

Introduction to Computer Security

Instructor:

Mahadevan Gomathisankaran

mgomathi@unt.edu

Today's Lecture

- Brief history of the field
- Terminology/Definitions
- What are the vulnerabilities
- Why and how these are exploited
- Who are involved
- How to prevent these attacks

- 1967: People starting to publish papers on computer security
- 1970: Influential (in some circles!) RAND report: “Security Controls for Computer Systems”
 - Originally classified – declassified in 1979
- 1964—1974?: MULTICS system development
- Mid-70’s: Many influential papers published in open literature
- Mid-70’s: Cryptography takes off in public research
- 1985: Department of Defense publishes “Trusted Computer System Evaluation Criteria” (Orange Book)
- 1991: Pretty Good Privacy, [Philip Zimmermann](#)
- 1994: Publication of “Common Criteria for Information Technology Security Evaluations”
- 2003: Publication of “The National Strategy to Secure Cyberspace”

History – Other side

- 1970's: Age of phone phreaking
- 1980's: BBSes, Legion of Doom, and Chaos Computer Club
- 1983: *War Games* movie comes out
- 1984: 2600 (The Hacker Quarterly) publication starts
- 1986: First PC virus in the wild (the “Brain virus”)
- 1988: The “Morris worm”
 - Automated spreading across the Internet
 - Exploited several bugs, including the first highly-visible “buffer overflow” exploit (of fingerd)
 - Around 6000 computers affected – 10% of the Internet at the time!
 - Morris convicted in 1990
 - CERT created largely because of this
- Early 1990's: Kevin Mitnick (“Condor”) years
 - Arrested several times
 - Went “underground” in 1992 and achieved cult status
 - Caught in Raleigh, NC in 1995
 - Well-known for “social engineering” skill

History – Other Side

- 1993: Kevin Poulsen hacks phones so he wins radio station contests (Porches, trips, cash, ...)
- 1999 – present: Widespread worms/viruses
 - 1999: Melissa (Word macro virus/worm)
 - Social Engineering
 - 2000: Love Letter (VBScript – did damage)
 - Social Engineering
 - 2001: Code Red (designed to DoS the White House, but hard-coded IP address so defeated)
 - Buffer Overflow Vulnerability in Microsoft IIS
 - 2001: Nimda (hit financial industry very hard)
 - Multiple infection points
 - 2003: “Slammer” (spread astoundingly fast)
 - Again uses buffer overflow in Microsoft SQL Server
- 1999: DDoS networks appear
 - 2000: Big attacks on Yahoo, eBay, CNN, ...
 - Today: “Bot-nets” with 10’s of thousands of bots

- Computer Security
 - (Wikipedia) The objective of computer security includes protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users.
 - (Garfinkel and Spafford) A computer is secure if you can depend on it and its software to behave as you expect.
 - (Stewart Lee) The objective of a trusted computer system is to control access by subjects (users) to objects (data). This control should be governed by a security policy.

- Security Policy
 - Statement of intent about the required control over access to the data
- Actors
 - Policy Writer
 - Policy Enforcer
 - Subject
 - Object
- *Quis custodiet ipsos custodes?*
 - Who will guard the guards themselves?

- Confidentiality
 - Concealment of Information or Resources
 - Information only available to authorized parties
- Integrity
 - Information is precise, accurate,
 - Modified
 - In acceptable ways
 - By acceptable People
 - Using appropriate process
 - Internally Consistent
 - Meaningful, and usable
 - Data integrity and Origin Integrity
- Availability
 - Services provide timely response, fair allocation of resources, quality of service

- Information Assurance
 - Authentication
 - Establishing the validity of a transmission, message, or originator (including verifying the identity of a participant)
 - Non-repudiation
 - Messages or actions are accompanied by proof which cannot be denied

- Computing System
 - A collection of hardware, software, storage, media, data and people
 - Perform some computing tasks
- A chain is no stronger than its weakest link
 - Weakest link !!
 - People
- Social Engineering Attacks
 - Kevin Mitnick

- Threat
 - A set of circumstances that has the potential to cause loss or harm (Textbook)
 - Interception, Interruption, Modification and Fabrication
 - Potential violation of security (Matt Bishop)
 - Disclosure, Disruption, Usurpation and Deception
 - Examples:
 - Snooping -> interception
 - Spoofing -> deception and usurpation

- System Susceptibility
 - The capacity of a system to be affected by a threat
- Access to the flaw
 - The ability of a threat to gain access to a system, either physically or logically (e.g. over the network)
- Capability to exploit the flaw
 - The ability of the threat to employ the knowledge and tools necessary to exploit the system to achieve the desired goal
- Vulnerability
 - *intersection* of a system susceptibility or flaw, access to the flaw, and the capability to exploit the flaw
 - A weakness in the security system

- Control
 - A protective measure to reduce or remove vulnerability
 - An action, device, procedure or technique
- *A threat is blocked by control of a vulnerability*
- Attack
 - An act of violation of the security using the vulnerabilities

- Trojan Horse
 - A trojan horse is a part of the program that otherwise conforms to the security policy
- Trapdoor
 - A feature built into a program/process such that the provision of specific input data allows it overcome the security policy
 - Read: *Reflections on Trusting Trust* by Ken Thompson

- Virus
 - A virus is a program that when executed operates entirely within the security policy
 - Uses trojan horse to attach itself
- Worm
 - A program that migrates from one Comp. Env. To another
 - Good worms: distribute software, propagate bug fixes, etc.
 - Bad Worms: carry viruses

- Overt channel
 - Communication channel that is used in the way it is intended to use
- Covert Channel
 - Mechanism for two processes to communicate in violation of security policy
 - Storage Channel
 - Timing Channel

Definitions from the Telecom Glossary 2000:

- *Mainframe*
 - A large computer, usually one to which other computers and/or terminals are connected to share its resources and computing power.
- *Server*
 - A network device that provides service to the network users by managing shared resources.
 - As in “client-server model”
 - Examples: print server, web server, mail server, file server, ...
- *End System*
 - A system containing the application processes that are the ultimate source and sink of user traffic
 - Examples: workstations, notebooks, PDAs, smartphones, etc.

- *Centralized*
 - All processing and data storage happens in one physically and electronically controlled place
 - Typical of mainframe shops
- *Distributed*
 - A set of servers and workstations run by one administrative group
 - Such a group is called a domain (or security domain)
 - Consistent naming and access control policies across the domain
- *Service-oriented*
 - Control a server but not clients
 - Service owns the data, so controls access
 - Example: Public web servers
- *Peer-to-peer*
 - Everyone is a client and a server
 - Each participant decides on their own access control policies

- Some systems are designated for specific, restricted operations on sensitive data
- Modes (From National IA Glossary)
 - Dedicated
 - System is specifically and exclusively dedicated
 - Processes one particular type or classification of information
 - All users with have a need-to-know all of the information
 - System-high
 - Similar to dedicated mode
 - Need-to-know is relaxed to “for some of the information.”
 - Compartmented/partitioned
 - The system separates data into need-to-know categories
 - A user has access to their compartmented information.
 - Multilevel
 - Different levels of information
 - The system enforces clearance/need-to-know

- Confidentiality
 - Interception/Eavesdropping/Wiretapping (sniffers)
 - Used to be commonly installed after a system break-in
 - Can (could?) capture passwords, sensitive info, ...
 - Some resurgence with wireless networks
 - Has always been a problem with wireless transmission!
 - Electromagnetic emanations (TEMPEST security)
 - Illicit copying (proprietary information, etc.)
 - Copied company documents, plans, ...
 - Copied source code for proprietary software
 - Non-electronic: “dumpster diving”, social engineering

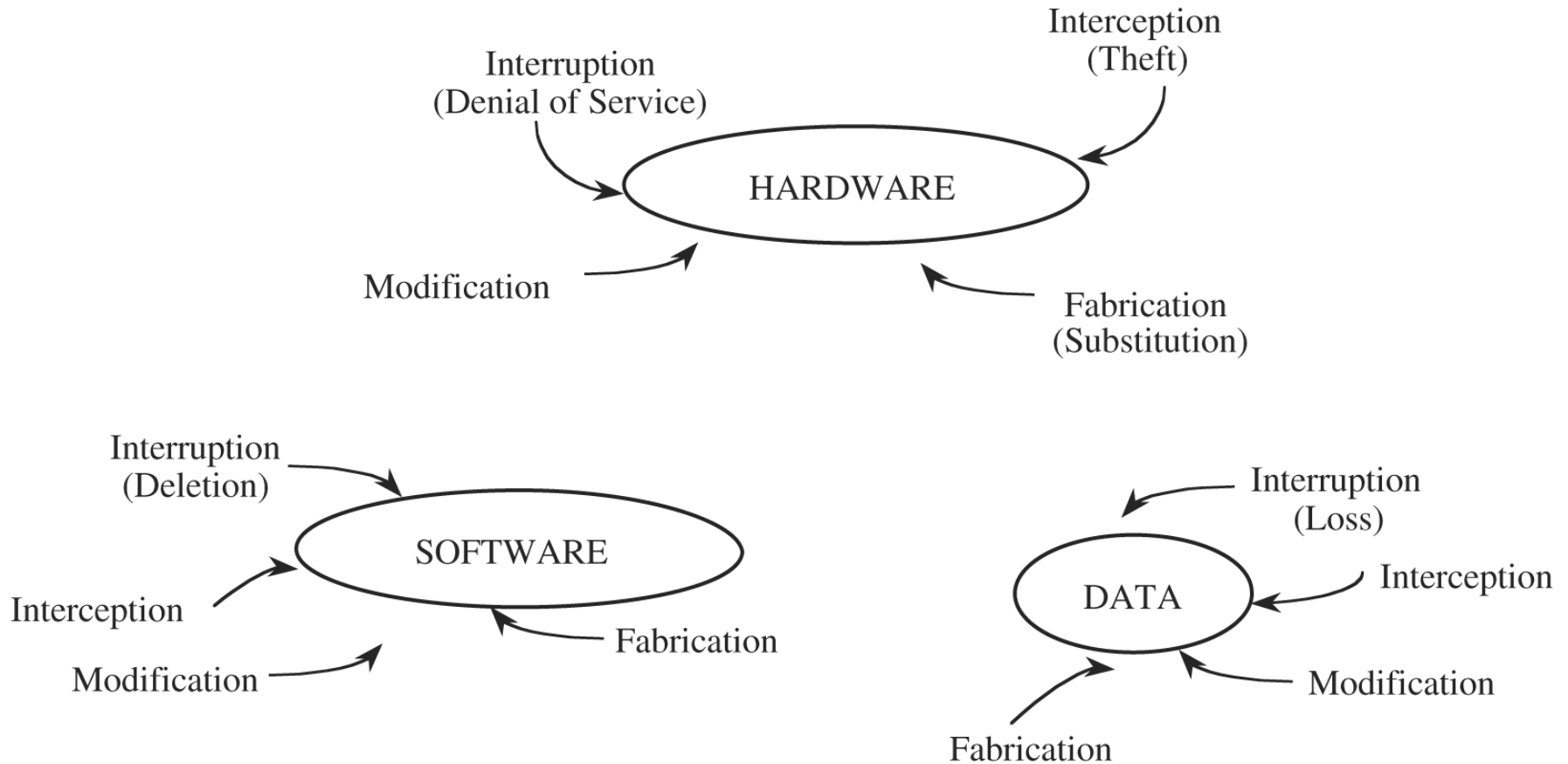
Note: Generally passive attacks – hard to detect!

- Integrity
 - Modification
 - Changing data values (database)
 - Changing programs (viruses, backdoors, trojan horses, game cheats,..)
 - Changing hardware (hardware key capture, ...)
 - Can be accidental corruption (interrupted DB transaction)
 - Many small changes can be valuable (e.g., salami attack)
 - Fabrication
 - Spurious transactions
 - Replay attacks
 - Identity spoofing
 - Somewhat related: fake web sites and “phishing”

- Availability
 - Denial of Service (DoS)
 - Commonly thought of as network/system flooding
 - Can be more basic: disrupting power
 - Deleting files
 - Hardware destruction (fire, tornado, etc.)
 - Distributed Denial of Service (DDoS)
 - Bot-nets of zombie machines that can be commanded to flood and disable “on-command”
 - Discovery of botnets with 10-100 systems is a daily occurrence; 10,000 system botnets are found almost weekly; and one botnet with 100,000 hosts has even been found (according to Johannes Ullrich, CTO of the Internet Storm Center).

- Kinds
 - Interruption, Interception, Modification, Fabrication
- Targets
 - Hardware, Firmware, Software, Data, Resources (e.g.: Network), People, Supplies

Vulnerabilities



Attacks and Attackers

- An attack is when a vulnerability is exploited to realize a threat
 - Typical attack actions were discussed in previous threats/vulnerabilities slides
- An attacker is a person who exploits a vulnerability
- Attackers must have Method, Opportunity, and Motive (MOM)
 - Method: Skills, knowledge and tools
 - Opportunity: Presence of vulnerabilities
 - Motive: \$, ?!

- Amateurs
 - Could be ordinary users (insiders) exploiting a weakness
 - Sometimes accidental discoveries
- Crackers
 - People looking specifically to attack
 - Motive is often challenge, not malice
 - Skill level ranges from very low (script kiddie) to high
- Career criminals
 - Organized crime beginning to get involved
 - Terrorists? (Cyber-terrorism)
- Government/military information warfare

Defense Objectives

- Prevention
 - Most effective, but very hard
- Deterrence
 - Increase the complexity
- Deflection
 - Create easier, dummy, decoy targets - honeypots
- Detection
 - Realtime detection -> very hard
- Recovery
 - Resume normal operation
 - Deal with loss or exposed data

- Definition
 - Using multiple layers of security to protect against failure of individual controls.
- Non-computer example
 - Multi-walled (or concentric) castles
 - Vats of boiling oil helped too...
- Computer security example
 - Internal systems with access control protections, on an internal network with an intrusion detection system, with connections from outside controlled by a firewall.

- A *control* is a protective measure to remove or reduce a vulnerability
 - Action, device, procedure, or technique
- Business motivation: Manage risk
 - Main purpose: Balance risk with costs
 - Risks can be prevented, deterred, detected and responded to, transferred, or accepted
- Risk Analysis:
 - Determine what controls are most cost-effective
 - Most “bang for the buck”

Controls - Examples

- Physical
 - Gates, guns, guards, badge readers, motion detector, etc.
- Administrative
 - Security training, Policies/Procedures, Guidelines, Hiring/Termination practices, Software Development Guidelines, etc.
- Technical
 - Cryptography
 - Access Control
 - Operating System controls (file rights, capabilities,...)
 - Application access restrictions (DB, web server, ...)
 - Network boundary (firewall, VPN, ...)
 - Advanced authentication (smart cards, tokens, ...)
 - Detection programs (virus scanners, IDS's)
 - Regularly test/evaluate (called “penetration testing” or “red teams” or “tiger teams”)

- Steps in Computer Security (or any security) design
 - Define Security Goals
 - Identify Vulnerabilities/Risks
 - Identify Threats
 - Define Security Policy
 - Design Controls

- Principle of Easiest Penetration
 - Not most obvious or most expected but easiest!
- Principle of Weakest Link
 - Security no stronger than weakest link
- Principle of Adequate Protection
 - Protect assets to a degree consistent with their value
- Principle of Effectiveness
 - Controls must be efficient, easy to use, appropriate, ... and used.

- Trust is fundamental to security
- Who/What to trust ?
- Trusting the software ?
 - Certification authorities
 - Trusted Platform Module – Trusted Computing Group
- Trusting the hardware ?
 - H/w trojans ?
- [Reflections on Trusting Trust](#), Ken Thompson

Reading Assignment

- *Information System Security: A Comprehensive Model*, John R. McCumber
- *A Model for Information Assurance: An Integrated Approach*, Victor Maconachy et. al.

Further Reading

- Cliff Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage* (1989)
 - Fun “spy story” – true story, but reads like a novel
- Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World* (2000)
 - Excellent take on security from a “big principles” point of view (mostly non-technical)
- Ross Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems* (2001)
 - Turning theory into secure practice
- Steven Levy, *Crypto: How the Code Rebels Beat the Government – Saving Privacy in the Digital Age* (2002)
 - History of crypto revolution that started in the 1970’s