

Information Security Basics

Culled from Notes by Kazuo Sugihara

ICS426: Computer System Security

<http://www2.hawaii.edu/~sugihara/course/ics426f09/notes/w01.html>

1. What Is Computer Information Security?

Definition: Security of a Computer System

- A state of being free from
 1. unauthorized use of the system and its resources,
 2. misuse of the system and its resources, and
 3. disturbance of the system's operations
- The field of study about techniques for achieving and maintaining such a secure state

Approaches to Security

1. Prevention of Threats → Policies

- i. Attempt to design a system so that it's perfectly secure
For an open system like most of systems these days, this approach *alone* is too idealistic and hence not practical.

2. Exclusion of Unknown Entities → Identification and Authentication

- i. Attempt to distinguish well-known entities (with good faith) from suspicious entities that are possibly malicious
This tends to make a system too closed and restrictive.

3. Hiding Important Information → Cryptography

- i. Attempt to make critical information incomprehensible
Theoretically, except one-time pad, there is no encryption scheme perfectly secure.
- ii. “In [cryptography](#), the **one-time pad (OTP)** is a type of [encryption](#), which has been proven to be impossible to [crack](#) if used correctly. Each bit or character from the [plaintext](#) is encrypted by a [modular addition](#) with a bit or character from a secret random [key](#) (or *pad*) of the same length as the plaintext, resulting in a [ciphertext](#). If the key is truly [random](#), as large as or greater than the plaintext, never reused in whole or part, and kept [secret](#), the ciphertext will be impossible to decrypt or break without knowing the key. It has also been proven that any cipher with the perfect secrecy property must use keys with effectively the same requirements as OTP keys.^[1] However, practical problems have prevented one-time pads from being widely used.”

4. Detection of Potential Threats → Monitoring, Auditing, Detection, and Confinement

- i. Attempt to identify violation of security policies or possible trials of intrusion to a system

No *single* approach is sufficient for the security of the *entire* system.

→ Combine them in balance of their pros & cons

Aspects on Security

- Component Level
 - Hardware
 - Software
 - Human
- System Level
 - Integration
 - Consistency
- Organization Level

Possible Targets of Security Threats

- *Information*: Unauthorized Access to the Information Stored in the System
- *Control*: Executing Unauthorized Control of the System or Its Component(s)
- *Functionality / Performance / Availability*: Disabling or Degrading the functionality, Performance or Availability of the System

Possible Source(s) of Security Threats

- Inside the System
- Outside the System
- Interface to the System (including communication channels)

Classes of Security Threats

1. **Disclosure**
 - Snooping, Trojan Horses
2. **Deception and Social Engineering**
 - Modification, spoofing, repudiation of origin, denial of receipt
3. **Disruption**
 - Modification
4. **Usurpation -**
 - Wrongfully seizing and holding
 - Modification, spoofing, delay, denial of service

- **Snooping** : the unauthorized interception of information; an example is passive wiretapping, where the attacker monitors communications.
- **Modification**: an example is active wiretapping, where the attacker injects something into a communication or modifies parts of the communication. Modification is sometimes called alteration.
- **Spoofing**: delegation is basically authorized spoofing. The difference is that the ones to which authority is delegated does not impersonate the delegator; she simply asserts authority to act as an agent for the delegator. **Definition**: Use by an authorized individual of legitimate identification and authentication (I&A) data to impersonate a legitimate user.

- **Denial of service:** this may not be due to an attack, but due to limits of resources. However, the effect here is critical. If you define security in terms of what users need to access, the inability to access is a security problem regardless of whether the reason is intentional (an attack) or unintentional (not an attack).
- **Social engineering:** is the act of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques. "Social engineering" as an act of psychological manipulation was popularized by hacker-turned-consultant Kevin Mitnick. Spoofing is an example of social engineering.

2. Access Control

Access control is to control actions or operations applied to resources (such as devices and data) in a system so that the system stays in safe states. It includes authentication, authorization, and audit.

In the case studies below: Discuss the possible security threats which can occur and how to address them:

U.S. Says Personal Data on Millions of Veterans Stolen

Reuters, Monday, May 22, 2006 1:22 PM

WASHINGTON (Reuters) - Personal data on about 26.5 million U.S. military veterans was stolen from the residence of a Department of Veterans Affairs data analyst who improperly took the material home, Veterans Affairs Secretary Jim Nicholson said Monday. The data included names, Social Security numbers and dates of birth for the veterans, Nicholson said, but "there is no indication at this time" that the data had been used for identify theft.

Nicholson said the theft of the data took place this month, but declined to identify the employee or the location of the burglary. "The employee has been placed on administrative leave pending the outcome of the investigation. We have a full-scale investigation going on in this," Nicholson told reporters by telephone. He said the FBI, local law enforcement authorities and his department's inspector general's office were looking into the matter.

"They believe that this was a random burglary and not targeted at this data," Nicholson added, saying there had been a series of burglaries in the community where the employee lived.

Nicholson identified the employee only as a male career department worker, not a political appointee. He said the employee "took home a considerable amount of electronic data from the VA which he was not authorized to do. It was in violation of our rules and regulations and policies."

EXTORTION PLOT LEADS TO CREDIT CARD THEFT

In what may be the largest credit card heist on the Internet, an 18-year-old Russian cracker claims to have stolen thousands of credit card numbers from an online store and dispensed them to visitors of his Web site. Before it was taken offline early Sunday morning, the rogue site, a page of which has been captured here, had doled out more than 25,000 stolen card numbers. Also included with the numbers were expiration dates and cardholder names and addresses.

With the click of a button, visitors could launch a script that purportedly obtained a valid credit card "directly from the biggest online shop database," according to a message at the site. The cracker, who goes by the nickname Maxus, claimed in an email to InternetNews.com to have breached the security of CDuniverse.com, an online music store operated by eUniverse, Inc. of Wallingford, Conn. Maxus said he had defeated a popular credit card processing application called ICVerify, from CyberCash

(CYCH) and obtained a database containing more than 300,000 customer records from CDuniverse. One of the victims confirmed that he had shopped at the online music store over a year ago.

According to Wilson, he was contacted by his credit card company's fraud division last week after someone had attempted to make an authorized charge to his card. Maxus said that he decided to set up the site, titled Maxus Credit Cards Datapipe, and to give away the stolen customer data after officials at CDuniverse failed to pay him \$100,000 to keep quiet about the security hole. Maxus claims the company agreed to the payment last month, but subsequently balked at initiating a wire transfer to a secret bank account because it might be noticed by auditors. After a week passed with no further contact from the company, Maxus said he put up his site and announced its presence Dec. 25th on an Internet Relay Chat group devoted to stolen credit cards.

Soon after launching his site, Maxus said it became so popular with credit card thieves that he had to implement a cap to limit visitors to one stolen card at a time. Apprehending Maxus will not be easy, said Richard M. Smith, an online security expert in Brookline, Mass., who helped federal agents track down the author of the Melissa virus, David L. Smith. Maxus appears to move about online using stolen accounts and relays his email through other sites to conceal the originating Internet protocol address, said Smith. "I think he's pretty free and clear and it's near zero that they will catch him," Smith said. (InternetNews.com 9 Jan 2000, New York Times 10 Jan 2000)

UC Berkeley breach affects 160,000

May 8, 2009

Matt Krupnick of *Contra Costa Times* [reports](#) that hackers may have stolen personal information from a decade's worth of current and former UC Berkeley students. Those affected include about 3,400 Mills College students who used or were eligible for UC Berkeley medical services. health insurance. Henry K. Lee of *The San Francisco Chronicle* [adds](#) that the hackers are thought to be overseas.

According to a university spokesperson, the breach involved records at the school's health center that contained Social Security numbers, information, immunization history and the names of treating physicians. No treatment-related records were breached. The data may appear to have been stolen between Oct. 9, 2008 and April 9, 2009.

In a statement linked from its home page, UC Berkeley states:

The campus learned of the breach in April, immediately removed from service the exposed databases to prevent any further attacks, and alerted campus police and the FBI. In all, more than 160,000 individuals will be alerted, including those who had their Social Security numbers accessed and others who may be at risk for identity theft. E-mails were issued starting today, and letters should start arriving over the next week. These communications will also include guidance on steps these individuals should take to guard against potential identity theft. A hotline has been established to answer any questions from individuals who received notices.

The victims of this crime are current and former UC Berkeley students (as well as their parents and spouses, if linked to insurance coverage) who had UHS health care coverage or received services. The campus is also sending notification letters to approximately 3,400 Mills College students who received, or were eligible to receive, health care at UC Berkeley.

The data for UC Berkeley students, alumni and their parents date back to 1999. The information involving Mills College former and current students dates back to 2001.

References

1. [Bishop2004] Matt Bishop, [*Introduction to Computer Security*](#), Prentice Hall, 2004.
2. [Landwehr1981] Carl E. Landwehr, "[Formal models for computer security](#)," *ACM Computing Surveys*, vol. 13, no. 3, pp.247-278, 1981.