THE UNIVERSITY OF BRITISH COLUMBIA

Malicious Logic

EECE 412

Session 17

Last Session Recap

Security policies

- Integrity Policies
  - Biba integrity model
  - Clark-Wilson integrity model
- Hybrid Policies
  - Chinese Wall model
  - Clinical Information Systems Security policy (self-study)
  - ORCON model
  - RBAC model

Outline

- Types of malicious logic
- Theory & Malware
  - Viruses
  - Worms
  - etc.
- Protection and Detection Techniques

THE UNIVERSITY OF BRITISH COLUMBIA

Malicious Logic

Malicious Code Types

- Trojan horse
- virus
- worm
- rabbit/bacterium
- logic bomb
- trapdoor/backdoor

Non-malicious program errors

- buffer overflow
  - data replaces instructions
- incomplete mediation
  - sensitive data are in exposed, uncontrolled condition
- time-of-check to time-of-use errors
  - leaving opportunity to changing data/request after it was checked/authorized and before it was used/processed
- mistakes in using security mechanisms

Whys

- Why is malicious logic bad?
- Why should we know how it works?

Trojan Horses

- has overt and covert effects
  - Examples of overt and cover effects?
- propagating Trojan horse
- Thompson's experiment with a Trojan horse

1. Add TH to a login program source code
   - login + TH = login'
2. Add TH to the complier
   - complier + TH = complier'
   - compile'(login) = login'
3. Add TH to the old compiler to build new compiler'
   - compile(compiler) = compiler'
   - compile'(login) = login'

- "Reflections on trusting trust"

THE UNIVERSITY OF BRITISH COLUMBIA

Computer Viruses

What's a Computer Virus?

Program that

1. "infects" other programs with itself, and
2. performs some (possibly null) action

Is a virus also a Trojan horse?

Classification of Virus Types

Virus Type	What infect		How run		Resident in memory		How hide		
	Boot sector	executable	executable	interpreted	Yes	No	Conceal infection	Encrypts itself	Changes form
Boot sector infectors	■		■						
Executable infectors		■	■						
Multipartite viruses	■	■	■						
TSR Viruses					■				
Stealth Viruses							■		
Encrypted Viruses								■	
Polymorphic Viruses									■
Macro Viruses				■					

Examples of Viruses

Virus Example	What infect		How run		Resident in memory		How hide		
	Boot sector	executable	executable	interpreted	Yes	No	Conceal infection	Encrypts itself	Changes form
Brain virus									
Jerusalem virus									
Encroacher virus									
Stealth (a.k.a., IDF) Virus									

THE UNIVERSITY OF BRITISH COLUMBIA

Computer Worms

What's a Computer Worm?

"a program that

1. can run independently and
2. can propagate a fully working version of itself to other machines."

E. Spafford in "A Failure to Learn from the Past"

What's the difference between computer worms and viruses?

THE UNIVERSITY OF BRITISH COLUMBIA

Other Forms of Malicious Logic

- rabbit/bacterium
  - replicates itself without limit to exhaust resource
- logic bomb
  - goes off when specific condition occurs
- trapdoor/backdoor
  - allows system access through undocumented means

THE UNIVERSITY OF BRITISH COLUMBIA

Malware Theory

Could we detect any malware?

Could an algorithm exist that would determine if an arbitrary program contains a malicious code?

Relevant Results

- There is no generic technique for detecting all malicious logic
- Detection and protection focuse on particular aspects of specific logic

THE UNIVERSITY OF BRITISH COLUMBIA

Particular Aspects of Malware and Corresponding Protection and Detection Techniques

Malware acting both as data and code

Approach: **Keep data and code separate**

Techniques

- Allow files to be either modifiable or executable but not both
- Change the type of modified executable to "data"
- Require explicit actions to make data executable

Malware uses privileges of authorized users

Approach: **Reduce the amount of damage**

Techniques:

- Restrict how far data can travel
- Exercise the principle of least privilege
- Sandboxing

Malware Uses Sharing to Cross Protection Domain Boundaries

Approach: **Prevent data sharing**

Techniques:

- Assign programs lowest security level in MLS systems

Malware Alters Files

Approach: **Detect Alterations**

Techniques:

- Signature blocks
  - Tripwire
- Virus signatures used by antivirus scanners

Malware Performs Actions Beyond Specification

Approach: Treat the problem as a Fault Tolerance one

Techniques:

- N-version programming: votes on results
- Proof-carrying code: proving compliance with safety requirements

Malware Alters Statistical Characteristics

Approach: Detect statistical changes

Techniques:

- Detecting abnormal activities on systems or networks