this Web that is making you a living? How can you participate in this ugly, ugly action? If you feel you need to do it to keep your job, think again. Send me email, and I'll personally help you to find a better job, with better pay, and WAY better karma. You need to walk away from this crappy gig while you still have some scrap of dignity. Hell, if you walk away, you can be a HERO! Think about that for a second, man!][37]

Other hackers took to placing the DeCSS source on T-shirts (later stopped by court order), hiding it in images, and even creating an epic 456-stanza haiku describing the

[37] Mr. Bad, Pigdog Journal DeCSS Distribution Center, PIGDOG JOURNAL, Feb. 16, 2000, at http://www.pigdog.org/decss/.

code.[38] More interestingly, from an innovation perspective, parasitic innovators began to compete against each other to generate the smallest, most elegant piece of code, with technical publications like *The Register* reporting the latest results.[39]

```
/*      efdtt.c      Author:  Charles M. Hannum <root@ihack.net>
/*      Thanks to Phil Carmody <fatphil@asdf.org> for additional tweaks.
/*      DVD-logo shaped version by Alex Bowley <alex@hyperspeed.org>
/*      Usage is:  cat title-key scrambled.vob | efdtt >clear.vob

#define m(i)(x[i]^s[i+84])<<

                  unsigned char x[5]      ,y,s[2048];main(
                  n){for( read(0,x,5     );read(0,s ,n=2048
                           ); write(1   ,s,n)         )if(s
                 [y=s      [13]%8+20]  /16%4  ==1      ){int
                 i=m(      1)17  ^256 +m(0)   8,k      =m(2)
                 0,j=      m(4)   17^ m(3)   9^k*     2-k%8
                 ^8,a     =0,c    =26;for   (s[y]    -=16;
                --c;j  *=2)a=     a*2^i&    1,i=i /2^j&1
                <<24;for(j=        127;     ++j<n;c=c>
                                   y)
                                   c

                          +=y=i^i/8^i>>4^i>>12,
                  i=i>>8^y<<17,a^=a>>14,y=a^a*8^a<<6,a=a
                >>8^y<<9,k=s[j],k         ="7Wo~'G_\216"[k
                 &7]+2^"cr3sfw6v;*k+>/n."[k>>4]*2^k*257/
                       8,s[j]=k^(k&k*2&34)*6^c+~y
                                 ;}}
```

Figure 4: The smallest DeCSS source, in the shape of the DVD logo.

This was truly innovation without direct utility, especially given that, even with DeCSS, it was more expensive to copy DVDs than it was to purchase them. The MPAA declared war, however, and the new pirate community engaged in innovation for the sole purpose of attacking a hated enemy.

Corporate Response to Pirate Innovations

The MPAA has followed the path blazed by other industry associations, using the DMCA and any other legal tools at its disposal to block software that helps circumvent copy

[38] Touretzky, D. S. (2000) Gallery of CSS Descramblers. Available at: http://www.cs.cmu.edu/~dst/DeCSS/Gallery. Features a wide range of examples

[39] Smith, Tony. "Tiny C Codes Bests Seven Line DVD Decoder." *The Register*, March 13, 2001.

protection. Pursuing this strategy brands all those who distribute or support DeCSS as criminals, and prevents any sort of potential accommodation. As the MPAA states, "We can never abandon the fight to preserve intellectual property rights, just because it is difficult. The stakes are too high. Should law enforcement stop fighting crime just because efforts are difficult?"[40] Though the MPAA has, in recent months, dropped some of its legal suits, they have announced their intention to continue to pursue the matter in the courts using different strategies.

While the MPAA has had some success suppressing the DeCSS code, it is unlikely that it will be completely successful. Pirate innovators communities have never been stamped out by the actions of a firm. Some firms, such as one covered in the next community, have even been successful in reaching a win-win accommodation with their parasitic innovators.

Community Five: "TiVo Hackers"

Unlike the other four communities profiled, this parasitic community is very tightly targeted around a single device produced by a single firm in a relatively small industry. Examining this narrowly defined, and tightknit, community, offers an opportunity to examine the birth of a parasitic community in microcosm, and to detail closely the birth of the community. Additionally, as one of the most recent parasitic communities, it offers a good example of how parasitic innovation has become more mainstream – a realm of hobbyists as well as hackers.

[40] MPAA, "DeCSS Faq," undated, [online: web] URL: http://www.mpaa.org/Press/

Description and history of the innovation community

TiVo was the first personal video recorder, or PVR, released on the market. A PVR works like its older cousin, the VCR, except that it records programming from television to a hard-disk, giving users a constant buffer of programming that they can pause, rewind, or record. The feature that sets PVRs apart from VCRs is that PVRs connect to a central information system via either the phone or the Internet, downloading program schedules and ensuring that the PVRs are always recording the desired programs, no matter when they are on. The connected nature of PVRs, and their essential similarities to computers (TiVo runs Linux), make them an ideal candidate for parasitic innovation. Their suitability for user innovation is further enhanced by their prominent place in the life of the user, as TiVo users often turn to fanaticism when praising their device.

Introduced in the fall of 1999, TiVo quickly gained a devoted, if small, following, and, almost as quickly gained a parasitic community. Although officially silent on "TiVo hacks," the company did nothing to either discourage or encourage their appearance. Since there was never a negative reaction from TiVo, the result has been a parasitic community that is neither underground nor pirate in nature, and which has a close perceived relationship with its host company[41]. Without an underground component, TiVo hacking is a very open activity, with modified TiVos offered for sale online, and well-received books on the subject published by major technical presses.

[41] As an interesting side note, there still seems to be a strain of the old phreaker/hacker ethic at work. Despite the fact that it isn't, the largest TiVo hacking community's site demands that information about hacks be posted in a forum called the "TiVo Underground."

Due to the relatively constrained and aboveground nature of TiVo hacking, there is an opportunity to get a slightly better picture of the parasitic innovation community associated with the product. One way of doing so is by looking at Usenet traffic, which is a major method of bulletin-board-like Internet communication. While Usenet traffic is only a small portion of the overall number of conversations about TiVo (some sites have hundreds of thousands of posts) it has the advantage of being accessible. Since Usenet, and, indeed, Internet conversations in general, tend to attract the highly technical, we would expect to find an over-representation of the parasitic community among these users. Even so, a general picture of the size of the TiVo parasitic community emerges in Figure 5, below.

With the exception of two periods, the second half of 2001 and the first half of 2002, the number of posts that were parasitic (that mentioned the common term for parasitic TiVo innovation, "TiVo hack") versus all posts regarding TiVo was around 5%. The numbers skyrocketed in from July of 2001 through July of 2002, but that seems to be due to the way that Google News, the source of this data, dealt with the addition of new, TiVo-specific groups to Usenet. In general, evidence suggests that we would expect that the 5% number would be approximately correct, even for these periods.

Figure 5

Time								
	2000 H1	**2000 H2**	**2001 H1**	**2001 H2**	**2002 H1**	**2002 H2**	**2003 H1**	**2003 H2**
TiVo Subscribers	44,000	130,000	240,000	380,000	466,000	624,000	700,000	1,300,000
Posts	12,200	17,000	22,900	27400	42,200	128,000	136,000	141,000
Parasite Posts	195	870	1780	3730	5400	6450	7160	8060
Percent of posts that were Parasitic	2%	5%	8%	14%	13%	5%	5%	6%

Data from Google Groups search of Usenet. TiVo subscriber numbers from company press releases and filings

The constancy of the 5% number is interesting, since it connects with other anecdotal evidence about the numbers of people engaged in permitted, non-pirate, non-underground parasitic innovation. For example, Will Wright, creator of the popular game *The Sims* has a rule of thumb that 5% or less of a game's audience will create their own content.[42] Regardless of the general applicability of the 5% figure, a second interesting result is that the size of the user innovation community did not substantively change over the exponential expansion of the general TiVo user base. Early adopters did not seem in general to be any more interested in hacking, nor did the importance of hacking fade as more users entered the system.

Despite the rapid growth of the community, and the constancy of the proportion of would-be hackers, the warm feelings between parasitic innovators and TiVo have the

[42] Game Developers Conference 2004, "User Created Content: Is It Worth It?" Roundtable, March 24, 2004.

effect of actually aligning the usually rambunctious community with the needs of the company. In fact, the TiVo community has become self-policing as the parasitic community actively enforces limitations on innovation that might harm the company. TiVo has two major types of exposure to danger from the parasitic community – threats to its business model and threats to its legal standing. The TiVo business model requires a monthly subscription to its central information service and the company is in constant legal jeopardy from television networks concerned about the ability of customers to skip commercials. Pirate innovators would clearly have incentive to find ways around the monthly subscription fee, and the utility of TiVo to many innovators would be greatly increased if it were modified to better skip commercials, transmit copied programs over the Internet, and otherwise commit violations of the Digital Millenium Copyright Act.

Interestingly, neither of these potential pirate innovations has become widespread. This has been thanks not to actions of the company, but rather to the policing of users themselves. The largest TiVo hacking site (along with smaller ones) has banned discussion of "video extraction" or copying of saved programs, as well as conversation about ways of getting around the subscription service. This sort of policing has been voluntary, as the board moderator of the largest site explained: "Please note that we wish for the topic of TiVo video extraction to be dropped on this site at this time. It raises too many concerns for this forum, and we wish not to be a part of it or have it here. TiVo had no say in why we did this and did not tell us to pull anything."[43] Some of this reaction is due to legal concerns, and some due to fear of a crackdown on boards discussing these topics, but the major reason seems to be a desire to shield TiVo from MPAA-like

[43] Donahue, Anne. "TiVo Hacking Cut Short," *Video Business*, June 25. 2001. p. 37

attention. This sort of self-policing is quite vigorous, even for those who have legitimate goals, as one TiVo hacker complains:

> I've been reading the TiVo community boards for a couple years now, and early pioneered hacks weren't often welcomed. I can remember when someone started doing the very earliest hack to allow an ethernet card to be attached. Many on the TiVo boards assumed the ethernet connection was to either extract movies for pirating on the internet, or for downloading show data from the internet instead of paying TiVo. Granted, the TiVo community does have some no-no subjects, and I can completely understand why they don't like anyone talking about getting around their $12.95 monthly service charge, but oftentimes other basic hacking projects fall into the "this is taboo to talk about" category.[44]

Of course, there are still a large number of underground, pirate sites where such material is discussed, but the mainline TiVo hackers have succeeded in surpressing a surprisingly large amount of material. The result has been a parasitic community tightly aligned with the company with which it works.

The parasitic community has created products of real value to both TiVo and the TiVo community. For example, the company Weak Knees now sells hard drive upgrades for TiVo that are enabled by techniques taken directly from the online parasitic community. They have already upgraded 100,000 TiVos, or approximately 10% of the total number of TiVos on the market - a phenomenal achievement since the upgrades are priced at $150-$350 a piece.[45] Clearly, the TiVo community shows that parasitic innovators can develop true innovation.

---

[44] Haughly, Matt. "Video Extraction and Tivo," *PVR Blog* (online), August 2, 2003. http://pvr.blogs.com/pvr/2003/08/video_extractio.html

[45] Diaz, Sam, "Add-on Kit Boosts TiVo Storage," *San Jose Mercury News*, January 26, 2004.

Corporate Response to Parasitic Innovations

TiVo has taken a fairly clever approach to its parasitic innovators. Unlike the tactics the game industry has used with modders, TiVo has chosen not to fully embrace its parasitic community. As one executive of ReplayTV, another PVR company with a policy like TiVo's, but more willing to speak on the record, stated, ""As long as people are only affecting themselves and accepting the potential risks, it's not a big deal to us."[46] In keeping with its unstated policy, TiVo provides no information, toolkits, or other help to those who would hack the system. The result is plausible deniability, most probably for legal reasons, as amateur hackers find ways to skip commercials using the device, and engage in other potentially dubious practices. This increases the value of TiVo, as its customers engage in the development that TiVo can't or won't do on its own, but which the company finds useful.

Tivo, then, is harnessing parasitic innovation by keeping the option to brand the community as pirates at any time. This position is ultimately dangerous, however, as parasitic communities can lash back when they feel betrayed. In the meantime, however, the community remains an interesting final case of parasitic innovation: a self-policing, non-pirate, non-underground example.

Conclusion

These cases represent a number of branches of a single source community, begun with phreakers, continued by hackers, and spread into various fields, legitimate and pirate, by

[46] Savetz, Kevin. "Hackers Channel Talents Toward TiVo, ReplayTV Video Recorders." *Knight Ridder Business* News, March 22, 2001.

PAGES (S) MISSING FROM ORIGINAL

CHAPTER TWO:
HOW PARASITIC COMMUNITIES WORK

The cases of parasitic innovation in the previous chapter provide an outline of the wide variety of different technology systems, time periods, and communities involved in the parasitic innovation phenomenon. For all of the differences between the communities, however, their similarities are much more compelling, and can yield clues as to how parasitic communities work in general The previous chapter discussed the output of various communities, leaving open the larger questions of methods and motivations. The methods of parasitic innovators in both building communities and sharing information are similar across all five groups studied, and provide clues into the success of communities as innovators, why parasitic communities are stable, and why they are difficult to contain. After examining these methods, this chapter will address the motives of parasitic innovators, which are shared to a remarkable degree, across the full range of communities. Understanding methods and motivation will then allow the development of practical theories on the nature of parasitic innovation.

Community Building and Information Sharing

This section will first examine the two key elements of parasitic communities that make them both self-sustaining and difficult to contain: information-sharing and community-building. Community-building turns individual parasitic users into a coherent group, giving them a common ethos and making it difficult for companies to react to a single

user without dealing with the community as a whole. Information-sharing mechanisms ensure that "secret" knowledge is quickly disseminated, making it impossible for firms to stop the flow of proprietary data and potentially damaging techniques. Together, these key aspects are what make parasitic communities both successful and threatening, and they show a remarkable degree of similarity across the communities examined.

While this chapter will later take up the issue of parasitic user motivations in more detail, the production and exchange of information is one of the highest ideals of all parasitic communities. Indeed, parasitic users of all types seem to have a common, almost obsessive, desire to tell insiders what they know. This sharing is the way users get recognized for their work, the way they discover new techniques, part of the "hacker" mentality, and in many cases stems from a genuine desire to teach. One of the first phreakers, Mark Bernay, traveled up and down the West Coast in the 1960s, putting stickers on phones outside high schools and colleges that told people to call a toll-free loopback pair if they wanted to hear something interesting. On the other part of the pair, he had a recording that gave callers information on how to find loopback pairs and other phreaking information.[47] This sort of driving desire to tell others about forbidden knowledge did not end with Bernay, however. As Bruce Sterling wrote, "Many hackers even suffer from a strange desire to *teach*— to spread the ethos and knowledge of the digital underground. They'll do this even when it gains them no particular advantage and presents a grave personal risk."[48] Parasitic users go further than their personal desire to

[47] Esquire, p. 124.
[48] Sterling, Bruce. *The Hacker Crackdown*, 1993. p. 58. Italics in original

share knowledge; like scientists, phreakers also believe in free exchange of information in general.

In the original underground parasitic movements, such as those of phreakers and hackers, information exchange and community were initially intimately tied together – if you could get access to the information, you were part of the cognoscenti in the underground environment. This created a small, relatively tight-knit group of pirate innovators.

In order to effectively communicate information, phreakers needed some method of talking with one another. Pursued by Bell, much of the history of phreaks has been the story of the search for places to discuss techniques and ideas relating to their "art." The most popular of these was finding ways to create secret party lines within the phone system where conferences could be held. The most famous of these went on for months in the 1970s, the lines always occupied by at least a few phreakers who had blue boxed themselves to the conference.[49] This method proved unsatisfactory in the long-run, however, as phreakers had no real control over conference lines, which could be shut off without notice. In addition, phone phreaks felt that conferences could be monitored by Bell, a fear that made conferences less than ideal.

The Printed Journal

The next stage in the spread of phone information was the printed journal. The first of these, the *Youth International Party Line*, or *YIPL,* was established in 1971, by Abbie Hoffman and someone calling himself Al Bell. As an offshoot of Hoffman's political

[49] Esquire, p. 125.

YIPPIE movement, *YIPL* was written with a political bent. The introduction (written in the shape of a bell) to the first issue read, "YIPL believes that education alone cannot affect the System, but education can be an invaluable tool for those willing to use it. Specifically, YIPL will show you why something must be done immediately in regard, of course, to the improper control of the communication in this country by none other than the BELL TELEPHONE COMPANY."[50] Articles in the early *YIPL* mixed politics and technology, the earliest example of what would be called "hactivism."

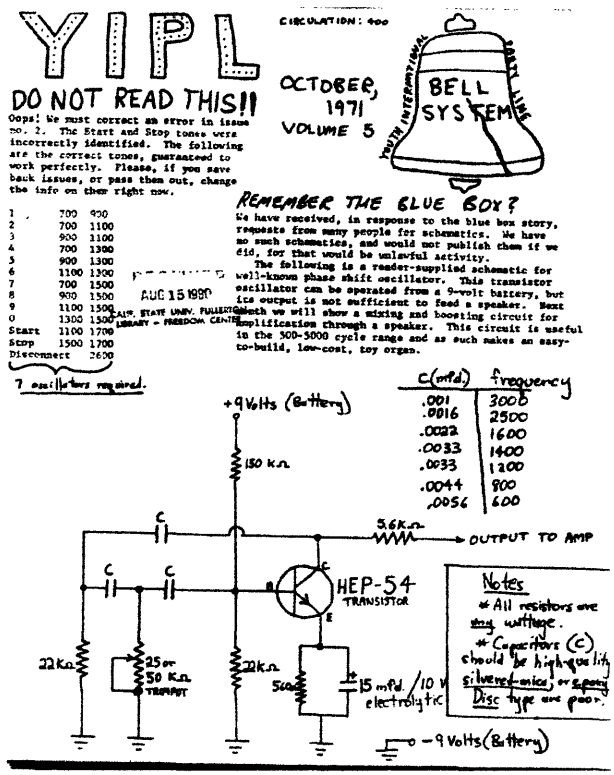

Figure 6: The First Issue of YIPL

Soon, however, Bell and Hoffman disagreed over the contents of *YIPL*, as Hoffman was dismayed by the technical, rather than political, nature of the magazine. As a result, in

[50] Anonymous, *Youth International Party Line,* Issue #1, 1971.

1973, Al Bell abandoned *YIPL* to found his own technical journal— *TAP*, the *Technological Assistance Program*. *TAP* was the leading source of phreaker information, providing everything from technical documents to the phone number for the Kremlin. *TAP* was written in a very technical and almost scientific style, probably either in homage to *The Bell System Technical Journal,* or in mockery of it. It remained at the center of phreaker affairs until 1983, when the home of the editor, then someone called Tom Edison, was burned and robbed by unknown criminals. Amid speculation that the phone company was at fault, *TAP* printed its final issue soon after, although it has been revived on a few occasions since.[51]

With *TAP* gone, the leading print journal became *2600, The Hacker Quarterly*, published continuously since 1984. With its back cover carrying loving photographs of pay phones from around the world, *2600*, is the journal of record for the pirate innovation community. Available on newsstands, *2600* has moved from its purely phreaker roots and demonstrates the holistic nature of the pirate innovation community. Current issues cover the full range of pirate innovations developed over the past twenty years, from hacking to exploiting the McDonald's WiFi computer network. And, as previously discussed, *2600* was taken to court over the DeCSS code. The importance of magazines such as *2600* began to fade, however, with the birth of electronic communications.

BBSes

By the time of the death of *TAP*, a new method of phreaker communication had risen to become the primary means of exchanging information. A Bulletin Board System or

[51] Haffner, Katie. *Cyberpunk*, 1995. p. 22.

BBS, is a computer, equipped with a modem and specialized software, which allows other users with modems to reach it remotely. Once on a BBS, users can exchange papers or programs, write electronic mail, or play online games. Best of all from the pirate innovators' perspectives, almost anyone with a computer and a modem can run their own BBS.

Bulletin Boards began springing up around the nation; by 1985, there were around 4,000, and, by 1990, over 30,000 BBSes existed in the United States alone.[52] Of course, only a fraction of these were devoted to parasitic innovation, but, even so, it is clear that BBSes brought about a new era of underground communication. Now, phreakers and early hackers could talk to each other *en masse*, as information sent to or "uploaded" onto one board would often be quickly copied to others. As a result, the discoveries of individual pirate innovators could be acted on by the community as a whole.

The primary way in which information is transferred on BBSes is through "philes." A phile, the peculiar phreaker spelling of file, is a text document containing information useful to hackers. Much of this material, is, of course, often of dubious value, but among all of the philes being uploaded to BBSes, there is a remarkable number that show impressive amounts of research and effort, and almost all have to do with parastic, primarily pirate parasitic, innovation. One partially complete site lists 2,229 original text philes related to phreaking alone, including 157 devoted purely to introductions to the

[52] Sterling, Bruce. *The Hacker Crackdown*, 1993. p. 69

field.[53] This does not count compilations, online articles from underground magazines, or other similar material – an astonishing output from an underground community.

These types of philes fall into four different categories. First, there are entire technical articles from Bell Labs or other research institutions that are patiently retyped and uploaded, often with extensive, intelligent commentary. An example of this sort of work is an anonymous electronic phile on caller ID. Not only did the author copy an entire Bell technical specifications sheet, but also apparently has a good understanding of it, to the point where he corrects a possible typo in the sheet by writing "I have copied this data as presented. I believe the transmission level is meant to be -13.5 dBm," instead of the 13.5 dBm given in the text.[54] These technical articles are closely related to the second major category of philes, those that contain the complete texts of long articles written on subjects of interests to phreakers and underground innovators, such as the 1971 Esquire article.[55]

Third, there are philes that contain original findings, such as circuit diagrams for new devices, descriptions of particular techniques or lists of specialized phone numbers that a phreaker has discovered. These sorts of highly technical articles are the key to the reason why parasitic communities are progressive, building on previous works. Some of these technical philes become classics, revised and updated like popular text books for over a

[53] Scott, Jason. *TEXTFILES*, [online: web] URL: www.textfiles.com, revised December 3, 2003.
[54] Anonymous, "Specs on Caller ID," *Empire Times zine*, July 10, 1992, http://www.flashback.se/archive/EMPTIME2.TXT.
[55] One Farad Cap,/AAG typed version of "Secrets of the Little Blue Box," in the *Phreaker's Manual.*

decade. Bioc Agent 003's seven part "Course in Basic Telecommunications," for example, is many pages in length and covers a vast range of phreaker topics.

The number of original philes reflects the fact that, in order for a phreaker to demonstrate his skill, he needs to produce information that has never been seen before, and it needs to stand up to the approval of his peers. Thus, the first person to accomplish a difficult task will be accorded respect in proportion to the crack's difficulty. Bruce Sterling explains it in this manner, "The way to win a solid reputation in the underground is by telling other hackers things that could have been learned only by exceptional cunning and stealth."[56] Being the first to do things is the best way to prove oneself to other phreakers.

The stress on being original is clear from the way philes are written. Usually, they prominently feature the name of the author, along with the name of the BBS or group to which they belong. Additionally, phreaker publications emphasize original documents. *The Legion of Doom Technical Journal*, for example, has very strict editorial standards, especially for an underground publication, as it says in its introduction:

> The articles contained herein, are totally original unless otherwise stated. All sources of information for a specific article is [sic] listed in the introduction or conclusion of the article. We will not accept any articles that are unoriginal, plagiarized, or contain invalid or false information[57].

If a phreaker wishes to get published, and see his name listed on many BBSs, he needs to do original, and interesting, research.

---

[56] Sterling, p. 59

[57] Various, *Legion of Doom Technical Journal*, Volume 1, Jan 1, 1987. [online: Web] URL: http://www.textfiles.com/magazines/LOD/lod-1

Besides technical information, philes serve the purpose of cementing community. Especially in the early days of phreaking, information-sharing and community-building went hand-in-hand. That is why the final type of philes were those that contained information on the status of fellow phreakers and BBSs, which serve to keep the community aware of arrests, the closing of BBSs, and retirements.[58] Like much else in the phreaker world, these were voluminous in detail, with elaborate minutes being kept of underground meetings, and hundreds of messages from various phreaker groups in some philes.

In addition to philes uploaded individually to BBSs, the paper hacker publications were converted to digital form with issues that compile the most useful philes. Generally, they are run by a few innovators who serve as editors, in the manner of editors of scientific journals, sifting through large number of philes to pick out and publish a few articles. Outside of publications like *Phrack and 2600*, other publications are produced by exclusive groups of accomplished hackers and uploaded to elite phreaker BBSs. Among these are colorfully-named organizations like the Cult of the Dead Cow, the Phreaks Against Geeks, and the infamous Legion of Doom. One site, containing an incomplete collection of these publications, listed 27 different group journals and magazines all dealing with phreaking.

What worked for phreakers, as might be expected, worked just as well for hackers. The two communities grew from each other, so philes about phreaking and hacking coexisted.

[58] See, for example, the Phreak World News, in every issue of *Phrack*.

The transition between the two communities was thus quite smooth, and it is unsurprising that both shared common characteristics, including a similar sense of ethics and a common paranoid worldview. More visibly, the phreaker language, with its substitutions of 3 for e, + for t, and odd misspelling continues today, making 3133+ (elite) a common expression for the best hackers. As computers got more interesting, and BBSs slowly gave way to newsgroups and the early Internet, the balance shifted from mostly phreakers to mostly hackers.

Before examining the next phase of information-sharing, however, it is worth examining the interconnectedness of information-sharing and community building in these early underground, pirate communities. The means of information-sharing itself shaped the nature of the community for phreakers and early hackers. The result was something similar to the way the scientific community works today – if you were educated enough to understand the material and work with it, you were part of the community and expected to share in its information exchange. As one phreaker wrote of the sharing of credit card codes:

> [The BBS members] introduced me to codez, illicit calling card codes which were stolen and then used to make free long distance phone calls. Thanks to the codez, I was able to maintain an active, nationwide presence on various BBSes. I became sort of addicted to codes, which normally did not last long because you shared all your codes with your online buddies, who would use them so much that the long distance service provider (I preferred Sprint) would get wise and shut them down a day and a half later.[59]

The incentives were similar to those of the world of science as well, where original published research brought reputations and rewards. Innovators who become famous (or

[59] "Scott," *BBS Life in the 1980s*, March 2000. Available at http://www.textfiles.com/history/golnar.txt

infamous) are more likely to be invited to join prestigious groups, be invited to hacker or phreaker gatherings and parties, and be adored by the next generation of innovators.

Early hackers and phreakers tended to gather together in groups based around particular BBSes, with group membership based on prestige. These groups became the social filters, the source of many of the published electronic magazines, and the unofficial research institutions of the parasitic world. They also occasionally acted like the teenage boys they often were, engaging in "wars," with various groups hacking each other's computers and trying to outdo the other's feats. One of the most famous of these wars, between the Legion of Doom and the Masters of Deception, ended up with a federal crackdown and substantial jail time for the people involved.[60]

In the BBS world, all community-building was very direct, whether among individuals or groups. Many BBSs carried some philes, but the "best" BBSs for hackers and phreakers were underground, and required a user to prove his or her worth before being given access. This was done either by sharing new, original philes or by convincing some more senior member of the community of the worth of the applicant. An example of the kind of tests and forms that were occasionally required of applicants to join groups or prove their worth can be found in Appendix B. Getting access to the deeper levels of the community was a relatively slow process, acting as a further filter on new members to the community. Information depended on building community connections. BBSes were intensely local, as they were reached by dial-up connection, resulting in a hierarchical

[60] "Hackers: Angels and Outlaws," documentary on TLC. Online transcripts and information can be found at: http://tlc.discovery.com/convergence/hackers/articles

system where the best regional user innovators were filtered through the best regional BBSes, leaving a small, elite community at the national level. Community-building and information-sharing were thus intimately connected.

The Internet

As can be seen in Figure 7, BBSes were in the upswing of an exponential growth curve until 1993. Not coincidentally, 1993 was the year that NCSA Mosaic, the first browser was launched, and the World Wide Web was born. The fading phreaker community and burgeoning hacker community took naturally to this new medium. In addition to these existing underground parasitic communities, the accessibility of the Internet would bring together new types of parasitic communities due to the greater ease of communication over the old BBSes.

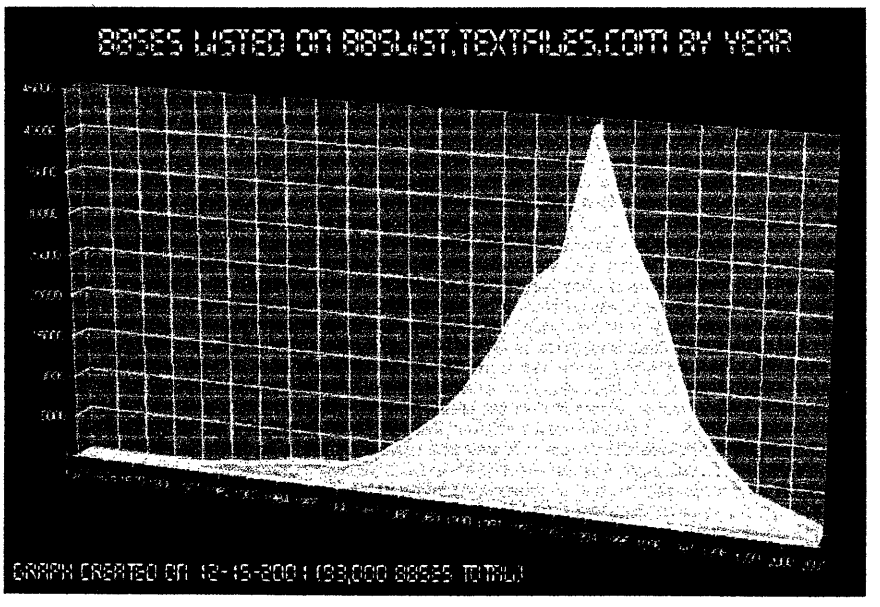

Figure 7: BBSes Listed on Textfiles.com

Not surprisingly, hackers, whose interest in computer networks predisposed them to an interest in such matters, used the full range of communications options made available over the Internet. Originally, they simply echoed some of the original infrastructure of the familiar BBSes, using mailing lists, FTP sites, and newsgroups to continue the sorts of discussion and file-trading originally conducted through dial-up modems. The nature of the Internet as a less local and therefore broader medium soon began to have an effect on the original underground communities.

Where previously hacker and phreaker groups were relatively local (The "414" which broke into Sloan-Kettering and Los Alamos took their name from the Milwaukee area code), the Internet opened the doors wider. Ironically, information was almost too free – it was too easy to get philes and too easy to enter the hacking world. One hacker describes it as follows:

> The Internet made everything that was once so hard to obtain so easy. IRC, email, ftp and webpages all open to Joe public. And in 1994 they flooded in, drove after drove causing great despair among the many old schoolers. Many of these people didn't appreciate their turf being overrun by these so-called lamers, so they closed their doors. While the old doors closed new doors opened, newsgroups, top100 web pages, anonymous ftp and the most infamous of all IRC offer channels.[61]

With barriers to information lowered, a lack of localization that made progress slow, and with the lack of mentor figures of older BBS members, the result was a partial dispersion of the hacker community. A few of the world-class innovators became the "elite," and they had a new audience, the "kiddies" who took techniques developed by elites and used

[61] Ipiggi, "A History of the Scene," April 10, 1999. Available at http://www.textfiles.com/piracy/thescene.txt

them for their own purposes without creating anything new. In the next chapter, we will discuss the elites and kiddies in more detail.

Even as the larger hacker and phreaker communities began to change, the Internet enabled other parasitic communities to use the tools previously only available to phreakers and hackers, gathering together in a way that multiplied their size and effect. Of these communities, both game modders and mod chip makers had roots in the phreaker and hacker world, and the others were heavily influenced by the early pirates, even if they were not always aware of their debt.

Community-building and information-sharing in the modding community, for example, is similar to that of the late-stage phreaker community – the computer bulletin board, or, more commonly recently, the Internet website. Each game has its own series of websites built by modders, each with its own discussion boards, download sites, and documentation. Some even have minute-by-minute breaking news about the game, where any review, designer interview, or new mod is instantly posted and discussed. Official websites of game designers sometimes incorporate these features as well, but they are often overshadowed by these unofficial "fan" sites.

The discussion boards and forums on these sites is where most cooperative innovation occurs, with people posting questions, answers, and individual mods. Since the modding community has essentially accepted as its norms that mods must be distributed for free, there is a high degree of reciprocity and free user assistance on the online forums, in a

way very similar to that identified by Lakhani and von Hippel.[62] In fact, this reciprocity was identified in informal surveys as a key in driving development of new mods:

> It is also nice to distribute your work for free because then others can add to it and release something even better. If everyone started charging for or not releasing their work we would have very small useless scenarios but if you can instantly get 90 new resources for your mod and use them for free you can create something great in less time.

Even with all of this information sharing, competition for respect and recognition can be brutal. Most sites have elaborate voting systems where each mod is rated and critiqued publicly, with only the most highly-rated receiving widespread distribution. Even further, meta-sites rank individual mod sites, identifying those with the best overall mods and forums.

Some of the same techniques carry into the communities without any basis in pirate or underground innovation. TiVo hackers, for example, gravitate around one or two major online discussion groups whose archives serve as repositories for knowledge in the way phreakers used philes. Users are expected to search the archives before posting questions or be treated to a harsh response from the board regulars. Even in this non-underground, non-pirate community, however, the information-sharing and community-building aspects harken back to the hackers and phreakers. In one example, a board member complains that he was not invited to participate in discussions about a particular technical project until he proved himself:

---

[62] Lakhani, Karim and Eric von Hippel, "How Open Source Software Works," *Research Polic,y* 1451 (2002) 1–21

> ... I also had never seen any source or discussion of successfully divorcing drives. I didn't even get an invitation to this "elite little club" until after I already had a fully working "mls" program.[63]

Echoes of the same processes can be found in other parasitic and non-parasitic communities, including the entirely aboveground open source community.

Commonalities

Regardless of the information sharing or technology used for communication in a parasitic community, some clear commonalities emerge. First, all of the parasitic communities place a tremendous value on information itself. Documentation is meticulous, as individual parasitic innovators record and publish massive amounts of information. Archives are maintained, in the case of some phreaker material, for over a quarter century, in informal ways, but it is rare to see documentation disappear. Part of this is due to the ethos of paranoia of many of the innovators, and ethic of back-up and redundancy that can only be learned by observing the fragility of the systems upon which they innovate, and which legitimate companies are just now beginning to adopt with the same fervor. Another reason is the desire for personal fame and recognition.

That same desire drives the second distinctive feature of all information-sharing by parasitic communities: the existence of mechanisms for peer-review, to separate out the good contributions from the chaff. In the early print and BBS days, this was done by individual editors or board operators, along with a regard for reputation, much as is currently done with scientific journals. Later, in the Internet era, elaborate reputational

[63] Tiger, Tivo Community Boards, post dated 4/15/04.

and computerized systems were added to the human component – message and mod rating systems, message board counters, administrative privileges, and webzine editors all became methods for selecting and propagating "good" work. This similarly creates and cements a community around this sort of good output, and reduces free-riding by making sure that those who play fair are identified.[64]

Finally, and perhaps most importantly, these two elements combine to make the communities bear a striking resemblance to scientific communities. This is clear not just from the pseudo-scientific jargon and imitated style of parasitic journals (these are, after all, people who truly see scientists as heroes), but also from their actions. Laura Koetzle, security analyst at Gartner, recognized this as well, stating specifically of hackers and phreakers that "This is a scientific process, it is uglier and has less glitz, but it is still scientific process. [In science, you] are only as good as the things you have published and the things that you have discovered, it works exactly the same way in this community."[65]

The combination of peer review and published records of experimentation has strong elements that are empirically progressive, in a Lakatosian view of science[66]. This makes sense if we define parasitic innovators as explorers in the same way physicists are – they are faced with a black box of a closed system (for phreakers, the Bell System, for physicists, the universe) and through experiment and theory develop a scientific

---

[64] See, for example. Takahashi, N. (2000). The Emergence of Generalized Exchange. *American Journal of Sociology*, Vol. 105, Iss. 4 (January 2000), pp. 1105-1134.
[65] Koetzle, Laura. Interview with author. March 11, 2004.
[66] Riggs, Peter, *Whys and Ways of Science,* Melbourne University Press, 1992. pp 60-94. For original articles, see, for example, Lakatos, Imre. *Criticism and the Growth of Knowledge*, New York: Cambridge University Press, 1970.

understanding of how the system operates. A history of work with falsifiability, combined with a sort of peer review, ensures that each new approach as to how a particular parasitic system might work, each new view as to what is inside the black box of the system, has more empirical power than the previous approach. Thus, parasitic communities make progress in understanding a field, and that progress is shared through the various information distribution mechanisms. This is not to argue that parasitic communities would fit Lakatos's definition, or that of any other major sociologist of science. Rather it is that parasitic communities share some of the characteristics of a scientific, progressive endeavor, and from that comes their power in cracking large and complex systems.

If the communities, from an outside perspective, work in a way closer to scientists than criminals, the question of their motivations remains.

Community Motivations and the Elite-Kiddie Divide

Understanding user motivation is the key to understanding how parasitic communities interact with firms. If the community's desire is to defraud, as many firms believe, then there is obviously little that can be done to create better relations between parasite and host company. I will argue, however, that most true, "elite" innovators are driven by the desire to discover and innovate, rather than the end results of pirate behavior. The realization that users are willing to innovate for individual satisfaction and recognition, not just economic utility is not new, of course, as Raymond discusses it as one of the characteristics of open source. For parasitic innovation, the way in which these

motivations outweigh both potential punishment (and, indeed, are sometimes enhanced by it) and the nature of recognition and individual reward in the underground, without any potential economic utility, has not been discussed in the literature, however. Further, the fact that these motivations are similar across the full range of user communities provides additional evidence that parasitic innovation is a unified phenomenon.

Examining the questions of motivations in detail quickly becomes complicated, however, since it is often a function that is affected by the reaction of legitimate firms, the subject of the next chapter. For the purpose of exploring parasitic innovators as a potentially benevolent, or at least ambivalent, force, it is sufficient to establish that the original motivations of parasitic innovators, and especially pirate innovators, are not inherently directed at theft or damage of property. These motivations indeed may come into play, but, as will be argued, they are a reaction to firm behavior, not an original state. This model of motivations for user-innovators as shaped by interaction between firms and users is also not in the existing literature, and will be expanded upon in the following chapter. In this chapter, I will attempt to demonstrate that the motivations of parasitic innovators are not, *prima facie*, inherently counter to the economic interests of the firm.

The law and the companies targeted by parasitic innovations, however, view the situation differently. From the earliest days of the parasitic phreaker community, AT&T always believed that phreakers are primarily financially motivated: they crack the phone system in order to steal the company's only commodity, the phone call[67]. In the company's eyes, if the phreaker's motivations are more sophisticated, it is because some of them do not

[67] *New York Times*, 1973

commit fraud because they are poor, but rather because they like to steal. In the words of AT&T attorney H. W. Claming, people seem to enjoy "getting something for nothing."[68] This same view, in different forms, has been expressed to describe the motivations of other parasitic communities as well.

To some extent, these accusations are true, but only for a portion of the hacker community. A large number of people do use the techniques developed by parasitic innovators for financial or destructive reasons, and, in the example of the phreaker community, many of these stole from the phone company with criminal intent. Bookies, for example, often used blue boxes, and the related black boxes which prevented people calling you from being charged, as a cheap way of placing bets.

The result exposes a common fallacy among firms. Companies assume that all parasitic innovators share a common goal. In fact, parasitic innovation communities are hardly monolithic, and are in fact divided into many sub-communities by goal, methods, interest, and affiliation. While many of these sub-communities may be specific to the particular community, all communities studied show a separation between two key groups, the "Elite" and the "Kiddie." Elite is a term used within parasitic communities, dating from at least the late 1970s, for those who truly innovate – the wizards who understand the proprietary system and constantly cause it to do things its makers never intended. Kiddie is a more recent descriptor, short for "script kiddie," meaning one who does not truly understand a system, but merely uses tools created by the Elites in order to exploit the system in their own way.

---

[68] *New York Times*, 1978

At first this might seem like a natural divide between experts who develop products and users who consume them, the difference between mechanics and those who drive cars. The Elite-Kiddie separation is more complicated, however. In a world where the heroes are essentially lauded for their intellectual or engineering achievements, such as parasitic communities, Elite status comes from achievement, combining aspects of both expert and rock star for aspiring Kiddies. Elites jealously guard their status and personal reputation, and generally respect the status of other Elites, if fairly earned – though they often engage in elaborate, puerile "wars" about which particular innovator is better than the other, and denigrate the skills of their rivals. Their status generally comes from original work, not from pranks or thefts, indicating a scientific bent to their motivations.

It is easy to establish that Elites are not primarily interested in parasitic innovation for the sake of theft. The economics of Elitedom just do not make rational sense and most pirate innovators do not really need the benefits that they acquire through parasitic innovation. A majority of Elite parasitic innovators live at home or in college dorms, supported by their parents.[69] If they do not, these innovators usually have normal day jobs, and play the role of hacker during their time off. Parasitic innovation, no matter how seriously it is taken, is a hobby. This has some advantages over a traditional corporate approach to innovation, where risk and reward must be carefully balanced. Parasitic innovators face no such restraint, which is precisely why they can spend so much time attempting to

[69] For demographics of the hacking community specifically, see Schell, Dodge, *The Hacking of America.* p 110.

perform unremunerated tasks, like spending hundreds of hours trying to guess the password of a computer system.

The lack of financial motivation is further evidenced by the fact that Elites do not seem to change their spending patterns for the technology upon which they innovate. Elite phreakers do not substantially change their paid phone use as a result of phreaking, nor do TiVo hackers use modifications that allow them to not pay monthly fees to TiVo.[70] The time and effort required to innovate far outweighs the actual value of the goods or services available, bringing parasitic user innovation closer to a hobby than anything else. Additionally, Elites tend to freely share information, destroying the potential for profit from their discoveries, and also often encouraging manufacturers to close exploits found by Elites.

Theft is not the key motivation for Elites. A personal sense of exploration, however, is. Exploration is different from creation, involving finding interesting facts about existing systems, rather than creating systems themselves. Parasitic innovators generally do not like creating as much as they like discovering, and the type of discovery that drives them most is discoveries within existing systems, preferably laced with a bit of danger and exhilaration – exploration in an almost Victorian sense. Elite parasitic innovators are aware of their own motivation. As Dildog, a well-known hacker who was part of the Cult of the Dead Cow hacking group, told the author, "I'm a synthesis addict. I like to find things, and the reward is worth the hunt. Sometimes, I will spend an extra few minutes

[70] "If you were to have examined my phone bill, it was virtually unchanged. My average bill was about $70 a month, and has not significantly dropped because of this discovery, and my attorney made it a point to mention that at the court hearing." Interview with Jon Draper, Ravenmatrix, July 27, 2002.

randomly poking at stuff just because there is the possibility of discovering – just searching and finding."[71]

Variations of the central exploration theme abound. For example, Control-C, a notorious phreak and hacker who worked for Michigan Bell after being caught by the Secret Service, defined hackers in terms of learning:

> The purpose of hacking is to learn. Learn the way a computer system runs. Learn how the telephone switching systems work. Learn how a packet switching network works. It's not to destroy things or make other peoples lives a mess by deleting all the work they did for the past week. The reason the Department of Justice has crackdowns on computer hackers is because so many of them are destructive. That's just stupid criminal behavior and I hope they all get busted. They shouldn't be around. You give real hackers a bad name.[72]

Desire to discover the beauty in complex systems is another common reason given by Elites, as a 17-year-old phreak just starting in 1997 stated:

> The reason I'm interested isn't for getting free phone calls or the sense of power you get from being able to outsmart a big corporation. It's mainly because there's so much knowledge just hidden from you, knowledge that you would never think to look for. There's beauty in the way things work. We're just blinded to it by the fact people don't want to tell us. [73]

Even groups whose parasitic innovation serves no purpose other than destruction, like computer virus writers, most often do not set the virii free, instead viewing creating them as a challenge, a way of discovering new ways to make a system perform in unexpected ways.[74]

---

[71] Interview with author
[72] Anonymous. "Interview with Control-C," Phreak, March 30, 1994
[73] Greg Nesteroff, BCIT Link, Canadian University Press, 1997
[74] Thomson, Clive. "The Virus Underground" *New York Times Magazine.* February 08, 2004.

The joy of discovery is common even among parasitic innovators that are neither underground, nor pirates. In informal surveys, modders overwhelmingly discussed the fun of what they were doing as a primary motivation:

> I like to mod things, I feel that my mod that is under way will give great joy to myself and others. I probably won't work with games in the future, but who the heck knows. Conclusion, I'm doing it because it's fun.
>
> The reason I mod things is to make the game more enjoyable. I do it mainly for my own pleasure, but sharing it with the rest of the community for others to enjoy too comes alongside naturally.

For pirate communities, this sense of the thrill of exploration is often further enhanced by the perceived danger of being a pirate, and in the sense of power that hacking into a secure system provides. Especially given that many pirate parasitic innovators are in their mid-teens to early twenties, the joy of pirate innovators goes beyond the usual thrill of innovation in more mature communities, and is at least partially an attempt to rebel or stand out in some way. Perhaps this is because the infamy one can achieve as a hacker or phreaker is unavailable to its members outside the community, where parasitic innovators' technical skills have less social impact. Pirate innovators thus often see themselves as pioneers, fighting against the oppressive powers that control the electronic frontiers. This sort of perspective tends to lead to almost megalomaniacal statements, like those of "The Mentor": "Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for."[75] This sort of bombast is very common among younger underground, pirate Elites, and is probably a

[75] Mentor, "Hacker Manifesto," Phrack #7, phile 3, January 8, 1986.

contributing factor for why many firms dismiss pirate innovators as disaffected teenagers out to vandalize, rather than as serious innovators.

If curiosity is one of the prime motivations of Elites, it is not the only one. Like open-source programmers, many Elites are indeed interested in recognition they receive from others in their communities. This search for recognition as one of the best provides a reward for innovation, just as it does in the open source movement discussed by Raymond and in experiments by Fisher and Ackerman.[76] The elaborate citation methods used in philes have already been discussed, and underground communities are extremely serious about playing up this perceived importance. This announcement by a game cracking group offers an example of how parasitic communities recognize achievement, "Once in a great while NTA extends a very exclusive invitation .... With that we honor the following traders & extend this rare invitation to the oldest and most respected, of Elite Groups on the Scene. [The right to use a /=RiSc= after a hackers name] denotes and carries unequaled distinction among our community and deserves the highest respect that it carries!"[77]

Emphasizing the importance of credit is perhaps my favorite quote from a piece of pirated material, in which Tyranny, a pirate who mods computers games so that they can be copied, complains about his trademark being stolen by another pirating group, Napalm:

---

[76] Fisher, R. J. and Ackerman, D., "The effects of recognition and group need on volunteerism: A social norm perspective," *Journal of Consumer Research*, 25(3), 262-275, 1998.
[77] Week in Warez Newsletter, July 30, 1995.

> At the bottom of their current NFO [A file taking credit for a particular pirated piece of software] there is a line stating Uncopyright (u) Napalm '96. Wow... That line has been my personal trademark for a very long time now, and I do not appreciate upstart newbie groups using it without my consent. Now this may not seem a big deal to many of you, but I seriously cannot think of a dumber thing to do than "pirate" someone else's line.[78]

Credit serves as both a reward in itself and as a way of separating oneself from the vast majority of the parasitic innovation community, the Kiddies. Kiddies provide a much larger group, with a much wider spread of possible motivations. Some are pure vandals, while others are aspiring Elites. Dildog described the motivation of these Elites-in-training:

> Driven by a sense of awe, they are generally people who discovered the hacker the community before they discovered the art of hacking, and are in the community long before they deserve to be. As they are underdogs, they have to pick up the pieces because they are not as cool as a big hacker. Every good hacker had to be a Kiddie first because that it what research is.[79]

These Kiddies are responsible for the vast majority of hacking damage, usually as a side effect of their relative inexperience. They are also more likely to be caught, and more likely to serve as examples of the nature of the parasite community.

The situation is more complicated than this Elites vs. Kiddies divide would indicate, however. Elites use the Kiddie community for their own purposes, allowing them to actually use the techniques created by the Elites in order to gain more attention to the Elite's work. Thus, writers of computer viruses will almost never themselves release a

---

[78] Tyranny, NFO for pirated copy of Backlash, available at http://www.textfiles.com/piracy/flame05.txt
[79] Interview

virus, but will post the code for one online, where Kiddies will often find it and set it free. Similarly, Elite hackers will often create a software package exploiting security flaws, and then make the software available for any Kiddie to use. This absolves the Elites of direct guilt, but still insures that their "beautiful discoveries" will become known to the world. Elites seem to not see this as making them in any part responsible for the crimes of Kiddies, often citing free speech as a reason for posting instructions for exploiting their discoveries.

Despite this symbiosis, Elites and Kiddies clearly have different motivations. Elites are truly driven by discovery, not theft. What determines how they will apply their skills, however, is not just their motivation but also the way that they interact with the firms upon which they act as parasites.

CHAPTER THREE:
THE PARASITIC INNOVATION CYCLE

The previous two chapters have demonstrated how and why parasitic innovators attack proprietary systems. The missing variable for a complete analysis, however, is an understanding of the way firms approach parasitic innovation. Firms seem to build proprietary systems in three potential situations. The first instance occurs when the infrastructure investment required before a product is introduced is very large. In such cases, such as the building of a phone network, it is to the firm's advantage to maintain control of the system in order to make sure that the firm is able to reap the long-term revenues required to make its initial investment. In the second instance, the business model for a particular product makes such a system appealing, since a locked proprietary base system allows the creation of a stream of add-ons which can be sold to this existing customer base. This "add-on" approach has become increasingly common, both in the software industry, with its proprietary operating systems and standards, and in the hardware industry, which increasingly uses incompatible or customized interfaces to lock users into particular upgrade paths. Finally, firms build proprietary systems in order to maintain a secure monopoly over certain kinds of IP extrinsic to the proprietary system itself, as in the case of encrypted DVDs or secured computer operating systems. In any of the three cases, the initial incentive of manufacturers is to maintain complete control of their systems.

Given that the purpose of a proprietary system is to control a revenue stream, rather than generate a one-time purchase, it is clear that firms using that approach are incentivized to protect their systems. It is not surprising, then, that in none of the cases did firms actually plan for or desire the appearance of a parasitic community. Indeed, firms seemed absolutely unprepared for parasitic innovators to appear in the way that they did, and with the strength of purpose that each community exhibited. In every case, firms put some work into securing their proprietary systems, but none of them was adequately prepared for the challenge posed by these seemingly spontaneous parasitic communities. After a few product cycles, security usually tightened, but was never entirely successful in stopping parasites. A key conclusion about parasitic innovation, then, is that if a parasitic community finds a proprietary system particularly worth exploring, firms cannot control the manifestation of the community.

Thus, to develop a firm strategy we must start with the assumption that regardless of how firms secure their systems, parasitic innovators will discover them. The question becomes one of trying to develop better ways of dealing with existing parasitic communities, rather than avoiding their appearance. This is already a reversal of the standard procedure in dealing with parasitic communities, which is the attempt to build unbreakable systems, rather than expecting systems to be broken.

Given the existence of parasitic innovators, the cases provide a source of data from which a model of the typical lifespan of a parasitic innovation community can be developed. This parasitic lifecycle model is shown in Figure 8.

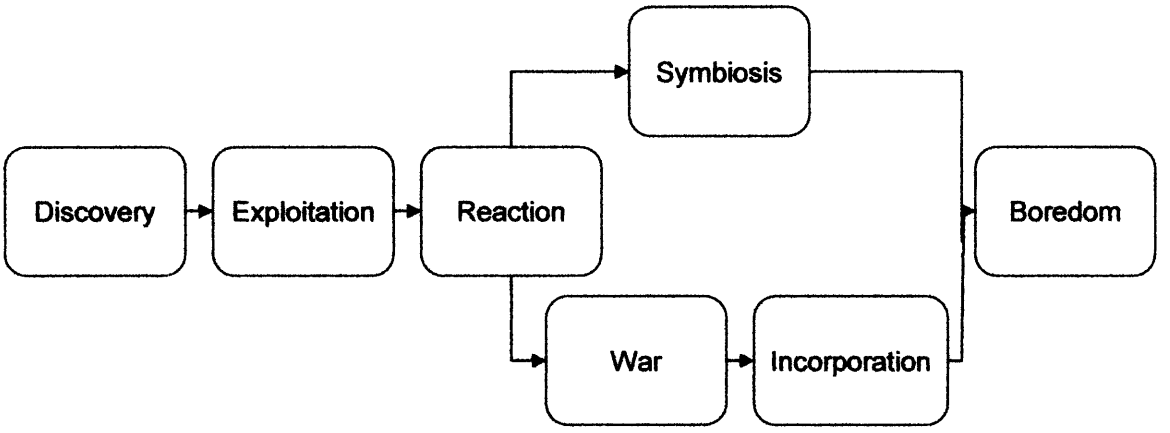

Figure 8: The Parasitic Innovation Cycle

Starting at the beginning, leftmost, portion of the diagram, the first two phases, Discovery and Exploitation, are marked by the formation of the structures and communities discussed in the previous chapters. These are populated by parasitic innovators whose motivations are similar to the driving forces of curiosity and recognition previously mentioned. During the Reaction phase, however, when companies begin to respond to the parasitic innovation community, motivations for the individual innovators may change dramatically. Before discussing this in detail, a fuller explanation of the initial phases of the model is in order.

Discovery

Discovery defines the earliest phase of a parasitic community, when the nature of the proprietary system is first discovered and the first exploration is performed. Discovery is the early days of the Elites in a community, and these initial Elites often become the "old men" of the community during later phases. Discovery tends to be small-scale, with only handfuls of users innovating, often through direct connections. In phreaking, this period

included the late 1960s, when the original MIT Tech Model Railroad Club's hacking of the phone system, including developing early blue boxes, was viewed as a natural extension of the work they were doing with early computers.[80] For game modders, this could been seen as the original Castle Smurfenstein, created for fun, with no purpose other than to make something interesting. During the Discovery phase, the innovators see their work as harmless, or even as helpful to firms since they are "checking out the system" for the firms.

Exploitation

Exploitation begins as discoveries made by these initial parasitic innovators are spread to the first Kiddies and destructive users. In the phreaker community, the 1971 *Esquire* article introduced a wave of potentially destructive users to the innovations of the first Elites, like the blue box. For the DeCSS community, the first commercial releases of an easily run DVD decrypter in 1999 proved the transition point. And, in the TiVo community, it was the packaging of user-downloadable applications to format and modify the TiVo hard drives that made Exploitation possible.

During the Exploitation period, the number of people with access to information grows quickly. This means both an expansion of the Kiddie community and a sharp increase in the number of potential and aspiring Elites. For this reason, Exploitation seems to be a time of great innovation – the act of parasitic innovation is not yet clearly outlawed, and many people are interested in becoming a part of this community by discovering and sharing new ideas. It is exactly this sort of sharing, however, that ultimately makes the

[80] Levy, Stephen. *Hackers*. p 83

community exploit the parasitic innovations too much. Kiddies eager to become recognized Elites publish easy guides to resolving technical problem and create software packages to automate the parasitic processes discovered. The social controls that kept information in the hands of Elites begin to break down as well, as BBSes and websites proliferate with the forbidden knowledge. Sometimes, early Elites divorce themselves from this phase, refusing to take responsibility for the process they started, as many early hackers/computer pioneers did when faced with more exploitative hacking.

Reaction

At some point after Exploitation begin, the Reaction phase occurs as the firm becomes aware of the parasitic innovators. This may happen because of economic damage, but more frequently as a result of a media story or an announcement by the parasitic innovators themselves, eager to share their discoveries with the world. The nature of the reaction by the firm or firms becomes the key element in determining the way the rest of the parasitic innovation cycle will proceed. An immediate negative reaction almost always leads to the War phase, while a mixed, neutral, or positive reaction most likely leads to Symbiosis. The nature of the reaction seems largely dependent on the nature of the firms in the industry, and their reasons for building proprietary systems.

Figure 9: Firm reactions to parasitic communities

	Firm Reaction	Starting Status	Current/ End Status	Nature of firms	Reason for proprietary
Phreakers	Neg.	Underground Pirate	Underground Pirate	Monopoly	Cost recoup.
Hackers	Neg.	Underground Pirate	Mixed	Small # of OS, many others	Add-on & IP protection
Game Modders	Pos.	Undergound Pirate	Open	Many small firms	Add-on
Mod Chips	Neg.	Open	Underground Pirate	Three firms	Cost recoup.
DeCSS	Neg..	Open	Pirate	Single trade organization	IP protection
TiVo	Pos.	Underground?	Open	Small firm in competitive industry	Add-on IP protection

Large, consolidated industries with limited numbers of players generally seem disposed to act in a negative way towards parasitic innovators. Partially this is due to the distance between the large firms and the innovators. Corporate managers without a parasitic background themselves cannot be expected to easily understand the motivations of the parasitic community. These large companies only see parasitic innovators as desiring to do whatever damage was caused in the Exploitation phase, rather than seeing that damage as an effect, rather than a goal, of innovation. A second possible explanation for the generally negative reaction of large firms is that large firms with exposure to a wide variety of legal and public relations concerns may wish to keep themselves well aware of the gray zone of parasitic innovation. Finally, large firms may have a bias against parasitic innovators because embracing user-innovators is risky, and markets with small numbers of competitors may not see the risk as being worthwhile.

Small firms, on the other hand, have been the only ones to embrace parasitic communities, doing so at considerable risk. In the case of game modding, it was the closeness of the game companies to their hacker ancestry that allowed them to understand and co-opt their parasitic communities. For TiVo, it was its position as new entrant, with a dubious future, that probably led it to welcome its innovators, since anything that gave it an edge would be worthwhile. Embracing parasitic innovation, then, is a strategy, and is more likely to be taken when firms are willing to bet big, or have otherwise run out of options.

Outside of firm size, the reasons for the firm's actions during the Reaction phase seem to be related to their reasons for implementing a proprietary system. Of the possible business reasons, the add-on model is apparently the most conducive to accepting parasitic innovation. This finding makes sense, because the innovation of parasitic users can become a draw for increased purchases of the original product (as in TiVo, with its capabilities expanded by parasitic innovators) or can occasionally be packaged as a product itself (as in the case of game mods later packaged and sold by firms). By giving up some residual revenue from controlling the add-on products, firms that successfully work with parasitic innovators can increase the utility of their core products, and still have some market for add-ons.

The cost recuperation proprietary business model is the one least suited to positive interaction with parasitic innovators. Since the goal of this sort of system is to pay for

upfront investment with long-term product lock-in, like the phone company recouping money from its massive network investment over the course of several decades, any method of circumventing the proprietary nature of the system can be a large danger. That is why firms with high degrees of initial investment, like the phone companies or game console makers which sell their products at a loss, seem to be the first to brand parasitic innovation as theft, and to pursue it most aggressively.

The cost recuperation model is not the only one that generally implies strong negative reactions to the parasitic community, however. Firms that turn to proprietary systems to protect extrinsic IP, whether that IP be content or trade secrets, are also strongly opposed to appeasing parasitic communities. These cases are, indeed, where the misunderstandings are greatest, since intellectual property rights are in the most direct conflict with the typical parasitic innovation ethic. From the perspective of the legal and regulatory tools used by firms against parasitic innovators, these IP conflicts are often less clear-cut in nature than the circumvention of cost recuperation methods, and therefore are pursued with more finesse than in the case of the phreakers or mod chip makers.

Regardless of underlying reasons, firms make a choice during the Reaction phase – attack the parasitic innovators or find accommodation with them. Of course, to some extent, by the Reaction phase "the genie is already out of the bottle, and there is no way firms can completely crush the exchange of information begun during Discovery or Exploitation. Many firms do attempt to pursue negative actions against parasitic innovators regardless,

either in hopes of wiping out the community or in the more realistic expectation of suppressing the further spread of information. When the attacks on the parasitic community begin, in the form of arrests, public statements, or technological counterattacks, the cycle moves on to the War phase.

War and L0phtcrack

The War phase involves full-on battles between the remaining innovators not scared off by the strong-arm tactics (or attracted to the danger) and the increasingly harassed firm or firms. The most significant aspect of the War phase is how it transforms the purpose of a parasitic community, altering its basic motivations. As has been demonstrated, Elites in early parasitic communities, even underground communities, tend to view themselves in fairly benign terms as "outside experts" or explorers within systems. While Kiddies may wreck havoc, Elites do not see their part in the damage being done, or at least are able to justify to themselves that they are not at fault.

As soon as an industry chooses a negative approach in the Reaction phase, the nature of the parasitic community changes. Many people are certainly scared off, but the rest become focused on the most secure, and therefore the most interesting systems. Combined with an "us vs. them" mentality, the result is a parasitic community out to do damage, and a continuing arms race between innovators and firms. This happened in the late phreaker community, as well as in game system mods and even in the case of DeCSS.

Just as companies are able to justify a negative reaction in response to theft, pirate innovators during the War phase justify themselves by appealing to higher principles. As Bell devoted more and more effort to trying to eliminate fraud, for example, phreakers came to see themselves as working to promote free information exchange, as opposed to the oppressive policies of Bell. This sort of confrontation-prone attitude helped convince phreakers that they were fighting against the government and big business to keep information, and technology, in the hands of the people. These idealist views on the freedom of information can be found in statements like Doctor Crash's:

> Hackers realize that the businesses aren't the only ones who are entitled to modern technology. They tap into online systems and use them to their own advantage. Of course, the government doesn't want the monopoly of technology broken, so they have outlawed hacking and arrest anyone who is caught. Even worse than the government is the security departments of businesses and companies. They act as their own "private armies" and their ruthless tactics are overlooked by the government, as it also serves their needs.[81]

More recently, in response to court decisions about DeCSS, there have been similar calls-to-arms appealing to the value of free speech over "corporate control". "Don't do this because you just want to copy DVD's -- that's not what this fight is about at all," *2600* magazine posted on its site after losing in court, "This is about freedom of information -- the right we all still have to LEARN how technology works."[82]

In some ways, this War phase is the common conception of the steady state of parasitic innovation, the norm in the movies and books for the "electronic underground" fighting

---

[81] Dr. Crash, *Phrack*, Issue #6, Phile 3,
[82] Kaplan, Karl. "First Ammendment Lawyer Takes on Movie Studios," *New York Times*, April 28, 2000.

against the law, attacking databases and defacing websites. Fortunately for the phenomenon of parasitic innovation, this is far from the truth. During the War phase, one of the biggest potential damages comes from a complete breakdown in communications between innovators and firms. An excellent case illustrating the damage that can be done, without direct attacks, in the movement from Exploitation to Reaction to War, is the story of L0phtCrack and Microsoft.

L0phtcrack was the product of a hacking group called L0pht Heavy Industries, which met regularly in a Boston loft (or, in phreaker/hacker parlance, "l0pht"). L0pht was one of the more famous Elite groups, and as would be expected in an Elite group, its members say that they became interested in hacking for the joy of discovery and for the recognition. Chris Wysopol ("Weld Pond") said that the "main draw for me and for a lot of people was figuring out how something worked that someone else built. It's exploration, as earlier hackers used to explore the phone systems."[83] While DilDog told the author, "Everyone's got their motivation. Mine was to be recognized within the hacker community."[84]

Driven by an interest in both recognition and discovery, L0pht ferreted out security holes in popular products, and then announced those holes to the company and the world. The stated aim was to improve the security of products, but there is no doubt that the notoriety was also a motivating factor. Inherently, then, there was nothing about L0pht that would indicate a propensity towards destructive activities. While they did make security holes

[83] Chris Wysopol, Interview with the author, March 22, 2004
[84] DilDog, Interview with the author, February 18, 2004

known to other Elites and Kiddies, companies were told about the issues at the same time.

In 1997, L0pht found a serious security flaw in Microsoft Windows NT, the flagship server operating system of the Microsoft line. Windows NT, in order to ensure compatibility with 1980s-era Windows systems, stored passwords in two ways, one very secure, and one limited to eight alphabetic letters in capital case, and therefore very easy to break. L0pht informed Microsoft, and the world, about this bug. Microsoft, however, chose to minimize its existence, announcing that "This is not a security flaw with Windows NT, but ... reinforces the importance of following basic security guidelines." [85] This was, at best, misdirection; the security flaw was real, and potentially serious. Then, when Microsoft performed some minor fixes to hide the problem, it did not credit L0pht for the original discovery. Even though Microsoft did not have the option to use legal means to stop L0pht, this was the equivalent of a negative choice during the Response phase, denying L0pht credit and essentially dismissing its work.

L0pht responded quickly, moving the parasitic cycle into a small-scale version of the War phase. They released L0phtcrack with a graphical interface, making it easy for any Kiddie to use. In their release notes, they wrote, "Thank you very little MS for dropping any reference to the l0pht...in reference to your recent... fix. If this is how you 'correspond' with people who point out problems to you it's no wonder that people prefer

[85] Douglas Thomas *Hacker Culture*, p. 107

to release things to the public instead of your 'proper' channels."[86] Microsoft kept denying that the L0phtcrack exposed any real security issues, and L0pht kept issuing new versions of its now popular software. The result was both a PR disaster and a missed opportunity for Microsoft. Many Kiddies used the software to break into Microsoft systems, leading in part to Microsoft's current reputation as a weak system from a security perspective. Ironically, Microsoft's trouble came from denying the free security help provided by the parasitic community in the first place. The L0phtcrack saga ended as the parasitic cycle moved into its next phase.

Incorporation

Eventually, the War phase, which is ultimately a battle of attrition, becomes too costly for both sides, since neither can gain mastery. From the firm perspective, crackdowns are partially effective, but new parasitic community members constantly appear to take the place of ones discouraged or incarcerated. For parasitic innovators, the fear of getting caught plus the aging of communities mean that many Elites begin to tire of the underground game and seek more legitimate uses of their talents. The result is the Incorporation phase, in which Elites and companies reach an uneasy accommodation with some Elites working with companies while others continue to war against the firms. Elites therefore fight against Elites, creating a tautology where Elites cause the problems that other Elites solve.

---

[86] Mudgenski Von Splat, "SMB Signing," Message on BugTrak board, February 6, 1998. Available at http://web.archive.org/web/19990127194759/http://www.geek-girl.com:80/bugtraq/1998_1/0176.html

The L0pht story shows how Incorporation can occur. In 2000, eager to make a living out of their hobby, L0pht joined with @stake, an internet security firm, to become a legitimate business. Soon after, Microsoft and other industry leaders including @stake unveiled what would become the responsible disclosure initiative. Responsible disclosure set forth a method for hackers to report security flaws, and to get credit for doing so. In return, the hackers would not release information on the flaw until thirty days had elapsed. Both communities therefore came to some sort of accommodation

At best, this phase is marked by, in the words of Laura Koetzle, "productive antagonism," in which the innovations of the parasitic community flow naturally into the world of firms, while still being driven by the desire to discover and challenge that characterizes early Elites. The Incorporation phase can also be a failure, as the newly co-opted Elites lose their "edge" and become driven by the same reward system as the firms upon which they once innovated. The story of L0phtcrack ends with just such a danger, as Daniel Greer, a researcher at @stake, published a very public report highly critical of Microsoft's security practices in 2003 and was fired. Critics claimed that this was at the insistence of Microsoft, a large customer of @stake. Weld Pond, former hacker and now VP of @stake, issued a statement that seemed to contrast with his former l0pht ties, "Security is much more complicated than focusing on this one issue. We think the way the paper is positioned ... is just not the answer."[87]

[87] Bridis, Ted. "Exec Fired over Report," *Seattle Post Intelligencer*. September 23, 2003. Available at http://seattlepi.nwsource.com/business/141444_msftsecurity26.html

Incorporation is not limited to the hacking community. Phreakers began to be part of an Incorporation movement, being hired by phone companies as security experts, just before the movement began to fade. Similarly, early game crackers were incorporated to some degree, channeled into legitimate mod-making. Virus writers are another example; many of the Elites now work directly with anti-virus companies.

The Incorporation phase is never entirely complete, however. Many individual Elites stay out of the responsible structure for philosophic reasons, or because it is just less fun. With responsible disclosure comes potential legal liability, for example. Worse, some hackers complain, is the assumption from the firms whose security holes they expose that the hackers are now responsible for helping firms solve the problems they discover. Generally, parasitic communities are uninterested in this sort of boring work. Additionally, the Kiddie population is continually developing new elites, not all of whom are in a position to be co-opted. Incorporation therefore becomes a long-standing civil war that lasts the remainder of the community's life.

Symbiosis

The Incorporation phase looks similar to the Symbiosis phase, which results if firms choose to react positively during the Reaction phase. Symbiosis describes the current state of the game mod industry, as well as the TiVo hacking community. Since firms choose not to pursue a negative strategy, a successful Symbiosis community needs to be self-sustaining. As long as the needs of the community's Elites and the needs of the company are not absolutely at cross-purposes, a symbiotic relationship can work.

Destructive innovation still can happen, but firms bet that such innovation is overwhelmed by the positive results of an empowered parasitic community. In the case of TiVo and game mods, this has proven a fruitful bet.

There are cases of failed Symbiosis, but when Symbiosis fails the firms supporting the innovation either go out of business, or instead choose the War phase. An example of this was the CueCat community. At the height of the dotcom excesses, a company called Digital Convergence spent $170 million giving away free bar-code scanners called CueCats. They were designed to scan special barcodes in magazine ads to give users more information on the products advertised. Originally, Digital Convergence welcomed a parasitic community, encouraging innovation.[88] As the community developed more ways of circumventing the CueCat's purpose (software allowing it to act as a mini-flashlight, book catalog tool, etc.), and therefore discouraging its intended use, Digital Convergence changed its mind. Despite attempts at cease-and-desist letters, it could not suppress the parasitic community, and the company failed soon after.

Boredom

Regardless of whether the parasitic innovation cycle travels through Incorporation or Symbiosis, parasitic communities are not eternal. Since they are driven by a combination of the desire for discovery and the desire to be recognized, as soon as the opportunities for either discovery or recognition fade, the community soon fades as well. This is the final phase in the cycle, Boredom. Given the rapid lifecycle of technology products, new

[88] Kahney, Leander. "Turning CueCat into CoolCat," *Wired News*, October 3, 2000. Available at http://www.wired.com/news/culture/0,1284,39139,00.html

and more interesting problems quickly become of interest, and obsolete ones become "uncool." Often, the main communities persist, such as the hacker community, but their areas of interest change, as in a shift in interest from accessing forbidden databases to discovering weaknesses wireless Internet hotspots.

The Boredom stage is usually accompanied by the commercialization of parasitic innovations. When Weak Knees started selling TiVo hard drives, innovation on that subject within the community fell. Similarly, the early computer hardware hacking communities disappeared as members like Steve Wozniak and Steve Jobs commercialized home computers. Communities do not disappear during Boredom, they simply move on to more interesting fields, starting the parasitic innovation cycle over again with a new technology and new firms upon which to innovate. This eternal aspect of parasitic user innovation is what makes it a persistent feature of proprietary systems, and makes it important to find better methods for firms to handle this sort of innovation in the future.

CONCLUSION:
TOWARDS A STRATEGY FOR PARASITIC INNOVATION

"What do you want?"
"Information."
"Whose side are you on?"
"That would be telling. We want... information... information..."
"Well, you won't get it"
"By hook or by crook, we will!"
- Introduction to *The Prisoner* (Often quoted by pirate innovators)

This paper has demonstrated the continuous nature of parasitic innovation, a phenomenon that is likely to persist for years to come. Fortunately, contrary to popular accounts, the best of these parasitic innovators, even of pirate innovators, are driven not by greed but by a desire for recognition and the thrill of discovery. Indeed, like the scientists they sometimes resemble, these Elite parasitic innovators form elaborate self-organizing communities and perform progressive work in discovering undiscovered aspects of proprietary systems. While they are truly innovative, they are not usually recognized by firms for their work.

The parasitic innovation cycle as it currently exists is not entirely satisfying. It does not properly tie the needs of the parasitic communities to that of firms, instead trusting that either benevolence (Symbiosis) or strong negative action (War and Incorporation) will lead to a positive outcome. From the cases examined in this paper, however, there is reason to believe that another method may prove more effective.

Instead of selecting a generally positive or negative strategy during the Reaction phase, as has been the case in each of the examples studied, firms might make another choice.

They may instead choose to deeply study their parasitic communities before deciding on a plan of action, and then, instead of reacting to the parasitic community as a whole, they may react separately to the Elite and Kiddie communities. There does not seem to be evidence in the current literature about this method being tried from the Reaction phase, but later actions taken by industry in aligning the needs of firms with Elites show that separation may be possible.

For example, the game industry, although it was not originally part of their strategy, now actively seeks out Elites from within the mod community. In constant struggle for recognition within a parasitic game community, the highest honor is to be recognized by game developers, who often skim the boards looking for talent. Great modders are often recognized by being given official responsibilities, such as control as a moderator of a board, or as a beta-tester of new software. The very best are hired outright:

> Keranen, Carlson, and many more would be hired by game companies largely on the strength of their mods. And unlike, say, the film and music industries, which are powered by personal acquaintance and face time, the discourse of games is defined online. Which is perhaps why the division between amateur and pro has remained so permeable. For modders wanting in, who you are doesn't ultimately depend on your experience or your contacts but on the quality of your mod file.[89]

By harnessing this accelerated user-to-user innovation, and selecting the best innovators from the modding community, game developers have helped keep their parasitic Elites aligned with the companies' own goals.

---

[89] Salon. p. 3.

Similarly, while it certainly was financially responsible for AT&T to identify blue box users and aggressively pursue fraud cases, more effort could have been made to harvest the best people and ideas from the phreaker movement, a tremendous source of innovation in the otherwise static telephone world. By approaching Elites as innovative hobbyists, rather than criminals, firms could provid them with tools that might have translated their destructive ideas into progressive ones. Indeed, before the company made it clear that it was not an option, most phone hackers often would have preferred to work for Bell, rather than against it. Often, phreakers insisted, as did Joe Engressia, a famous blind hacker, that they "want to work for Ma Bell," and phreaking was the closest they could come to it.[90] By aggressively going after all phreakers AT&T lost access to talent and innovation.

Elites do not necessarily have to be offered jobs in order to work with companies, though the literature shows that it serves as a motivational factor.[91] Recognition for achievement is all that many innovators, especially hackers like those of the old L0pht, want. In the words of Dildog, "What [the innovators] are discovering is to them some phenomenonal discovery, though to [the firms] it is a pain in the ass. A certain amount of respect is due to the hackers, a thank you, a cordial response."[92] The lack of respect shown to parasitic innovators is often given as a reason for their attacks on particular firms, such as Microsoft. Perceived arrogance is another magnet for negative innovation.

---

[90] Esquire, p.124
[91] Lerner, J. and J. Tirole (2002), "Some Simple Economics of Open Source", *Journal of Industrial Economics*, 50(2), pp. 197-234.
[92] Interview

This does not mean that firms need to pander to parasitic innovators, or perform the equivalent of paying protection money to an Elite mob. Instead, firms need to nurture positive parasitic Elites, even as they try more aggressive means to address the Kiddies. There is a need to understand the parasitic innovator's viewpoint, and that can only happen through close interaction. Even TiVo's benign neglect leaves too much to chance. For firms faced with parasitic innovation, the way that game companies treat modders is a better model. They have no tolerance for game copying, though they know it exists, and instead try to set up rewards for Elites that encourage positive participation. They especially use non-monetary rewards, such as public praise and the potential of a job, to encourage Elites to act in a positive way, reducing the amount of material produced for destructive Kiddies.

Building a close interaction between firm and parasitic community means challenging the way that pirate communities are currently viewed. The editor-in-chief of the journal *Computers and Security* summarized the prevailing industry view with, "Let's not glamorize those who transgress the law. Let's not legitimize what they do. Let's limit our contacts with them. Let's not hire them. Let's make it clear that we are not for them."[93] This approach is a recipe for a continuous War phase in the parasitic cycle. In contrast, the demands of at least a portion of the Elite community are relatively mild, "People really have to train themselves to respond correctly when faced with a security

[93] Schultz, Eugene. "Taking a Stand on Hackers," *Computers and Security*. Volume 21, Issue 5, Page 383 (1 October 2002)

hole in their products. The correct response is 'Thank you for finding a bug in our product'.... Not 'They published WHAT? Who are these evil hackers?'."[94]

Of course, there are firms that are accommodating to pirate innovators, just as there are Elites who will never work with firms in a positive way. However, firms usually only become accommodating during the Incorporation phase, after much damage has been done, while destructive Elites will not be eliminated by any amount of legal or corporate action. Firms should instead work with willing Elites from the Reaction phase onward to reach an accommodation that will work for both groups. In order to achieve this more effective approach, firms will need to be able to recognize the sometimes discomfiting actions of Elite parasitic innovators without feeling that they are compromising their own values or jeopardizing their business legally.

Parasitic communities are a significant phenomenon, one which is only likely to grow as proprietary systems become more popular. Only by changing the ways firms interact with these often strange but always innovative user communities can we hope to maximize their positive impacts while reducing their destructive effects. Until then, parasitic innovators will continue to work, whether in public or underground, exploring, expanding, and undermining.

[94] Blue Boar, "The Truth about ThievCo," August 28, 1998. Available on textfiles.com

BIBLIOGRAPHY

I. Personal Interviews and Correspondence

Dildog, Interview with author, February 18, 2004.

Douglas, Thomas. Telephone interview with author. February 4, 2004.

Koetzle, Laura. Interview with author. March 11, 2004.

Scott, Jason. Email correspondence. April 27, 2004.

Wysopol, Chris. Interview with the author, March 22, 2004

II. Primary Documents on Parasitic Communities

The sources below were written by members of the parasitic communities being studied, and therefore often have strong biases.

Anonymous. "Interview with Control-C," *Phreak*, March 30, 1994

Anonymous, "Phreak2K". Date unknown. [online: Web] URL: http://www.textfiles.com/phreak/

Anonymous, "Specs on Caller ID," Empire Times zine, July 10, 1992. [online: web] URL: http://www.flashback.se/archive/EMPTIME2.TXT.

Anonymous, *Week in Warez Newsletter*, July 30, 1995.

Anonymous, Youth International Party Line, Issue #1, 1971

Blue Boar, "The Truth about ThievCo," August 28, 1998.

Bioc Agent 003, "Basic Telecommunications, Part IV," June 15, 1984. [online: Web] URL: http://www.textfiles.com/phreak/BIOCAGENT/basicom4.phk

Chesire, Richard, "The Tap Newsletter," Modified February 4, 1986. [online: Web] http://spaceyideas.com/cheshire/tap.html

Curzio, Christopher. "CueCat Hacker," Website:http://www.accipiter.org/projects/cat.php Last accessed April 24, 2004.

Deicide, "The Neophytes Guide to Hacking," August 8, 1993. [online: Web] URL: http://www.textfiles.com/hacking/guidehak.txt

Dr. Crash, *Phrack*, Issue #6, Phile 3. No date.

Ipiggi, "A History of the Scene," April 10, 1999. [online: web] URL: http://www.textfiles.com/piracy/thescene.txt

Jedi, "phile 1.9", *P/HUN Newsletter #1*. March 30, 1988. [online: Web] URL: http://www.etext.org/CuD/Phun/phun-1

Johnson, Andy. "Official Castle Smurfenstein Homepage." Last visited May 1, 2004. [online: Web] URL: http://evlweb.eecs.uic.edu/aej/smurf.html

Kapln, Ian. "The Demise of @Stake?" December, 2003. [online: Web] URL: http://www.bearcave.com/misl/misl_tech/demise_of_atstake.html

Krackowicz, "The Basics of Kracking Parts 1-9," *Krackowicz's Kraking Korner*, date unknown (probably 1982-1983). [online: Web] URL: http://www.textfiles.com/100/krckwczt.app

Martin, Brian. "The Not So Scientific Process," *Attrition.org*. August 22, 2000. [online: Web] URL: http://www.attrition.org/security/rant/z/jericho.004.html

Mentor, "Hacker Manifesto," *Phrack* #7, phile 3, January 8, 1986.

Mr. Bad, Pigdog Journal DeCSS Distribution Center, PIGDOG JOURNAL, Feb. 16, 2000, [online: Web] URL: http://www.pigdog.org/decss

MPAA, "DeCSS Faq," undated. [online: web] URL: http://www.mpaa.org/Press/

Mudgenski Von Splat, "SMB Signing," Message on BugTrak board, February 6, 1998. [online: web] URL: http://web.archive.org/web/19990127194759/http://www.geek-girl.com:80/bugtraq/1998_1/0176.html

One Farad Cap,/AAG. Typed version of "Secrets of the Little Blue Box," *Phreaker's Manual*. undated.

Ravenmatrix, Interview with Jon Draper. July 27, 2002.

Scott," BBS Life in the 1980s, March 2000. [online: web] URL: http://www.textfiles.com/history/golnar.txt

Tiger, Tivo Community Boards, post dated 4/15/04.

Touretzky, D. S. Gallery of CSS Descramblers. 2000. [online: web] URL: http://www.cs.cmu.edu/~dst/DeCSS/Gallery

Tyranny, NFO for pirated copy of Backlash, [online: web] URL: http://www.textfiles.com/piracy/flame05.txt

Various, *Legion of Doom Technical Journal*, Volume 1, Jan 1, 1987. [online: Web] URL: http://www.textfiles.com/magazines/LOD/lod-1

III. Specific Articles and Popular Information

These sources provide information in a popular format about topics of relevance to the study of parasitic innovation.

Bauer, Mick. "Q&A with Chris Wysopal (Weld Pond)," Paranoid Penguin. September 01, 2002.

Becker, David. "Xbox Hacking Not for Amateurs," CNET News. May 22, 2002. [online: web] URL: http://news.com.com/2100-1040-924666.html

Bridis, Ted. "Exec Fired over Report," *Seattle Post Intelligencer*. September 23, 2003. [online: web] URL: http://seattlepi.nwsource.com/business/141444_msftsecurity26.html 1

Diaz, Sam, "Add-on Kit Boosts TiVo Storage," *San Jose Mercury News*, January 26, 2004.

Donahue, Anne. "TiVo Hacking Cut Short," *Video Business*, June 25. 2001. p. 37

Ferguson, Kevin. "The Short Strange Trip from Hacker to Entrepreneur," *Business Week Online*, March 2, 2000. Available at: http://www.businessweek.com/smallbiz/content/mar2000/ep000302.htm

Game Developers Conference 2004, "User Created Content: Is It Worth It?" Roundtable, March 24, 2004.

Glave, James. "Debate over Windows NT Password Breaker," *Wired News*. February 13, 1998. Available at http://www.wired.com/news/technology/0,1282,10303,00.html

"Hackers: Angels and Outlaws," documentary on TLC. Online transcripts and information can be found at: http://tlc.discovery.com/convergence/hackers/articles

Haughly, Matt. "Video Extraction and Tivo," *PVR Blog*, August 2, 2003. [online: web] URL: http://pvr.blogs.com/pvr/2003/08/video_extractio.html

Kahney, Leander. "Turning CueCat into CoolCat," *Wired News*, October 3, 2000. [online: web] URL: http://www.wired.com/news/culture/0,1284,39139,00.html

Kaplan, Karl. "First Amendment Lawyer Takes on Movie Studios," *New York Times*, April 28, 2000.

Kleinfeld, N. R.., "The Myriad Faces of Fraud on the Phone," *New York Times*, June, 1977

Lemke, Tom. "Spam Harmed Economy." *Washington Times*. November 9, 2003.

Miller, Jeff. "Grey Hat Hacker Mudge," *Mass High Tech*. January 26, 2004.

Nesteroff, Greg. *BCIT Link*. Canadian University Press, 1997

Pegorano, Rob. "Hollywood to Viewers," Washington Post. August 25, 2000.

Poulson, Kevin. "Microsoft Reveals Security Plan," *SecurityFocus*, November 9, 2001. Available online at: http://www.securityfocus.com/news/281

Savetz, Kevin. "Hackers Channel Talents Toward TiVo, ReplayTV Video Recorders." *Knight Ridder Business News*, March 22, 2001.

Schultz, Eugene. "Taking a Stand on Hackers," Computers and Security. Volume 21, Issue 5, Page 383. 1 October 2002.

Silver, Roy. "Blue Box is Linked to Fraud," *New York Times* May 5, 1973

Smith, Tony. "Tiny C Codes Bests Seven Line DVD Decoder." *The Register*, March 13, 2001.

Staff, *Business Communications Review*, 1995, p. 22

Staff, "ATT Monitored Millions of Calls," *Wall Street Journal*, May 6, 1977. p. 40.

Staff, Washington Post, June 14, 1978. p. D11.

Warren, Rob. "Openlaw DVD/DeCSS Faq," Berkman Center for Cyberlaw, Harvard University. Updated May 3, 2000.

Zager, Marsha, "Who are the Hackers?" *NewsFactor Network*, September 17, 2002 [online: web] URL: http://www.newsfactor.com/perl/story/19419.html

IV. General Works on Aspects of Parasitic Innovation

These sources are in-depth discussions of particular parasitic communities.

Au, Wagner James. "Triumph of the Mod," *Salon*, April 16, 2002. [online: web] URL: http://www.salon.com/tech/feature/2002/04/16/modding/

Hafner, Katie and Markoff, John. *Cyberpunk*. Simon and Schuster:New York, 1981.

Kleinfeld, Sonny. *The Biggest Company on Earth*. Holt Rinehart & Winston, 1983.

Knightmare. *Secrets of a Super Hacker*. Loompanics: Port Townsend, WA. 1994.

Levy, Stephen. *Hackers*. Anchor Press: New York, 1984.

Loper, Karl. "Profiling Hackers," PowerPoint Presentation. Date Unknown. Available at http://www.unt.edu/cjus/Course_Pages/CJUS_4870/

Rosenbaum, Ron. "Secrets of the Little Blue Box," *Esquire*. October, 1971, p. 124

Schell, Bernadette H. *The Hacking of America : who's doing it, why, and how.* Westport, CT : Quorum Books, 2002.

Scott, Jason. TEXTFILES, www.textfiles.com, revised December 3, 2003

Sterling, Bruce, *The Hacker Crackdown*, New York: Bantam Books, 1992.

Stoll, Cliff, *The Cuckoo's Egg,* New York: Pocket Books, 1989.

Thomas, Douglas. *Hacker Culture*. University of Minnesota Press: Minneapolis. 2002.

Thomson, Clive. "The Virus Underground" *New York Times Magazine.* February 08, 2004.

V. Academic References

These sources have been peer-reviewed and published in the academic press.

Conner and Rummelt (1991), "Software Piracy: An Analysis of Protection Strategies", *Management Science*, 37, pp. 125-139.

Fisher, R. J. and Ackerman, D., "The effects of recognition and group need on volunteerism: A social norm perspective," *Journal of Consumer Researc*h, 25(3), 262-275, 1998.

Franke, Nikolaus and Sonali Shaw. "How Communities Support Innovative Activities," Accepted for publication in *Research Policy*. January, 2002. [online: Web] URL: http://userinnovation.mit.edu/papers/9.pdf

Gholson, Barry, William Shadish, Robert Neimeyer, and Arthur Houts, editors. *Psycology of Science*. Cambridge University Press, Cambridge. 1989.

Lakatos, Imre. *Criticism and the Growth of Knowledge*, New York: Cambridge University Press, 1970.

Lakhani, K. and R. Wolf (2001), "Does Free Software Mean Free Labor? Characteristics

of Participants in Open Source Communities," BCG Survey Report, Boston, MA: Boston Consulting Group. [online: web] URL: http://www.osdn.com/bcg/.

Lakhani, Karim and Eric von Hippel, "How Open Source Software Works," *Research Polic,y* 1451 (2002) 1–21

Lerner, J. and J. Tirole (2002), "Some Simple Economics of Open Source", *Journal of Industrial Economics*, 50(2), pp. 197-234.

Meyer, Gordon, "The Social Organization of the Computer Underground," unpublished thesis, 1989. [online: Web] IRL: http://bak.spc.org/dms/archive/hackorg.html.

Morrison, Pamela D., Roberts, John H., von Hippel, Eric, "Determinants of Information Sharing in a Local Environment" *Management Science*, December, 2000, Vol. 46, Issue 12

Raymond, E. (1999). *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary.* Cambridge, England: O'Reilly.

Riggs, Peter, *Whys and Ways of Scienc*e, Melbourne University Press: Melborne, 1992.

Takahashi, N. (2000). The Emergence of Generalized Exchange. *American Journal of Sociology*, Vol. 105, Iss. 4 (January 2000), pp. 1105-1134.

von Hippel, E. (1988). *The Sources of Innovation.* New York: Oxford University Press.

von Hippel, E., S. Thomke and M. Sonnack (1999). "Creating Breakthroughs at 3m." *Harvard Business Review*, 77(5): 47-57.

VI. Multimedia Material

Goldstein, Emmanuel, et al. "Off the Hook," Radio Program. Archives at http://www.2600.com/offthehook/

Soerensen, Stif-Lennart, *New York City Hackers,* 2001. Available at http://uit.no/breifilm/4276/

Tourqie (Annaliza Savage), *Unauthorized Access,* 1995. Available at http://www.fish.com/UA

APPENDIX A: QUANTITATIVE METHODS

I originally conducted three preliminary attempts to quantify the impact of parasitic innovation in various fields, attempting specifically to quantify how various types of communities relate to their host industries. Two of these techniques proved overly problematic, though the third could be workable with additional resources.

My first effort was to attempt to quantify positive and negative efforts by examining the ratio of responses that enable destructive behavior compared to responses that discourage destructive behavior for the the game modding and hacker communities. I searched popular online forums for terms that are used to describe acts of destructive parasitic innovation, such as "crack," "CD-Key," "serial," "pirate," and "warez," and then examine the community response. I then attempted to code destructive and productive responses, real examples of which are below in Table 3.

Destructive Response	Co-opted Response
N/A: I really need a working Halo CD Key 'cause I don't have one...so if you have one, send me it please, it will help alot! **THEMAN:** pgqtg-4x4j3-68m87-b28tr-j2cbj **PRAVIS:** Thanks!!!!	**KORRUPTION:** well ive lost my legit cd key but still got wc3 on my comp and wondering if any1 knew where how 2 find where 2 find 1 ?? **$LAYER:** How Can you Lose your LEGiT **CD-Key**?... My Suggestion is to Send your Original CD Back to Blizzard explaining the situation, and they should give you another Legit **Cd-key**... or call blizzard tech support :-) **SPY005:** Hmmm, contact the game company. That's the only legal thing to do **KAO:** Its on the back of your cd

The problem with this approach was not the data gathering itself, but rather that the positive or negative nature of the responses were determined more by the nature of the computerized discussion board itself than any other factor. Some boards were moderated, for example, which meant that they enforced discussion rules. Other boards were simply popular with parasitic innovators, while others had one or two problem members who posted CD-keys and other material. The end result of this diversity was an inability to clearly control for the appropriate variable, making this technique impracticable.

The second method of measuring destructive and productive results of innovation was through direct survey of parasitic groups. These surveys were conducted using contacts from online forums. In simple, non-statistical tests, I was able to get detailed responses to online surveys asking about parasitic innovation, for non-underground communities such as game modders, but gaining meaningful results from underground communities appeared problematic. Given this paper's focus on underground communities even more than those not underground, controlled surveys of these limited populations were not actively pursued, although responses collected to the initial surveys are included in this paper. Surveys may still prove useful in future work, but was of limited utility in this study.

The third measure of the quantitative effects of parasitic innovators were to look directly at community product. I will do this by surveying software developed by each parasitic community, and coding the number of desirable applications (ie. mods) compared to the

number of destructive applications (ie CD-Key generators). Additionally, to measure whether the parasitic community is actively developing constructive or destructive products, I will examine what proportion of positive and negative products are being actively developed.

APPENDIX B: TESTS FOR KIDDIES

Below are two examples of the kinds of form used to request membership in hacker/phreaker groups. Both show an interesting mix of real technical knowledge and obvious social immaturity. The spelling and capitalization in both are unchanged from the original. Both are taken from

---

Riders of Death Application Form
/\
Please edit this form with your favorite editor program and upload it to
the RoD home site at 305-885-0409. If you dont have access there,.just
leave me a message saying that you have something to upload me, and that
you are applying for RoD. And just apply for access.. you will get access
as soon as i can get to my computer and validate you!

Answer these questions truthfully and to the best of your knowledge.
/\

What is the handle you want to use?
What is your *REAL* name
Do you have anything to do with the FBI, police, cia, or any government
agencies?
If yes, which one?
Are you into h/p/a?
What can you contribute to us that will benefit the RoD?
If you are into h/p, please give me an example of an x.25 packet system,
and list 1 company that serves the needs for x.25 packet communications.
What is your home phone number? (for verification purposes only)
We dont need to know your address, but it is better for our records.
please put it here if you want to.
Name some people that could vouch for you?
Please tell me what is a CBI, UNIX system, and Telenet.
What do you like doing in your spare time with your computer
what kind of computer do you have?
Do you know how to access a board through tymnet/telenet

Okay, that's pretty much it. If you have any questions or comments, feel
free to leave me, Sarah Connor, a message on any of the following boards

<<<<<<<<<<<<<<<<<<>>>>>>>>>>>>>>>>>
<> <>
<> [< ACiD ALLiANCE >] <>
<> <>
<> MOTTO: BEiNG ELiTE SUXS <>
<> <>
<<<<<<<<<<<<<<<<<<>>>>>>>>>>>>>>>>>

PHiLE: iNFO BEG FORM

Ok, so you decided to download the iNFO BEG FORM. Here are the rules of filling out this form. YOU MUST LEAVE THiS FORM iN THE CONDiTiON iT WAS iN, the only editing i will except are when you fill in the blanks, if you change, or upload something else then please delete this phile from your directory now. YOU MUST ANSWER ALL QUESTiONS TRUTHFULLY OR TO THE BEST OF YOUR KNOWLEDGE, that's all i ask for. Now here's how you'll get validated(maybe), we will take you information into account, if all the information is complete and truthful and correct, you have a pretty good chance. Then i, $ector Not Found, and White Fang will discuss the possiblity of validating you.

Off Hand here are the Access Levels of the ACiD ALLiANCE.

-=ACCESS LEVELS=-
- PREZ - PRESiDENT -
- PHRiER - PREFERED MEMBER -
- SNARF - NORMAL MEMBER -
- LEECH - NEW MEMBER -

if you get validated you will recieve LEECH status, at this status you will have some access to stuff. in order to gain SNARF status, you must prove yourself to us, by suppling us with with information that is useful to the rest of us. Such as Text Philes you write, Text Philes you obtain, info on Ma Bell, any programming ability you have and other of such nature. To become a prefered user, you must provide us with an outstanding participation toward the ACiD ALLiANCE. ok this intro is long enuf already.

Oh yea, one more thing, all information that you release to us will be Keep confidental from all users except users with PHRiER Status.

+----------+

1/27/91

[< ACiD ALLiANCE >]
iNFO FORM:

1. WHAT iS YOUR HANDLE YOU GO BY MOST
2. WHAT iS YOUR REAL NAME (FULL), ADDRESS, STATE, ZiP, VOiCE NUMBER
3. WHAT'S YOUR BiRTHDATE 00/00/00
4. WHAT KiND OF COMPUTER DO YOU OWN
5. WHAT COMPUTERS DO YOU HAVE EXPERiENCE WiTH
6. DO YOU PROGRAM, AND iF YES, iN WHAT LANGUAGES DO YOU PROGRAM iN
7. AND iF YOU PROGRAM, WHAT ARE SOME OF THE PROGRAMS THAT YOU HAVE WRiTTEN
8. ARE YOU AFFiLATED WiTH ANY LAW ENFORCEMENT AGENCiES, SOFTWARE COMPANiES,
   TELEFONE COMPANiES.
9. DO YOU PHREAK, iF YES THEN WHAT DO YOU PHREAK WiTH
10. DO YOU HACK, WHAT SiSTEMS DO YOU HACK ON
11. ARE YOU WiLLiNG TO SHARE iNFORMATiON YOU LEARNED WiTH THE OTHER MEMBERS
12. ARE YOU A LEECH
13. ARE YOU ELiTE
14. WHAT DO YOU THiNK OF WAREZ
15. DO YOU RUN A BOARD, iF YES PUT YOUR BOARD # DOWN HERE AND NUP.
16. iF YOU RUN A BOARD, DO YOU WiSH TO HELP DiSTRiBUTE OUT MATERiAL
17. ARE YOU iN ANY OTHER GROUPS(Phela, Phrack, NARC, CHiNA)
18. ARE YOU WiLLiNG TO CONTRiBUTE TO THE GROUP
19. DO YOU HAVE ANY ARTiSTiC ABiLiTiES
20. NAME SOME THiNGS THAT YOU DO ON YOUR COMPUTER(iF YOU BEAT YERSELF WHiLE WATCHiNG ANiMATED GiF'S THEN GO TALK TO THG)
21. HAVE PHREAK/HACK MAGS DO YOU READ
23. NAME SOME TEXT PHiLES YOU HAVE WRiTTEN
24. HOW CAN YOU BENiFiT US
25. NAME AT LEAST 10 PHRACK BOARDZ THAT YOU ARE ON
26. NAME AT LEAST 10 OTHER PHREAKERS, CRACKERS, HACKERS THAT YOU KNOW
27. DO YOU CRASH BOARDZ
28. DO YOU CARD
29. DO YOU HAVE ELECTRONiC ABiLiTY

30. DO YOU PROGRAM ViRii, iF YES WiLL YOU UPLOAD YOUR SOURCE TO US AND NAME A FEW THAT YOU HAVE WRiTTEN.
31. DO YOU HAVE A VMB, iF YES PUT iT DOWN HERE
32. NOW PUT DOWN ANYTHiNG ELSE THAT i MiGHT OF MiSSED THAT CAN HELP YOU OBTAiN MEMBERSHiP.
-==========-

OK NOW FOR THE VOCABULARY QUiZ(AND YOU THOUGHT THiS iS PHOR ONLY ENGLiSH)
DEFiNE THE FOLLOWiNG:

1. CHiNA 2. NARC 3. PHRACK 4. PHREAK 5. PHREAKiNG 6. HACKiNG 7. HACKER 8. ELiTE 9. ESS 10. CNA 11. BLUE BOX 12. BLACK BOX 13. SiLVER BOX 14. RED BOXiNG 15. GREEN BOXiNG 16. CAPTAiN CRUNCH 17. 2600 MAG 18. 2600 HZ 19. MF TONES 20. TROJAN 21. ViRii 22. ANSi BOMB 23. VMB 24. VMS 25. UNiX 26. LoD 27. CODE THiEF 28. TiMNET 29. TELENET 30. CARDiNG 31. CARDER 32. LEECH 33. LOOP 34. PBX 35. 950 36. WHAT iS THE PURPOSE OF PHREAKiNG TO YOU 37. THG 38. iNC 39. PE 40. BRiDGE 41. NUA 42. NUi 43. OD 44. GOD 46. CiS 47. VAX 48. HP 3000 49. HP 2000 50. BOUNCE SiSTEM 51. TRW 52. CBi 53. NUP 54. MSC 55. WAT 56. SWEEP 57. EXTENDER 58. CODE 59. TRUNK 60. WHiTE BOX 61. YELLOW BOX 62. SCARLET BOX 63. BUD BOX 64. LUNCH BOX 65. LUTZiFER 66. QSD 67. PAD 68. PSN 69. CHEESE BOX 70. BREWER ASSOCiATES 71. EASiEST WAY TO CRASH TELEGAURD 2.5i 72. EASiEST WAY TO CARSH WWiV 4.10 - 4.12 73. AFTERSHOCK 74. ANi 75. COSMO 76. CYBER SYSTEM 77. ACD 78. CAMA 79. CCiS 80. FAST BUSY 81. CO 82. ETS 83. NPA 84. SF 85. KP 86. CLEAR BOX 87. BEiGE BOX 88. PURPLE BOX

OK THAT'S ENUF DEFiNiTiONS GOT LOTS MORE BUT iF YOU KNOW THiS MUCH MAYBE YOU MiGHT MAKE iT. EH? WELL GUYS HERE YOU HAVE COMPLETED THiS iNFO BEG FORM. NOW UPLOAD THiS BACK TO THE WOLF'S DEN AT 602-241-1898 AND WE'LL GET TO YOU AS SOON AS POSSiBLE JUST KEEP CALLiNG.]>amaged $ectorz -=EOF=- □

APPENDIX C:

CULT OF THE DEAD COW'S RESPONSE TO MICROSOFT

The cDc released Back Orifice in 1998, which performed similar functions to L0phtcrack. Microsoft chose to deny the seriousness of a problem, issuing a press release to that effect. cDc's response, in part, is given below.

"This is our response to Microsoft's damage control statement of 1998-Aug-04. For a statement regarding our motives for releasing this tool, take a gander at our moral justifications.

last revision: 1998-Aug-10

Microsoft

On July 21, a self-described hacker group known as the Cult of the Dead Cow released a tool called BackOrifice, and suggested that Windows users were at risk from unauthorized attacks.

Microsoft takes security seriously, and has issued this bulletin to advise customers that Windows 95 and Windows 98 users following safe computing practices are not at risk...

...and Windows NT users are not threatened in any way by this tool.

cDc

Actually, we released it on August 3rd.

Incidentally, it's been downloaded at least 35,000 times as of 11:55pm, August 7th.

This is simply false. Our view is no degree of "safe computing practices" can compensate for the security bugs and lack of functionality in Windows 95 & 98.

For the present. But remember that the tool has been around for less than a week.

The Claims About BackOrifice

According to its creators, BackOrifice is "a self-contained, self-installing utility which allows the user to control and monitor computers running the Windows operating system over a network". The authors claim that the program can be used to remotely control a Windows computer, read everything that the user types at the keyboard, capture images that are displayed on the monitor, upload and download files remotely, and redirect information to a remote internet site.

Back Orifice does not do anything that the Windows 95/98 operating system was not intended to do. It does not take advantage of any bugs in the operating system or use any undocumented or internal APIs. It uses documented calls built into Windows to do such things as:

- Reveal all cached passwords. This includes passwords for web sites, dialup connections, network drives and printers, and the passwords of any application that stores user passwords in the operating system. (This Windows feature was implemented apparently so the user won't be inconvenienced by having to remember his passwords every time he uses his

computer.)

- Create shares hidden to the user and list the passwords of existing shares.
- Make itself mostly invisible. Back Orifice does not appear in the control-alt-delete list of running programs, and can only be killed by a low level process viewer which Windows 95 does not ship with. To their credit, Windows 98 does ship with a process viewer, but it is not installed by default.

The Truth About BackOrifice

BackOrifice does not expose or exploit any security issue with the Windows platform or the BackOffice suite of products.

Back Orifice has nothing to do, at all, with the Back Office suite. In fact, the Back Office suite only runs on NT, which isn't even supported by Back Orifice yet. Apples and Oranges.

BackOrifice does not compromise the security of a Windows network.

cDc would like to know where exactly Microsoft is getting its definition of 'compromise the security'.

Instead, it relies on the user to install it...

Back Orifice does **not** rely on the user for its installation. To install it, it simply needs to be run. Thanks to some actual exploits, there are several ways a program could be run on a windows computer, not only without the user's approval, but without the user's knowledge.

...and, once installed, has only the rights and privileges that the user has on the computer.

This is correct. Once installed, Back Orifice can only do what the user sitting at the computer could do, if he has programs that do everything that Back Orifice does.

This includes:

- seeing what's on the screen
- seeing what's typed into the keyboard
- installing software
- uninstalling software
- rebooting the computer
- viewing stored passwords
- viewing and editing the system registry
- connecting and disconnecting the machine to other network hosts using **anyone's** username & password
- running arbitrary plugins or programs, which of course could employ any manner of exploit or attack

For a BackOrifice attack to succeed, a chain of very specific events must happen:

- The user must deliberately install, or be tricked into

Not at all. Thanks to various security bugs and common system misconfigurations, there are often ways to deliver and execute arbitrary code on a

installing the program

Windows machine.

Even lacking such an exploit, it's easy enough to provide the average Windows users a reason for downloading & installing programs from untrusted sources. It happens all the time.

- The attacker must know the user's IP address.

Untrue. Back Orifice can sweep a range of IP addresses and network blocks to hunt for installations of its server software.

- The attacker must be able to directly address the user's computer; e.g., there must not be a firewall between the attacker and the user.

Incorrect. The mere presence of a firewall or proxy server is not in itself a complete solution.

What Does This Mean for Customers Running Windows 95 and Windows 98?

BackOrifice is unlikely to pose a threat to the vast majority of Windows 95 or Windows 98 users, especially those who follow safe internet computing practices. Windows 95 and Windows 98 offer a set of security features that will in general allow users to safely use their computers at home or on the Internet. Like any other program, BackOrifice must be installed before it can run.

Clearly, users should prevent this installation by following good practices like not downloading unsigned executables, and by insulating themselves from direct connection to the Internet with Proxy Servers and/or firewalls wherever possible.

cDc remembers a day when PC software was written by anyone who had a creative idea for a cute, useful, interesting, or even just plain silly program and being able to share that program with friends who might also enjoy the program. It is unfortunate that the only software we're allowed to run now is written by large companies. It's a good thing we can still trust them not to do something unwanted to our computer!

Generally, computers running Windows 95 and Windows 98 are not vulnerable if:

- The computer is not connected to the outside world

Unless someone **on the inside** wants control of your machine.

Perhaps your employer is using B.O. to keep track of its human resources. (As a matter of fact, in most states this would be entirely legal.) Or suppose one of your coworkers is just plain nosy.

In these circumstances, it doesn't matter if your computer is on the internet.

- The computer is connected to

Unless the dynamic address assigned is always in

the Internet through an Internet service provider that dynamically assigns IP addresses - as the vast majority of ISPs already do.

the same subnet, (as the vast majority of ISPs do). In which case, **B.O. can scan a range of IP addresses to find your machine at its new address.**

- The computer is on a network with a firewall or proxy server between it and the attacker.

See above ("firewalls").

What Does This Mean For Customers Running Windows NT?

There is no threat to Windows NT Workstation or Windows NT Server customers; the program does not run on the Windows NT platform. BackOrifice's authors don't claim that their product poses any threat to Windows NT. Windows NT Workstation and Server offer a comprehensive set of security features that make it the best choice for business users' mission-critical applications.

Don't go upgrade to Windows NT just yet.

We will be releasing a Windows NT version as soon as we get around to installing that OS.

What Customers Should do

Customers do not need to take any special precautions against this program. However, all of the normal precautions regarding safe computing apply:

Customers should keep their software up to date and should never install or run software from unknown sources -- this applies to both software available on the Internet and sent via e-mail. Reputable software vendors digitally sign their software to verify its authenticity and safety. Companies should use the security features provided by Microsoft products, to prevent the introduction of this and other malicious software, and should monitor network usage to prevent insider attacks.

Rather than having to abstain from using non-big company "Reputable Vendor" software, how about providing some protection? How about the ability to monitor and even prevent disk and registry access so people can run software with confidence, so that even if the author has malicious intent, the software has become infected with an unknown virus or trojan, or there is a bug or malfunction, there is no damage it can do.