School of Electrical Engineering and Computing

SENG2250/6250
SYSTEM AND NETWORK SECURITY
(S2, 2020)

Introduction

THE UNIVERSITY OF NEWCASTLE AUSTRALIA

Course Organisation

Lectures

SENG2250: Pre-recorded videos

SENG6250: Pre-recorded videos + extra f2f lectures

Labs (Online or f2f)

Mondays	14:00 – 16:00 @ HC49/ES105 OR
Mondays	16:00 – 18:00 @ HC49 OR
Tuesdays	11:00 – 13:00 @ ES105 OR
Tuesdays	13:00 – 15:00 @ ES105 OR
Wednesdays	09:00 – 11:00 @ ES105 OR

(No labs in Week 1 and Week 13)

Consultation Times

Lecturer: Dr. Nan Li

Office: ES222

Email: Nan.Li@newcastle.edu.au

Phone: 4921 6503

Consultation Time

Thursday: 10:00 – 12:00 (Zoom/f2f)

Demonstrator and Marker

- **Mr. Cody Lewis**
  - *Cody.Lewis@uon.edu.au*

- **Mr. Prajna Sariputra**
  - *Prajna.Sariputra@uon.edu.au*

- Cody and Prajna will be both demonstrators and markers.

Contact

- 4 Forums will be opened.
  - *General*
  - *A1*
  - *A2*
  - *A3*
- Consultation time
- Email
  - *It is the **preferred** method if the forums and consultation time do not suit you.*
- Zoom

What is about the course?

- What will be covered?
  - *A wide range of topics in **System and Network security**.*
  - *Introduction of fundamental security concepts, e.g,*
    - Cryptography
    - Security protocols
  - *Protocol and system design.*
- What will NOT be covered? Some examples
  - *Hacking techniques.*
  - *Practical system and network attacks - COMP3500☺*
- Knowledge required
  - *Basic computer network/system knowledge.*
  - *Programming skills: C/C++/Java/Python.*

Objectives - SENG2250

- Fundamental
  - *Understand security concepts, notions, protocols and mechanisms.*
- Objectives
  - *Identify key security requirements and trends in a distributed networked computing environment.*
  - *Describe security threats and develop security functionalities to counteract the security threats.*
  - *Apply security techniques and mechanisms to develop secure systems and protocols.*
  - *Utilise analytical skills for evaluating security protocols and mechanisms.*
  - *Evaluate authentication and access control security functionalities in distributed systems and networks.*

Contents – SENG2250

Week	Topic	Assessment
1	Introduction	A1 out
2	Cryptographic Techniques	
3	Key Management and Distribution	
4	User Authentication	A1 due
5	Access Control	A2 out
6	Operating System Security	
7	Distributed System Security (Fundamentals)	A3 out
8	Distributed System Security (WS security, OAuth)	A2 due
9	Network Security (IPSec)	
10	Network Security (SSL/TLS)	
11	Network Security (Wireless security)	
12	Application Security (Email security, PGP, etc.)	A3 due
13	Revision	

Note: The order of topics and due date of assignments are subject to change.

Assessments – SENG2250

	Assessment Name	Due Date	Involvement	Weighting
1	Assignment 1 – Security Fundamentals	Week 4	Individual	10%
2	Assignment 2 – Authentication and System Security	Week 8	Individual	15%
3	Assignment 3 – Network Security and Secure Coding	Week 12	Individual	25%
4	Formal Examination*	EXAM PERIOD	Individual	50%

Lectures

- Pre-recorded videos (weekly)
  - *Main video (1~1.5 hours) : will go through the lecture slides.*
  - *Short video (< 10 mins): will explain some topics which may be difficult and/or important.*
- Where are the videos?
  - *All videos are in Blackboard **UONCapture** tab.*
  - *You may also click ▶ icon for short videos.*

Labs

- We will have a special arrangement for the labs.
  - *Most of the labs can be done on your own computer.*
    - Demonstrators will be online for help.
  - *Some of the labs may require the special lab settings.*

- It is designed based on the objective of the course.

- You will need to do activities/thinking/discussion/self-study...

References

- William Stallings. Network Security Essentials: Applications and Standards. Prentice Hall, 6th edition, 2016.

- C.P. Pfleeger and S.L. Pfleeger. Security in Computing. Prentice Hall , 4th(or 5th) editions, 2007 (2015).

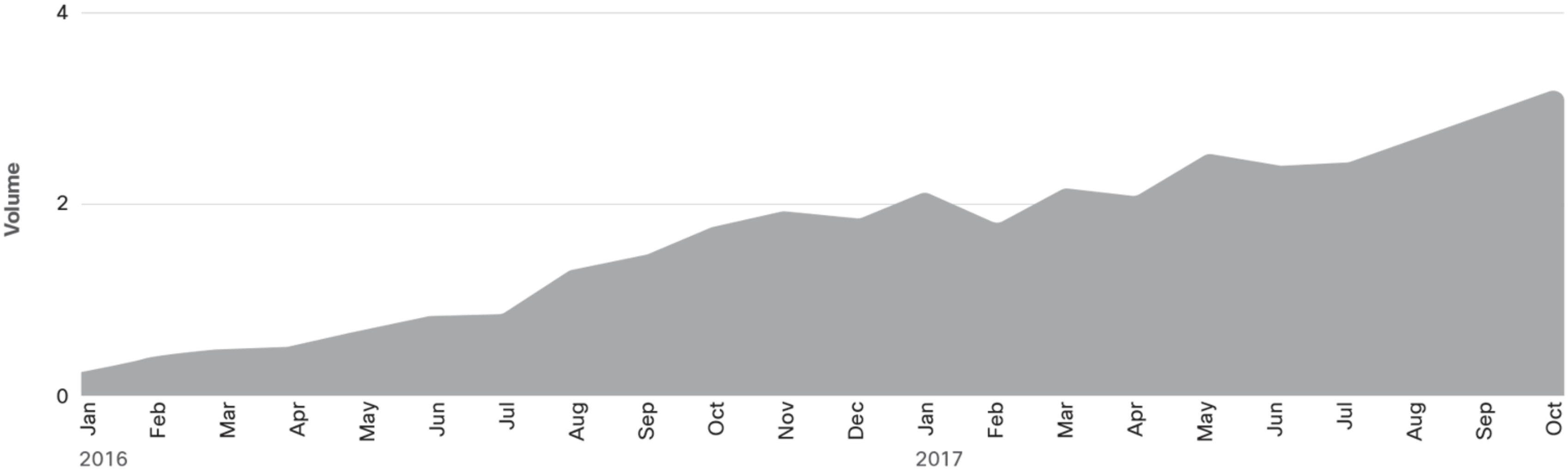
Welcome to SENG2250/6250

System and Network Security

Why does security matter?

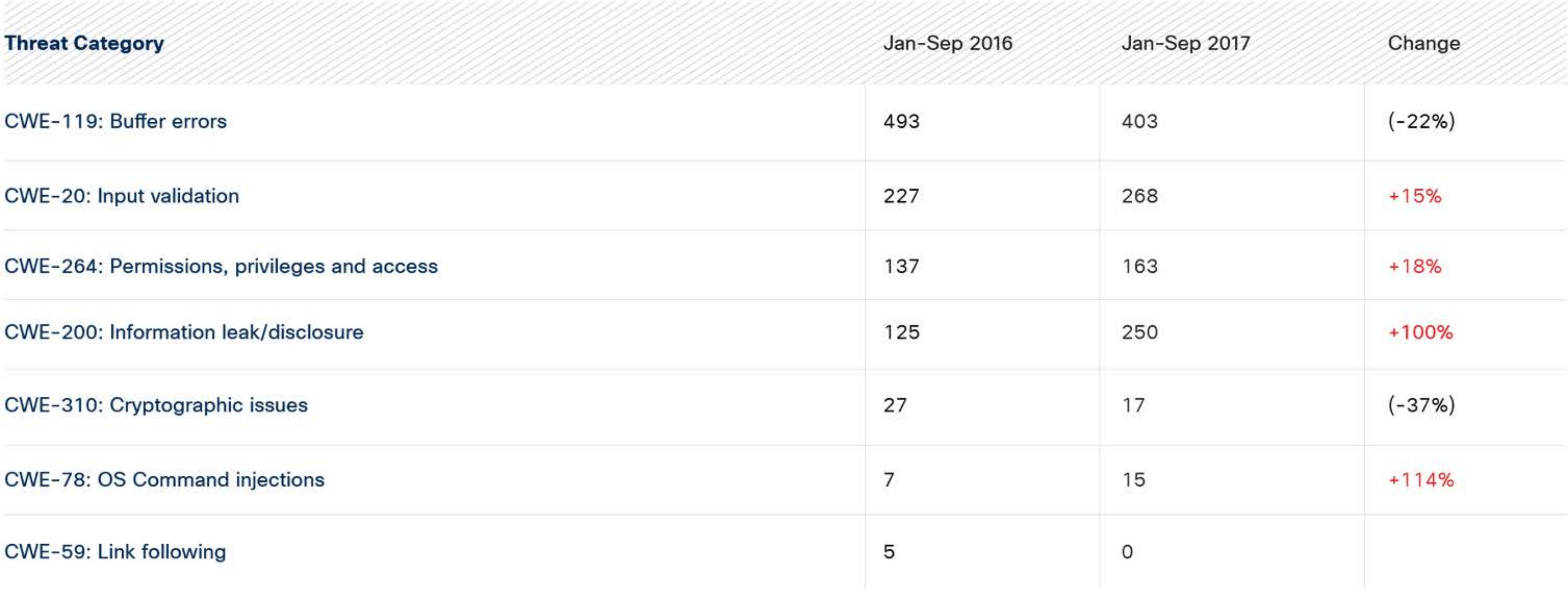
- Computer and network security really matter because of some people do actually attack computer systems and networks, for various reasons.
  - *Money: e.g., ransomware*
  - *Sensitive data*
  - *Intelligent property*
  - *Industrial sabotage*
  - *Computing power and resources*
  - *Fun*
  - *…*
- Increasing computer crimes and financial losses.

Overall of Security Events



Source: Cisco Security Research

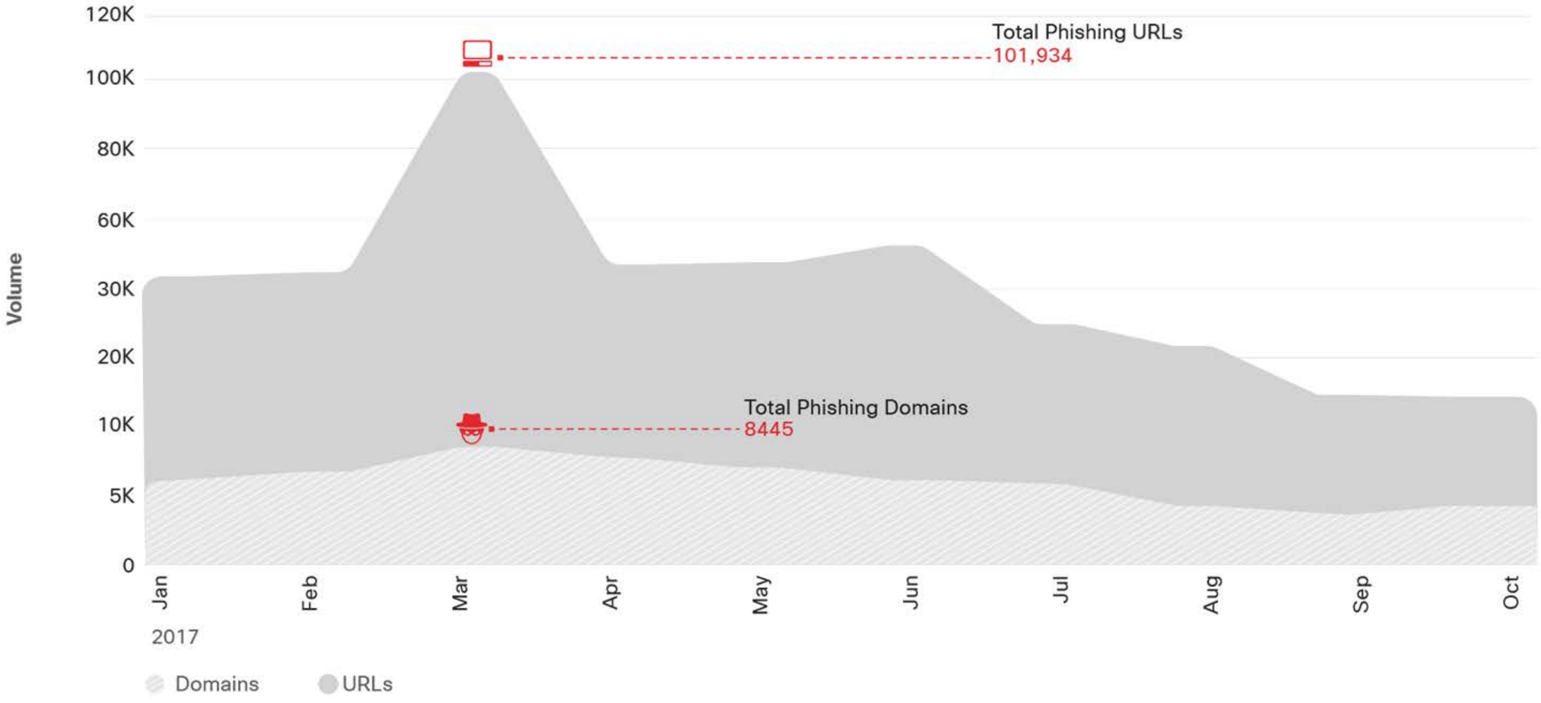
Common Weakness Enumeration (CWE) Vulnerabilities



Threat Category	Jan-Sep 2016	Jan-Sep 2017	Change
CWE-119: Buffer errors	493	403	(-22%)
CWE-20: Input validation	227	268	+15%
CWE-264: Permissions, privileges and access	137	163	+18%
CWE-200: Information leak/disclosure	125	250	+100%
CWE-310: Cryptographic issues	27	17	(-37%)
CWE-78: OS Command injections	7	15	+114%
CWE-59: Link following	5	0	

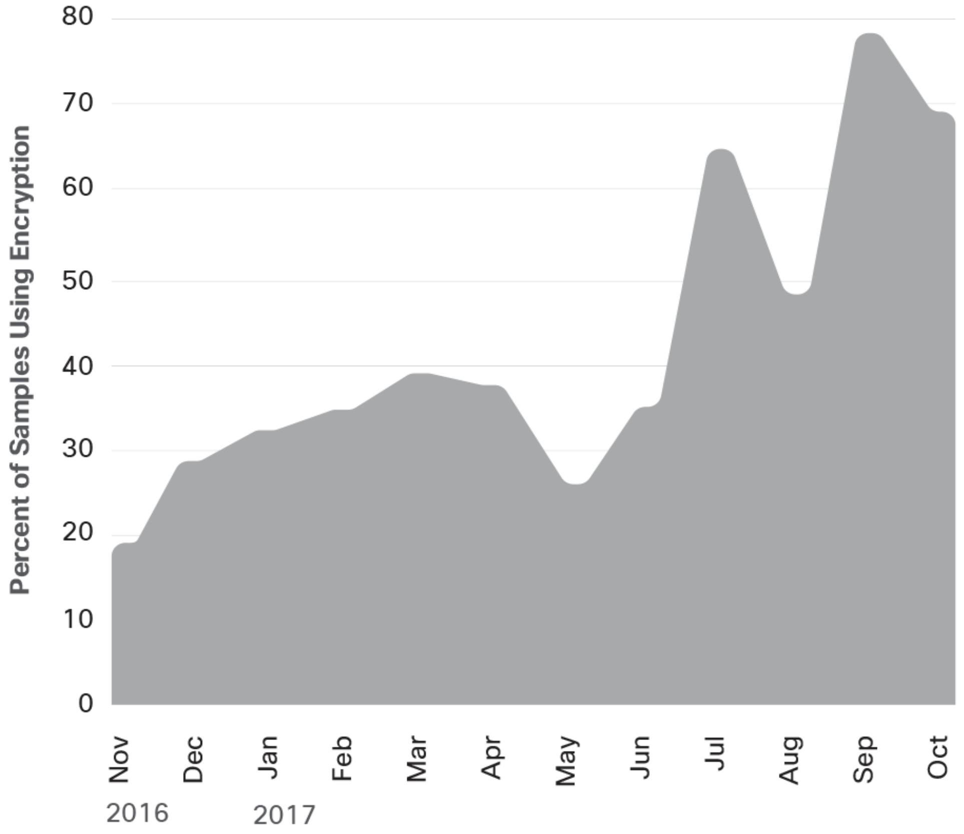
Source: Cisco Security Research

Phishing



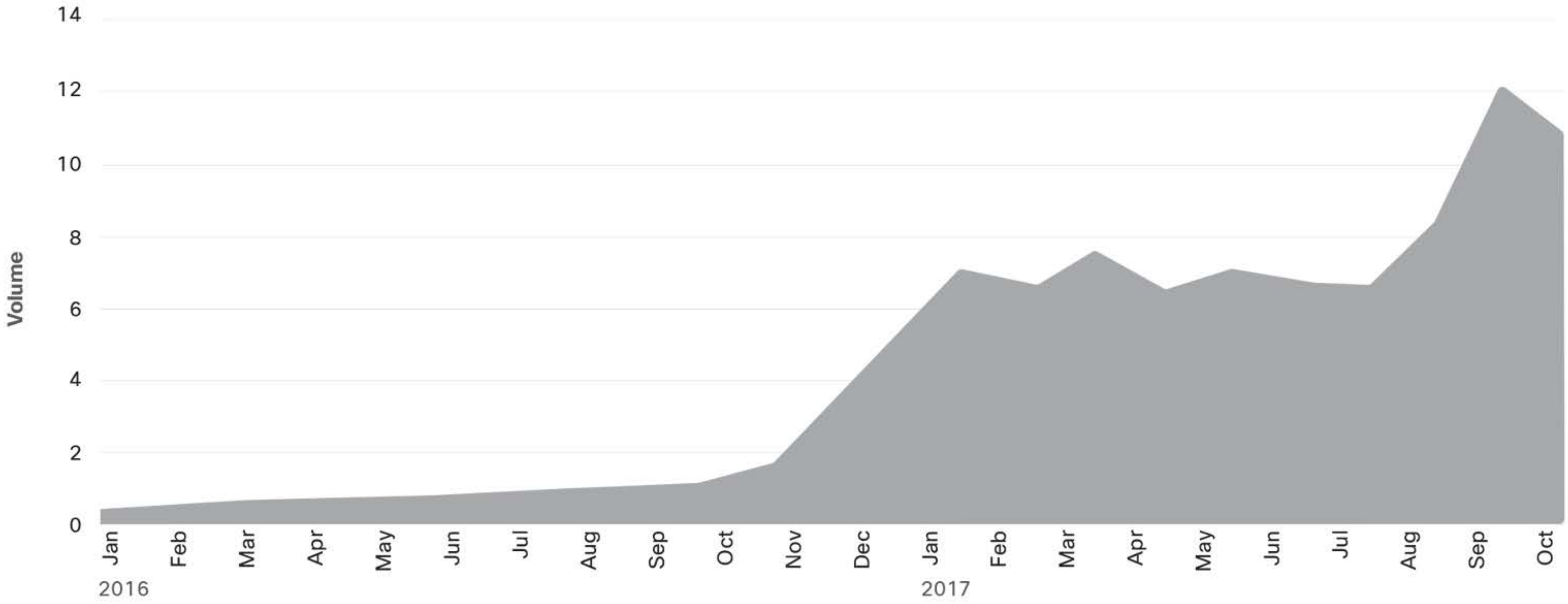
Source: Cisco Security Research

Malicious Binaries Over Encrypted Communication



Source: Cisco Security Research

Overall Malware Volume



Source: Cisco Security Research

What is security?

- System features/functionalities
  - *The more, the better*
- System correctness
  - *Desired Input → desired output*
- Security
  - *Unexpected input → controllable output*
  - *System complexity → more vulnerabilities*
  - *More secure → less efficient, less convenient, more cost*

The Goal of Security

- Prevent an attack (before it happens)
  - *This is the ideal solution.*
  - *This is where technology should be helping most!*
- Detect the attack (when it happens)
  - *Know what is going on, who is causing it*
  - *This is really where technology is helping most!*
- Recover from an attack (as soon as possible)
  - *Stop the attack.*
  - *Assess and repair the damage caused.*

The Art of (Cyber) War

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

Sun Tzu

C.I.A – Security Properties

- Confidentiality: Assets should be accessible to authorised parties only.

- Integrity: Assets should be unmodifiable by unauthorised parties.

- Availability: Assets should be available to authorised parties.

Confidentiality

- Prevent assets from accessing by unauthorised parties.
  - *E.g. individuals, organisation, government.*
- Access control mechanisms support confidentiality.
  - *E.g. cryptography (keys), encryption.*
- Confidentiality also applies to the existence of data, which is sometimes more revealing than the data itself.
- Resource hiding is another important aspect.
  - *Sites wish to conceal their configuration as well as what systems they are using;*
  - *Organisations may not wish for people to know about specific equipment they are using.*
- Assumptions and trust underlie confidentiality mechanisms.

Integrity

- Integrity includes
    - *data integrity: the content of the information*
    - *origin integrity: the source of the data, often called authentication.*
- Integrity mechanisms fall into two classes:
    - *Prevention mechanisms*
        - Seek to maintain the integrity of the data by blocking any unauthorised attempts to change the data or any attempts to change the data in unauthorised ways.
        - E.g. Access control.
    - *Detection mechanisms:*
        - Do not try to prevent violations of integrity; they simply report that the data's integrity is no longer trustworthy.
        - E.g. MAC, digital signatures.

Confidentiality and Integrity

- With confidentiality, the data is either compromised or it is not, but integrity includes both the correctness and the trustworthiness of the data.
- The origin of the data (how and from whom it was obtained), how well the data was protected before it arrived at the current machine, and how well the data is protected on the current machine all affect the integrity of the data.
- Thus evaluating **integrity** is often difficult.

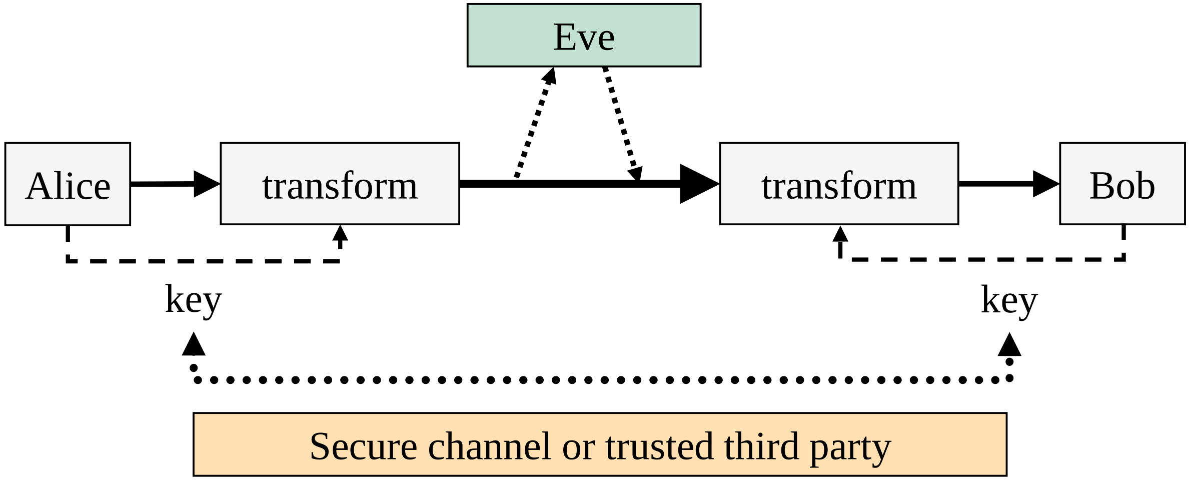
Availability

- Availability is very much linked to reliability as well as of system design because an unavailable system is as bad as no system at all.
- Someone may deliberately deny access to data or to a service by making it unavailable.
- Attempts to block availability are called, denial-of-service (DoS) attacks.
  - *DoS attacks are difficult to detect because it requires the analyst to determine if unusual patterns of access are attributable to deliberate manipulation of resources or of environment.*
  - *Sometimes DoS attacks just seem to be atypical events or in some cases they are not even atypical. Statistical models are important here esp. of network traffic.*

Authenticity and Accuracy

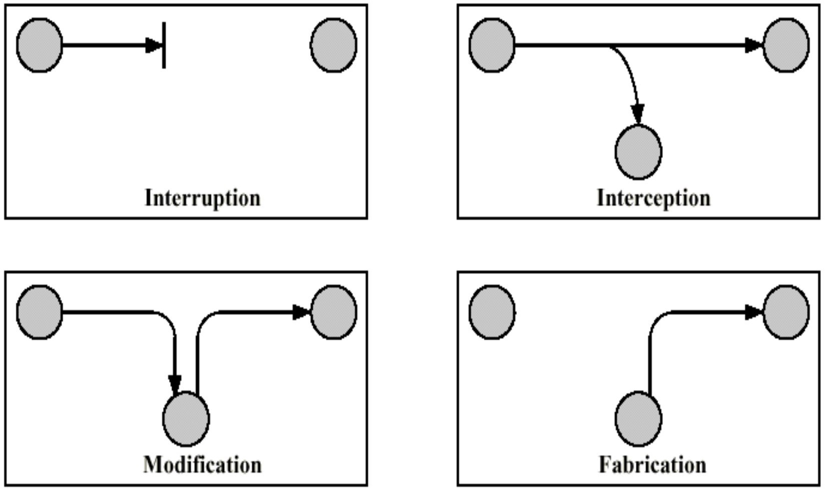
- Authenticity
  - *The origin of assets should be assured and the assets should be unforgeable by unauthorised parties.*
  - *E.g., Impersonation, forgery of digital signatures*
- Accuracy
  - *Be free from mistakes and errors*
  - *Provide information as end user expects*
  - *E.g., $ = AUD/USD/... ?*

Security Model



- Secure channel: A protected channel which is assumed to be free from attackers. (sometimes hard to find)
- Trusted Third Party (TTP): A party which is trusted by all parties of a communication.

Security Issues



- Interruption: An attack on availability (Active).
- Interception: An attack on confidentiality (Passive).
- Modification: An attack on integrity (Active).
- Fabrication: An attack on authenticity (Active).

Vulnerabilities and Attacks

- **Vulnerability:** A weakness in the system that it could be exploited to harm the system or assets.
  - *Account password is too simple: 12345678*

- **Attack:** An exploitation of one or more system vulnerabilities by using specific techniques in an attempt to cause some damage.
  - *Guess/brute force password to gain the access to account.*

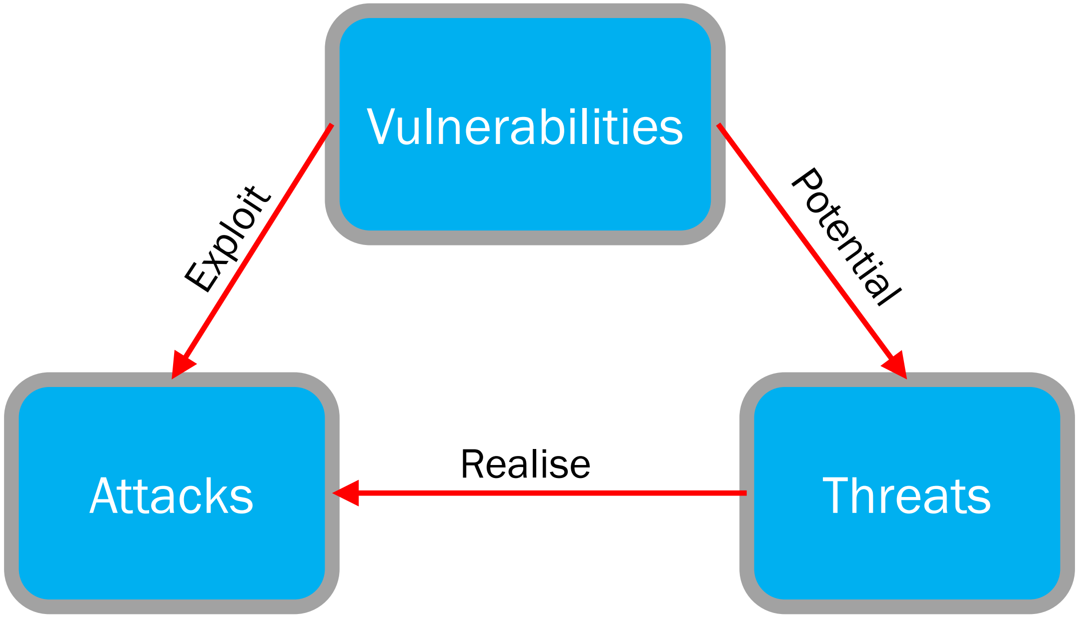
Attacks

- Security attacks
  - *Consists of goals and a set of actions that exploits vulnerability (i.e., an identified weakness) in controlled system*
  - *Accomplished by threat agent that damages or steals information*
- Relationship with CIA triangle.
  - *An attack aims at breaking one or more properties of CIA.*
  - *CIA provides directions of defending specific attacks.*
    - E.g., technical tools.

Security Threats

- Threat: A potential danger which may be presented by exploiting some vulnerabilities in attacks.
  - *The account may be accessible by unauthorised parties.*
- The violation need not occur for there to be a threat.
- The fact that the violation *MIGHT* occur is a threat.
- If the action occurs then it is an attack.
- The one who causes the attack to happen is an **attacker/adversary**.

Relationship



Main Categories of Threats

- Disclosure
  - *Unauthorised access to information. (C)*
- Deception
  - *Acceptance of false data. (I, A)*
- Disruption
  - *Interruption or prevention of correct operation. (A)*
- Usurpation
  - *Unauthorised control of some part of the system. (A)*

Examples of Threats

Types of Threats	**Potential Attacks (example)**
Loss of credentials	Unauthorised access
Social engineering	Impersonation, password recovery
Malware (Virus/Worms/Trojan Horses…)	Sensitive data disclosure, Zombies
Implementation flaws	Buffer overflow
Spam/Phishing	Break access control, fraud
Sniffing	Network attacks like spoofing, SYN attack, etc.
DoS/DDoS	Prevent online services
Rogue SSL certificate	Man-in-the-middle
…	

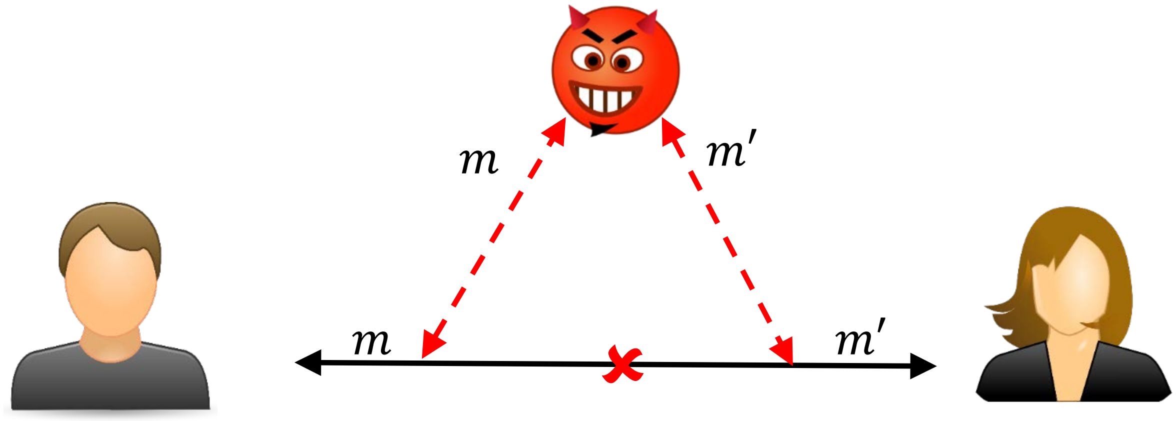
Examples of Attacks

Types of Attacks	Goals/Consequences
Malicious code	Execute viruses, scripts, etc to compromise system.
Virus hoax	Transmit a virus hoax with real virus attached.
Back door	Gain access to system via unauthorized method.
Password crack	Reverse-calculate a password to access information.
Brute force	Gain a password by trying all possible combinations.
Dictionary	Guess a password by using a set of common passwords.
DoS/DDoS/Mail Bombing	Block legitimate requests for services.
Spoofing	Gain unauthorized access to system/information.
Man-in-the-middle	Modify information during data transmission.
Spam	Waste system resources.
Sniffer	Monitor network data to steal/analyse information.
Phishing	Obtain private information.
Social engineering	Gain access of information by convincing people.
…	

Examples

- Man-in-the-Middle (MITM) Attack
- Distributed Denial-of-Service (DDoS) Attack

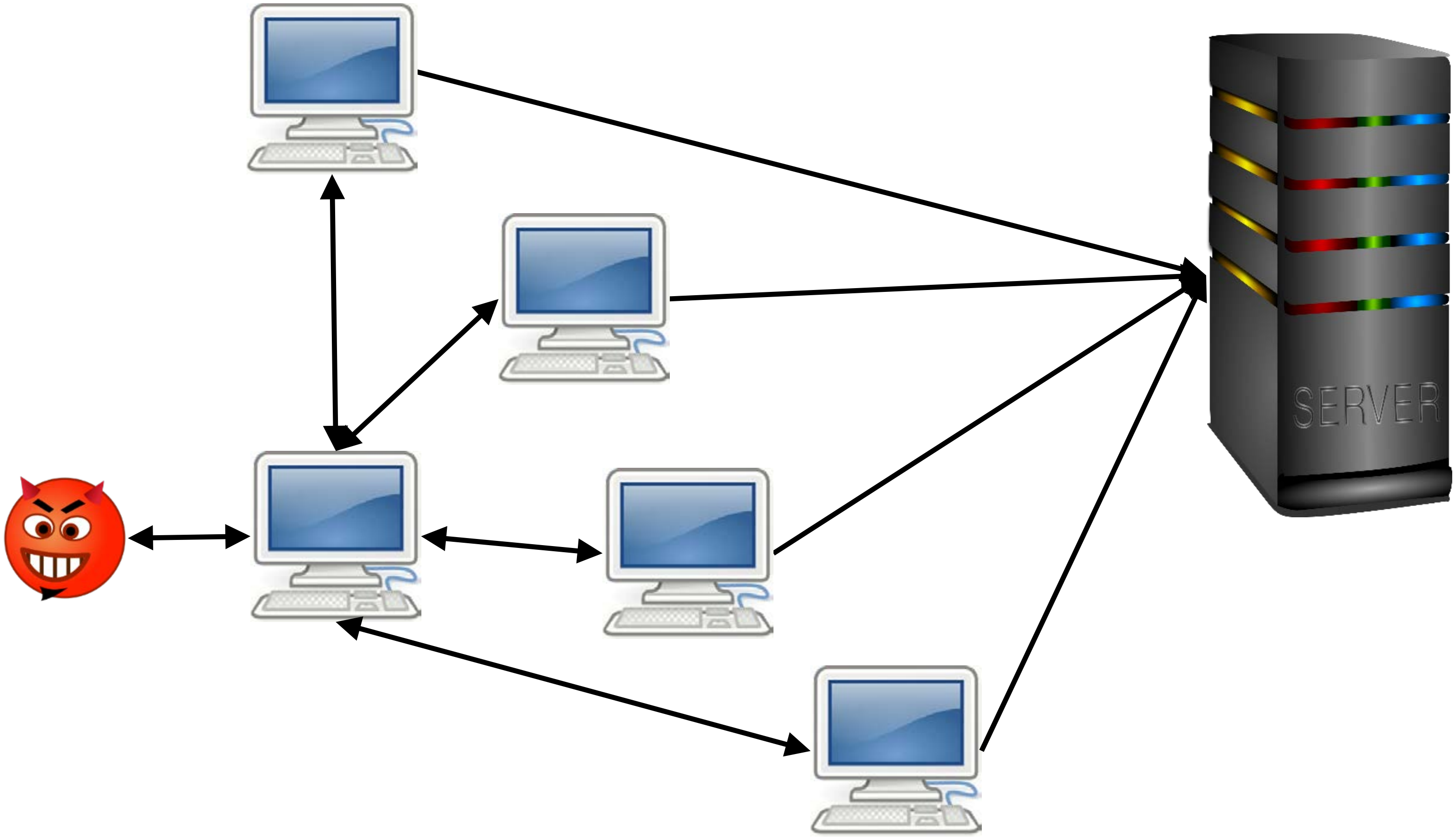
Man-in-the-Middle (MITM)



What security properties might be violated?

General and Powerful Attack

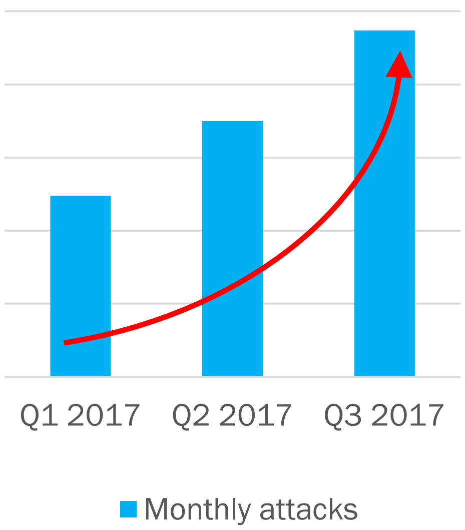
DDoS



DDoS

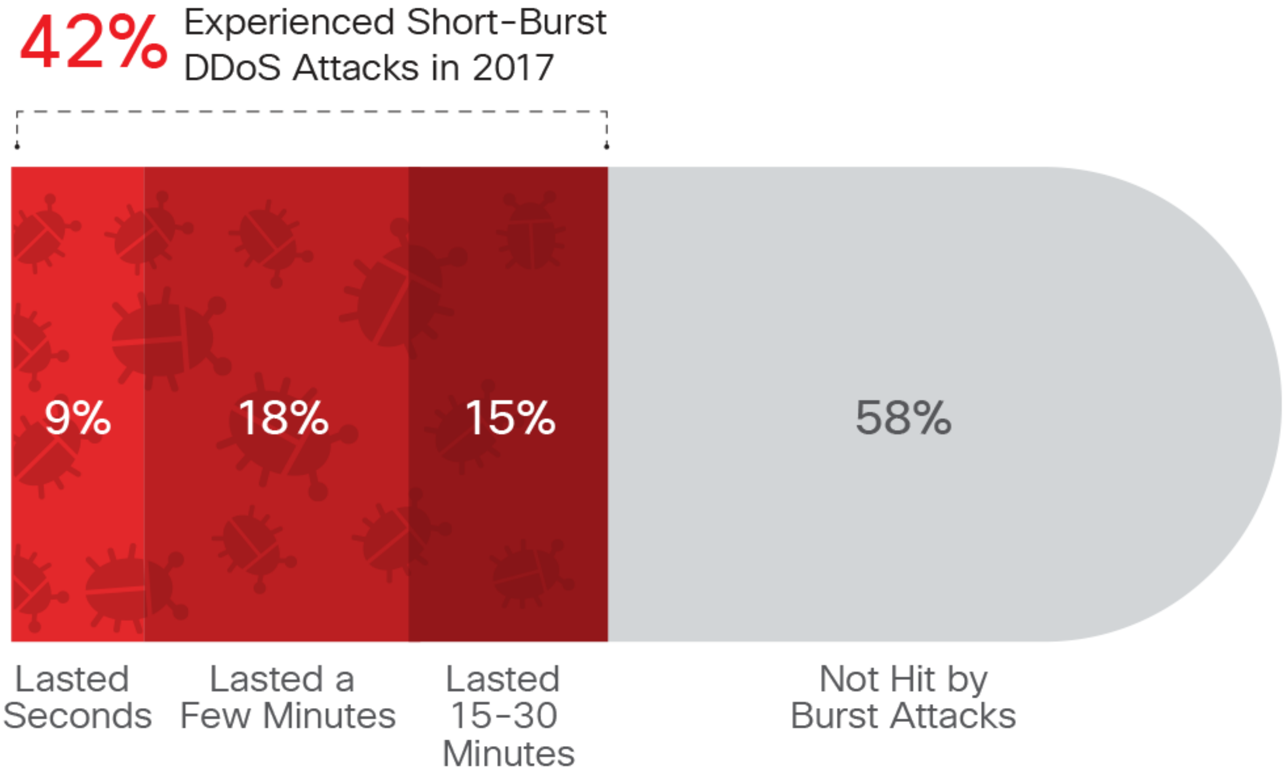
- Computers are harder to control
  - *Security improvement*

- Internet of Things
  - *Lack of security protection mechanisms.*
  - *Large scale*
  - *Make DDoS attack cheaper and easier*



- Dramatic increment benefit from “advantages” of IoT.

DDoS

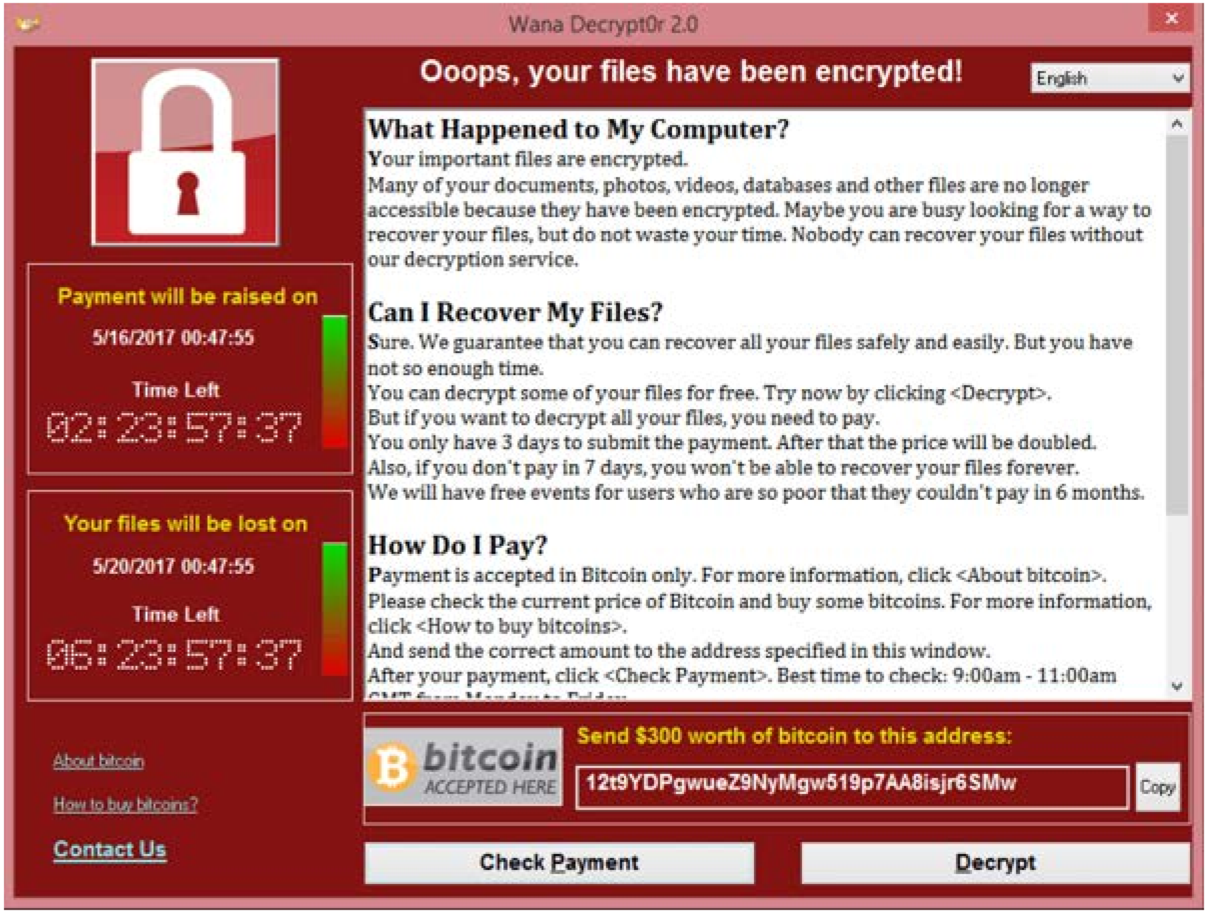


Source: Radware

Ransomware

- Lock computer system, mobile phones or data, attacker is seeking a ransom to release.
  - *Encryption*
  - *Disable system services*
  - *…*
- Victims are asking to
  - *Pay*
  - *Buy*
- Example
  - *WannaCry (bitcoin)*

Example



Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

Tools for Security Protection

- Cryptography
- Intrusion detection system
- Access control
- Firewall
- Anti-virus
- Security protocols/systems
- System monitors
- …