Module 1

Principles of Cybersecurity

So, Canvas is down

How do we analyze a security incident?

- What is the **system under attack**?
- What is the **vulnerability** and **method of attack**?
- What is the **attacker's objective**?
- What **assets** are threatened?
- What are the **defenses** for these assets and why did they fail?

Canvas breach (2026)

- The **system under attack** is Canvas, learning management software
- The **vulnerability and attack** is so far unknown, but probably involves social engineering

> [ShinyHunter's] operations primarily leverage sophisticated **voice phishing (vishing)** and **victim-branded credential harvesting sites** to gain initial access to corporate environments by obtaining single sign-on (SSO) credentials and multi-factor authentication (MFA) codes.
>
> *(Mandiant Google report on ShinyHunters, January 2026)*

Canvas breach (2026)

- The attacker's **objective** is to threaten data leakage for ransom
- The **asset** being threatened is the privacy of millions of students and teachers
  - Or, Canvas's reputation
- The defenses' weaknesses are unclear, but probably involved poor MFA practices and excessive data access

Another security incident…

- Bitstamp compromise (2015)
- Around 10,000 bitcoins drained from company hot wallet
- Recovery was not possible
- Six employees received highly targeted scam e-mails tailored to their specific interests
- Each attachment had a VBA script that was run automatically and would download and run malicious software

Bitstamp compromise (2015)

- What is the **system under attack**?
- What is the **vulnerability** and **method of attack**?
- What is the **attacker's objective**?
- What **assets** are threatened?
- What are the **defenses** for these assets and why did they fail?

This course's challenge

Security is multi-faceted.

- Networks, software, hardware, data, crypto, …
- Since the attacker only needs to find the weakest point, we need to understand all involved technologies

CMPT 403

Class times: Wed 3:30-4:20 PM
Fri 2:30-4:20 PM

Grading

30%	3x Assignments
25%	Mid-term Exam
15%	Assignment-based Quiz
30%	Final Exam

Assignments

Each Assignment has a:

- Written Component

- Programming Component

A grace period can be considered for serious issues. You must e-mail me at least 48 hours before the deadline to request a grace period.

Otherwise, late submissions will receive a penalty (~10% per day).

Contact

E-mail: taowang@sfu.ca

Please preface your e-mail title with “CMPT403”.

Any questions are welcome!

Principles of CIA

Confidentiality

Information is secret

Integrity

Information/System is correct

Availability

System is usable

Principles of CIA

- Distributed Denial of Service (DDoS)
  - The attacker used a botnet of IoTs (Mirai) that was created by guessing trivial passwords
  - Another attacker (AISURU) uploaded a malicious firmware update for Totolink routers

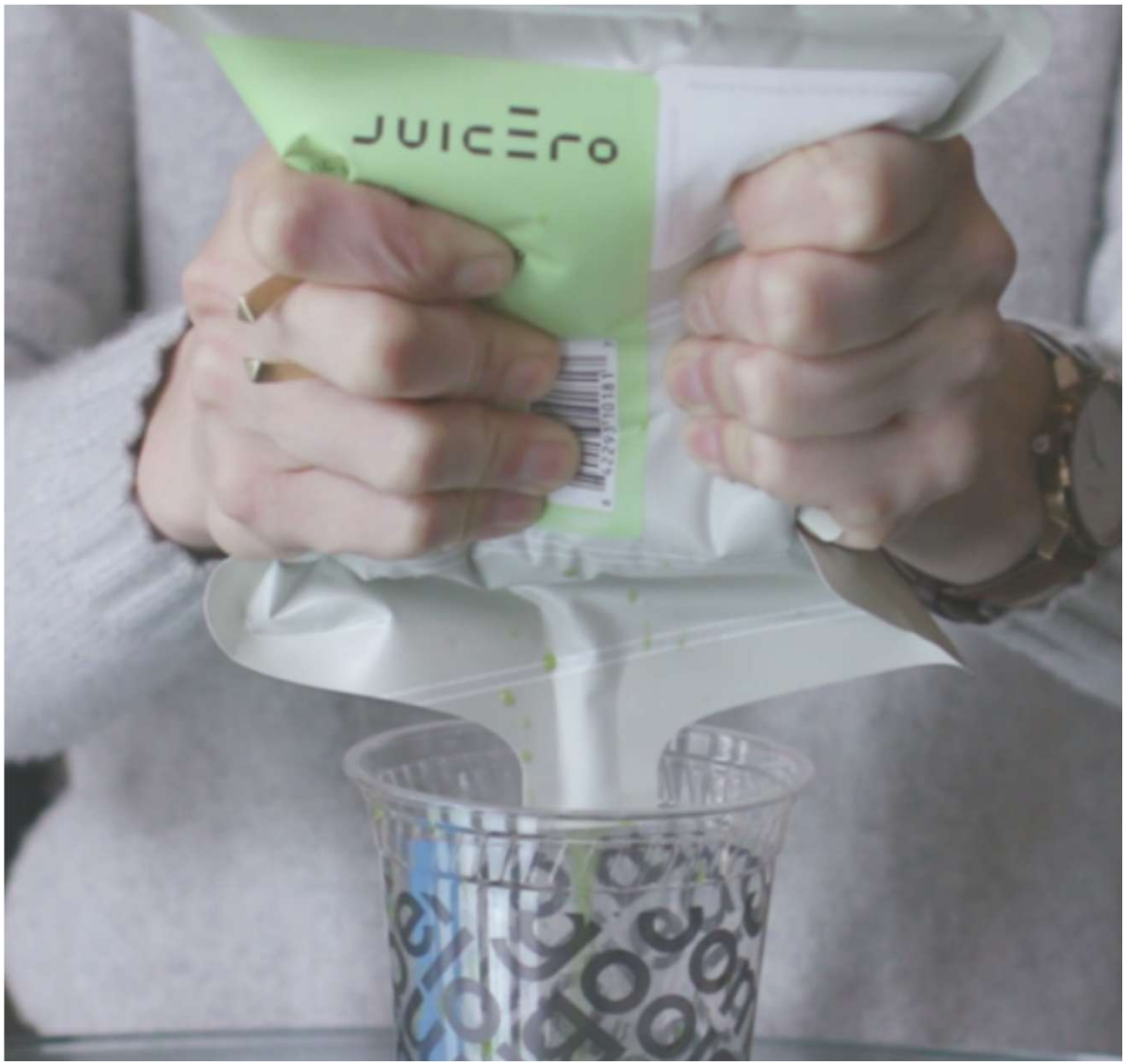
Which principle is violated?
(Confidentiality, Integrity, Availability)

Security by design

- Implementation vulnerabilities are common and more easily patched, but design issues are fundamental
- Design flaws:
  - Wrong threat model
  - Wrong user model
  - Security was not considered
  - Intentional insecurity

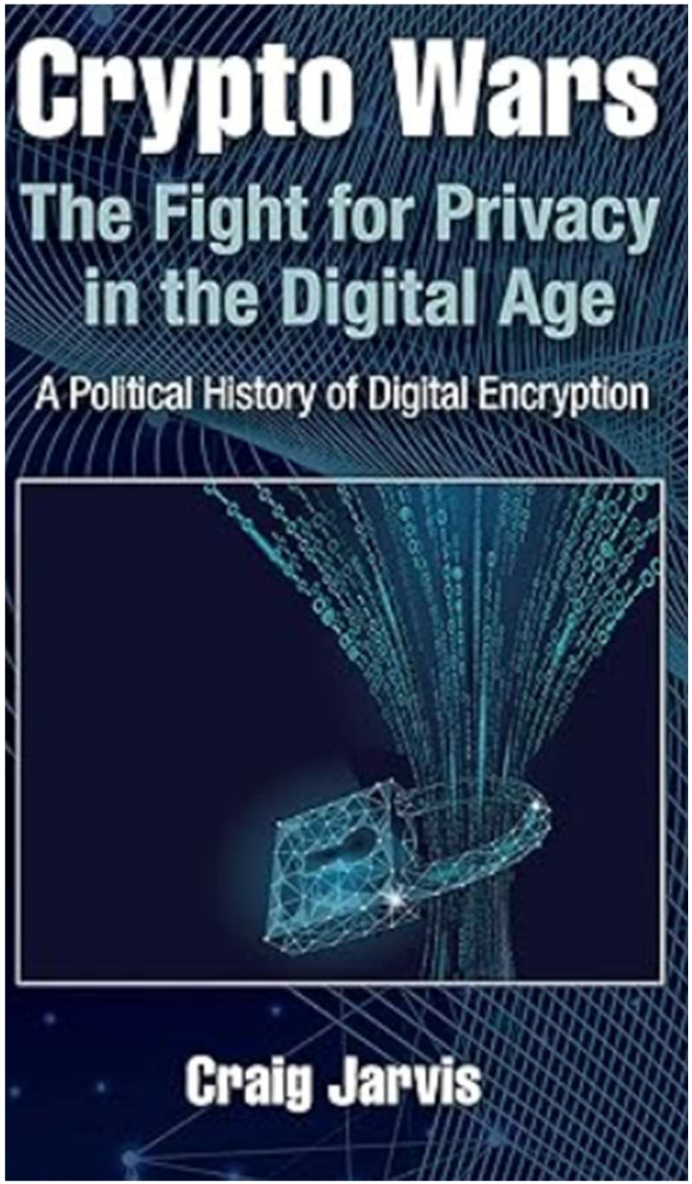
Wrong threat model: a juicer…

Wrong threat model: a juicer…



Wrong user model

Intentional Insecurity



Threat Modeling - STRIDE

Spoofing
Acquiring fake identity

Tampering
Modifying information/code

Repudiation
Erasing past actions

Information leak
Data leakage, breach

Denial of Service
Harming availability

Escalation of Privilege
Gaining permissions/root

Spiderman Rule

With great power
comes great responsibility!

Principles of Secure Design

Security by Design:

Security should be considered starting from the design phase

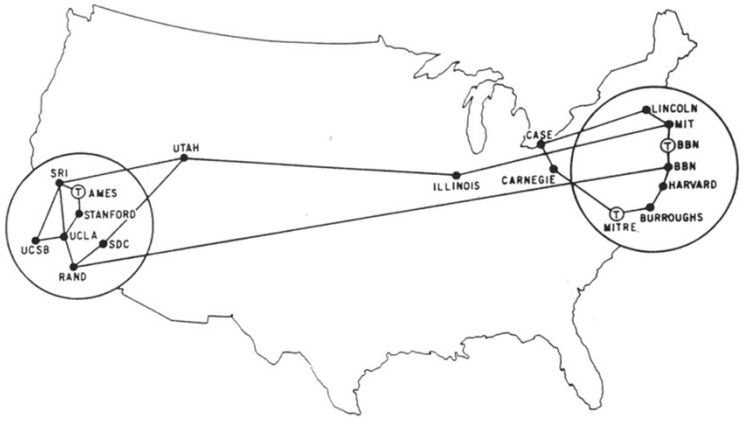
(Vulnerabilities should be considered starting from the design phase)

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

Principles of Secure Design

Adapted from Saltzer and Schroeder's Principles:

1) The System's design should be open and simple
2) Failure should be expected, safe, and recoverable
3) Always remember the human element

1) Open and Simple Design

Do not rely on Security through Obscurity:

Hide details of the implementation
to prevent compromising analysis

1) Open and Simple Design

Examples of Security through Obscurity:

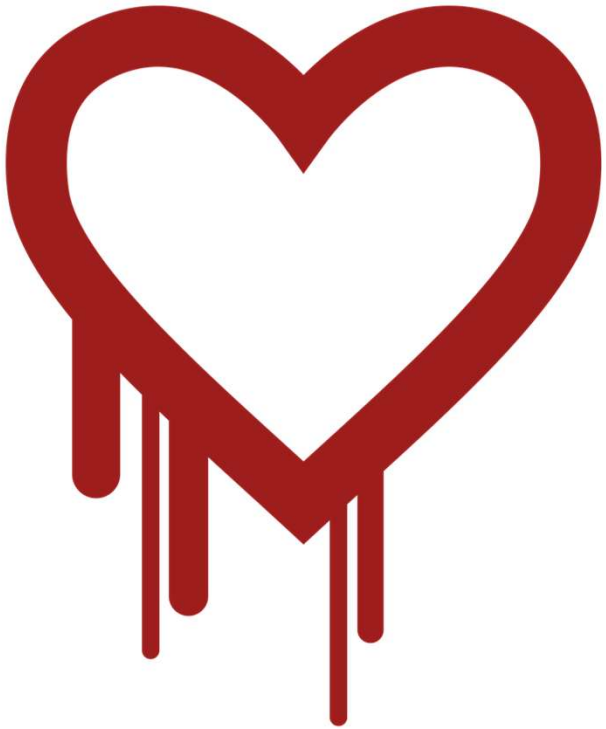
- Terms of Service + lawsuits barring reverse engineering
- Cryptosystems where the algorithms are secret
- Closed-source code

1) Open and Simple Design

“Given enough eyeballs, all bugs are shallow”

-- Linus Torvalds

1) Open and Simple Design

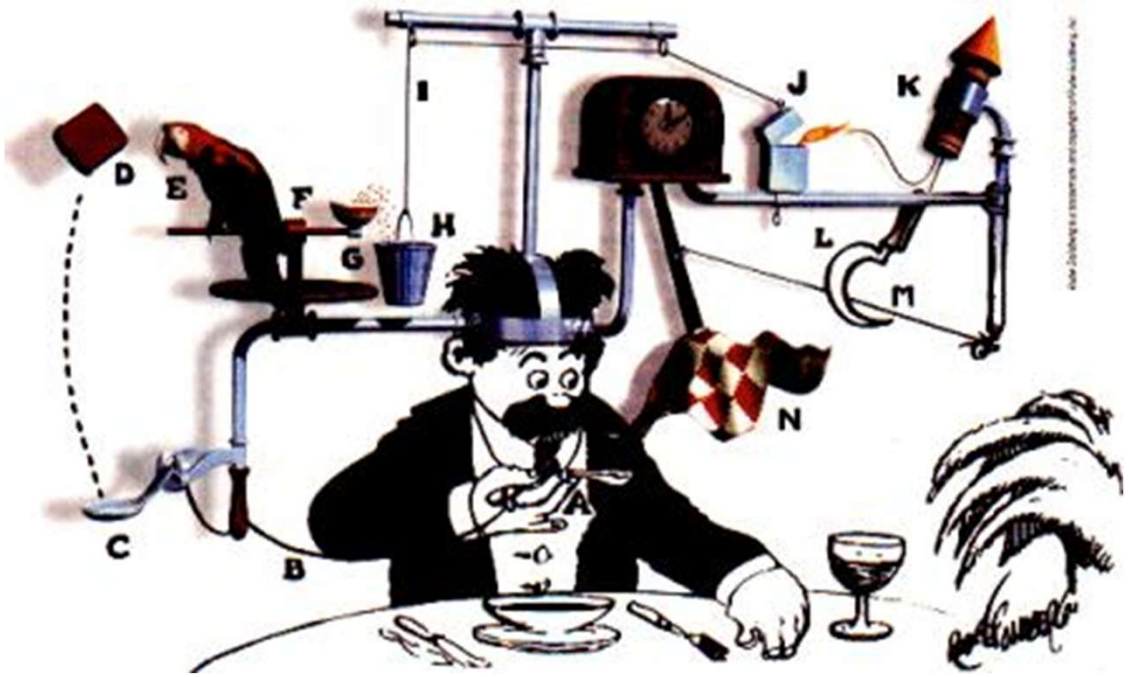


Heartbleed (2014):
Serious open-source software bug

Should we pay the eyeballs to look?

1) Open and Simple Design

KISS Principle: Keep it simple/stupid



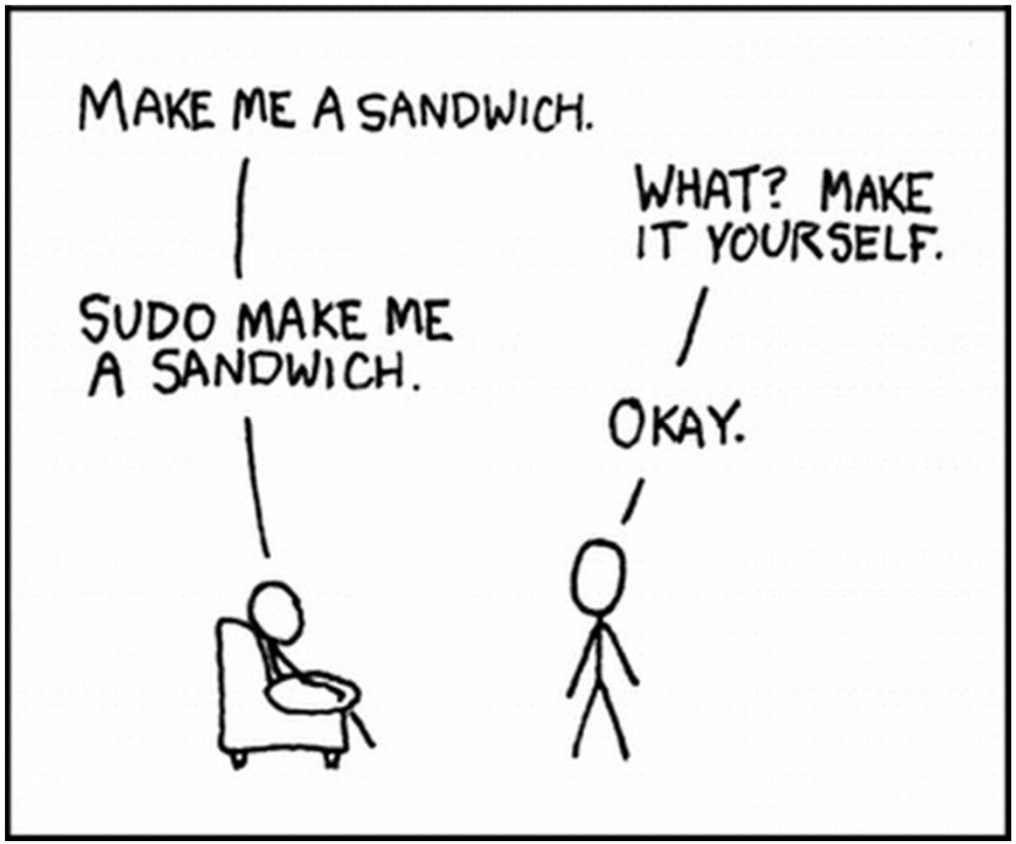
2) Safe and Recoverable Failure

Minimize the damage caused by a failure or compromise

Examples:

- Distributed databases, backups
- Minimize privileges (root access)
- Logging, monitoring

2) Safe and Recoverable Failure



2) Safe and Recoverable Failure

SSL Downgrade Attack:

- SSL 3.0 upgraded to TLS 1.0 after discovery (and publication!) of vulnerability
- Attacking client, masquerading as victim: “Sorry, I don’t speak TLS 1.0. Can we use SSL 3.0?”
- Victim establishes SSL 3.0 connection with server, attacker breaks it
- Default is not secure

3) The Human Element

"Humans are the weakest link in any security system"

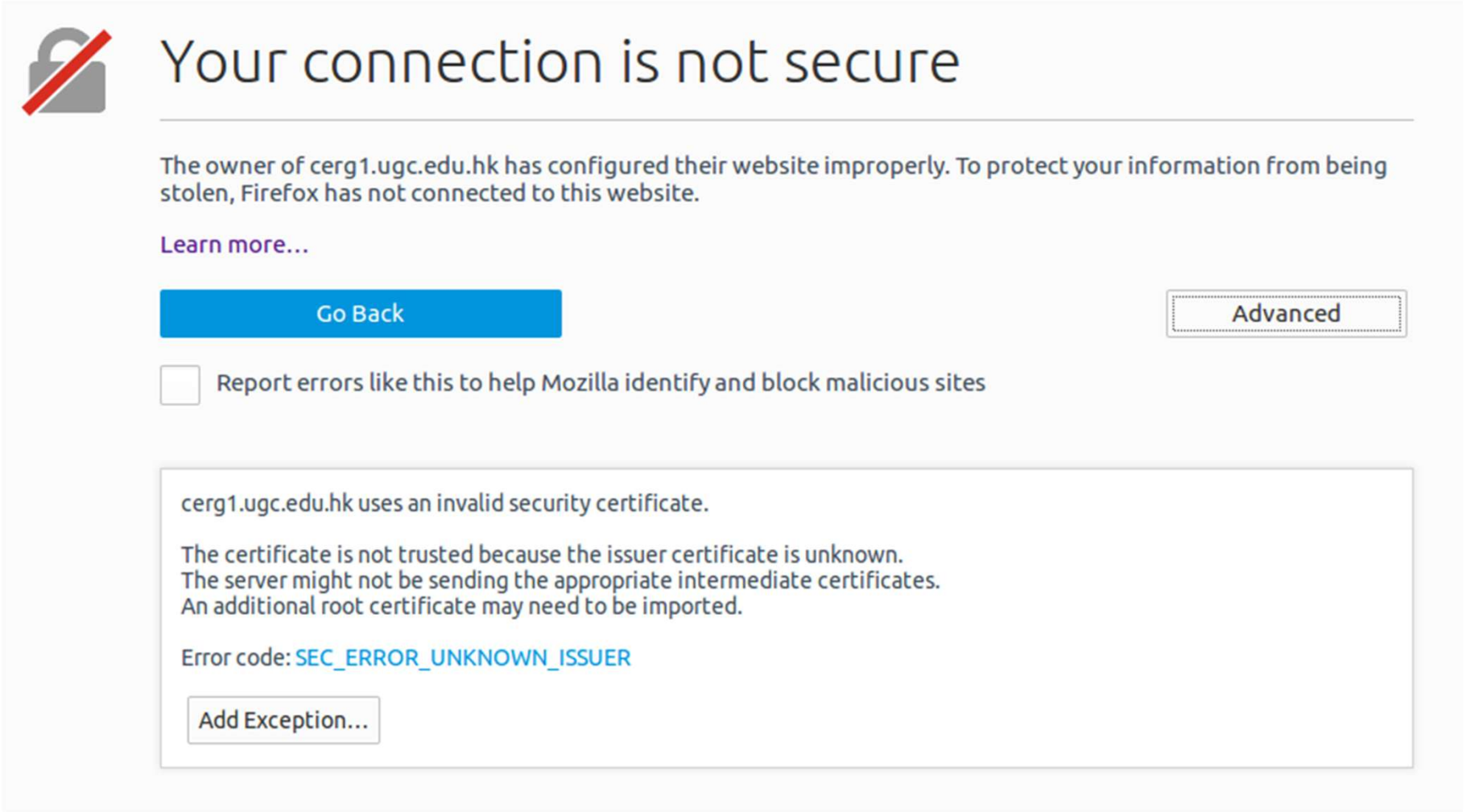
- Almost all modern attacks have an element of social engineering (e.g. "spear phishing")
- It is difficult to communicate security information
- It is difficult to understand humans

3) The Human Element

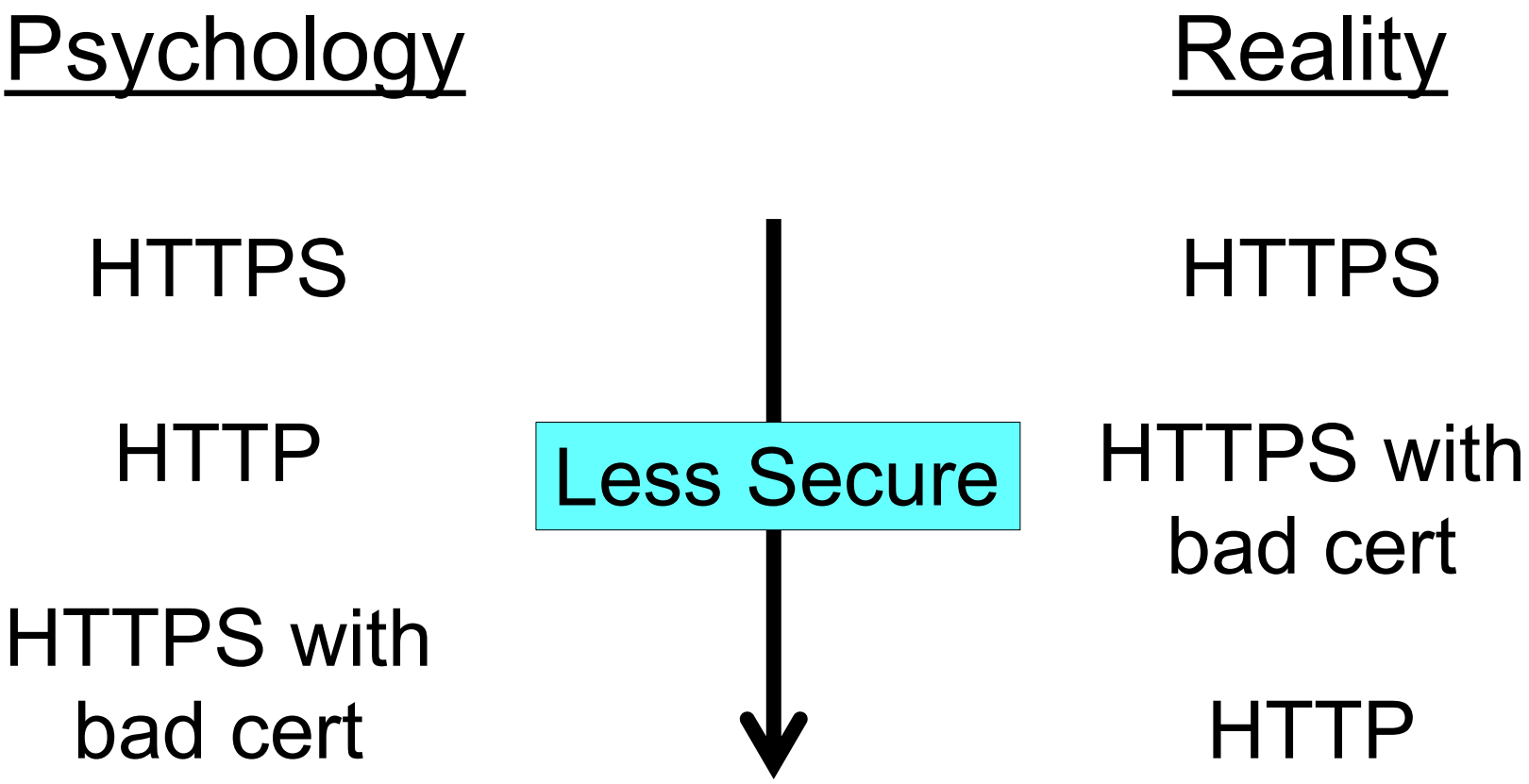
Security should be intuitive to the human psyche.

- The secure choice should be the psychologically acceptable one
- “Android is asking you for the following permissions…”
- Trivially spoofable “identifiers”

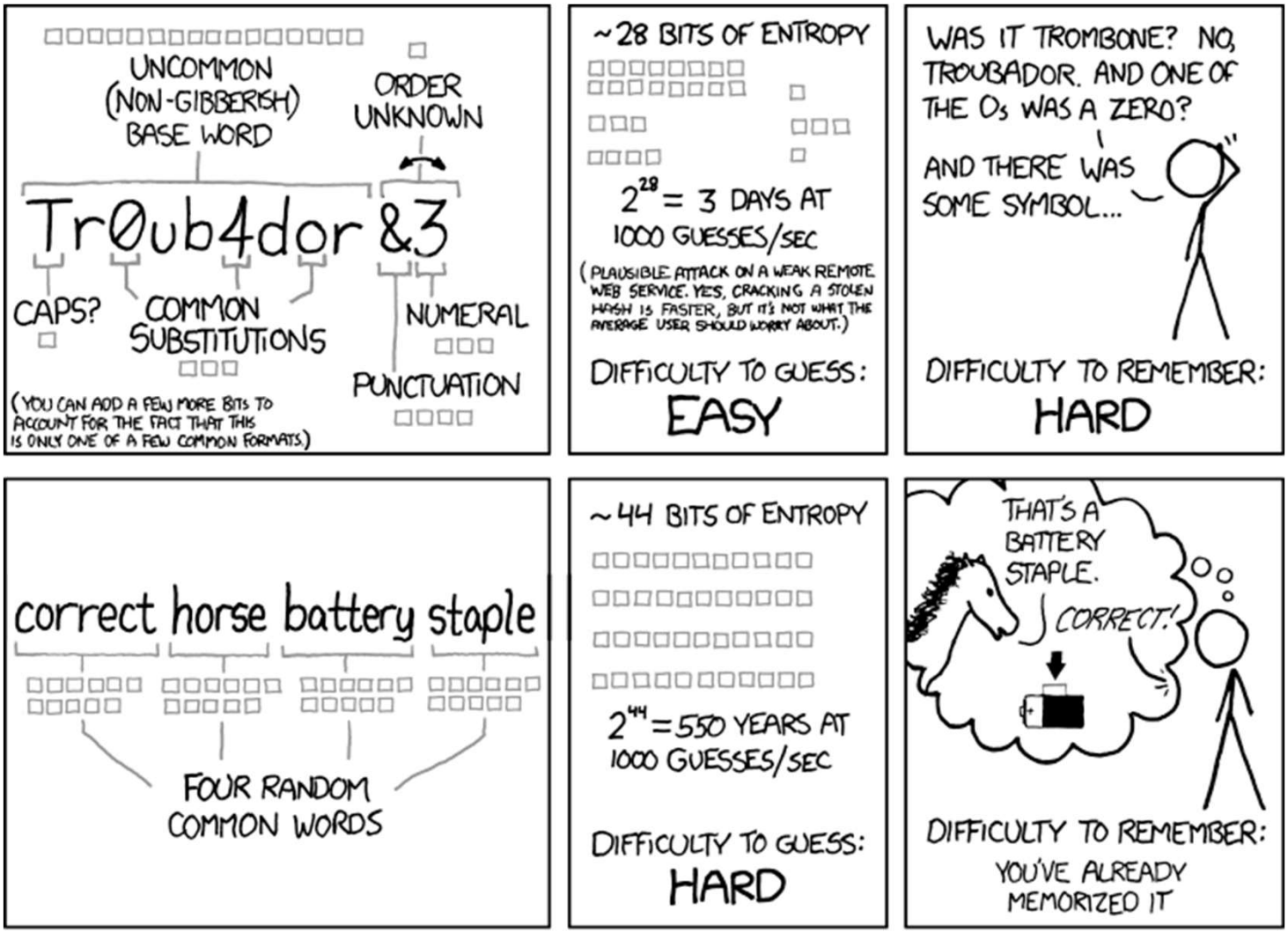
3) The Human Element



3) The Human Element



3) The Human Element



3) The Human Element

The other side of the equation:
the attacker is human too.

Think like an attacker!

- The attacker will not expend too much effort or take too much risk for too little gain.
- The attacker can and will frequently make mistakes, exposing their attack.
- The attacker will choose easy targets if they are available.
- Attacks can have vastly different profiles and strategies

Let’s analyze with security principles

What principles were possibly violated in the Canvas breach?

- Privileges were not minimized; credentials for someone with access to all data was stolen
- It is possible someone fell for a social engineering attack
- Data exfiltration monitoring did not trigger/exist
- Even now, Canvas relies on Obscurity
  - A vast amount of information was protected by unknown defenses

An important question…

Is Computer Security Science?

- What is science?
- Is mathematics science?
- **Should** computer security be science?
- Should computer security learn from physics?

Let’s talk about security incidents

Office of Personnel Management breach (2015)

Results:

- 22 million highly personal records of government employees
- Including 5.6 million fingerprints
- US accuses China of attack
- Washington Post reports that US spies were recalled from C

Incident details

Method of attack

- Two related attacks: OPM falsely believed and announced
- **Social engineering** was involved
- OPM noted for using **old, unpatched** OS's
- "mcutil.dll" (McAfee security dll file) was exfiltrating data to
- Poor security practices noted – many employees had **root**

Incident analysis

Questions to ask:

- What are the vulnerabilities exploited by the attacker?
- How can the vulnerabilities be patched?
- What changes should be made?
- How might the attacker evolve their strategy in response to