MSU IAC Cyber Security Training
Module 1
Securing Data From Risk

General Information

Learning Objectives

When you finish this unit you will:

1.1 Understand the importance of securing data;

1.2 Understand the different types of threats and how the three basic security properties can be used to defend against them;

1.3 Understand the difference between a security policy and a security mechanism;

1.4 Know how an identity is authenticated;

1.5 Know how to pick a password that is hard to guess;

1.6 Understand how authentication and authorization differ;

1.7 Understand how important the “human factor” is in protecting data; and

1.8 Know some of the principles underlying data protection.

Why Worry about Security of Data?

- Your personal information
- Other people's personal data
  - May need to be protected by law
- Data gathered about people can reveal much about their behavior
  - Medical records
  - Data from smart meters
- Whistleblowers!
- Some data is proprietary or contains intellectual property

Threat

Defined as a *potential* violation of security

- Important to know: it need not happen; it just needs to be possible

Some threats are more critical than others

- The threat of a computer being lost while being taken on a trip
  - Laptop: fairly high because it is portable and easy to carry
  - Mainframe: rarely travels once it is installed because it is non-portable and difficult to carry

Examples of Threats

ComputerWeekly.com

412 million user accounts exposed in FriendFinder Networks hack

Los Angeles Times

UCLA Health System data breach affects 4.5 million patients

The New York Times

Yahoo Says 1 Billion User Accounts Were Hacked

By VINDU GOEL and NICOLE PERLROTH DEC. 14, 2016

More Examples of Threats

WIRED

AN UNPRECEDENTED LOOK AT STUXNET, THE WORLD'S FIRST DIGITAL WEAPON

LegalBugle

The Neighbors From Hell

Among the most famous of these cases was that of the so-called "neighbors from hell." Lara Love and David Jackson victimized over 30 of their neighbors with a massive identity theft scheme, taking advantage of the trusting nature of their friends in order to steal their identities using unsecured wireless networks, the documents found in the trash and even by stealing their wallets.

Bloomberg the Company & Its Products

Bloomberg

AP The Associated Press @AP Following

Breaking: Two Explosions in the White House and Barack Obama is injured

Reply Retweet Favorite More

3,063 RETWEETS 144 FAVORITES

12:07 PM - 23 Apr 13

and the market reacted accordingly: From 1:08 p.m. to 1:10 p.m., the Dow Jones Industrial average plunged more than 100 points, from 14697.15 to 14548.58. Just as quickly though, it rebounded. By 1:13 p.m., it was back

And Still More Threats …

DoS attack on major DNS provider brings Internet to morning crawl

VARIETY

Amazon Cloud Services Outage Takes Down Amazon Video, Websites and Internet-Connected Light Bulbs

21 OCT 16 Hacked Cameras, DVRs Powered Today's Massive Internet Outage

Georgia President's Web Site Falls Under DDOS Attack

What Is Security?

- A security policy is a statement of what is, and is not, allowed
- Varies among institutions

- A security mechanism is something that enforces the security policy
- This does *not* define what security is!

- A "secure" system is one in which the mechanisms enforce the security policy.

Lab Exercise #1

The difference between “policy” and “mechanism” is *crucial*.

- You can often do things that are not allowed
  - These are breaches of security because they violate the *policy*
- You sometimes cannot do things that are allowed
  - This is a *denial of service* and may also be a breach of security
- The mechanism controls what you *are able to* do; the policy, what you are allowed to do

This exercise has you match the policy element with the appropriate mechanism

LAB 1:

The following questions are about security in general.

Match the mechanism with the policy it enforces.

Policy statement	Mechanism
a. Users must authenticate themselves before using the system.	1. File protection mechanisms allow a user to turn off read permission for the group “students”.
b. Only users physically present at the system can use it.	2. The password changing program requires all passwords to be at least 16 characters long, with at least 2 digits, 2 symbols (like “+” or “@”), and both upper and lower case letters.
c. Users must pick passwords that are hard to guess.	3. The company blocks all streaming video from entering its internal network.
d. Student files will be protected so other students cannot read them.	4. When the account number is entered, the customer information associated with that account will be retrieved and displayed.
e. Only vendor-authorized programs may be used on the system.	5. The login mechanism checks that the password entered corresponds to the user account entered.
f. Customers of the store may use the web to check their accounts.	6. Each program will be checked to ensure it is approved for use by the vendor before the program is run.
g. Employees may not stream videos during work hours.	7. Networks have been disconnected from the system.

LAB 1:

The following questions are about security in general.

Match the mechanism with the policy it enforces.

Answers:
A-5;
B-7;
C-2;
D-1;
E-6;
F-4;
G-3

Policy statement	Mechanism
a. Users must authenticate themselves before using the system.	5. The login mechanism checks that the password entered corresponds to the user account entered.
b. Only users physically present at the system can use it.	7. Networks have been disconnected from the system.
c. Users must pick passwords that are hard to guess.	2. The password changing program requires all passwords to be at least 16 characters long, with at least 2 digits, 2 symbols (like "+" or "@"), and both upper and lower case letters.
d. Student files will be protected so other students cannot read them.	1. File protection mechanisms allow a user to turn off read permission for the group "students". .
e. Only vendor-authorized programs may be used on the system.	6. Each program will be checked to ensure it is approved for use by the vendor before the program is run.
f. Customers of the store may use the web to check their accounts.	4. When the account number is entered, the customer information associated with that account will be retrieved and displayed
g. Employees may not stream videos during work hours.	3. The company blocks all streaming video from entering its internal network.

Basic Elements of Security

Policies are composed of three types of elements:

- *Confidentiality*, or keeping secrets from some set of people;
- *Integrity*, or making sure data and systems are trustworthy:
  - *Data integrity* means only authorized changes are made only by authorized people;
  - *Origin integrity* means the original data is trustworthy, and its source is trusted to produce trustworthy data;
- *Availability*, or making sure the system performs at an acceptable level of service

Confidentiality

Confidentiality means keeping data to a group of people

Some examples:

- Military classifications and clearances
  - CONFIDENTIAL, SECRET, TOP-SECRET…
- Industry
  - Proprietary data, trade secrets
- Academia
  - Perhaps grades, financial aid, personal information

Privacy

Like confidentiality but focuses on *control* of information

Doctor can see patient's medical record

- If patient controls to whom the doctor can show it, and what the doctor can do with it, the medical record is private
- If the doctor can show it to anyone, or can use it for her own purposes without the patient's consent, it's not private

Integrity

Data integrity means only authorized changes are made only by authorized people

Alice works in the registrar's office at a university, and is authorized to change addresses but nothing else in the record

- She updates the address of a student; that's fine
- She changes a grade in a student's record without faculty approval; that violates data integrity

Integrity and Trust

If something is “trustworthy” then you can trust it.

- Different people have different understandings of what “trust” means
- In practice, based on evidence (“assurance evidence”)

Both trustworthiness of source and of data affect its integrity

Availability

A contract or notice defines what level of service will be provided

- Called “quality of service” (abbreviated as “QoS”)

Resource is available if the user can get the QoS expected

In the past it meant one of two things:

- An entity could access the resource
  - Quality of service here is ability to make contact
- The resource is distributed “fairly” among the entities
  - Quality of service is that each entity gets as much service as any other entity

Denial of Service Attack

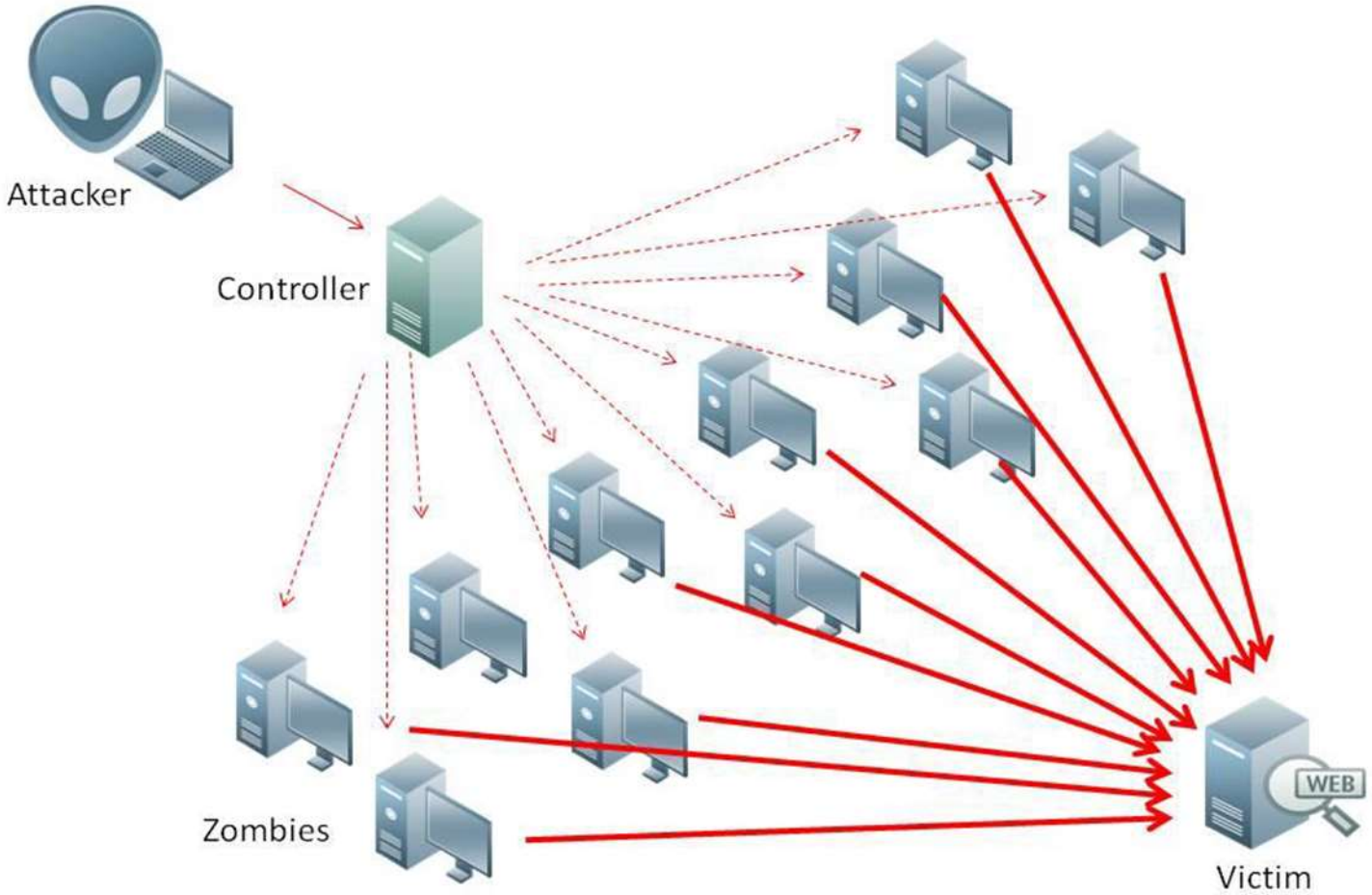


Image by Nasanbuyn
From Wikimedia Commons
Used under Creative Commons
Attribution Share-Alike 4.0
International license

Lab Exercise #2

Understanding the three properties of security will help you ask the right questions about what someone means when they talk about “securing” data.

This exercise gives you several scenarios and asks you to classify them as violations of confidentiality, integrity, or availability (or some combination of these).

Who Are We Talking About?

Something that identifies an entity

- Your name
- Your DNA

For a computer:

- A host name (www.cnn.com)
- An IP address (151.101.24.73)
- An Ethernet (MAC) address (9e:87:22:e2:39:d2)

Authentication

Authentication is proving your identity

- Giving your password to log into gmail.com to read your email (“what you know”)
- Showing your driver’s license when you go through security at the airport (“what you have”)
- Using your fingerprint to unlock your laptop or smartphone (“what you are”)

Initializing Identity

Authentication requires a database of information

- To authenticate someone, compare the information they give you with the corresponding information in the database
- When someone signs up, their authentication information is put into the database
- What happens if the wrong information goes into the database?

Passwords

An example of “what you know”

- Best: random long passwords that are easy to remember
  - Contradictory (“random long” … “easy to remember”)
  - Or, use a password manager
- In practice: pick 2 or 3 sequences of characters that are meaningful to you and combine them
  - Make it as long as possible, with as great a mixture of letters, numbers, and symbols as you can

More on Passwords

Example of passwords that are easy to guess:

- “hello” — dictionary word
- “mycomputer” — two dictionary words put together
- “qwertyuiop” — top row of letters on U.S. keyboard
- “311t3$p34k” — replace letters with digits and symbols (“elitespeak”)

Examples of passwords that are hard to guess:

- “WtBvStHbChCsLm?TbWtF.+FSK
- “>2-;:Pm,)3YSDN[@CEO?Xc:rx[”

Lab Exercise #3

Picking passwords is hard, especially given the resourcefulness of password attackers. Programs automate this, but they work from lists of words or characters and from algorithms. So you have to pick passwords that are very unlikely to be guessed.

The two parts of this question ask you to think about what makes a password hard to guess.

Puzzler

This exercise asks you to look at a characteristic of passwords that increases the time required to guess the password by trying different possible passwords.

Passphrases

Sometimes easier to remember than random passwords

Pick several words and string them together, separated by blanks

Examples:

- “correct horse battery staple”
- “A home and a country should leave us no more”
- Any line from a book provided the line is not well known

Lab Exercise #4

Passphrases are often touted as a good way to increase the difficulty of guessing what you use to authenticate. They are substantially better than short passwords, but they are not a panacea.

This exercise asks you to reflect on that.

Tokens

Something you possess that authenticates you

Examples:

- Hotel room card key
- Smartphone
- Asynchronous token (generates unique password at each use); bank token at right, a Digipass 270 security token, used for online banking, is an example

Image by D4m1en
From Wikimedia Commons
Used under Creative Commons
Attribution Share-Alike 3.0
Unported license

Biometrics

Use a physical characteristic to authenticate

Examples:

- Fingerprint scanner
- Palmprint scanner
- Voice recognition device
- Iris (eye) scanner

Image by Mark Pellegrini
From Wikimedia Commons
Used under Creative Commons
Attribution Share-Alike 2.5
Generic license

Multifactor Authentication

Use at least two factors to prove identity

- Must be two *different* factors

Example: Google multifactor authentication ("2-step verification")

- Initially: you sign up for it to protect your Gmail account
- When you log into Gmail, *before* you get access to your email, Google sends you a 6-digit code
- You must enter the 6-digit code into the web page to access your email

Mutual Authentication

- You authenticate to a system that claims to be running the XYZ service; it also provides proof that it is in fact the XYZ service you think.
  - "Mutual" because just as you authenticate to the server, it authenticates to you.

- Example: When someone in plain clothes says "I'm a police officer; please show me your identification", you ask her to show you her badge.
  - She's authenticating her identity and that she is a police officer
  - You're authenticating yourself to her

Principle of Separation of Privilege

Every access requires meeting more than one condition

- Capturing a castle: cross the moat, go over the outer wall, then over the inner wall
- Multifactor authentication: meet two conditions (the two factors)

Image: Beaumaris Castle cadw.wales.gov.uk

Lab Exercise #5

Multifactor authentication is a common term, usually as “two-factor authentication”. Like any other authentication mechanism, it has to be implemented carefully.

This exercise asks you to consider what is, and is not, true two-factor authentication.

Who Can Do What to What

Authorization is the set of rights a user has

- Note it is *not* authentication; it presumes you have authenticated, and your identity is known
- The two are independent
  - Some mechanism other than authenticating mechanism checks what the user can do

Authorization Principles

These are the main ones

- Principle of Least Privilege: a user should have *exactly* those rights needed to perform her job, and no more
- Principle of Separation of Privilege: every access should require satisfying more than one condition (also called “separation of duty”)
- Principle of Complete Mediation: all accesses must be checked to ensure they are authorized

Example

Post Office: you need to pick up a package

- Authentication: you prove who you are (by showing a state-issued ID like a driver's license)
- But if you are not the addressee, you are not authorized to pick up the package
  - Delegation: the addressee may have told the Post Office that you would pick up her email, in which case you are authorized to pick it up
- If you are the addressee, you are authorized to pick up the package

Example of Separation of Privilege

Outer firewall controls access to both the DMZ and the Intranet

- Everyone is authorized to access the DMZ (public web servers are here)
- To get into the Intranet, user must authenticate to the inner firewall, which then determines if that user is authorized to use the Intranet

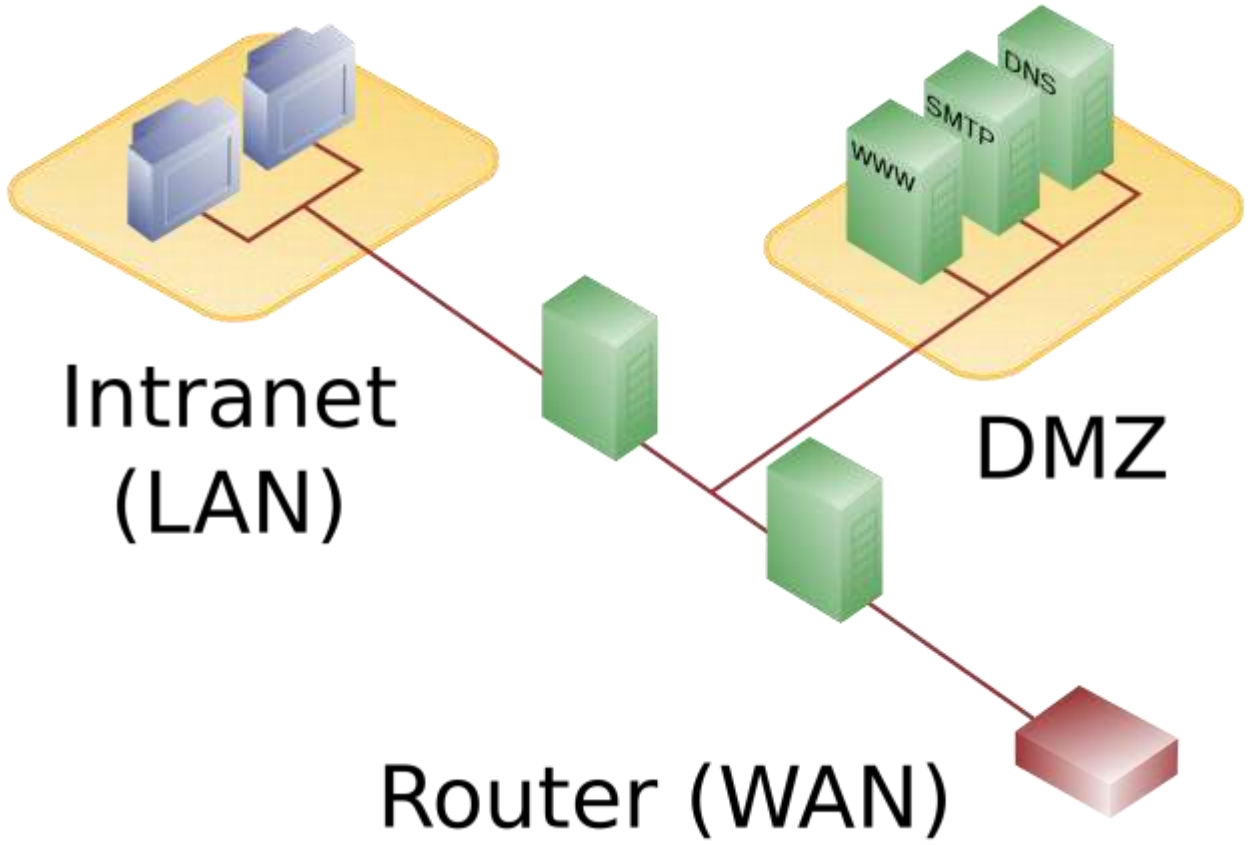


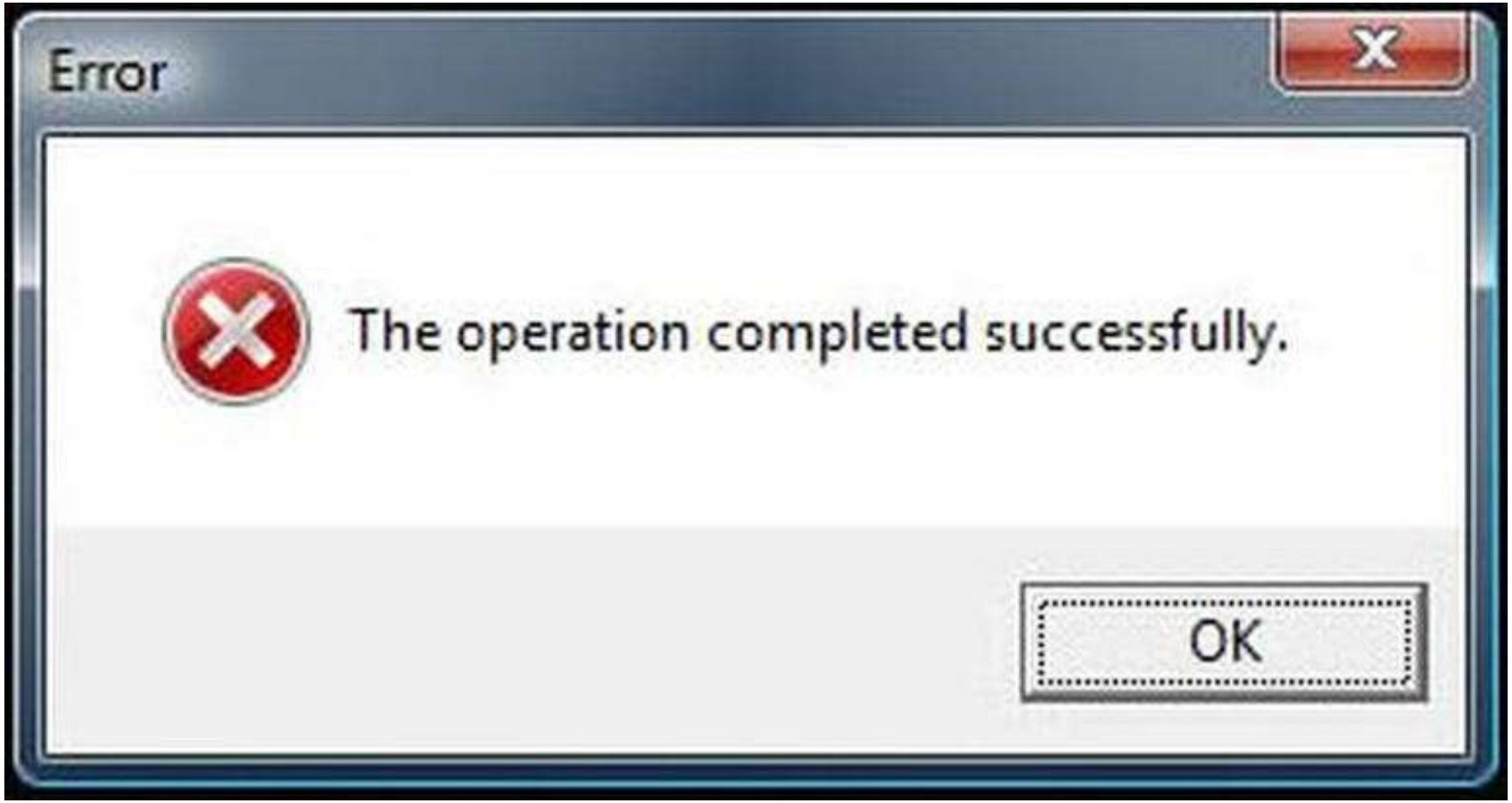
Image by Sangre Viento from Wikimedia Commons
Released by the author into the public domain

People and Security

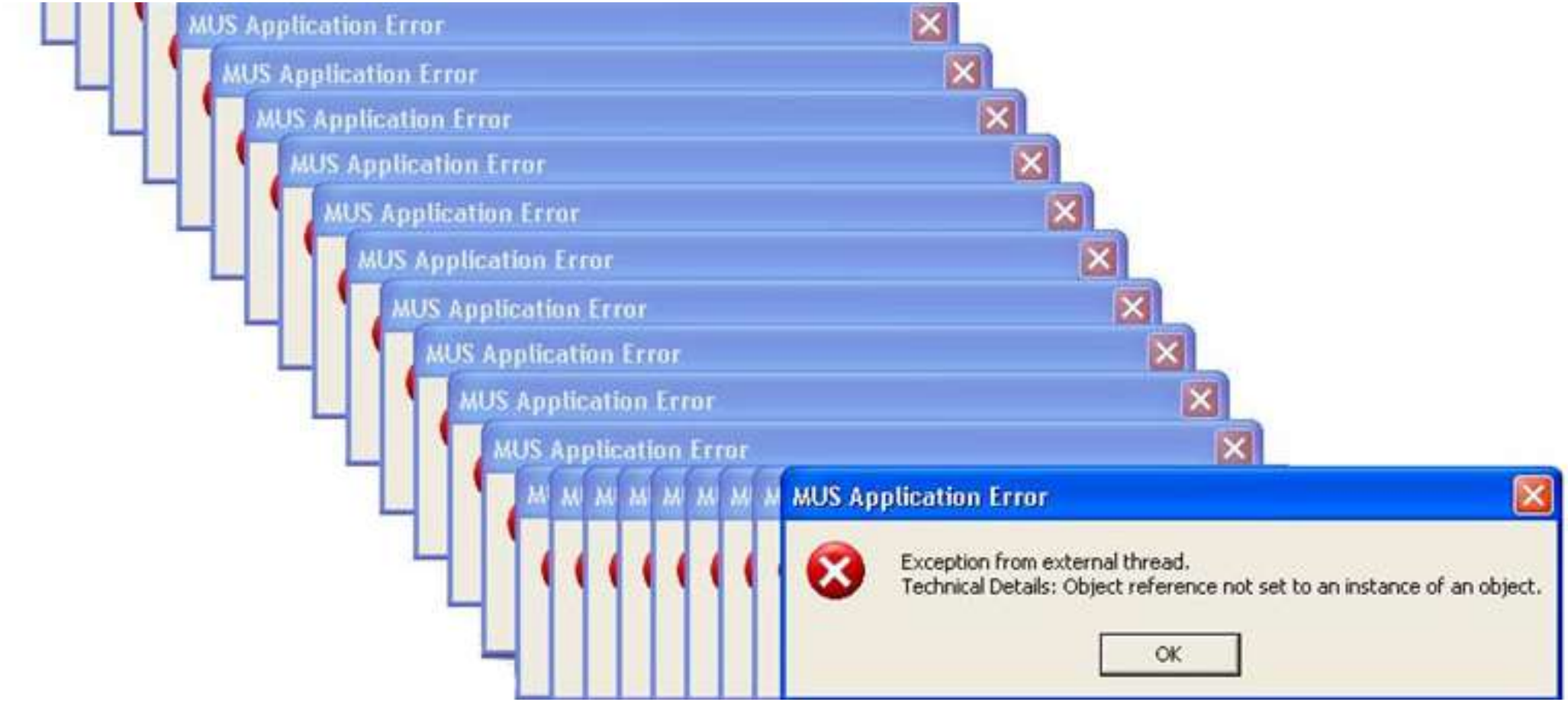
Principle of Least Astonishment: security mechanisms should be designed so that users understand the reason that the mechanism works the way it does and that using the mechanism is simple.

- In other words, the mechanism should fit the “mental model” of the user
- In simpler terms, don’t let the mechanism surprise them!

What's Wrong with This?



Here's Another



The Problem

- If users do not understand what is happening, they may make the situation worse
  - This also goes for administrators too!
- Need to take into account who the mechanism is intended for
  - Computer scientists may need less explanation than home users
- But designers and implementers assume people like them will be using the system
- Hence cryptic error messages like these are unhelpful:
  - Lint's little brain is fried
  - Shannon and Bill say this can't happen

Big Puzzler

The way software conveys information to a user can either make or break the program. The most useful program in the world will not be used if the user cannot figure out how to do so in a way that the user finds most productive.

This question asks you to look at this problem.

Conclusion

- This covered background material for securing data
- A lot of it focused on what “securing” means
  - In terms of the kind of access
  - In terms of the people who can access it