Security needs on networks

- **Confidentiality**: Only authorized people - e.g., the sender and recipient of a message, and not any eavesdroppers - can know the message.

  Implemented using encryption

- **Authentication**: When Bob receives a message that purports to be sent by Alice, Bob can be sure that the message was really sent by Alice.
- **Integrity**: When Bob receives a message, he can be sure that it was not modified en route after Alice sent it.
- **Non-repudiation**: Alice cannot later deny that the message was sent. Bob cannot later deny that the message was received.

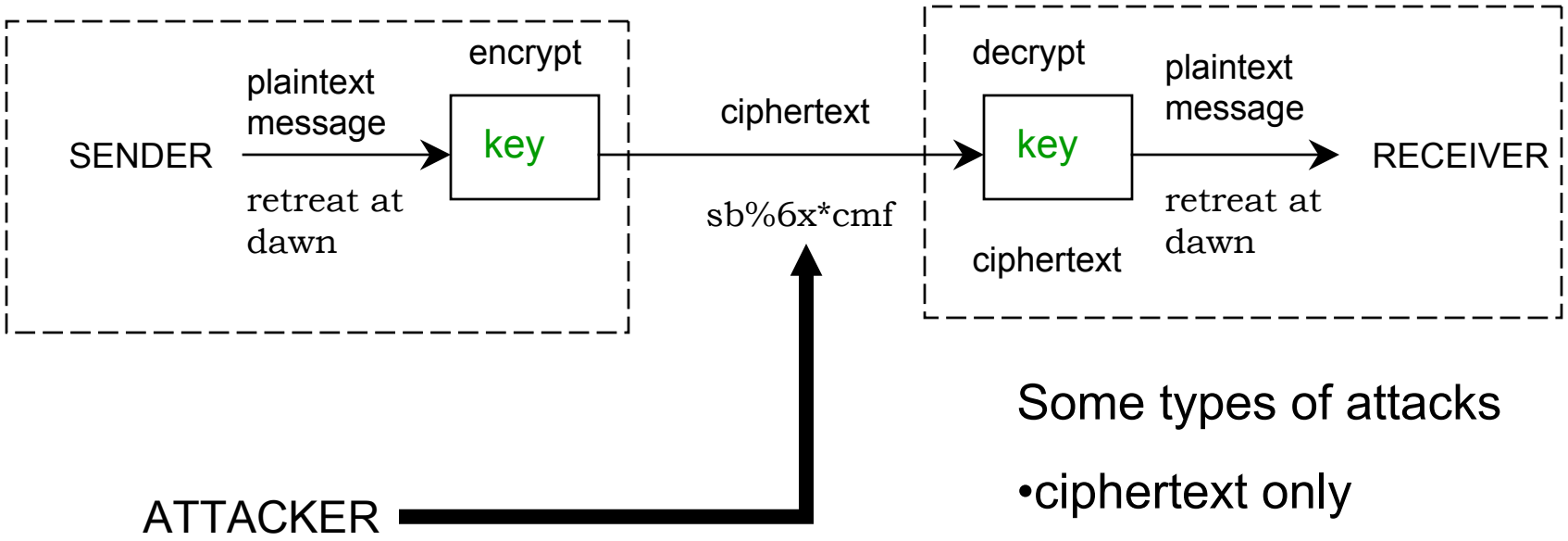
  Implemented using digital signatures

Application areas for security

- Interactive communication
- Data storage
- Store and forward messaging (e.g. email)

- Security is a lot more than encryption.
- Privacy is a lot more that security.

Cryptosystems



Some types of attacks

- ciphertext only
- known plaintext
- chosen plaintext
- chosen ciphertext
- rubber hose

Kerkhoffs's Principle

- Auguste Kerkhoffs, "La Cryptographie Militaire", 1883

- Cryptographic systems should be designed in such a way that they are not compromised if the opponent learns the technique being used. In other words, the security should reside in the choice of key rather than in obscure design features.
  - quoted from Ross Anderson How to Cheat at the Lottery (1999)

Secret key encryption (Symmetric algorithms)

- The encryption key is the same as the decryption key: if you can encrypt a message, you can decrypt the message.
- If Alice wants to send a message to Bob, they must first agree on a shared key.
- In a well-designed system, the attacker must try all possible keys in order to read or forge messages: no shortcuts.

Data Encryption Standard (DES)

- Designed by IBM in 1975, with help from NSA
- Keys are 56 bits long, so there are 2^{56} keys, or about 70,000,000,000,000,000
- 2^{56} is a big number, but not that big. In August 1998, the Electronic Frontier Foundation demonstrated that a special-purpose machine built from standard parts at a cost of $200,000 could break DES in 56 hours.
- Big governments have a lot more than $200,000 to spend on cryptanalysis.
- Each time you add a bit to the key length, you double the time required to break the system.
- NIST is specifying a new encryption standard (Rijndael)

Secure key distribution is critical

- With a symmetric system like DES, Alice and Bob have to agree on a shared secret.
  - Doesn't work well on a large scale
  - Doesn't work with people who haven't met in advance
- But there is a great idea:
- Diffie-Hellman key agreement (1976):*
- Alice and Bob can create a shared secret key by exchanging messages, even if they have never met before and have made no prior arrangements, and even if everyone can eavesdrop on the messages!
- **In 1997, it was revealed the this idea was actually first discovered in 1974, by Malcolm Williamson of GCHQ (British Intelligence)*

The basic approach

- Find a *one-way function*, that is, a function that is quick to compute but slow to invert.
- Example: Multiplication and factoring - You can multiply two numbers in time proportional to the number of digits. But (as far as anyone knows), the time required to factor a number grows as the size of the number. So, we could quickly multiply a pair of 500 digit numbers. But if we give people the product, it will take them on the order of 10^{500} times as long to factor the number as it took us to do the multiplication.
- A factor of 10^{500} is a lot more than the difference between a laptop PC and any computer power available to the NSA (we think).

The one-way function for Diffie-Hellman

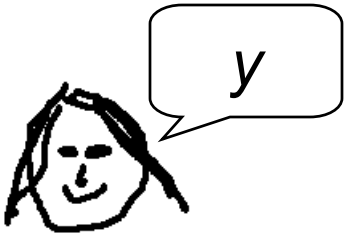
- Modular exponentiation: Given a prime p, and numbers a and w less than p, compute $y=a^w$ modulo p. (Can be done in $\log_2 w$ steps.)

- Discrete log problem: Given p, a, and y, find a w such that $y=a^w$ modulo p. (Requires time on the order of p as far as anyone knows.)

- So if we take p to be a 500 digit prime, the difference between the computing effort to compute powers mod p versus computing discrete logs mod p is on the order of 2^{500}

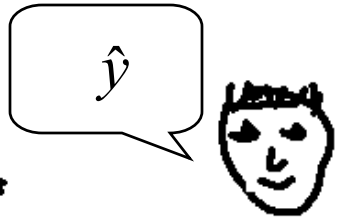
Diffie-Hellman Key Agreement

Start with public, standard values of *p* and *a*



Alice

Eve



Bob

Pick a private number *w*

Compute $y = a^{w} \bmod p$

Shout out *y*

Compute $\hat{y}^{w} \bmod p$

Pick a private number $\hat{w}$

Compute $\hat{y} = a^{\hat{w}} \bmod p$

Shout out $\hat{y}$

Compute $y^{\hat{w}} \bmod p$

But Alice and Bob have computed the same number, because

$$\left(\hat{y}^{w} = (a^{\hat{w}})^{w} = a^{w\hat{w}} = (a^{w})^{\hat{w}} = y^{\hat{w}}\right) \bmod p$$

Call this shared number *K*

Eavesdroppers know $y = a^{w} \bmod p$ and $\hat{y} = a^{\hat{w}} \bmod p$

But going from these to $a^{w\hat{w}} \bmod p$ requires solving the discrete log problem (as far as anyone knows)

Public-key encryption (asymmetric algorithms)

- Alice picks her secret number *w*, computes the corresponding *y,* and publishes *y* in a directory (like the telephone directory).
- If Bob wants to send a message to Alice
  - picks his own secret number $\hat{w}$, and computes $\hat{y}$
  - uses $\hat{w}$, together with Alice's *y* to compute *K*
  - uses *K* as the key to encrypt a message, with some symmetric algorithm (e.g. DES)
  - sends the encrypted message to Alice, along with $\hat{y}$
- When Alice receives the message, she uses $\hat{y}$ and her secret number *w* to compute *K*, and she decrypts the message
- In this scheme, *w* is Alice's *secret key* and *y* is her *public key*
- Anyone who knows Alice's public key can send her a message, but only Alice can decrypt these messages.

Security needs on networks

- **Confidentiality**: Only authorized people - e.g., the sender and recipient of a message, and not any eavesdroppers - can know the message.

  Implemented using encryption

- **Authentication**: When Bob receives a message that purports to be sent by Alice, Bob can be sure that the message was really sent by Alice.
- **Integrity**: When Bob receives a message, he can be sure that it was not modified en route after Alice sent it.
- **Non-repudiation**: Alice cannot later deny that the message was sent. Bob cannot later deny that the message was received.

  Implemented using digital signatures

Digital signatures

- Also introduced by Diffie and Hellman in 1976.
- Given a secret key *w,* the corresponding public key *y*, and a message *M,* generate a number *S* such that
  - *S* is easy to compute if you know *w* and *M*
  - *S* is computationally infeasible to compute if you don't know *w*
  - *S* is easy to "check" if you know *M* and *y*, that is, a certain equation involving *M* and *S* and *y* must hold
- So to "sign" a message *M,* compute *S* using your secret key. Anyone can check *S* by using your public key.
- If the message was tampered with, the signature won't check. [integrity]
- No one else could have produced *S,* since producing *S* requires knowing your secret key. [authentication and non-repudiation]

Digital signatures and PK encryption

- PK encryption: People send you messages encrypted with the aid of your public key; you decrypt these with your corresponding secret key
- Digital signatures: You sign using your secret key; people check the signature using your corresponding public key
- The digital signature algorithm is a lot like the Diffie-Hellman algorithm
- The best-known public-key algorithm, called RSA, can be used both for encryption and digitial signatures. In fact, you can even use the same secret key for decrypting and signing.
- Is it a good idea to use the same secret key for decrypting and signing?

Certificates and Certifying Authorities*

- How do we know that "Alice's public key" actually belongs to Alice?
  - Alice goes to a *Certification Authority* (CA), demonstrates her identity, and shows her public key. The CA digitally signs Alice's public key, producing a *certificate.* Anyone can check the validity of the certificate by using the CA's public key.
- How do we know the CA's public key is really the CA's public key?
  - 1. The CA also has a certificate, signed by some well-known and trusted authority like the US Post Office (chain of trust); and/or
  - 2. Lots of people you trust have vouched for it (web of trust)

*Loren M Kohnfelder. *Towards a Practical Public-key Cryptosystem*. Bachelor's thesis, EECS Dept., Massachusetts Institute of Technology, May, 1978.

National Security Agency

There is a very real and critical danger that unrestrained public discussion of cryptologic matters will seriously damage the ability of this government to conduct signals intelligence and the ability of this government to carry out its mission of protecting national security information from hostile exploitation.

-- Admiral Bobby Ray Inman (Director of the NSA, 1979)

FEDERAL BUREAU OF INVESTIGATION

Unless the issue of encryption is resolved soon, criminal conversations over the telephone and other communications devices will become indecipherable by law enforcement. This, as much as any issue, jeopardizes the public safety and national security of this country. Drug cartels, terrorists, and kidnappers will use telephones and other communications media with impunity knowing that their conversations are immune from our most valued investigative technique.

- FBI Director Louis Freeh, testimony before the House Judiciary Committee, March 30, 1995

CALEA, October 1994

… a telecommunications carrier … shall ensure that its equipment, facilities, or services … are capable of … expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept … all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier concurrently with their transmission to or from the subscriber's equipment, facility, or service, or at such later time as may be acceptable to the government …

TOP SECRET

TOP SECRET

30007

THE WHITE HOUSE

WASHINGTON

January 17, 1991

MEMORANDUM FOR THE HONORABLE DICK CHENEY
Secretary of Defense

THE HONORABLE WILLIAM P. BARR
Attorney General

THE HONORABLE ROBERT M. GATES
Director of Central Intelligence

SUBJECT: Legislative Strategy for Digital Telephony (S)

On December 30, 1991, I sent to the President a memorandum seeking his approval for a legislative strategy for digital telephony. The substance of that memorandum is attached. On January 15, 1992, he approved the following course of action:

- Justice should go ahead now to seek a legislative fix to the digital telephony problem, and all parties should prepare to follow through on the encryption problem in about a year. Success with digital telephony will lock in one major objective; we will have a beachhead we can exploit for the encryption fix; and the encryption access options can be developed more thoroughly in the meantime. (TS)

Brent Scowcroft

Attachment

TOP SECRET
Declassify on: OADR

TOP SECRET

10

Clipper

- Designed by the NSA: “For telephones only”
- Authorized by classified Clinton directive in April 1993 (publicly announced only that they were evaluating it). Standards released in Feb. 1994
- “Voluntary” (but government will buy only Clipper phones)
- Built-in (“back door”) key that is split: each half held by a different government agency
- Encryption algorithm classified: Clipper chips must be tamperproof and therefore expensive
- Clipper phones do not interoperate with non-Clipper phones
- “Capstone” chip for computer data and communications

Export controls

- Encryption technology classified by State Department as a “munition” (until December, 1996)
- Illegal to export hardware, software, technical information
- Illegal to provide material or technical assistance to non-US personnel, including posting on the internet to be available outside the US
- In December, 1996, jurisdiction transferred to Commerce Department, but restrictions remain.
- Export regulations being challenged in the courts (*Bernstein v. US Dept. of State, et. al.*)

NIST meetings with industry, Fall 95

- Allow export of up to 56-bit algorithms, provided the keys are escrowed with government approved “escrow agents”
- But
  - no interoperability between escrowed and non-escrowed systems
  - escrow cannot be disabled
  - escrow agents must be certified by US government or by foreign governments with whom US has formal agreements
- Talks broke down

Interagency working group draft, May 96

- *Industry and government must partner in the development of a public key-based key management infrastructure and attendant products that will assure participants can transmit and receive information electronically with confidence in the information's integrity, authenticity, and origin and which will assure timely lawful government access.*
- Escrow is the price of certification (CA might be also function as an EA)

Courting industry, Fall 96 - ...

- Shift jurisdiction of crypto exports from State to Commerce
- Allow export of any strength, so long as has key escrow (now known as key recovery - KR)
- Immediate approval of export for 56-bit DES, provided company files a plan for installing KR in new 56-products within two years
- Increased granting of export licenses for restricted applications (e..g, financial transactions)

Legislation, 1997

- Bills introduced all over the map, ranging from elimination of export controls to bills that would mandate key recovery for domestic use.

The RISKS of Key Recovery, Key Escrow, & Trusted Third Party Encryption

A Report by an Ad Hoc Group of Cryptographers and Computer Scientists

- Hal Abelson
- Ross Anderson
- Steven M. Bellovin
- Josh Benaloh
- Matt Blaze
- Whitfield Diffie
- John Gilmore
- Peter G. Neumann
- Ronald L. Rivest
- Jeffrey I. Schiller
- Bruce Schneier

Some technical observations

- If Alice and Bob can authenticate to each other, then they can use Diffie-Hellman to establish a shared key for communications
- The security requirements for CAs are very different from those for escrow agents
- Implementing basic crypto is cheap, adding a key recovery infrastructure is not.
- Crypto is necessary not only for electronic commerce, but to protect the information infrastructure. But key escrow may make things less secure, not more:
  - Repositories of escrowed keys could be irresistible targets of attack by criminals
  - If thousands of law enforcement personnel can quickly get access to escrowed keys, then **who else can??**

More recently …

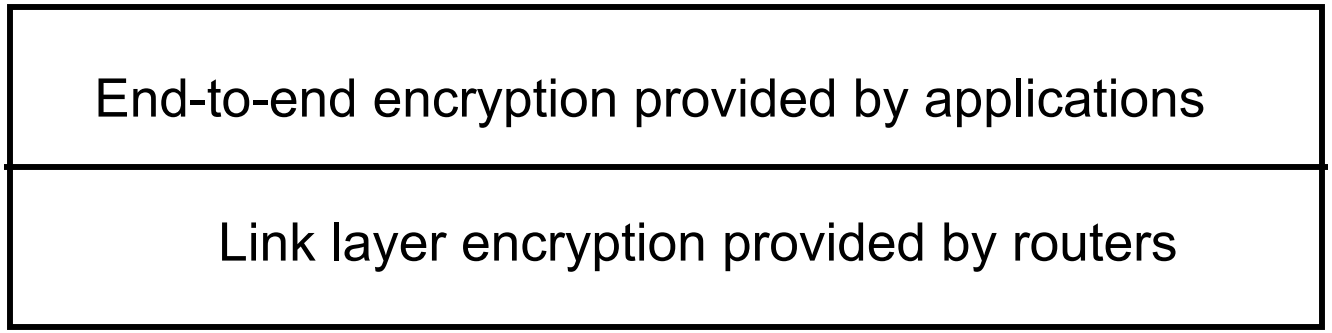
- Jan, 2000: Commerce Department issues new export regulations on encryption, relaxing restrictions
- Sept. 13, 2001: Sen. Judd Gregg (New Hampshire) calls for encryption regulations, saying encryption makers "have as much at risk as we have at risk as a nation, and they should understand that as a matter of citizenship, they have an obligation" to include decryption methods for government agents.
- By Oct., Judd had changed his mind about introducing legislation.

END

“Private doorbell” system

- Proposed by CISCO, summer 1998
- Encryption done in the network routers.
- Every router has a “back door channel” that lets the operator get at the unencrypted data.
- Government goes to operator with warrant, operator provides plaintext.
- Claim that routers with this capability should be exportable.

Encryption can happen at multiple levels



Industry claims and issues

- Customers want security for electronic commerce, for protecting remote access, for confidentiality of business information.
- Export restrictions are a pain in the butt.
- There is plausible commercial demand for “exceptional access” to stored encrypted data (e.g., is someone loses a key); but little demand for access to encrypted communications, and no commercial demand for surreptitious access.

Law enforcement claims and issues

- Wiretapping is a critical law-enforcement tool.
- Wiretaps are conducted on specific, identified targets under lawful authority.
- For wiretapping, access to escrowed keys must occur without knowledge of the keyholders.
- Many criminals are often sloppy and/or stupid: They won't use encryption unless it becomes ubiquitous. Some criminals are far from sloppy or stupid: They will use encryption if it is available.
- Evidence obtained from decryption must hold up in court.
- There is a need for international cooperation in law enforcement.

National security establishment claims and issues

- We can't tell you, but they are really serious.
- NSA is rumored to be carrying out blanket interceptions of communications on a massive scale, using computers to filter out the "interesting" traffic.

Civil libertarian claims and issues

- As computer communication technology becomes more pervasive, allowing government access to communications becomes much more than traditional wiretapping of phone conversations.
- How do we guard against abuse of the system?
- If we make wiretapping easy, then what are the checks on its increasing use?
- There are other tools (bugging, data mining, DNA matching) that can assist law enforcement. People have less privacy than previously, even without wiretapping.

Some architecture/policy issues

- Are we worrying about access to stored data, or eavesdropping on communication channels, or both?
- Where do keys come from? Who generates them?
- Do we treat signature keys differently from encryption keys?
- Who can be an authorized escrowed agent? Can people escrow their own keys?
- Who has liability if escrowed keys are compromised?
- What are the legal standards for getting access to escrowed keys?
- Why should people use these systems? (E.g., regulations, legal sanctions, tax incentives, liability incentives, … .)

Food for thought …

- What parallels do you see between this history of encryption control and the more recent developments in copyright control?
  - What are some major similarities?
  - What are some major differences?
  - Are there any lessons you can draw?