

DATACOMM

John Abbott College JPC

Datacomm Security

M. E. Kabay, PhD, CISSP
Director of Education, ICESA
President, JINBU Corp

Copyright © 1998 JINBU Corp.
All rights reserved

DC 6 - 1

Datacomm Security

- Data Integrity
- Sources of Error
- Controlling Errors
- Other Elements of Security

DC 6 - 2

Data Integrity

- Integrity refers to correctness and completeness
- Switched telephone system has variable quality
 - Some virtual circuits are silent
 - Others are noisy--contain random and non-random extraneous and transient signals
- Effects of noise
 - Obliterates differences between 0s and 1s
 - High-frequency transfers especially susceptible to distortion of signal
 - Results in data loss
- Noise originates in electrical interference
 - e.g., lightning storms, motors, transmitters

DC 6 - 3

Sources of Error

Options for handling errors

- Check nothing
- Error detection with flagging
- Error detection with request for retransmission
- Forward error correction (FEC)
 - intelligent receiver
 - detect and correct certain errors

DC 6 - 4

Controlling Errors

- Echo Checking
- Parity Checking
- Cyclical Parity
- Hamming Code
- Checksums
- Cyclical Redundancy Check

DC 6 - 5

Controlling Errors

Echo Checking

- Send back all data to host (transmitter) for comparison with original message
- Echoplex data transmission on old terminals sent data to host and then back to display
- Expensive: at least doubles transmission time
- Effectiveness depends on how errors are detected solely on the host
- May introduce false positives where terminal received data OK but return to host had noise
- Used for critical applications

DC 6 - 6

Controlling Errors

Parity Checking

- Typically checks every character
- Add a parity bit to each 7-bit character
- Even parity
 - 0 if even # of 1s in byte
 - 1 if odd # of 1s in byte
- Odd parity
 - 0 if odd # of 1s in byte
 - 1 if even # of 1s in byte
- Does not permit correction of the error

DC 6 - 7

Controlling Errors

Cyclical Parity

- Two or more parity bits
- Permits detection of more types of error than simple parity check
- Can have each parity bit depend on specific bits in byte
 - E.g., parity bit #1 could check bits 1, 3 & 5 of a 6-bit sequence;
 - parity bit #2 could check bits 2, 4 & 6 of the 6-bit sequence

DC 6 - 8

Controlling Errors

Hamming Code

- FEC using 4 parity bits per byte
- Places parity bits in positions 1, 2, 4 & 8
- Data bits in positions 3, 5, 6, 7, 9, 10 & 11
- Each data bit is part of the parity calculation for two or three parity bits
- Can detect all single-bit errors and exactly correct the error
- High overhead (4 parity bits for 7 data bits) has kept applications rare

DC 6 - 9

Controlling Errors

Checksums

- Add up the data
- Append results to data
- After transmission, recalculate checksum
- Compare new checksum with transmitted checksum

DC 6 - 10

Controlling Errors

Cyclical Redundancy Check

- Similar to checksum
- Uses more complicated arithmetic; e.g., addition, multiplication, division, subtraction
- Generates a hash total
- Can ensure that almost all errors, including multi-bit errors, will be caught
- Widely used
 - client account numbers
 - telephone and credit card numbers

DC 6 - 11

Other Elements of Security

NIST goals of datacomm: message should be

- sealed--unmodifiable without authorization
- sequenced--numbered to prevent loss or duplication
- secret--incomprehensible except to authorized recipient(s)
- signed--non-repudiable authentication
- stamped--non-repudiable receipt of message

DC 6 - 12

Datacomm Security

- Secure Transmission Facilities
- Passwords
- Historical and Statistical Logging
- Closed User Groups
- Firewalls
- Encryption
- Confidentiality and Authenticity

DC 6 - 13

Secure Transmission Facilities

Transmission media have different vulnerabilities

- Easiest to tap: wireless & cellular telecomm
- Easy: twisted pair, coax
- Possible: satellite and terrestrial microwave
- Hardest: fibre optic lines

DC 6 - 14

Passwords

- Security uses I&A: identification and authentication
- Identification depends on user ID
- Authentication can depend on
 - what you know; or
 - what you have; or both
 - what you are (or how you do stuff)
- Commonest form of authentication is password
- Other devices include one-time password generator
- Call-back devices limit access to known locations

DC 6 - 15

Historical and Statistical Logging

- Historical:
 - record all data passing through device
 - AKA *audit trails*
- Mainframe systems typically log
 - all login/logout
 - file opens/closes & which records changed
 - device requests (printers, tapes....)
- Statistical logging
 - How long user IDs access specific files
 - Does not keep record-level detail

DC 6 - 16

Closed User Groups

- Set of user IDs that can access information
- Can also define CUGs on VANs such as CompuServe
- ICSA has CUGs for clients taking on-line courses

DC 6 - 17

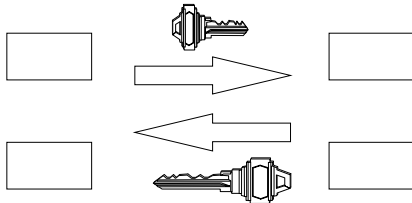
Firewalls

- Firewall = data filter to examine all inbound and outbound data
- Firewall can prevent intruders from gaining access to certain parts (or any) of system
- Accept inbound connection only from trusted hosts
- Can set up internal firewalls to segregate certain systems from each other; e.g., research computers protected from sales users
- Application-level firewalls search data stream for e-mail, database access, file transfers
- Firewalls susceptible to *IP address spoofing*

DC 6 - 18

Encryption

- Scramble data using a key and descramble using a key
- Key is a secret data sequence

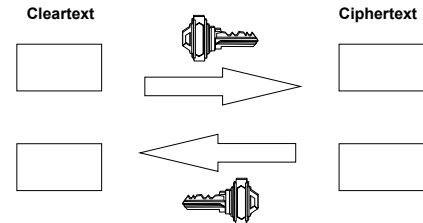


DC 6 - 19

Encryption

Symmetrical algorithms; e.g., DES

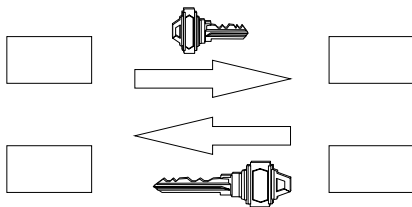
- Problem of key management & distribution
- Number of key pairs rises as n^2



DC 6 - 20

Encryption

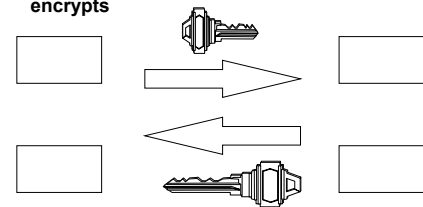
- Asymmetrical algorithms
- Keys and algorithms may both be different for encryption and decryption



DC 6 - 21

Encryption

- Public Key Cryptosystem; e.g., PGP
- Generate 2 keys: keep 1 private, make 2 public
- Only the other key can decrypt what 1 key encrypts



DC 6 - 22

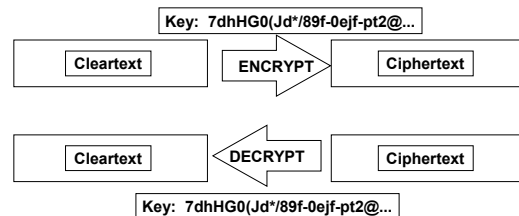
Confidentiality and Authenticity

- To keep message secret, encrypt using recipient's *public* key
- To prove origin of message, encrypt message using author's *private* key
- Current applications generally create a checksum and encrypt it with private key--faster than encrypting entire message
- See <<http://www.pgp.com>> for freeware version of PGP for private use

DC 6 - 23

Encryption: DES

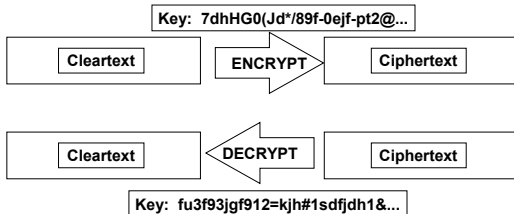
- Data Encryption Standard
 - example of symmetric encryption algorithm
 - especially useful for storing encrypted data



DC 6 - 24

Encryption: PKC

- Public Key Cryptosystem
 - example of asymmetric encryption
 - especially good for communications and for digital signatures



DC 6 - 25

Encryption: PKC (cont'd)

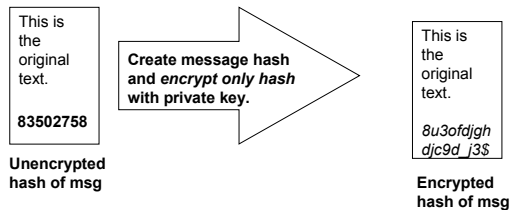
PGP is an example of the PKC

- Key generation produces 2 keys
- Each can decrypt *only* the ciphertext produced by the other
- One is defined as *public*
- Other is kept as *private*
- Can easily send a message so only the desired *recipient* can read it:
 - encrypt using the _____'s _____ key
 - decrypt using the _____'s _____ key

DC 6 - 26

Encryption: PKC (cont'd)

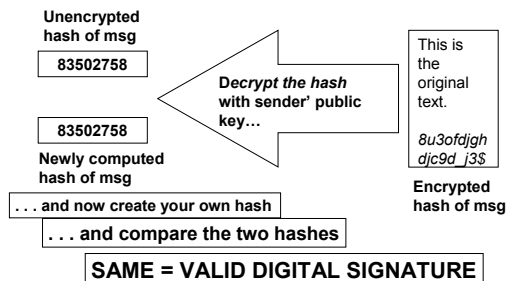
- Signing a document using PKC



DC 6 - 27

Encryption: PKC (cont'd)

- Verifying the signature using PKC



DC 6 - 28

Communications Encryption

- Encrypted messages
 - ideally all messages should be encrypted
 - public messages should be signed digitally
- Virtual Private Networks
 - packets destined for remote network are encrypted before being sent to remote system
 - automatically decrypted upon receipt

DC 6 - 29

Homework

- Read Chapter 6 of your textbook in detail, adding to your workbook notes as appropriate.
- Review and be prepared to define or expand all the terms listed at the end of Chapter 6 of your textbook (no hand-in required)
- Answer all the exercises on pages 128 of the textbook using a computer word-processing program or *absolutely legible* handwriting (hand in *after* quiz tomorrow morning)

DC 6 - 30