

IF3291
Jaringan Komputer dan Pengamanannya



Network Security

Bugi Wibowo (bugi@informatika.org)
Mei 2006
Informatika – STEI – ITB



Introduction

- Early network use:
 - Universities to send mails
 - Corporate to share resource
 - No attention for security
- Nowadays:
 - millions of ordinary citizens
 - banking, shopping, and filing tax returns
 - network security is a potentially massive problem

Security

- A broad topic and covers a multitude of sins
 - Making sure that nosy people cannot read, or secretly modify messages intended for other recipients
 - Deal with people trying to access remote services that they are not authorized to use
 - Most security problems are intentionally caused by malicious (bad) people trying to gain some benefit, get attention, or to harm someone
- Involves a lot more than keeping it free of programming errors. It involves outsmarting often intelligent, dedicated, and sometimes well-funded opponents

5/10/2006

3

Who?

most common perpetrators

Adversary	Goal
Student	To have fun snooping on people's e-mail
Cracker	To test out someone's security system; steal data
Sales rep	To claim to represent all of Europe, not just Andorra
Businessman	To discover a competitor's strategic marketing plan
Ex-employee	To get revenge for being fired
Accountant	To embezzle money from a company
Stockbroker	To deny a promise made to a customer by e-mail
Con man	To steal credit card numbers for sale
Spy	To learn an enemy's military or industrial secrets
Terrorist	To steal germ warfare secrets

4



Problems

- Network security problems:
 - Secrecy: also called confidentiality, has to do with keeping information out of the hands of unauthorized users
 - Authentication: deals with determining whom you are talking to before revealing sensitive information or entering into a business deal
 - Nonrepudiation: deals with signatures
 - Integrity: how can you be sure that a message you received was really the one sent and not something that a malicious adversary modified in transit

5/10/2006

5



Where & How?

- Physical layer: wiretapping can be foiled by enclosing transmission lines in sealed tubes containing gas at high pressure
- Data link layer: packets on a point-to-point line can be encrypted as they leave one machine and decrypted as they enter another
- Network layer:
 - Firewalls: keep good packets and bad packets out
 - IP security

5/10/2006

6

Where & How?

- Transport layer: entire connections can be encrypted, end to end, that is, process to process
- Application layer: issues such as user authentication and nonrepudiation can only be handled in the application layer
 - Except for physical layer security, nearly all security is based on cryptographic principles
 - There is no one single place. Every layer has something to contribute!
 - Most security failures are due to incompetent employees, lax security procedures, or insider fraud, rather than clever criminals

5/10/2006

7

Solutions

- Focus on networking issues, rather than operating system and application issues
 - EXCLUDED:
 - user authentication using biometrics
 - password security
 - buffer overflow attacks
 - trojan horses
 - login spoofing
 - viruses
 - worms

5/10/2006

8



Solutions

- Topics:
 - Cryptography: Kerckhoff's principle of having a publicly-known algorithm and a secret key
 - Symmetric-Key Algorithms
 - Public-Key Algorithms
 - Digital Signatures & Management of Public Keys
 - Communication Security
 - IPSec, Firewall, Wireless Security
 - Authentication Protocols
 - E-Mail Security & Web Security
 - PGP, PEM, S/MIME
 - Secure DNS, SSL, HTTPS

5/10/2006

9



Social Issues

- Privacy: restrict what other people can see about us
 - Tel-co's and ISP's provide wiretaps
 - Cryptography for secure communication: PGP, SSL
 - Anonymous Remailers: privacy is best served by not having authentication. No one could tell where the message really came from
- Freedom of Speech vs. censorship
 - Steganography: science of hiding messages = "covered writing"
- Copyright: granting to the creators of Intellectual Property the exclusive right to exploit their IP for a period of time
 - Napster did not actually copy any music, but it holds a central database that helped other people infringe
 - Is it a crime to keep music you have paid for and legally downloaded on your hard disk where others might find it?

5/10/2006

10

TUGAS

- Buat 5 kelompok untuk meringkas dan mempresentasikan materi network security
- Pembagian topik adalah sebagai berikut:
 - Kelompok 1: Cryptography, Symmetric-Key Algorithms dan Public-Key Algorithms
 - Kelompok 2: Digital Signatures & Management of Public Keys
 - Kelompok 3: Communication Security
 - Kelompok 4: Authentication Protocols
 - Kelompok 5: E-Mail Security & Web Security
- Bahan untuk presentasi diambil dari textbook (Tanenbaum) dan bisa diakses di web (kur2003)

5/10/2006

11

TUGAS

- Hasil ringkasan:
 - Softcopy dikirimkan ke bugi@informatika.org
 - Hardcopy dikumpulkan di kelas tanggal 16 Mei 2006
- Presentasi dilakukan pada jadwal kuliah:
 - Kelompok 1,2, dan 3: Selasa 16 Mei 2006
 - Kelompok 4 dan 5: Rabu 17 Mei 2006

5/10/2006

12