Computer Security Risk Analysis

Lecture 1

George Berg
Sanjay Goel
University at Albany
Outline

- Computer Crime
- Definitions
- Attacks
- Information Assurance
- Vulnerabilities & Risks
Course Information

• Course Web pages:
  – The main course web page:
    • www.cs.albany.edu/~berg/risk_analysis
    • The pages will be up today or tomorrow.
  – The current link to the course description:
    • www.albany.edu/~goel/classes/spring2004/inf766
Cyber Crime
The Beginning - 1988

- In 1988 a “worm” program written by a college student shut down about 10 percent of computers connected to the Internet.
  - This was the beginning of the era of cyber attacks.
- Today we have about 10,000 incidents of cyber attacks which are reported and the number grows.
Cyber Crime
1994

• A 16-year-old music student, Richard Pryce, better known by the hacker alias “Datastream Cowboy,” was arrested and charged with breaking into hundreds of computers including those at the Griffiss Air Force base, NASA and the Korean Atomic Research Institute.
  – His online mentor, “Kuji,” is never found.

• Also that year, a group directed by Russian hackers broke into the computers of Citibank and transferred more than $10 million from customers' accounts.
  – Eventually, Citibank recovered all but $400,000 of the pilfered money.
Cyber Crime
1994

• In February, Kevin Mitnick is arrested for a second time. He is charged with stealing 20,000 credit card numbers.
  – He eventually spends four years in jail and on his release his parole conditions demand that he avoid contact with computers and mobile phones.

• On November 15, Christopher Pile becomes the first person to be jailed for writing and distributing a computer virus.
  – Mr Pile, who called himself “The Black Baron,” was sentenced to 18 months in jail.

• The US General Accounting Office reveals that US Defense Department computers sustained 250,000 attacks.
Cyber Crime
1999

• In March, the Melissa virus goes on the rampage and wreaks havoc with computers worldwide.
  – After a short investigation, the FBI tracks down and arrests the writer of the virus, a 29-year-old New Jersey computer programmer, David L Smith.

• More than 90 percent of large corporations and government agencies were the victims of computer security breaches in 1999.
Cyber Crime 2000

• In February, some of the most popular websites in the world such as Amazon and Yahoo are almost overwhelmed by being flooded with bogus requests for data.

• In May, the ILOVEYOU virus is unleashed and clogs computers worldwide.
  – Over the coming months, variants of the virus are released that manage to catch companies that didn't do enough to protect themselves.

• In October, Microsoft admits that its corporate network has been hacked and source code for future Windows products has been seen.
Cyber Crime

2003

• In August Sobig-F hits the Internet hard, flooding e-mail servers and inboxes slowing Corporate networks slowing to a crawl.
  – It becomes the most damaging virus on record with damage worth $29.7 billion.

• This worm propagates by mass-mailing copies of itself using its own Simple Mail Transfer Protocol (SMTP) engine.
  – It collects email addresses from files on infected systems.
Cyber Crime

Crisis

- The Internet has grown very fast and security has lagged behind.
- Large scale failures of the Internet can have a catastrophic impact on the economy which relies heavily on electronic transactions.
- Legions of hackers have emerged as impedance to entering the hackers club is low.
- It is hard to trace the perpetrators of cyber attacks because
  - Real identities are easily camouflaged.
  - The ubiquity of the network.
Cyber Crime

Why is it increasing?

- Rapid Growth of Computer Literacy.
- Widespread Availability of Hacker Tools.
- Increased Espionage and Terrorism.
- Increased Recreational and Nuisance Hacking.
- Industry Pressure to Downsize, Automate, and Cut Costs.
- Shift from Proprietary Systems to Networked Solutions With Open Protocols.
- Increased Dial-in and Network Access.
Definitions

Attacks

• **Cyber Intrusion**: unauthorized access of a computer program or system.

• **Cyber Attack**: malicious behavior leading to a software system security incident such as an intrusion, an exploit, or degradation of system functionality.

• **DOS**: a malicious attack to create a Denial of Service condition in the attacked system.
Definitions

Attacks

• **Vulnerability**: a flaw in software or a system that produces an exploitable weakness.

• **Exploit**: a malicious technique deliberately targeting a system or program vulnerability.

• **Control (Mitigation)**: a measure taken to close or minimize a vulnerability.
Definitions

Roles

• **Hacker:** (1) someone who “hacks” code, or (2) a network or computer intruder. The latter come in two versions:
  – White-hat (good guys)
  – Black-hat (bad guys)
Definitions

Roles

• **Crackers**: malicious hackers. The term is sometimes used for attackers focusing on password cracking.
• **Web-Whackers**: (1) someone who builds or maintaining web services, or (2) a hacker looking for web weakness.
• **Script Kiddie**: a novice hacker using attack scripts without the underlying knowledge how they work.
• **Insider**: a person with legitimate access or association with some aspect of the environment or system.
• **Hacktivist**: a hacker, cracker, or web-whacker motivated by social or political causes.
Definitions

Modes

• **Spoof**: to create a fake email or IP (Internet Protocol) address, or to impersonate an actual address or URL.

• **Virus**: malicious code implanted in electronic files and transmitted via human activity like opening or sharing a contaminated file (*e.g.* ILoveYou).

• **Worm**: malicious code, implanted in systems or files, that can self-replicate without human intervention (*e.g.* Blaster, Nimda).

• **Trojan Horse**: malicious code implanted in systems or files that opens a “backdoor” for the attacker to gain access to the system (*e.g.* Back Orifice).

• **Logic Bomb**: destructive program timed to go off at a later date.
Definitions

Tools

- **Sniffer**: a network packet reader.
- **Snort**: (1) wireless sniffer, (2) network Intrusion Detection System (IDS).
- **Social Engineering**: gleaning confidential information (e.g. passwords) by non-technical means. For example,
  - Finding passwords left out in the open,
  - Conning people into revealing passwords or other information.
Attack

Motives

• Hackers (recreational, malicious, professional)
• Espionage (State and Industrial)
• Sabotage
• Electronic Theft
• Vandalism and Hacktivism
• Information Warfare
Attack Scenarios

• Terrorism and Acts of War
  – Warfare or terrorist event
  – Combined with loss of critical infrastructure

• Industry Instability
  – Downsizing
  – Disgruntled employees
  – Revenge attack

• Deregulation
  – Increased rates
  – Disgruntled customers
  – Revenge attack
### Attack Scenarios

- **Increased World Trade**
  - Increased resistance to WTO
  - More organized anarchists
  - Sabotage of host cities

- **Increased Electronic Theft and Fraud**
  - Decreased prosecution
  - More electronic theft
  - More electronic extortion

- **Increased Nuisance Hacking**
  - Increased computer literacy
  - Curiosity + Challenge + Activism
  - Hacking and Hacktivism
Attack Scenarios

• Curious Student War-Dialing or War-Driving.
• Bored Person With Ping Sweeper and Port Scanner.
• Insider Duped Into Installing a Trojan.
• Insider Bribed Into Sabotage or Espionage.
• Unscrupulous Person With Sniffer.
Information Assurance

Definition

- **Information Assurance:** Operations that protect and defend information and information systems (IS) by ensuring the following properties:
  - **Availability:** Timely, reliable access to data and information services for authorized users.
  - **Integrity:** Protection against unauthorized modification or destruction of information.
  - **Authentication:** Assures the identities of the sender and receiver are true.
  - **Confidentiality:** Assurance that information is not disclosed to unauthorized persons, processes, or devices.
  - **Non-repudiation:** Guarantee that a message or data can be proven to have originated from a specific person.
  - **Access Control:** Any mechanism by which a system grants or revokes the right to access data, or perform some action.
Information Assurance

Implementation

• Confidentiality:
  – Encryption
  – Dedicated communications lines
  – Hidden messages (steganography)

• Integrity:
  – Authenticated access controls
  – Encryption
  – Dedicated communications lines

• Availability:
  – Centralized v. Distributed data storage
  – On-Demand v. Broadcast v. Publish-Subscribe
  – Authenticated access controls
Information Assurance

Implementation

• Access Control:
  – Physical access control
  – Electronic access control
  – Password v. PIN v. Encryption
  – Multi-tiered controls (defense in depth)

• Authentication:
  – Encryption
  – Single-factor v. Two-factor authentication
  – Multi-factor authentication
  – Biometrics

• Non-repudiation
  – Encryption
  – Return receipt message digest
Authentication

Implementation

• Single Factor Authentication
  – Password/PIN
• Two-factor Protection
  – Password + {PIN | SSN | factoid}
• Strong Two-factor Protection
  – Password + Magnetic-strip
  – Password + Programmable ID Device
  – Password + Biometrics
• Strong Three-factor Protection
• Authentication via Encryption
Network Protection
Implementation

- Multi-Factor Authentication
- Restricted Communications
  - Packet filtering (Hardware & Software)
  - Routers & Switches
  - Firewalls (Hardware & Software)
  - Proxies & DMZs
- Authenticated Communications
- Authenticated & Encrypted Communications
  - Virtual Private Network (VPN)
  - Public Key Infrastructure (PKI)
Vulnerabilities & Risks
Stand Alone Computers

• **Vulnerability:**
  – Physical access by authorized or unauthorized persons.
  – Visual access by unauthorized persons.

• **Risks:**
  – Theft of machine
  – Theft or corruption of data
  – Loss of privileged information
  – Theft of personal identity
Vulnerabilities & Risks
Stand Alone Computers

• Mitigation:
  – Physical access control
  – Password / PIN access control
  – Teach password / PIN management
  – Use strong passwords & obfuscate password length
  – Monitor last logins
  – Multi-factor access control
Vulnerabilities & Risks
Network Connections

• Vulnerability:
  – Remote access by authorized or unauthorized persons
  – Subsequent access to attached equipment

• Risks:
  – Theft or corruption of data
  – Loss of privileged information
  – Theft of personal or system identity
  – Hijacked systems
  – Broadcast storm
Vulnerabilities & Risks

Network Connections

• Mitigation:
  – All previous Basic mitigations
  – Access warning statements
  – Automated reporting features
  – Audit/Access logs
  – Verify identity (defense in depth)
  – Verify settings (e.g., “Are you Sure?”)
  – Multi-tiered access controls
Vulnerabilities & Risks
Modem Connections

• Vulnerability:
  – Remote access by authorized or unauthorized persons
  – Phone number accessible *via* war-dialer or social engineering
  – Programmed attack on access restrictions
  – Phone system vulnerabilities
  – Open for incoming connections

• Risks:
  – Theft or corruption of data
  – Loss of privileged information
  – Theft of personal or system identity
  – Hijacked systems
  – Downstream liability
Vulnerabilities & Risks

Modem Connections

• Mitigations:
  – All previous Extended mitigations
  – Automated Disconnects/Time-outs
  – Modem access controls
    • Dial-back modems
    • Password controlled access
    • Key/lock devices
    • Encryption
Vulnerabilities & Risks
Public Network Connections

• Vulnerability:
  – Remote access to system(s)
  – Network address accessible via Ping Sweep
  – Port number and function accessible via Port Scan
  – Programmed attack on access restrictions
  – DOS and D-DOS vulnerabilities

• Risks:
  – Theft or corruption of data
  – Loss of privileged information
  – Theft of personal or system identity
  – Hijacked system(s)
  – DOS and D-DOS Attack
  – Downstream liability
Vulnerabilities & Risks

Public Network Connections

- Mitigations:
  - All previous mitigations
  - Network access controls and security
  - Automated lock-outs
  - Proactive log analysis
  - Encrypted data storage
  - Defense in depth
  - Separation of functionality
Vulnerabilities & Risks
Public Network Connections

• Mitigations:
  – Pre-expired / Time-expired passwords
  – Password change policy and enforcement
  – Virus scanners, firewalls, intrusion detection systems
  – IP security, protocol tunneling, virtual private networks
  – Public key certificates
  – Proactive event analysis
Passwords

Protection

- **Strength:** \( P(C, n) \sim Cn \) with \( C \) characters and length \( n \)
- **Weak:**
  - Short in length
  - Limited character set
  - All upper case or lower case or digits only
  - Forms a word, acronym, name, or date
- **Strong:**
  - 6 or more characters of mixed case
  - At least one special character or digit
  - No words, acronyms, names, or dates
Passwords

Storage

• In the clear on file system.
  – This is not a very good alternative, as a user that gains access to the file has all of the passwords.

• On a dedicated authentication server.
  – This is somewhat better, though a compromise of the authentication server will still reveal users' passwords.
Passwords

Storage

• Encrypted.
  – This way, compromising the password file will not reveal users' passwords.

• Hashed
  – Use a one-way hash function, such as MD5. When the user presents the password, it is hashed and compared against the stored value. Knowledge of the hashed password is inadequate to authenticate oneself to the machine.

• Salting
  – Involves storing a value hash(pwd; salt); salt, where salt is a per user value.
  – Salting prevents pre-computation of hashes by an adversary, which makes breaking more common passwords at least a little more difficult.
  – Reuse of passwords, either by two users with the same password or one user with the same password on two systems, will not be evident from salted hash.
Passwords

Security

• Access control:
  – Useful for all users to be able to access some of the information in the password file, but not have access to the actual passwords.
  – Many systems break the password file into two pieces, one with useful user information, such as the user's default UNIX shell, and another “shadow” password file that is stored in a secret place that contains the actual passwords.
Passwords

Security

• Changing passwords
  – Changing passwords frequently improves security, though it makes passwords harder to remember.
  • A trade-off.
  – DoD says that passwords should be changed at least once a year.
  – Reuse of recent passwords is usually not recommended.
  • Some systems do not allow a user to change their password to any recently used one.
Password

Security

Password hashed and stored
  – Salt added to randomize password & stored on system
• Password attacks launched to crack encrypted password

Password Security

Hash Function

Client

Hashed Password

Server

Compare Password

Hashed Password

Stored Password

Allow/Deny Access
Password Attacks

Types

• Dictionary Attack
  – Hacker tries all words in a dictionary to crack a password.
  – 70% of people use dictionary words as their passwords.

• Brute Force Attack
  – Try all permutations of the available letters & symbols.

• Hybrid Attack
  – Words from dictionary and their variations used in attack.
Password Attacks

Types

- Social Engineering
  - People write passwords in different places.
  - People disclose passwords naively to others.

- Shoulder Surfing
  - Hackers slyly watch over peoples shoulders to steal passwords.

- Dumpster Diving
  - People dump their trash papers in garbage which may contain information to crack passwords.
Password Attacks

War Dialing

A hacker exploits weak passwords & uncontrolled network modems easily:

Steps:

• Hacker gets the phone number of a company.
• Hacker runs war dialer program:
  – If original number is 555-5532 he runs all numbers in the 555-55xx range.
  – When modem answers he records the phone number of modem.
• Hacker now needs a user id and password to enter company network:
  – Companies often have default accounts e.g. temp, anonymous with no password.
  – Often the root account uses company name as the password.
  – For strong passwords, password cracking techniques exist.
Password Attacks

Brute Force

• Find a valid user ID
• Create a list of possible passwords
• Rank the passwords from high probability to low
• Type in each password
• If the system allows you in – success!
• If not, try again, being careful not to exceed the password lockout threshold
  – (the number of times you can guess a wrong password before the system shuts down and won’t let you try any more)
Password Attacks

PBE- Password Based Based Encryption

• Passwords are stored as a hash on the computer
  – A hash is an irreversible transformation of data into a string of fixed length
  – Input string -> hash function -> fixed length output string (hash)
  – Whenever a user types a password the system hashes it and compares it to the stored hash on the system
  – If the hashes match the user is authenticated

• Passwords are cracked by using:
  – Dictionary Attack
  – Hybrid Attack
  – Brute Force Attack

• The general algorithm for cracking passwords is:
  – Find a valid user id
  – Create a list of possible passwords
  – Rank the passwords from high probability to low
  – Type in each password until the system allows you in
Password Attacks

Windows Passwords

• Passwords are stored in a security Database
  – Security Account Manager (SAM)
  – File Location \Windows\system32\config\SAM
  – World Readable file (locked by system kernel when system is running)
  – A copy of password database copied to Windows\repair directory

• Two hashing algorithms are used to encrypt passwords
  – NT hash & LANMAN Hash

• NT hash
  – Converts password to Unicode and uses MD4 hash algorithm to obtain a 16-byte value

• LANMAN hash
  – Password is padded with zeros until there are 14 characters.
  – It is then converted to uppercase and split into two 7-character pieces
  – An 8-byte odd parity DES key is computed from each half
  – DES keys are combined to get 16-byte one way hash
Password Attacks
Windows Passwords - Weaknesses

• LAN Manager hashing scheme
  – Compromises for backward compatibility with LAN Manager
  – Breaks passwords into two 7-character words
  – Does not have case sensitivity
  – Brute force attack takes a lot longer for one full string than two half strings
  – Most users have numbers at end of password so first half string is usually letters
  – Case insensitivity further reduces complexity of cracking
• No Salts
Password Attacks

Security

• Salting
  – A salt is a random piece of data that is combined with a password before it is encrypted
  – Each user has their own salt, so no 2 hashes are the same.
  – If 2 people have the same password, they will have different salts, resulting in different encrypted passwords
  – Salting makes it harder to Brute Force a password
  – With a salt, you have to compute the hash of each word for each user using their unique salt

• Iteration count
  – Number of times a password is hashed repeatedly
  – It is an attempt to make the attacker spend more time to test possible passwords

• Enable Account Lockout
  – Specify how many times an authentication fails against a valid user account before the user is denied access
Password Attacks
Windows Passwords

• How to protect your NT System
  – Disable LAN Manager Authentication
  – Enforce strong passwords through a policy
  – Implement SYSKEY security
  – Use one-time passwords
  – Use Biometric authentication
  – Audit access to key files
  – Limit domain administrator access

• Different programs for NT-password cracking
  – L0phtcrack
  – NTSweep
  – NTCrack
  – PWDump2
Passwords

Good Passwords

• Mix upper and lower case
• Use non-words, such as ``stowishy."
• Include non-alphanumeric characters
• Mix numbers and letters
• Perform a substitution, such as o → 0 or l → 1
• Pick letters from a longer pass-phrase or sentence
• Computer generation
  – This generates hard to remember combinations.
• Passwords must be stored somewhere.
  – The user must remember the password, either by memorizing it or by writing it down,
  – The computer must remember the password so that it can be checked when the user presents it.