Module 1

Principles of Cybersecurity

Let’s talk about security incidents

Bitstamp compromised (2015)

Results:

- Around 19,000 bitcoins drained from company hot wallet into unknown wallet
- Recovery was not possible
- Attacker remains unknown

Incident details

Method of attack

- Six employees received **highly targeted scam e-mails** tailored to their specific interests
  - One received a concert ticket to Punk Rock Holiday 2015
  - One received an invitation to join ACM’s International Honour Society
- Each attachment had a **VBA script** that was run automatically and would download and run malicious software
- Microsoft Security Essentials prevented two attacks

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 our changes?

  Very similar attacks: 2020 Twitter hack, Bitfinex hack, etc.

Let’s talk about security incidents

Office of Personnel Management breach (2015)

Results:

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

Incident details

Method of attack

- Two related attacks: OPM falsely believed and announced that first attack was defeated
- **Social engineering** was involved
- OPM noted for using **old, unpatched** OS’s
- “mcutil.dll” (McAfee security dll file) was exfiltrating data to “opmsecurity.org”, registered under “Tony Stark”
- Poor security practices noted – many employees had **root access** to all data, poor **security monitoring**

Incident analysis

Questions to ask:

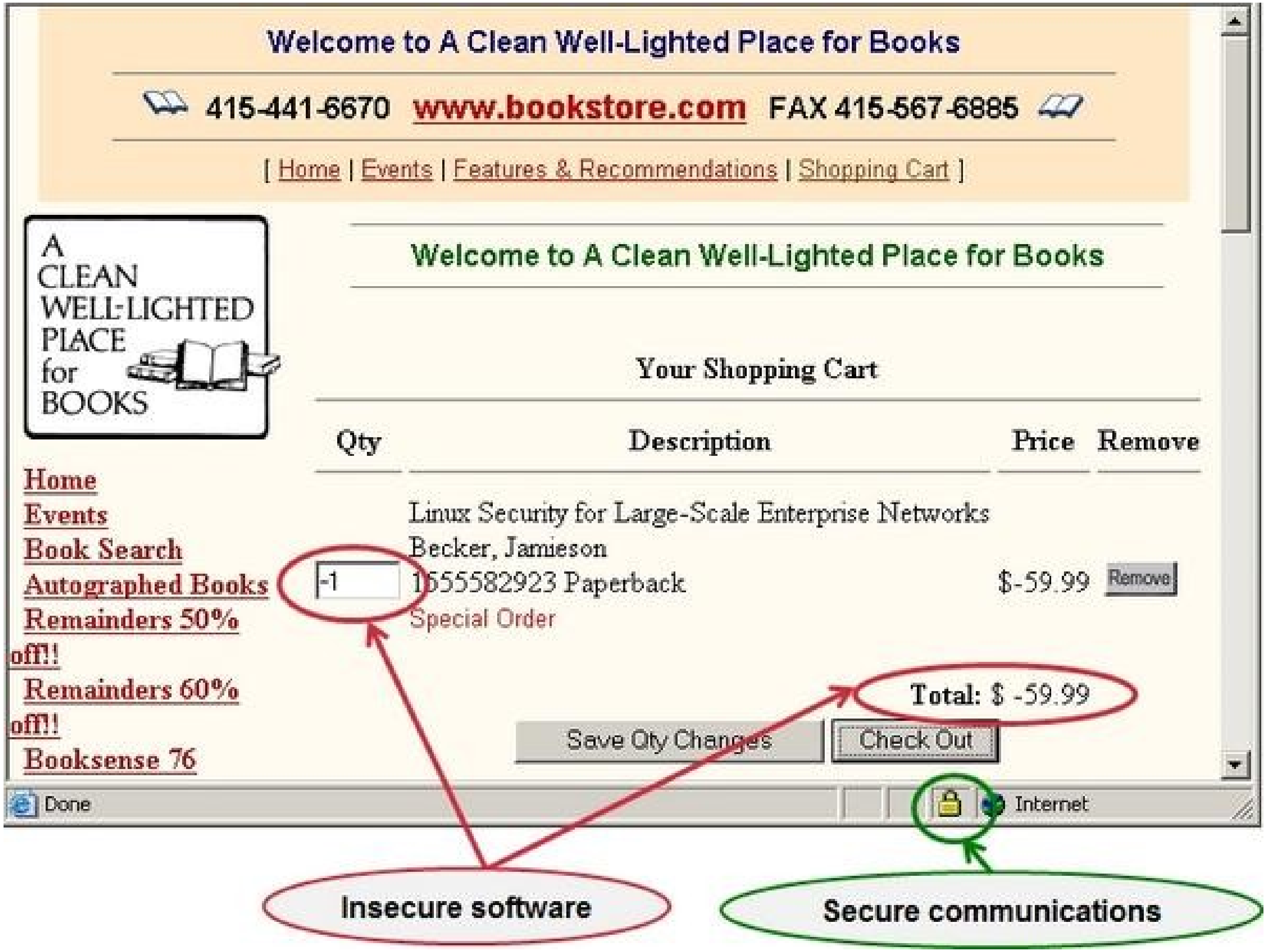
- What are the vulnerabilities exploited by the attacker?
- How can the vulnerabilities be patched?
- What changes should be made?
- How might the attacker evolve their strategy in response to our changes?

This course’s challenge

Security is multi-faceted.

- Networks, software, hardware, data, crypto, ...
- Since the attacker only needs to find the weakest point, the defense needs to understand **all** relevant technologies

This course’s challenge



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

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

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

Total: $ -59.99

Insecure software

Secure communications

CMPT 403

Class times:	We 1:30-2:20, Fr 12:30-2:20
TA:	Alireza Ali Sam
Place:	WMC3260

Grading

45%	3x Assignments (15%)
25%	Mid-term Exam
30%	Final Exam

Assignments

Each Assignment has a:

- Written Component

- Programming Component

You may obtain a grace period of exactly 48 hours at no penalty by e-mailing me with any reason before the due date.

A further grace period can be considered for serious issues. E-mail me early to discuss.

Otherwise, late submissions may receive a penalty or a 0.

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)

- Money was stolen from an online exchange

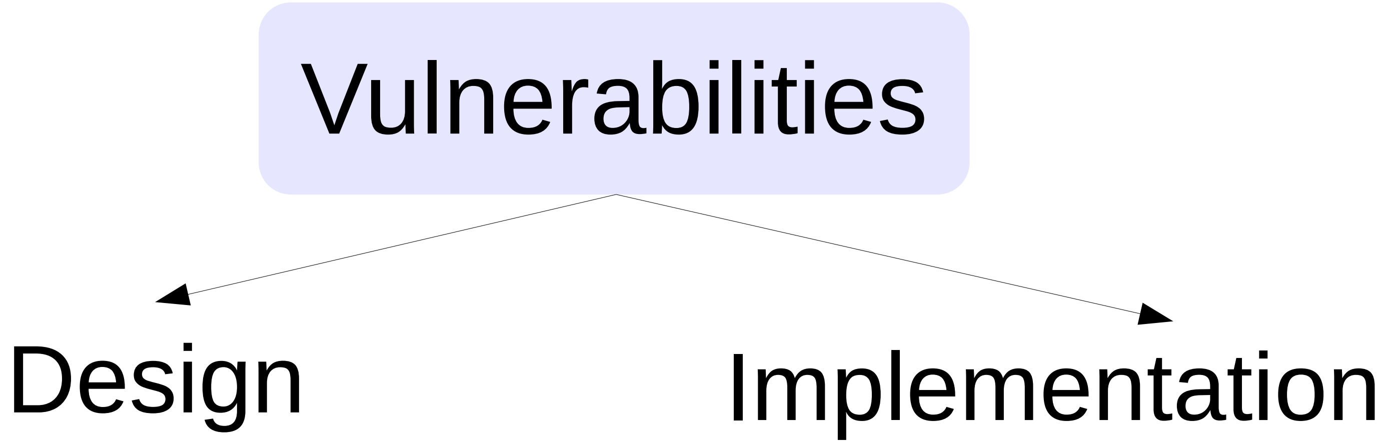
Which principle is violated?
(Confidentiality, Integrity, Availability)

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?



Vulnerabilities

Design

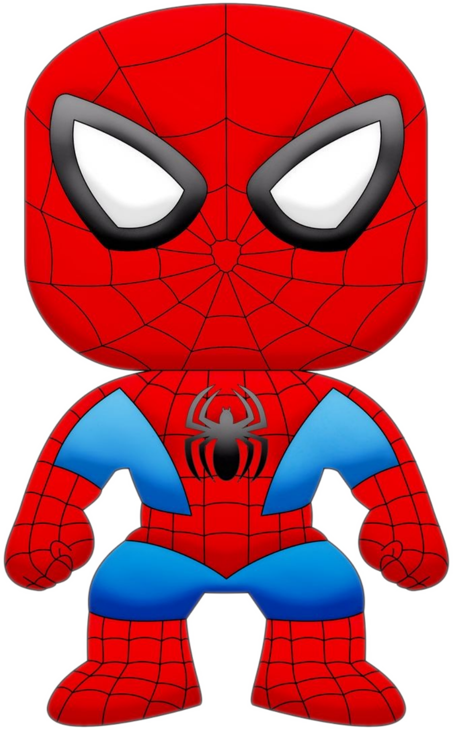
Implementation

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

Errors in coding, hardware;
Intentional errors, etc.

Spiderman Rule

With great power
comes great responsibility!



Principles of Secure Design

Security by Design:

Security should be considered starting from the design phase

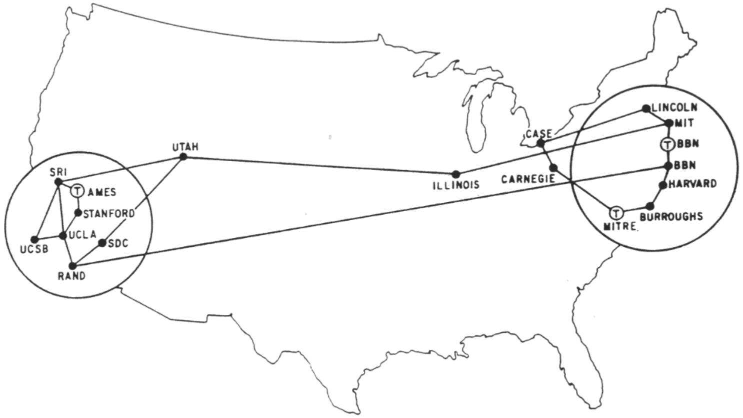
(Vulnerabilities should be considered starting from the design phase)

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)



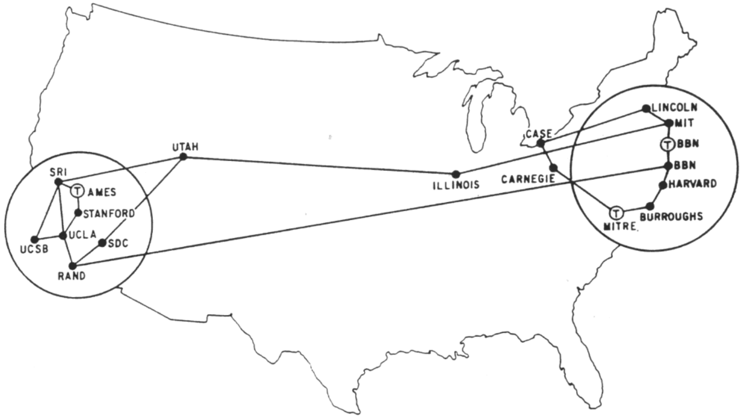
MAP 4 September 1971

Principles of Secure Design

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

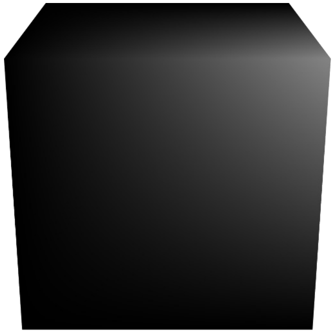
Adapted from Saltzer and Schroeder’s Principles:

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

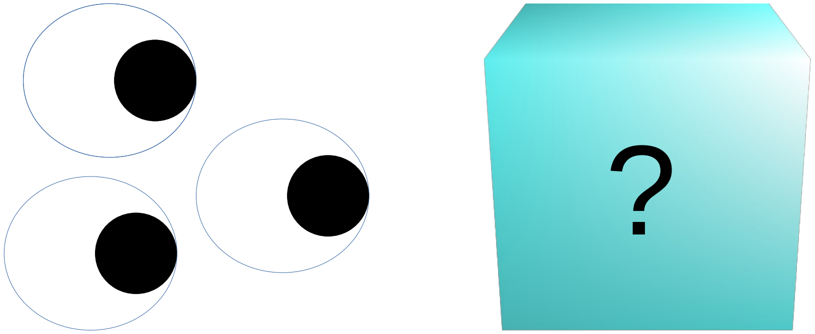
- Cryptosystems where the algorithms are secret

- Closed-source code

1) Open and Simple Design

“Given enough eyeballs, all bugs are shallow”

-- Linus Torvalds



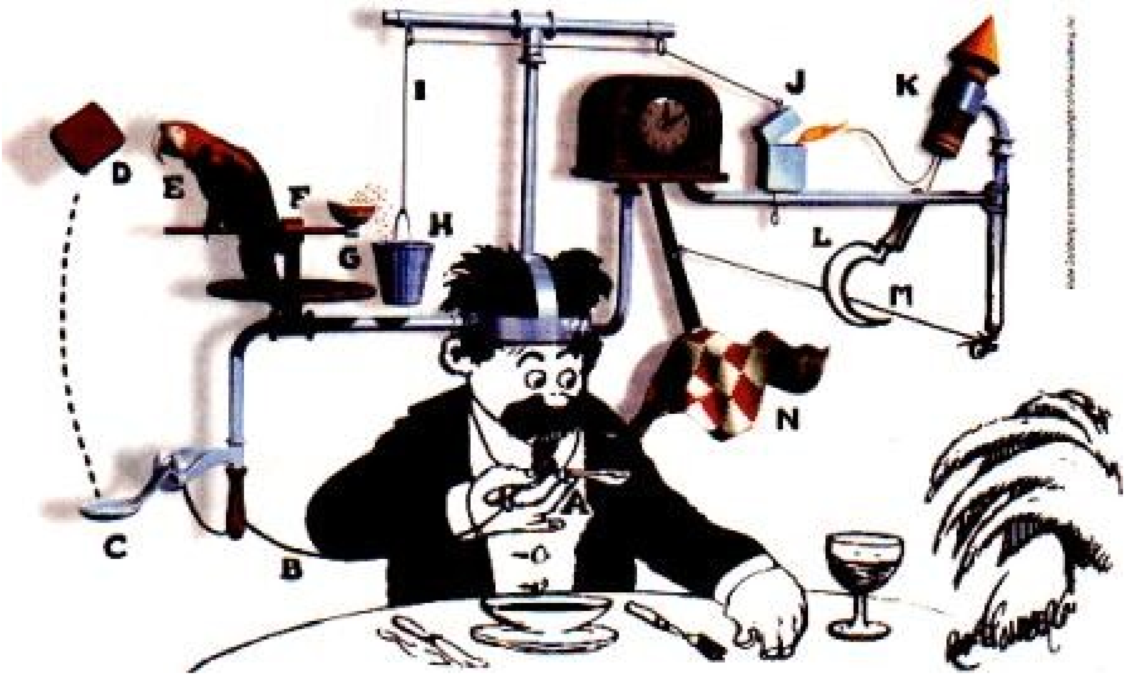
1) Open and Simple Design

Heartbleed (2014):
Serious open-source software bug

“The eyeballs weren’t looking”

1) Open and Simple Design

KISS Principle: Keep it simple/stupid



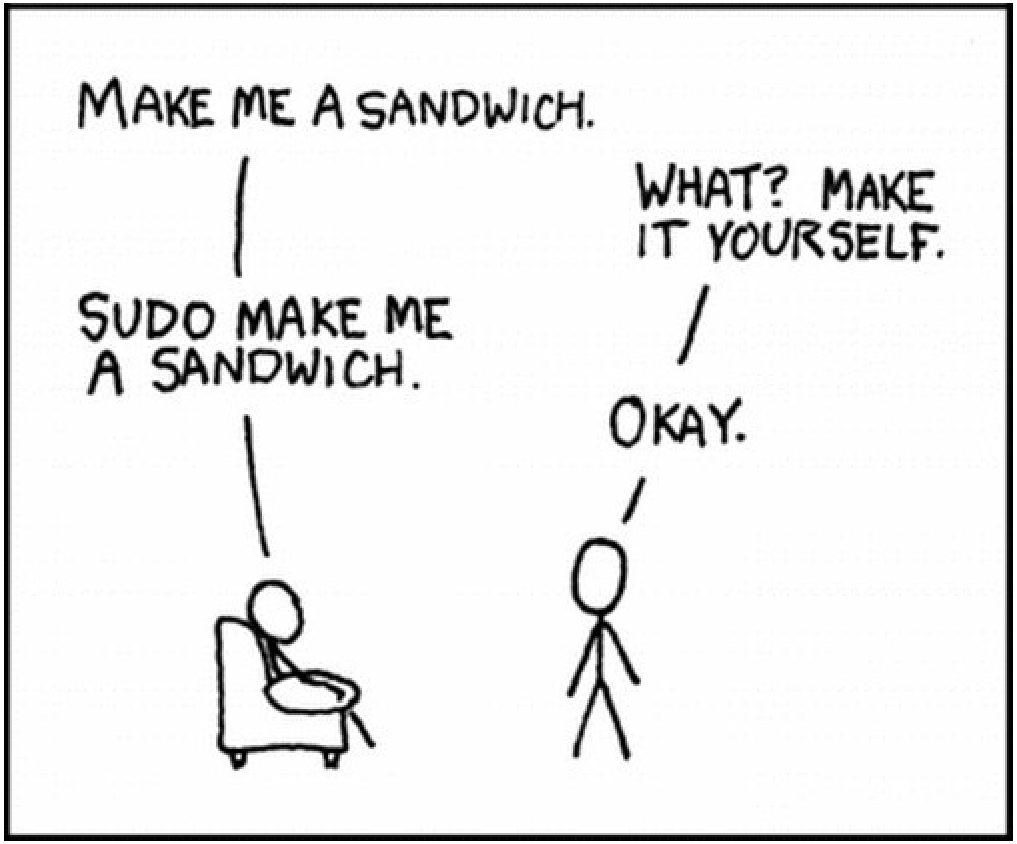
2) Safe and Recoverable Failure

Minimize the damage caused by a failure or compromise

Examples:

- Distributed databases, backups
- Minimize access to root
- Logging

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”

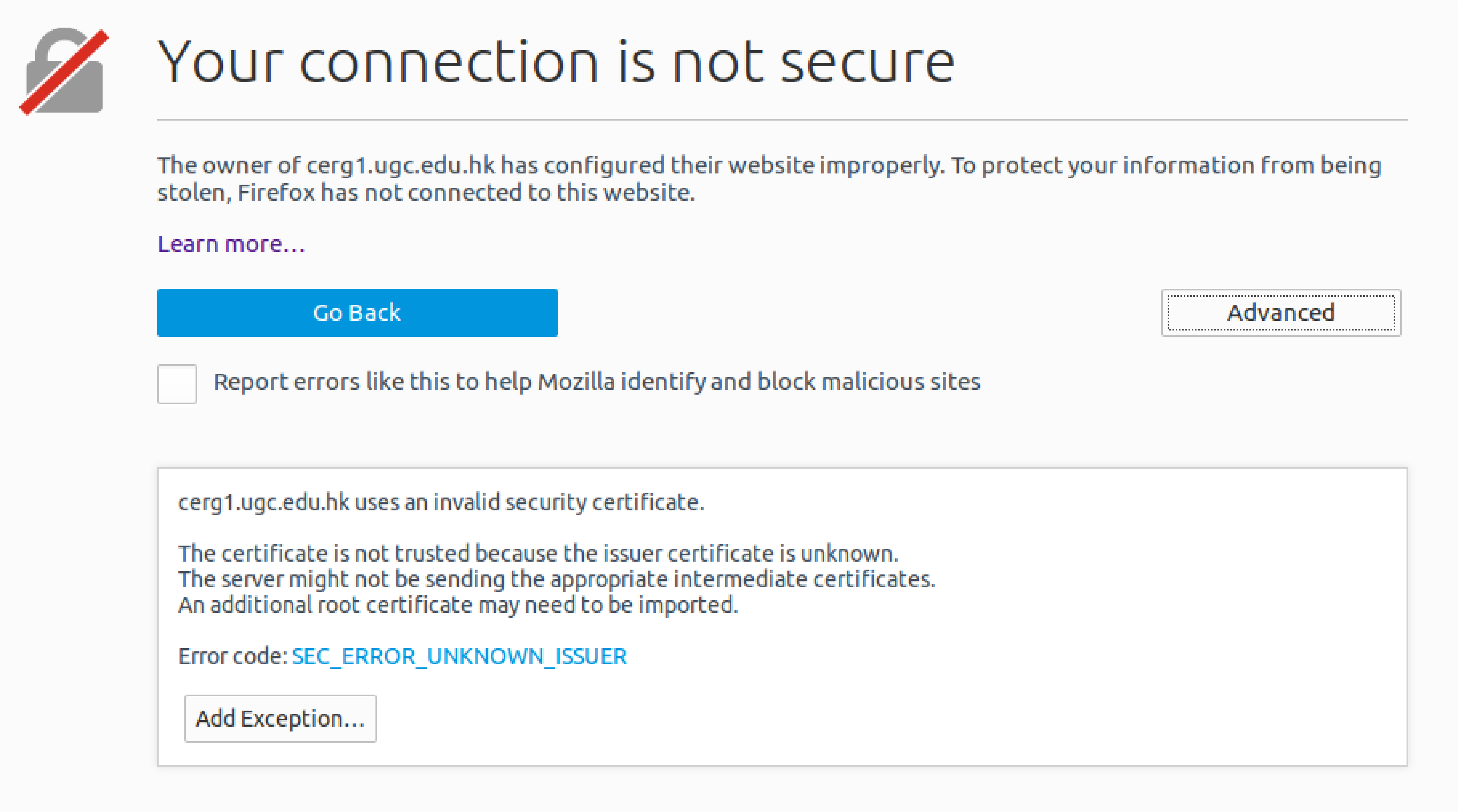
- Almost all modern attacks have an element of social engineering (e.g. “spear phishing”)
- A system that relies on human perfection is an insecure system

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 that people do not know are spoofable

3) The Human Element



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…

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

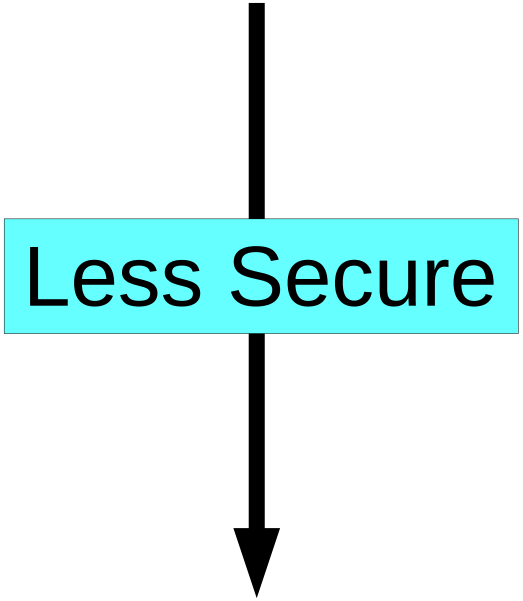
cerg1.ugc.edu.hk uses an invalid security certificate.

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

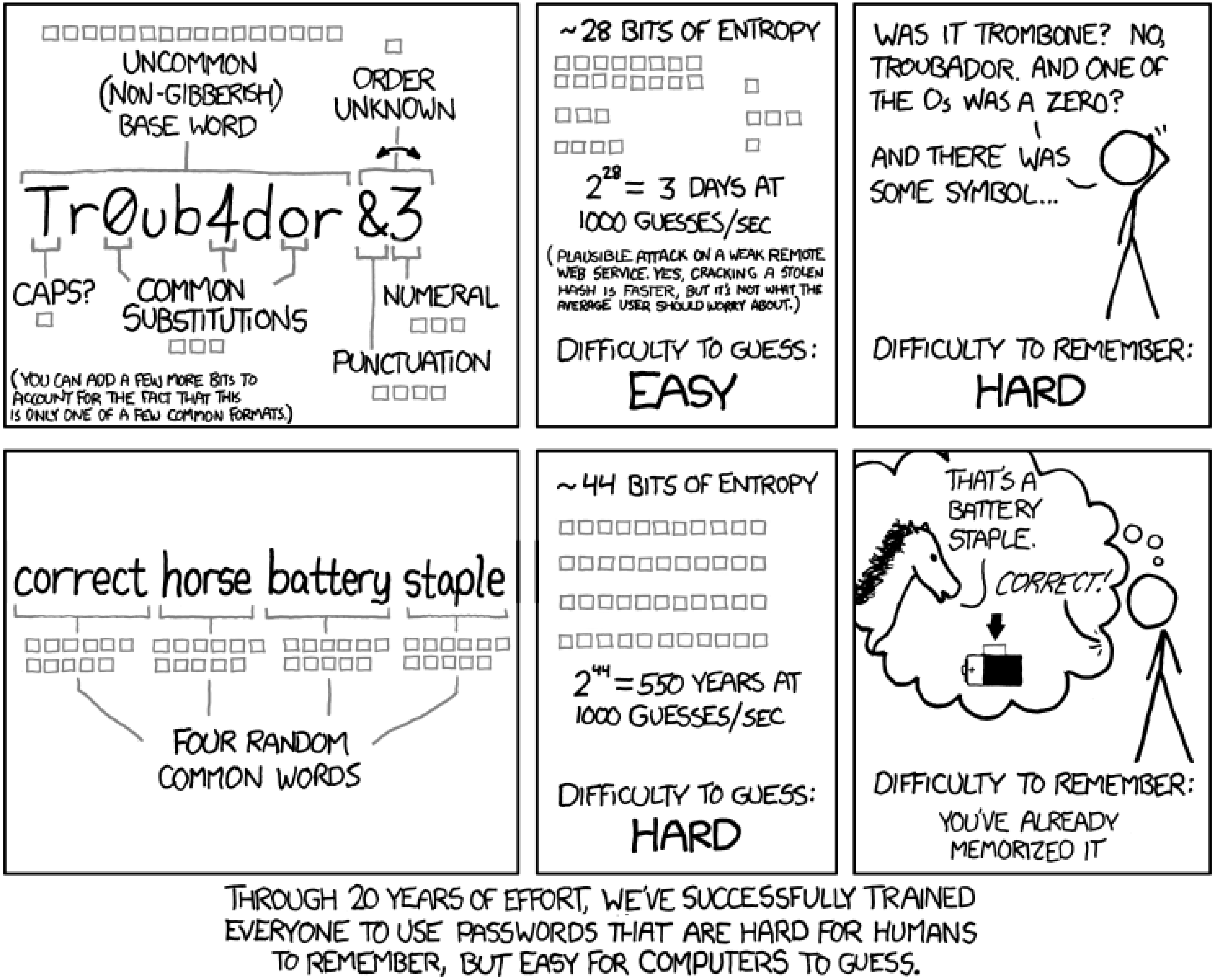
3) The Human Element

Psychology	Reality
HTTPS	HTTPS
HTTP	HTTPS with bad cert
HTTPS with bad cert	HTTP



Less Secure

3) The Human Element


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

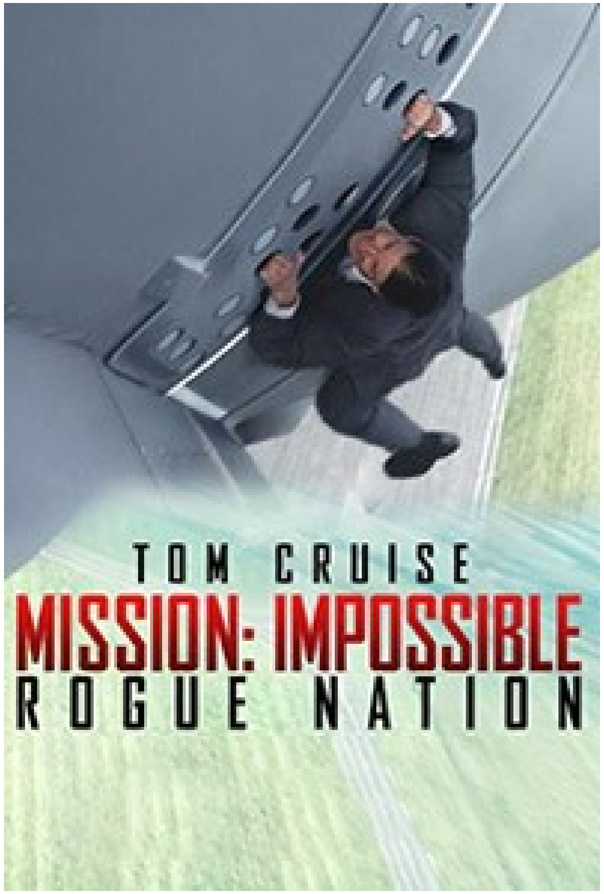
3) The Human Element

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.

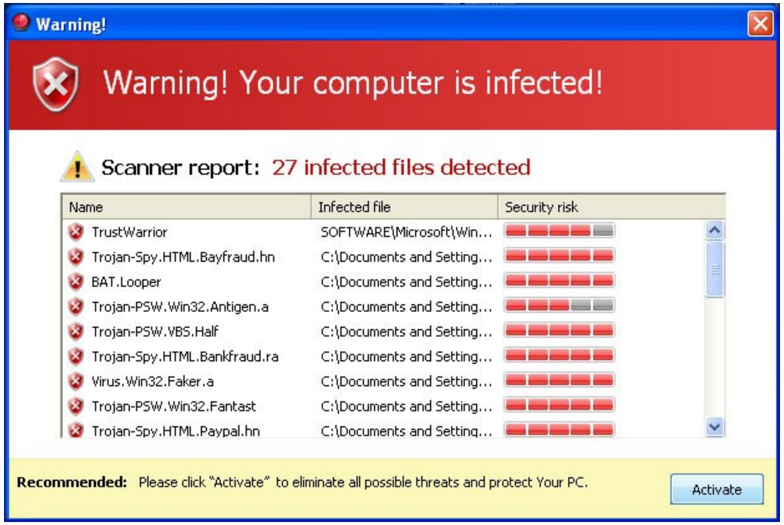
Let’s analyse with security principles

- 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



Let’s analyse with security principles

- 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
- The buffer overflow uses libc functions to escalate privileges



Warning!

Warning! Your computer is infected!

Scanner report: 27 infected files detected

Name	Infected file	Security risk
TrustWarrior	SOFTWARE\Microsoft\Win...	🟥🟥🟥🟥⬜
Trojan-Spy.HTML.Bayfraud.hn	C:\Documents and Setting...	🟥🟥🟥🟥🟥
BAT.Looper	C:\Documents and Setting...	🟥🟥🟥🟥🟥
Trojan-PSW.Win32.Antigen.a	C:\Documents and Setting...	🟥🟥🟥⬜⬜
Trojan-PSW.VBS.Half	C:\Documents and Setting...	🟥🟥🟥🟥🟥
Trojan-Spy.HTML.Bankfraud.ra	C:\Documents and Setting...	🟥🟥🟥🟥🟥
Virus.Win32.Faker.a	C:\Documents and Setting...	🟥🟥🟥🟥🟥
Trojan-PSW.Win32.Fantast	C:\Documents and Setting...	🟥🟥🟥🟥🟥
Trojan-Spy.HTML.Paypal.hn	C:\Documents and Setting...	🟥🟥🟥🟥🟥

Recommended: Please click “Activate” to eliminate all possible threats and protect Your PC.