



WEEK I

SECURITY GOALS

AND PRINCIPLES

SE 4472 - Information Security



Western
Engineering



WHISPER
LAB

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

CYBERSECURITY



CYBERSECURITY

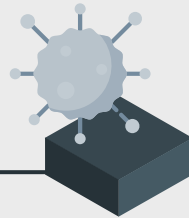
INFORMATION SECURITY

Protecting information with
cryptography and secure
communication protocols



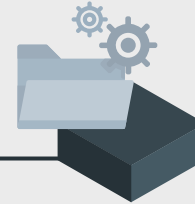
SOFTWARE SECURITY

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



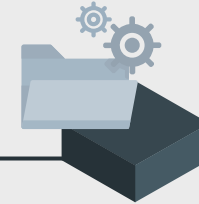
SOFTWARE SECURITY

Preventing the exploitation
of vulnerabilities and
execution of malicious code



SYSTEMS SECURITY

Preventing
unauthorized/unprivileged
access to cyber systems and
resources



THIS COURSE

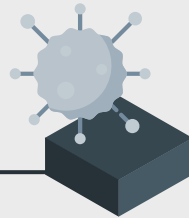
INFORMATION SECURITY

Protecting information with cryptography and secure communication protocols



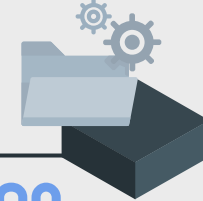
SOFTWARE SECURITY

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



AUTHENTICITY

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



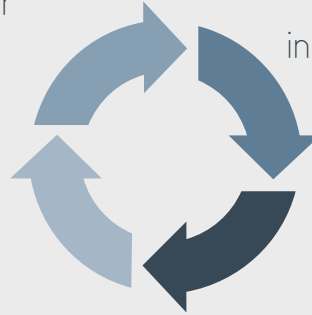
INTEGRITY

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



AVAILABILITY

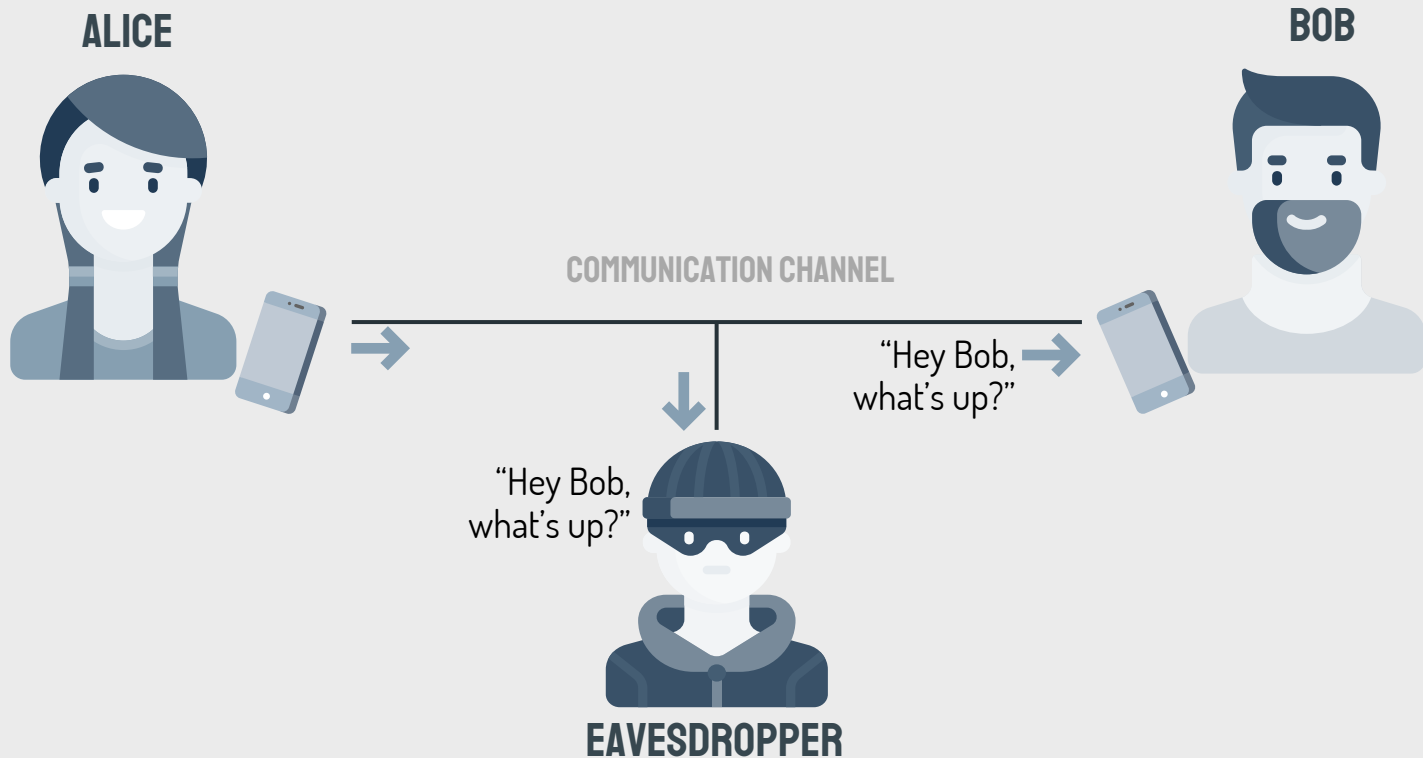
The continued ability for authorized parties to access an information system



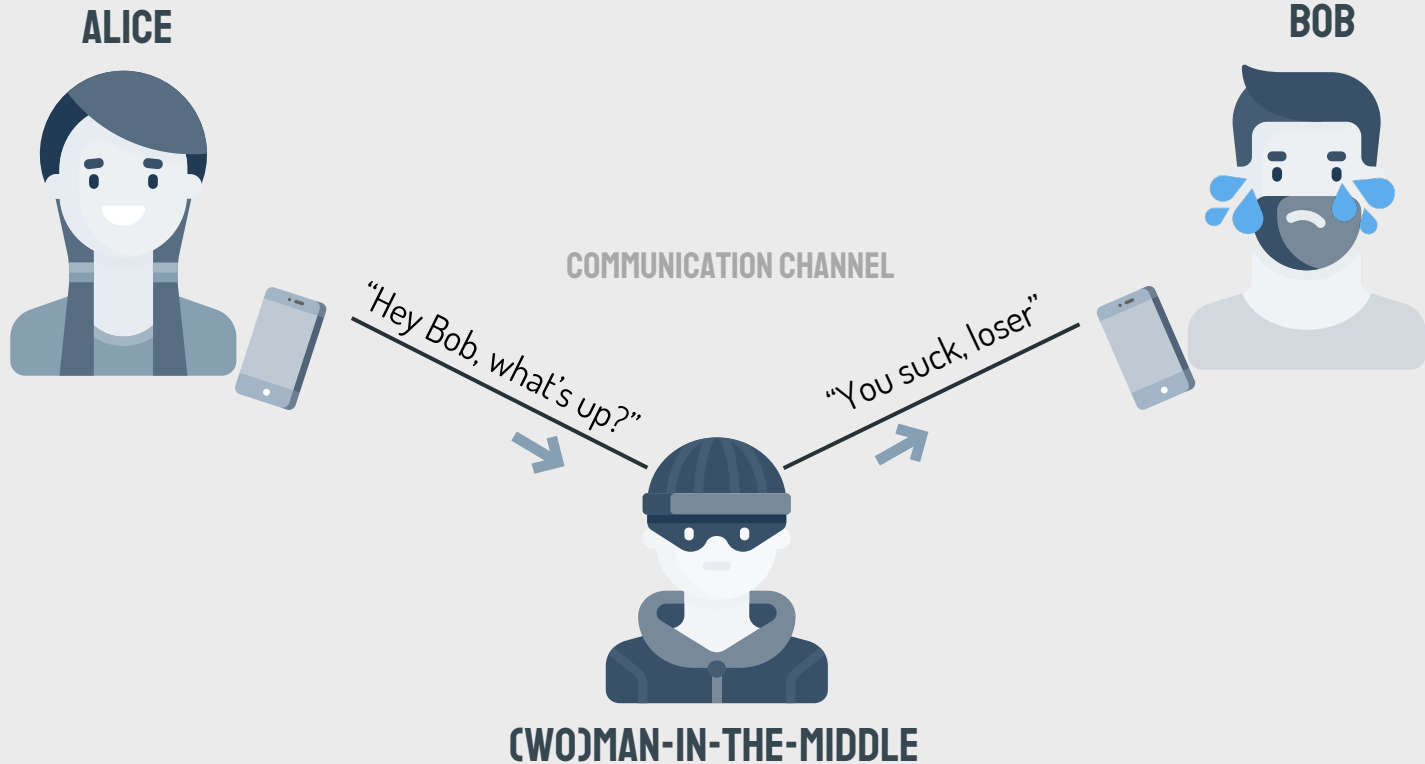
A MENTAL MODEL OF COMMUNICATION SECURITY



A MENTAL MODEL OF COMMUNICATION SECURITY



A MENTAL MODEL OF COMMUNICATION SECURITY



Wi-Fi: en1

Time	Source	Destination	Protocol	Length	Info
89	4.228948	10.0.1.18	93.184.216.34	HTTP	491 GET / HTTP/1.1
91	4.256381	93.184.216.34	10.0.1.18	HTTP	1077 HTTP/1.1 200 OK (text/html)
95	4.332606	10.0.1.18	93.184.216.34	HTTP	417 GET /favicon.ico HTTP/1.1
99	4.369623	93.184.216.34	10.0.1.18	HTTP	1079 HTTP/1.1 404 Not Found

Text-based text data: text/html (46 lines)

```

<!doctype html>\n
<html>\n
<head>\n
  <title>Example Domain</title>\n
\n
  <meta charset="utf-8" />\n
  <meta http-equiv="Content-type" content="text/html; charset=utf-8" />\n
  <meta name="viewport" content="width=device-width, initial-scale=1" />\n
  <style type="text/css">\n
    body {\n
      background-color: #f0f0f2;\n
      margin: 0;\n
    }\n
  </style>\n
  <div style="text-align: center; padding: 10px 0 0 0;">\n
    <h1>Example Domain</h1>\n
    <p>This domain is currently for sale. Would you like to purchase it?</p>\n
  </div>\n
</html>
  
```

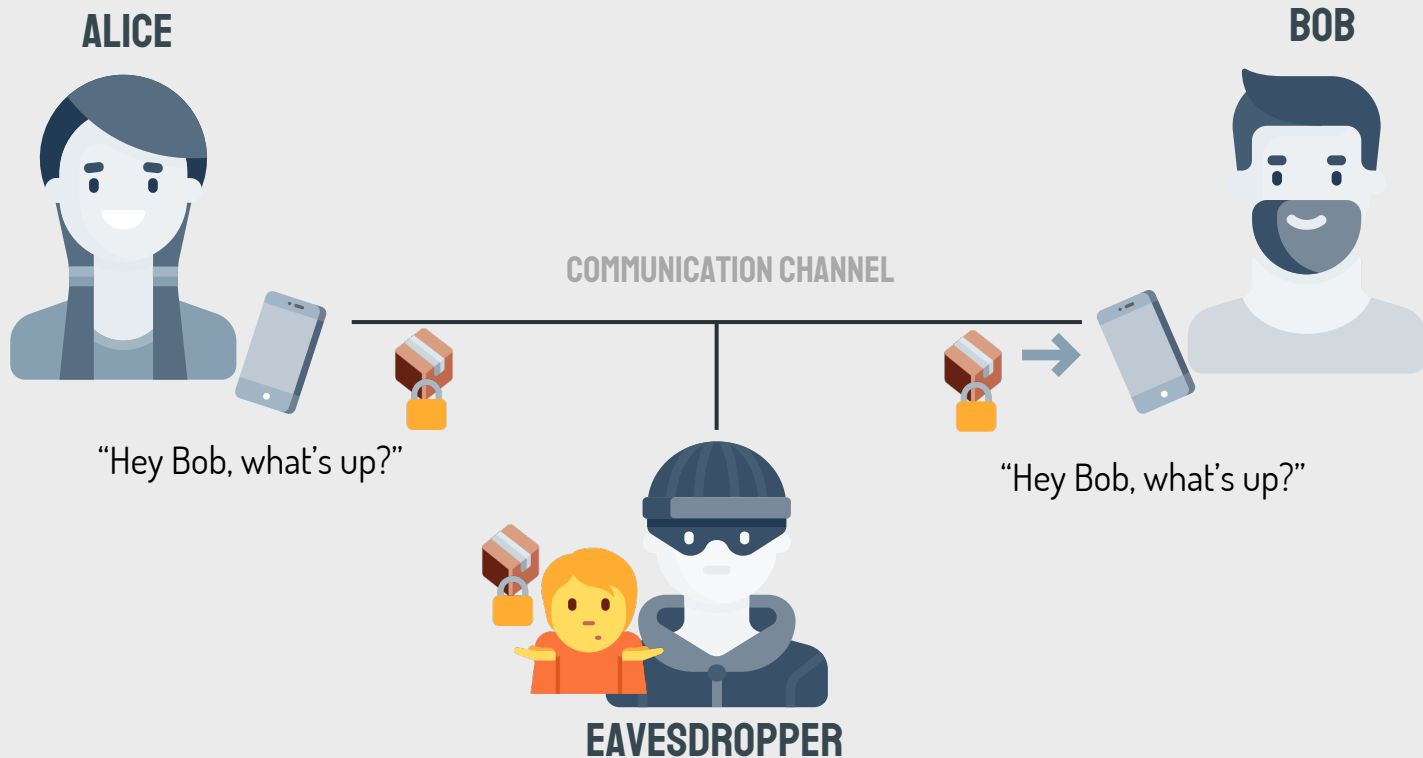
3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a <!doctype e htm
3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 <html>< head>
20 20 3c 74 69 74 6c 65 3e 45 78 61 6d 70 6c 65 <title >Exam
20 44 6f 6d 61 69 6e 3c 2f 74 69 74 6c 65 3e 0a Domain< /title
0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 . <me ta cha
65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 et="utf- 8" />
20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 <meta http-e
69 76 3d 22 43 6f 6e 74 65 6e 74 2d 74 79 70 65 iv="Cont ent-ty
22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f " conten t="tes

WHAT YOUR COMPUTER SENDS OVER THE WIRE

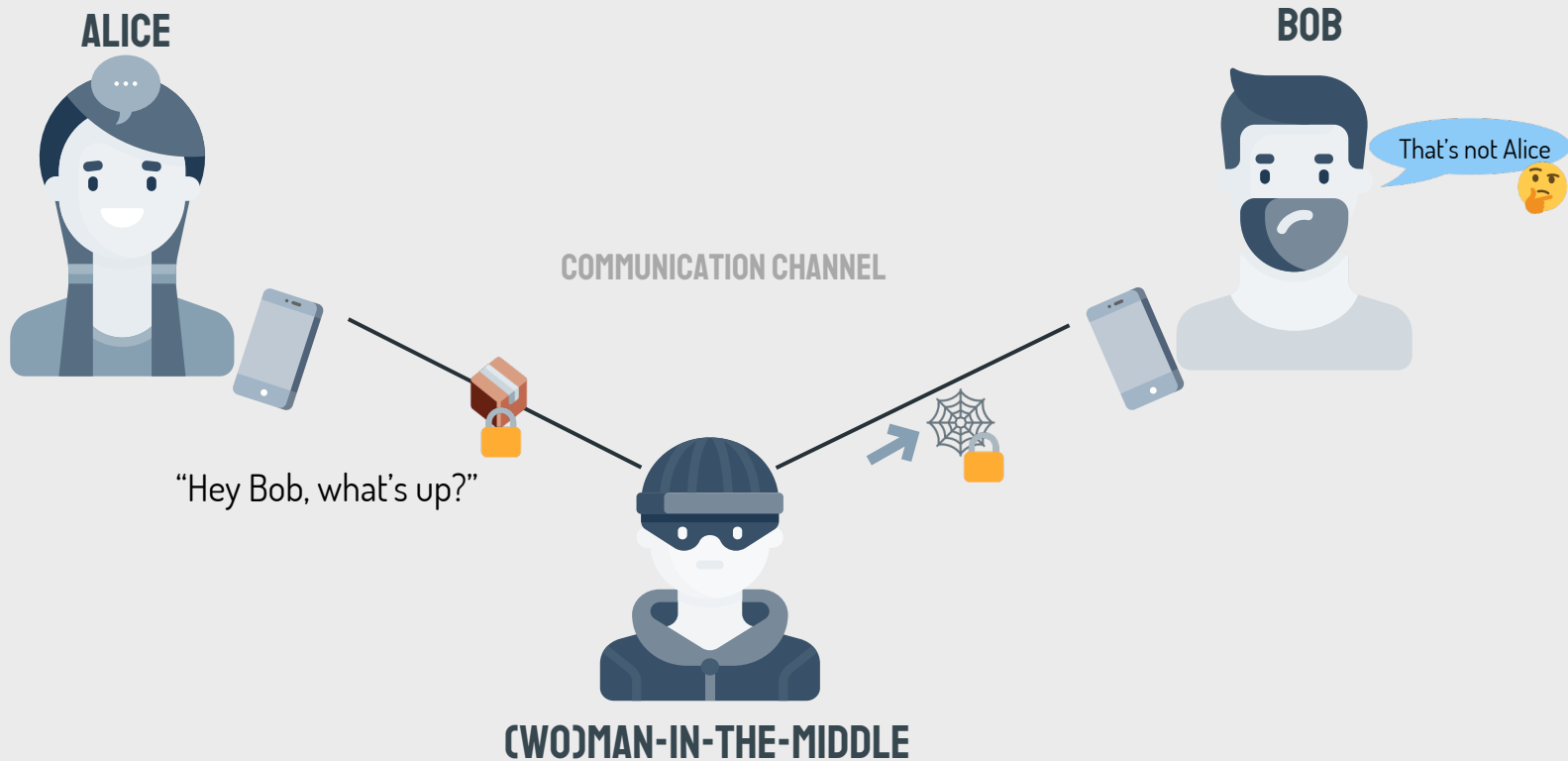
Example Domain

Not Secure | example.com

A MENTAL MODEL OF COMMUNICATION SECURITY



A MENTAL MODEL OF COMMUNICATION SECURITY





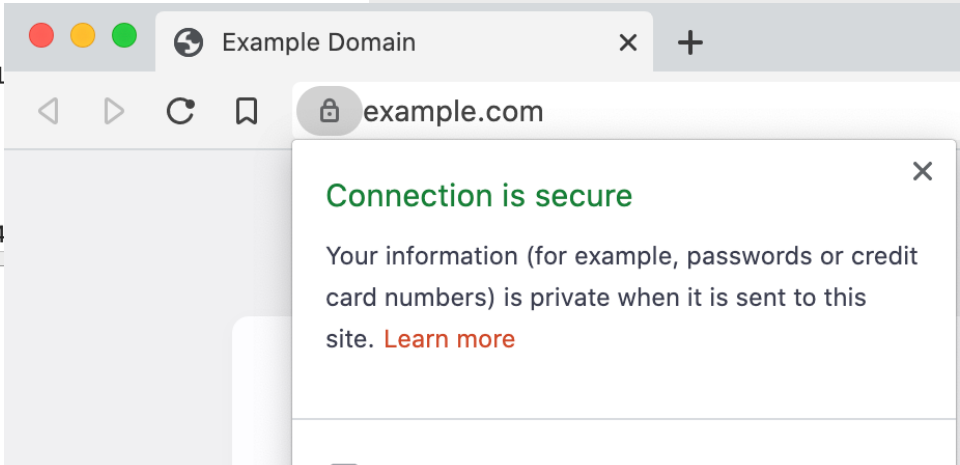
Time	Source	Destination	Protocol	Length	Info
214092	10.0.1.18	104.18.26.211	TLSv1...	146	Application Data
214224	10.0.1.18	104.18.26.211	TLSv1...	187	Application Data
214225	10.0.1.18	104.18.26.211	TLSv1...	213	Application Data
229922	104.18.26.211	10.0.1.18	TLSv1...	582	Application Data, Applicatio
230215	10.0.1.18	104.18.26.211	TLSv1...	85	Application Data
230612	104.18.26.211	10.0.1.18	TLSv1...	85	Application Data
235872	104.18.26.211	10.0.1.18	TLSv1...	769	Application Data
235875	104.18.26.211	10.0.1.18	TLSv1...	85	Application Data

stamps]
ayload (528 bytes)
t Layer Security
3 Record Layer: Application Data Protocol: http-over-tls
que Type: Application Data (23)
sion: TLS 1.2 (0x0303)
gth: 461
rpted Application Data: bf8ac0c40e6b29eb06aca2711a23388c98a95e8d785a1

3 Record Layer: Application Data Protocol: http-over-tls
que Type: Application Data (23)
sion: TLS 1.2 (0x0303)
gth: 57
rpted Application Data: 49a4ab51b6b7650d5147d7a1990ba523accb9fa303974

```
2 fb 5e 46 dc 88 1f a1 29 a8 5a 08 00 45 00 <".^F... .).Z..E.  
8 4a c5 00 00 38 06 a8 04 68 12 1a d3 0a 00 .8J...8...h...  
2 01 bb ee 82 8d 5e 9d f8 73 5e e6 26 50 18 ...^...s^&P.  
2 4d 61 00 00 17 03 03 01 cd bf 8a c0 c4 0e .BMa... ..  
9 eb 06 ac a2 71 1a 23 38 8c 98 a9 5e 8d 78 k)...q. #8...^x  
7 8d 51 5e f9 e3 a0 ed e3 c1 0f 2b a9 ae 08 Z..Q^... ..+...  
b 2b 33 0d 71 7f 6d 12 c5 81 97 f7 ae 70 ea ...+3.q.m ...p.  
2 ce 16 20 88 41 c4 fb 7f c5 50 f0 cc a8 62 ...).A...Y...C
```

WHAT YOUR COMPUTER SENDS OVER THE WIRE



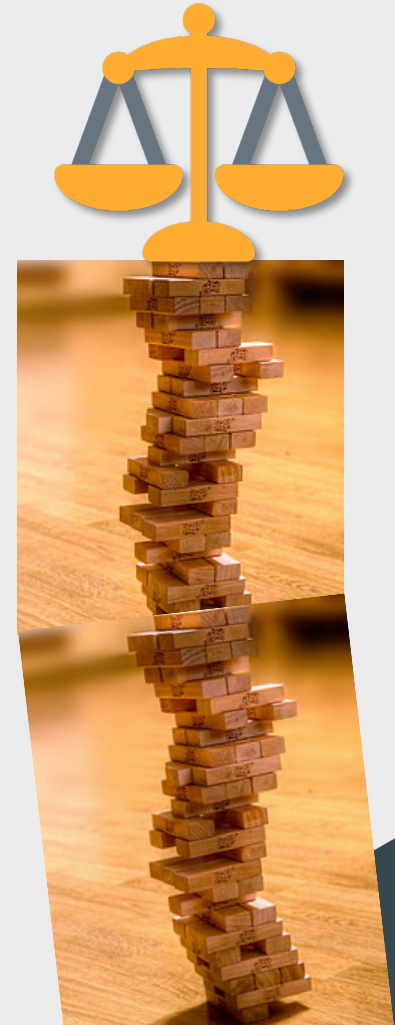
“DON’T roll your own
crypto!”

—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”

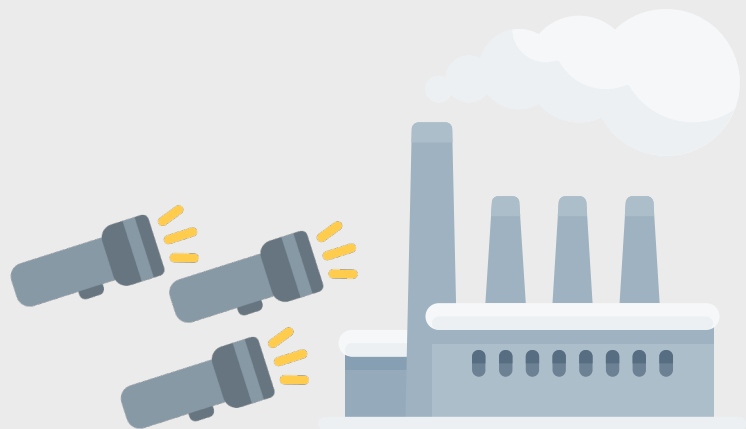
—CLAUDE SHANNON



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



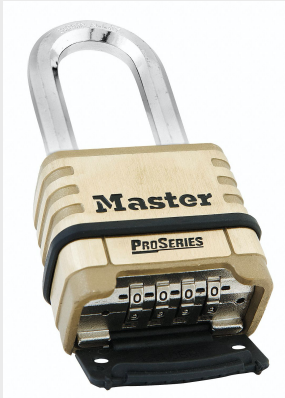
When in doubt, use
brute force

—KEN THOMPSON



BRUTE FORCE

SCENARIO: EACH LOCK PROTECTS AN IMPORTANT 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>

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik** and illustrations by **Stories**