THE UNIVERSITY OF BRITISH COLUMBIA

Malicious Logic

EECE 412

Outline

- Malware
  - Viruses
  - Worms
    - Stuxnet worm
  - Trojan horses
  - Other malware
- Protection and Detection Techniques
  - Limitation of malware detection
  - Possible solutions

Types of security flaws

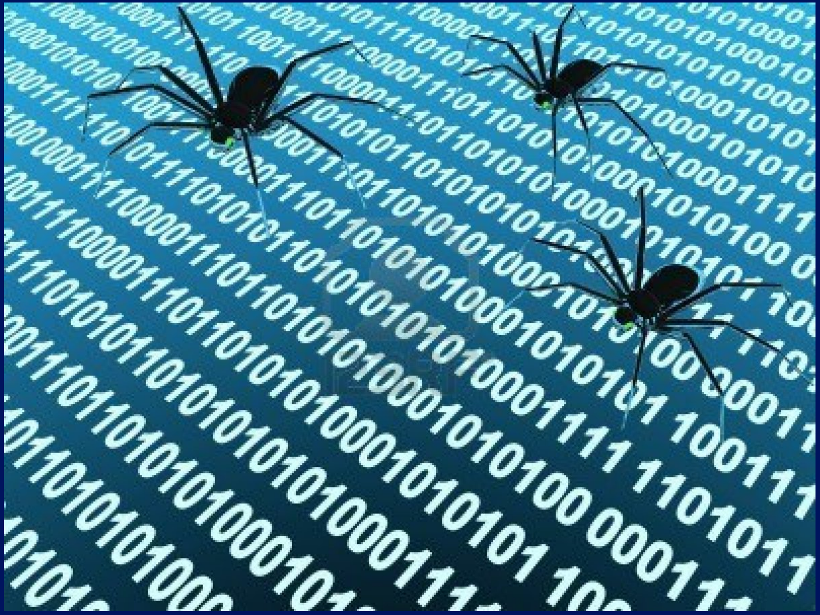
- Malicious logic is intentionally developed to attack systems; we call it malware.
- Non-malicious program errors are occur because of unintentional mistakes made by developers, which cause malfunctions.

Non-malicious program errors

- buffer overflow errors
  - occur when |input| > |buffer|
  - replaces instructions with data
- incomplete mediation errors
  - occur when the application accepts incorrect data from the user
  - are failures to perform "sanity checks" on data
- time-of-check to time-of-use (TOCTTOU) errors
  - occur in asynchronous programs when shared data is changed after it is checked but before it is used
  - are also known as "race condition" errors
- mistakes in using security mechanisms

Malicious code types

- (computer) virus
- worm
- trojan horse
- trapdoor/backdoor
- rabbit/bacterium
- logic bomb



Whys

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

Computer Virus

What’ s a Computer Virus?

Program that

1. “infects” other programs with itself, and
2. performs some (possibly null) actions
3. relies on a host program to propagate from one system to another

Computer Worm

What' s a Computer Worm?

"an independently replicating and autonomous infection agent, capable of seeking out new host systems and infecting them via the network"

Jose Nazario in

"Defense and Detection Strategies Against Internet Worms"

What' s the difference between computer worm and virus?

Functions of a Worm (network)

1. Reconnaissance: finding hosts to attack
2. Attack: launching an attack
3. Communication: enabling communications among worm nodes as well as with other central location(s)
4. Command: providing interface for receiving commands
5. Intelligence: managing information about the worm nodes

THE UNIVERSITY OF BRITISH COLUMBIA

Stuxnet

Talk about Stuxnet

http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html

Overview of Stuxnet

- A highly sophisticated computer worm which targets industrial and factory system (Siemens programmable logic controllers)
- Malware discovered July 10; old versions (June 2009) later found
- Spreads using four vulnerabilities (Windows shortcut, Windows print spooler, Windows server RPC, plus undisclosed)
- Also infects via USB drives
- Peer-to-peer control/update network
- Written by five people over six months

Seimens Programmable Logic Controllers (PLCs)

Industrial Control Systems (ICSs) are operated by a specialized assembly like code on PLCs.

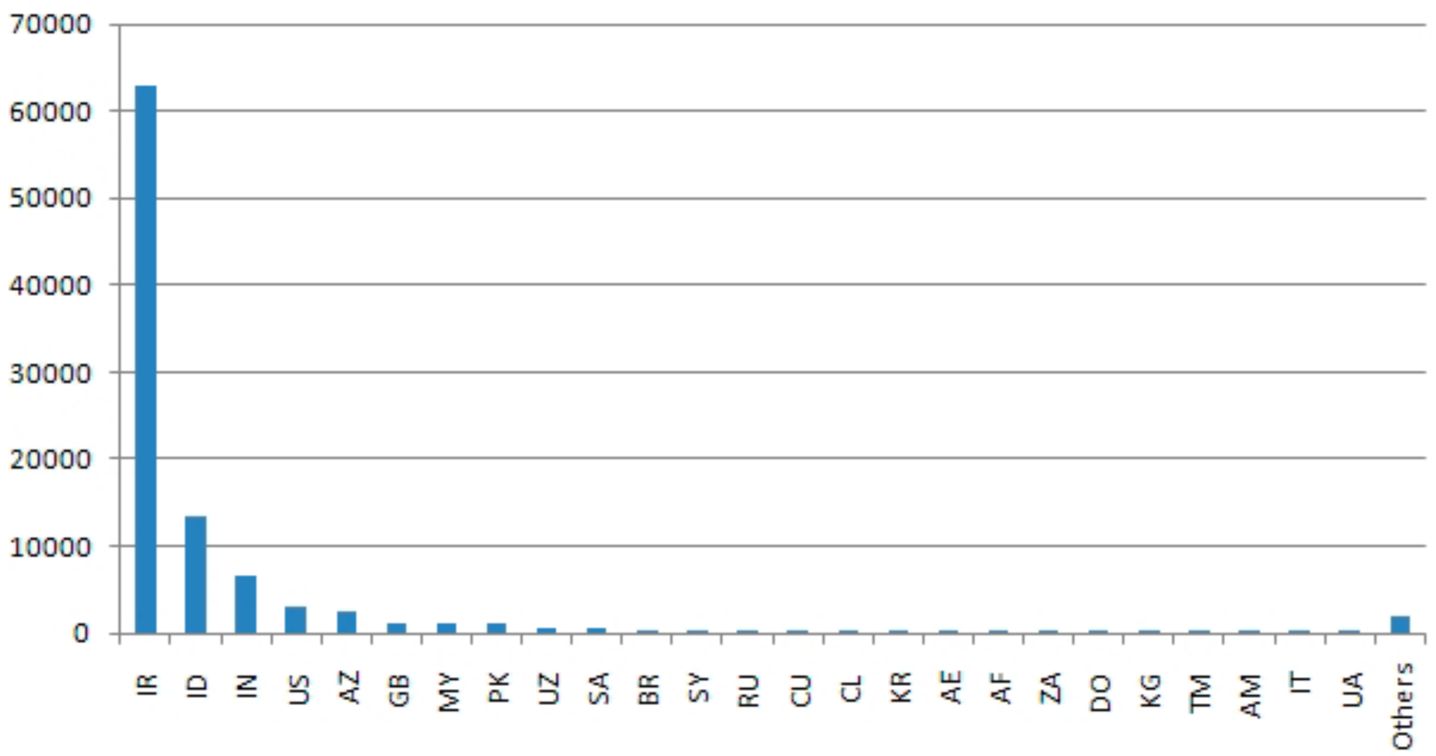
Functions of Stuxnet Worm

1. Reconnaissance
    - Analysis of documents (stolen by an insider?) about target ICS and PLC
2. Attack
    - Zero-day exploits
    - Windows rootkit
    - PLC rootkit
3. Communication
    - USB drive, Targeted emails (initial delivery)
    - HTTP, Remote Procedure Call (RPC)
4. Command
    - Typical command and control infrastructure
    - P2P updates within Local LAN
5. Intelligence
    - P2P updates without command and control infrastructure

Stuxnet’s characteristics

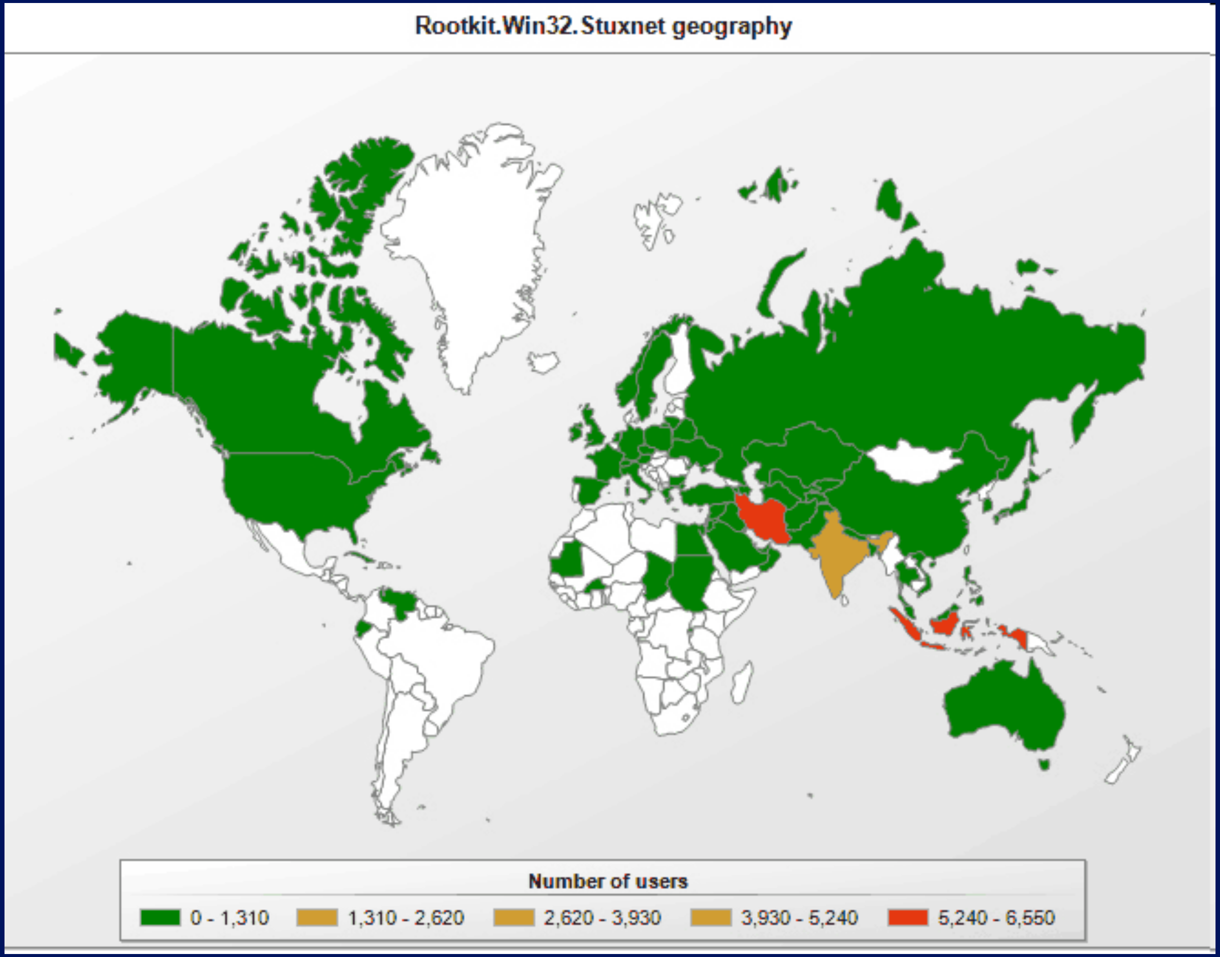
Aspect	Stuxnet	Common malware
Targeting	Extremely selective	Indiscriminate
Type of target	Industrial control systems	Computers
Size	500 Kbytes	Less than 1 Mbytes
Probable initial infection vector	Removable flash drive	Internet and other networks
Exploits	Four zero-days	Possibly one zero-day

A targeted attack on industrial locations in Iran



Graph shows concentration of Stuxnet-infected computers in Iran

Windows rootkit geography



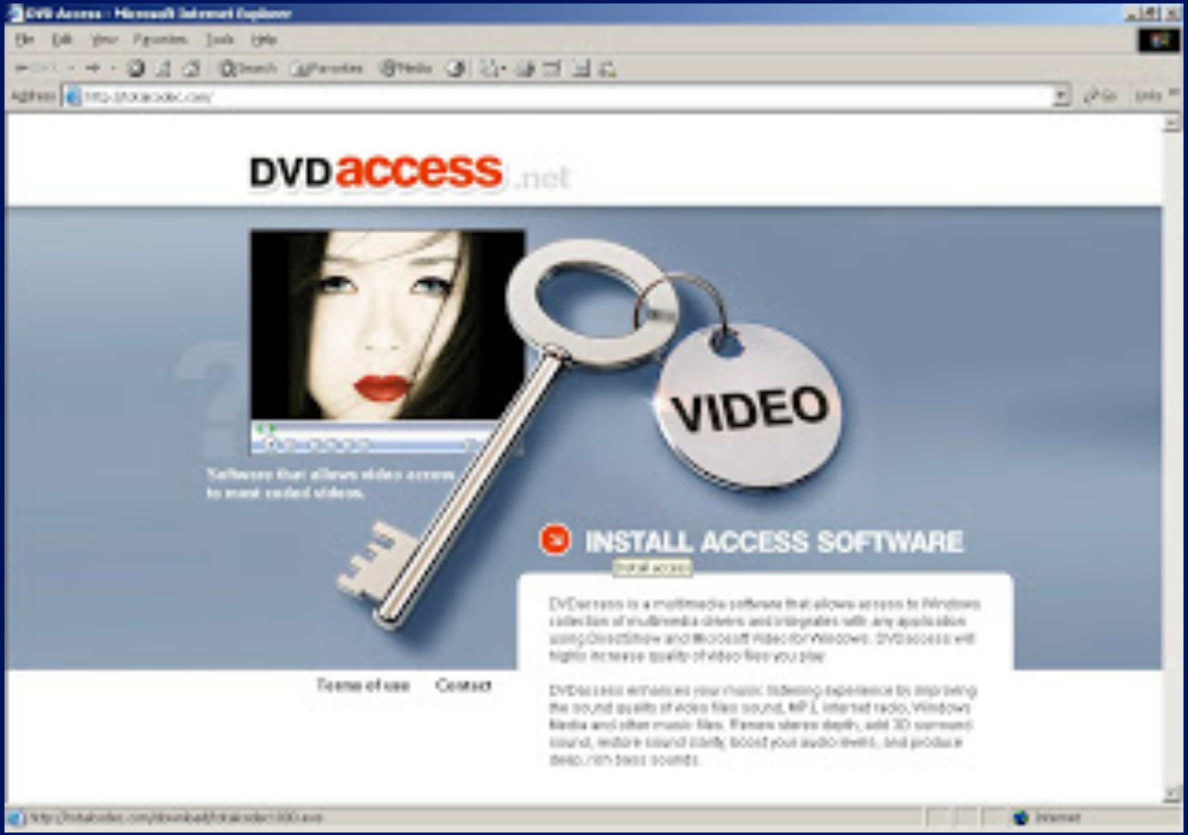
Trojan Horse

What’ s a Trojan Horse?

Program that

1. “masquerades” as a legitimate file or helpful program, but
2. has some unexpected function

An example: fake codec



Software that allows video access to most coded videos.

DVDaccess is a multimedia software that allows access to Windows collection of multimedia drivers and integrates with any application using DirectShow and Microsoft Video for Windows. DVDaccess will highly increase quality of video files you play.

DVDaccess enhances your music listening experience by improving the sound quality of video files sound, MP3, internet radio, Windows Media and other music files. Renew stereo depth, add 3D surround sound, restore sound clarity, boost your audio levels, and produce deep, rich bass sounds.

The downloads from this site informs the user that it will permit you to view free porn videos online, but installing this codec will actually install harmful Trojan horse program on the system.

Other Forms of Malicious Logic

- rabbit/bacterium
  - replicates itself continually to exhaust system resources
- logic bomb
  - goes off when specific conditions are met
- trapdoor/backdoor
  - allows system access through undocumented means

THE UNIVERSITY OF BRITISH COLUMBIA

Malware Theory

Anti virus software programs

Are they really effective?

Could we detect any malware?

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

Malware detection is undecidable

(See “Computer viruses: Theory and experiments”, 1987)

Proof. Assume there exists some program A that correctly detects all viruses.

- A would take in a program P and determine whether P is a virus and would return True if it is; otherwise, return False.

To show the contradiction under this assumption, we can construct a program X with A as a subroutine as follows:

X: {If A(X) is True, then halt; otherwise spread.} (We can see that X can be a virus or normal program depending on the output of A.)

When we run A with X as input, we can see the contradiction. A either loops on X forever or produces output (True or False).

If it produces some output then that output is always wrong, no matter whether it is True or False. Thus, there is no A that decides whether X is a virus or not.

The meaning of undecidability

- Undecidability means there is no procedure that:
  - a) always gives the correct answer
  - b) always terminates
- Therefore, we should give up one of these to solve an undecidable problem.
- Detection and protection focus on particular aspects of specific logic

Particular Aspects of Malware and Corresponding Protection and Detection Techniques

Malware Acts 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: **Limit user account access and minimize user privileges**

Techniques:

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

Malware Uses Sharing to Cross Protection Domain Boundaries

Approach: **Prevent data sharing**

Techniques:

- Assign the lowest level in Multi-Level Security (MLS) to programs

Malware Alters Files

Approach: **Detect Alterations**

Techniques:

- Signature blocks
  - these signature blocks can be 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 Behaves Different than Normal Software

Approach: **Detect statistical changes due to malware’s behaviors**

Techniques:

- Detecting abnormal activities on systems and/or networks

Summary

Aspect of Malware	Protection/Detection Technique
Acting both as data and code	Keep data and code separate
Using privileges of authorized users	Limit user account access and minimize user privileges
Using sharing to cross protection domain boundaries	Prevent data sharing
Altering files	Detect alterations
Performing actions beyond specification	Treat the problem as a Fault Tolerance one
Behaving different than normal software	Detect statistical changes due to their behaviors

Who will win the race?

Malware writers or AV companies?

Limitation of AV scanners

The percentage of early (near 0-day) detections by top AV products (AntiVirus Performance Statistics, http://winnow.oitc.com/malewarestats.php) shows that malware attacks are in the vast majority of cases going undetected.

AVG	22%
Avast	22%
Kaspersky	44%
BitDefender	46%
McAfee	23%
Symantec	23%
NOD32	40%
Microsoft	18%
Sophos	27%

Module summary

- theory of malware
  - Viruses
  - Worms (real example: Stuxnet)
  - etc.
- protection and detection techniques