WEEK 1

SECURITY GOALS AND PRINCIPLES

SE 4472 - Information Security

Western Engineering

WHISPER LAB

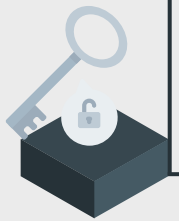
CYBERSECURITY

The practice of protecting computers, servers, mobile devices, networks and data from unauthorized, disclosure, access and modification

CYBERSECURITY

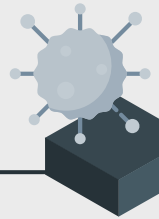
INFORMATION SECURITY

Protecting information with cryptography and secure communication protocols



SOFTWARE SECURITY

Preventing the exploitation of vulnerabilities and execution of malicious code



SYSTEMS SECURITY

Preventing unauthorized/unprivileged access to cyber systems and resources

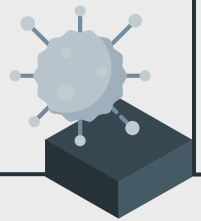
CYBERSECURITY

INFORMATION SECURITY

Protecting information with cryptography and secure communication protocols

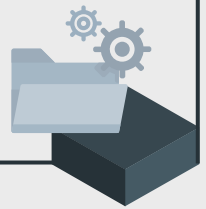
SOFTWARE SECURITY

Preventing the exploitation of vulnerabilities and execution of malicious code



SYSTEMS SECURITY

Preventing unauthorized/unprivileged access to cyber systems and resources



THIS COURSE

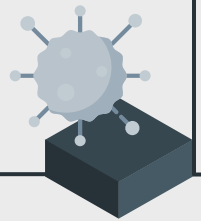
CYBERSECURITY

INFORMATION SECURITY

Protecting information with cryptography and secure communication protocols

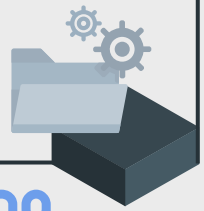
SOFTWARE SECURITY

Preventing the exploitation of vulnerabilities and execution of malicious code



SYSTEMS SECURITY

Preventing unauthorized/unprivileged access to cyber systems and resources



ECE 9609

INTRODUCTION TO HACKING

SECURITY PRINCIPLES

CONFIDENTIALITY

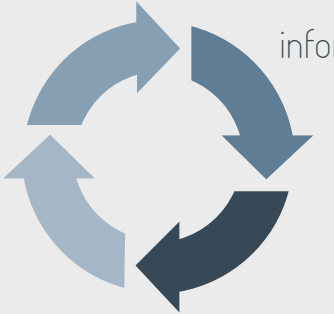
The ability to keep information secret or private from non authorized parties

INTEGRITY

The ability to detect alterations to information sent by an authorized party

AUTHENTICITY

The ability of an authorized party to prove its identity to another

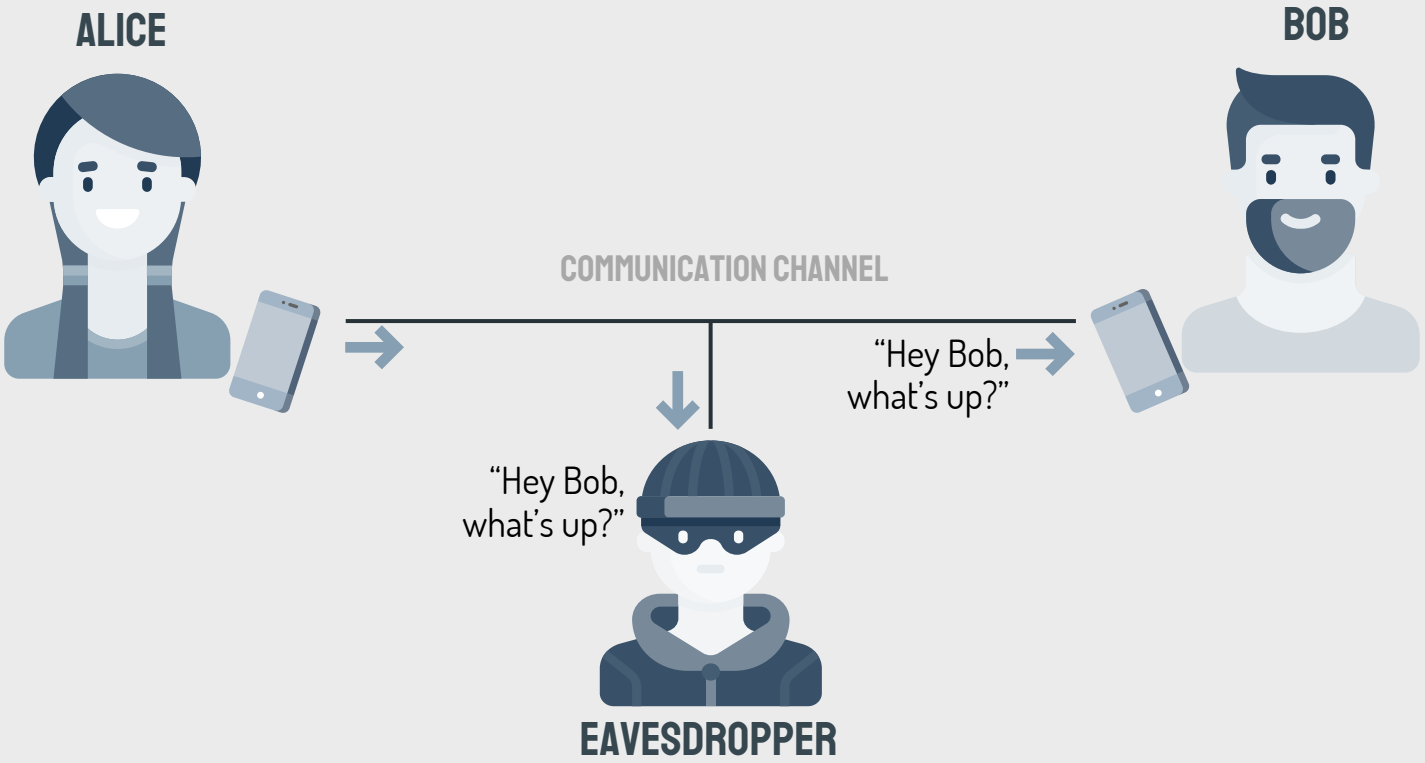


AVAILABILITY

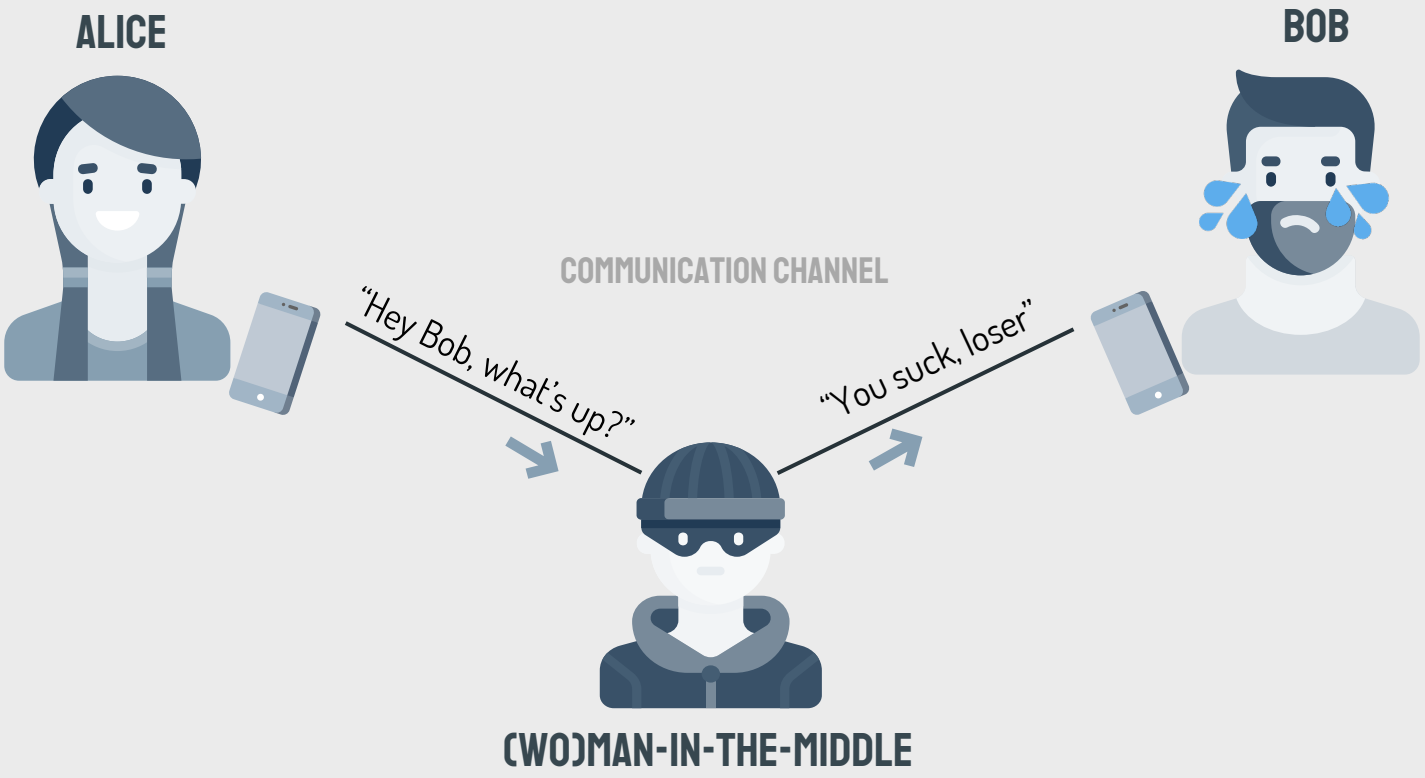
The continued ability for authorized parties to access an information system

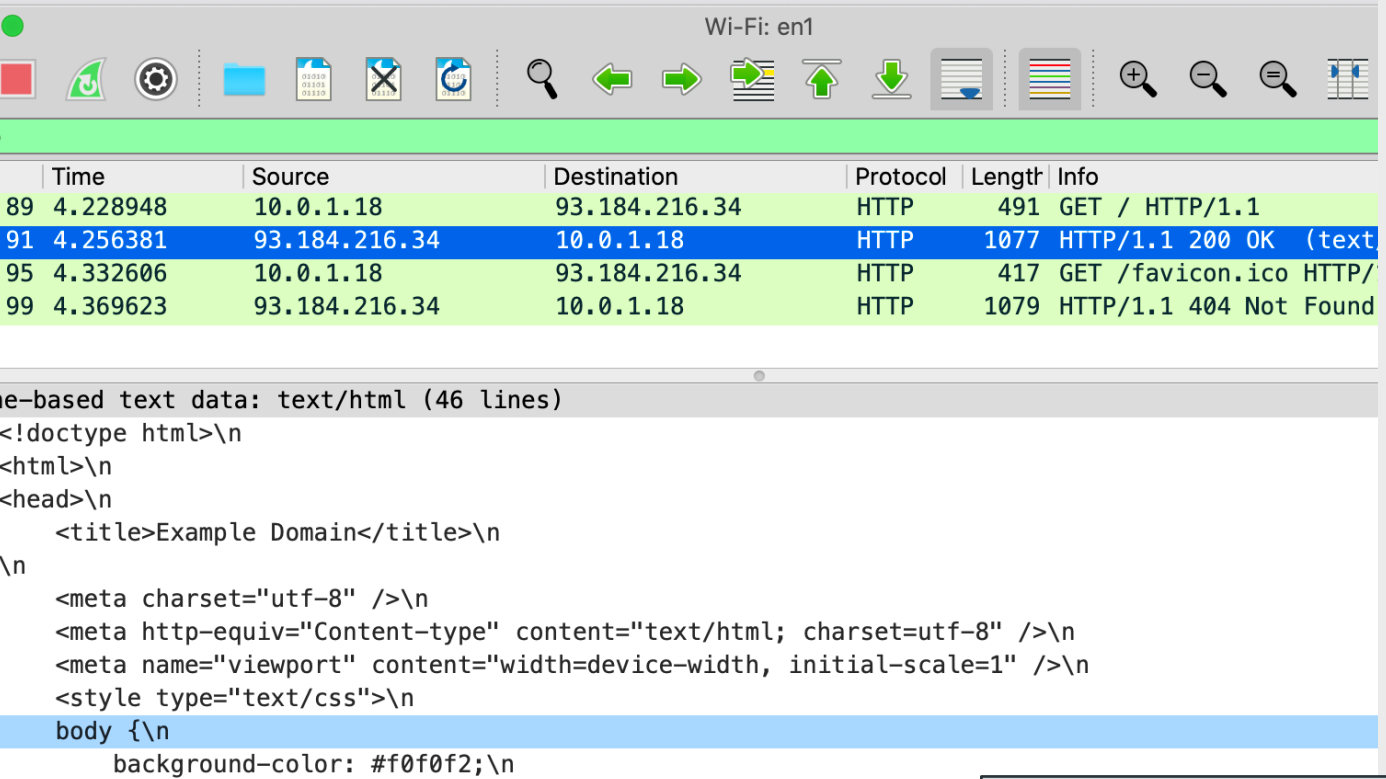
A MENTAL MODEL OF COMMUNICATION SECURITY

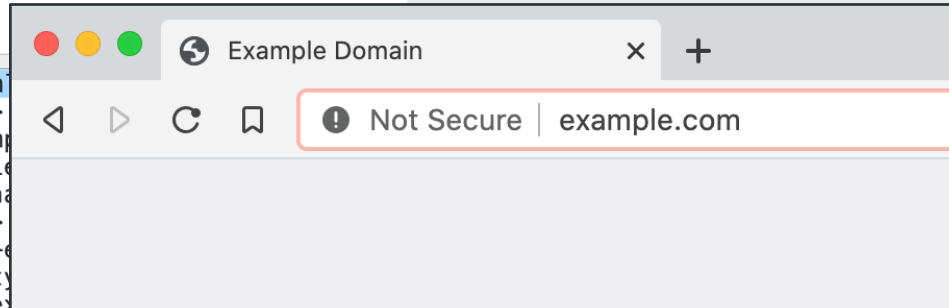
A MENTAL MODEL OF COMMUNICATION SECURITY



A MENTAL MODEL OF COMMUNICATION SECURITY

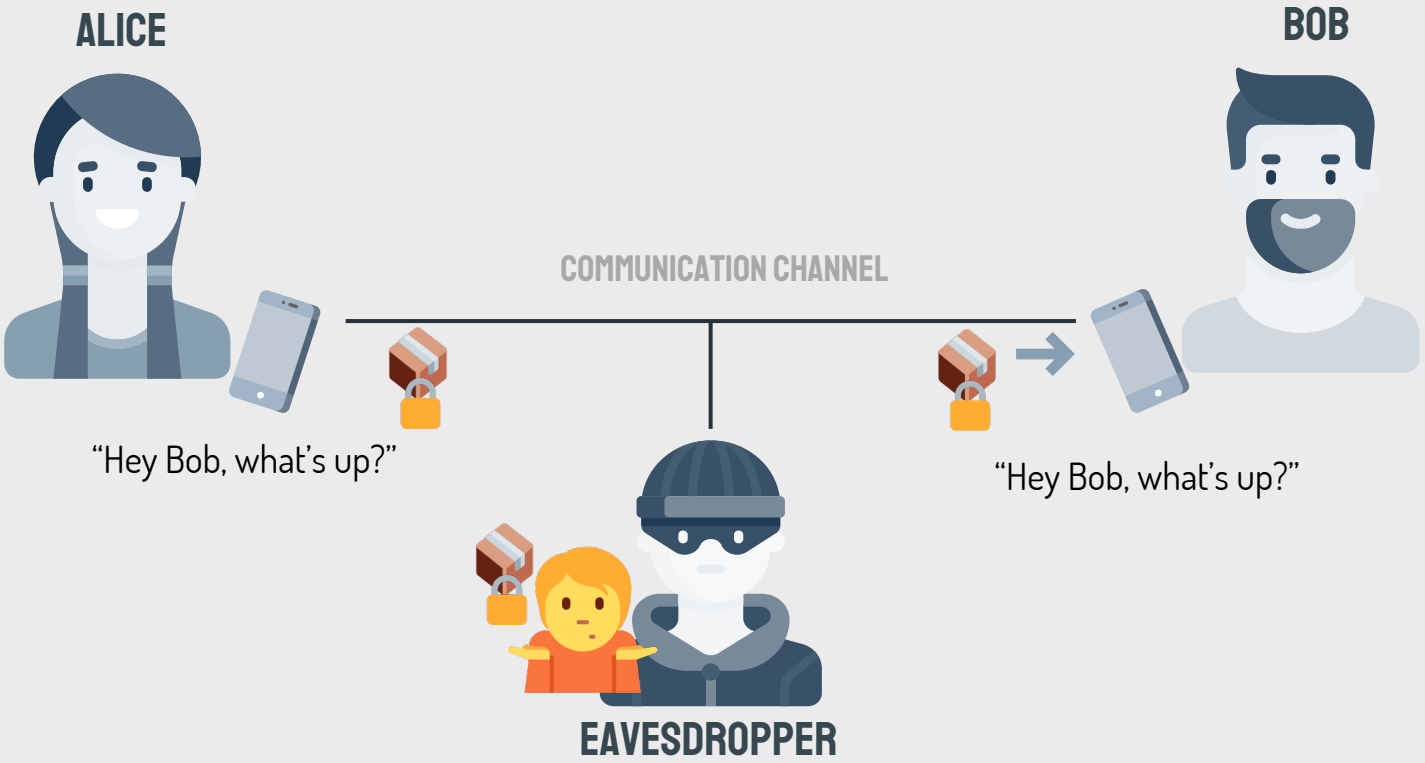




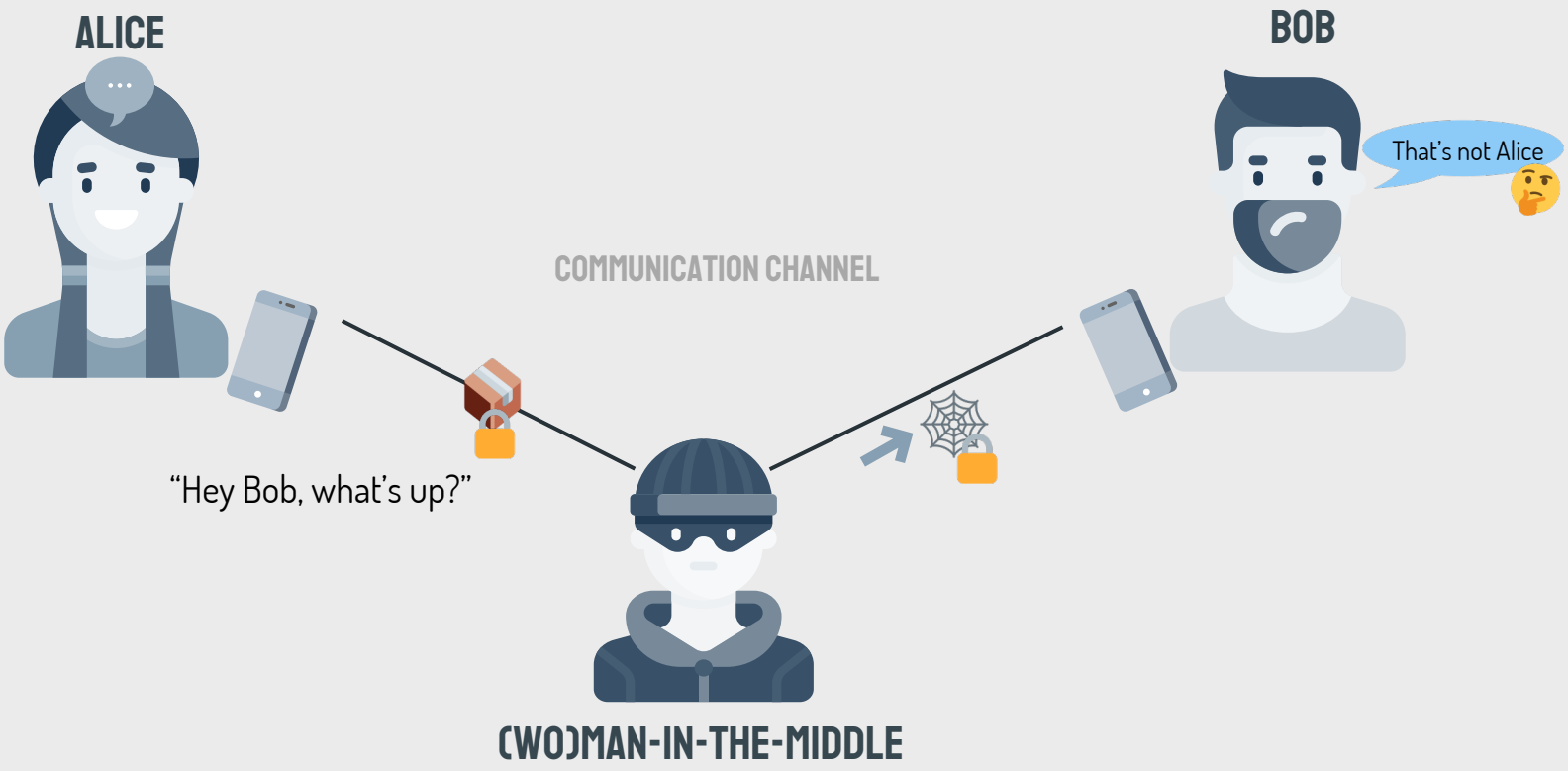


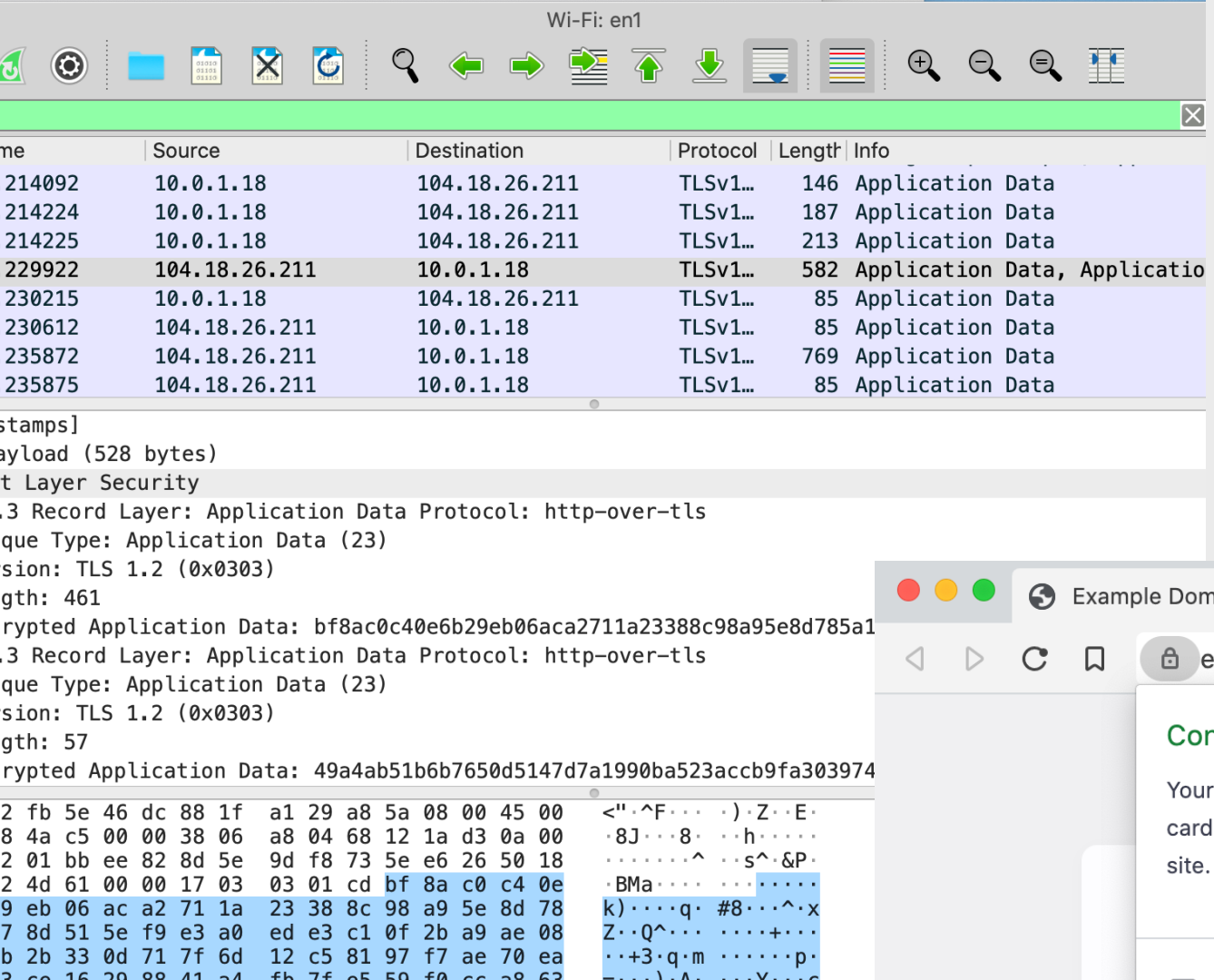
WHAT YOUR COMPUTER SENDS OVER THE WIRE

A MENTAL MODEL OF COMMUNICATION SECURITY

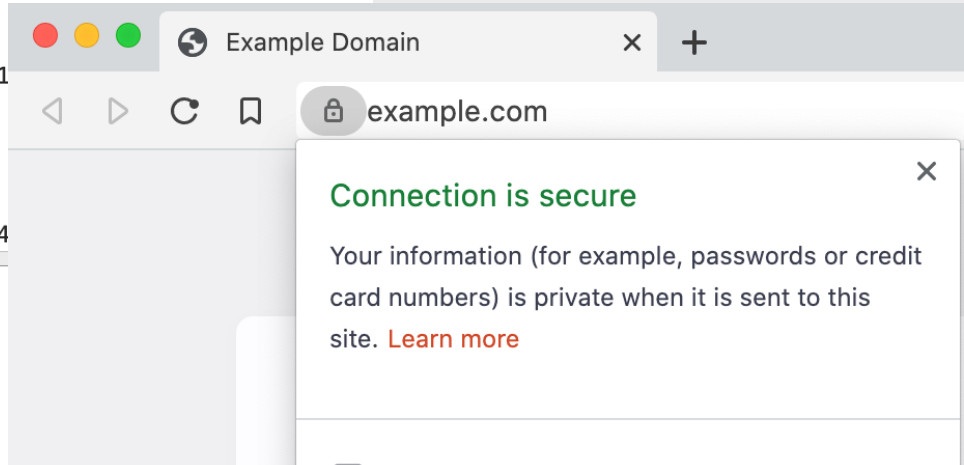


A MENTAL MODEL OF COMMUNICATION SECURITY



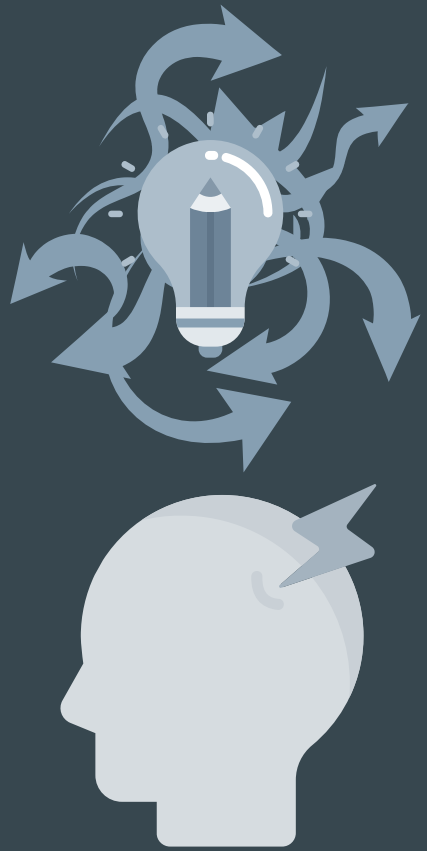


WHAT YOUR COMPUTER SENDS OVER THE WIRE



“DON’T roll your own crypto!”

—UNKNOWN



DON'T ROLL YOUR OWN CRYPTO

- VERY easy to get wrong
- Many subtle, unimagined threats
- Asymmetric disadvantage (you vs. smartest attackers in the world)
- Only takes one line of code (e.g., goto fail, heartbleed, etc)
- Rapid changes in best practices
- Good, free, secure, well studied tools already available anyway

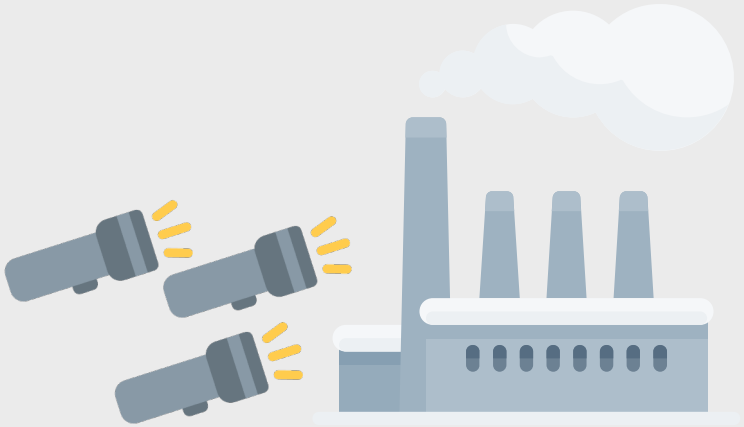
“The enemy knows the system”

—CLAUDE SHANNON

KERKHOFF'S PRINCIPLE

Security by design, not security through obscurity

Assume the bad guys know your algorithm/method. It should *still* be secure



Usually cryptography is not broken, it's bypassed

—ADI SHAMIR

When in doubt, use brute force

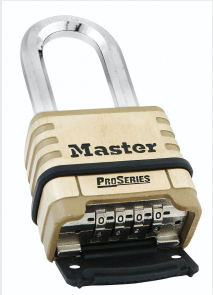
—KEN THOMPSON

BRUTE FORCE

SCENARIO: EACH LOCK PROCTECTS AN IMPORANT MESSAGE IN A BOX . THE METAL IS TOO STRONG TO BREAK. YOU JUST HAVE TO FIND THE COMBINATION

HOW MUCH WORK DO YOU HAVE TO DO?

BITS OF SECURITY



Bits of security

log_2 (number of combinations you expect to have to try)

So eg. trying 1024 = 2^10 combinations on average is 10 bits of security.

BITS OF SECURITY

Bits of security

How many bits of security is reasonable? What's the smallest number where you wouldn't worry about there ever being a chance of all the computers in the world (past and future) being able to try all the combinations?

QUESTIONS?

Contact Prof. Essex:
aessex@uwo.ca
@aleksessex

See course website for slides and videos:
https://whisperlab.org/security