1.264 Lecture 17

Web security, part 2

Certifying authorities and public keys

- How to obtain public keys
  - Can’t keep all possible recipient keys on your system
  - Can’t ask recipient to send it to you, because he/she might be spoofer
  - Don’t (can’t?) have large public database:
    - Costs, performance for hundreds of millions of keys a concern
- Certifying authorities (CAs)
  - Commercial entities, whose public keys are in your browser
  - Ask user to send you their digital certificate, signed by a CA, before you communicate with them
  - From certificate, you verify their identity and get their public key
  - CA encrypts the certificate and its hash with the CA’s private key
  - User (you) decrypts the certificate with the CA public key and check the hash to make sure the certificate has not been altered

Obtaining a digital certificate for your server

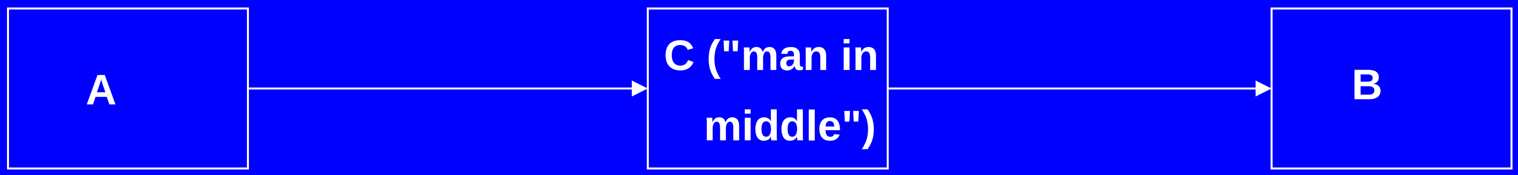
1. Generate a public/private key pair on your system
2. Keep private key and send "certificate request" to CA:
   - Includes public key and identifying information about you
3. Pay CA fee
4. CA verifies your identity, cursorily or extensively
5. If you are ok, CA creates certificate body with your public key and ID info:
   - Server ("site") certificate has URL
   - Browser ("personal") certificate has name and email address
6. CA generates message digest from certificate and signs it with its private key, creating the actual certificate
7. CA sends certificate to you.

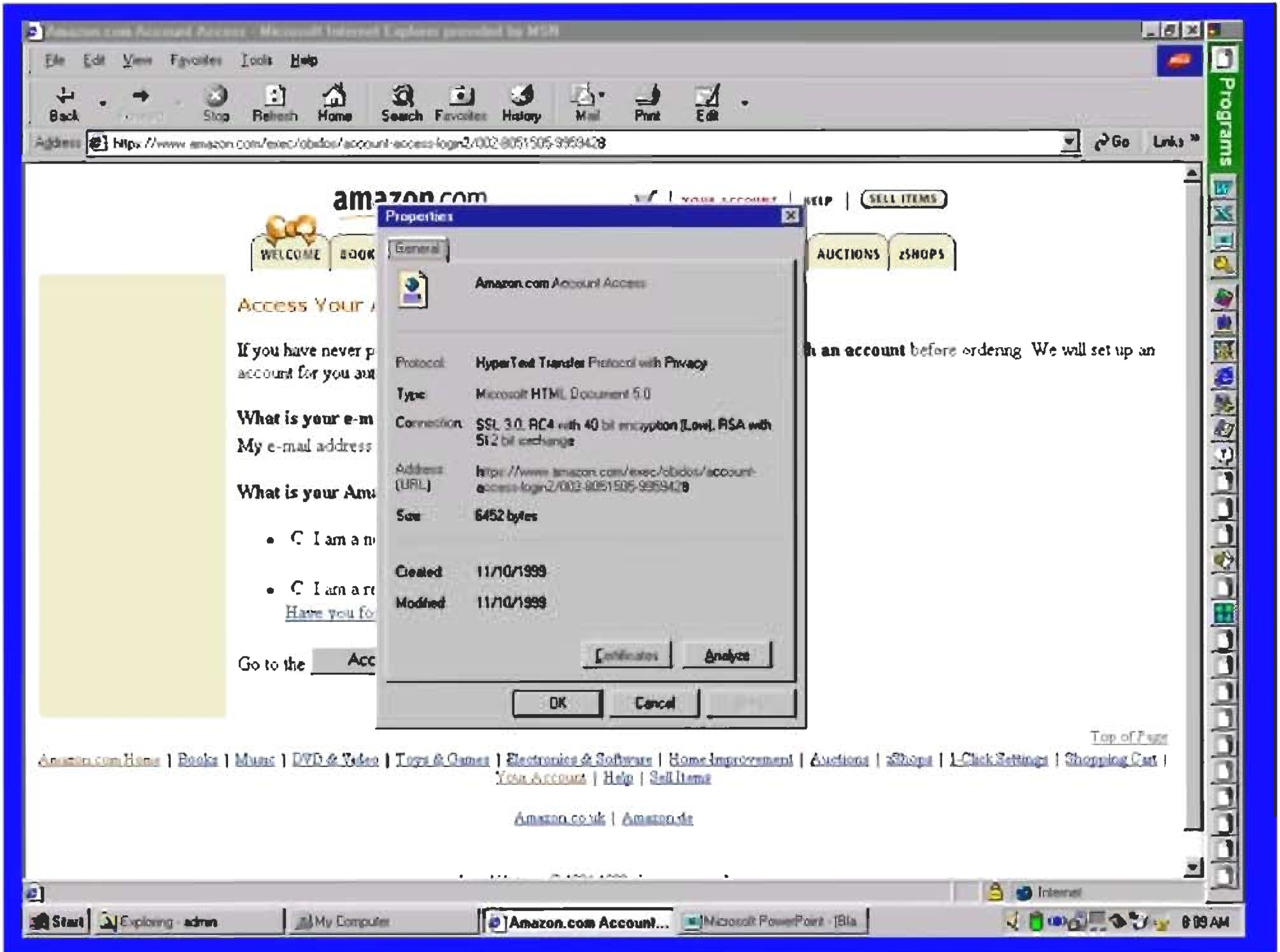
Root CAs and certificate chains

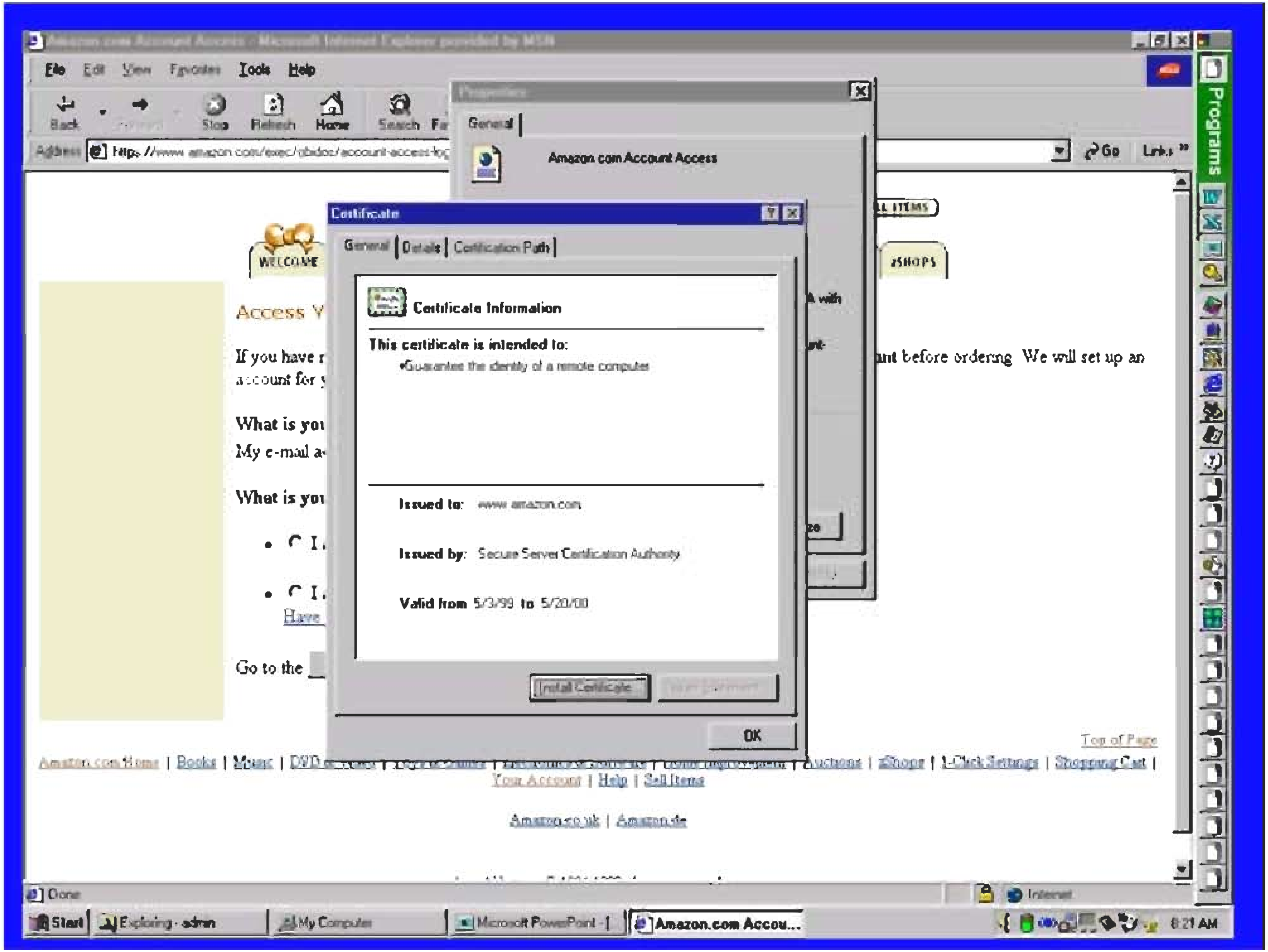
- Root CAs have certificates on browser or Web server
  - Must believe Microsoft, Netscape and your system vendor are ok
- Root CAs can sign other CA's public keys
  - Signature includes the root CA's certificate
  - Chains of certificates can be created
    - Last certificate contains certificates of every CA in the chain, so it can be traced back to the original root CA
    - You use first CA's public key to get 2nd CA's public key, which you use to get 3rd CA's public key, etc.
    - Chains typically used in intranets today to verify browsers via a chain of servers
    - SET and digital payment schemes also use chains
- It's reasonable to generate and administer your own public and private keys when number of sites is limited

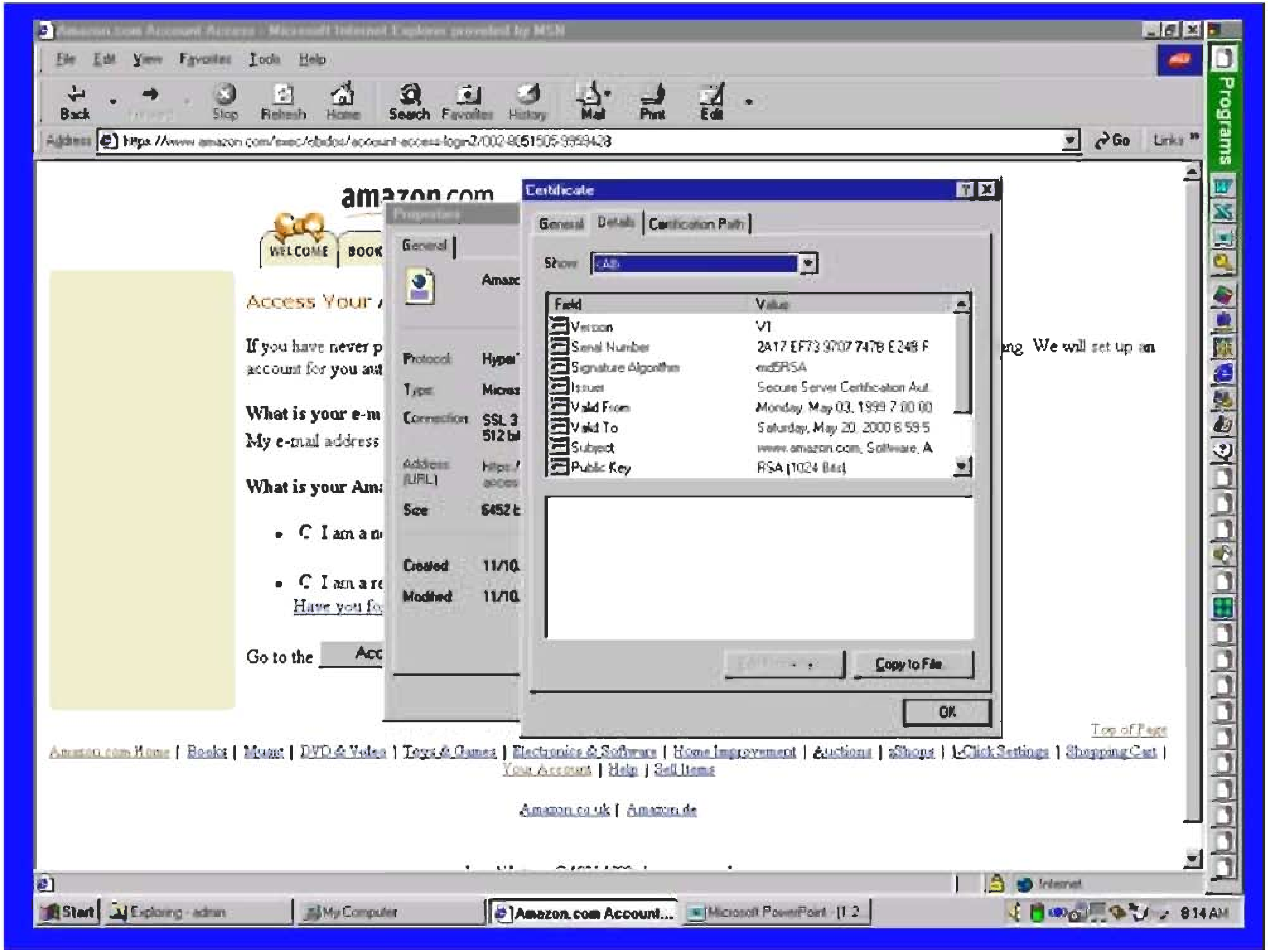
Certificate problems

- Events invalidating public/private key pair
  - Theft, change of ID info, compromise of key
  - Disk corruption (private key is encrypted via password on disk)
  - Certificate revocation list (CRL) intended but often not implemented
    - Technically, should check against CRL before communicating
  - Certificates generally expire in a year, but that’s a long time…
- Privacy is impossible, because you are identified to other party
  - Diffie-Hellman algorithm allows encryption w/o authentication
  - D-H is susceptible to ‘man in the middle’ attacks:

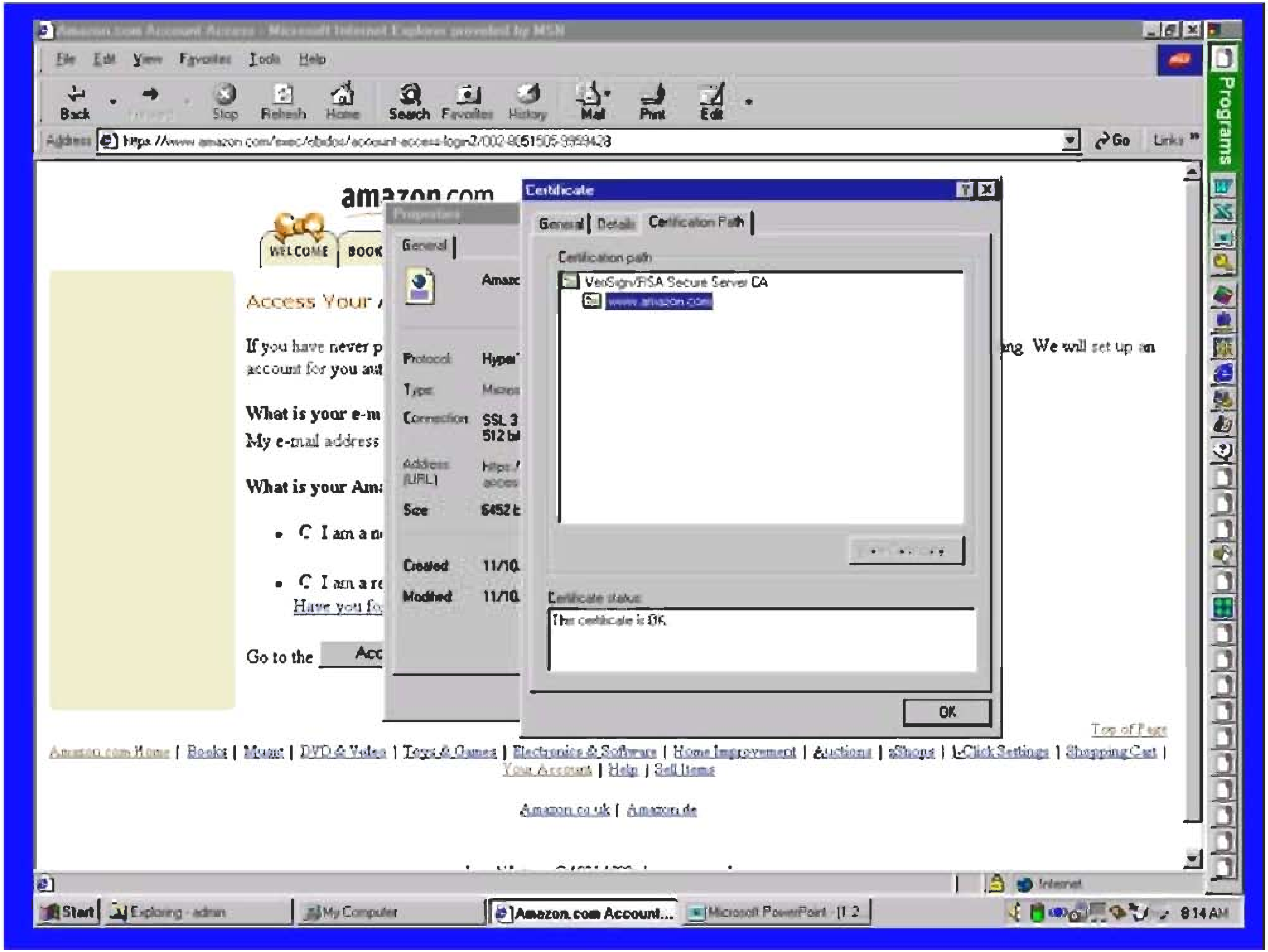



File Edit View Favorites Tools Help
Back Stop Refresh Home Search Favorites History Mail Print Edit
Address https://www.amazon.com/exec/obidos/account-access-login2/002-8051505-9959428
Go Links
amazon.com
YOUR ACCOUNT | HELP | SELL ITEMS
WELCOME BOOK AUCTIONS zSHOPS
Access Your
If you have never p
account for you au
an account before ordering. We will set up an
What is your e-m
My e-mail address
What is your Am
I am a n
I am a r
Have you fo
Go to the Acc
Properties
General
Amazon.com Account Access
Protocol HyperText Transfer Protocol with Privacy
Type Microsoft HTML Document 5.0
Connection SSL 3.0, RC4 with 40 bit encryption (Low); RSA with 512 bit exchange
Address (URL) https://www.amazon.com/exec/obidos/account-access-login2/002-8051505-9959428
Size 6452 bytes
Created 11/10/1999
Modified 11/10/1999
Certificates Analyze
OK Cancel
Top of Page
Amazon.com Home | Books | Music | DVD & Video | Toys & Games | Electronics & Software | Home Improvement | Auctions | zShops | 1-Click Settings | Shopping Cart | Your Account | Help | Sell Items
Amazon.co.uk | Amazon.de
Internet
Start Exploring - admin My Computer Amazon.com Account... Microsoft PowerPoint - [Bla
8:09 AM
Programs


File Edit View Favorites Tools Help
Back Stop Refresh Home Search
Address https://www.amazon.com/exec/obidos/account-access-log
Go Links
Programs
Properties
General
Amazon.com Account Access
Certificate
General Details Certification Path
Certificate Information
This certificate is intended to:
•Guarantee the identity of a remote computer
Issued to: www.amazon.com
Issued by: Secure Server Certification Authority
Valid from 5/3/99 to 5/20/00
Install Certificate
OK
WELCOME
zSHOPS
Access Y
If you have r
account for y
What is you
My e-mail a
What is you
Have
Go to the
unt before ordering. We will set up an
Top of Page
Auctions | zShops | 1-Click Settings | Shopping Cart |
Your Account | Help | Sell Items
Amazon.co.uk | Amazon.de
Done
Internet
Start
Exploring - admn
My Computer
Microsoft PowerPoint - [
Amazon.com Accou...
8:21 AM



File Edit View Favorites Tools Help
Back Stop Refresh Home Search Favorites History Mail Print Edit
Address
Go
Links
amazon.com
WELCOME
BOOK
Access Your
If you have never p
account for you an
We will set up an
What is your e-m
My e-mail address
What is your Am
I am a n
I am a re
Have you fo
Go to the
Properties
General
Protocol:
Type:
Connection:
SSL 3
Address (URL):
Size:
Created:
Modified:
Certificate
General
Details
Certification Path
Show:
Field
Value
Version
V1
Serial Number
Signature Algorithm
md5RSA
Issuer
Secure Server Certification Aut
Valid From
Monday, May 03, 1999 7:00:00
Valid To
Saturday, May 20, 2000 6:59:5
Subject
www.amazon.com, Software, A
Public Key
RSA (1024 Bits)
Copy to File
OK
Top of Page
Amazon.com Home | Books | Music | DVD & Video | Toys & Games | Electronics & Software | Home Improvement | Auctions | zShops | 1-Click Settings | Shopping Cart | Your Account | Help | Sell Items
Amazon.co.uk | Amazon.de
Internet
Start
Exploring - admin
My Computer
Amazon.com Account...
Microsoft PowerPoint
Programs


File Edit View Favorites Tools Help
Back
Stop
Refresh
Home
Search
Favorites
History
Mail
Print
Edit
Address
Go
Links
Programs
amazon.com
WELCOME
BOOK
Access Your
If you have never p
account for you an
What is your e-m
My e-mail address
What is your Am
I am a n
I am a r
Have you fo
Go to the
Properties
General
Protocol:
Type:
Connection:
SSL 3
512 bi
Address: (URL)
Size:
Created:
11/10
Modified:
11/10
Certificate
General
Details
Certification Path
Certification path
VeriSign/RSA Secure Server CA
www.amazon.com
Certificate status
This certificate is OK.
OK
ing. We will set up an
Top of Page
Amazon.com Home | Books | Music | DVD & Video | Toys & Games | Electronics & Software | Home Improvement | Auctions | zShops | 1-Click Settings | Shopping Cart |
Your Account | Help | Sell Items
Amazon.co.uk | Amazon.de
Internet
Start
Exploring - admin
My Computer
Amazon.com Account...
Microsoft PowerPoint
8:14 AM

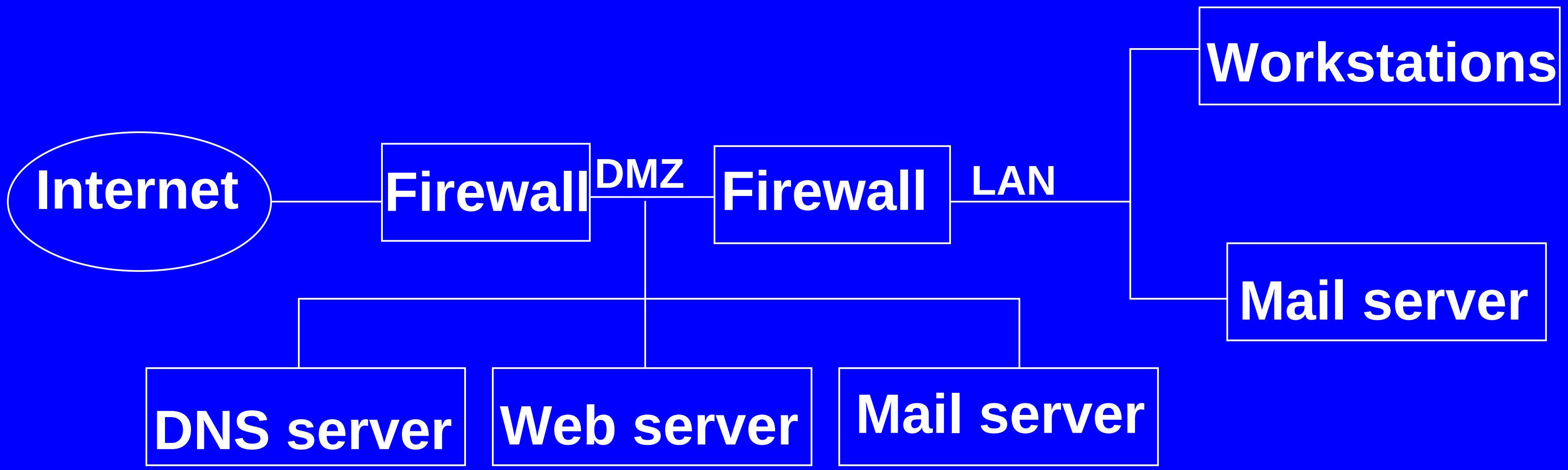
Secure IP: IPsec

- At what layer (1,2,3,4 or 7?) does SSL work?
- TCP/IP (and IP itself) are not secure
  - Never intended for current use
- IPsec allows encryption of TCP/IP headers and/or data
  - IPsec requires replacing TCP/IP stack of every PC accessing server
  - No one wants the support costs of this; it will happen slowly
  - IPSec is very similar to SSL but encrypts IP packets (which contain HTTP and HTML traffic)
  - IPSec must work in many more situations and is much more complex
- Keys, certificates, etc. make up Public Key Infrastructure (PKI). Certificates are X.509 standard, PKI is various others
- This entire lecture has been essentially about network security
  - We now turn to server and client security briefly
  - Server security is mostly a matter of configuration and care

Firewalls

- Without firewalls, weakest PC on internal network can be attacked and compromised, and in turn compromise others
  - Attacker replaces some PC operating system calls with his/her own, or wreaks other havoc
  - Almost impossible to monitor all PCs for suspicious activity
- Firewalls place special machine between internal network and Internet
  - Direct traffic from PCs to Internet not allowed; all traffic via firewall
- Firewall runs stripped-down version of Windows or UNIX
  - No unnecessary services, no untrusted software
  - Logs of all activity
  - Application level proxies inspect packets (intrusion detection)
    - Layer 7: HTTP (port 80) proxy can search for and disallow binary payloads
    - Layer 3 and 4: Packet-level proxies look at headers, destinations…

Firewall configuration



Firewall:

- Filters based on TCP/IP headers (source, destination…)
- Disallows direct connections across firewall (proxy)
- Application level firewall inspects packet contents
  - E.g., scans email for viruses, HTTP for binaries
- Audit

Current Security Issues

- Denial of service (DoS), distributed denial of service (DDoS)
  - Packet floods (TCP-SYN, ACK, RST; UDP; ICMP-ping)
  - Source of flood is often a compromised system
  - IP spoofing (fake IP source address) is often used
  - TCPv4 is not designed with security/protection features
  - ‘Kits’ exist on Internet to generate such attacks
    - User interface to select target, type of attack, machines to compromise if possible
  - Microsoft systems targeted more than UNIX now; UNIX was primary target earlier
  - Chat (IRC) used to control agents, spread attacks
  - High degree of automation in DoS attacks

Current Security Issues, p.2

- DNS attacks (BIND)
  - Solution is to run latest version of DNS
- CGI script holes
  - Most example scripts on Net have security holes
  - Don’t use CGI
- Remote procedure calls (COM, CORBA, other)
  - Disable if not using; move to SOAP
- Microsoft IIS Web server
  - Some recommend switching to Apache/Tomcat
  - Microsoft needs to patch all the vulnerabilities
- Sendmail (UNIX) runs with root privilege
  - Upgrade to latest version. Was written as grad student project
- NFS, mountd, shares for mounting remote disks (UNIX, Win)
  - Gives root privilege (UNIX), default read-write permissions (Win)
- Accounts with weak or no passwords, including root/Admin
- IMAP, POP email protocols have weak security
- SNMP has weak security (default password ‘private’ rarely reset)
  - Can let hacker control routers.

Types of threats

- All these weaknesses are exploited by:
  - Worms: Program copies itself to other machines and propagates itself
  - Viruses: Program alters or infects existing programs or files, which then propagate it
  - Trojans: Program that neither copies nor replicates, but directly damages the attacked system. Typically spread by email.
  - Definitions at http://www.symantec.com/avcenter/refa.html

Security Initiatives

- **Proof-carrying code, proof-carrying authorization**
  - Server-sent code contains safety proof that code complies to a stated security policy
  - Client has proof validator
- **Smart cards, biometrics for authentication**
  - Can be defeated fairly easily still (fake fingers, iris copies…)
- **Advanced Encryption Standard (AES) or Rijndael algorithm, to replace DES**
  - 128 to 256 bit symmetric key algorithm. See nist.gov
- **Firewalls with cryptographic analysis of programs**
  - ZoneAlarm is free and effective
- **Intrusion detection**
  - Analyze network traffic, examine individual packets within data stream to identify threats from authorized users, hackers who have thwarted control systems

Security Realities

- People are the major issue
  - Tiger team results
  - Simple passwords, on post-it notes. Etc.
- Security in most systems is weak
  - Even with certificates, encryption, PKI, etc., if a password is weak, you can get someone's certificate
  - Most software has a lot of bugs, and some can be exploited by attackers. Unless software is correct, security is hard to do.
- Security is based on
  - Prevention: client, server, network configuration
  - Detection: firewall and other analysis
  - Response: software, hardware, configuration changes
- Security always has a large performance hit

Summary

- Public key infrastructure (PKI) for network security
  - Certificates, encryption, certificate authorities, IPsec (future)
  - Expensive currently
  - Multivendor implementations don’t work well
  - Expected to improve over the next few years
- Move to XML, XSL, XSchema, and de-emphasis of JavaScript, applets, etc. for client security
  - XML can be sent and received symmetrically by clients, servers
  - Uses port 80 (HTTP) which is a fairly safe (restricted) protocol
- Continued improvement in server operating systems for server security, and client systems for client security
  - CERT (www.cert.org), other security services continue alerts, fixes
  - Windows, Linux automated updates