CN318
Computer Network Security

Week 2:- Fundamental Security Concept

By

Dr. Piya Techateerawat

Why we need Network Security?

- To protect company assets
- To gain a competitive advantage.
- To comply with regulatory requirements.
- To keep your job

Why we need Network Security?

- Survey 1999
  - $45 billion from theft of "proprietary information"
  - Average responding companies report 2.45 incidents with estimated cost of $500,000 per incident.
  - Financial fraud raise from 388,000 in 1998 to 1,400,000 in 1999

Computer Network Security

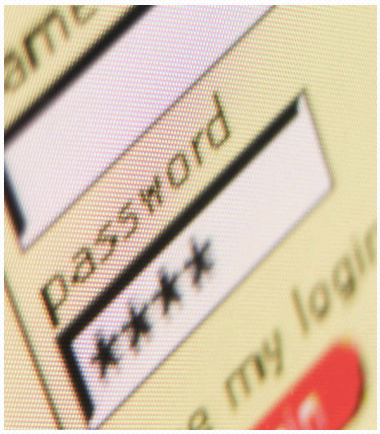
- **The Security Trinity**
  - Prevention
  - Detection
  - Response
- Security Models
- Basic Terminology
- Risk Assessment

Computer Network Security

- The Security Trinity
  - **Prevention**
  - Detection
  - Response
- Security Models
- Basic Terminology
- Risk Assessment

Prevention

- **Definition**
  - Impossible to protect all vulnerabilities.
  - Implement with sufficient strength
  - The most cost effective.
- **Example**
  - Password
  - Physical Protection

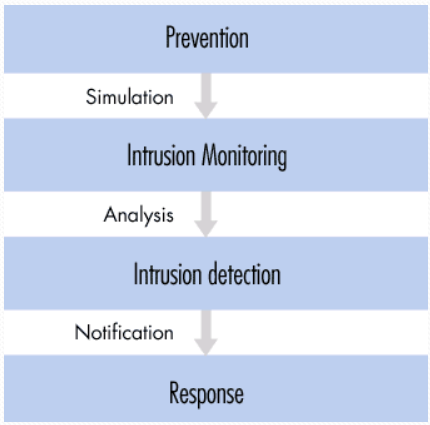


Computer Network Security

- The Security Trinity
  - Prevention
  - **Detection**
  - Response
- Security Models
- Basic Terminology
- Risk Assessment

Detection

- To detect potential security problems in the current system.
- E.g.
  - Intrusion Detection System

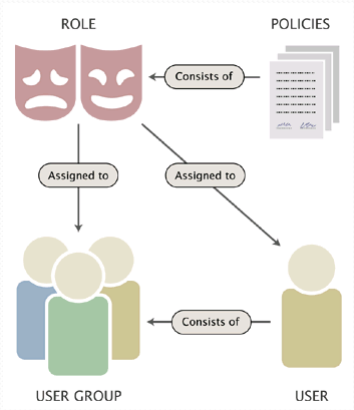


Computer Network Security

- The Security Trinity
  - Prevention
  - Detection
  - **Response**
- Security Models
- Basic Terminology
- Risk Assessment

Response

- Plan or Policy to act with vulnerabilities in the appropriate situation.



Computer Network Security

- The Security Trinity
  - Prevention
  - Detection
  - Response
- **Security Models**
- Basic Terminology
- Risk Assessment

Security Models

- **Security by Obscurity**
  - If no one knows the exist system, then it won't be a target.
- **Perimeter Defense**
  - As a border security protection e.g. firewall that protect intruder to break-in the internal system
- **The defense in depth**
  - Separated monitoring each systems and its defense.
  - The most difficult to implement and high cost.

Computer Network Security

- The Security Trinity
  - Prevention
  - Detection
  - Response
- Security Models
- **Basic Terminology**
- Risk Assessment

Basic Terminology

- **Threats:-** Anything that can disrupt the operation, function or availability of a network.
- **Vulnerabilities:-** weakness in design, configuration or implementation of a network system.(poor design, implementation, management)
  - Physical
  - Hardware and Software
  - Media
  - Transmission
  - Human

Basic Terminology

- Identification
- Authentication
- Authorization (Access Control)
- Availability
- Confidentiality
- Integrity
- Accountability

Computer Network Security

- The Security Trinity
  - Prevention
  - Detection
  - Response
- Security Models
- Basic Terminology
- **Risk Assessment**

Risk Assessment

- Identify and prioritizing assets
- Identifying vulnerabilities
- Identifying threats and their probabilities
- Identifying countermeasures
- Developing a cost benefit analysis
- Developing security policies and procedures

Risk Assessment

- What do you want to safeguard?
- Why do you want to safeguard it?
- What is its value?
- What are the threats?
- What are the risks?
- What are the consequence of its loss?
- What are the various scenarios?
- What will the loss of the information or system cost?

Case Study – Palin's Yahoo Mail

Palin is the governor of Alaska. She was named John McCain's vice-presidential running mate on Aug. 29.

Case Study – Palin's Yahoo Mail

- Hackers say they have gained access to U.S. vice presidential candidate Sarah Palin's Yahoo account and published some of its contents on the Wikileaks Web site.
- On Wednesday, Wikileaks published several screen shots of Yahoo e-mail messages, e-mail addresses of Palin family members and associates, and other data that hackers claim to have obtained from Palin's private Yahoo account.
- One e-mail message appears to be from Alaska Lieutenant Governor Sean Parnell, complaining to Palin about an interview by Alaska radio show host Dan Fagan. "Arghhh! He is so inconsistent and purposefully misleading," Palin apparently writes in response.

Case Study – Palin's Yahoo Mail

- A hacking group known as Anonymous gained access to Palin's Yahoo account late Tuesday night and sent the information to Wikileaks, which acts as an anonymous clearinghouse for leaked documents.
- "Governor Palin has come under criticism for using private e-mail accounts to conduct government business and in the process avoid transparency laws," Wikileaks wrote in a note accompanying the material. "The list of correspondence, together with the account name, appears to re-enforce the criticism."
- Late Wednesday, the McCain-Palin campaign confirmed the hack. "This is a shocking invasion of the Governor's privacy and a violation of law," the campaign said in a statement. "The matter has been turned over to the appropriate authorities and we hope that anyone in possession of these emails will destroy them."

Case Study – Palin's Yahoo Mail

- Palin may have been using several Yahoo addresses in order to keep e-mail from friends and family separate from her other mail, said Adam O'Donnell, director of emerging technologies with e-mail security vendor Cloudmark.
- Palin's e-mail practices had been discussed in the press in the days before the hack, after Alaska activist Andree McLeod had sought to obtain more than 1,000 e-mail messages that Palin had withheld following a public records request.
- Last week, the Washington Post reported that Palin routinely handled governor's business from the address gov.sarah@yahoo.com. However, that is not the account that Anonymous hacked. Screen shots of the Yahoo pages posted to Wikileaks show that they had access to a gov.palin@yahoo.com address.

Case Study – Palin's Yahoo Mail

- There are several ways that attackers could have gained access to this account, O'Donnell said. They could have simply guessed her password, or had enough of her personal information to trick Yahoo into resetting the password. A more sophisticated attacker might have somehow installed key-logging software on Palin's computer or obtained the information though a phishing attack, he said.
- Yahoo declined to comment on the matter, saying that it does not comment on specific user accounts for privacy reasons.
- Made up of a loosely knit group of volunteer hackers, Anonymous gained notoriety earlier this year for launching an online attack against the Church of Scientology's Web site.

Case Study – Palin's Yahoo Mail

- Discussion:-
  - What ?
  - Where ?
  - When ?
  - Why ?
  - How ?
  - Problem/Improvement?

Case Study – Palin's Yahoo Mail

After taking picture, photo shooter have to run away from guard.

Case Study – Palin's Yahoo Mail

20 millions CPU Power Server Farm @ Dream Work for Shrek 3

Reference

- http://networkinstruments.files.wordpress.com/2008/04/password_star.jpg
- http://www.windowsecurity.com/img/upl/ids_rys11049723546982.gif
- http://ez.no/var/doc/storage/images/ez_publish/technical_manual/3_8/images/concepts_and_basics/user_group_policy_role/30015-1-eng-GB/user_group_policy_role_doc.png @ 9 Oct 2008
- http://www.cyberciti.biz/tips/wp-content/uploads/2007/06/server-farm-dreamworks-animation-studio.png

Q & A