DENNIS GUNAWAN


# IF470 COMPUTER SECURITY

## 02 USER AUTHENTICATION

# REVIEW: INTRODUCTION TO COMPUTER SECURITY

- How Dependent Are We on Computers?
- What Is Computer Security?
- Threats
- Harm
- Vulnerabilities
- Controls

# COURSE SUB LEARNING OUTCOMES (SUB-CLO)

- Sub-CLO 2
  - Students are able to relate authentication to its implementation in their daily life (C3)

# OUTLINE

- Attack
  - Impersonation / Failed Authentication
- Vulnerability
  - Faulty or Incomplete Authentication
- Countermeasure
  - Strong Authentication

# INTRODUCTION

- Computers have replaced many face-to-face interactions with electronic ones
  - A computer system does not have the cues we do with face-to-face communication that let us recognize our friends
  - Instead computers depend on data to recognize others

- The basis of computer security is controlled access
  - **Someone** is authorized to take **some action** on **something**
  - For access control to work, we need to be sure who the "someone" is
  - If we mistakenly confirm identification of that someone, access control is ineffective

# Impersonation

A system cannot distinguish a real user from an imposter

# FAILED AUTHENTICATION

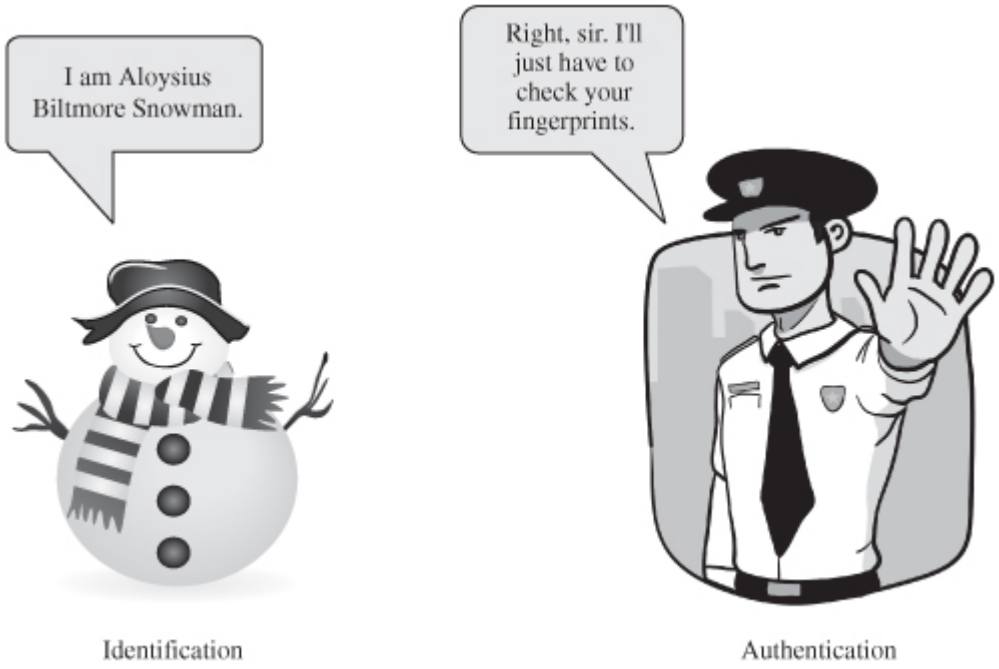
- Determining who a person really is consists of two separate steps

**IDENTIFICATION**

The act of asserting who a person is

**AUTHENTICATION**

The act of proving that asserted identity



# IDENTIFICATION VERSUS AUTHENTICATION

- If you send email to someone, you implicitly send along your email account ID so the other person can reply to you
- Your bank account number is printed on checks you write
- Your debit card account number is shown on your card

- Identities are often well known, public, not protected, predictable, and guessable
- If someone's identity is public, anyone can claim to be that person

# IDENTIFICATION VERSUS AUTHENTICATION

- Authentication should be reliable
- Although identifiers may be widely known or easily determined, authentication should be private
- If the authentication process is not strong enough, it will not be secure

# FAULTY OR INCOMPLETE AUTHENTICATION

## Example

- 2 authentication mechanisms used in the email protocol
  - The password that protects the email account
  - The system's function for replacing a supposedly forgotten password
- Weak security questions
- Elementary tools available to any attacker
  - Public knowledge about a person
  - A little deduction

# FAULTY OR INCOMPLETE AUTHENTICATION

- Password protection seems to offer a relatively secure system for confirming identity-related information, but human practice sometimes degrades its quality

## REMEMBER

How much information about us is known

–

sometimes because we reveal it ourselves

# PASSWORD USE

Even though they are widely used, passwords suffer from some difficulties of use

- Loss
  - What if the user loses the password?
  - The operators or system administrators cannot determine what password a user had chosen previously
- Use
  - Supplying a password for each access to an object can be inconvenient and time consuming
- Disclosure
  - If a user discloses a password to an unauthorized individual, the object becomes immediately accessible
- Revocation
  - To revoke one user's access right to an object, someone must change the password
    - The user must inform any other legitimate users of the new password because their old password will fail

# ATTACKING AND PROTECTING PASSWORDS

How secure are passwords themselves?

# ATTACKING AND PROTECTING PASSWORDS

Passwords are somewhat limited as protection devices because of the relatively small number of bits of information they contain

# ATTACKING AND PROTECTING PASSWORDS

- No password
- The same as the user ID
- Is, or is derived from, the user's name
- Common word list (password, secret, private) plus common names and patterns (qwerty, aaaaaa)
- Contained in a short college dictionary
- Contained in a complete English word list
- Contained in common non-English language dictionaries
- Contained in a short college dictionary with capitalizations (PaSsWorD) or substitutions (digit 0 for letter O)
- Contained in a complete English dictionary with capitalizations or substitutions
- Contained in common non-English dictionaries with capitalization or substitutions
- Obtained by brute force, trying all possible combinations of lowercase alphabetic characters
- Obtained by brute force, trying all possible combinations from the full character set

- 12 steps an attacker might try in order to determine a password
  - These steps are in increasing degree of difficulty (number of guesses)
  - They indicate the amount of work to which the attacker must go in order to derive a password
  - Always succeed?

# DICTIONARY ATTACKS

- Several network sites post dictionaries of phrases, science fiction characters, places, mythological names, Chinese words, Yiddish words, and other specialized lists
- All these lists are posted to help site administrators identify users who have chosen weak passwords
  - The same dictionaries can also be used by attackers of sites that do not have such attentive administrators

# PASSWORDS LIKELY FOR A USER

- People typically choose personal passwords, such as the name of a spouse, child, brother or sister, pet, street name, or something memorable or familiar
  - A list of only a few hundred possibilities at most
  - Takes under a second
- People find something in the password process that is difficult or unpleasant
  - People are unable to choose good passwords, perhaps because of the pressure of the situation
  - They fear they will forget solid passwords

# PROBABLE PASSWORDS

Think of a word.

# PROBABLE PASSWORDS

Is the word you thought of long?

Is it uncommon?

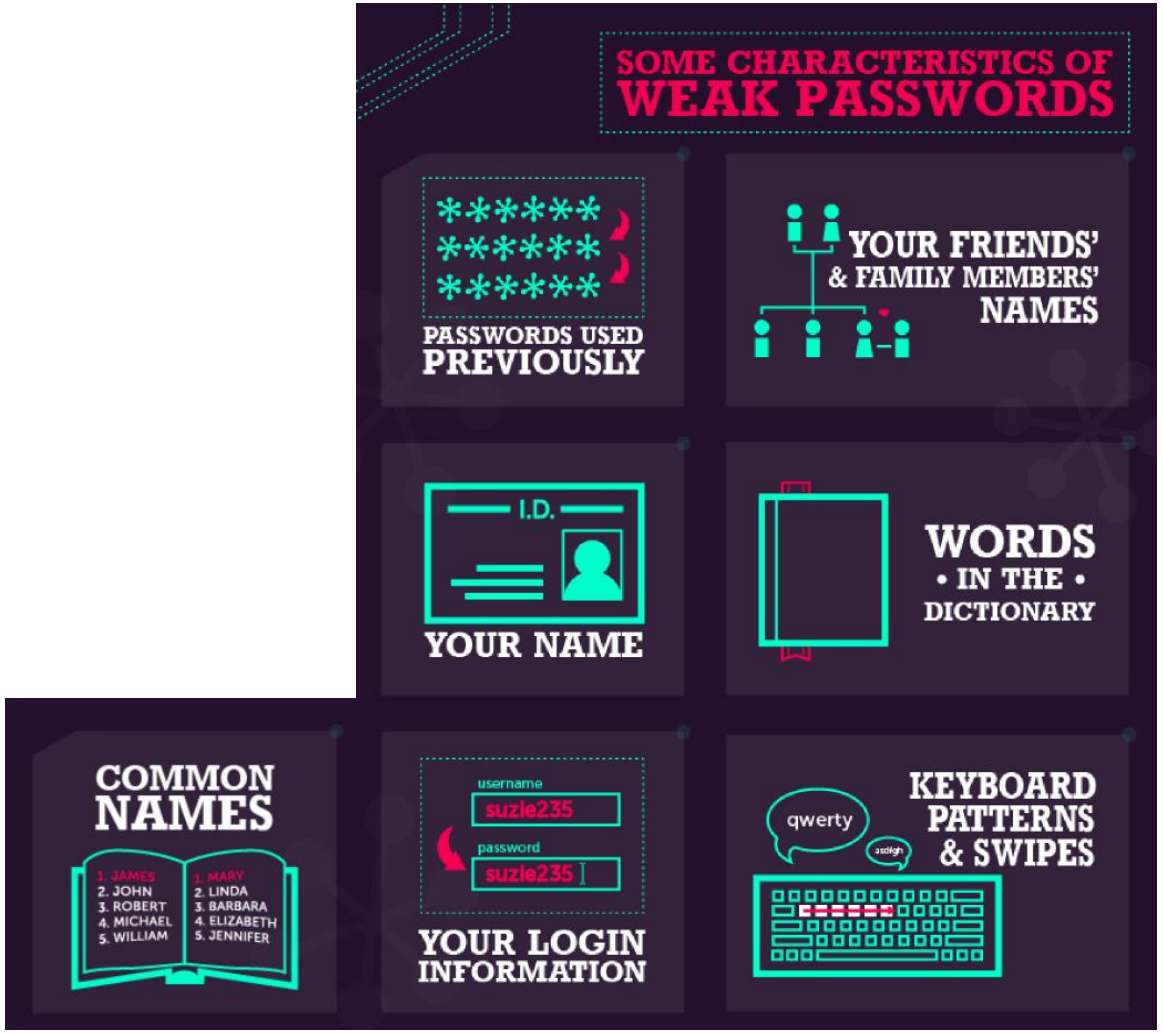
Is it hard to spell or to pronounce?

# PROBABLE PASSWORDS

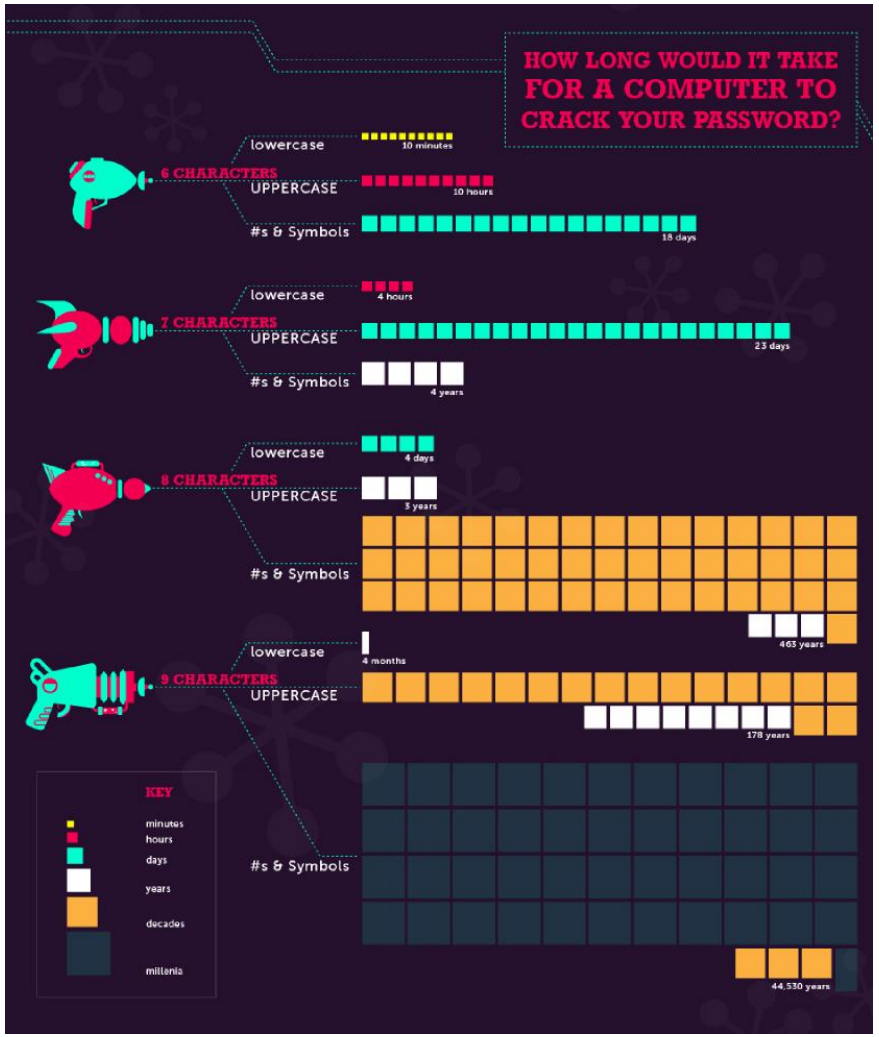
The answer to all 3 of these questions is probably

NO

# PROBABLE PASSWORDS




# PROBABLE PASSWORDS

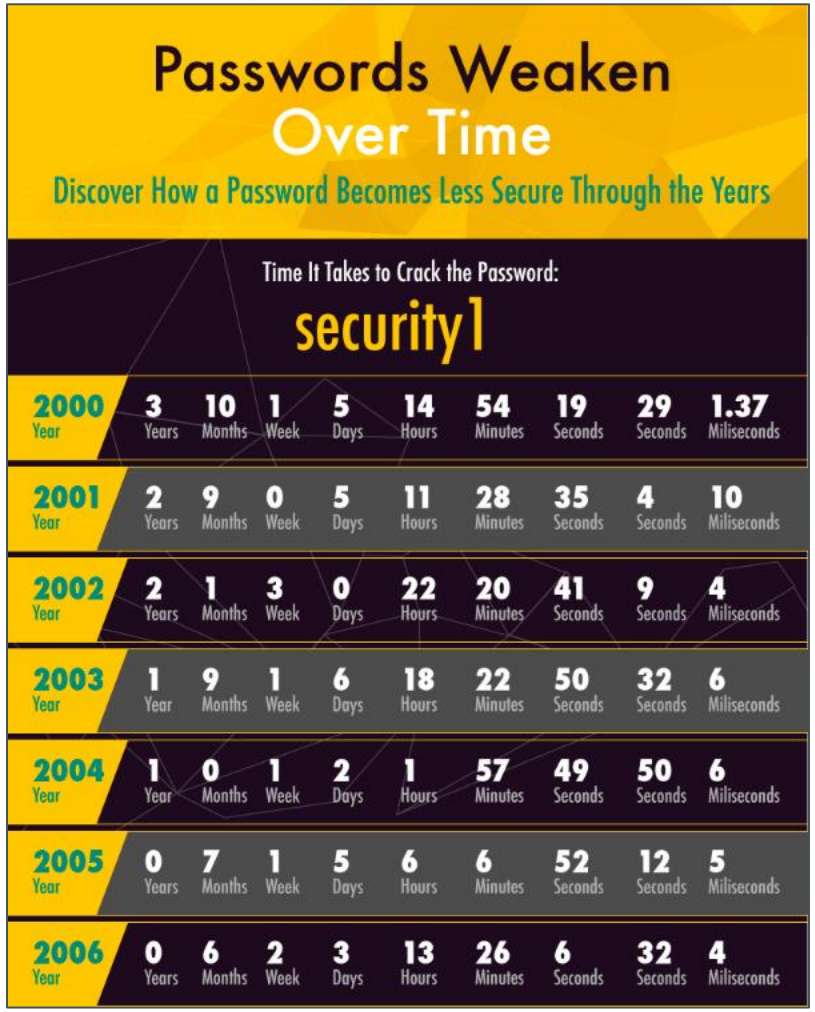



# EXHAUSTIVE ATTACK

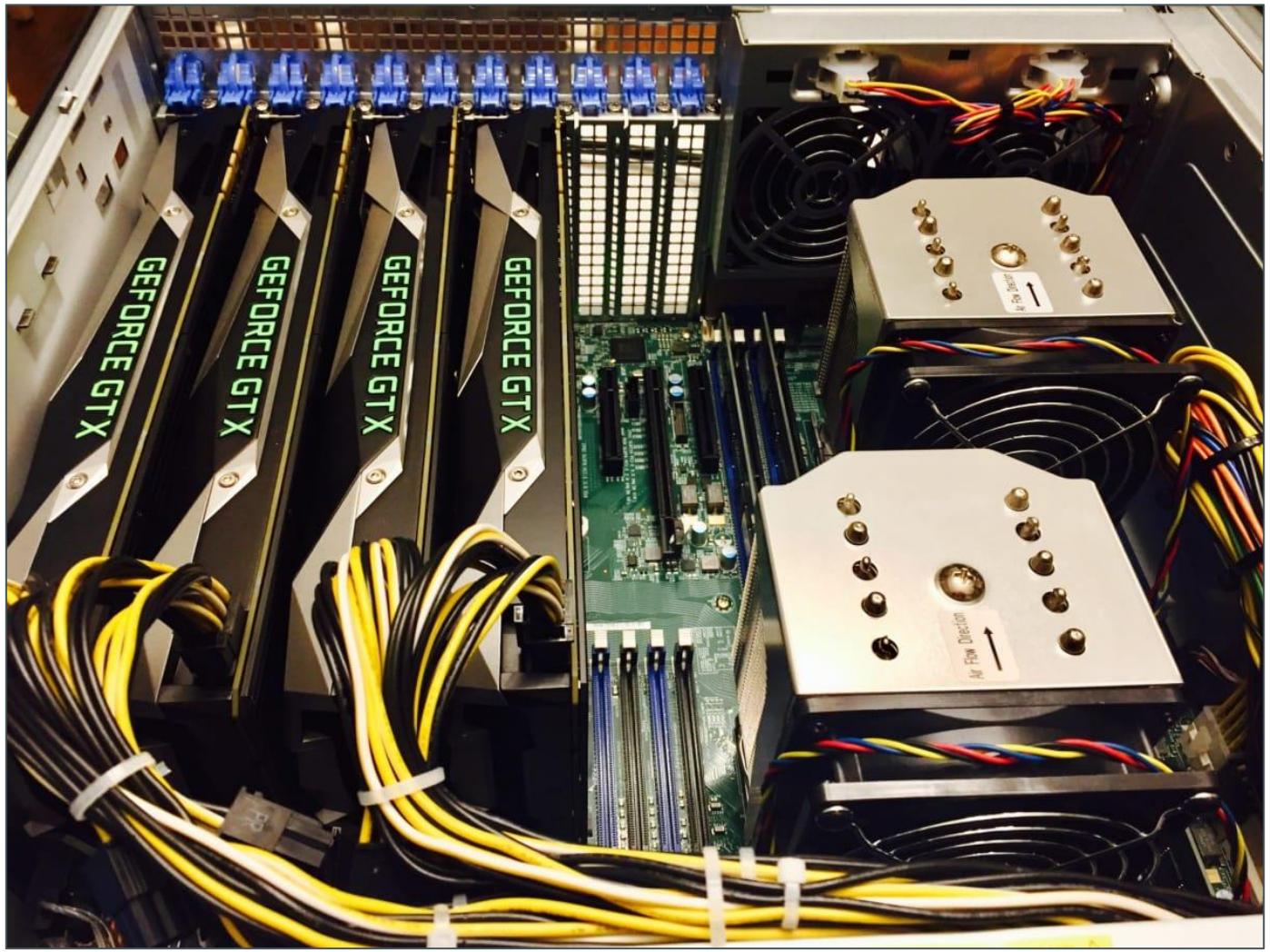
## Brute Force

The attacker tries all possible passwords, usually in some automated fashion

# PASSWORD STRENGTH OVER TIME



# PASSWORD CRACKING RIG: CRACKING ON A "BUDGET"



# PASSWORD CRACKING RIG: CRACKING ON A "BUDGET"

## THE POWER OF GEFORCE GTX 1050

| | GeForce GTX 1050 Ti | GeForce GTX 1050 (3GB) | GeForce GTX 1050 (2GB) |
|---|---|---|---|
| GPU Architecture | **Pascal** | **Pascal** | **Pascal** |
| NVIDIA CUDA® Cores | **768** | **768** | **640** |
| Frame Buffer | **4 GB GDDR5** | **3 GB GDDR5** | **2 GB GDDR5** |
| Memory Speed | **7 Gbps** | **7 Gbps** | **7 Gbps** |
| Boost Clock | **1392 MHz** | **1518 MHz** | **1455 MHz** |

## GEFORCE GTX 1080 Ti

### GPU Engine Specs:

| | |
|---|---|
| NVIDIA CUDA® Cores | **3584** |
| Boost Clock (MHz) | **1582** |

### Memory Specs:

| | |
|---|---|
| Memory Speed | **11 Gbps** |
| Standard Memory Config | **11 GB GDDR5X** |
| Memory Interface Width | **352-bit** |
| Memory Bandwidth (GB/sec) | **484** |

# PASSWORD CRACKING RIG: CRACKING ON A "BUDGET"


## PARTS & COST LIST

**1 x SuperMicro SYS-7048GR-TR 4U Server with X10DRG-Q Motherboard** = $1,989.99 (NewEgg)

**2 x Intel Xeon E5-2620 v3 2.4 GHz LGA 2011-3 85W** = $469.98 (Ebay)

**4 x Nvidia GTX 1070 Founders Edition** = $1,737.14 (Jet.com)

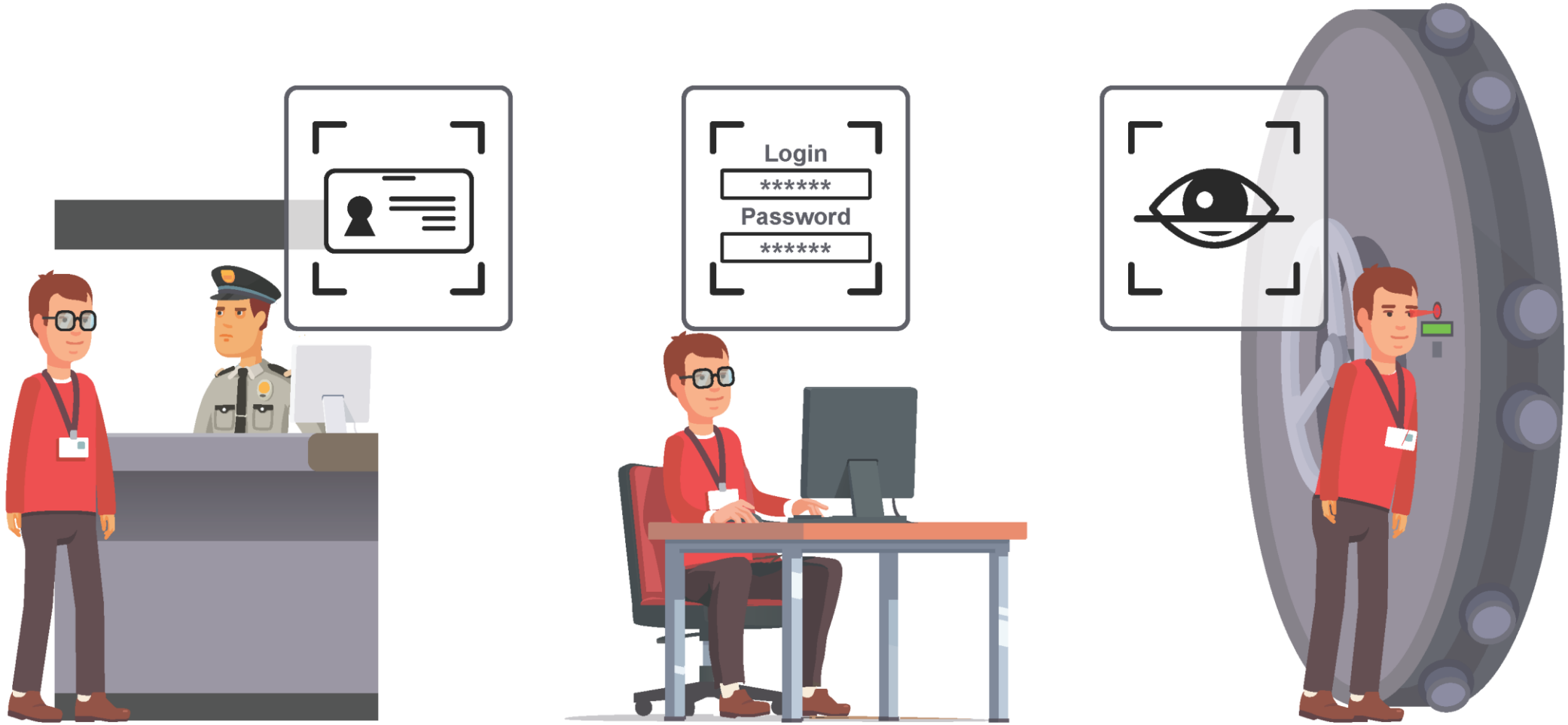
**2 x Samsung 850 Pro 512GB SATA3 SSD** = $412.24 (Jet.com)

**4 x Kingston Server ValueRAM DDR4 2133MHz 16GB** = $391.96 (NewEgg)

**TOTAL** = $5001.31

**costs include shipping & handling

# STRONG AUTHENTICATION



# STRONG AUTHENTICATION

## Something the user knows

- Passwords
- PIN numbers
- Passphrases
- Secret handshake
- Mother's maiden name

## Something the user is

- Fingerprints
- Hand geometry (shape and size of fingers)
- Retina and iris (parts of the eye)
- Voice
- Handwriting
- Blood vessels in the finger or hand
- Facial features, such as nose shape
- Keystroke dynamics

## Something the user has

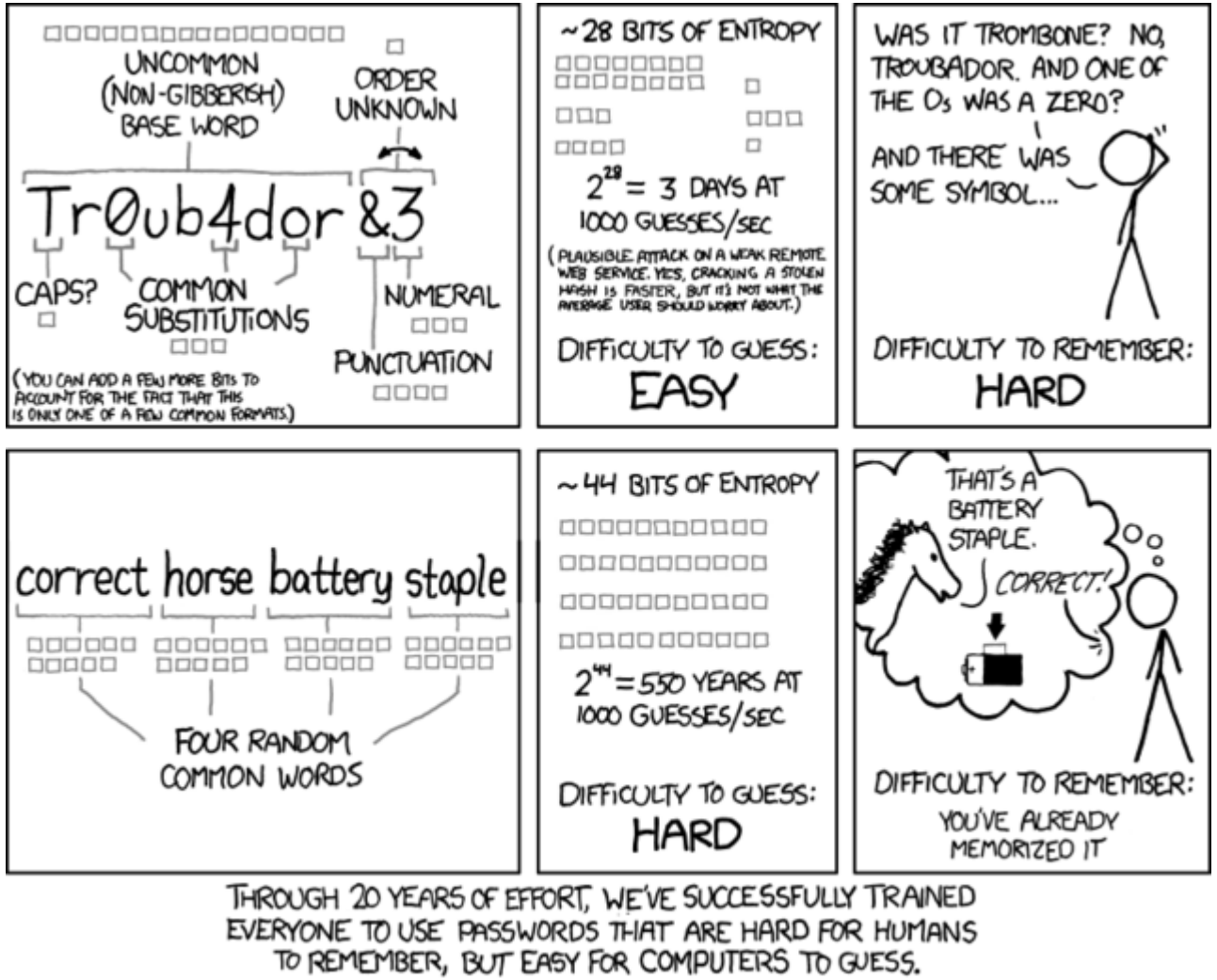
- Identity badges
- Physical keys
- Driver's license
- Uniform

# KNOWLEDGE: SOMETHING YOU KNOW

- Chosen carefully, passwords can be strong authenticators

- If we do use passwords, we can improve their security by a few simple practices
  - Use character other than just a-z
  - Choose long passwords
  - Avoid actual names or words
  - Choose an unlikely password
  - Change the password regularly
  - Don't write it down if physical security is a serious risk
  - Don't tell anyone else (vs social engineering)

# KNOWLEDGE: SOMETHING YOU KNOW




- 2Brn2Bti? (to be or not to be, that is the question)
- PayTaxesApril5th
- UcnB2s (you cannot be too secure)
- The first letters of words from a song
- A few letters from different words of a private phrase
- Something involving a memorable basketball score

# KNOWLEDGE: SOMETHING YOU KNOW

- Security questions could be improved by choosing something the real user knows but an imposter would be unlikely to know
  - Email account
    - From what email address you received frequent messages
    - Whether you tended to send 1-10, 10-50, 50-100, or 100+ messages per day
    - Whether your account was established before 2006, in 2006, in 2007, or in 2008
    - When you last logged in
    - When you had a gap of 7 or more days without accessing your account
  - Another type of account would have asked different kinds of questions, instead of "mother's maiden name" that for a while seemed as if it were going to become the universal authenticator

# KNOWLEDGE: SOMETHING YOU KNOW


# KNOWLEDGE: SOMETHING YOU KNOW

# BIOMETRICS: SOMETHING YOU ARE

## Biometrics

Biological authenticators, based on some physical characteristic of the human body

- Advantages
  - Cannot be lost, stolen, forgotten, lent, and is always available, always at hand
- Several problems
  - Intrusive
  - Costly
  - Single point of failure
  - Variation reduces accuracy
  - Speed limits accuracy
  - False readings
  - Forgeries are possible

# BIOMETRICS: SOMETHING YOU ARE

| | Is the Person Claimed | Is Not the Person Claimed |
|---|---|---|
| **Test Is Positive (There is a match)** | True Positive | False Positive |
| **Test Is Negative (There is no match)** | False Negative | True Negative |

## False Positive or False Accept

- A reading that is accepted when it should be rejected

## False Negative or False Reject

- A reading that is rejected when it should be accepted

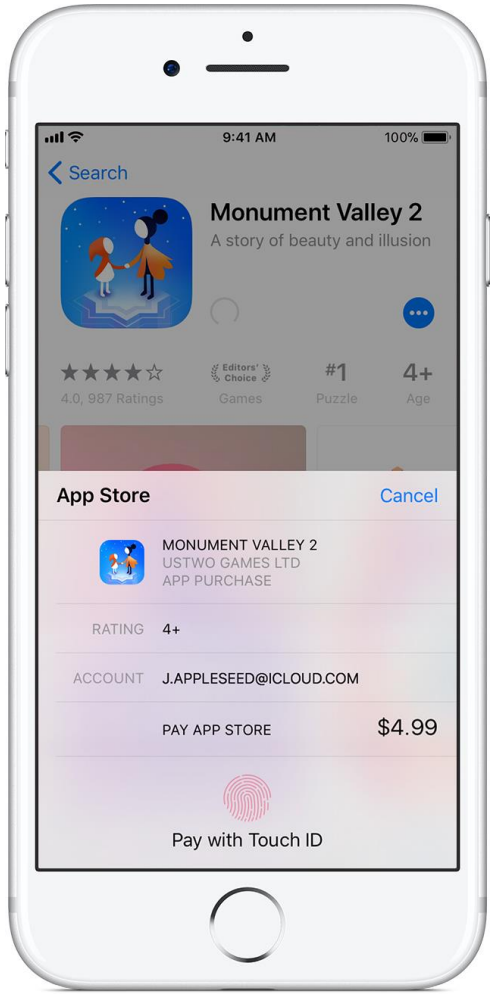
- Often, reducing a false positive rate increases false negatives, and vice versa
- The consequences for a false negative are usually less than for a false positive
  - An acceptable system may have a false positive rate of 0.001 percent but a false negative rate of 1 percent

# BIOMETRICS: SOMETHING YOU ARE


# BIOMETRICS: SOMETHING YOU ARE

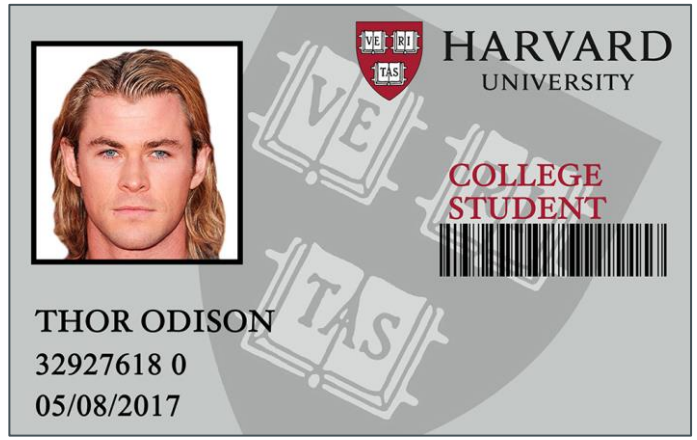
- All biometric readers operate in 2 phases
  - A user registers with the reader
    - A characteristic of the user is captured and reduced to a set of data points
    - The user may be asked to present the characteristic several times so that the registration software can adjust for variations
    - Registration produces a pattern, called a template, of the data points particular to a specific user
  - The user later seeks authentication from the system
    - The system remeasures the characteristic of the user and compares the new measurements with the stored template
    - If the new measurement is close enough to the template, the system accepts the authentication

# BIOMETRICS: SOMETHING YOU ARE

# TOKENS: SOMETHING YOU HAVE

You have a physical object in your possession




# TOKENS: SOMETHING YOU HAVE


- Another kind of authentication token has data to communicate invisibly
  - Credit cards with a magnetic stripe
  - Credit cards with an embedded computer chip
  - Access cards with passive or active wireless technology

# TOKENS: SOMETHING YOU HAVE

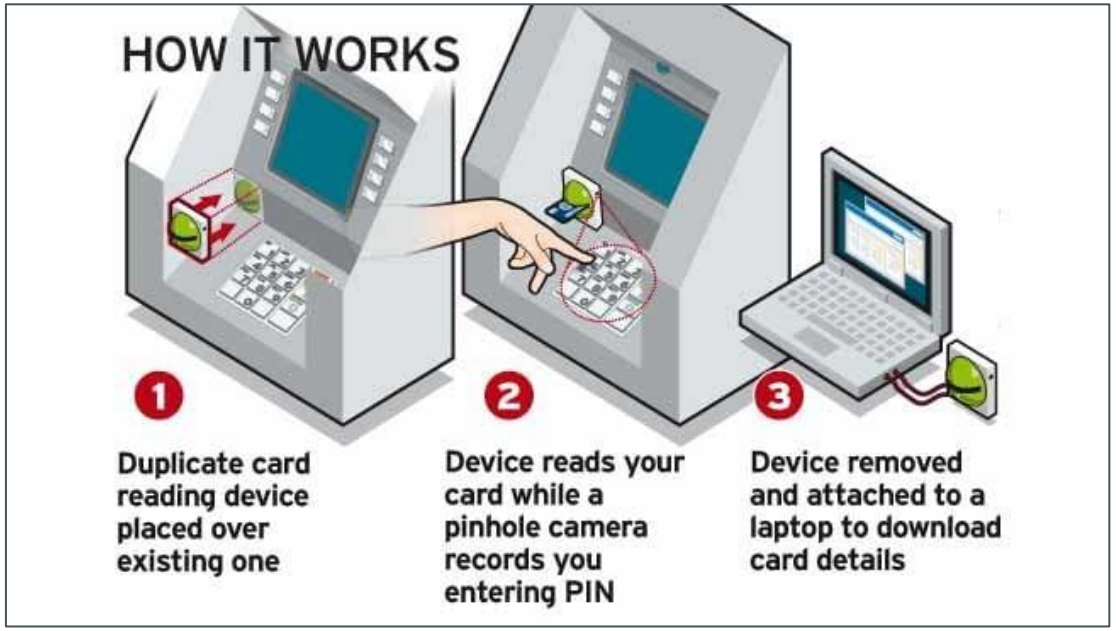
Of course, tokens can be LOST and, with appropriate tools and techniques, COPIED

# TOKENS: SOMETHING YOU HAVE

## Skimming

The use of a device to copy authentication data surreptitiously and relay it to an attacker

# TOKENS: SOMETHING YOU HAVE




# TOKENS: SOMETHING YOU HAVE

- The value of a static token remains fixed
  - Keys
  - Identity cards
  - Passports
  - Credit and other magnetic stripe cards
  - Radio transmitter cards (called RFID devices)
- Static tokens are most useful for onsite authentication
- Remote authentication
  - Being able to prove your identity to a person or computer somewhere else
  - Distance increases the possibility of forgery
- Dynamic token generators are useful for remote authentication, especially of a person to a computer

# TOKENS: SOMETHING YOU HAVE

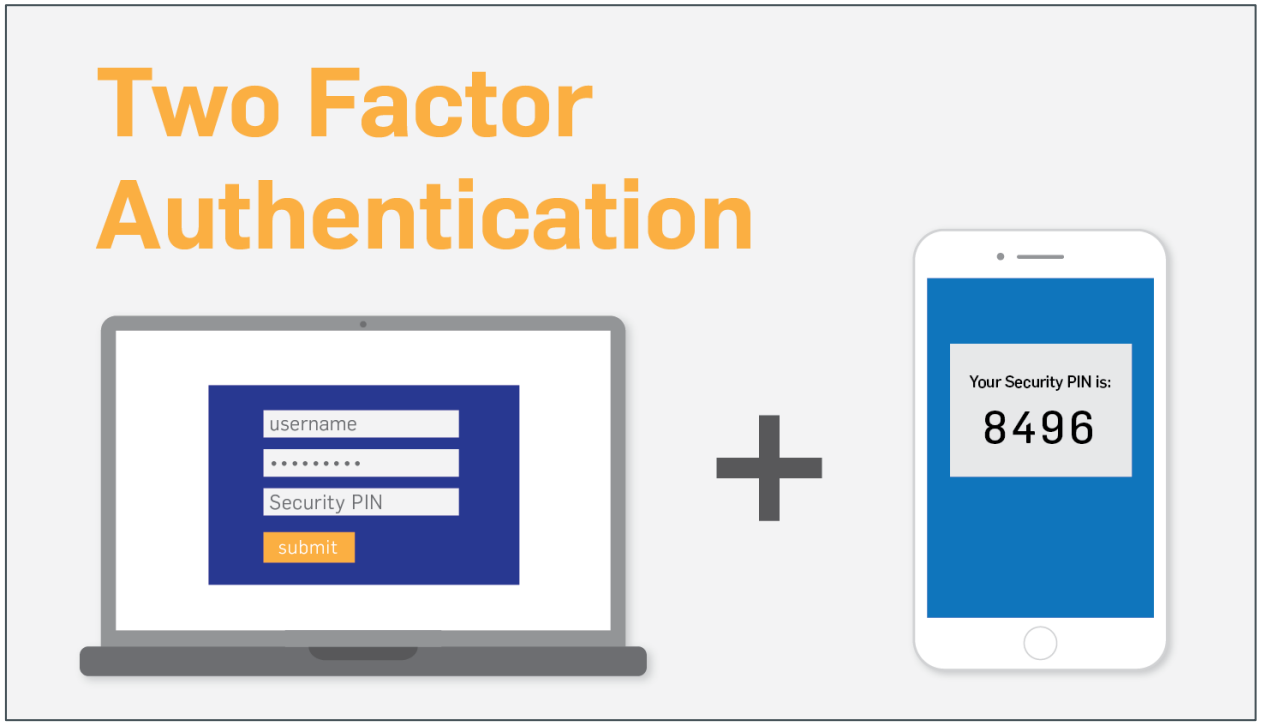
## Dynamic Authentication Token

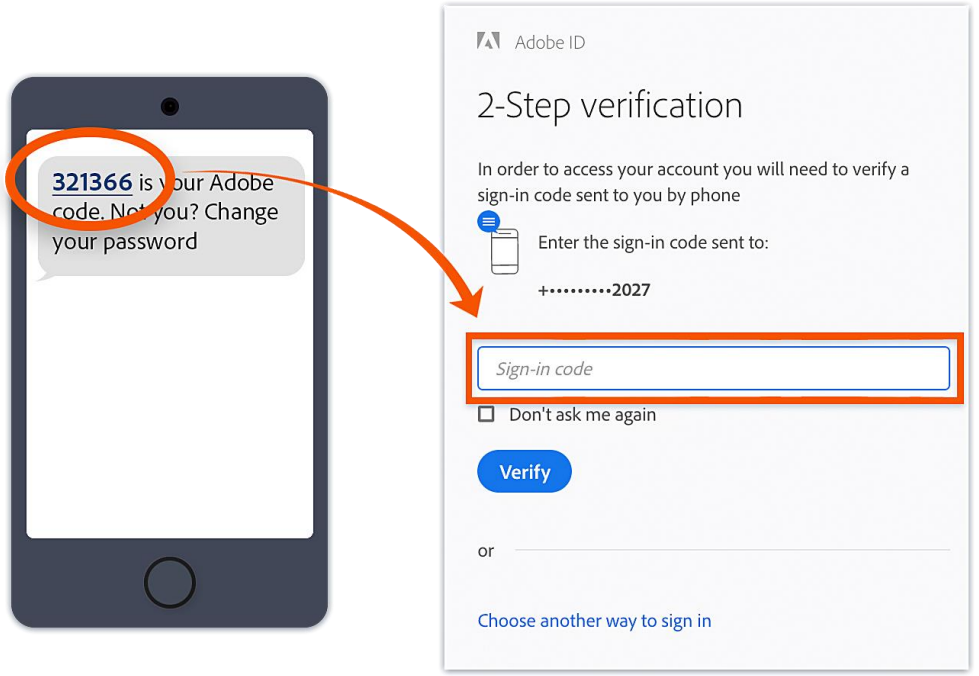
**A device that generates an unpredictable value that we might call a pass number**

- Some devices change numbers at a particular interval, for example, once a minute
- Others change numbers when you press a button
- Others compute a new number in response to an input, sometimes called a challenge

# MULTIFACTOR AUTHENTICATION

# MULTIFACTOR AUTHENTICATION



# MULTIFACTOR AUTHENTICATION

Which value of *n*
makes *n*-factor authentication optimal?

# MULTIFACTOR AUTHENTICATION

As the number of forms increases,
so also does the user's inconvenience

From a usability point of view,
large values of *n* may lead to
user frustration and reduced security

# SECURE AUTHENTICATION

Suppose Adams works in the accounting department during the shift between 8:00 a.m. and 5:00 p.m., Monday through Friday. Any legitimate access attempt by Adams should be made during those times, through a workstation in the accounting department offices.

- The system protects against 2 problems
  - Someone from outside might try to impersonate Adams
  - Adams might attempt to access the system from home or on a weekend, planning to use resources not allowed or to do something that would be too risky with other people around

# SECURE AUTHENTICATION

- Limiting users to certain workstations or certain times of access can cause complications
  - When a user legitimately needs to work overtime
  - A person has to access the system while out of town on a business trip
  - A particular workstation fails

- However, some companies use these authentication techniques because the added security they provide outweighs inconvenience

# REFERENCES


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

# NEXT WEEK: PROGRAM SECURITY

- Threat
  - Program Flaw Leads to Security Failing
- Vulnerability
  - Incomplete Mediation
  - Race Condition
  - Time-of-Check to Time-of-Use
  - Undocumented Access Point
- Ineffective Countermeasure
  - Penetrate-and-Patch
- Countermeasure
  - Identifying and Classifying Faults
  - Secure Software Design Elements
  - Secure Software Development Process
  - Testing
  - Defensive Programming

# 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