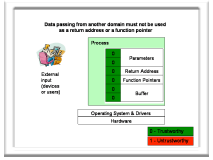


# 2110413 Computer Security

Lecture 11

Secure Bit, Internet Laws & Reviews

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

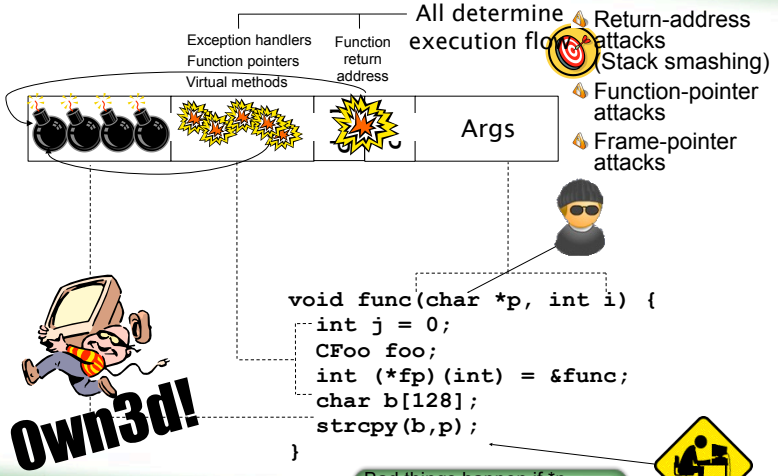
# Outline

- Secure Bit, Canary Bit
- Internet Law
  - Concepts & Case Study
- Reviews

# Secure Bit

- A tag (bit) is added to every byte of memory.
- Moving data across domain causes the associated secure bit of target to be set.
- There is no way to clear the bit.

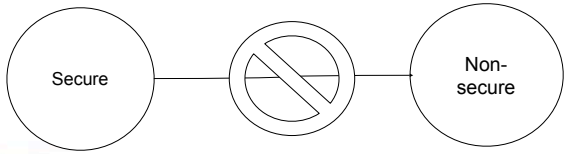
## Stack Buffer Overflows at Work




Michael Howard, Microsoft

# Secure System

- ***Definition 4:*** A **security policy** is a statement that partitions the states of the system into a set of authorized, or secure, states and a set of unauthorized or nonsecure, states. [Bishop]
- ***Definition 5:*** A **secure system** is a system that starts in an authorized state and cannot enter an unauthorized state. [Bishop]





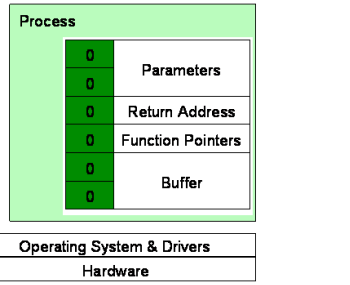

# Protocol Enforcement

- "Threat surface" is defined as all possible input crossing from the software interface.
- A domain is a boundary with respect to the current process
- ***sbit_write*** mode is added to a processor for passing data across domain (set Secure Bit)
- The ***kernel*** will use this mode to move data across domains.
- ***Call, Jump, and Return instructions*** are modified.



**Data passing from another domain must not be used as a return address or a function pointer**

External input (devices or users)




# Components of Laws

- Territorial borders (geographical borders and physical borders)
- Power (Control over physical space)
  - e.g. the U.S. government does not impose its trademark law on a Brazilian business operating in Brazil.
- Effects (direct impact)
  - e.g. a large sign over "Jones' Restaurant" in Rio de Janeiro is unlikely to have an impact on the operation of "Jones' Restaurant" in Oslo, Norway
- Legitimacy
- Notice (boundary changes)

## Yahoo!, Inc. v. La Ligue Contre Le Racisme Et L'antisemitisme, 169 F. Supp. 2d 1181 (N.D. Cal. 2001)

- LICRA - NGO dedicated to eliminate anti semitism.
- Yahoo - organized under the laws of Delaware with head quater in Santa Clara, California

## What else?

- Playboy Enter., Inc. v. Chuckleberry Publ'g, Inc., 939 F. Supp. 1032 (S.D.N.Y. 1996)
- Singapore and Chewing Gum

# What do we need?

- the needs of the interstate and international systems
- the relevant policies of the forum
- the relevant policies of other interested states and the relative interests of those states in the determination of the particular issue
- the protection of justified expectations
- the basic policies underlying the particular field of law
- • certainty, predictability and uniformity of result
- • ease in the determination and application of the law to be applied

# Reviews

# Security and Privacy

*"Security is the first cause of misfortune."*
*Old German Proverb*

- Security
  - Who can do what when?
- Privacy
  - The freedom to control access to our personal information

# Security or Privacy?

- a hacker is able to compromise a computer system and find out that a person
  is **a homosexual**
  or
  is **infected with a bad decease.**


# Reminders

# Paper

- Due last day of class
- A 5-10 page paper
- Theme is security analysis of various operating systems using the knowledge learned from this class.
- I will provide a list of topics for you to pick.

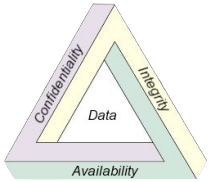
# Security

- "***The protection of resources from being accessed by an unauthorized person at a particular time.***"

"**Who** can **do what when**?"

# Authorized and Unauthorized

- Commonly partitioned using two properties of data
  - confidentiality
  - integrity
- Availability (e.g. Fault Tolerant)
- Data
  - sensitive information, secrecy, and privacy






# Access Control Models

- Mandatory Access Control (MAC)
  - Principle: Users are untrustworthy and must be controlled.
- Discretionary Access Control (DAC)
  - Principle: Users are responsible for their own data.
- Role-Based Access Control (RBAC)
  - Principle: least privilege.



# ACL v.s Capability

- ACL
  - Associate with object
  - Object got a list of who can do what with the object.
- Capability
  - Associate with subject
  - Think of capability as a token for key.
  - Granting a permission is passing a key to another person.

# Multilevel Security

- Within an organization
- MAC
- Bell Lapadula
- Biba



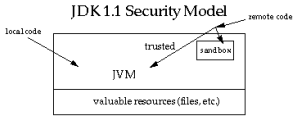

# How to Audit?

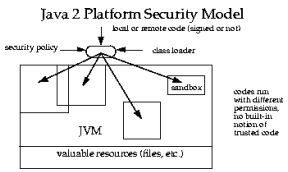
- Audit Trails
  - Physical trails
  - Log files
- Analysis Tools
  - Statistic
  - Data Mining

| S.No. | Table | Column Name | Type of Changes | Old Value | New Value | Updated By | Date Log |
|---|---|---|---|---|---|---|---|
| 1 | LEADPARTNER | LEADPARTNER NAME | INSERT | - | Testing Lead Partner | Wilson Sim | 02/05/2006 09:26:32am |
| 2 | LEADPARTNER | LEADPARTNER NAME | INSERT | - | scstester | STEVEN THAME | 04/05/2006 10:04:26am |
| 3 | LEADPARTNER | LEADPARTNER NAME | INSERT | - | Singapore Computer Systems | WILSON SIM | 05/05/2006 02:00:21pm |
| 4 | LEADPARTNER | LP_ID | INSERT | - | 291 | ADMIN | 07/04/2006 08:41:00am |
| 5 | LEADPARTNER | NAME | UPDATE | Test Triggers | Test Triggers 1 | ADMIN | 07/04/2006 08:45:05am |
| 6 | LEADPARTNER | NAME | UPDATE | Lokesh Co Ltd | Lokesh Co Ltd 1 | Wilson Sim | 07/04/2006 08:57:22am |
| 7 | LEADPARTNER | NAME | UPDATE | Lokesh Pandey155 | 345 | SCS | 07/04/2006 11:27:47am |
| 8 | LEADPARTNER | NAME | UPDATE | Lokesh Pandey155 | 345 | SCS | 07/04/2006 11:27:47am |
| 9 | LEADPARTNER | NAME | UPDATE | Lokesh Pandey155 | 345 | SCS | 07/04/2006 11:27:47am |
| 10 | LEADPARTNER | NAME | UPDATE | Lokesh Pandey155 | 345 | SCS | 07/04/2006 11:27:47am |
| 11 | LEADPARTNER | NAME | UPDATE | Lokesh Pandey155 | 345 | SCS | 07/04/2006 11:27:47am |

# How to minimize trust?

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



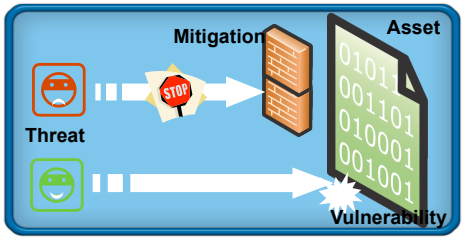



# Modern Encryption

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

# Threat Analysis

- Secure software starts with understanding the threats
- Threats are not vulnerabilities
- Threats live forever, they are the attacker's goal(s)








# A Threat Modeling Process