Operation Security & & Malicious Software

- Understand the core of Operations Security (OPSEC)
- Define & identify targets and threats
- Establish countermeasures
- Identify the Critical Information Commandments
- Decipher the value of information

- Have you ever taken precautions against Someone...
 - ...breaking into your house while you're on vacation?
 - ... stealing your purse?
 - ...stealing packages from your car while your shopping?
 - ... fraudulently using your credit card?

Then you have used OPSEC!

 OPSEC is a risk management instrument that enables a manager or commander to view an operation or activity from the perspective of an adversary. It is a process of <u>identifying</u>, <u>analyzing</u> and <u>controlling</u> critical information.

- Identify Critical Information
- Analyze Threats
- Discover Vulnerabilities
- Assess Risks
- Develop Countermeasures

• Identify Critical Information:

 Credit card numbers, travel dates, passwords, patterns, changes in patterns, inspection results, information base systems, etc..

• Analyze Threat:

 Adversaries, Intelligence agencies – Open source information, corporate/state sponsored spies, eavesdropping, photographing, etc...

- Discover Vulnerabilities:
 - Flow of information, operations, timing of events, how an adversary would acquire the information, etc...
 - How would the loss of such data impact the organization?
- Assess Risks:
 - Estimated loss \$ x impact of risk x likelihood of risk = \$

Develop Countermeasures:

 are based on the vulnerabilities and inherent risks.

- computer viruses have got a lot of publicity
- one of a family of malicious software
- effects usually obvious
- have figured in news reports, fiction, movies
- getting more attention than deserve
- are a concern though

The Most Common Types Of Program To Be Infected by A Virus

- exe
- com
- vbs
- Mp3
- bin
- script files
- macros

Malicious Software



Trapdoors

- secret entry point into a program
- allows those who know access bypassing usual security procedures
- have been commonly used by developers
- a threat when left in production programs allowing exploited by attackers
- very hard to block in O/S
- requires good s/w development & update

- one of oldest types of malicious software
- code embedded in legitimate program
- activated when specified conditions met
 - eg presence/absence of some file
 - particular date/time
 - particular user
- when triggered typically damage system
 modify/delete files/disks

- program with hidden side-effects
- which is usually superficially attractive
 eg game, s/w upgrade etc
- when run performs some additional tasks
 - allows attacker to indirectly gain access they do not have directly
- often used to propagate a virus/worm or install a backdoor
- or simply to destroy data

- program which secretly takes over another networked computer
- then uses it to indirectly launch attacks
- often used to launch distributed denial of service (DDoS) attacks
- exploits known flaws in network systems

- a piece of self-replicating code attached to some other code
- propagates itself & carries a payload
 - carries code to make copies of itself
 - as well as code to perform some covert task

- virus phases:
 - dormant waiting on trigger event
 - propagation replicating to programs/disks
 - triggering by event to execute payload
 - execution of payload

- can classify on basis of how they attack
- parasitic virus
- memory-resident virus
- boot sector virus
- stealth
- polymorphic virus
- macro virus

- macro code attached to some data file
- interpreted by program using file -eg Word/Excel macros
 - –esp. using auto command & command macros

- spread using email with attachment containing a macro virus
- triggered when user opens attachment
- or worse even when mail viewed by using scripting features in mail agent
- usually targeted at Microsoft Outlook mail agent & Word/Excel documents

- replicating but not infecting program
- typically spreads over a network
- using users distributed privileges or by exploiting system vulnerabilities
- widely used by hackers to create zombie PC's, subsequently used for further attacks, esp DoS
- major issue is lack of security of permanently connected systems, esp PC's

- worm phases like those of viruses:
 - dormant
 - propagation
 - search for other systems to infect
 - establish connection to target remote system
 - replicate self onto remote system
 - triggering
 - execution

- viral attacks exploit lack of integrity control on systems
- to defend need to add such controls
- typically by one or more of:
 - prevention block virus infection mechanism
 - -detection of viruses in infected system
 - reaction restoring system to clean state

- have considered:
 - various malicious programs
 - trapdoor, logic bomb, trojan horse, zombie
 - viruses
 - worms
 - countermeasures

Public Key Cryptosystem

- Essential steps of public key cryptosystem
 - Each end generates a pair of keys
 - One for encryption and one for decryption
 - Each system publishes one key, called public key, and the companion key is kept secret
 - It A wants to send message to B
 - Encrypt it using B's public key
 - When B receives the encrypted message
 - It decrypt it using its own private key

Alice wants Bob to send her a message. She:

- selects two (large) primes p, q, TOP SECRET,
- computes n = pq and φ(n) = (p-1)(q-1), φ(n) also TOP SECRET,
- selects an integer e, 1 < e < φ(n), such that gcd(e, φ(n)) = 1,
- computes d, such that de ≡ 1 (mod φ(n)), d also TOP SECRET,
- gives public key (e, n), keeps private key (d, p, q).

RSA Example

- 1. Select primes: p=17 & q=11
- **2.** Compute $n = pq = 17 \times 11 = 187$
- 3. Compute $\varphi(n) = (p-1)(q-1) = 16 \times 10 = 160$
- 4. Select e : gcd (e, 160) =1; choose e=7
- 5. Determine d: $de=1 \mod 160$ and d < 160 Value is d=23 since $23 \times 7 = 161 = 10 \times 160 + 1$
- 6. Publish public key $KU = \{7, 187\}$
- **7.** Keep secret private key KR={23,17,11}

RSA Example cont

- sample RSA encryption/decryption is:
- given message M = 88 (nb. 88<187)
- encryption:

 $C = 88^7 \mod 187 = 11$

• decryption:

 $M = 11^{23} \mod 187 = 88$

Q & A

Questions ?