Distributed Systems

Protection & Security

Paul Krzyzanowski
pxk@cs.rutgers.edu

You need to get into a vault

- Try all combinations.
- Try a subset of combinations.
- Exploit weaknesses in the lock's design.
- Open the door (drilling, torch, …).
- Back-door access: walls, ceiling, floor.
- Observe someone else opening
  - note the combination.

You need to get into a vault

- Ask someone for the combination.
  - Convince them that they should give it.
  - Force it (gunpoint/threat).
- Convince someone to let you in
- Find a combination lying around
- Steal a computer or file folder that has the combination.
- Look through the trash

What can the bank do?

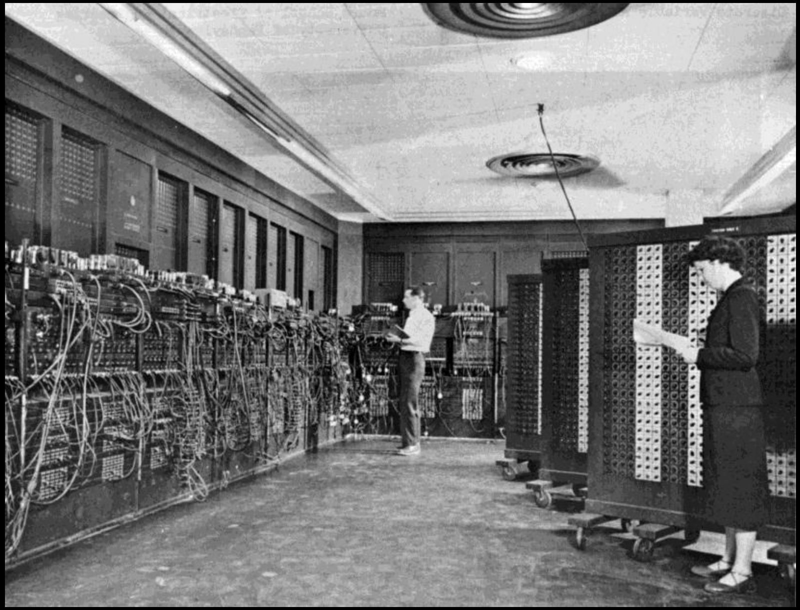
- Install a better lock
  - What if theirs is already good?
- Restrict physical access to the vault (guards)
  - You can still use some methods
- Make the contents of the vault less appealing
  - Store extra cash, valuables off-site
  - This just shifts the problem
- Impose strict policies on whom to trust
- Impose strict policies on how the combination is stored
  - Policies can be broken

Firewalls and System Protection

Computer security… then

Issue from the dawn of computing:

- Colossus at Bletchley Park: breaking codes
- ENIAC at Moore School: ballistic firing tables
- single-user, single-process systems
- data security needed
- physical security



Computer security… now

- Sensitive data of different users lives on the same file servers
- Multiple processes on same machine
- Authentication and transactions over network
  - open for snooping
- We might want to run other people's code in our process space
  - Device drivers, media managers
  - Java applets, games
  - not just from trusted organizations

Systems are easier to attack

Automation

- Data gathering
- Mass mailings

Distance

- Attack from your own home

Sharing techniques

- Virus kits
- Hacking tools

Attacks

- Fraud
- Destructive
- Intellectual Property Theft
- Identity Theft
- Brand Theft
  - VISA condoms
  - 1-800-COLLECT, 1-800-C0LLECT
  - 1-800-OPERATOR, 1-800-OPERATER
- Surveillance
- Traffic Analysis
- Publicity
- Denial of Service

Cryptographic attacks

Ciphertext-only attack

- Recover plaintext given ciphertext
- Almost never occurs: too difficult
- Brute force
- Exploit weaknesses in algorithms or in passwords

Known plaintext attack

- Analyst has copy of plaintext & ciphertext
- E.g., Norway saying "Nothing to report"

Chosen plaintext attack

- Analyst chooses message that gets encrypted

  E.g., start military activity in town with obscure name

Protocol attacks

- Eavesdropping
- Active attacks
  - Insert, delete, change messages
- Man-in-the-middle attack
  - Eavesdropper intercepts
- Malicious host

Penetration

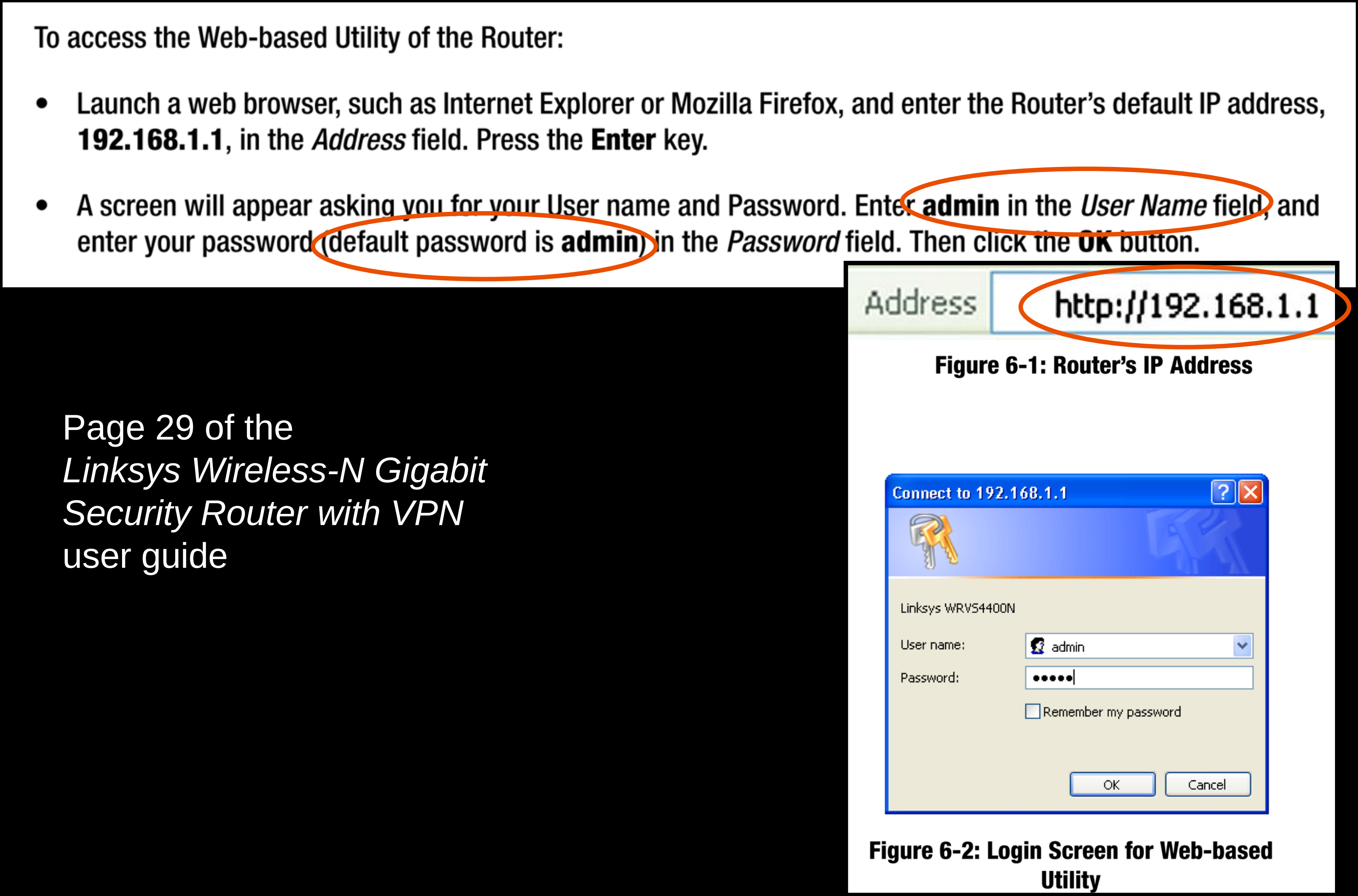
Guess a password

- system defaults, brute force, dictionary attack

Crack a password

- **Online vs offline**
- **Precomputed hashes (see rainbow tables)**
  - **Defense: Salt**

Penetration: Guess/get a password



To access the Web-based Utility of the Router:

- Launch a web browser, such as Internet Explorer or Mozilla Firefox, and enter the Router's default IP address, **192.168.1.1**, in the *Address* field. Press the **Enter** key.

- A screen will appear asking you for your User name and Password. Enter **admin** in the *User Name* field, and enter your password (default password is **admin**) in the *Password* field. Then click the **OK** button.

Address http://192.168.1.1

Figure 6-1: Router's IP Address

Connect to 192.168.1.1

Linksys WRVS4400N

User name: admin

Password: •••••

□ Remember my password

OK Cancel

Figure 6-2: Login Screen for Web-based Utility

Page 29 of the
Linksys Wireless-N Gigabit Security Router with VPN
user guide

Penetration: Guess/get a password

Check out

- http://www.phenoelit-us.org/dpl/dpl.html
- http://www.cirt.net/passwords
- http://dopeman.org/default_passwords.html

Penetration

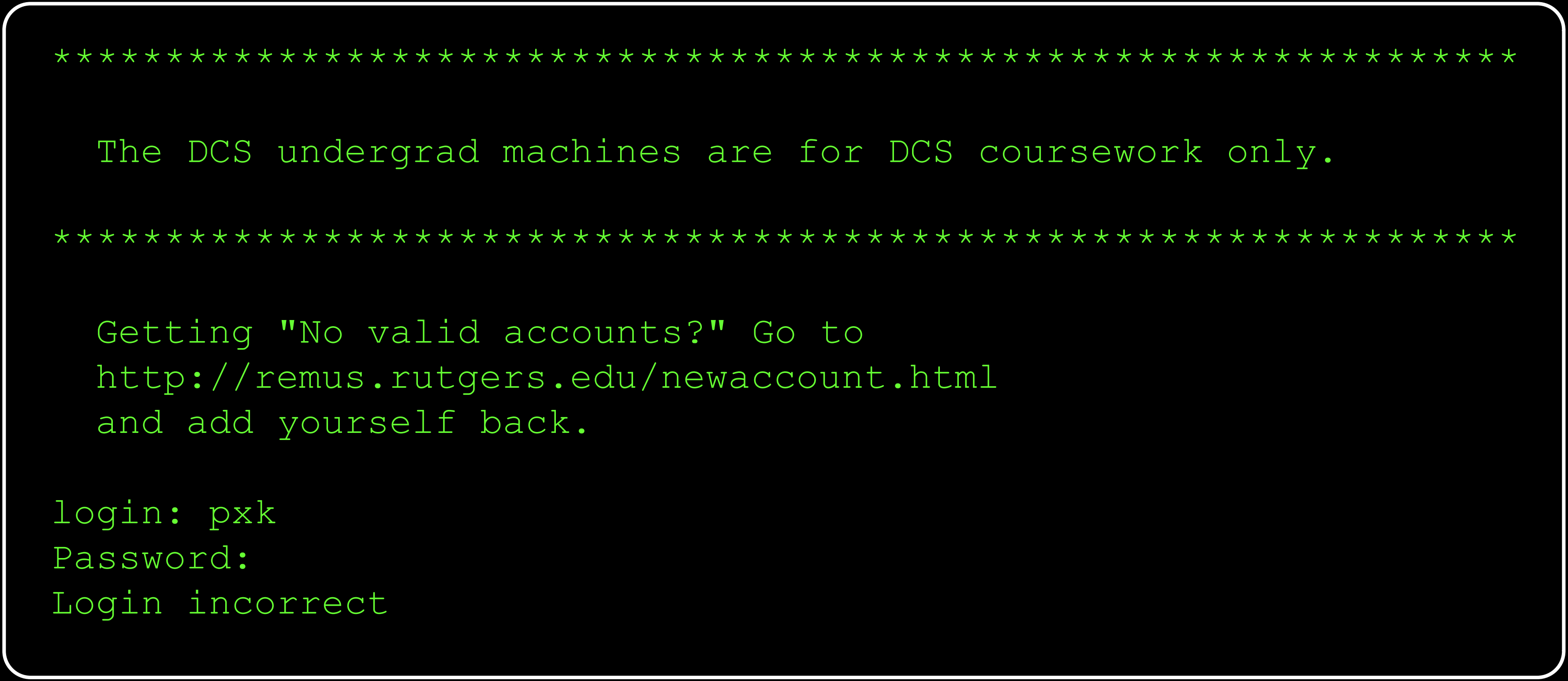
Social engineering

- people have a tendency to trust others
- *finger* sites – deduce organizational structure
- myspace.com, personal home pages
- look through dumpsters for information
- impersonate a user
- Phishing: impersonate a company/service

Penetration

Trojan horse

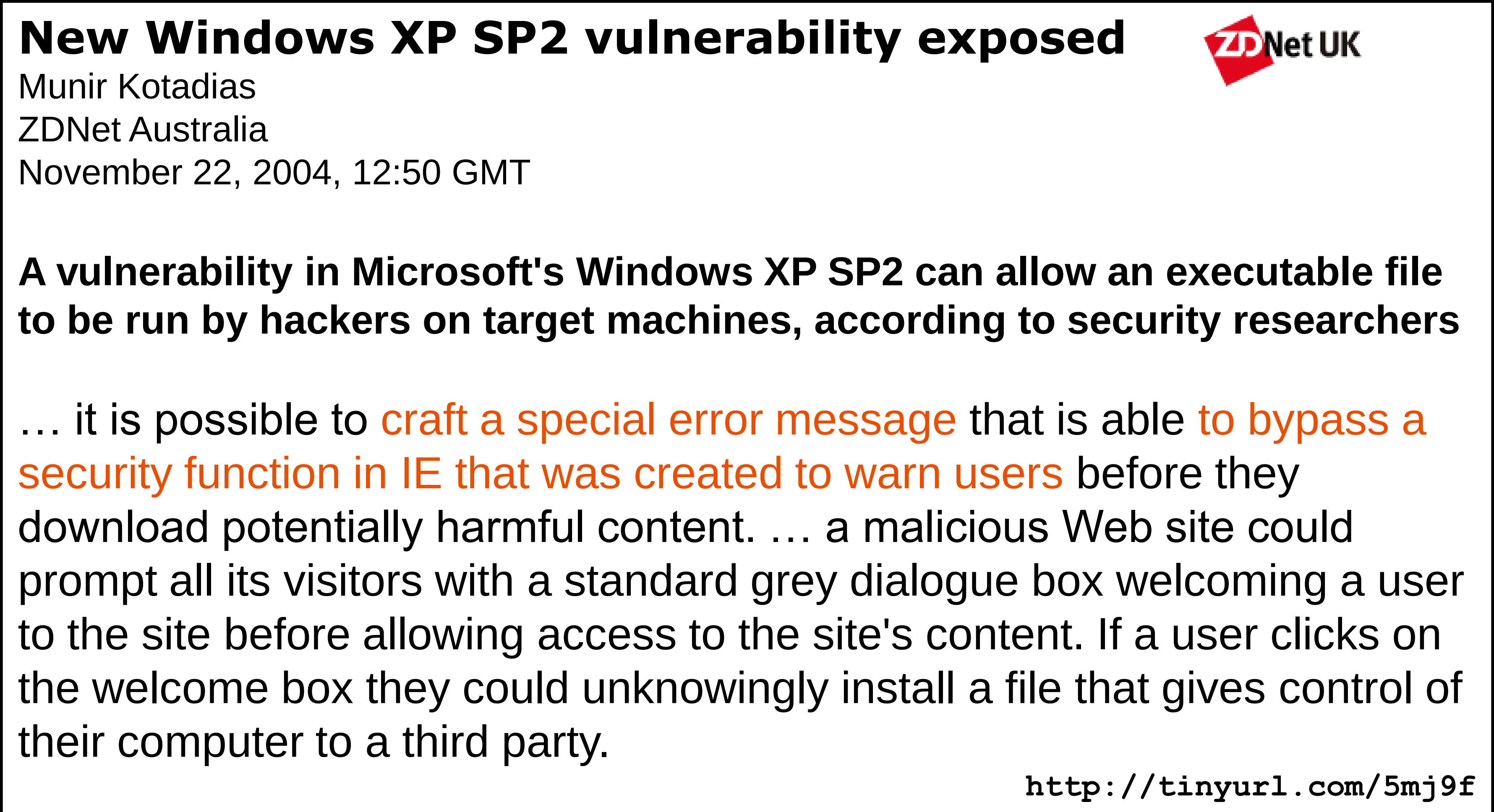
- program masquerades as another
- Get the user to click on something, run something, enter data



```
*****************************************************************

  The DCS undergrad machines are for DCS coursework only.

*****************************************************************

  Getting "No valid accounts?" Go to
  http://remus.rutgers.edu/newaccount.html
  and add yourself back.

login: pxk
Password:
Login incorrect
```

Trojan horse

Disguising error messages



New Windows XP SP2 vulnerability exposed

ZDNet UK

Munir Kotadias
ZDNet Australia
November 22, 2004, 12:50 GMT

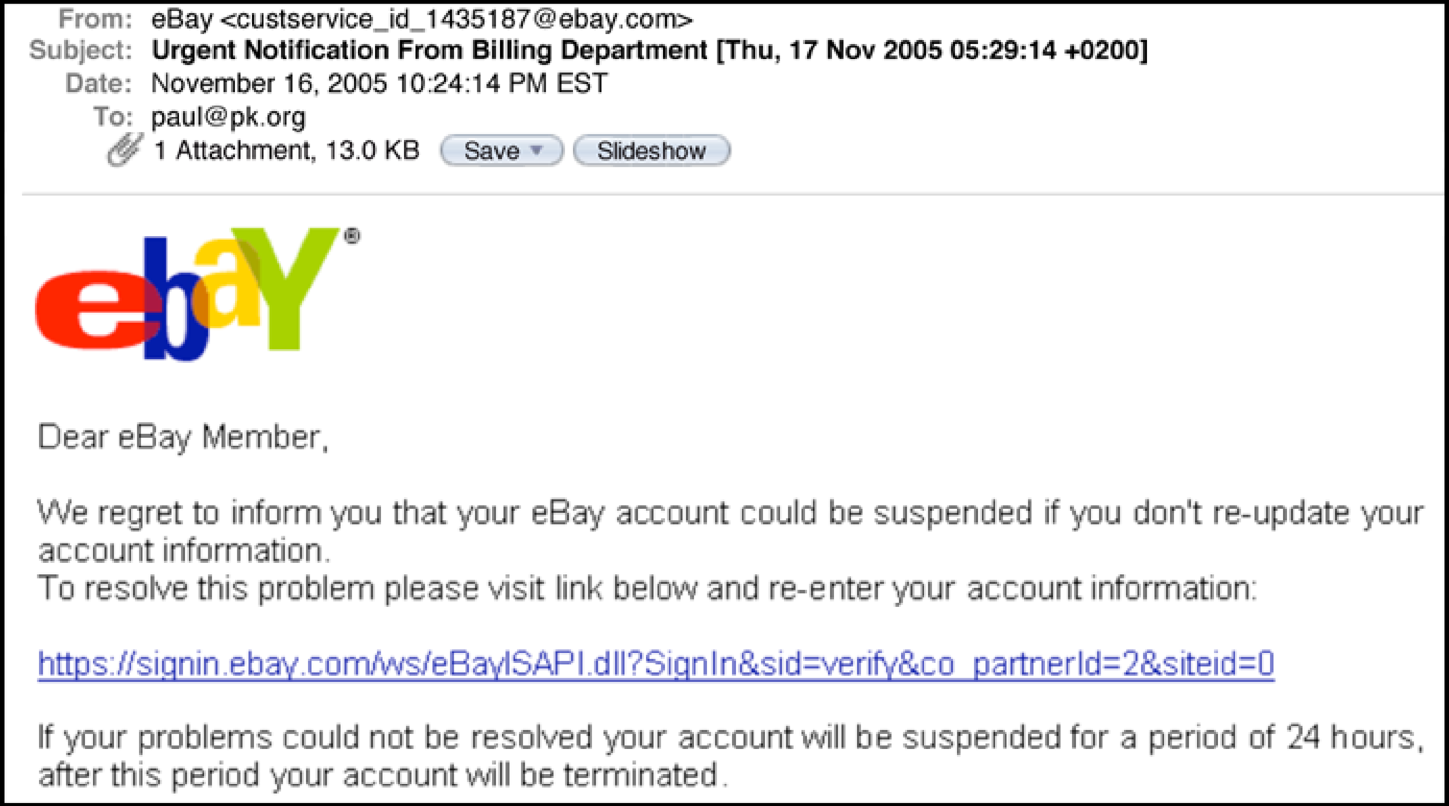
A vulnerability in Microsoft's Windows XP SP2 can allow an executable file to be run by hackers on target machines, according to security researchers

… it is possible to craft a special error message that is able to bypass a security function in IE that was created to warn users before they download potentially harmful content. … a malicious Web site could prompt all its visitors with a standard grey dialogue box welcoming a user to the site before allowing access to the site's content. If a user clicks on the welcome box they could unknowingly install a file that gives control of their computer to a third party.

http://tinyurl.com/5mj9f

Phishing

Masqueraded e-mail



From: eBay <custservice_id_1435187@ebay.com>
Subject: **Urgent Notification From Billing Department [Thu, 17 Nov 2005 05:29:14 +0200]**
Date: November 16, 2005 10:24:14 PM EST
To: paul@pk.org
1 Attachment, 13.0 KB

Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0

If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

Malicious Files and Attachments

Take advantage of:

- Programs that automatically open attachments
- Systems that hide extensions yet use them to execute a program – trick the user

love-letter.txt.vbs

resume.doc.scr

Exploiting bugs

Exploit software bugs

- Most (all) software is buggy
- Big programs have lots of bugs
  - *sendmail, wu-ftp*
- some big programs are *setuid* programs
  - *lpr, uucp, sendmail, mount, mkdir, eject*

Common bugs

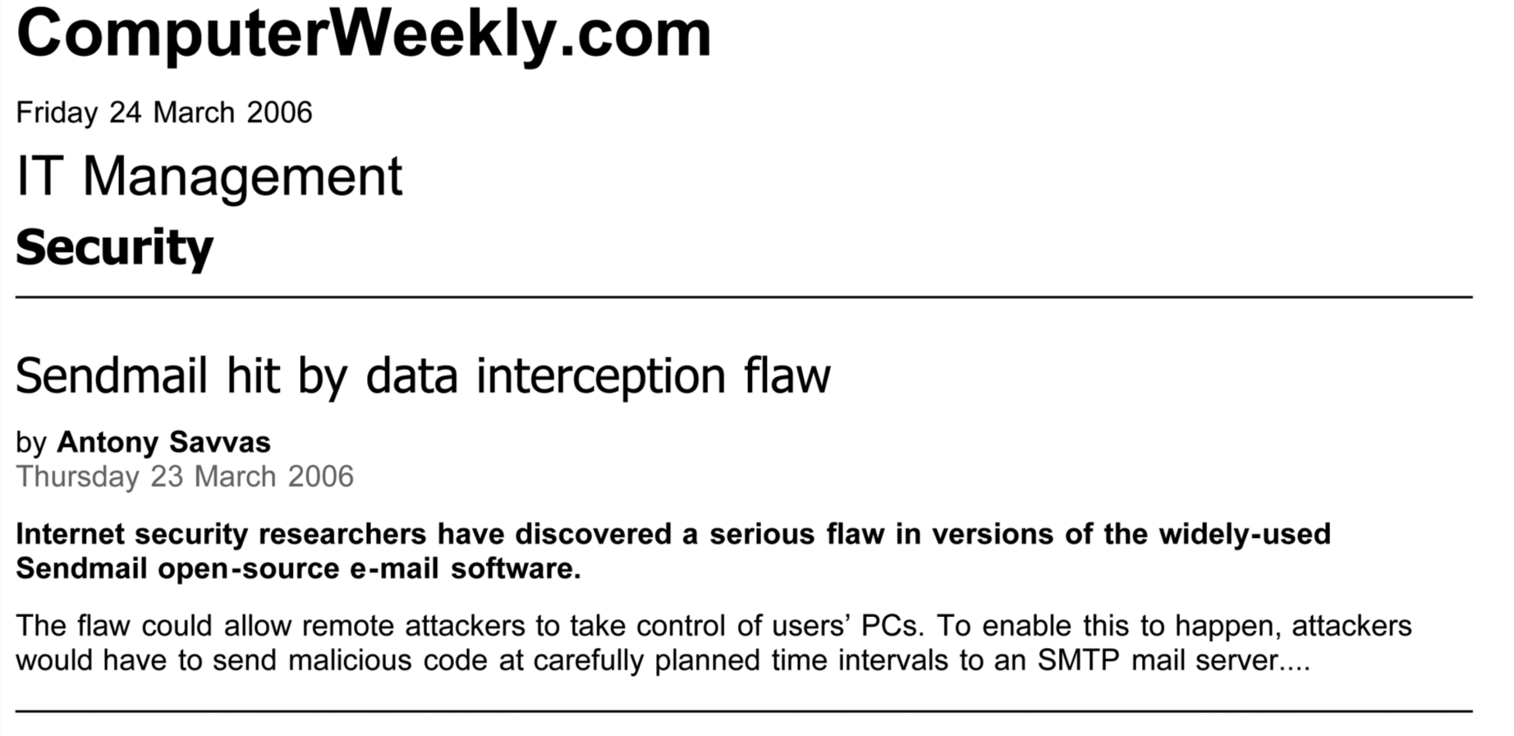
- buffer overflow
  (blindly read data into buffer)
  - e.g., *gets*
- back doors and undocumented options

The classic buffer overflow bug

gets.c from V6 Unix:

```
gets(s)
char *s;
{ /* gets (s) - read a string with cgetc and store in s */
   char *p;
   extern int cin;
   if (nargs () == 2)
       IEHzap("gets  ");
   p=s;
   while ((*s = cgetc(cin)) != '\n' && *s != ’\0')
       s++;
   if (*p == '\0') return (0);
   *s = '\0';
   return (p);
}
```

Buggy software



ComputerWeekly.com

Friday 24 March 2006

IT Management

Security

Sendmail hit by data interception flaw

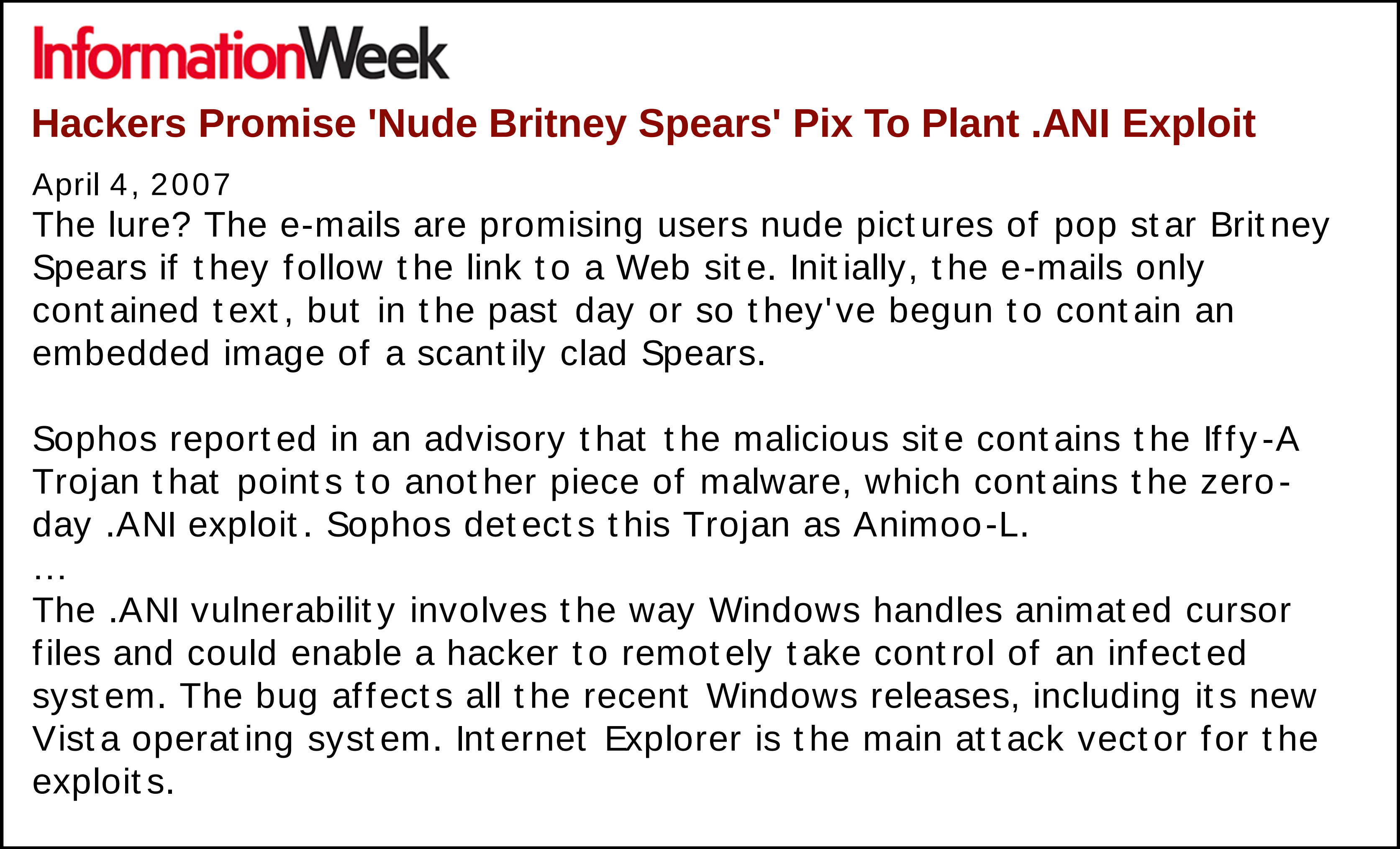
by **Antony Savvas**
Thursday 23 March 2006

Internet security researchers have discovered a serious flaw in versions of the widely-used Sendmail open-source e-mail software.

The flaw could allow remote attackers to take control of users' PCs. To enable this to happen, attackers would have to send malicious code at carefully planned time intervals to an SMTP mail server....

sendmail has been around since 1983!

Buggy software



InformationWeek

Hackers Promise 'Nude Britney Spears' Pix To Plant .ANI Exploit

April 4, 2007

The lure? The e-mails are promising users nude pictures of pop star Britney Spears if they follow the link to a Web site. Initially, the e-mails only contained text, but in the past day or so they've begun to contain an embedded image of a scantily clad Spears.

Sophos reported in an advisory that the malicious site contains the Iffy-A Trojan that points to another piece of malware, which contains the zero-day .ANI exploit. Sophos detects this Trojan as Animoo-L.

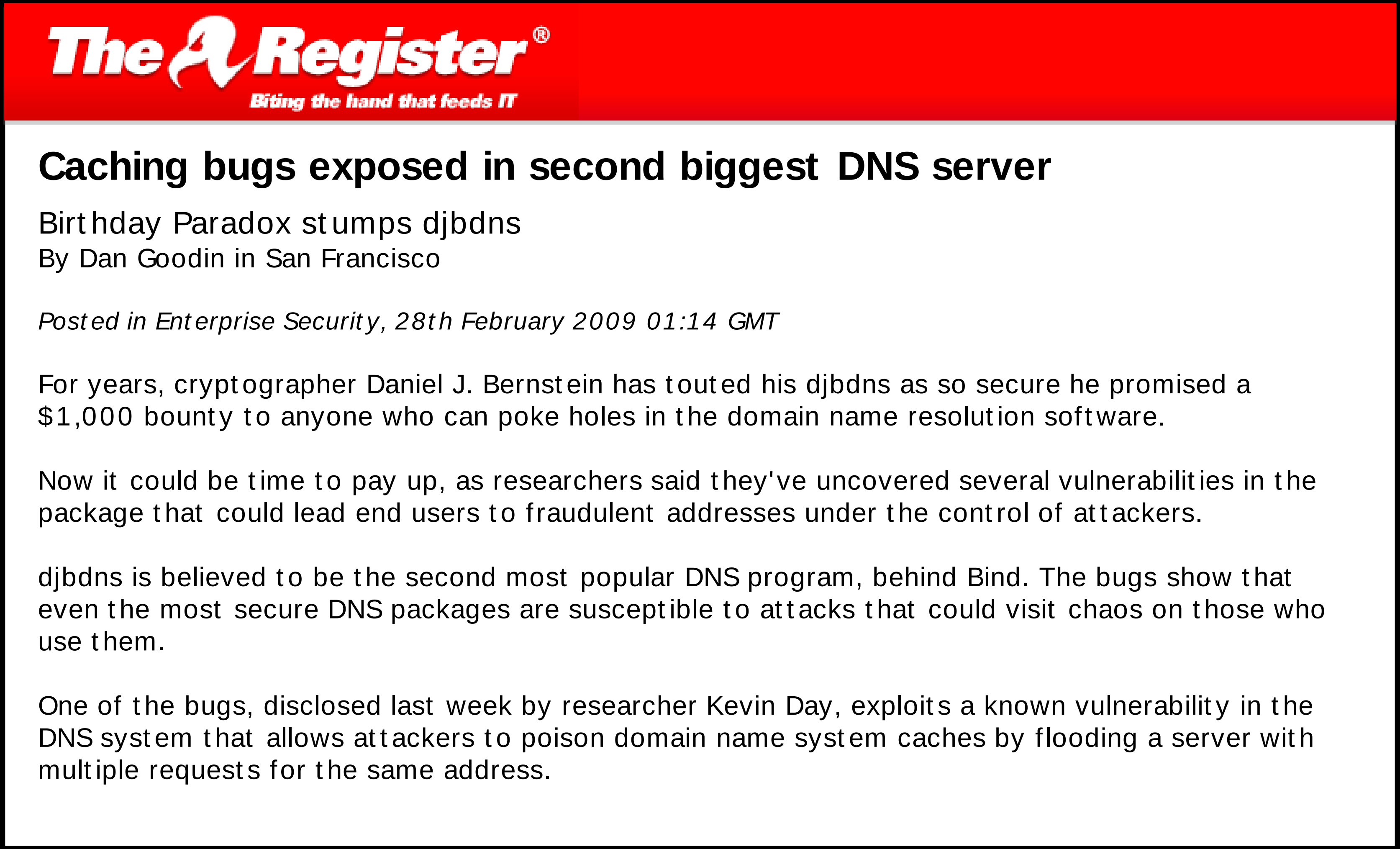
…

The .ANI vulnerability involves the way Windows handles animated cursor files and could enable a hacker to remotely take control of an infected system. The bug affects all the recent Windows releases, including its new Vista operating system. Internet Explorer is the main attack vector for the exploits.

Microsoft: *Vista Most Secure OS Ever!*

http://tinyurl.com/yvxv4h

Buggy software



The Register®
Biting the hand that feeds IT

Caching bugs exposed in second biggest DNS server

Birthday Paradox stumps djbdns
By Dan Goodin in San Francisco

Posted in Enterprise Security, 28th February 2009 01:14 GMT

For years, cryptographer Daniel J. Bernstein has touted his djbdns as so secure he promised a $1,000 bounty to anyone who can poke holes in the domain name resolution software.

Now it could be time to pay up, as researchers said they've uncovered several vulnerabilities in the package that could lead end users to fraudulent addresses under the control of attackers.

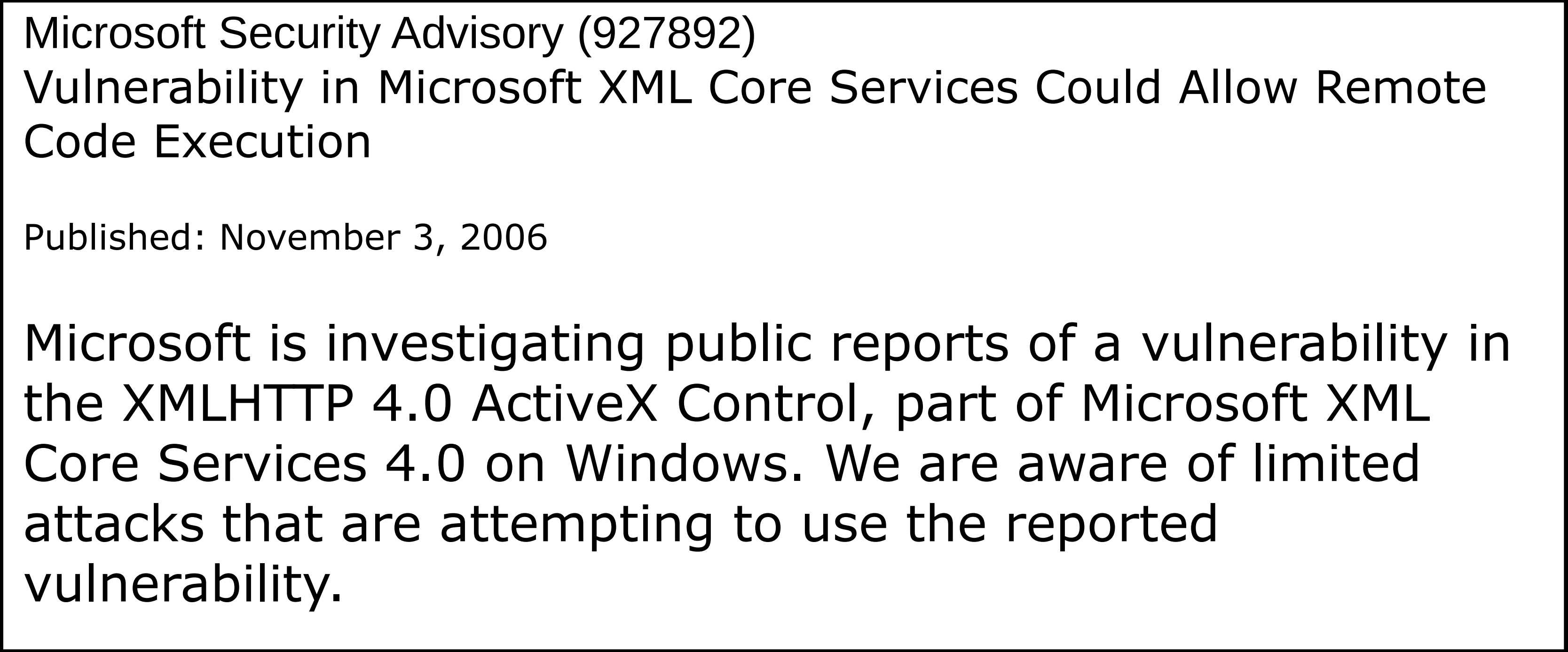
djbdns is believed to be the second most popular DNS program, behind Bind. The bugs show that even the most secure DNS packages are susceptible to attacks that could visit chaos on those who use them.

One of the bugs, disclosed last week by researcher Kevin Day, exploits a known vulnerability in the DNS system that allows attackers to poison domain name system caches by flooding a server with multiple requests for the same address.

DNS bug!

http://tinyurl.com/dclq9b

Buggy software



Microsoft Security Advisory (927892)

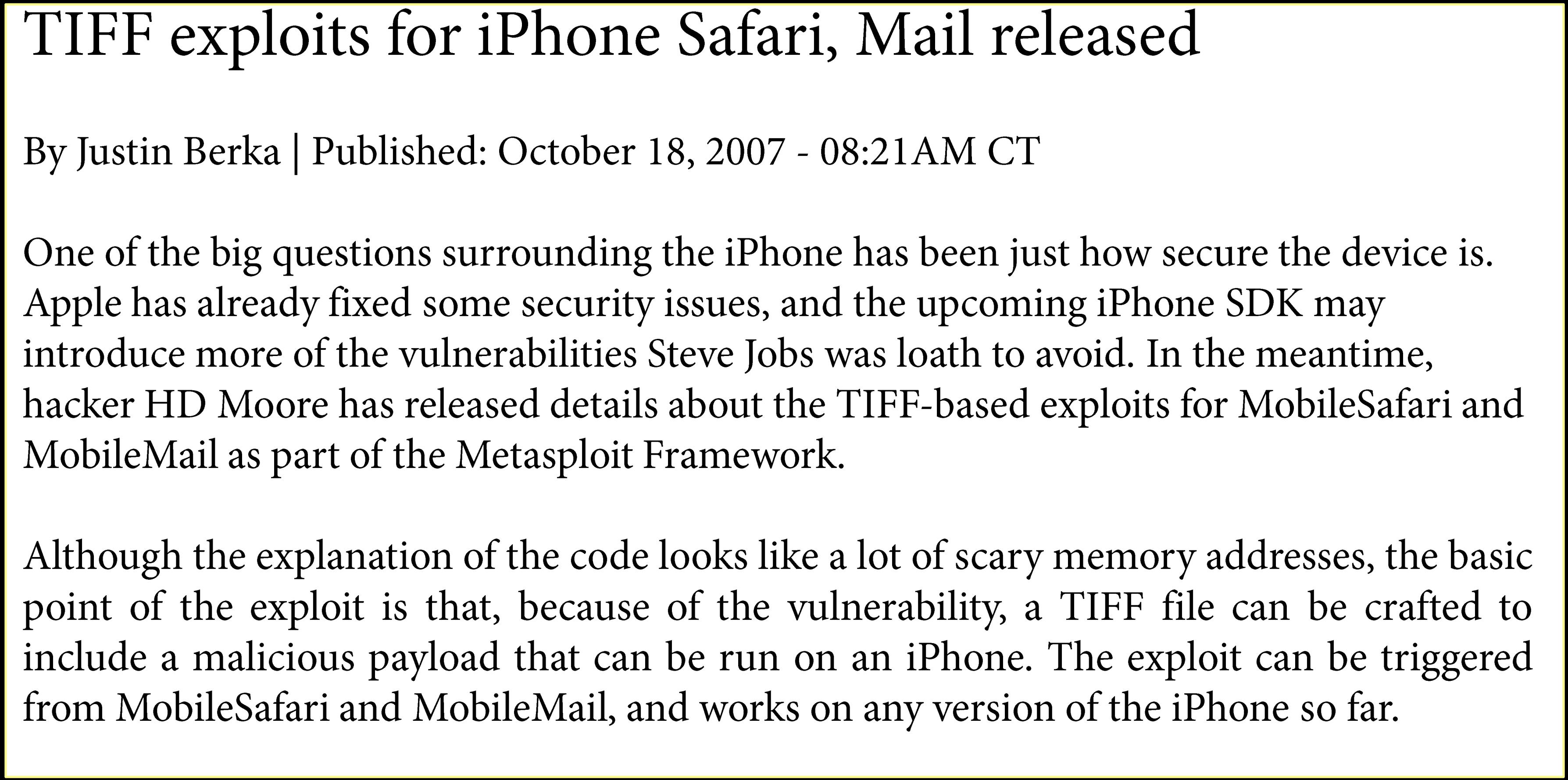
Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution

Published: November 3, 2006

Microsoft is investigating public reports of a vulnerability in the XMLHTTP 4.0 ActiveX Control, part of Microsoft XML Core Services 4.0 on Windows. We are aware of limited attacks that are attempting to use the reported vulnerability.

http://www.microsoft.com/technet/security/advisory/927892.mspx

Buggy Software



TIFF exploits for iPhone Safari, Mail released

By Justin Berka | Published: October 18, 2007 - 08:21AM CT

One of the big questions surrounding the iPhone has been just how secure the device is. Apple has already fixed some security issues, and the upcoming iPhone SDK may introduce more of the vulnerabilities Steve Jobs was loath to avoid. In the meantime, hacker HD Moore has released details about the TIFF-based exploits for MobileSafari and MobileMail as part of the Metasploit Framework.

Although the explanation of the code looks like a lot of scary memory addresses, the basic point of the exploit is that, because of the vulnerability, a TIFF file can be crafted to include a malicious payload that can be run on an iPhone. The exploit can be triggered from MobileSafari and MobileMail, and works on any version of the iPhone so far.

Mistakes (?)

HP admits to selling infected flash-floppy drives

Hybrid devices for ProLiant servers pre-infected with worms, HP says

Gregg Keizer 08/04/2008 07:08:06

Hewlett-Packard has been selling USB-based hybrid flash-floppy drives that were pre-infected with malware, the company said last week in a security bulletin.

Dubbed "HP USB Floppy Drive Key," the device is a combination flash drive and compact floppy drive, and is designed to work with various models of HP's ProLiant Server line. HP sells two versions of the drive, one with 256MB of flash capacity, the other with 1GB of storage space.

Seriously bad when combined with Windows' autorun when a USB drive is plugged in!

- This feature cannot be disabled easily

http://tinyurl.com/5sddlg

Penetration: the network

Fake ICMP, RIP packets

(router information protocol)

Address spoofing

- Fake a server to believe it's talking to a trusted machine

ARP cache poisoning

- No authentication in ARP; blindly trust replies
- Malicious host can provide its own Ethernet address for another machine.

Penetration: the network

Session hijacking

- **sequence number attack**: fake source address and TCP sequence number responses

Penetration

UDP

- no handshakes, no sequence numbers
- easy to spoof

Penetration

Many **network services** have holes

- fake email with SMTP
- *sendmail* bugs
- snoop on *telnet* sessions
- *finger*
  - old versions have *gets* buffer overflow
  - social engineering
- unauthenticated RPC
  - access remote procedures
  - fake *portmapper*, causing your programs to run instead of real service

Penetration

IE

- Malformed URLs
- Buffer overflows
- ActiveX flaws
- PNG display bugs
- Jscript
- Processing of XML object data tags
- Registry modification to redirect URLs

Penetration

- NFS
  - stateless design
  - once you have a file handle, you can access files or mount the file system in the future
  - data not encrypted
- rlogin, rsh
  - modify .rhosts or /etc/hosts.equiv
  - snoop on session
  - fake your machine or user name to take advantage of .rhosts

Penetration

- X windows
  - tap into server connection (port 6000+small int)   [hard!]
    - get key strokes, contents of display
- Remote administration servers
  - E.g. Microsoft BackOffice
- Java applets
- Visual Basic scripts
- Shell script bugs
- URL hacking
- et cetera, et cetera ….

Denial of Service (DoS)

Ping of death

take a machine out of service

- IP datagram > 65535 bytes is illegal but possible to create
- Reassembly of packets causes buffer overflow on some systems

Denial of Service: SYN Flooding

SYN flooding

take a machine out of service

Background:

3-way handshake to set up TCP connection

1. Send **SYN** packet
   - receiver allocates resources – limit to number of connections
   - new connections go to backlog queue
   - further SYN packets get dropped
2. *Receiver sends acknowledgement* (**SYN/ACK**) and waits for an ACK
3. Sender sends ***ACK***

Denial of Service: SYN Flooding

- Send SYN masqueraded to come from an unreachable host
  - receiver times tries to send SYN/ACK
  - times out eventually
    - 23 minutes on old Linux systems
    - BSD uses a Maximum Segment Life = 7.5 sec
    - Windows server 2003 recommends 120 sec.

Denial of Service and DDoS

- Other denial of service attacks:
  - Software bugs (esp. OS)
  - ICMP floods
  - ICMP or RIP redirect messages to alter routes to imposter machines
  - UDP floods
  - application floods

- Distributed Denial of Service (DDoS) attacks
  - Multiple compromised machines attack a system (e.g., MyDoom)

Direct System Access

- Boot alternate OS to bypass OS logins
  - E.g., Linux on a CD
- Third-party drivers with backdoors or bugs
- Then … Modify system files
  - Encrypted file system can help

- Rogue administrators

Worms

Type of process that spawns copies of itself

- potentially using system resources and hurting performance
- possibly exploiting weaknesses in the operating system to cause damage

Example: 1988 Internet worm

Robert Tappan Morris Jr.'s Internet worm

- exploit *finger*'s *gets* bug to load a small program (99 lines of C)
- program connects to sender and downloads the full worm
- worm searches for other machines:
  - .rhost files
  - finger daemon
  - sendmail DEBUG mode
  - password guessing via dictionary attack: 432 common passwords and combinations of account name and user name

Virus

- Does not run as a self-contained process
- code is attached onto another program or script

- **File infector**
  - primarily a problem on systems without adequate protection mechanisms
- **Boot-sector**
- **Macro (most common now…VB)**
- **Hypervisor**
  - **install on virtual machines (newest form of attack)**

Botnets

New Kraken worm evading harpoons of antivirus programs

By Joel Hruska | Published: April 08, 2008 - 01:42PM CT
ars technica

Researchers at Damballa Solutions have uncovered evidence of a powerful new botnet they've nicknamed Kracken. The company estimates that Kraken has infected 400,000 systems ....

Specific details on the newly discovered botnet are still hard to come by, but rhetoric isn't. Damballa currently predicts that Kraken will continue to infect new machines (up to 600,000 by mid-April). **Compromised systems have been observed sending up to 500,000 emails a day**, and 10 percent of the Fortune 500 are currently infected. The botnet appears to have multiple, redundant CnC (Command and Control) servers hosted in France, Russia, and the United States.

http://tinyurl.com/5y2x8g

Penetration from within the system

- Malicious software in your computer
  - Can access external systems
  - Internal network, data, other computers
- Dialers
  - Dial 900 number, alternate telephony provider, modify dialing preferences
  - Not interesting now that modems are practically extinct
- Remote access
- Adware
  - Deliver ads via program or another program
- Spyware
  - Scan system, monitor activity
  - Key loggers

Key loggers

- Record every keystroke
- Windows *hook*
  - Procedure to intercept message traffic before it reaches a target windows procedure
  - Can be chained
  - Installed via *SetWindowsHookEx*
  - WH_KEYBOARD and WH_MOUSE
    - Capture key up, down events and mouse events
- Hardware loggers

Rootkits

- Replacement commands (or parts of OS) to hide the presence of an intruder
  - ps, ls, who, netstat, …
- Hide the presence of a user or additional software (backdoors, key loggers, sniffers
- OS can no longer be trusted!

E.g., Sony BMG DRM rootkit (October 2005)

  - Creates hidden directory; installs several of its own device drivers; reroutes Windows system calls to its own routines
  - Intercepts kernel-level APIs and disguises its presence with cloaking (hides sys files)

Dealing With Rootkits

- Restrict permission to modify system files
- Vista:
  - Requires kernel-mode software to have a digital signature (x64-based systems only)

Protection Mechanisms

Operating system protection

OS and hardware give us some protection

access to...

CPU	*process scheduler*
memory	*MMU, page table per process*
peripherals	*device driver, buffer cache*
logical regions of persistent data	*file systems*
communication networks	*sockets*

Protection via authorization

Operating system enforces access to objects

access matrix

objects

domains of protection

	file F	file G	printer H
user A	R	RW	W
user B	RX		
user C			
group X	RW		
group Y			

Protection: access control list

access controls associated with object

objects

domains of protection

	file F	file G	printer H
user A	R	RW	W
user B	RX		
user C			
group X	RW		
group Y			

Protection: capability list

access controls associated with domain

present a "capability" to access an object

objects

domains of protection

	file F	file G	printer H
user A	R	RW	W
user B	RX		
user C			
group X	RW		
group Y			

Security

AAA

The Three A's

- Authentication
- Authorization
- Accounting

Security

AAA+A

The Four A's

- Authentication
- Authorization
- Accounting
- Auditing

Authentication

Identification &
Network-safe authentication

- Cleartext passwords (PAP) - *bad idea*
- One-time passwords
- Challenge-response

vulnerable to man-in-the-middle attacks

- Shared secret keys (distribution must be secure)

- Cleartext passwords are not network safe!

Authentication

Identification & Network-safe authentication

- Trusted third party
  - E.g., Kerberos tickets
- Public key authentication, certificates
- Source address validation (may be spoofed)
- Establish covert communication channel first
  - Diffie Hellman common key
  - Public keys
  - Kerberos
  - … then use cleartext passwords

Identification versus Authentication

- Identification:
  - Who are you?
  - User name, account number, …
- Authentication:
  - Prove it!
  - Password, PIN, encrypt nonce, …

- Biometrics
  - Identification: 1 out of many
    - *Who is this?*
  - Authentication: 1:1
    - *Let me scan your fingerprint and validate it's you.*

…versus Authorization

Access Control

Once we know a user's identity:

- Allow/disallow request
- Operating system enforces system access based on user's credentials
    - Network services usually run in another context
    - Network server may not know of the user
    - Application takes responsibility
- Contact authorization server
    - Trusted third party that will grant credentials
    - Kerberos ticket granting service
    - RADIUS (centralized authentication/authorization)

Accounting

If security has been compromised

… *what happened?*

… *who did it?*

… *how did they do it?*

Log transactions

- Logins
- Commands
- Database operations
- *Who looks at audits?*

Log to remote systems

- Minimize chances for intruders to delete logs

Network Access Control (NAC)

- Authenticate before the switch will route your packets
- Common for Wi-Fi hotspots
- NAC sometimes uses ARP poisoning to relay ARP requests so that traffic will go through the gateway
- Query RADIUS or LDAP server to determine what a user is authorized to access

Intrusion Detection

- External
  - Network activity
  - Network-application protocols
- Internal
  - Host-based

Network Intrusion Detection

Examine traffic going through a network choke (hub, switch, or router)

- Software on device or routed through port mirroring

Detect:

- Dangerous code (viruses, buffer overflow)
- Port scans (including stealth port scans)
- Web server attacks
- SMB probes
- Excess network traffic

Log and/or drop packets that are deemed dangerous

Testing an IP port

TCP/IP:

Test by connect() call or sending a SYN packet

- Open (accepts connections
- Denied (host sends reply that connections will be denied)
- Dropped (no reply from host)

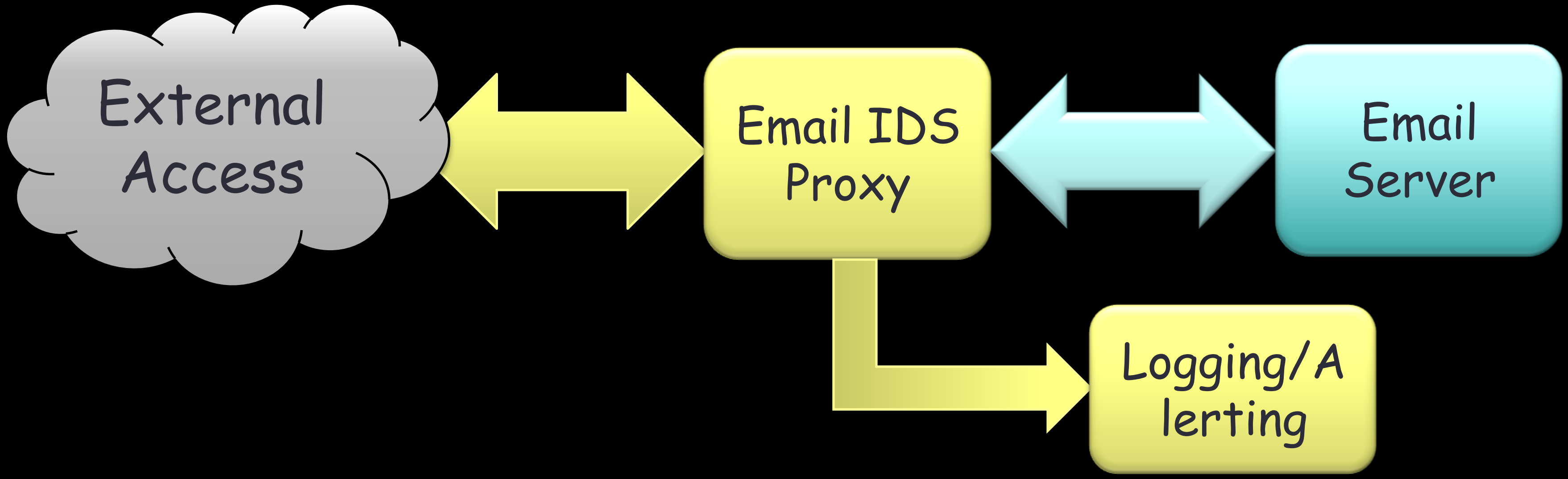
UDP/IP:

- Systems will often send ICMP packets as a reply informing you that a port is not in service

Intrusion Detection Proxies

Application-specific proxies

- Specific to a protocol
- Network interface to proxy instead of application



Host-Based Intrusion Detection

- Host-resident software
- Analyze/log:
  - Virus signature scans
  - file changes
  - system call activity
  - logins
  - admin operations
  - changes to hosts file
  - installation of new drivers, new software, keyloggers
- Off-host logging is better
- Detect "unusual activity"

Virus Scanning

- Search for a "signature"
  - Extract of the virus that is (we hope!) unique to the virus and not any legitimate code.
- Some viruses are encrypted
  - Signature is either the code that does the decryption or the scanner must be smart enough to decrypt the virus
- Some viruses mutate to change their code every time they infect another system
  - Run the code through an emulator to detect the mutation

Virus Scanning

- You don't want to scan through hundreds of thousands of files
  - Search in critical places likely to be infected (e.g., \windows\system32 or removable media)
- Passive disk scan or active I/O scan

Worm Scanning

- Worms do not attach themselves to files
  - Searchfor worm files (standalone programs)

- Search incoming email

Defense from malicious software

- Access privileges
  - Don't run as administrator
  - Warning: network services don't run with the privileges of the user requesting them
- Signed software
  - Validate the integrity of the software you install
- Personal firewall
  - Intercept and explicitly allow/deny applications access to the network
  - *Application-aware*
    - *What program is the network access coming from?*

Code Integrity: Signed Software

- Signed software
- Per-page signatures
  - Check hashes for every page upon loading
  - OS X & Vista/Windows 7:
    - OS X: codesign command
    - Vista: signwizard GUI
  - XP/Vista/Windows 7: (Microsoft Authenticode)
    - Hashes stored in system catalog (Vista/Win7) or signed & embedded in file
  - OS X:
    - Hashes & certificate chain stored in file

Microsoft Authenticode

A format for signing executable code
(dll, exe, cab, ocx, class files)

Microsoft Authenticode

Software publisher:

- Generate a public/private key pair
- Get a digital certificate: VeriSign class 3 Commercial Software Publisher's certificate
- Generate a hash of the code to create a fixed-length digest
- Encrypt the hash with your private key
- Combine digest & certificate into a Signature Block
- Embed Signature Block in executable

Recipient:

- Call *WinVerifyTrust* function to validate:
  - Validate certificate, decrypt digest, compare with hash of downloaded code

Microsoft Vista code integrity checks

- Check hashes for every page as it's loaded
  - Done by file system driver
- Hashes in system catalog or embedded in file along with X.509 certificate.
- Check integrity of boot process
  - Kernel code must be signed or it won't load
  - Drivers shipped with Windows must be certified or contain a certificate from Microsoft

Auditing

Go through software source code and search for security holes

- Need access to source
- Experienced staff + time
- E.g., OpenBSD

Complex systems will have more bugs

- And will be harder to audit

System complexity

Windows complexity: lines of code

OS version	Year	Lines
3.1	1992	3 million
NT	1992	4 million
95	1995	15 million
NT 4.0	1996	16.5 million
98	198	18 million
2000	2000	35-60 million
XP	2001	35 million
Vista	2007	50 million

Source: Secrets & Lies, Schneier
InformationWeek, April 3, 2006, p. 34-35, BigSoftware Rides Again

System complexity

OS complexity: number of system calls

OS version	Year	Sys calls
Unix 1st edition	1971	33
4.3 BSD Net 2	1991	136
Linux 1.2	1996	211
SunOS 5.6	1997	190
Linux 2.0	1998	229
Win NT 4.0 sp3	1999	3,433

Source: Secrets & Lies, Schneier

Other security needs

- Access control: privacy
  - Multilevel security
    - Unclassified, Confidential, Secret, Top Secret, Top Secret/Special Compartmented Intelligence
    - Generally does not map well to the civilian world
  - Restrict access to systems, network data
- Anonymity
- Integrity

Dealing with application security

- Isolation & memory safety
  - Rely on operating system
- Code auditing
  - If possible – need access to code & staff
- Access control checking at interfaces
  - E.g., Java security manager
- Code signing
  - E.g., ActiveX
- Runtime/load-time code verification
  - Java bytecode verifier, loader
  - Microsoft CLR

The end