2110413 Computer Security

Lecture 5

Integrity, encryption, & buffer overflow

Krerk Piromsopa, Ph.D.
Department of Computer Engineering
Chulalongkorn University

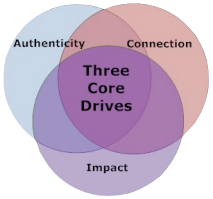
Outline

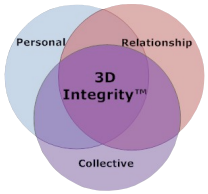
- Definition
- Trust
- Hardware
- Cryptography (intro.)
- Physical Temper Resistance
- Protection against Buffer-overflow attacks

Integrity

"Integrity without knowledge is weak and useless, and knowledge without integrity is dangerous and dreadful."
Samuel Johnson (1709 - 1784)

- Integrity is a characteristic that belongs to people who are self-actualized. It is the quality or condition of being whole, complete, unbroken, and undivided. Knowing oneself heightens a person's integrity.
- Applying to data, it also refers to the state of being whole and undivided or the condition of being unified and





The forth A

- Integrity is sometime referred as ***Authenticity***—hence it is sometime mentioned as the forth "A" of security components.
- How can we preserve the integrity of data?

Trust

"Real integrity is doing the right thing, knowing that nobody's going to know whether you did it or not."
Oprah Winfrey, in Good Housekeeping

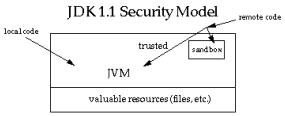
- Trust is a a basis for every security model.
- I trusted you. What does it mean?
  - believe in the reliability, truth, ability, or strength of [M-W]
- What do you trust?

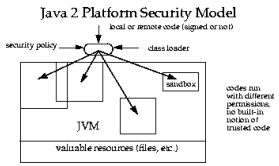
Trust in action

- single user operating system with no protection (DOS, CP/M, Windows < NT)
- Embedded Systems (Appliances)
- What else?

How to minimize trust?

- Trust with respect to boundary
  - Sandbox
  - Domains (isolation)



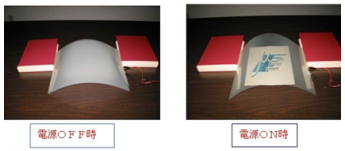


Pop Quiz

- Who do you trust to sign your code?
- Is a signed applet (or ActiveX) a safe program?
- What mechanism is necessary to implement sandbox and/or domain?

Hardware support

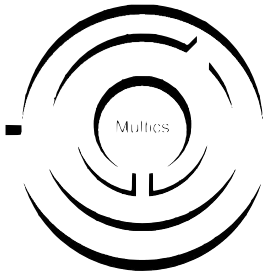
- Electronic curtain
  - Ring
    - Segmentation
    - Page
- Tagged Memory



9

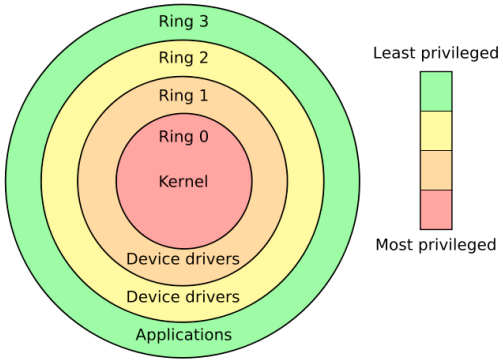
Ring

- Back as far as Multics (1960)
- Processor provides memory compartments
  - Segmentation
  - Page
- How many rings do we really need?



10

Intel 386



11

Integrity without hardware support

12

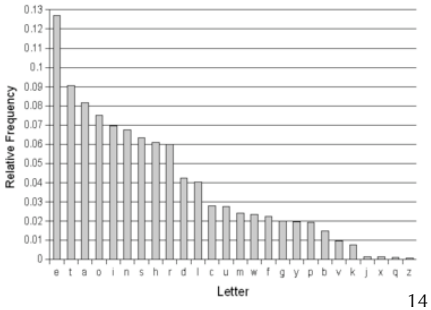
Encryption: History

- Monoalphabetic Substitution Cipher
- Julius Caesar (50 BC) used it.
  - `abcdefghijklmnopqrstuvwxyz`
  - `SECURITYABDFGHJKLMNOPQVWXZ`
- What is...? YRFFJ VJMFU

13

Hacking

- Given a sufficiently large encoded message, it can readily be "cracked" by comparing the frequency of letter occurrences in the coded message with the frequency of letter occurrences in the language used for the message.



14

Try this

- Gur fbyhgvba gb gur pvcure vf gur anzr nhoerl juvpu jnf qvssvphyg gb fbyir orpnhfr yvfgf bs cgbyrzl pbafgryyngvbaf jrer vapbafvfgrag. Vg gbbx frireny snvyrq nggrzcgf orsber svaqvat n jbexnoyr yvfg.

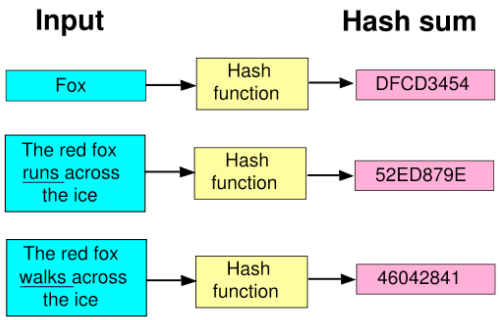
15

Modern Encryption

- Hash Digests(short input > long output)
- Stream Cipher
  - RC4 (SSL, WEP, WPA, etc...)
- Block Cipher
  - DES, Blowfish, AES
- Public Key

16

Hash function



Collision ??

17

Early Stream Cipher

Vigenere (1467)

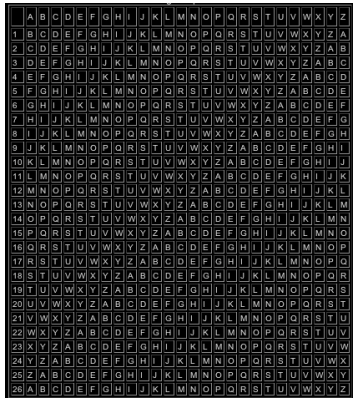
first Polyalphabetic cipher

LUCKYLUCK
COMPUTING

NIOZSECPQ

$$C_i \equiv P_i + K_i \pmod{26}$$

$$P_i \equiv C_i - K_i \pmod{26}$$



18

Early Block Cipher

Playfair

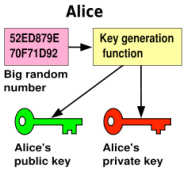
F I R S T
A M E N D
B C G H K
L O P Q U
V W X Y Z

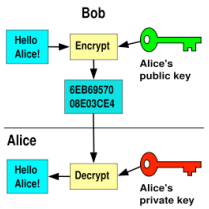
- Grouping data in two, and use the corner to encode data.
- Example,

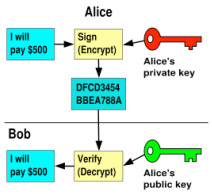
CO MP UT ER
OW EO ZD GE

19

Public Key

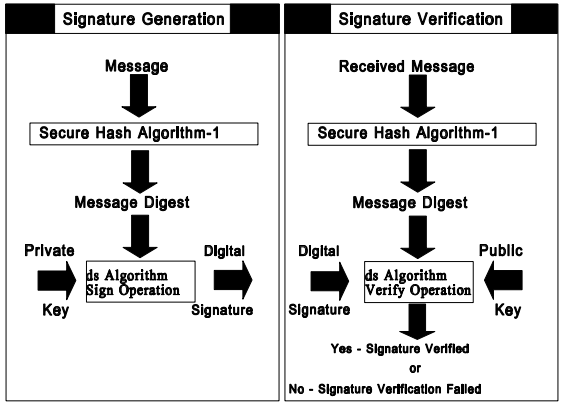






20

Digital Signature



21

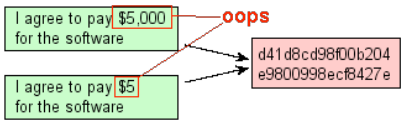
POP Quiz

- What kind of security do we get from encryption?
- Most people think that encryption is secure.
  Do you agree or disagree?

22

Other issues

- Key management (see PKI)
- Collision of hashing function
  http://www.mathstat.dal.ca/~selinger/md5collision/



23