MIS 131: Information Systems Administration

Part V: IT Security

Section C: Hacking and Countermeasures

Hacking: A Serious Threat

- Definition: *Hacker*
  - 1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities.
  - 2. One who programs enthusiastically.
  - 3. A person who is good at programming quickly.
  - 4. An expert at a particular program, as in 'a Unix hacker'.
  - 5. [Deprecated] A malicious meddler who tries to discover sensitive information by poking around. The correct term for this sense is "cracker."

Motivations for Hacking

- For fun
- As a challenge
- As a legitimate job (“white-hat”)
- For personal gains (“black-hat”)

Brief History of Hacking

- Pre-1969: Operators as pranksters
- 1960s: Hacks (MIT) were simply programming shortcuts to speed up computing task
- 1969:
  - Dennis Ritchie and Ken Thompson

- 1970s: Cap’n Crunch Cereal’s giveaway whistle produced a 2600 MHz sound used in telephones (“phone phreaking”)

Vietnam vet John Draper

Brief History of Hacking

- 1980: Start of “Golden Age” with the introduction of IBM PC
- 1984 – 1990: Great Hacker War
  - Legion of Doom vs. Masters of Deception
- 1986: Federal Computer Fraud and Abuse Act
  - Led to arrest and time served for many hackers
  - Initially, not punitive enough ($10,000 fine and community service, a year in prison, etc.)
- 1994: Russian hacker stole $10M from Citibank -> everything recovered except $400,000

Phiber Optik, a.k.a. Mark Abene

Robert Morris was the first person convicted under the Federal Computer Fraud and Abuse Act of 1986.

Vladimir Levin

Brief History of Hacking

- Y2K+
  - “Denial of Service” in CNN, Yahoo, E-Bay, etc.
  - “I Love You” virus
  - Attacks on secure sites like FBI, White House, and Microsoft
  - Cyber-terrorism

Important Hacking Terms

- Back door
  - A hole in a security system deliberately left in place by designers intended for use by service technicians
- Cracker
  - One who breaks security on a system
  - Coined by hackers in defense against journalistic misuse of the term "hacker"
  - The term reflects strong revulsion at the theft and vandalism perpetrated by cracking rings

Important Hacking Terms

- Sneaker
  - An individual hired to break into places in order to test their security
  - Analogous to "tiger team"
- Phreaking
  - The art and science of cracking a phone network
- Security through/by obscurity
  - Hacker term for vendors' favorite way of coping with security holes — namely, ignoring them
- Social engineering
  - A non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures

Important Hacking Terms

- Deep magic
  - A security technique central to a program
  - In most cases, composed by a “true wizard”
  - Many techniques in cryptography, signal processing, graphics, and artificial intelligence are considered deep magic
- True wizard
  - A person who knows how a complex piece of software or hardware works
  - Someone is a hacker if he/she has general hacking ability, but is a wizard only if he/she has detailed knowledge

Important Hacking Terms

- Virus
  - A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes
  - Viruses can also replicate themselves
- Worm
  - A program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down

Important Hacking Terms

- Trojan horse
  - A malicious, security-breaking program disguised as something benign, such as a directory lister, archiver, or game
- Sniffer
  - Program/device that monitors data traveling over a network
  - Can be used both for legitimate network management functions and for stealing information off a network (e.g. password sniffer)
  - Can be extremely dangerous since they are virtually impossible to detect and can be inserted almost anywhere

Important Hacking Terms

- Logic bomb
  - Also called “slag code”
  - Programming code added to an application or operating system that lies dormant until a predetermined period of time
  - Typically malicious in intent, acting in the same ways as a virus or Trojan horse once activated

Other Interesting Terms

- RTFM – “Read The F___ng Manual” - Used by gurus to brush off questions they consider trivial or annoying
- Lots of MIPS but no I/O - person who is technically brilliant but who can't seem to communicate with human beings effectively
- KISS Principle – “Keep It Simple Stupid”
- Foo – term of disgust

Standard Hacking Procedure

- Discovery (“casing” the establishment)
  - Footprinting – process of accumulating data on a network environment to find ways to intrude (looks for vulnerabilities); usually non-intrusive (e.g. company website)
  - Scanning – searches Internet addresses for any computer particularly vulnerable to a backdoor break-in
  - Enumerating – listing of information (i.e. users) in a network
  - Sniffing

Standard Hacking Procedure

- Penetration and exploitation
  - May or may not be malicious
- Covering one’s tracks
  - Disabling auditing
  - Clearing event log
  - Hiding files

Types of Hacks

- System hacking
  - – Breaking into and exposing vulnerabilities of a specific operating system
- Network hacking
  - – Gaining entry into a specific network
- Software/Application hacking
  - – Bypassing software security (e.g. password protection, serial numbers, etc.)

Most Common Attacks

- Denial of Service (DoS)
  - Also known as “distributed denial of service”
  - With a scanner, hacker looks for vulnerable computers to serve as launch point
  - Master computer signals, slave computers simultaneously send out requests for information (called “IP packets”) that bombard victim’s network and shuts it down
  - Smurf attack – hacker forges victims address, sends out “ping” to a large network; victim receives overwhelming response

Most Common Attacks

- Buffer overflow
  - Receiving computer in a network must allocate enough memory for incoming packet
  - Programs are vulnerable if size of packet is not checked
  - Corruption occurs if data in one buffer overflows into another

Most Common Attacks

- Virus, worms, and Trojans
- Footprinting, scanning, enumerating, sniffing
- Spoofing
  - Fooling software or hardware
  - E-mail spoofing
  - IP spoofing
- Pilfering
- Pornographic pictures and materials
- Reverse engineering (software hack)

Countermeasures

- Myth: Breaking into a system to test and expose its vulnerability (commonly called "penetration testing") will minimize if not totally eliminate the hole
- Fact: There a million ways to break into a system!

Areas Requiring Protection

- Physical
  - Servers, data centers, data storage devices
- Network
  - Firewall
  - Intrusion detection
  - Payload security (e.g. encryption)
- Operating System
  - Built-in security functions (e.g. file permissions, personal firewall, etc.)
- Application
  - Authentication using biometrics

Prominent Information Security Agencies

- DoD (U.S. Department of Defense)
  - Established the “Orange Book”
    - Department of Defense Trusted Computer System Evaluation Criteria
    - Provides guidelines in information security implementation

Prominent Information Security Agencies

- NCSC (National Computer Security Center, est. 1983)
- Published the Rainbow Series
  - Named after the different colors of their covers
  - Green Book : Password Management
  - Tan Book : A Guide to Understanding Audit in Trusted Systems
  - Teal Green Book : A Glossary of Computer Security Terms
  - Salmon Book : A Guide to Writing the Security Features User’s Guide for Trusted Systems

Encryption

- Process of scrambling data to make it undecipherable to those not authorized to peruse it
- Used to implement “payload security”
- Cryptography – science of encryption and decryption

Popular Encryption Standards

- DES
- IDEA
- Public key cryptography

DES

- Data Encryption Standard
- Produced by the U.S. National Bureau of Standards
- Approved by ANSI in 1981 for business use
- 20+ years old -> aging and getting less secure
- Uses a 56-bit key to encrypt and decrypt a message
- Free for use (no royalties)

IDEA

- Objective is to make DES more secure
- Originally called PES (Proposed Encryption Standard), added ‘I’ for improved (IPES) -> IDEA (International Data Encryption Algorithm)
- Royalties paid to a Swiss company -> not widely-used
- Used in PGP (“Pretty Good Privacy”, a free encryption software and de facto standard)
- Uses 128-bit encryption
- Only one way to hack: brute force!

Public Key Cryptography

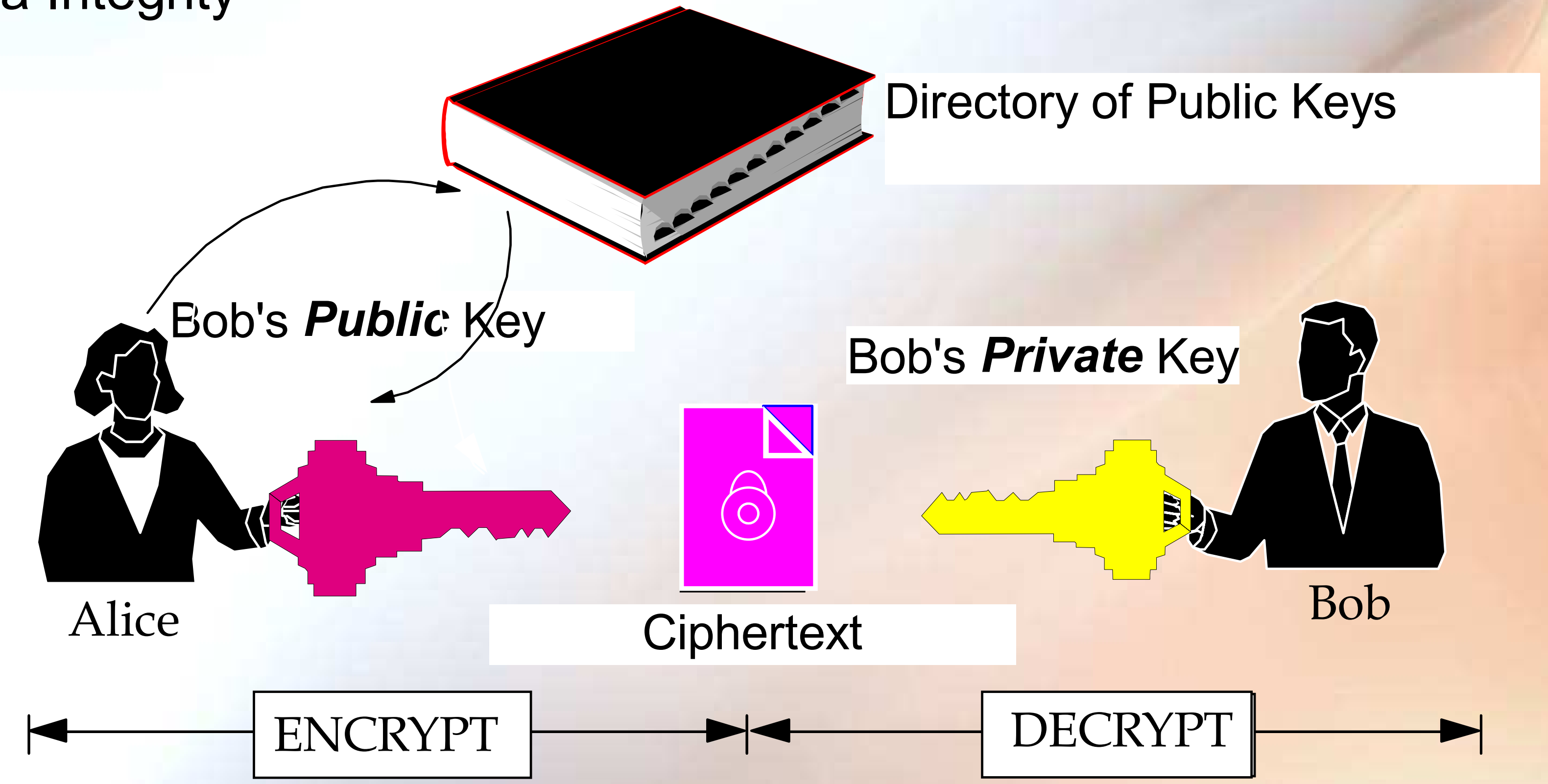
- Proposed by Whitfield Diffie and Martin Hellman at Stanford University
- Translated into a practical method a year later by Ron Rivest, Adi Shamir, and Leonard Adleman, at the Massachusetts Institute of Technology
- Also known as RSA
- Used as wrapper to transmit a security key (e.g. IDEA)

Public Key Cryptography

- Generates a pair of keys (very large integers, sometimes 2048 bits or 600+ decimal digits long!) related mathematically in a peculiar but useful way
- Encrypts with one key and decrypts with the other
- Chooses one to be the “public key” given out to anyone

Public Key Cryptography

- Alice encrypting a file for Bob
- Encryption provides:
  - Confidentiality
  - Data Integrity



Public Key Encryption

- Private key is strongly encrypted (e.g. needs password or other authentication to unlock) and kept in the owner's computer; backup kept in safe place
- Can't hackers reproduce the private key? Yes and No!
  - Yes: can be reversed engineered (get the prime factors of the "modulus" then raise it to "exponent")
  - No: time element
- Disadvantage: Slow! Hence, used only to encrypt short data (e.g. keys) instead of long messages

Important Terms

- Symmetric key ciphers – an encryption system that uses only one key to encode and decode messages
- Ciphertext – the encrypted message
- Key – number used for encryption
- Passphrase – (a.k.a. password) used to unlock the key and decrypt the ciphertext
- Trusted system – employs sufficient hardware & software integrity measures to allow its use for processing a range of sensitive or classified information

Authentication

- Major objective is proof of identity
- Attempts to identify the legitimate user and determines actions he/she is allowed to perform
- Also attempts to find those posing as others

Key Elements of Authentication

- Person (or group) to be authenticated
- Distinguishing characteristics
- Proprietor for system being used
- Authentication mechanism
- Access control mechanism for limiting the actions of authenticated person or group

Biometric Authentication

- Automated method for verifying identity of a person based on physiological or behavioral characteristics
- Provides stronger system
- Implemented through *two-factor-authentication* (combines something one knows with something one has)

Types of Biometric Authentication

- Retinal or iris scan
- Fingerprint matching
- Face geometry
- Hand geometry
- Voice recognition
- Signature verification
- Keystroke dynamics

Digital Signatures

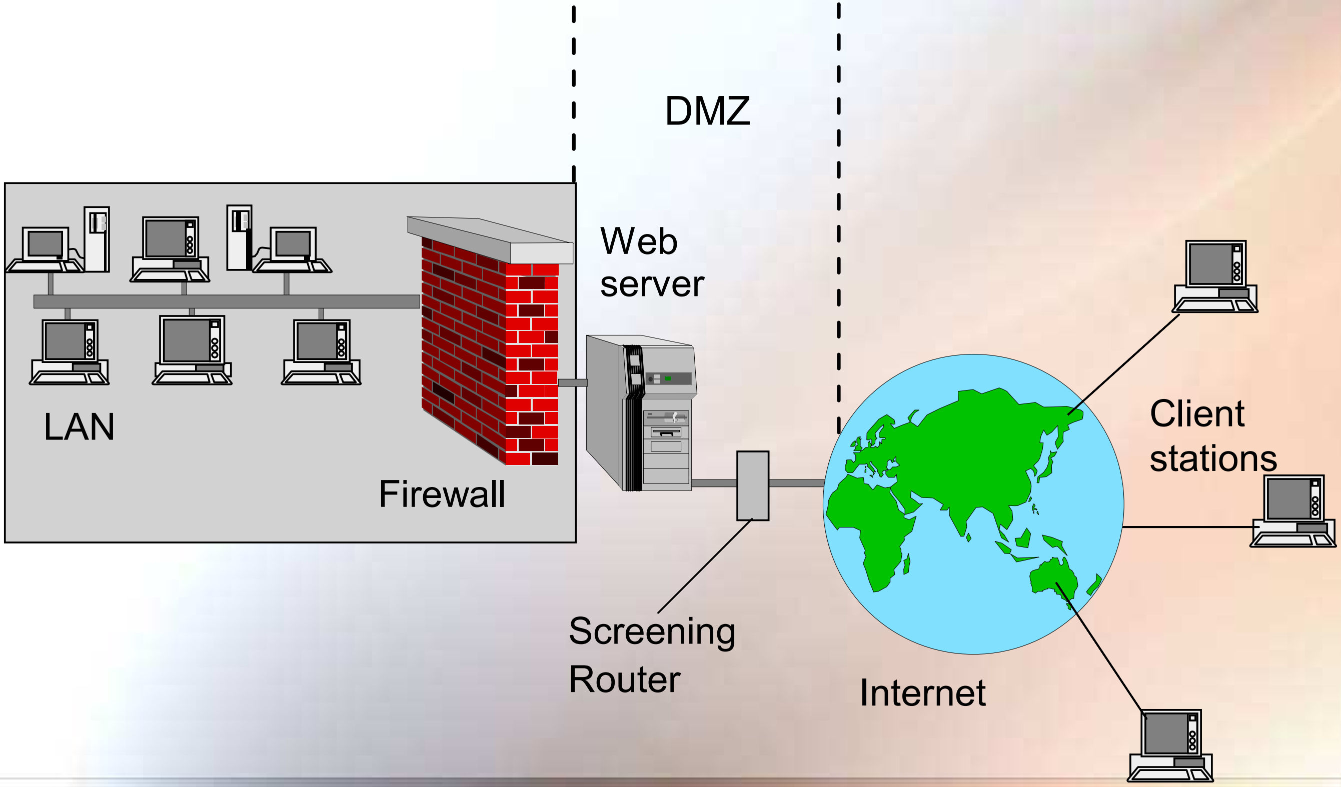
- Messages crunched down to fixed number of bits (message digest, usually 128) using a hash function
- Encrypted message then encoded using sender’s private key
- File -> crunch -> hash -> sender’s private key encrypt = digital signature
- A step further: encrypt the entire message!

Example of a Digital Signature

```
-----BEGIN PGP SIGNED MESSAGE-----
1 Jan 1997

Perth, Australia

Spock, please do not go ahead with the order for the 4 million
tons of alumina. Instead, contact Dr. McCoy and let him know we
will be considering it again at the Board Meeting on 11 Jan and will
let him have our decision then.

Jim Kirk

-----BEGIN PGP SIGNATURE-----
Version: 2.6.3ia
Charset: cp850
iQEVAwUBM1HeovrQml8kGPQBAQHMqgf/atqUN0d4gXLQ5jZ8hsLEkGW1Eb16xdv
9Kg5EhpxEZMV3tvdnNY5JL0E+n/QoEMo9aN/z04YTuwx2zZJCo6Uq4aND8Ikzxynh
Yb/yIwAyEnorIfanWXt/MNtO0vwZooiqGgIGTc8SHIyOgGuahH87i7rafz5RAQbz
NqqVJHTWQo/xcMNbQ+uLP9+nWyhnXB562cY5bicOf39rBrtGkeN2dKUxgHNxmR/f
QkHwypohUSLnhIFAi7VgzifqdNjj5Gme35NCUkKRSt8Pnyef7h0LLABXb/XOr/AQ
7D1J4kg4GDOXANp5WdzabT8DJjDCYn3ZFGImKH9XsbJ71rfMAMCIGg==
=w7Il
-----END PGP SIGNATURE-----
```

Firewall

- Hardware or software that protects a network from intrusion by outside users
- Often associated with protection from unauthorized users on the Internet



Firewall

- Does not completely isolate a network from other networks
- Can stem from one of two basic policies:
  - Everything not specifically permitted is denied
  - Everything not specifically denied is permitted
- Seeing the glass half-full or half-empty

Firewall Implementation Techniques

- Packet filtering – determines whether an information packet (based on source/destination address, port, etc.) should be permitted to pass through the firewall
- Network Address Translation (NAT) – a technique that translates a universal address into an internal address

Firewall Implementation Techniques

- Proxy server (a.k.a. application level gateway) – much stricter than packet filtering and designed to regulate access only to specific applications
- Circuit-level gateway – proxy server without packet processing and filtering; operates on network layer

Intrusion Detection

- Automated applications or manual policies used to investigate possible break-ins
- Examples:
  - Raytheon’s BladeRunner (server-based; monitors network traffic to prevent transmission of sensitive data)
  - HP’s Praesidium (detects unauthorized access, root exploits, buffer overflows, and other unusual behavior)
  - CERT Intruder Detection Checklist (suggests examining log files, system binaries, etc. to see if the system has been compromised)

IT Security in the 21st Century

- Increasing reliability of systems
- Self-healing computers
- Intelligent system for early intrusion detection
- Intelligent systems in auditing and fraud detection
- Artificial intelligence in biometrics
- Expert systems for diagnosis, prognosis, and disaster planning
- Smart cards
- Anti-hacker products
- Ethical issues in implementing security