

Module 1

Principles of Cybersecurity

What is “Cybersecurity”?

“I have a son. He's 10 years old. He has computers. He is so good with these computers, it's unbelievable. The security aspect of cyber is very, very tough. And maybe it's hardly doable... We have so many things that we have to do better, and certainly cyber is one of them.”

-- Former U.S. President, Donald Trump

What is “Cybersecurity”?

cyber 

adjective | cy·ber | \ˈsī-bər\
Popularity: Top 30% of words

Definition of CYBER

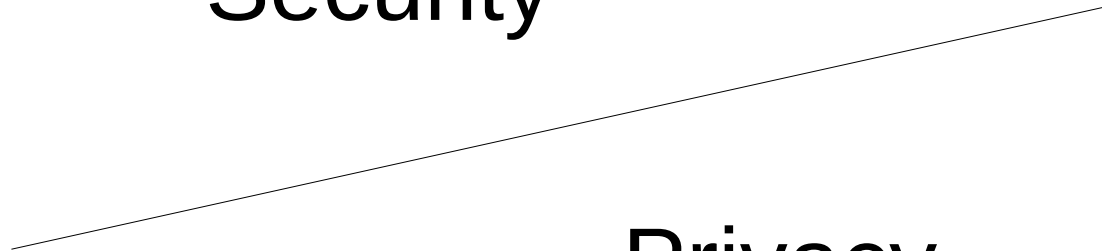
: of, relating to, or involving computers or computer networks (as the Internet) <the *cyber* marketplace>

What is “Cybersecurity”?

Protection of assets, systems, secrets



Security



Privacy



Protection of identity, behavior, expression

CMPT 479

Class times: Monday 2:30 – 3:20 pm
Thursday 2:30 – 4:20 pm

TA: Saghar Irondoust
Jiawen Zhang

Place: This Zoom meeting



Grading

45%	3x Assignments (15%)
10%	Online Self-Assessment
20%	Mid-term Exam
25%	Final Exam

Online Self-Assessment

- One assessment for each module
- Due one week after module, midnight
- Posted on Canvas

Assignments

Each Assignment has a:

- Written Component
- Programming Component

There is a grace period (no penalty) of **exactly 48 hours** after the Assignment due date, at midnight.

If you need an extension of more than 48 hours, you must tell me with a valid reason before the Assignment due date.

Contact

E-mail: taowang@sfu.ca

Please preface your e-mail title with “CMPT479”.

Any questions are welcome!

What is the price of security?

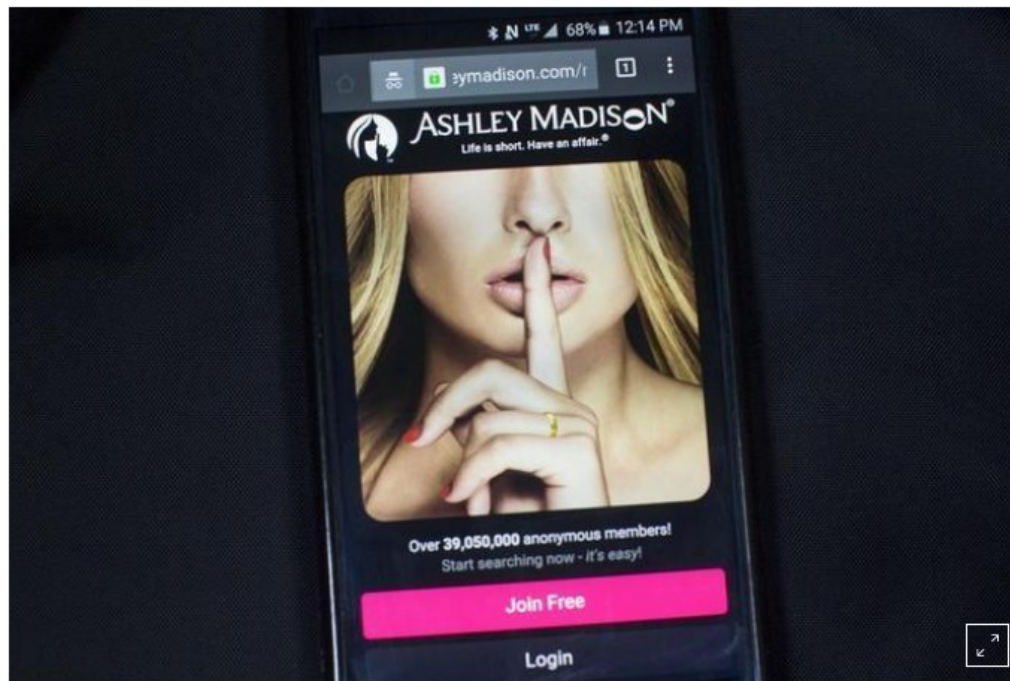
Ashley Madison parent in \$11.2 million settlement over data breach

Jonathan Stempel

2 MIN READ



(Reuters) - The owner of the Ashley Madison adultery website said on Friday it will pay \$11.2 million to settle U.S. litigation brought on behalf of roughly 37 million users whose personal details were exposed in a July 2015 data breach.



A photo illustration shows the Ashley Madison website displayed on a smartphone in Toronto, August 20, 2015. REUTERS/Mark Blinch

What is the price of security?

Verizon, Yahoo agree to lowered \$4.48 billion deal following cyber attacks

Anjali Athavaley, David Shepardson

3 MIN READ



(Reuters) - Verizon Communications Inc ([VZ.N](#)) said on Tuesday it would buy Yahoo Inc's YHOO.O core business for \$4.48 billion, lowering its original offer by \$350 million in the wake of two massive cyber attacks at the internet company.

At least 1 billion accounts compromised

What is the price of privacy?

EDITORS' PICK | 19,081 views | Jul 24, 2019, 12:05pm

FTC Slaps Facebook With \$5 Billion Fine, Forces New Privacy Controls



Michael Nuñez Forbes Staff

Social Media

I'm an associate editor covering Facebook and social media.



Principles of CIA

Confidentiality

Information is secret

Integrity

Information/System is correct

Availability

System is usable

Principles of CIA

<Login>

Welcome back, customer!



Alice



Attacker
(Eavesdropper)



Bob

Which principle is violated?
(Confidentiality, Integrity, Availability)

Principles of CIA

Change the password to <mypassword>.

Okay.



Alice



Attacker

(Man in the middle)



Bob

Which principle is violated?
(Confidentiality, Integrity, Availability)

Principles of CIA

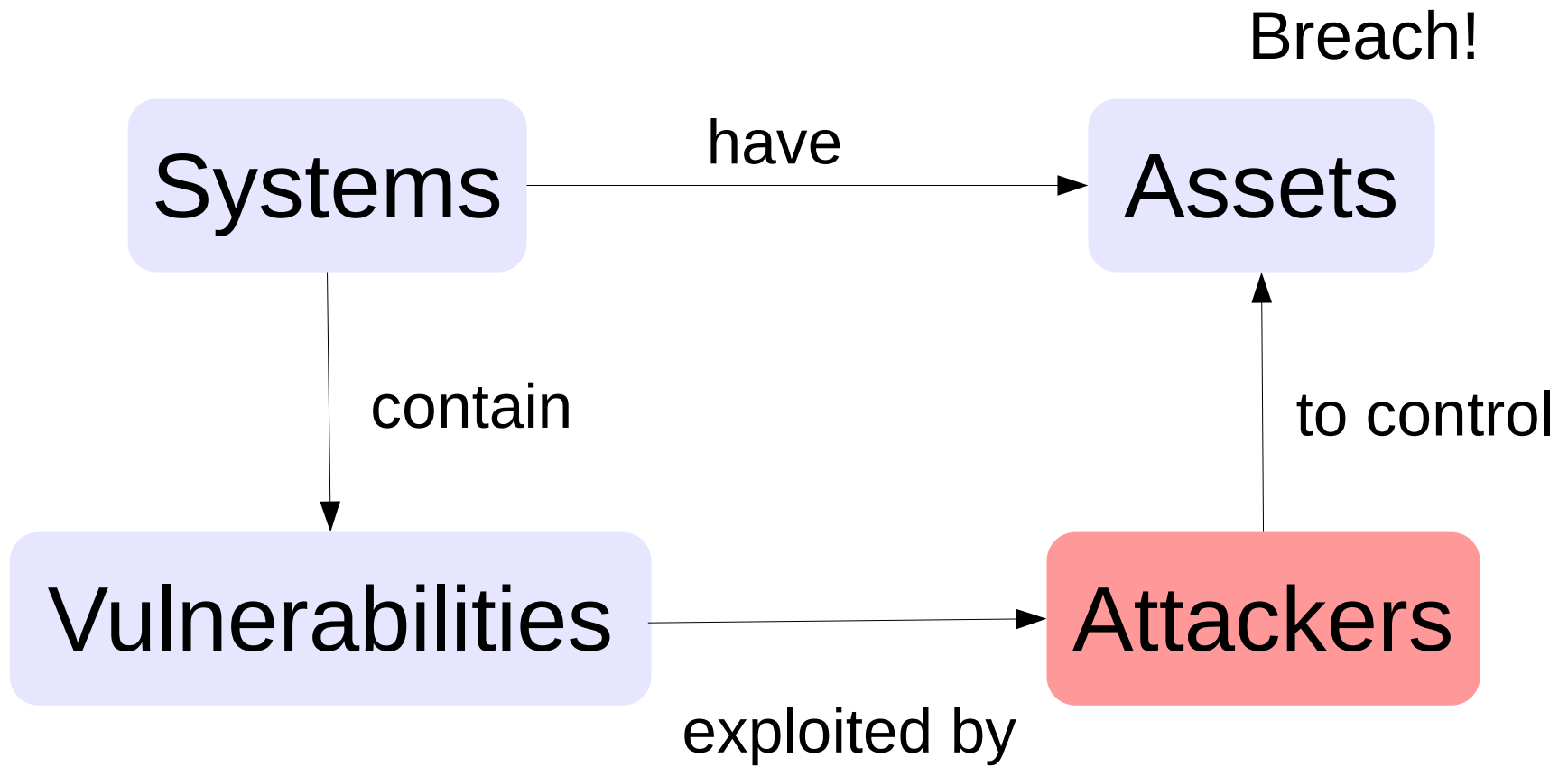
- Distributed Denial of Service (DDoS)
- Money was stolen from an online exchange

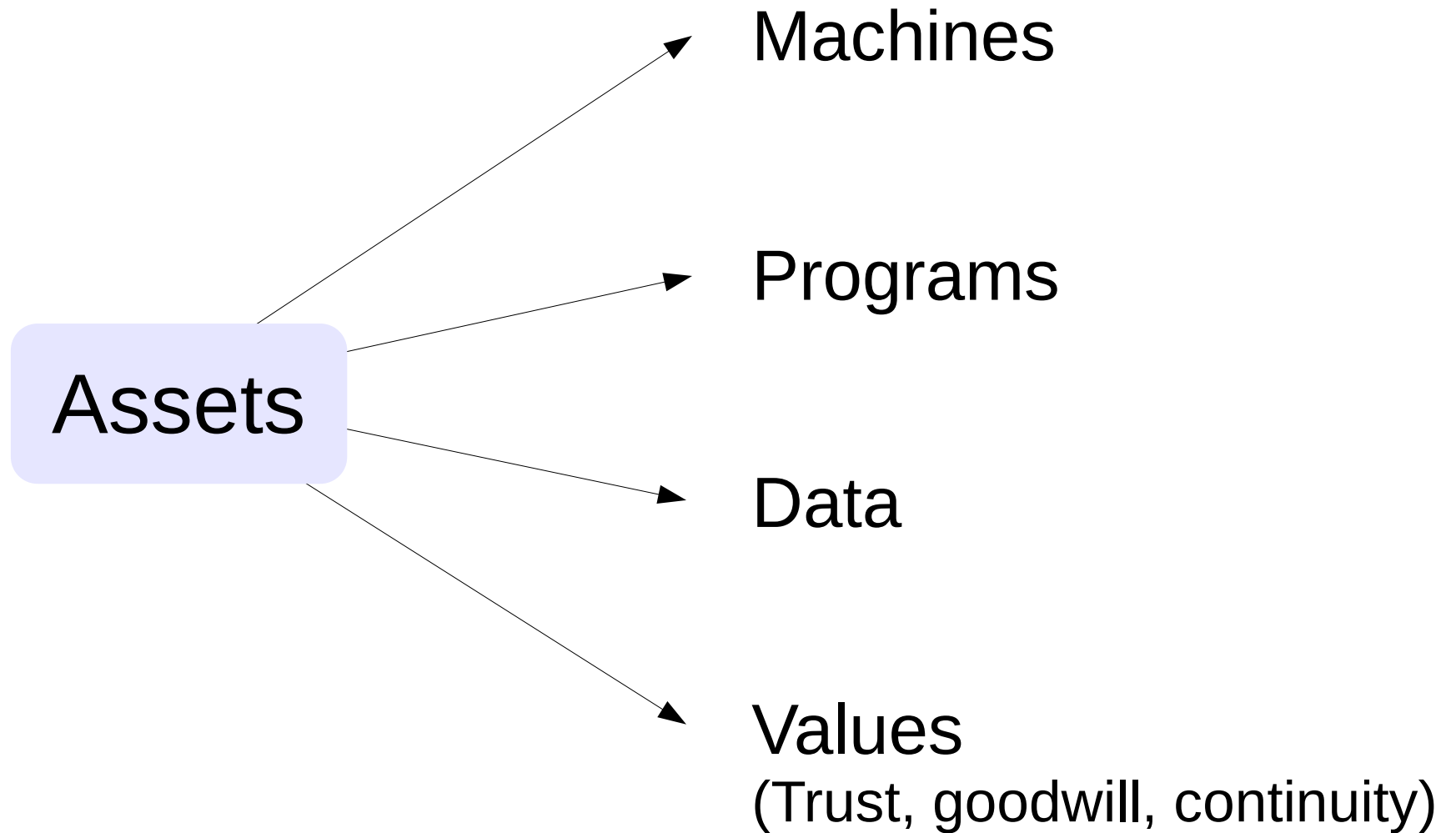
Which principle is violated?
(Confidentiality, Integrity, Availability)

Principles of CIA

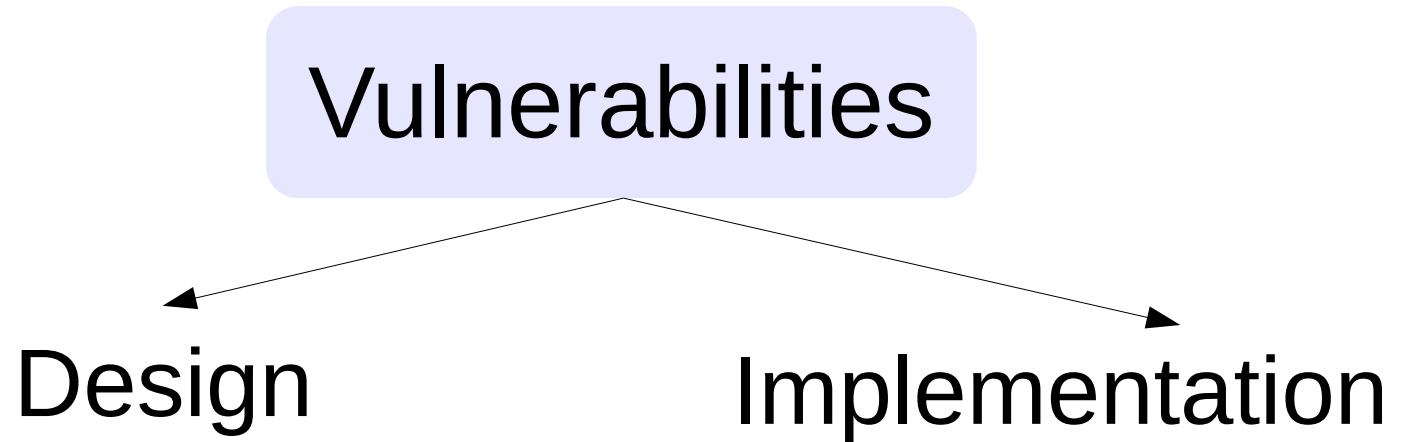
- Distributed Denial of Service (DDoS)
 - The attacker used a botnet that was created by guessing trivial remote access passwords
- Money was stolen from an online exchange
 - The owners are forced to shut down the service
 - It turns out the attack was successful because an administrator opened a malicious file

Which principle is violated?
(Confidentiality, Integrity, Availability)





Where do vulnerabilities come from?



Wrong threat model/user model, didn't design for security, etc.

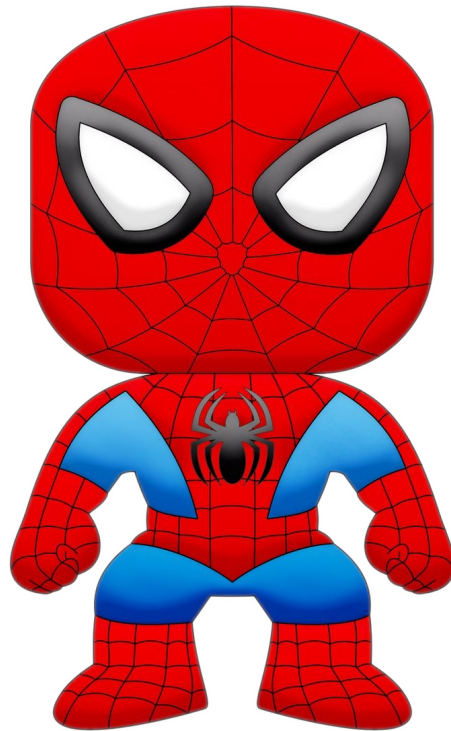
Errors in coding, hardware; Intentional errors, etc.

Vulnerability by design



Spiderman Rule

*With great power
comes great responsibility!*



Privacy

Is privacy the same as confidentiality?

Welcome back, customer!
Last week you purchased:
.....



Alice



Attacker
(Eavesdropper)



Bob

Privacy

Is privacy the same as confidentiality?

Welcome back, customer!
As a reward, please use
this gift code for your next purchase: ...



Alice

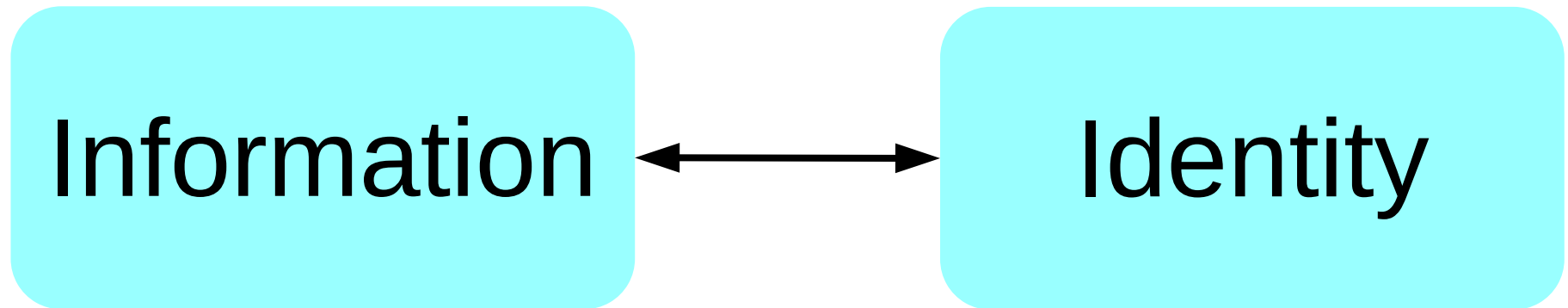


Attacker
(Eavesdropper)



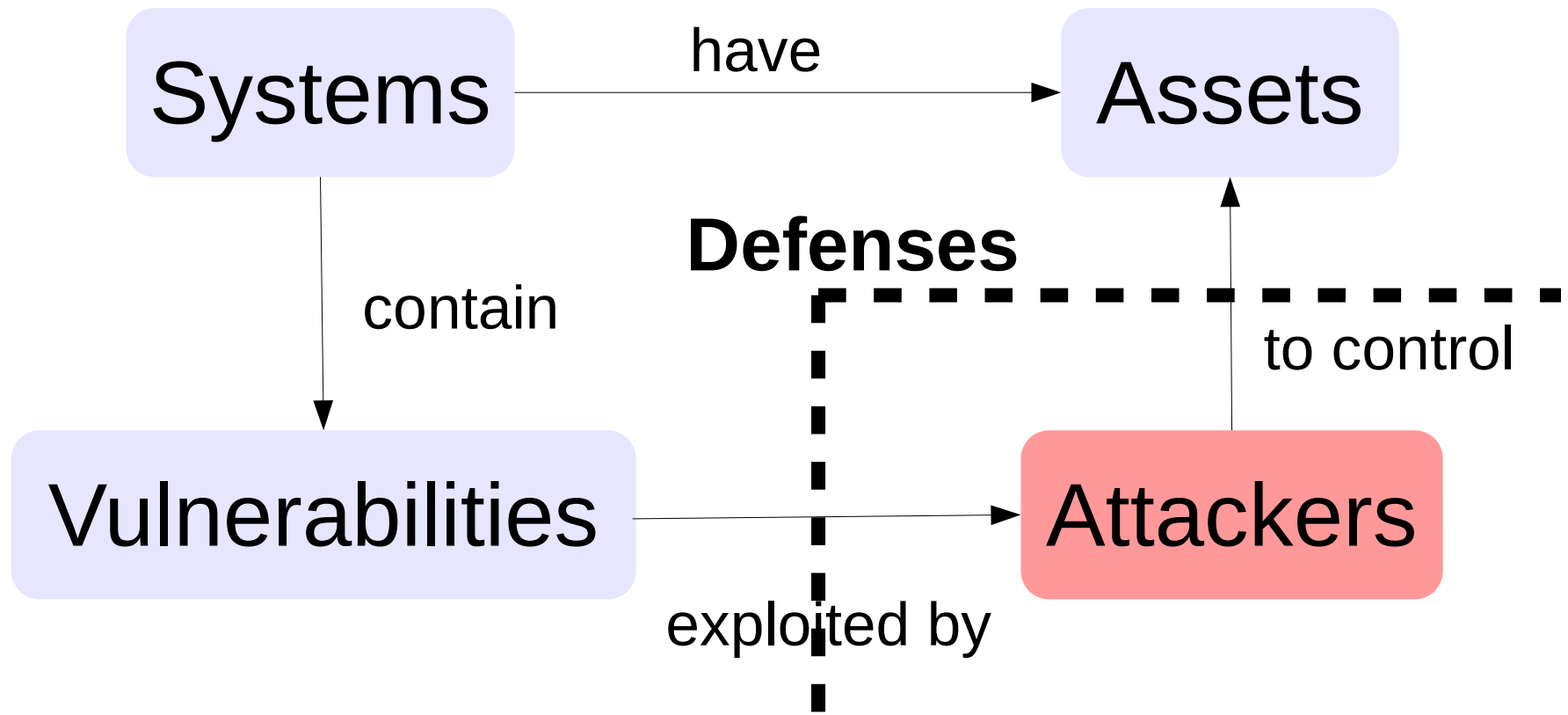
Bob

Privacy



Issues: Expression, social vulnerability,
behavioral analysis, discrimination

Protections: Anonymization, disassociation,
security



Defensive Strategy

Risk Management:

A risk is something that could damage, destroy, or disclose data

Essential for convincing upper management to adopt security countermeasures!

- Quantitative Risk Analysis
- Qualitative Risk Analysis

Quantitative Risk Analysis

For any given risk, calculate single loss expectancy (SLE):

$$\text{SLE} = \text{Asset Value} * \text{Exposure Factor}$$

←
% of assets exposed
to the risk

Then calculate the company's annual loss expectancy (ALE):

$$\text{ALE} = \text{SLE} * \text{annualized rate of occurrence}$$

If your proposed countermeasure can reduce ALE more than the cost of the countermeasure, it's good!

Principles of Secure Design

Security by Design:

*Security should be considered starting from
the design phase*

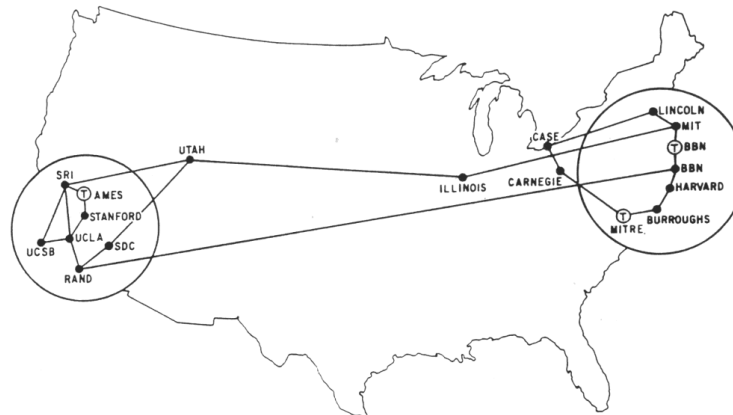
*(Vulnerabilities should be considered starting from
the design phase)*

Principles of Secure Design

Is the Internet secure by design?

The goal [of ARPANET] was to exploit new computer technologies to meet the needs of military command and control against nuclear threats, achieve survivable control of US nuclear forces...

-- Stephen J. Lukasik, Director of DARPA (1967-1974)



MAP 4 September 1971

Saltzer and Schroeder's Principles of Secure Design

1) Open Design

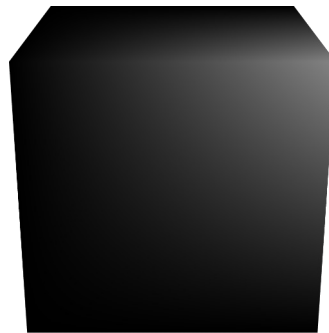
*The system's design
should be openly available to everyone.*

Saltzer and Schroeder's Principles of Secure Design

1) Open Design

Opposite of Security through Obscurity:

Hide details of the implementation
to prevent compromising analysis



Saltzer and Schroeder's Principles of Secure Design

1) Open Design

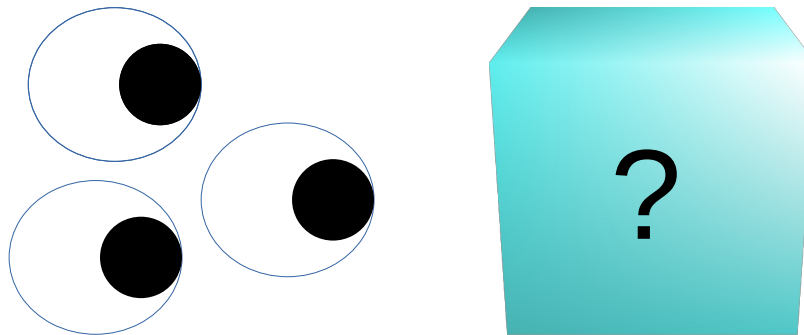
Examples of Security through Obscurity:

- Terms of Service + lawsuits barring reverse engineering
- Cryptosystems where the algorithms are secret

Saltzer and Schroeder's Principles of Secure Design

1) Open Design

"Given enough eyeballs, all bugs are shallow"
-- Linus Torvalds



Saltzer and Schroeder's Principles of Secure Design

1) Open Design



Heartbleed (2014):
Serious open-source software bug

“The eyeballs weren’t looking”

Saltzer and Schroeder's Principles of Secure Design

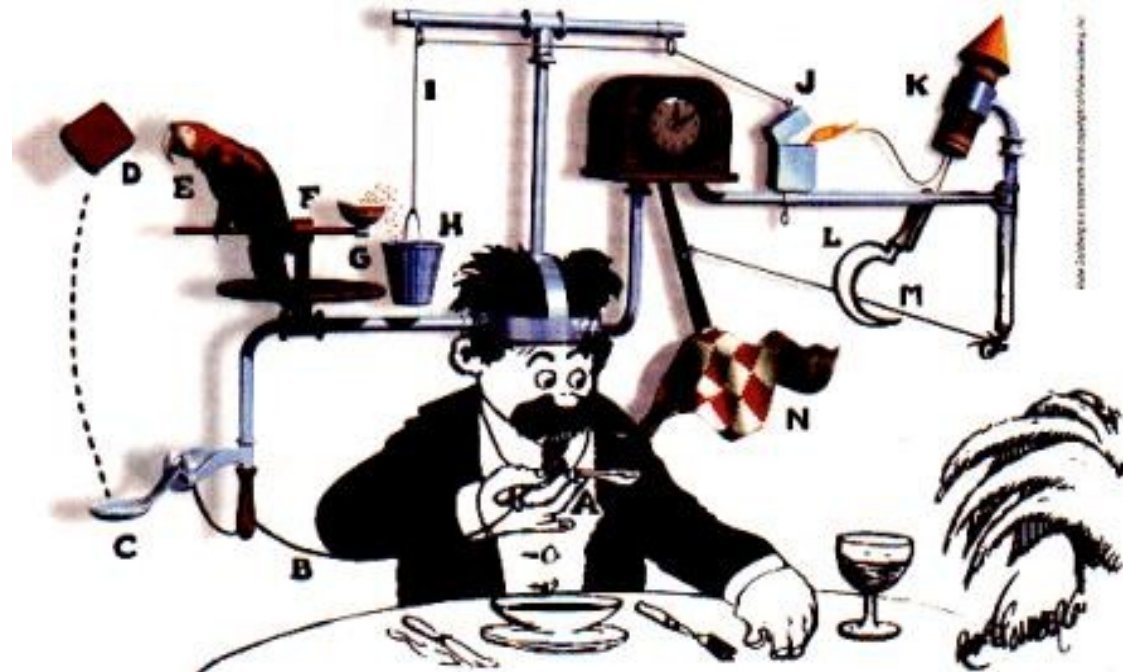
2) Economy of Mechanism

*The system should be simple enough
to understand and analyze.*

Saltzer and Schroeder's Principles of Secure Design

2) Economy of Mechanism

KISS Principle: Keep it simple/stupid



Saltzer and Schroeder's Principles of Secure Design

2) Economy of Mechanism

- Helpful for security analysis
- Encourages good design
- Complicated solutions are bypassed by simple workarounds



Juicero (2016-2017)
*Complicated solution,
simple workaround*

Saltzer and Schroeder's Principles of Secure Design

3) Least Common Mechanism

The amount of shared mechanisms that all users depend on should be minimized.

Saltzer and Schroeder's Principles of Secure Design

3) Least Common Mechanism

Examples for web hosting:

- Use multiple data centers
- Backup your database
- Localize computations

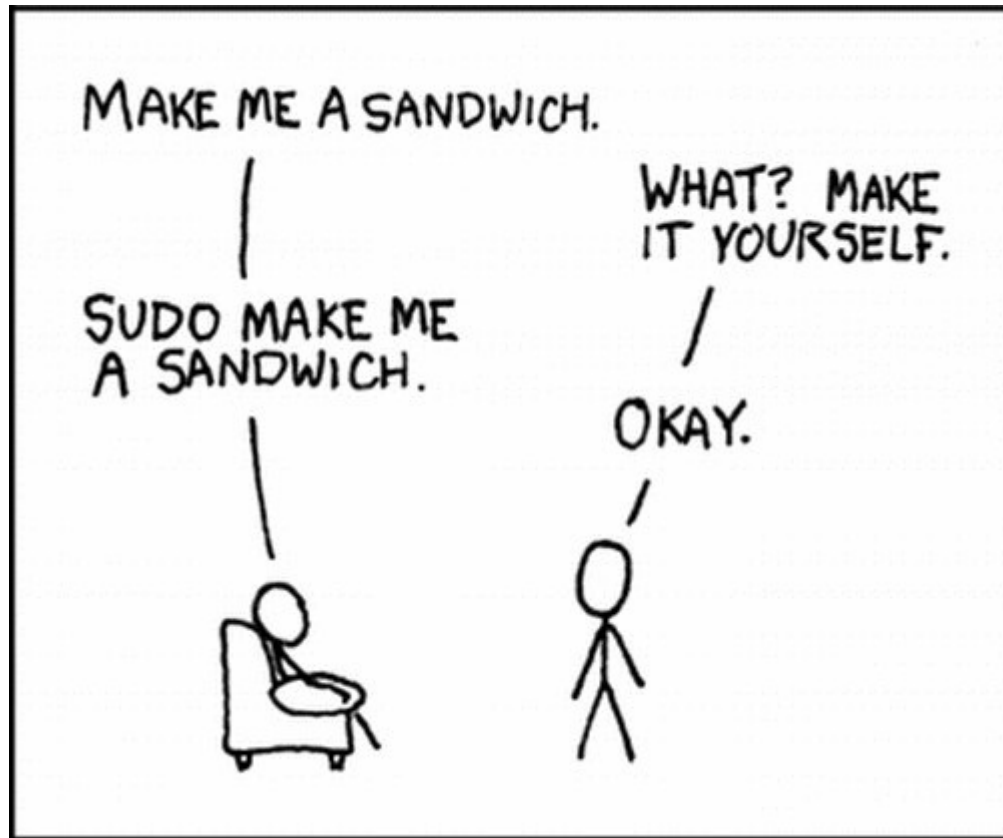
Saltzer and Schroeder's Principles of Secure Design

4) Least Privilege

A subject should only be given the minimum necessary privileges for completing its task.

Saltzer and Schroeder's Principles of Secure Design

4) Least Privilege



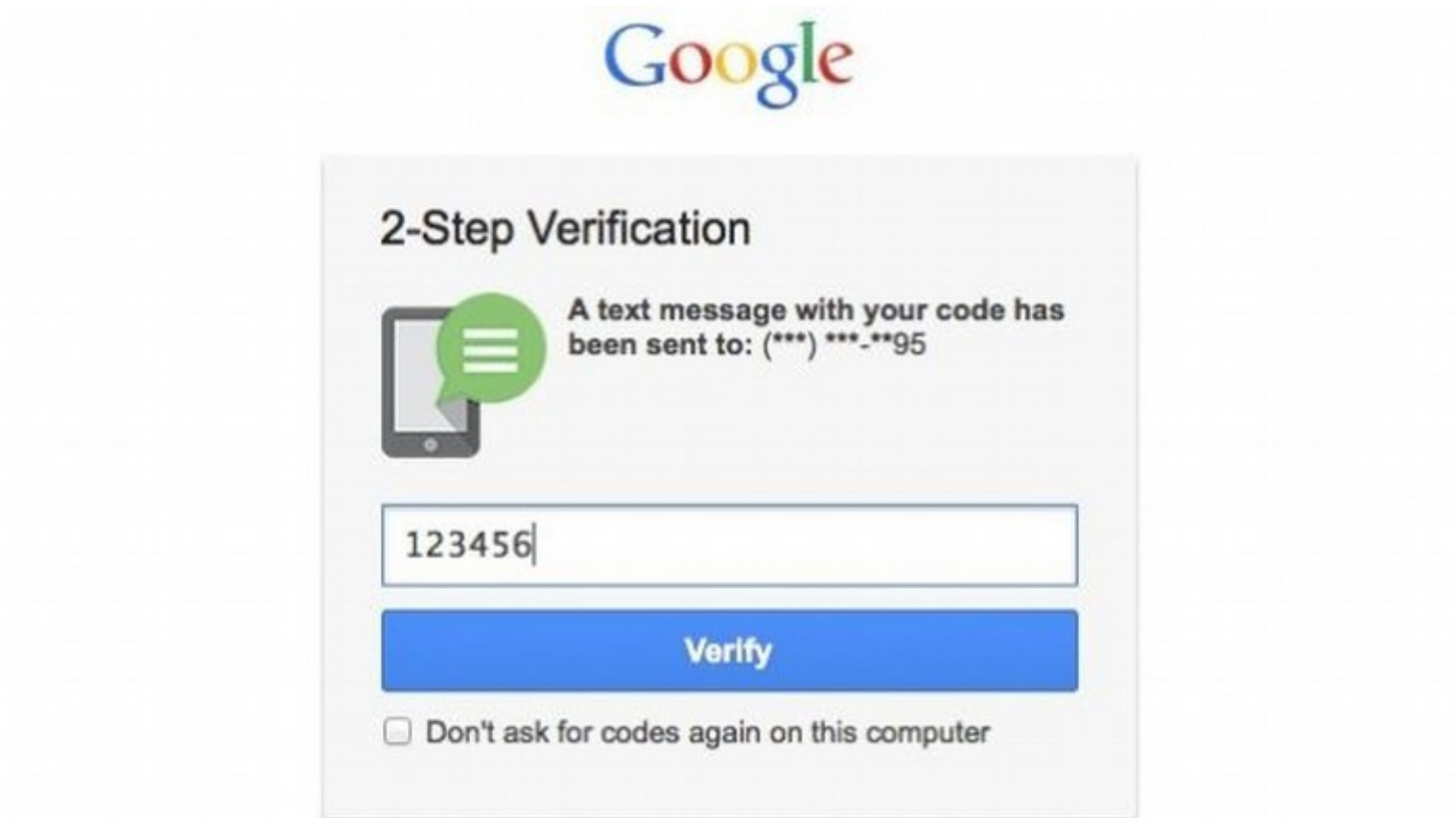
Saltzer and Schroeder's Principles of Secure Design

5) Separation of Privileges

*The system should grant permission
based on multiple conditions.*

Saltzer and Schroeder's Principles of Secure Design

5) Separation of Privileges



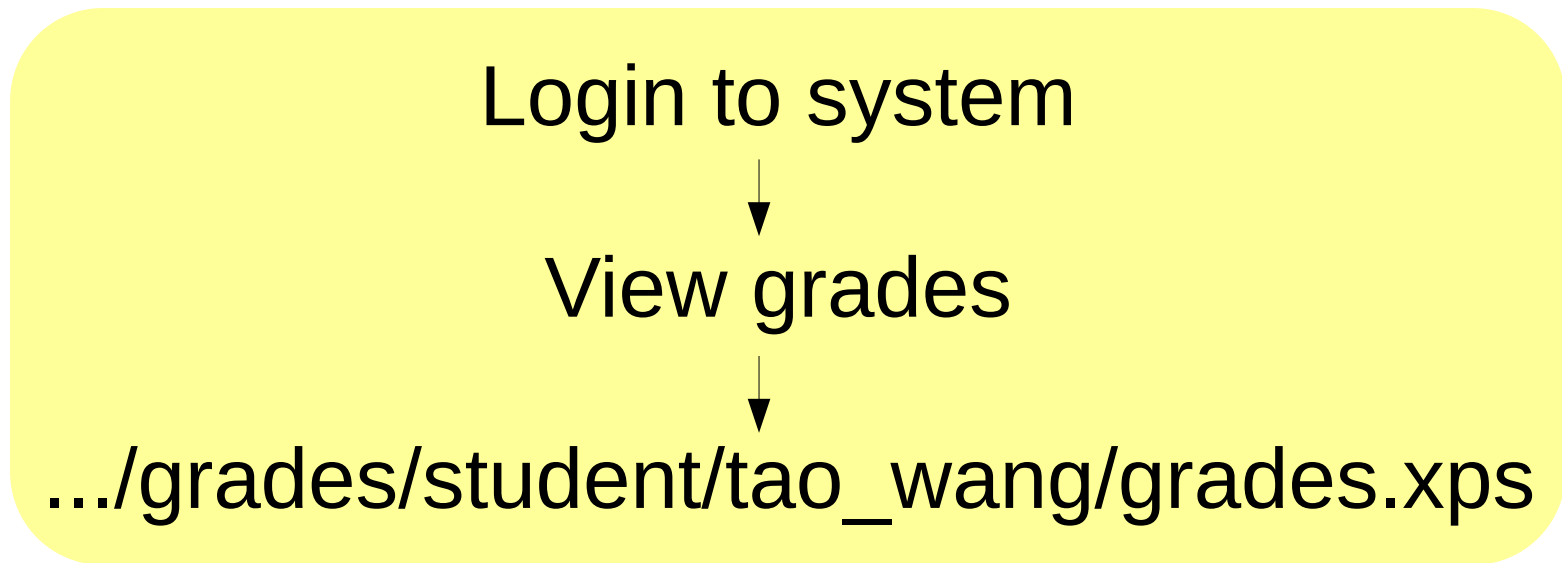
Saltzer and Schroeder's Principles of Secure Design

6) Complete mediation

All accesses should be checked.

Saltzer and Schroeder's Principles of Secure Design

6) Complete mediation



What if we change this?

Related: TOCTTOU, cookie manipulation

Saltzer and Schroeder's Principles of Secure Design

6) Complete mediation

The screenshot shows a web browser window displaying a shopping cart for 'A Clean Well-Lighted Place for Books'. The page includes a header with contact information and navigation links. The main content area shows a table with one item: 'Linux Security for Large-Scale Enterprise Networks' by Becker, Jamieson, priced at \$-59.99. The quantity is set to -1. A 'Total: \$ -59.99' is displayed at the bottom right. The browser's status bar shows 'Done' and 'Internet' with a lock icon. Red and green circles and arrows highlight specific elements: a red circle around the quantity input field labeled 'Insecure software', a red circle around the total price labeled 'Total: \$ -59.99', and a green circle around the lock icon in the status bar labeled 'Secure communications'.

Welcome to A Clean Well-Lighted Place for Books

415-441-6670 www.bookstore.com FAX 415-567-6885

[[Home](#) | [Events](#) | [Features & Recommendations](#) | [Shopping Cart](#)]

A CLEAN WELL-LIGHTED PLACE for BOOKS

Welcome to A Clean Well-Lighted Place for Books

Your Shopping Cart

Qty	Description	Price	Remove
-1	Linux Security for Large-Scale Enterprise Networks Becker, Jamieson 1555582923 Paperback Special Order	\$-59.99	Remove

Home
Events
Book Search
Autographed Books
Remainders 50% off!!
Remainders 60% off!!
Booksense 76

Save Qty Changes [Check Out](#)

Total: \$ -59.99

Done Internet

Insecure software

Secure communications

Saltzer and Schroeder's Principles of Secure Design

7) Fail-safe defaults

Upon failure, the system should revert to a secure default.

Saltzer and Schroeder's Principles of Secure Design

7) Fail-safe defaults

POODLE (Padding Oracle on Downgraded Legacy Encryption):

- SSL was updated to TLS to remove a padding oracle vulnerability
- Clients could force servers to downgrade to SSL again
- Hard to fix because some clients genuinely hadn't updated to TLS (2014)

Saltzer and Schroeder's Principles of Secure Design

8) Psychological Acceptability

Security should be intuitive to the human psyche.

Saltzer and Schroeder's Principles of Secure Design



Your connection is not secure

The owner of cerg1.ugc.edu.hk has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

[Learn more...](#)

Go Back

Advanced

Report errors like this to help Mozilla identify and block malicious sites

cerg1.ugc.edu.hk uses an invalid security certificate.

The certificate is not trusted because the issuer certificate is unknown.
The server might not be sending the appropriate intermediate certificates.
An additional root certificate may need to be imported.

Error code: [SEC_ERROR_UNKNOWN_ISSUER](#)

Add Exception...

Saltzer and Schroeder's Principles of Secure Design

Psychology

Reality

HTTPS

HTTPS

HTTP

Less Secure

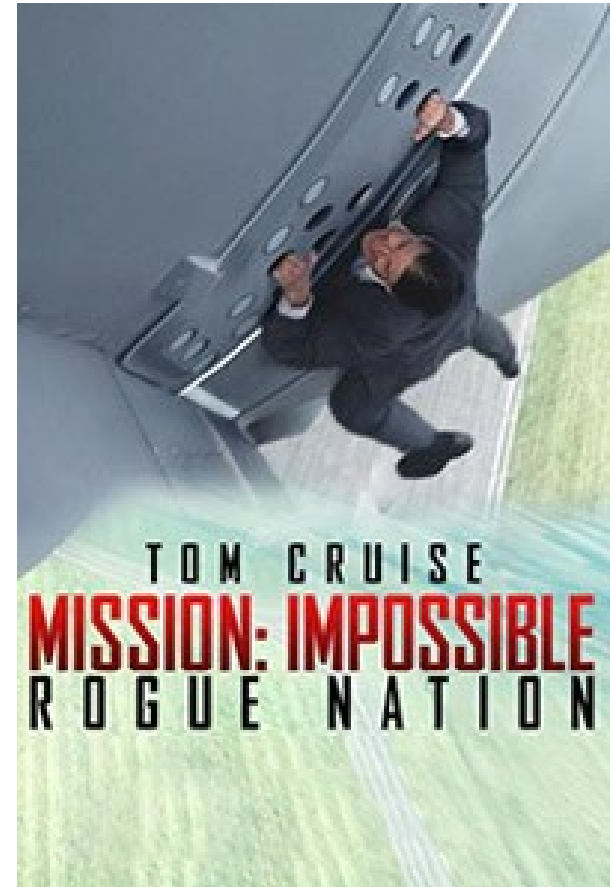
HTTPS with
bad cert

HTTPS with
bad cert

HTTP

Which Principles are Used/Violated?

- Tom Cruise's partner needs to enter a secure facility, which has three combination locks and biometric analysis (fingerprint, gait analysis)
- To put his profile on the system so he can bypass the biometric tests, Tom Cruise dives into a water control system, tears out the old profile drive, and inserts a new profile drive
- Once inside, his partner steals information about 2.4 billion pounds in various bank accounts of the PM



Which Principles are Used/Violated?

- I am scared, so I install the recommended anti-virus. A window pops up asking for admin privileges, I grant it.
- The anti-virus code is not available, so I don't know what it's really doing; I can only trust it
- The anti-virus is actually a virus, and it exploits a buffer overflow in glibc
- glibc is used by all programs written in C; many programs can trigger the virus

