DENNIS GUNAWAN

IF470 COMPUTER SECURITY

05 ILLICIT DATA ACCESS

REVIEW: MALICIOUS CODE

- Threat
  - Malware – Virus, Trojan Horse, and Worm
- Technical Details
  - Malicious Code
- Vulnerability
  - Voluntary Introduction
  - Unlimited Privilege
  - Stealthy Behavior – Hard to Detect and Characterize
- Countermeasure
  - Hygiene
  - Detection Tools
  - Error Detecting and Error Correcting Codes
  - Memory Separation
  - Basic Security Principles

COURSE SUB LEARNING OUTCOMES (SUB-CLO)

- Sub-CLO 5
  - Students are able to relate illicit data access to real case in their daily life (C3)

OUTLINE

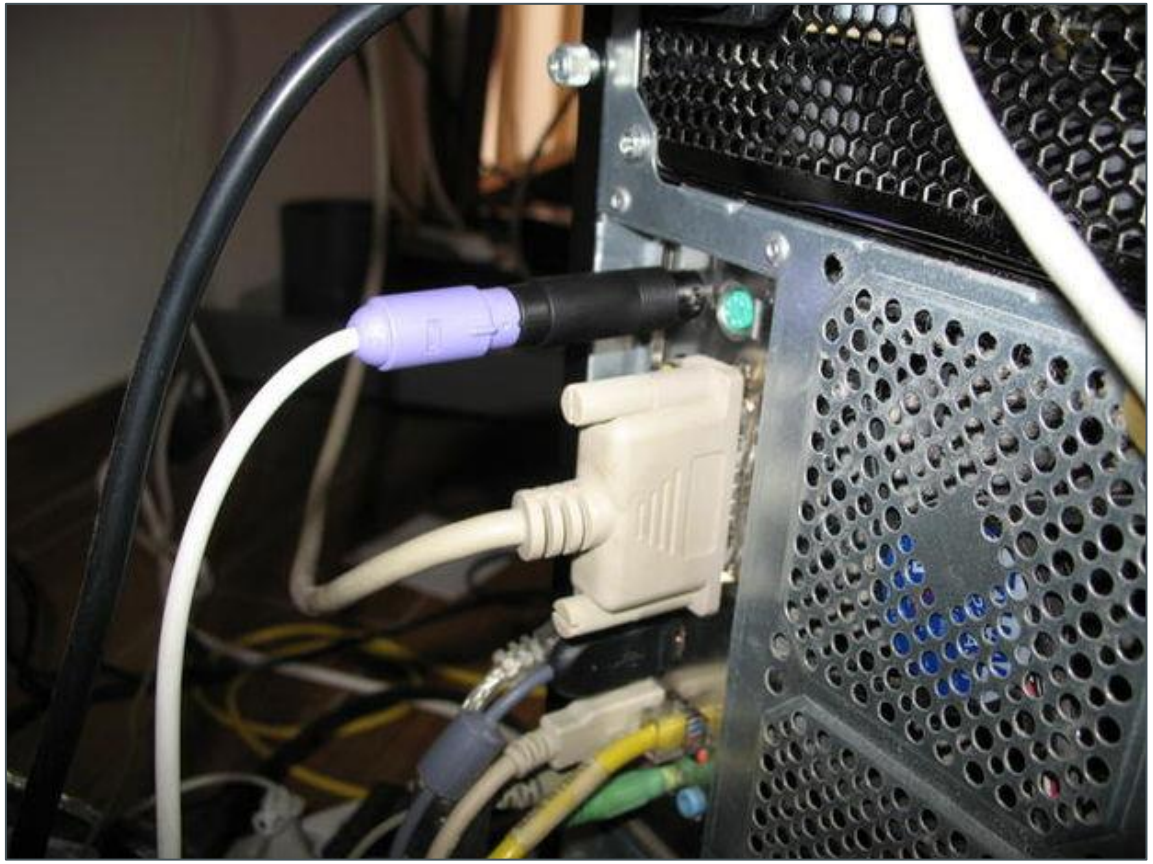
- Attack
  - Keylogging
- Threat
  - Illicit Data Access
- Harm
  - Data and Reputation
- Vulnerability
  - Physical Access
  - Misplaced Trust
  - Insiders
  - System Subversion
  - Weak Authentication
- Failed Countermeasure
  - Security through Obscurity
- Countermeasure
  - Physical Access Control
  - Strong Authentication
  - Trust / Least Privilege

KEYLOGGING

Silently records every key pressed on the keyboard into a file that can subsequently be transferred to another computer

- Hardware keylogger
- Software keylogger

HARDWARE KEYLOGGER



KEYLOGGING

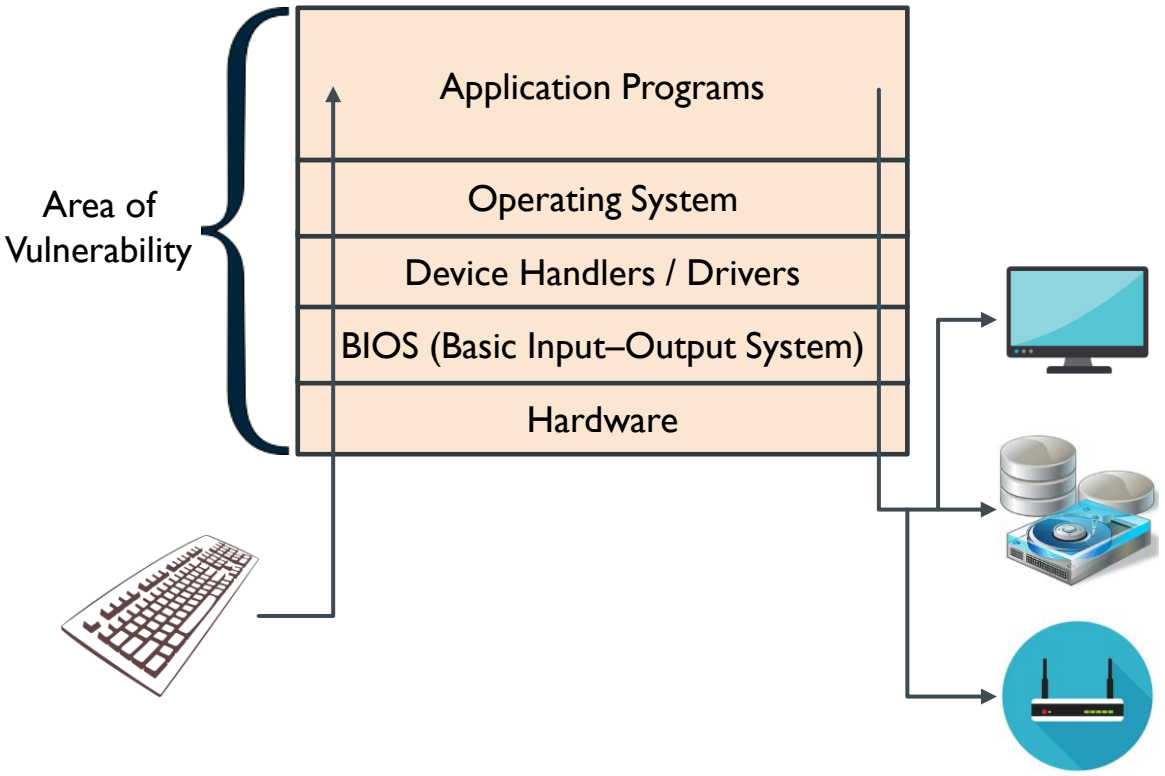
The threat is not simply that someone will install a keylogging device

–

Someone will obtain unauthorized access to data

KEYLOGGING

- There are many points of exposure between a user's fingers on a keyboard and the application program
- At any point, data can be copied or modified



KEYLOGGING

You may think of a computer as "safe",

in the sense that once you type something,

it is secure within the computer

- If anyone has had physical access to your computer, it may now contain added hardware that can act maliciously
- Even without physical access, malicious code planted in the system is similarly capable of intercepting data

KEYLOGGING

- Keystroke loggers are small and unobtrusive
- On a typical desktop configuration the keyboard connection is on the back, seldom inspected or touched
- It would be easy to see but not notice an additional component

KEYLOGGING

- An important aspect of this attack is stealth
  - Modifications made to internal hardware would be well hidden
    - Who looks inside a computer?
  - With so many attached devices, something else plugged into a USB port would not attract attention

KEYLOGGING

- Installing the key logger would have taken only a few seconds
  - Unplug the keyboard from the computer
  - Reconnect it and the logger to the chassis

- Thanks to plug-and-play hardware
  - The operating system would helpfully install the new device right away or when the machine was restarted

KEYLOGGING

- A physical attack does pose a high risk to the attacker
- A student caught in the faculty lounge needs a convincing explanation for being there
  - "I'm helping Mr. Roberts create some history slides"
  - "Ms. Ono asked me to check this computer she was having trouble with"
- A questionable act with a plausible explanation will often pass

KEYLOGGING

- The attacker is lazy
  - We cannot expect the attacker to take a hard route if an easier one is possible
- When analyzing security threats and vulnerabilities, do not overlook obvious or simple attacks

- Several ways students could break into a school's computer system
  - Late-night breaking and entering
  - Stealing the computer for off-site analysis over a weekend
  - Hiring a computer expert to find a weakness in the grade management program
- Why work so hard when all you have to do is plug one tiny device into a USB port?

HARM

- Confidentiality and integrity of all data accessible through the system
- Reputation

PHYSICAL ACCESS

If a bad guy has unrestricted physical access to your computer, it's not your computer anymore

- Someone with physical access could read or destroy data and plant malicious code
- Unrestricted physical access can allow more harm than just theft

MISPLACED TRUST

- Society requires a large measure of implicit trust to function but we remain on our guard
- We protect ourselves by considering potential misuses of that trust and preventing some when we can do so reasonably easily

- A motorist whose car breaks down may trust a stranger who offers to help, but the motorist watches the stranger for any signs of potential harm
- We may give our house key to a friend or neighbor but only after knowing that person long enough to have developed a sense of trust
- When taking a car in for service we leave the key with the mechanic, trusting that the car and mechanic will be there when we return
  - We may confer limited trust by leaving only the car's key, not keys to our house and office as well

MISPLACED TRUST

- Trust is a social quality
  - Somewhat different from the mechanical, technological, deterministic nature of computers

- A computer system includes not just hardware and software but also people that use, develop, maintain, and administer the other part of the system

SOCIAL ENGINEERING

Using social skills and personal interaction
to get someone to reveal security-relevant information
and perhaps even to do something
that permits an attack

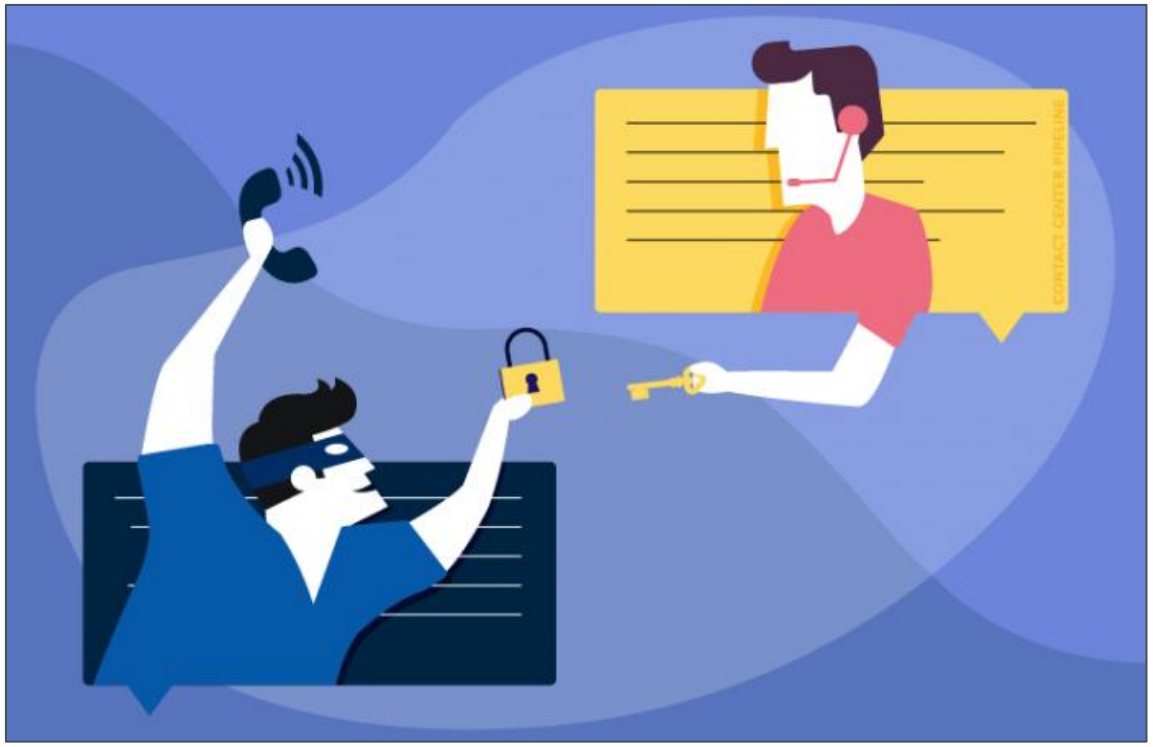
- People are by nature trusting and helpful
- Persuade the victim to be helpful

SOCIAL ENGINEERING

"Hello, this is John Davis from IT support. We need to test some connections on the internal network. Could you please run the command ipconfig/all on your workstation and read to me the addresses it displays?"

- The request sounds innocuous
- Unless you know John Davis and his job responsibilities well, you should suspect the caller could be an attacker gathering information on the inside architecture

SOCIAL ENGINEERING



- The attacker often impersonates someone inside the organization who is in a bind
  - "My laptop has just been stolen and I need to change the password I had stored on it"
  - "I have to get out a very important report quickly and I can't get access to the following thing"

SOCIAL ENGINEERING

- The attacker impersonates someone in a high position
  - The division vice president
  - The head of IT security
- Their names can sometimes be found on a public web site, in a network registration with the Internet registry, or in publicity and articles
- The attack is often directed at someone low enough to be intimidated or impressed by the high-level person

SOCIAL ENGINEERING

- A direct phone call and expressions of great urgency can override any natural instinct to check out the story
- The victim will think nothing is wrong and not report the incident
- An attacker has little to lose in trying a social engineering attack
  - At worst it will raise awareness of a possible target

PRESUMED INNOCENCE

- Maintenance worker
  - Escorted while performing work
  - Without the escort, we do not want to be discourteous
    - We tend not to ask a stranger why he is here, who he works for, or how to verify his identity

- Someone carrying cumbersome boxes follows us to a locked door
  - Good manners incline us to be helpful
  - We may politely open and hold the door

PRESUMED INNOCENCE

- Physical access is especially vulnerable to this problem because of the face-to-face nature of the contact
- We are more likely to challenge a faceless individual at the other end of a telephone call or email message than someone in person

INSIDERS

Perimeter Security

Security engineers often envision
a system's security as a strong defensive wall
surrounding the sensitive system and data inside

- A perimeter defense divides the world into
  - Outsiders
    Those whose access is blocked or controlled by the perimeter security mechanisms
  - Insiders
    Those who necessarily bypass or are incorporated within the perimeter defense

INSIDERS

A simple banking system that uses Automated Teller Machines (ATMs)

- Outsiders
  - Ordinary users
    - Withdraw funds
    - Make deposits
    - Transfer money
  - Their actions are strictly limited to certain accounts to which access is carefully controlled
- Insiders
  - Bank employees
    - Load cash into the ATM
    - Retrieve deposits
    - Repair the machinery
  - These insiders require greater privileges than ordinary users in order to accomplish their work

INSIDERS

- Some insiders have the potential to cause great harm
  - The maintenance engineer could take all the money instead of loading it into the ATM
  - A teller could move thousands of dollars from one customer account to another
- Several factors prevent these threats
  - Insiders hold positions of trust
  - The bank has layers of internal controls
  - Principles of separation of duty and least privilege
    - The actions of any one insider are limited

SYSTEM SUBVERSION

- Data are vulnerable everywhere from the user's fingers on the keyboard through hardware and software up to the application

- What are some other ways of extracting sensitive data?
  - Sense the electromagnetic waves generated as different keys are pressed
  - Scour memory while a program is running, to find sensitive data items that can be copied
  - Look for data in deleted files

- A dedicated adversary will explore many possible points of weakness to find one that is feasible and effective to attack

WEAK AUTHENTICATION

- A simple password mechanism produces a false positive for anyone who learns the password
  - By guessing, recording, deducing, or some other means
- The U.S. Defense Department changes access codes to some very sensitive resources at least every 24 hours
  - That frequency significantly reduces the degree of harm that can come from a guessed or stolen authenticator

WEAK AUTHENTICATION

When was the last time you changed your password?

SECURITY THROUGH OBSCURITY

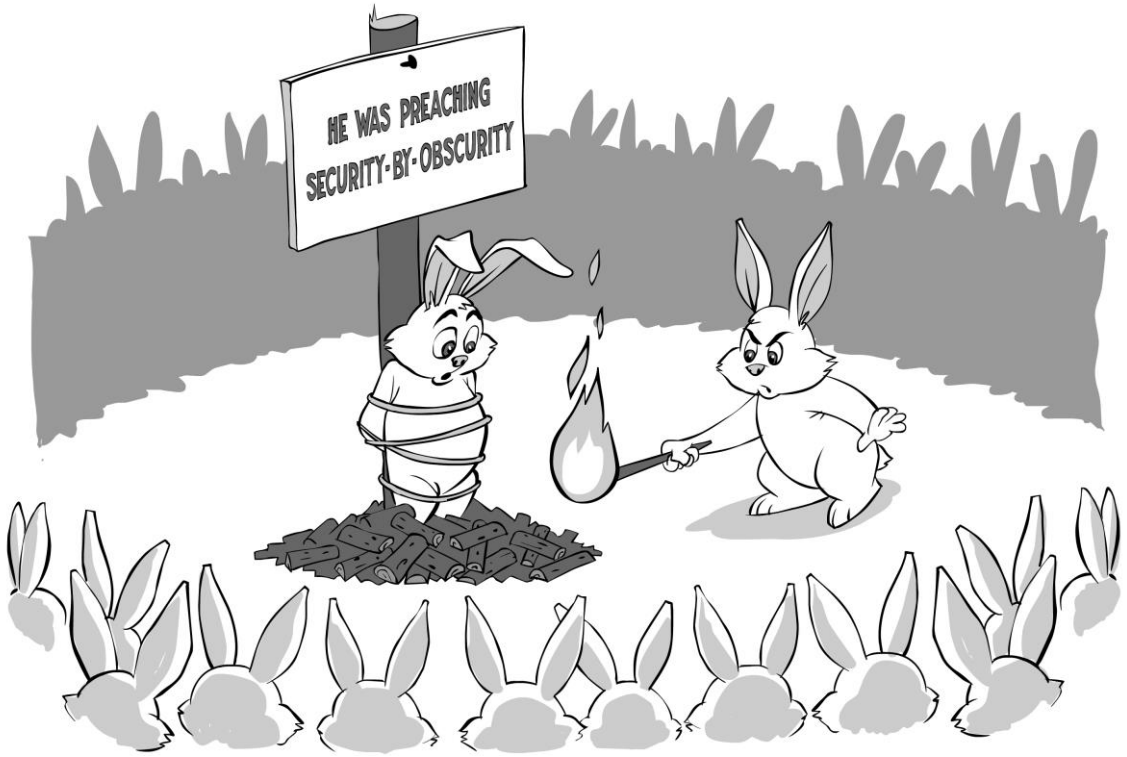
- Assuming the attacker will not find a vulnerability
- Belief that a system can be secure as long as nobody outside its implementation group is told anything about its internal mechanisms

The system must not depend on secrecy,

and security should not suffer

if the system falls into enemy hands

SECURITY THROUGH OBSCURITY



- Security through obscurity is a faulty countermeasure
- It assumes the attacker will always take the hard approach and never the easy one

PHYSICAL ACCESS CONTROL

Preventing Access

- For some devices, protection is more important than detection
  - Keep people away from the equipment
  - Keep someone from reading or changing certain systems or information

- Access-control devices are needed both to prevent access by unauthorized individuals and to record access by those authorized
  - Attackers can be either insiders or outsiders

- A record of accesses can help identify who committed an act after the fact

PHYSICAL ACCESS CONTROL

Guard

- Must be on duty continuously
  - 24-hour operation? Vacation? Illness?
- Must personally recognize someone or recognize an access token
  - People can lose or forget badges
  - Terminated employees and forged badges
- There is no way to know who (employee or visitor) has had access in case a problem is discovered
  - Unless the guard records the name of everyone who has entered a facility

PHYSICAL ACCESS CONTROL

Lock

- Easier, cheaper, and simpler to manage than a guard
- No record of who has had access
- Keys are lost or duplicated
- What if one's hands are filled with hardware or other things?
- Some people prop open locked doors

PHYSICAL ACCESS CONTROL

Cards with radio transmitters / Magnetic stripe cards / Smart cards with chips

- Easy for the computer to capture identity information
  - Who entered and left the facility, when, and by which routes
- Some of these devices operate by proximity
- Easy to invalidate an access authority when someone quits or reports the access token lost or stolen

PHYSICAL ACCESS CONTROL

Piggybacking

A person walks through the door that someone else has just unlocked

PHYSICAL ACCESS CONTROL

- A limited-access computer room makes it harder for an attacker to tamper without being noticed
- Sometimes just making it harder or riskier for the attacker is enough to discourage the attack

PHYSICAL ACCESS CONTROL

Detecting Access

- For some devices, it may be enough to detect that an attempt has been made to access, modify, or steal hardware or software
  - Chaining down a disk makes it unusable
  - Instead, we try to detect when someone tries to leave a protected area with the disk or other protected object

- A locking panel over the USB port area to prevent unauthorized access

- Tamper-evident screws and seals can show if a computer has been opened (for example, to install hardware)

PHYSICAL ACCESS CONTROL

- Physical access controls are most appropriate where one control can protect many high value resources
  - A single guard or lock protects a roomful of machines against theft
- Sometimes, physical access controls are too coarse
  - Someone is either barred from access to a room or can do anything to anything in the room

STRONG AUTHENTICATION

- Keylogging can cause compromise of any password, regardless of its length or complexity
- Not knowing of a compromise, the real user does not think there is any reason to change
- Another limitation of passwords: static nature
- A password does not distinguish who enters it
- The way to counter this limitation of passwords is to design passwords that change

ONE-TIME PASSWORDS

- A one-time password changes every time it is used
- Instead of assigning a static word to a user, the system assigns a series of passwords, sometimes called dynamic passwords

How It Works

- The user and system both have access to identical lists of passwords
  - Humans have trouble maintaining these password lists
- Human-generated passwords and machine-generated ones

ONE-TIME PASSWORDS

- Example of a user-computable authentication function
  - System date and time
  - Assign the letters A, B, …, J to the digits 0 to 9
- A date and time like 24/05/2010 14:20 could produce the password CEAFCABABECA
  - For the entire year 2010 all passwords will be of the form xxxxCABAxxxx
  - For the month of May they will all be of the form xxAFCABAxxxx

- Sort of easy to compute
- Someone who intercepted several passwords in a row, especially on different days, might be able to deduce the pattern

ONE-TIME PASSWORDS

- Dilemma
  - If they are easy for the user to generate, they may also be easy to guess
  - If they are complicated enough to preclude deduction, they may also be hard for a human to generate mentally

- Intercepted password is useless since it cannot be reused
- Limited by the complexity of algorithms people can be expected to remember

PASSWORD-GENERATING TOKEN

- Each user is issued a different device that generates a different random number sequence that is programmed into the device when it is manufactured
- Synchronous token
  - Related to time
  - The device displays a random number, generating a new number every 30 or 60 seconds
- There is a small window of vulnerability during which an eavesdropper can reuse an intercepted password

CHALLENGE-RESPONSE TOKEN

- Each user is assigned a different challenge function to compute
- The kinds of mathematical functions used are limited only by the ability of the user to compute the response quickly and easily
  - Many users cannot perform simple arithmetic in their heads

- $f(x) = x + 1$
- $f(x) = 3x^2 - 9x + 2$
- $f(x) = px$ (x^{th} prime number)
- $f(x) = d \times h$ (date x hour of the current time)
- $f(a_1a_2a_3a_4a_5a_6) = a_3a_1a_1a_4$

RESPONSE-GENERATING TOKEN

- The user enters the challenge number, and the device computes and displays the response for the user to type in order to log in

- Asynchronous token generator
  - Unrelated to time
  - The response to the challenge 12345 will always be 97531
    - Assuming that is the result of the function for that particular token
    - A new challenge for each use

- Eliminates the small window of vulnerability in which a user could reuse a time-sensitive authenticator

CONTINUOUS AUTHENTICATION

- 2 approaches
  - Authentication can be renewed
    - Repeated authentication is unpopular with users
    - Widely used for machine-to-machine connections
  - A connection between parties can be protected to thwart interception
    - Encryption mathematically scrambles a communication so that only the intended sender and receiver can productively unscramble it

- Establishing authentication once is not always sufficient in an electronic interaction
  - A moment after you establish confidence, the other side can change
- These 2 approaches significantly reduce, but do not eliminate, the question of whether an authenticated party is still the same party

PASSWORD CHANGE FREQUENCY

- Usability suffers from too frequent password changes

- Forced to change a password every day or week
  - Forget
  - Write passwords on a note stuck to the computer screen
  - Choose weak, easily guessed passwords

TRUST / LEAST PRIVILEGE

- We are careful about who we trust with what

- Maintain an audit log
  - A running list of actions performed
  - A list of the changes made would let the officials quickly correct false values and know that all other values were intact
  - Audit logs are a good way to monitor who does or does not need what privileges

- Granularity
  - The amount of detail in information recorded
  - Finding the proper balance between too much and too little is challenging

REFERENCES

- Pfleeger, Charles P. and Shari Lawrence Pfleeger (2012), *Analyzing Computer Security*, 1st Edition, Prentice Hall.

NEXT WEEK: PHYSICAL DATA LOSS

- Threat
  - Loss of Data
  - Disaster
- Vulnerability
  - Physical Access
  - Unprotected Availability of Data
  - Unprotected Confidentiality of Data
- Countermeasure
  - Policy
  - Physical Security
  - Data Redundancy (Backup)
  - Encryption

AS THE WORLD IS INCREASINGLY INTERCONNECTED, EVERYONE SHARES THE RESPONSIBILITY OF SECURING CYBERSPACE

Vision

To become an **outstanding** undergraduate Computer Science program that produces **international-minded** graduates who are **competent** in software engineering and have **entrepreneurial spirit** and **noble character**.

INFORMATIKA
UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA

Mission

1. To conduct studies with the best technology and curriculum, supported by professional lecturer
2. To conduct research in Informatics to promote science and technology
3. To deliver science-and-technology-based society services to implement science and technology