**Agenda**

- Last time (Tues Feb 20)
  - "A Note on Distributed Computing" (sort of)
  - Security (chap 7)
- This time
  - Security (chap 7)
- Next time (Thurs Mar 1)
  - Dis File systems (chap 8)
- Reminder: Drop date is tomorrow
- Next week: spring break
- Tuesday Mar 13: Dis file systems (chap 8), Assign #3 out
- Thurs Mar 15: Name services (chap 9)
- Tues Mar 20: Midterm (chap 1-9, not 6)

---

**Before we start: Assignment #1**

- A lot of 90s
- Ray’s server: 230,000+ msgs over 5+ days
  - "HO1" really wanted to "Keep alive"
- Software structure matters!
  - One big “main” is not sufficient
  - We were lenient this time, but we won’t be next time (Assignment #2)
- Did any groups get their clients talking with each other?

---

**Before we start: Assignment #2**

- I’ve replied to all design emails...
- “OutwardFacing” and “IMServers” are NOT allowed to communicate via sockets.
- General model
  - Machine 1: OutwardFacing
  - Machine 2: miregistry1 and IMServer1
  - Machine 3: miregistry2 and IMServer2
  - Machines do not share a file system
  - Dev: All on one machine is ok
- OutwardFacing is presumed to not crash
  - Why? Because it’s simple (no state). AND I wanted to simplify the assignment a little.

---

**Before we start: Assignment #2**

- Servers should be assumed to be restarted via sys admin or via an auto-start upon system reboot (i.e., the person has no special knowledge of your app)
- General design principle: decouple the apps in dis system
  - Arguably basic O-O principles: only the interface matters!
- Everyone using their own machines? (NOT 002a machines?)
- Let’s CC Ray on ALL email!
- New due date: Tues Mar 6 12:30pm (mid Spring break)
  - We’ll print things out for you if need be

---

**Security – basics**

- Security perimeter / boundaries
- Intruder: crosses security perimeter without authorization
- Vulnerability: weak point
- Threat: intent to inflict damage on a system
- Attack: carry out a threat
  - Insider vs. outsider
- Risk: likelihood that the system will not be able to enforce its security policy (including the continuation of critical operations) in the face of an attack.

- Prevent, detect, limit, tolerate
Designing secure systems – general issues

- Hard to predict all possible attacks and loopholes.
- Balance cost and inconvenience against threats.
- Worst-case assumptions and guidelines:
  - Interfaces are exposed.
  - Networks are insecure.
  - Limit the lifetime and scope of each secret.
  - Algorithms and program code are available to attackers.
  - Attackers may have access to large resources.
  - Minimize the trusted base.

Establishing Trust

- “assured reliance on the character, ability, strength, or truth of someone or something”
- Who do you trust in your computing life?
  - People, software, machines, services
- How do you develop trust in each of these?
  - People: personal relationship, “told” to trust them
  - Software: Know authors personally, see MD5, sandboxing techniques (Java, .NET),
  - Machines: PKI, [Open]SSH
  - Services: PKI, [Open]SSH

Risk

- Risk is the likelihood that the system will not withstand the attack
- Risk avoidance focuses on removing all vulnerabilities to prevent an attack
- Risk management allows risk to a certain degree
- Risk acceptance simply allows the possibility of an attack

Security Principles

- Accountability
- Least Privilege
- Minimize the complexity of trusted components
- Default Security
- Defense in depth

Assurance

- The goal of assurance is to prove that the algorithm or device works as intended
- How can we give such an assurance?
  - The algorithm/process is correct/sound
  - The device was tested extensively
  - The device was built by CS451 students

An interlude…

- Some slides from Peter Gutmann’s talk last week…
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

Bypass firewall software
• Block access to anti-virus vendor sites (MTX, Mydoom)
• Modify anti-virus software to propagate the virus (Varicella)

Other Malware Functions (ctd)

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

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 impersonate 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)
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)

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

Other Malware Functions (ctd)

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
Use NT native API to create registry entry names that the Win32 API can’t process
Pop up messages requesting payment of money and may disable your computer if you don’t pay up (WGA)
• Disables PC with the only option being to pay up (SPP)

Other Malware Functions (ctd)

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
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

Malware Then and Now

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 ⇒ it’s not there
  I ran this Anna Kournikova thing and nothing happened. Why not?
  — Anti-virus vendor support call

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

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

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)

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)

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, birthdate, 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 disclose 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