EECS 3482

Introduction to Computer Security

Introduction to Information/Computer Security

Instructor: N. Vlajic, Fall 2021

Learning Objectives

Upon completion of this material, you should be able to:

- Describe the key security requirements of confidentiality, integrity and availability (CIA).
- Describe the CNSS security model (McCumber Cube).
- Identify today's most common threats and attacks against information.
- Distinguish between different main categories of malware.

Required Reading

Computer Security, Stallings: **Chapter 1**

Computer Security, Stallings: **Chapter 6**

Introduction

- **Computer** – general purpose device that can be programmed to carry out a set of arithmetic or logical operations automatically
  - examples:
    - desktops
    - laptops, tablets
    - mobile phones
    - printers, servers
    - routers, firewalls
    - IoT devices
    - industrial controllers …

  - **alternative definition**: electronic device for storing and processing of data/information

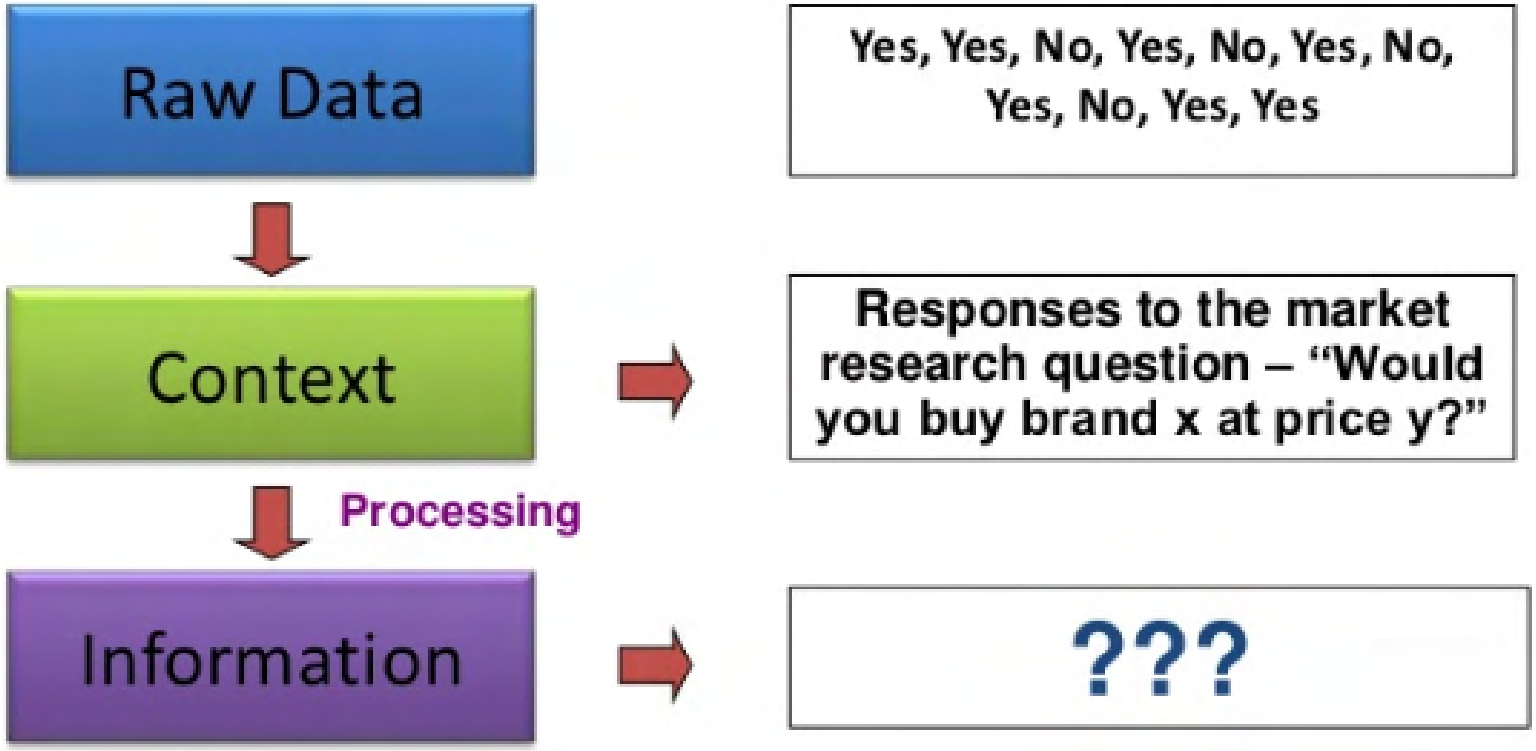
Introduction (cont.)

- **Data vs. Information**

Data	Information
• Raw Facts • Unorganized • Unprocessed • Chaotic or Unsorted • Input to a Process	• Useful & Relevant • Organized • Processed • Ordered or Sorted • Output of a Process
01000111 11101100 10100001 00111010 01011101 00001101 …	lottery win: $238,000.00

In many organizations, information/data is seen as the most valuable asset !!!

Introduction (cont.)

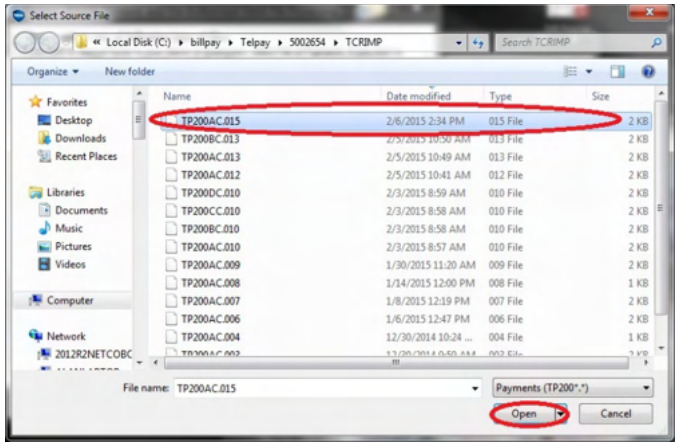


http://www.slideshare.net/mrcox/btec-national-in-ict-unit-3-data-vs-information

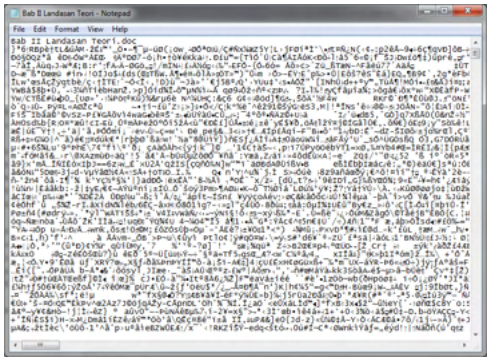
Introduction (cont.)

Question:

Does compromise to/of data always lead to compromise of information??



Think of an encrypted file …



Introduction (cont.)

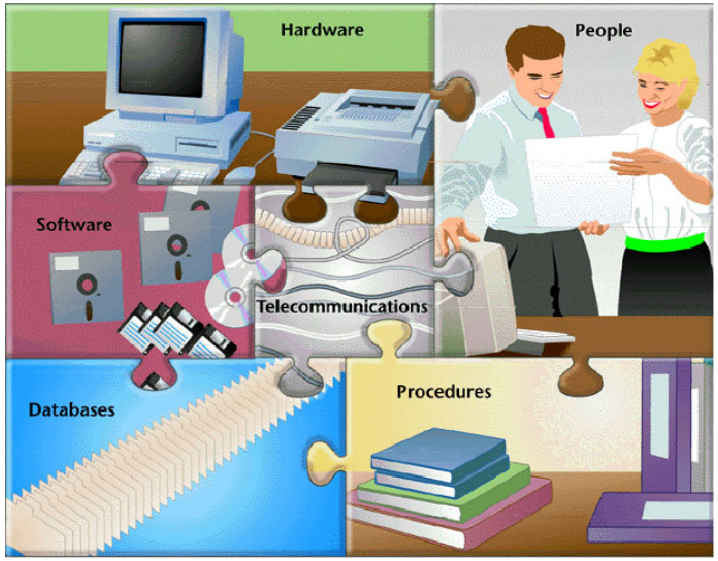
- **Information Technology** – technology involving development OR use of computer systems & networks for the purpose of processing & distribution of data/information

  - categories of IT jobs:
    - IT engineer - develops new or upgrades existing IT equipment (software or hardware)
    - IT architect - draws up plans for IT systems and how they will be implemented
    - IT administrator - installs, maintains, repairs IT equip./system
    - IT manager - oversees other IT employees, has authority to buy technology and plan budgets
    - IT security specialist - creates and executes security applications to maintain system security and safety

Introduction (cont.)

IT System

- **Information System** – entire set of **data** as well as **software**, **hardware**, **networks**, **people**, **procedures & policies** that deal with processing & distribution of information (data) in an organization
  - each component has its own strengths, weaknesses, and its own *security requirements*



Information/data is
- stored on computer hardware,
- manipulated by software,
- transmitted by networks,
- used by people,
- controlled by procedures & policies

Introduction (cont.)

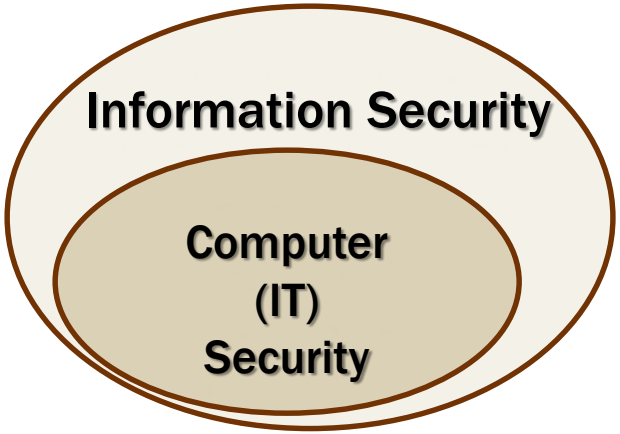
Security = state of being secure, free from danger.

- **Information Security** – practice of defending digital information from unauthorized
  - access
  - use
  - recording
  - disruption
  - modification
  - destruction, …

C.I.A.

Introduction (cont.)

- **Computer Security vs. Information Security**
  - terms are often used interchangeably, but …
  - computer security (aka IT security) is mostly concerned with information in 'digital form'
  - information security is concerned with information in any form it may take: electronic, print, etc.



- **Information System** – entire set of data as well as software, hardware, networks, people, procedures & policies ...

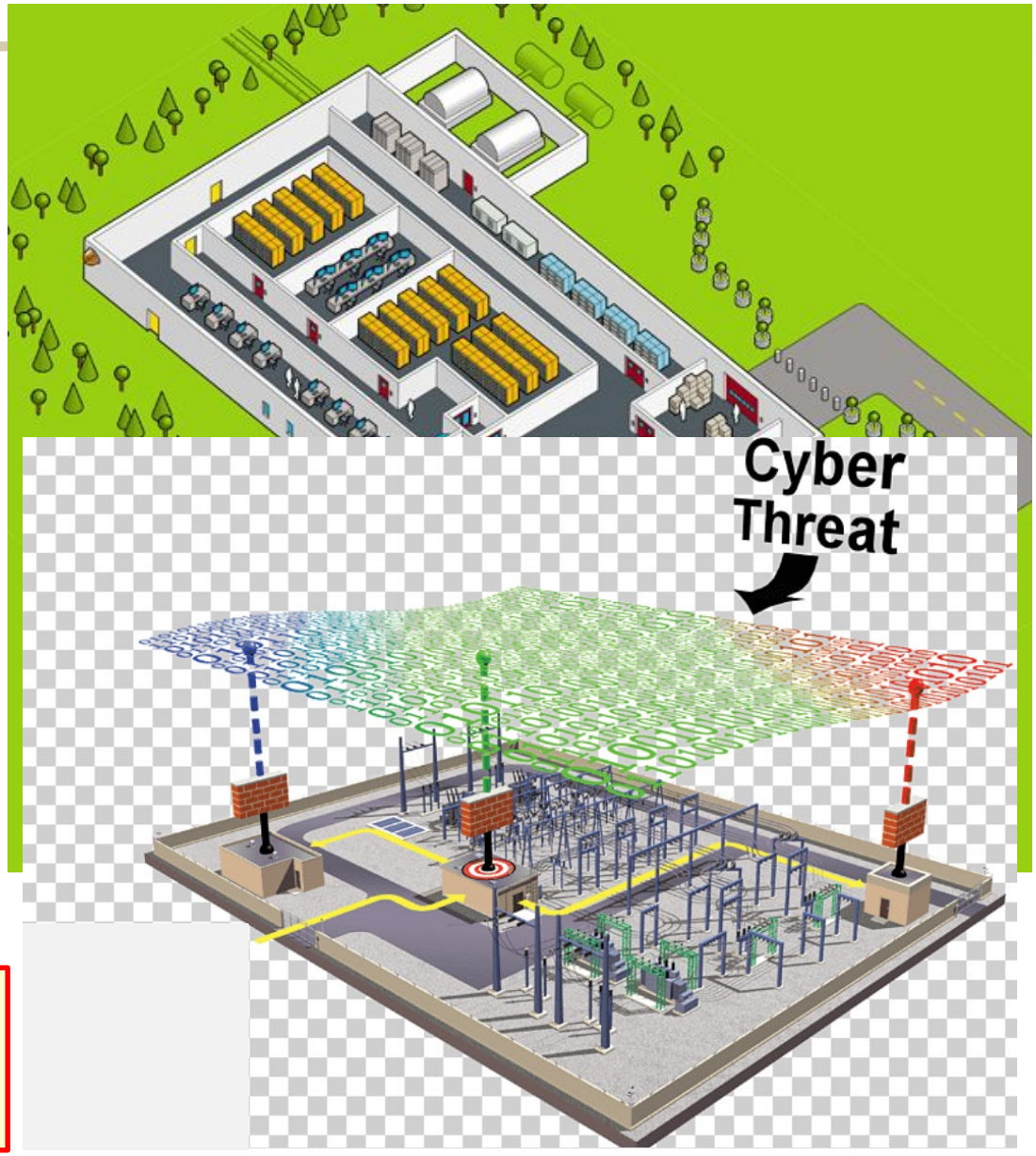
Consider a data center with perfectly protected IT system, from the **digital / computer** perspective.

Is DATA in this center safe ??

flood

fire

earthquake



Non-digital security should NOT be overlooked!!!

Introduction (cont.)

Data Center Security is much more than digital

1. **Build on the right spot.**
   avoid locations prone to earth-quakes, floods, hurricanes, … near high-ways and airports

3. **Pay attention to walls.**

4. **Avoid windows.**

6. **Keep a 100-foot buffer zone around the site.**
   in case of deliberate vandalism …

13. **Plan for secure air handling.**
    prevent overheating or injection of biological and chemical substances from outside

18. **Prohibit food in the computer rooms.**
    spillages or infestation can lead to equipment / data damage

https://www.cisco-eagle.com/blog/2008/01/30/data-center-security-is-much-more-than-digital/

http://www.csoonline.com/article/2112402/physical-security/physical-security-19-ways-to-build-physical-security-into-a-data-center.html?page=3

Introduction (cont.)

CISSP®

Certified Information Systems Security Professional

Environmental and life safety controls

- **Class A** – fires are common combustibles such as wood, paper, etc. This type of fire is the most common and should be extinguished with water or soda acid.
- **Class B** – fires are burning alcohol, oil, and other petroleum products such as gasoline. They are extinguished with gas or soda acid. You should never use water to extinguish a class B fire.
- **Class C** – fires are electrical fires which are fed by electricity and may occur in equipment or wiring. Electrical fires are Conductive fires, and the extinguishing agent must be non-Conductive, such as any type of gas.
- **Class D** – fires are burning metals and are extinguished with dry powder.
- **Class K** – fires are kitchen fires, such as burning oil or grease. Wet chemicals are used to extinguish class K fires.

Introduction (cont.)

Must know!

- **Types of Fires & Fire Extinguishers**

Type (Fire / Extinguisher)	CLASS A Combustible materials (e.g. paper & wood)	CLASS B Flammable liquids (e.g. paint & petrol)	CLASS C Flammable gases (e.g. butane and methane)	CLASS D Flammable metals (e.g. lithium & potassium)	Electrical Electrical equipment (e.g. computers & generators)	CLASS F Deep fat fryers (e.g. chip pans) cooking oil	Comments
Water	✓	✗	✗	✗	✗	✗	Do not use on liquid or electric fires
Foam	✓	✓	✗	✗	✗	✗	Not suited to domestic use
Dry Powder	✓	✓	✓	✓	✓	✗	Can be used safely up to 1000 volts
CO2	✗	✓	✗	✗	✓	✗	Safe on both high and low voltage
Wet Chemical	✓	✗	✗	✗	✗	✓	Use on extremely high temperatures

https://surreyfire.co.uk/types-of-fire-extinguisher/

Introduction (cont.)

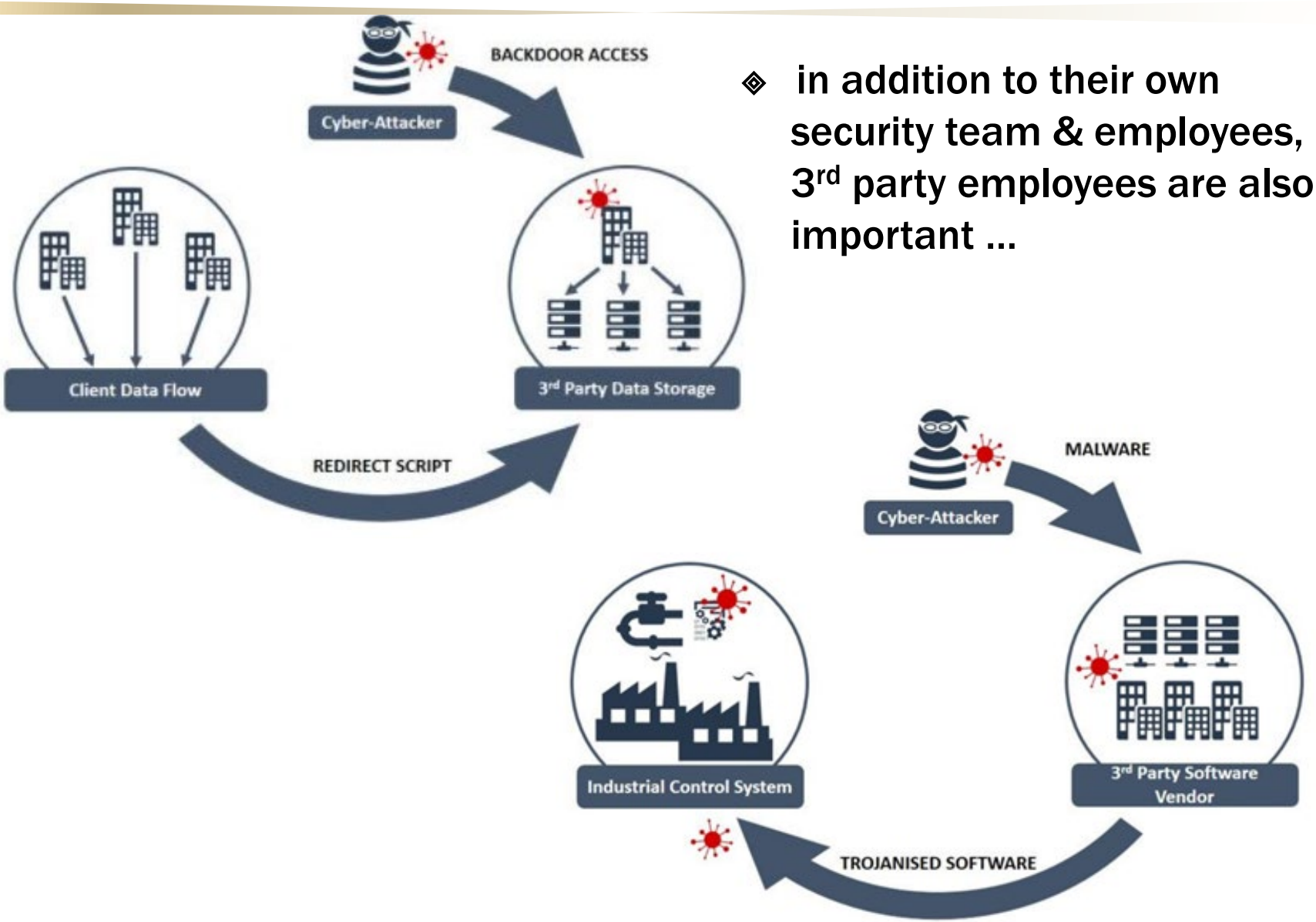
Introduction (cont.)

- **Who is responsible for 'security of information'?**

"In the last 20 years, technology has permeated every facet of the business environment. The business place is no longer static – it moves whenever employees travel from office to office, from office to home, from city to city. Since business have become more fluid, …, information security is no longer the sole responsibility of a small dedicated group of professionals, …, it is now the responsibility of EVERY employee …."

https://www.business.att.com/learn/research-reports/cybersecurity-isnt-just-for-the-it-team-to-manage.html

• Role of 'Supply Chain' / 3rd Party Businesses ...



- in addition to their own security team & employees, 3rd party employees are also important ...

Introduction (cont.)

- **BYOD – the good and the bad**

Bring Your Own Device

Managing The BYOD Revolution

Thousands of organizations around the world are going BYOD to save money and improve productivity by allowing more end-users to use their own personal devices in the office, classroom or out in the field.

BENEFITS OF BYOD

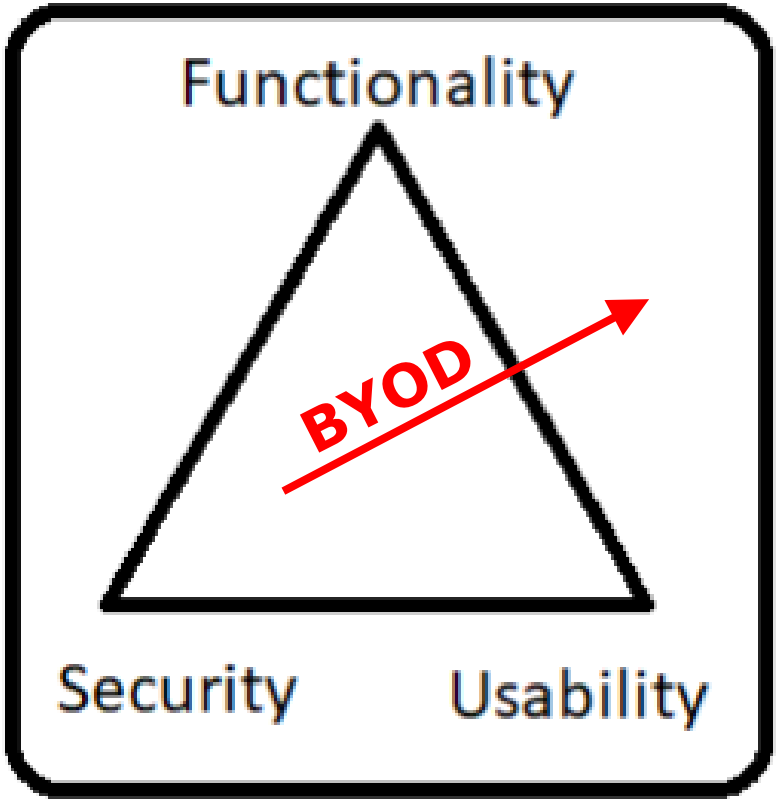
It's expensive for organizations to purchase new or update old technology systems and devices	Organizations, schools and governments are recognizing how technology and mobile access can enhance learning, working and general productivity	Organizations with limited resources and tight budgets want cost-effective ways to increase access to technology	Studies show that most employees prefer to use their own devices rather than those issued by their organizations	Employees in the workplace and students in educational environments can use the devices they already own like laptops, tablets and mobile phones to connect to company IT resources

Source: BrightPath Foundation

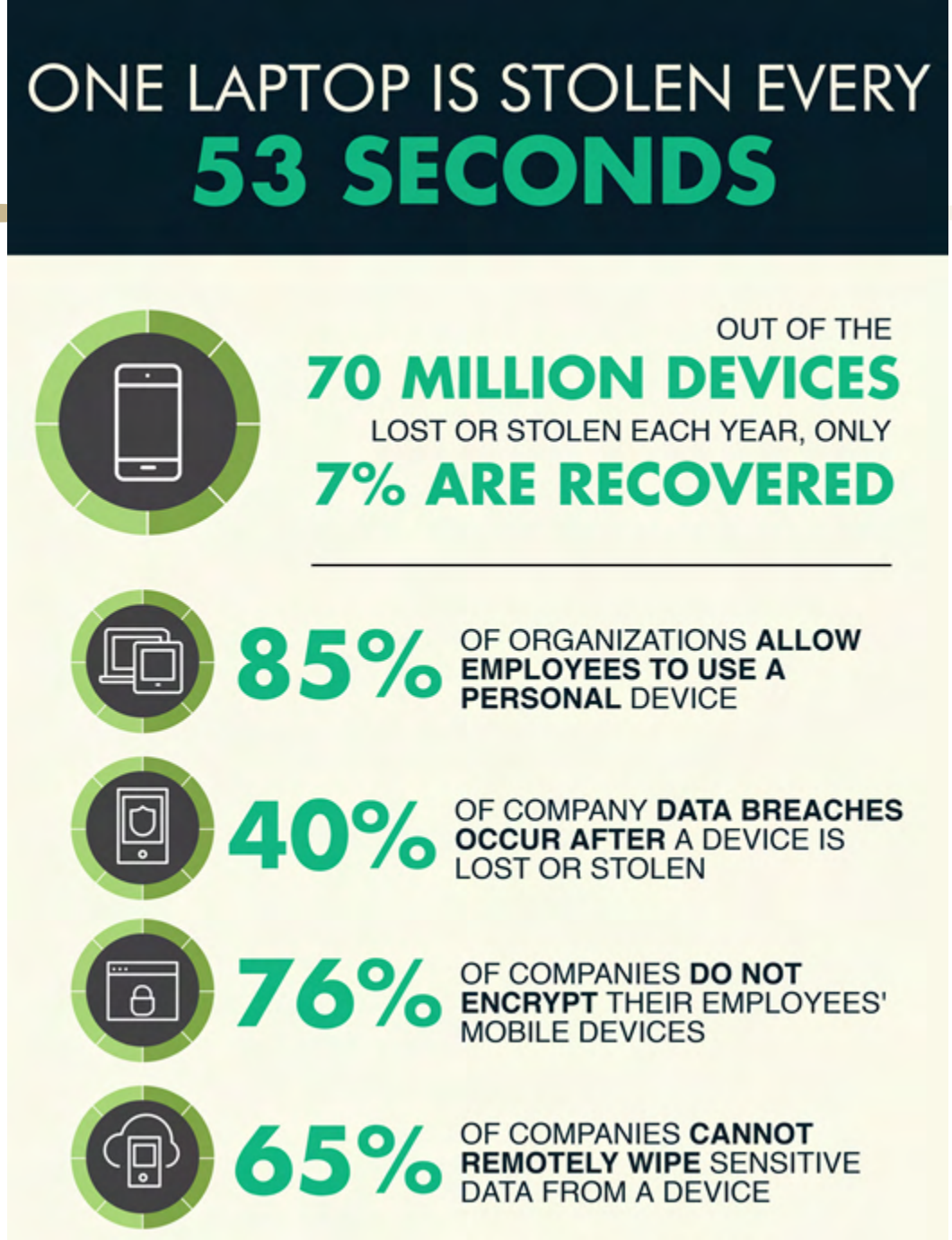
http://lawinquebec.com/wp-content/uploads/2013/06/BYOD.jpg

Introduction (cont.)

- BYOD – the good and the bad (cont.)



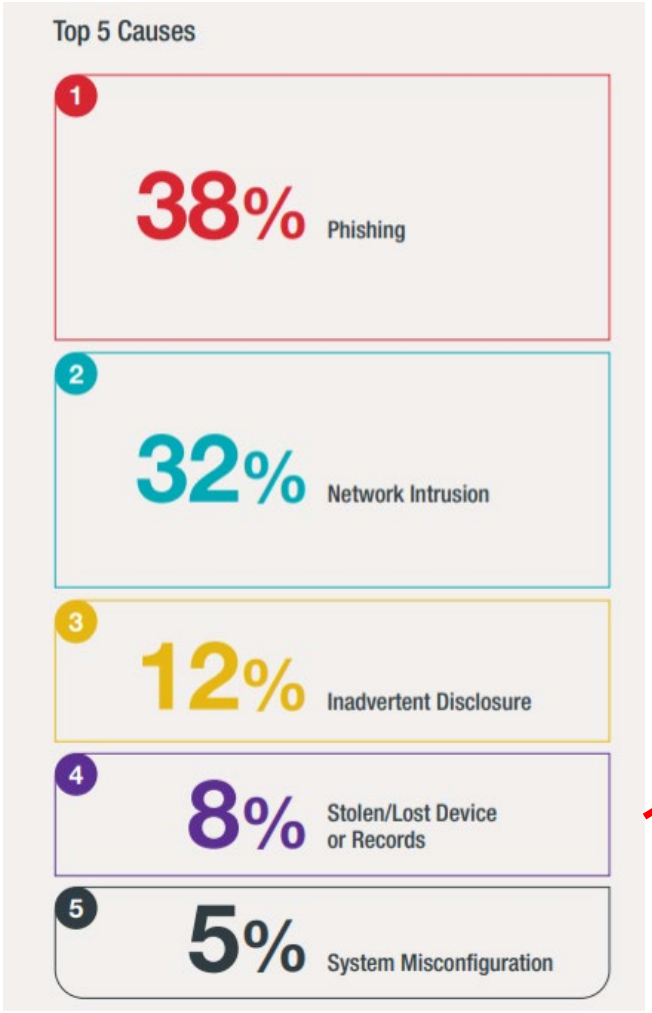
3 main aspects of technology use.



https://www.mxotech.com/2019/06/three-serious-byod-security-risks-every-business-owner-should-know-about/

Introduction (cont.)

Causes of Incident Response in Cyber Security



en.wikipedia.org › wiki › BakerHostetler

BakerHostetler - Wikipedia

BakerHostetler is an American 1,000-attorney law firm founded in 1916. One of the firm's founders, Newton D. Baker, was U.S. Secretary of War during World ...

Headquarters: None (first office was in Cleve… **No. of offices:** 17
No. of attorneys: 1,000 **Revenue:** $732 million (2020)

Humans are the weakest link !!!

1,000+
Incidents in 2019

2020 BakerHostetler Data Security Incident Response Report
https://f.datasrvr.com/fr1/620/24943/2020_DSIR_Report_(003).pdf

Organization	Description of security breach	Number of identities exposed
Grays Harbor Pediatrics, WA	A backup tape, stolen from an employee's car, was used for storing copies of paper records; patients may have had their names, Social Security numbers, insurance details, driver's license information, immunization records, medical history forms, previous doctor records, and patient medical records stolen	12,000
Tulane University, LA	A university-issued laptop was stolen from an employee's car. It was used to process 2010 tax records for employees, students, and others; the information included names, Social Security numbers, salary information, and addresses	10,000
Seacoast Radiology, NH	Patient names, Social Security numbers, addresses, phone numbers, and other personal information were exposed by a security breach	231,400
Centra, GA	A laptop was stolen from the trunk of an employee's rental car that contained patient names and billing information	11,982
Stony Brook University, NY	Student and faculty network and student IDs were posted online after a file with all registered student and faculty ID numbers was exposed	61,001
deviantART, Silverpop Systems Inc., CA	Attackers exposed the e-mail addresses, usernames, and birth dates of the entire user database	13,000,000
Twin America LLC, CitySights, NY	An attacker inserted a malicious script on a Web server and stole the customer database that contained customer names, credit card numbers, credit card expiration dates, CVV2 data, addresses, and e-mail addresses	110,000
Ohio State University, OH	Unauthorized individuals logged into an Ohio State server and accessed the names, Social Security numbers, dates of birth, and addresses of current and former students, faculty, staff, University consultants, and University contractors	750,000
Gawker, NY	Attackers gained access to the database and accessed staff and user e-mails and passwords	1,300,000

NEWS ANALYSIS

Attackers hack European Space Agency, leak thousands of credentials 'for the lulz'

A group of hackers operating under the Anonymous banner hacked the European Space Agency (ESA) and leaked the data for no reason other than for "lulz." Over 8,000 people will not find anything amusing about the breach since their names, email addresses and passwords were posted in one of three data dumps on JustPaste.it.

CSO's Steve Ragan analyzed the 8,107 passwords exposed, finding 39% (3,191) were three-character passwords, 16% (1,314) were eight-characters passwords which could have easily been cracked, and only 22 20-character passwords; the longest password had 24 characters with the rest of the leaked passwords falling somewhere in-between the extremes.

OFFICIAL! Good passwords more difficult than rocket science

https://www.computerworld.com/article/3014539/attackers-hack-european-space-agency-leak-thousands-of-credentials-for-the-lulz.html

https://nakedsecurity.sophos.com/2015/12/16/official-good-passwords-more-difficult-than-rocket-science/

C.I.A. of Information Security

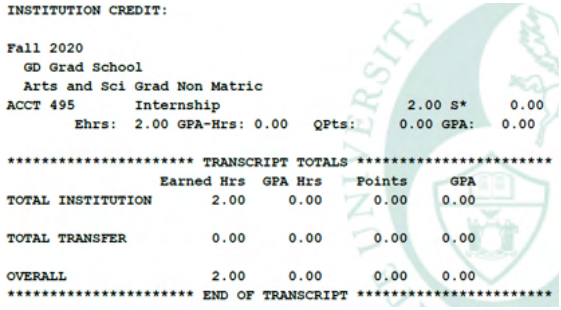
- **C.I.A. Triangle** – 3 key characteristics of information that must be protected by information security:
  - **confidentiality** - only authorized parties can view private information
  - **integrity** - information is changed only in a specified and authorized manner (by authorized users)
  - **availability** - information is accessible to authorized users whenever needed

Different organizations may view one of the CIA components as being more important than others!!!

C.I.A. of Information Security (cont.)

Example: DATA CONFIDENTIALITY

Student grade – an information asset of high importance for student.



INSTITUTION CREDIT:

Fall 2020
GD Grad School
Arts and Sci Grad Non Matric
ACCT 495 Internship 2.00 S* 0.00
Ehrs: 2.00 GPA-Hrs: 0.00 QPts: 0.00 GPA: 0.00

********** TRANSCRIPT TOTALS **********

	Earned Hrs	GPA Hrs	Points	GPA
TOTAL INSTITUTION	2.00	0.00	0.00	0.00
TOTAL TRANSFER	0.00	0.00	0.00	0.00
OVERALL	2.00	0.00	0.00	0.00

********** END OF TRANSCRIPT **********

- In US, release of such information is regulated by **Family Educational Rights and Privacy Act** (FERPA).

  Grade information should only be available to students, their parents and employees that require this information to do their job.

- In Canada, the same issue is regulated by **Personal Information Protection and Electronic Documents Act** (PIPEDA).

Technology

Greenwich University fined £120,000 for data breach

21 May 2018 Share

The University of Greenwich has been fined £120,000 ($160,000) by the Information Commissioner.

The fine was for a security breach in which the personal data of 19,500 students was placed online.

The data included names, addresses, dates of birth, phone numbers, signatures and - in some cases - physical and mental health problems.

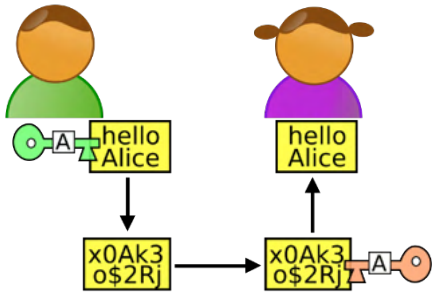
It was uploaded onto a microsite for a training conference in 2004, which was then not secured or closed down.

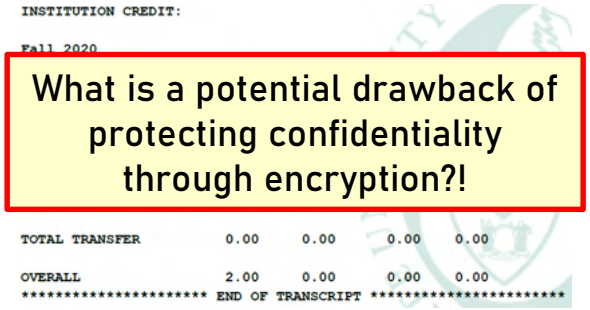
The Information Commissioner said Greenwich was the first university to receive a fine under the Data Protection Act of 1998 and described the breach as "serious".

C.I.A. of Information Security (cont.)

Example: How to ensure data confidentiality?

- cryptography




INSTITUTION CREDIT:

Fall 2020

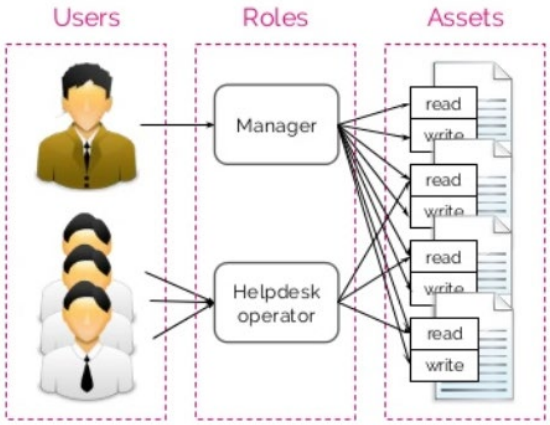
What is a potential drawback of protecting confidentiality through encryption?!

TOTAL TRANSFER	0.00	0.00	0.00	0.00
OVERALL	2.00	0.00	0.00	0.00

********** END OF TRANSCRIPT **********

- strong access control

only select (trusted) can access data – use 'strong' password



- limiting number of places where data can appear

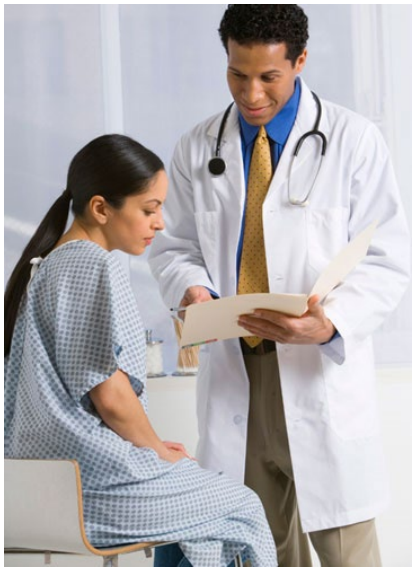
(e.g., cannot be stored on an USB)

C.I.A. of Information Security (cont.)

Example: DATA INTEGRITY

Patient information in a hospital – the doctor should be able to trust that the information is correct and current.

Inaccurate info could result in serious harm to the patient end expose the hospital to massive liability.



- In US, **Health Insurance Portability and Accountability Act** (HIPAA) regulates the collection, storage, and transmission of sensitive personal health care information.

  Hospital is responsible for safeguarding patient information against error, loss, defacing, tampering and unauthorized use.

  (Ontario's Personal Health Information Protection Act - PHIPA)

C.I.A. of Information Security (cont.)

Cottage Health, Touchstone Medical Imaging, and University of Rochester Medical Center (URMC): $3 million each

2019 saw three large HIPAA violations; $3 million each for Cottage Health & Touchstone Medical Imaging.

Cottage health was fined for two breaches — one in 2013 and another in 2015 — resulting in electronic protected health information (ePHI) affecting over 62,500 individuals being leaked. Both incidents involved servers holding ePHI being accessible over the internet.

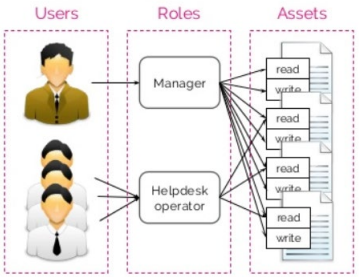
Tennessee-based Touchstone Medical Imaging was fined after leaving the protected health information (PHI) of over 300,000 patients available online through an exposed FTP server. Touchstone was notified about this exposure by the FBI in 2014 but claimed no patient PHI was exposed.

https://www.csoonline.com/article/3410278/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html

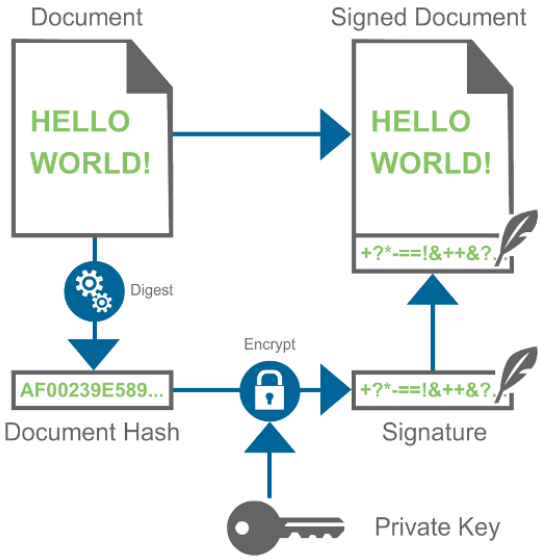
C.I.A. of Information Security (cont.)

Example: How to ensure data integrity?

- **strong access control** - good at preventing attacks on data integrity



- **cryptography (hashing)**
  - detects attacks on data integrity



- **documenting system activity (logging) - who did what and when** - detects attacks on data integrity

C.I.A. of Information Security (cont.)

Example: **DATA AVAILABILITY**

Accessible and properly functioning web site – a key asset for an e-commerce company.

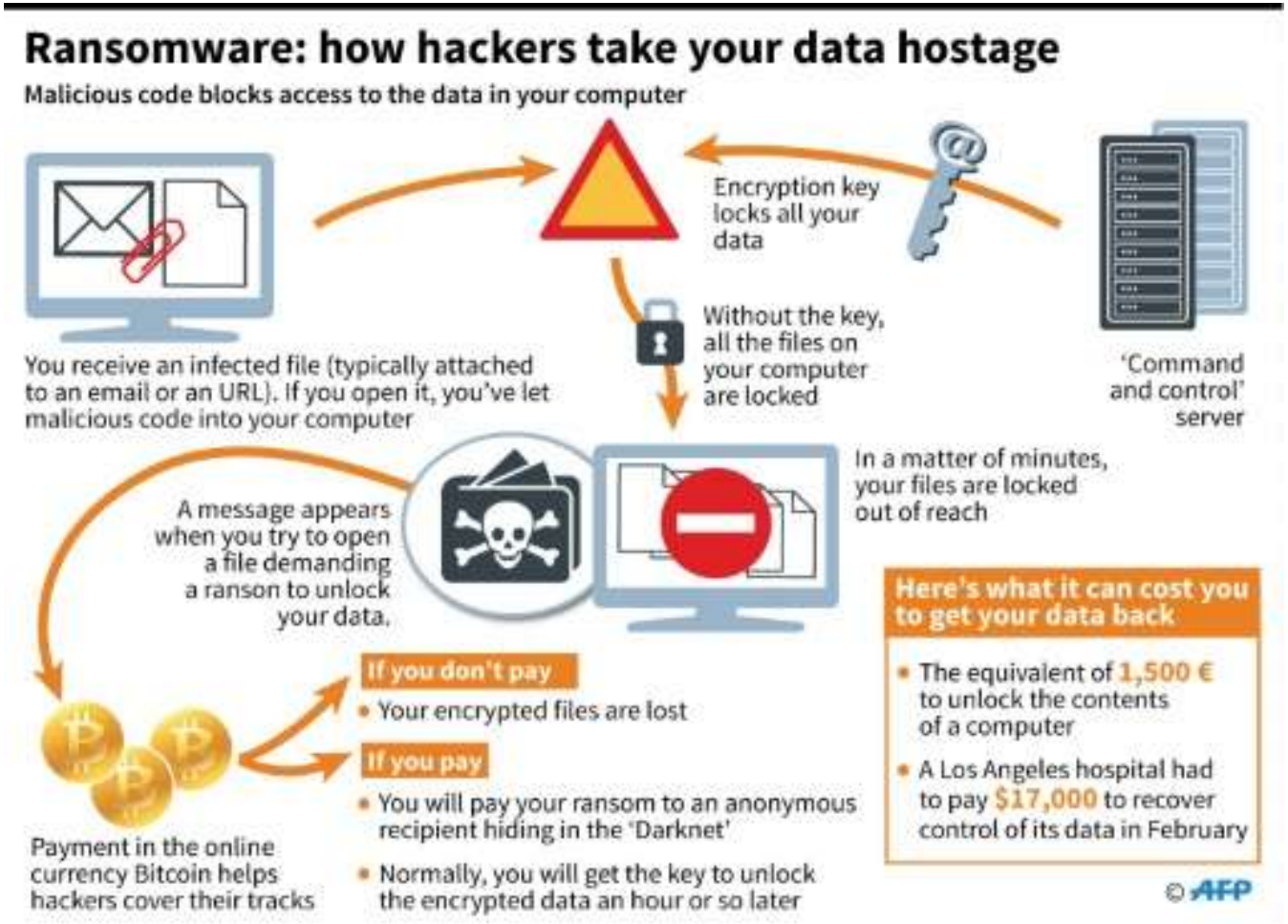
E.g., a **DDoS attack** could make the site unavailable and cause significant loss in revenue and reputation.

- In US, Computer Fraud and Abuse Act (CFAA) applies to DoS-related attacks.
- In Canada, DoS activities are regulated under Criminal Code of Canada, Section 342: Unauthorized Use of Computer

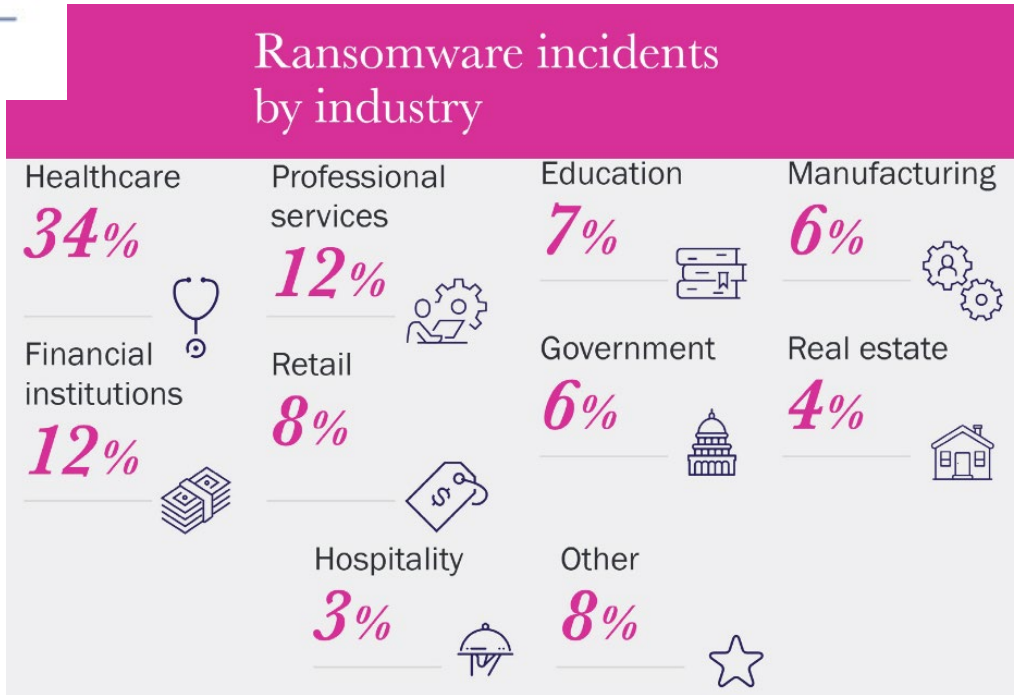
Do you know any other types of attack on data availability??

C.I.A. of Information Security (cont.)

- besides DoS, ransomware is another way to attack data availability



https://phys.org/news/2017-05-alarm-global-ransomware.html

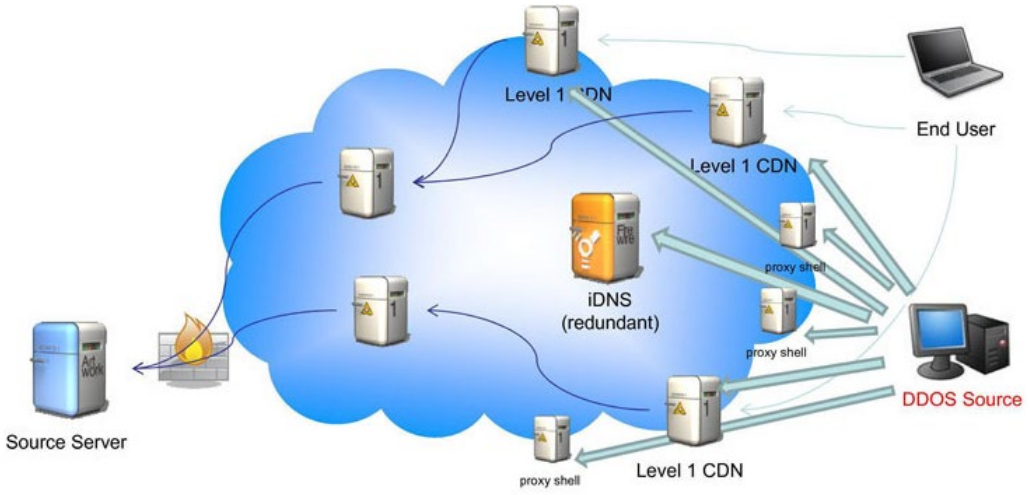


https://www.bleepingcomputer.com/news/security/70-percent-of-ransomware-attacks-targeted-smbs-bec-attacks-increased-by-130-percent/

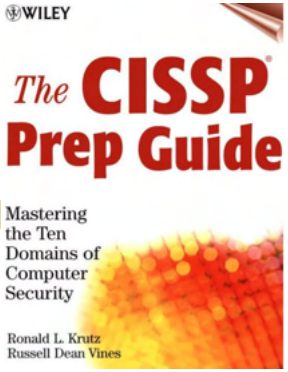
C.I.A. of Information Security (cont.)

Example: How to ensure data availability?

- **anti-DDoS system** (in case of attack that attempt to prevent access by blocking the bandwidth/server):
  e.g., content distribution networks, scrubbing centers



- **well established backup procedure** (in case of attacks that prevent access by encrypting or destroying data)



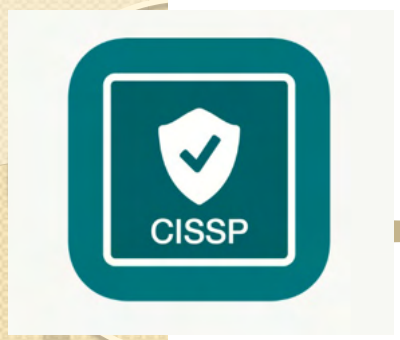
Related to information security, the guarantee that the message sent is the message received with the assurance that the message was not intentionally or unintentionally altered is an example of which of the following?

A. integrity

B. confidentiality

C. availability

D. identity



https://www.yeahhub.com/cissp/question-bank-05.php#answer

Which of the following is a principle of the CIA Triad that means authorized subjects are granted timely and uninterrupted access to objects?

A. Identification

B. Availability

C. Encryption

D. Layering

Alice, a York student, regularly backs up the content of her laptop on a portable hard-drive. By doing so, Alice is actually improving/strengthening:

A) confidentiality and integrity of her data

B) confidentiality and availability of her data

C) integrity and availability of her data

D) none of the above; portable hard-drives are generally a bad idea

C.I.A. of Information Security (cont.)

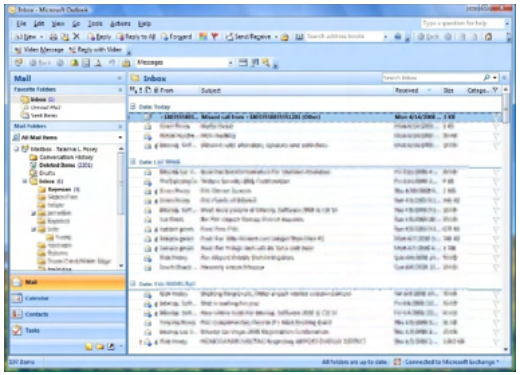
Example: CIA of different IT components

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted CD-ROM or DVD is stolen.	
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Table 1.3 Computer and Network Assets, with Examples of Threats.

C.I.A. of Information Security (cont.)

Example: attack on software ⇔ attack on data



attack on integrity of software

e.g., malware injected into email client or email server

could result in compromise of

- **data confidentiality**
- **data integrity**
- **data availability**

C.I.A. of Information Security (cont.)

Is there anything else to protect / add ???

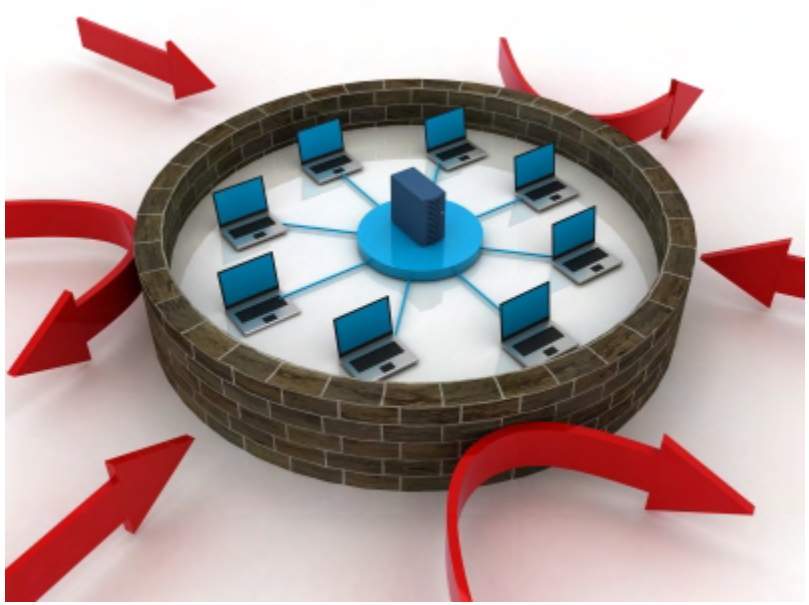
https://securityboulevard.com/2019/08/cia-triad-best-practices-for-securing-your-org/

C.I.A. of Information Security (cont.)

- **Extended C.I.A. Triangle** – some security experts feel that additional concept need to be added to (i.e., reinforced in) the traditional CIA triad:
  - **authenticity** - being able to verify that users are who they claim to be, and that each data input has come from a trusted source
  - **accountability** - being able to trace actions of an entity uniquely to that entity

Forensics, incident response

Where & how do we start evaluating and building/protecting a security system?

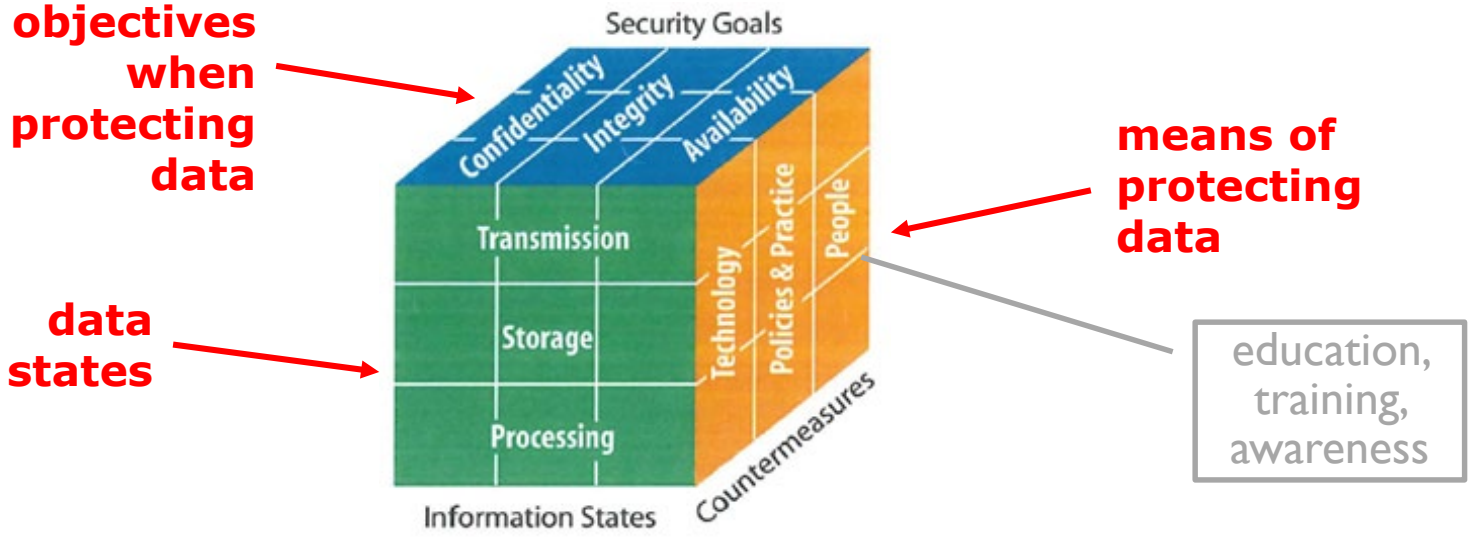


We know that we want to protect the CIA of data. But,

1) Data can reside in several different states.
2) Data can be attacked/protected in several different ways – e.g., through technology or through people.

CNSS Security Model

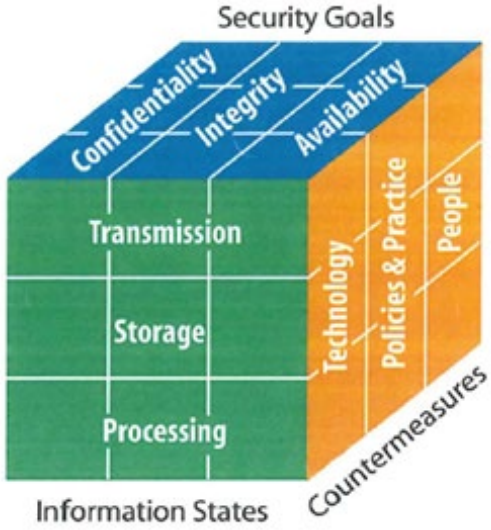
- **CNSS = Committee on National Security Systems**
- **McCumber Cube** – Rubik's cube-like detailed model for establishment & evaluation of info. security
  - to develop a secure system, one must consider not only key security goals (CIA) but also how these goals relate to various states in which information resides and full range of available security measures



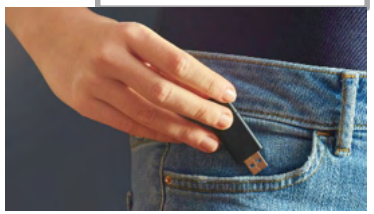
CNSS Security Model (cont.)

CNNS Category 2: Information States

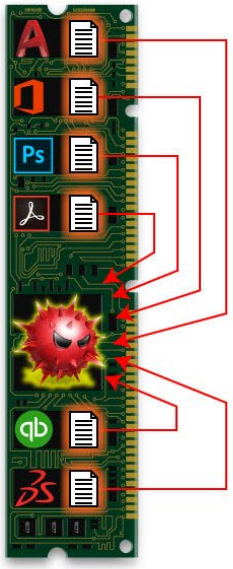
- **Storage** - aka '*data at rest*', is data stored in permanent (secondary) memory, such as hard disk, USB, removable drive
- **Transmission** - aka '*data in transit*' - data being transferred between systems, in <u>electronic form</u> OR <u>physical form</u>
- **Processing** - aka '*data in use*' - data being <u>actively examined</u> or <u>modified</u>



USB key taken out of office …

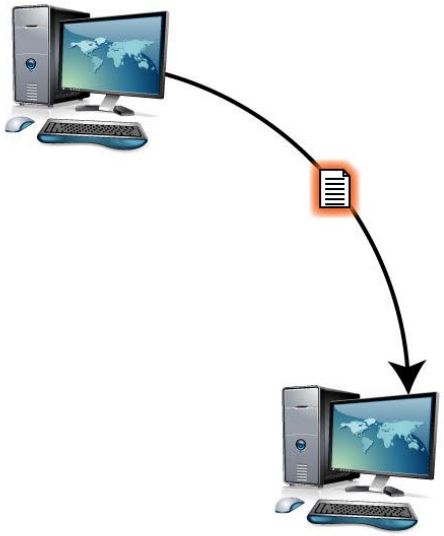


CNSS Security Model (cont.)



Data "In Use"

Data "At Rest"



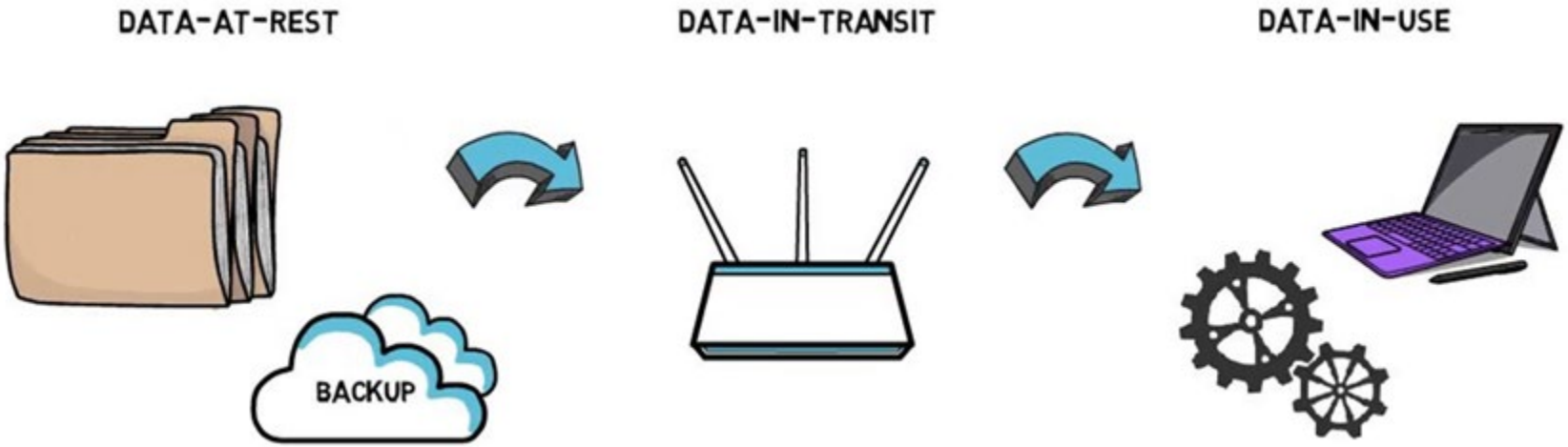
Data "In Transit"

Data In Use is when it is being processed by a running application, and is loaded in (RAM) memory (and then manipulated by the CPU) …
Open files (e.g., MSWord, PDF, …) are considered data In Use by respective applications.

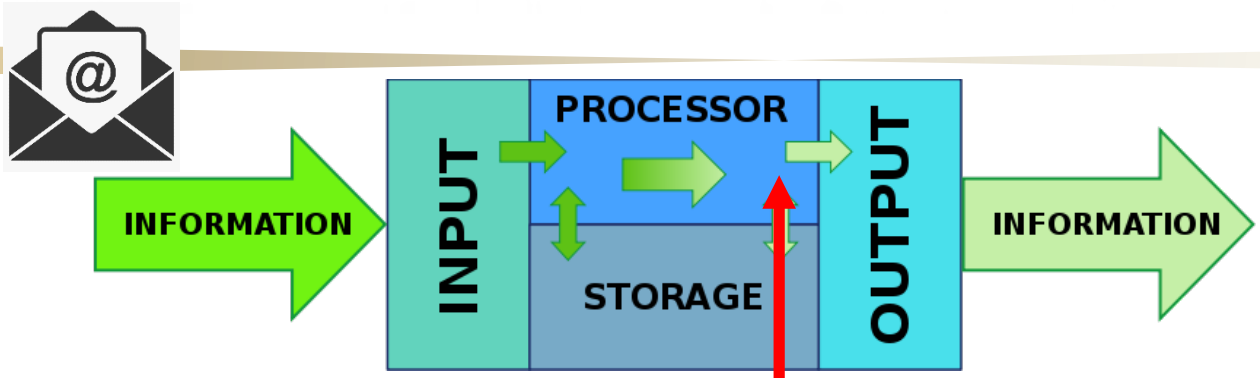
https://www.a1logic.com/2018/06/21/protecting-data-in-use/

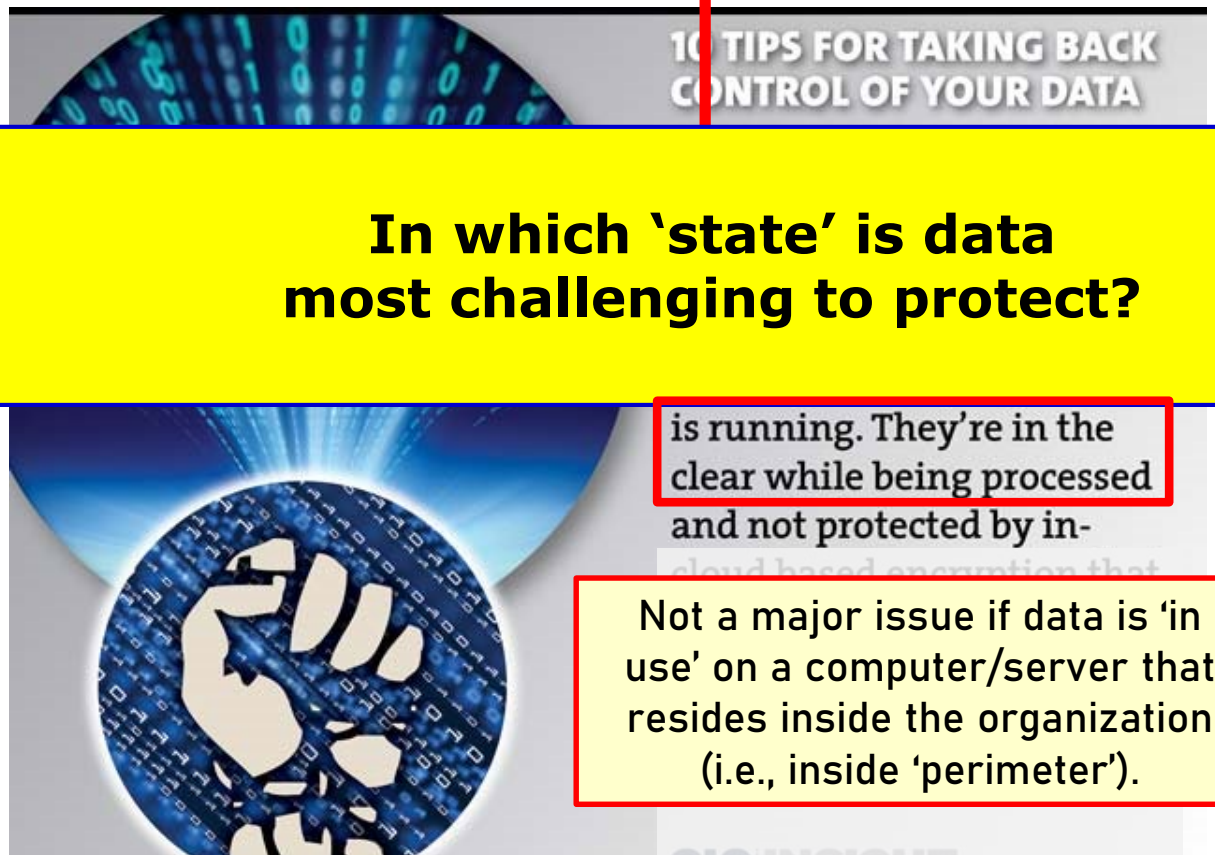
CNSS Security Model (cont.)

Example: Downloading of course notes …



CNSS Security Model (cont.)





In which 'state' is data most challenging to protect?

Not a major issue if data is 'in use' on a computer/server that resides inside the organization (i.e., inside 'perimeter').

CNSS Security Model (cont.)

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

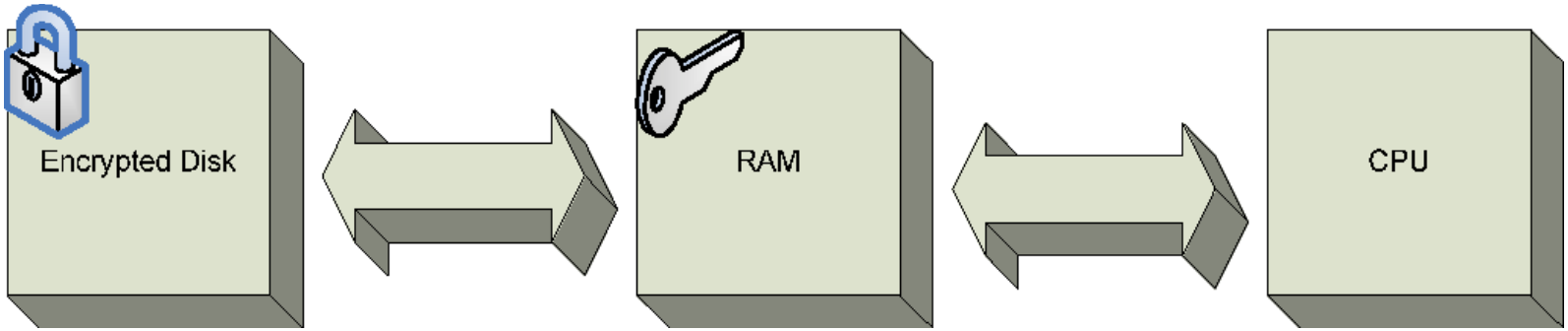
PUTTING ON A BRAVE FACE —

Intel promises Full Memory Encryption in upcoming CPUs

JIM SALTER - 2/26/2020, 2:29 PM

Data stored in the encrypted enclave is only decrypted within the CPU—and even then, it is only decrypted at the request of instructions executed from within the enclave itself.

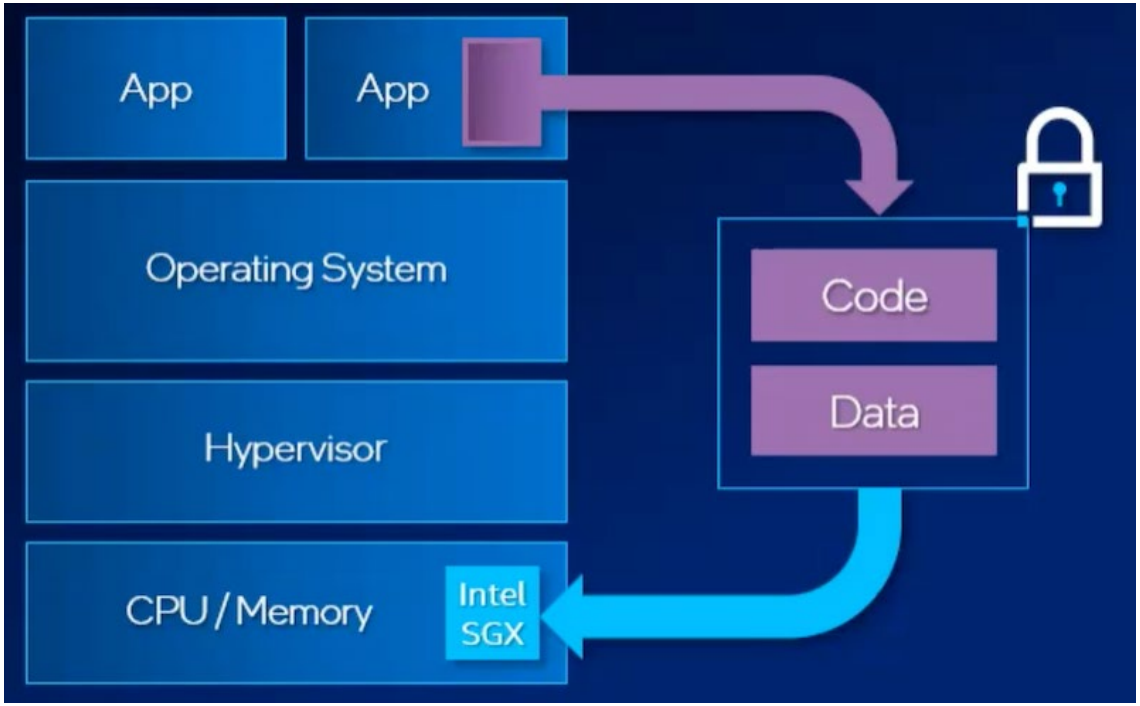
https://arstechnica.com/gadgets/2020/02/intel-promises-full-memory-encryption-in-upcoming-cpus/



CNSS Security Model (cont.)

Digging Deeper into the Zero Trust Nature of Intel SGX

June 24, 2021 • Add Comment • by Zach DeMeyer

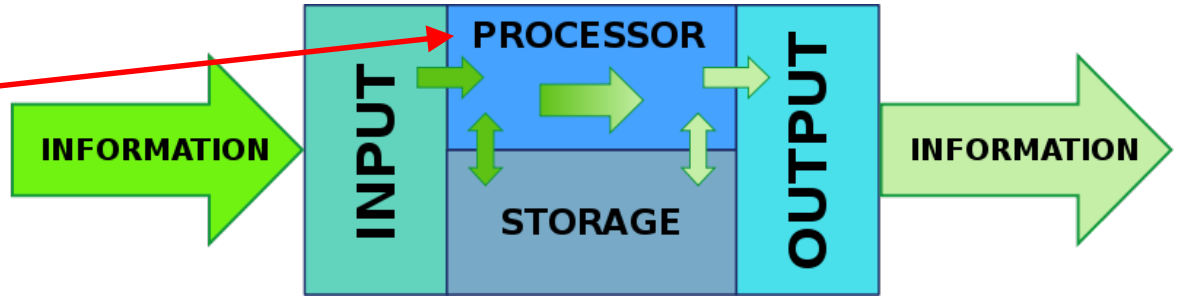


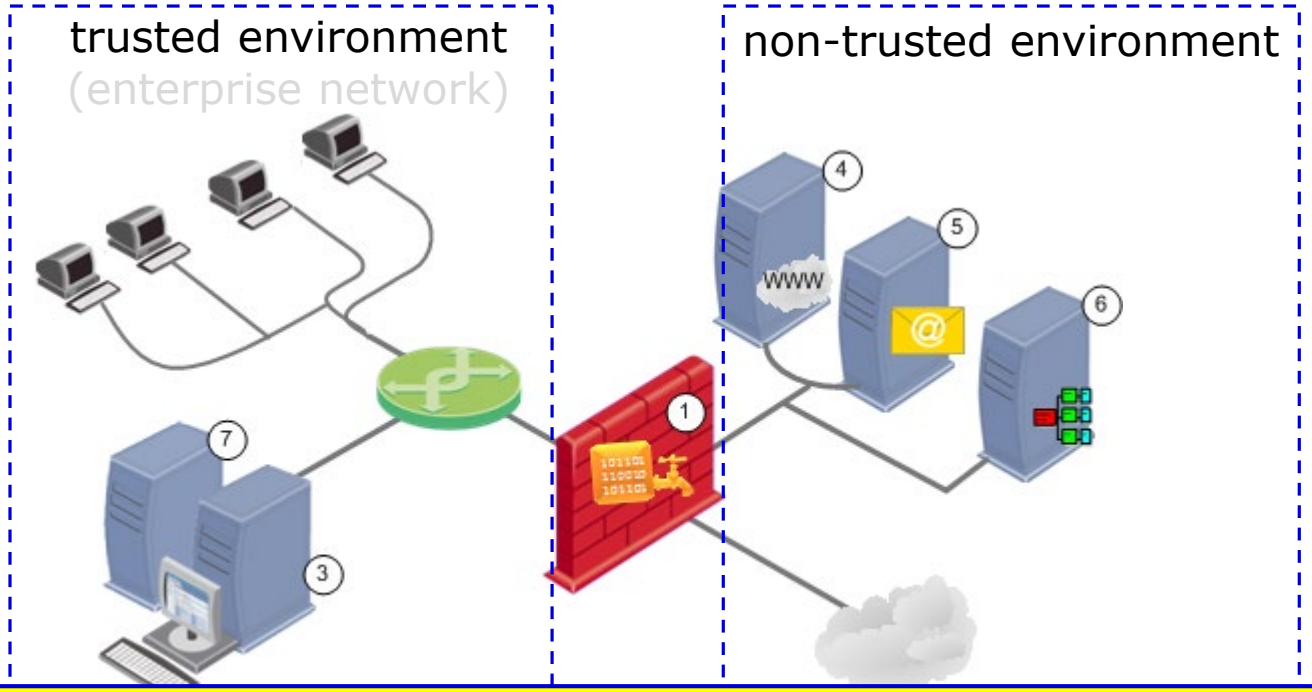
When configured, Intel SGX allocates a section of memory, now up to an entire terabyte, which is set aside as an encrypted data enclave.

Slower processing and still no 'in CPU' protection !!!

https://gestaltit.com/tech-talks/intel/intel-2021/zach/digging-deeper-into-the-zero-trust-nature-of-intel-sgx/

Not a major issue if data is 'in use' on a computer/server that resides inside the organization (i.e., inside 'perimeter').

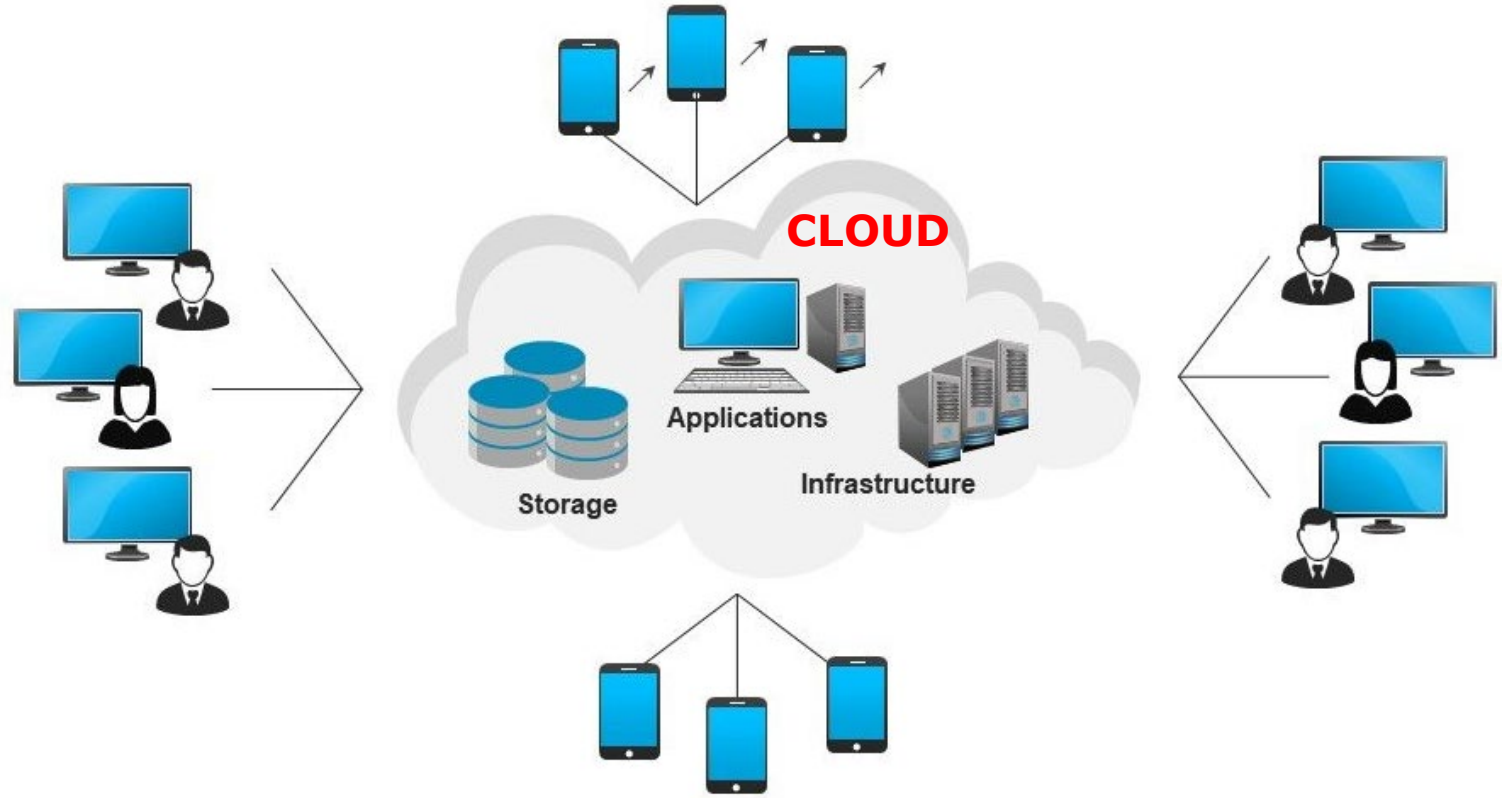




'Data in use' is not in danger in computers/systems that have other protections in place (access control, firewall, antivirus, …).

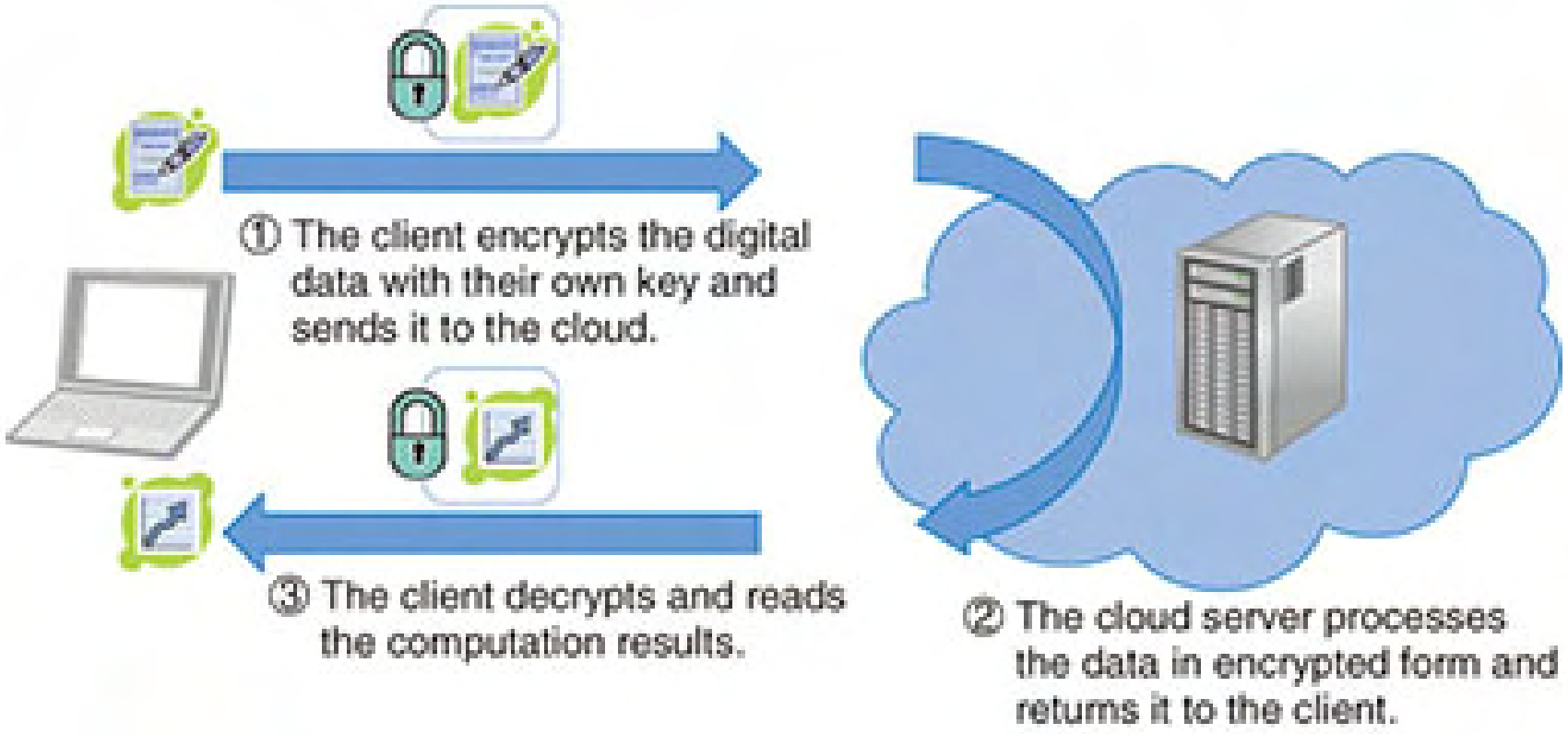
CNSS Security Model (cont.)

But, what if data is 'in use'
outside the trusted network/environment?!
(e.g., in case of Cloud Computing)



CNSS Security Model (cont.)

Example: Protection of Data in the Cloud

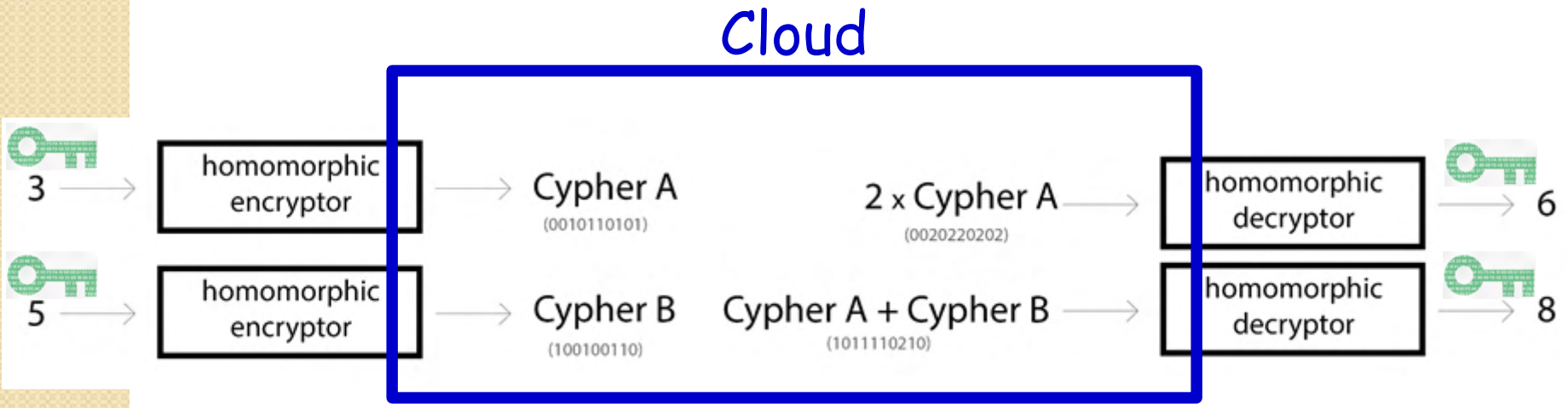


https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201407fa5.html

CNSS Security Model (cont.)

Example: Homomorphic Encryption

Homomorphic Encryption is a special type of encryption though. It allows someone to modify the encrypted information in specific ways *without being able to read the information*. For example, homomorphic encryption can be performed on numbers such that multiplication and addition can be performed on encrypted values without decrypting them. Here are a few toy examples.



https://iamtrask.github.io/2017/03/17/safe-ai/

CNSS Security Model (cont.)

Example: Homomorphic Encryption (cont.)

Performance

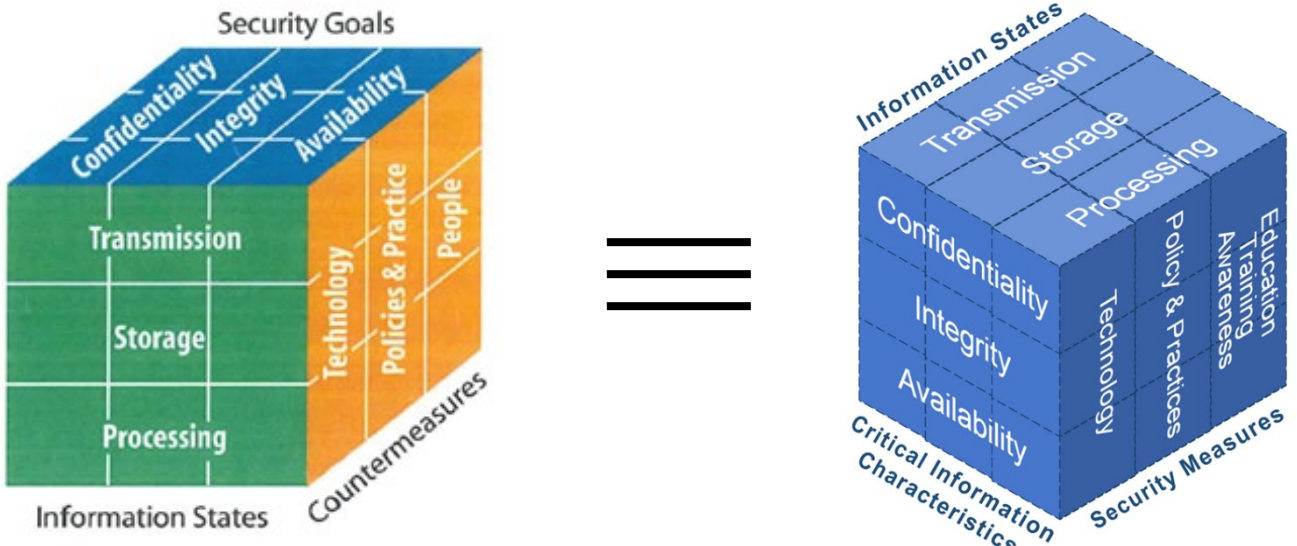
- A little slow…
- First working implementation in mid-2010, ½ -hour to compute a single AND gate
  - 13-14 orders of magnitude slowdown vs. computing on non-encrypted data
- A faster "dumbed down" version
  - Can only evaluate "very simple functions"
  - About ½-second for an AND gate

http://www.slideshare.net/NYTechCouncil/computing-on-encrypted-data

CNSS Security Model (cont.)

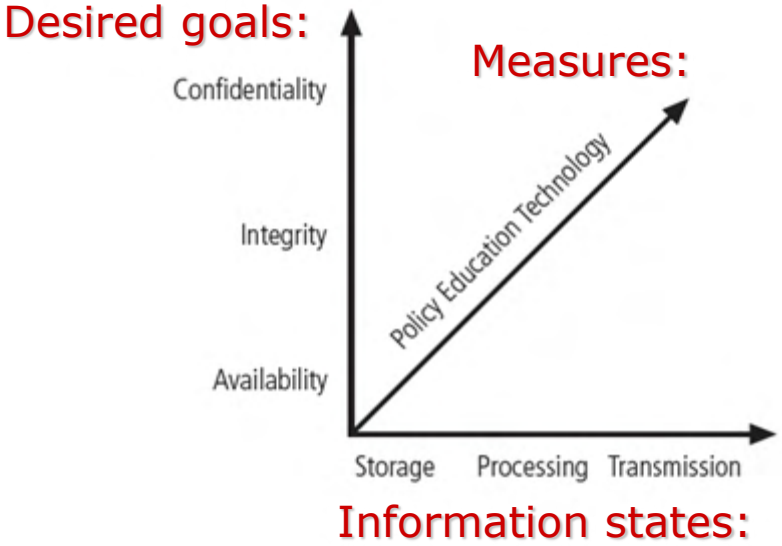
CNSS Category 3: Countermeasures/Safeguards

- **Technology** - software and hardware solutions (e.g., antivirus, firewall, IDS system, cryptography, backups, etc.)
- **Policy and practices** - administrative controls, such as management directives (e.g., acceptable use policies)
- **People** - aka awareness, training, education - ensure that users are aware of their roles & responsibilities



CNSS Security Model (cont.)

- Each of 27 cells in the cube represents an area that must be addressed to secure an information system
  - e.g., intersection between data integrity, storage and technology implies the need to use technology to protect data integrity of information while in storage
    - solution: new 'file check sum' (cryptographic hash) is calculated every time a critical file is modified …



CNSS Security Model (cont.)

Example: How to protect
- confidentiality of data
- while in transit (e.g., moved to/by USB)
- through education/awareness?

Scenario: An employee stores company information on a personal USB drive, in order to transfer it to another computer (e.g., work from home)

Safeguard: Educate employees about the importance of carefully handling data and encrypting data before transferring it to insecure 'movable' media – *in case that USB is infected or lost, encryption ensures that data cannot be read*

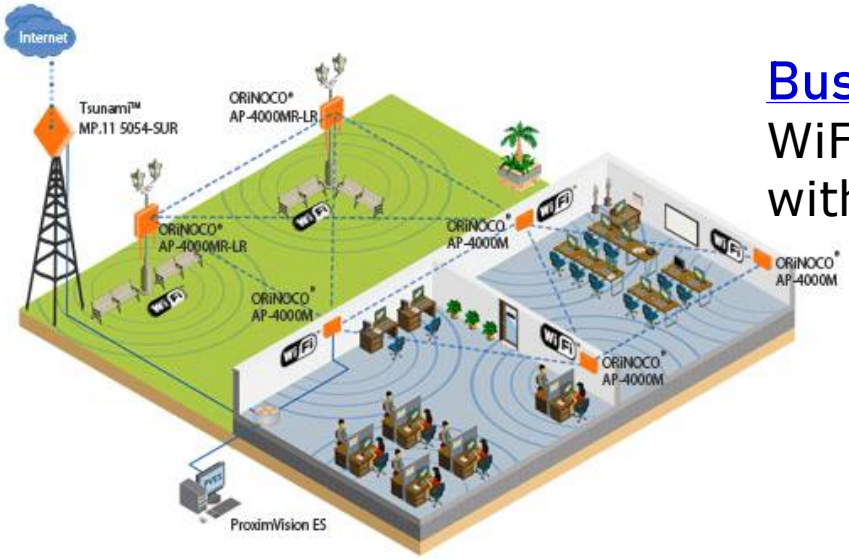
CNSS Security Model (cont.)

Are all 27 aspects of security worth investing into at every company?

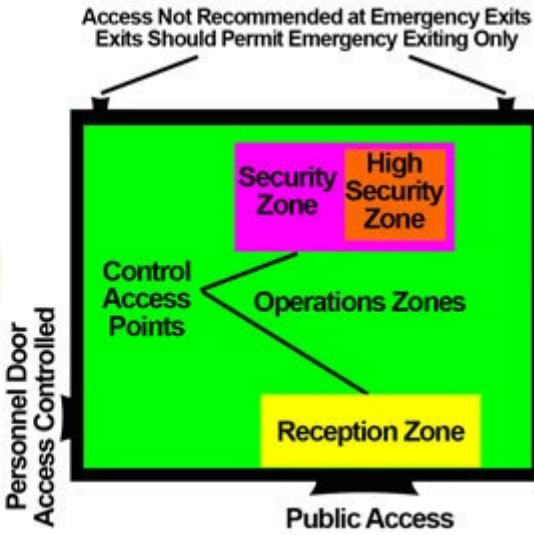
(could be too time consuming and/or too costly)

CNSS Security Model (cont.)

Example: Protecting Confidentiality of Data 'In Transit' Over Wireless Medium …



Busy downtown office:
WiFi used in an area that is within outside reach.

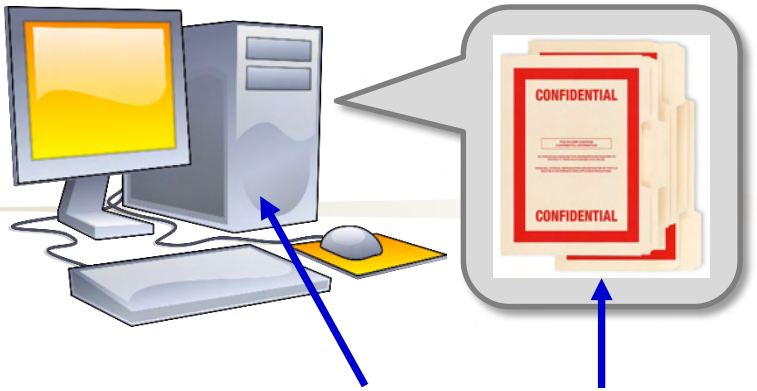


Remote nuclear plant:
WiFi used in an area that is NOT within outside reach.

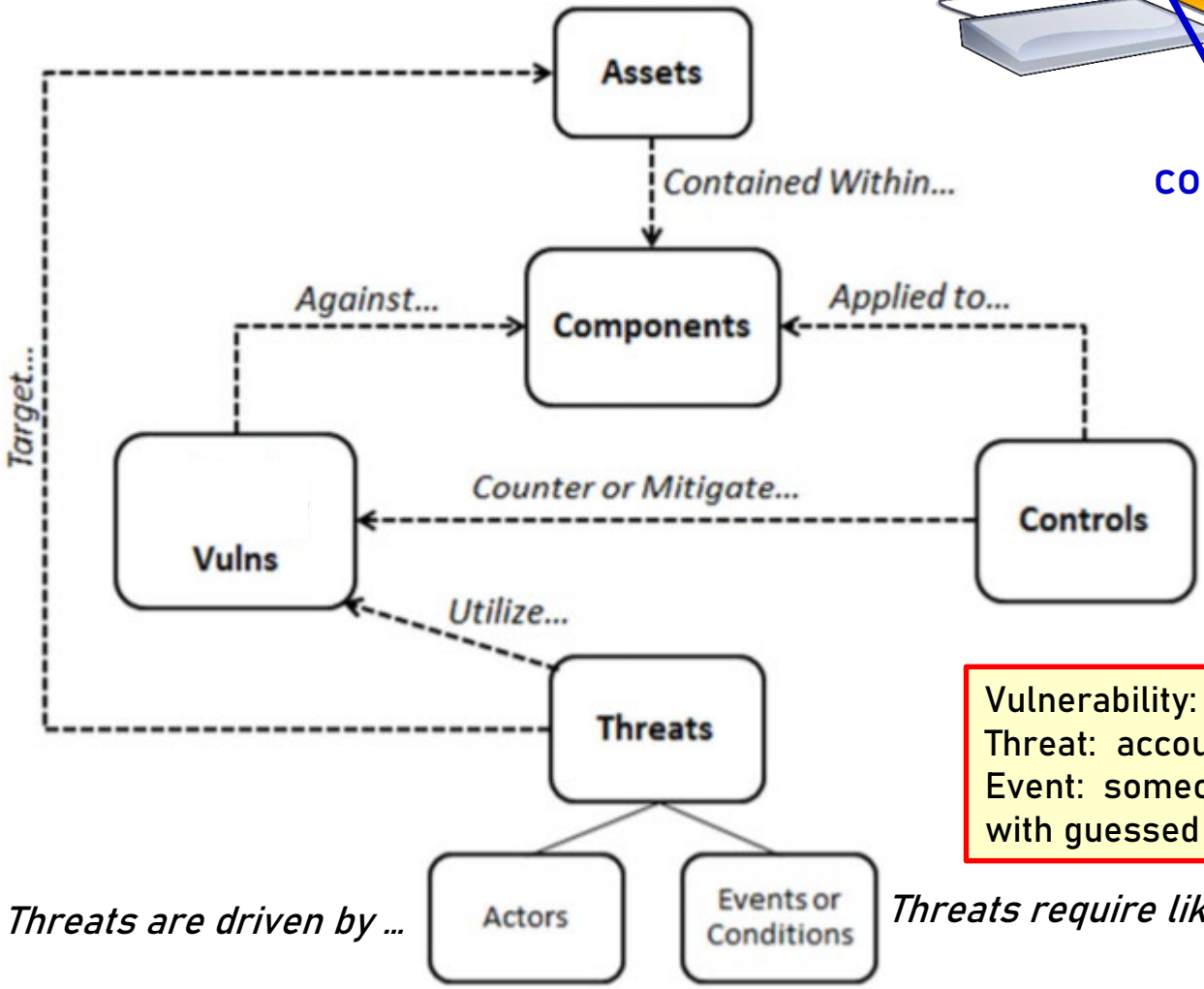
Developing a 100% secure system would be great. But, most companies start developing their 'security systems/defences' by first understanding their most significant threats !!!

McCumber model is appropriate/excellent for evaluation but no so much for the design of a security system.

Threats



component asset



Threats are driven by …

Threats require likely execution of ….

Vulnerability: weak password
Threat: account takeover
Event: someone attempting logins with guessed password

Figure 3 - Threats, Assets and Controls Relationship Model

https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Threat-Driven-Approach.pdf

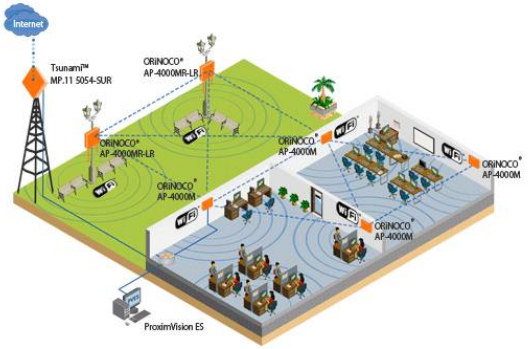
Threats (cont.)

hacker attacks a computer/network

IT administrator did not regulate temperature in server room

- **Security Threat** - any event (action/inaction) that may / may not happen, but has the potential to cause disclosure, alteration, loss, damage or unavailability of a company's (or an individual's) assets
- Three main components of a security threat:
  - **Target** [asset/resource with vulnerability]: organization's system resource that might be attacked
    - information/data (its confidentiality, integrity, availability), software, hardware, communication facilities and networks, etc.
  - **Agent** [may or may not be present]: people/organizations originating the threat – intentional or non-intentional
    - employees, ex-employees, hackers, commercial rivals, terrorists, ...
  - **Event**: possible action that exploits target's vulnerability
    - malicious / accidental destruction or alteration of information, misuse of authorized information, etc.

Threats (cont.)



Example: Threat in WiFi network

Asset with v.
WiFi-signal carrying important data within outsider' reach

Agent
competitor or hacker actually interested in seizing data

Threat

Event
it is possible for someone, by investing time & effort, to capture/sniff wireless data

NO EVENT ⇒ NO THREAT !!!

Threats (cont.)

Example: Threat in WiFi network

Asset with v.
WiFi-signal carrying important data within outside reach

Agent
competitor or hacker interested in seizing data

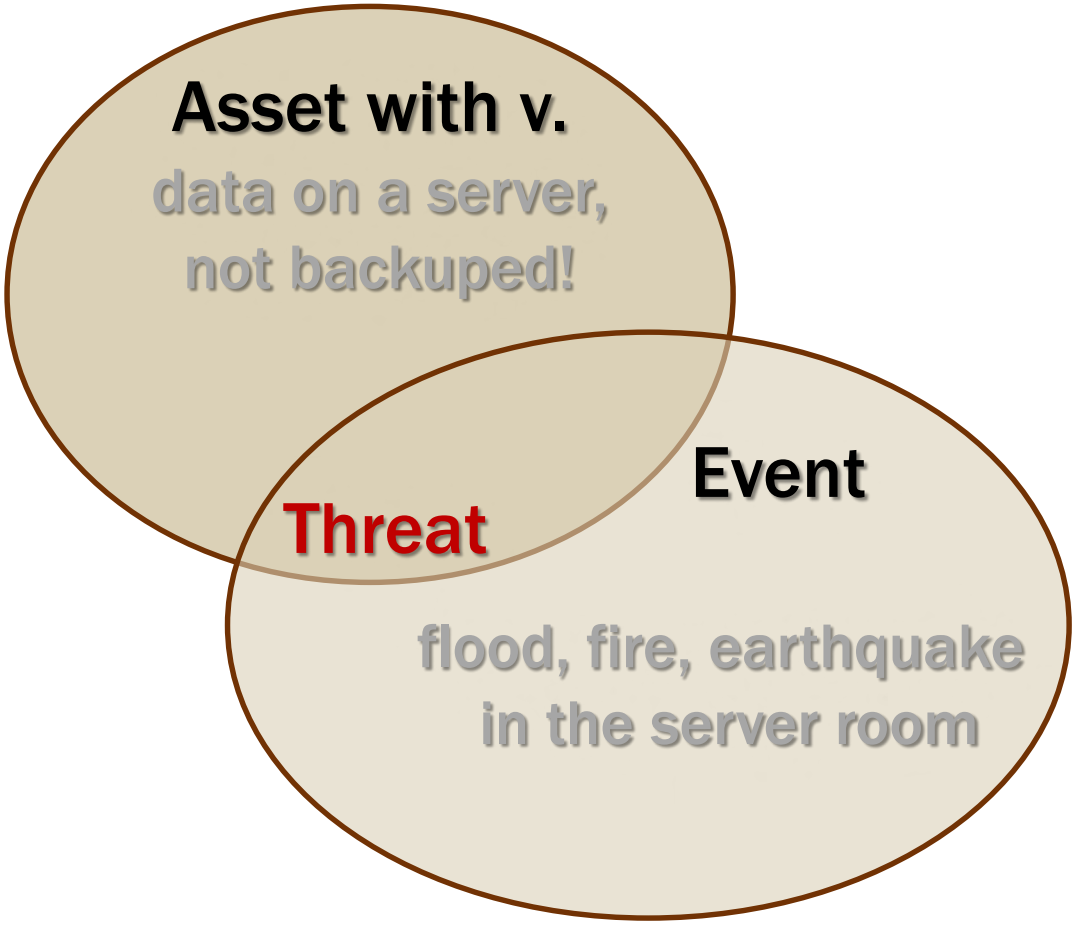
Event
in spite of time & effort competitor/hacker cannot reach wireless signal

Recall, in the case of nuclear facility this was not always possible !!!

NO EVENT ⇒ NO THREAT !!!

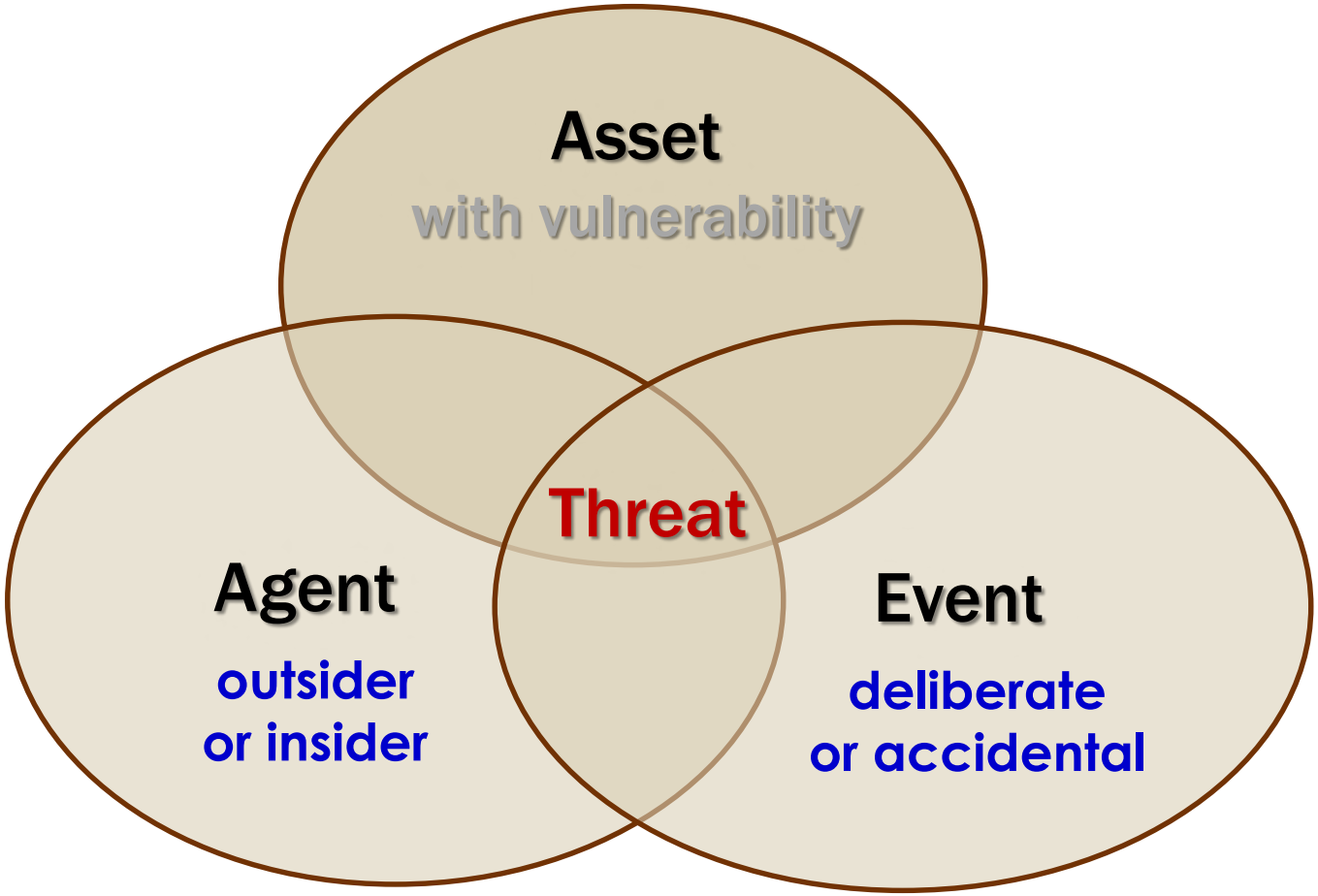
Threats (cont.)

Example: Threat without Agent



Threats (cont.)

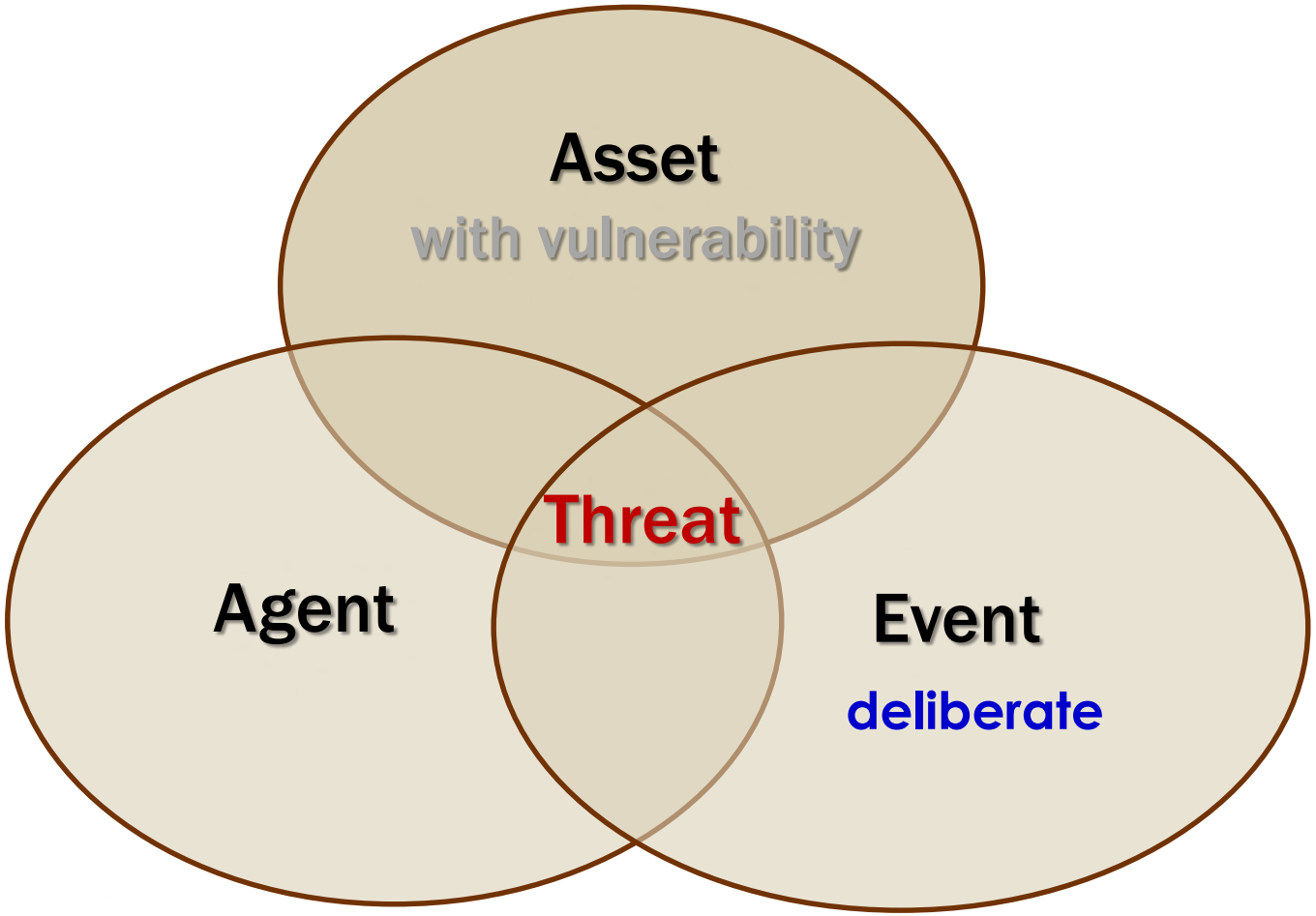
Example: outsider vs. insider, deliberate vs. accidental



Example of insider causing accidental threat: SysAdmin has added a new software to the system and has forgotten to change the password

Threats (cont.)

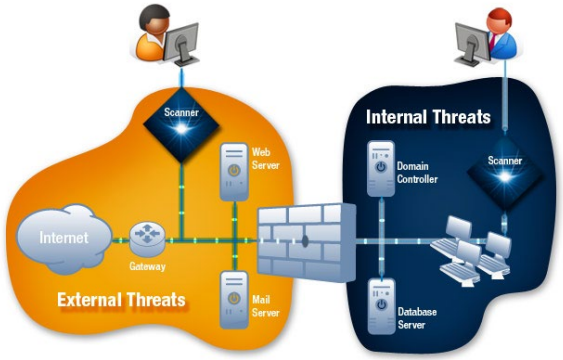
Example: attack definition



THREAT EVENT DELIBERATELY EXECUTED BY AGENT = ATTACK

Threats (cont.)

- Criteria for threat identification/prioritization :
  - asset identification
    - e.g. what are the company's main assets:
      (a) web servers (e-commerce company), or
      (b) workstations (software develop. company)?



  - threat identification [asset-vulnerability, agent, event]
    - some assets have multiple vulnerabilities (e.g., web-server) but they are not all equally likely to be exploited ...
  - organizational strategy regarding risk
    - different threats pose different risks

Threat Agents

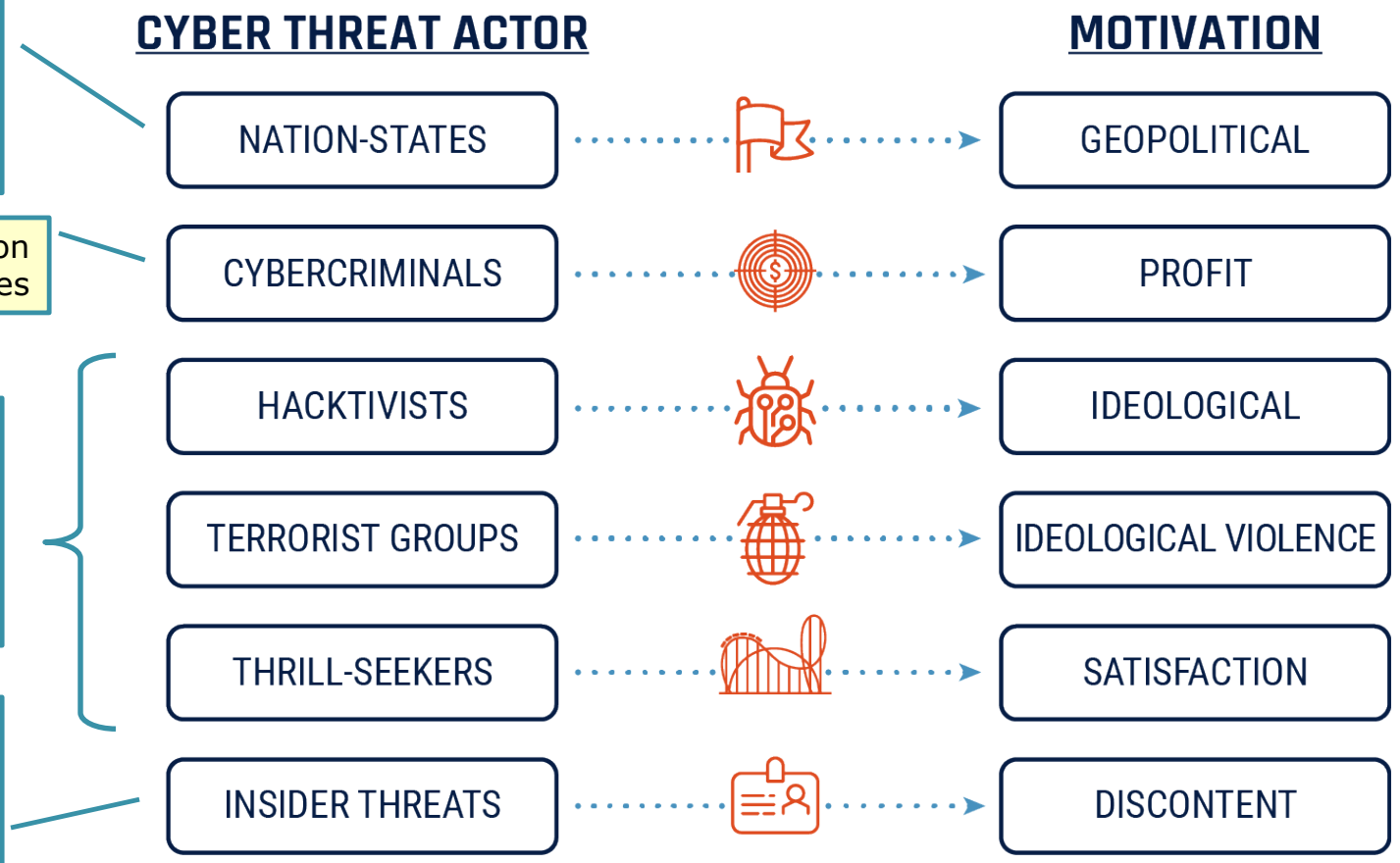
- **Main Categories of Threat Agents :**

most sophisticated threat actors, with dedicated resources and personnel, and extensive planning and coordination

have moderate sophistication compared to nation-states

typically at the lowest level of sophistication as they often rely on widely available tools that require little technical skill to deploy

particularly dangerous because of their access to internal networks that are protected by security perimeters



https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors

Threat Events

- **Main Groups of Threat Actions/Events :**

Threat	Example	
Act of human error or failure	Accidents, employee mistakes	with human agent
Compromises to intellectual property	Piracy, copyright infringement	with human agent, ATTACKS
Deliberate acts of espionage or trespass	Unauthorized access and/or data collection	with human agent, ATTACKS
Deliberate acts of information extortion	Blackmail for information disclosure	with human agent, ATTACKS
Deliberate acts of sabotage or vandalism	Destruction of systems or information	with human agent, ATTACKS
Deliberate acts of theft	Illegal confiscation of equipment or information	with human agent, ATTACKS
Deliberate software attacks	Viruses, worms, macros, denial-of-service	with human agent, ATTACKS
Deviations in quality of service by service provides	Power and WAN quality of service issues from service providers	with human agent
Forces of nature	Fire, flood, earthquake, lightning	no human
Technical hardware failures or errors	Equipment failure	no human
Technical software failures or errors	Bugs, code problems, unknown loopholes	no human
Technological obsolescence	Antiquated or outdated technologies	no human

Threat Events (cont.)

- **Top Threat-Driven Expenses (C-ACM study)**

2012 JISSec Ranking	Categories of Threats	Rate	Rank	Combined	2003 CACM Rank
1	Espionage or trespass	3.54	462	16.35	4
2	Software attacks	4.00	306	12.24	1
3	Human error or failure	4.30	222	9.55	3
4	Theft	3.61	162	5.85	7
5	Compromises to intellectual property	3.59	162	5.82	9
6	Sabotage or vandalism	3.11	111	3.45	5
7	Technical software failures or errors	3.17	105	3.33	2
8	Technical hardware failures or errors	2.88	87	2.51	6
9	Forces of nature	2.76	81	2.24	8
10	Deviations in quality of service from service providers	2.88	72	2.07	10
11	Technological obsolescence	2.66	57	1.52	11
12	Information extortion	2.68	18	0.48	12

Rating of different threat events based on their frequency and significance – things changeover time …

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

Lab 1

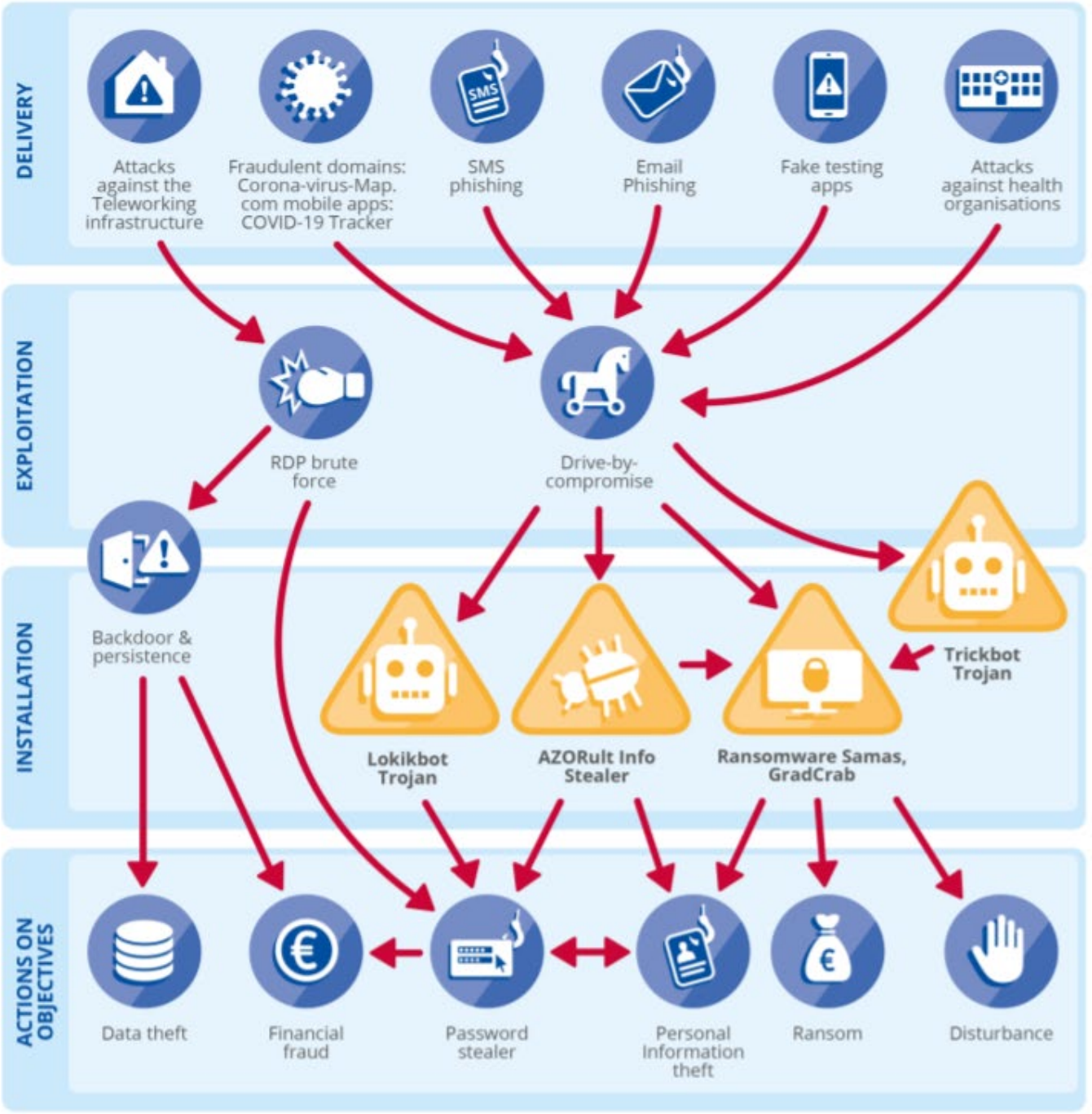
Top Threats 2019-2020		Assessed Trends	Change in Ranking
1	Malware ↗ (software attack)	—	—
2	Web-based Attacks ↗ (human error or failure)	—	↗
3	Phishing ↗	↗	↗
4	Web application attacks ↗	—	↙
5	Spam ↗	↙	↗
6	Denial of service ↗	↙	↙
7	Identity theft ↗	↗	↗
8	Data breaches ↗	—	—
		↗	—
		↙	↙

https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

THREAT LANDSCAPE MAPPING

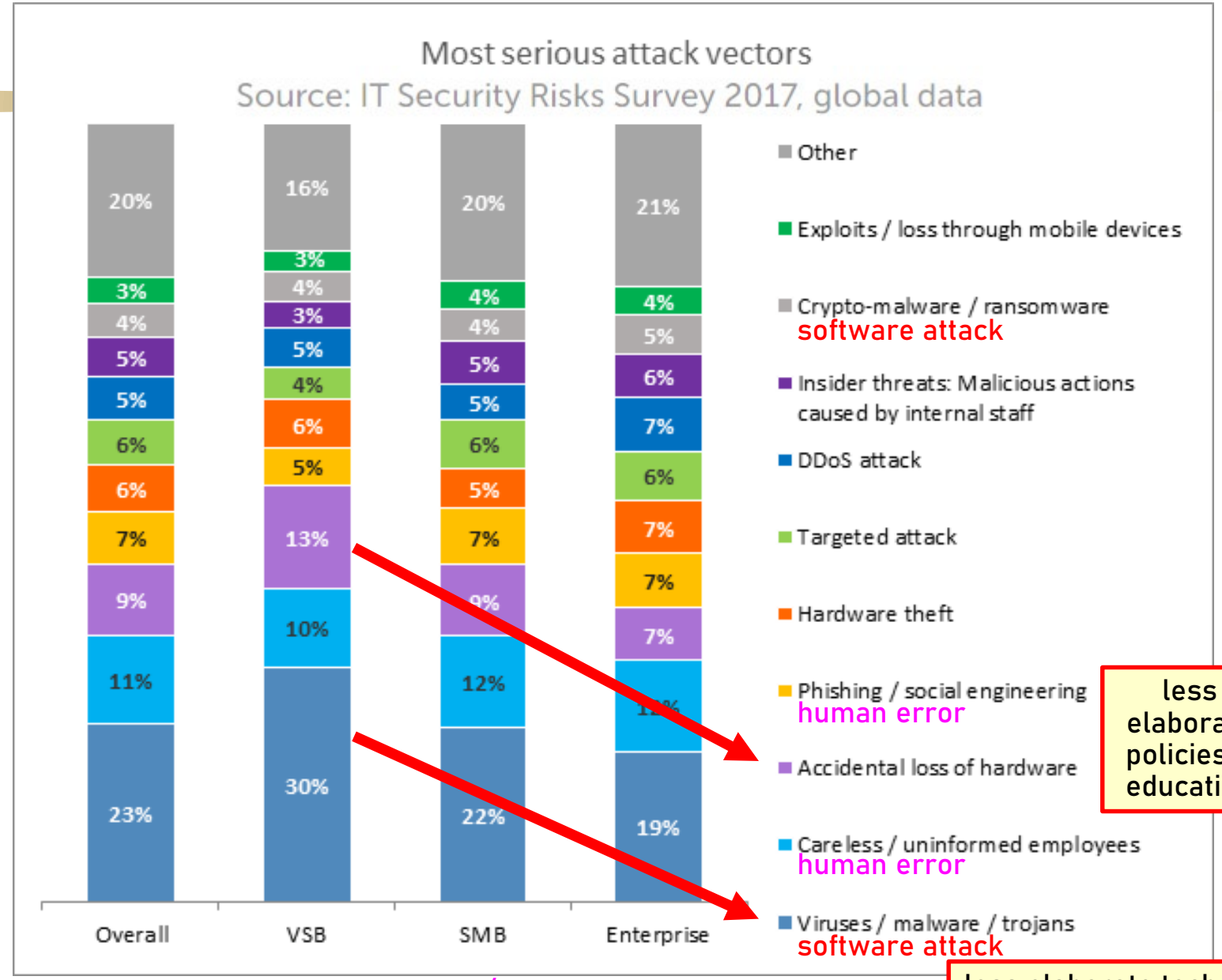
Exploitation by cybercriminals and advanced persistent threat (APT) groups of the current coronavirus (COVID-19) global pandemic.



https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/threat-landscape-mapping-infographic-2020

kaspersky daily

https://www.kaspersky.com/blog/the-human-factor-in-it-security/



less elaborate policies & education

very small business

small/medium business

less elaborate technical defences in VSB

Threat Events (cont.)

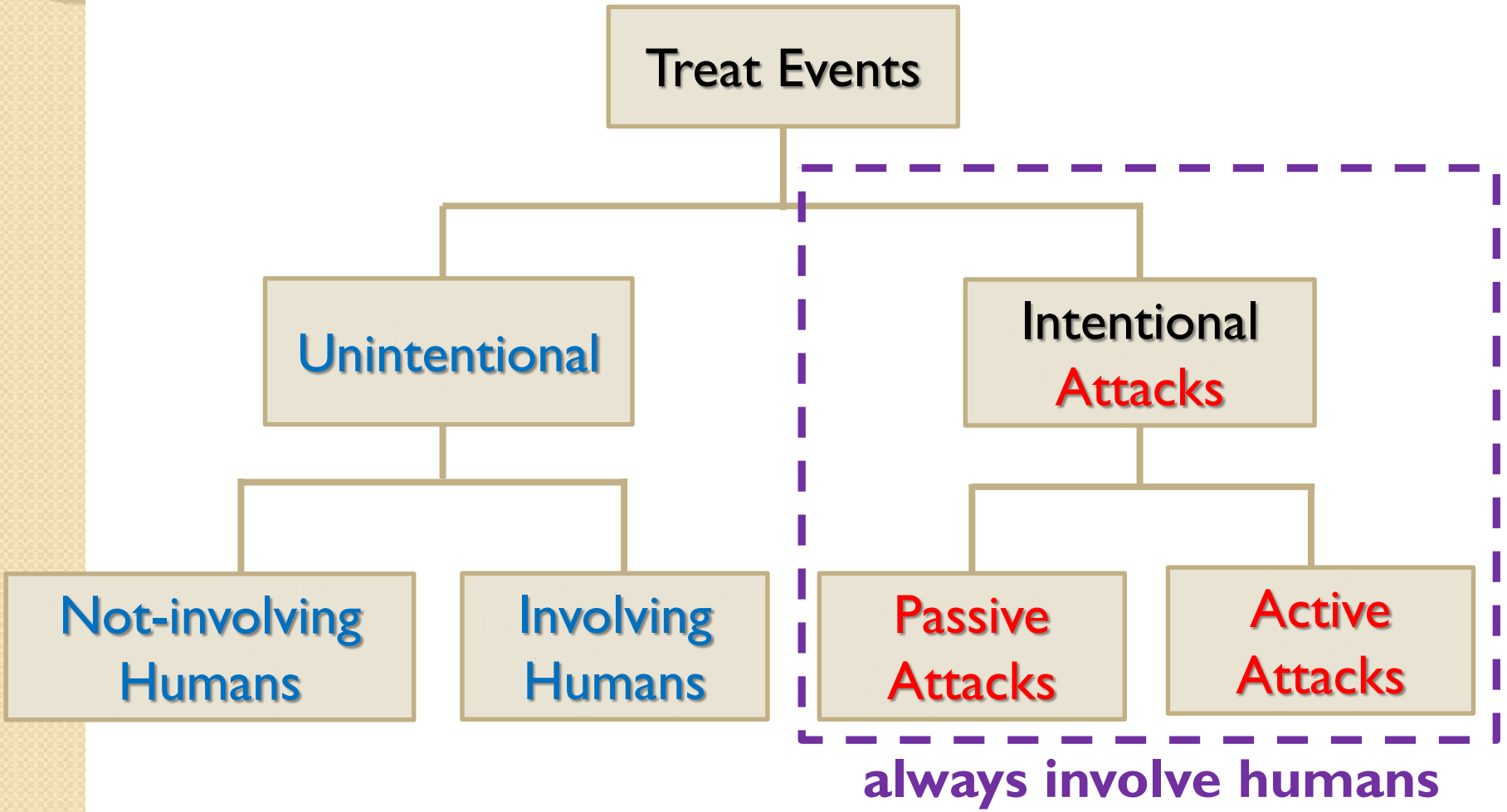
Top 10 biggest cyber threats to organizations

1. Phishing (22%)
2. Malware (20%)
3. Cyberattacks (to disrupt) (13%)
4. Cyberattacks (to steal money) (12%)
5. Fraud (10%)
6. Cyberattacks (to steal IP) (8%)
7. Spam (6%)
8. Internal attacks (5%)
9. Natural disasters (2%)
10. Espionage (2%)

https://assets.ey.com/content/dam/ey-sites/ey-com/en_ca/topics/advisory/ey-global-information-security-survey-2018-19.pdf

Threat Events (cont.)

- **Categories of Threat Events** :



Threat Events: Unintentional & No Human

- **Forces of Nature**
  - fire, flood, earthquake, hurricane, tsunami, dust contamination, …
  - cannot be fully predicted/prevented
  - organization must implement controls to limit damage as well as develop incident response plans and business continuity plans

Hurricane Harvey, for instance, put Houston data centers to the test. Edward Henigin, CTO of Data Foundry Inc. in Austin, said their North Houston data center is a "purpose-built facility designed to withstand Category 5 hurricane wind speeds." Just before Hurricane Harvey last year, the company brought on additional staff to maintain the data center throughout the emergency and provided food, showers, cots, books and video games for employees who remained at work five straight days. The major data center providers in Houston reported that there was no interruption of service during the emergency. This is impressive, as Hurricane Harvey damaged 203,000 homes and cost at least $125 billion in reparations.

https://www.idexpertscorp.com/articles/data-security-and-natural-disasters/

Threat Events: Unintentional & No Human

- **Hardware and Software Failures and Errors**
  - cannot be fully predicted/prevented by the organization
  - causes of **hardware** failures: wear, tear, age, operating environment (e.g., high temperature, moisture, dust), …
  - best defences against hardware failures:
    - redundancy (e.g., backup servers)
    - continuous monitor hardware devices (where & how deployed)
  - causes of **software** failures: difficulty of testing software for all possible inputs & all possible operating conditions; OS evolutions and software incompatibilities …
  - best defences against software failures:
    - keep up-to-date with software updates and vulnerabilities
    - continuously monitor and maintain software system

hardware breaks, software crashes

Threat Events: Unintentional & No Human

Hitachi

Backblaze Hard Drives Quarterly Failure Rates for Q2 2021

Reporting period: 4/1/2021 through 6/30/2021 inclusive

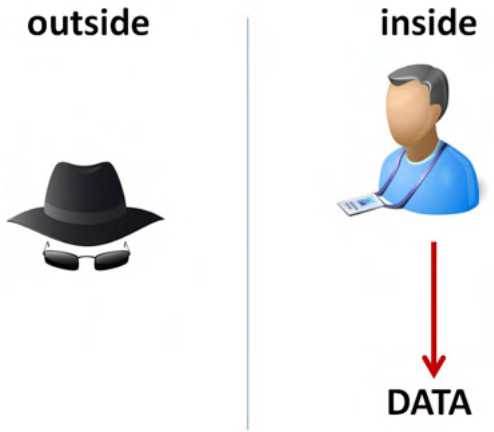
MFG	Model	Drive Size	Drive Count	Avg. Age (months	Drive Days	Drive Failures	AFR
HGST	HMS5C4040ALE640	4TB	3,209	62.1	291,656	5	0.63%
HGST	HMS5C4040BLE640	4TB	12,610	56.4	1,158,839	14	0.44%
Seagate	ST4000DM000	4TB	18,795	68.3	1,714,240	91	1.94%
Toshiba	MD04ABA400V	4TB	98	73.3	8,974	1	4.07%
Seagate	ST6000DX000	6TB	886	74.8	80,626	-	0.00%
HGST	HUH728080ALE600	8TB	1,077	40.7	98,004	1	0.37%
Seagate	ST8000DM002	8TB	9,733	56.9	885,873	33	1.36%
Seagate	ST8000NM0055	8TB	14,404	47.1	1,310,887	45	1.25%
Seagate	ST10000NM0086	10TB	1,199	44.5	109,134	3	1.00%
HGST	HUH721212ALE600	12TB	2,600	21.0	234,416	-	0.00%
HGST	HUH721212ALE604	12TB	10,754	4.5	789,373	3	0.14%
HGST	HUH721212ALN604	12TB	10,831	26.9	985,447	14	0.52%
Seagate	ST12000NM0007	12TB	3,552	31.7	726,571	41	2.06%
Seagate	ST12000NM0008	12TB	19,970	15.1	1,847,092	46	0.91%
Seagate	ST12000NM001G	12TB	10,557	9.2	894,875	10	0.41%
Seagate	ST14000NM001G	14TB	8,359	6.6	601,727	26	1.58%
Seagate	ST14000NM0138	14TB	1,653	6.8	151,236	23	5.55%
Toshiba	MG07ACA14TA	14TB	31,913	10.2	2,740,341	55	0.73%
Toshiba	MG07ACA14TEY	14TB	424	6.5	37,856	2	1.93%
WDC	WUH721414ALE6L4	14TB	8,400	6.8	751,725	10	0.49%
Seagate	ST16000NM001G	16TB	4,857	3.1	314,266	15	1.74%
Toshiba	MG08ACA16TEY	16TB	1,430	5.4	103,324	1	0.35%
WDC	WUH721816ALE6L0	16TB	624	3.0	47,963	-	0.00%
		Totals	**177,935**		**15,884,445**	**439**	**1.01%**

https://www.backblaze.com/blog/backblaze-drive-stats-for-q2-2021/

Backblaze

Threat Events: Unintentional With Human

- **Act of Human Error or Failure**
  - organization's own employee's are one of its greatest threats
  - examples:
    - revelation of classified data (e.g., phishing)
    - accidental deletion or modification of data
    - failure to protect data
    - storing data in unprotected areas
    - entry of erroneous data



Much of human error or failure can be prevented!

  - preventative measures:
    - training and ongoing awareness activities
    - enhanced control techniques:
      - require users to type a critical command twice
      - ask for verification of commands by a second party

Threat Events: Unintentional With Human

Example: Is this a cyber-security threat event?

Justify your answer!

You are depositing $500 cash at your bank.
The bank clerk types/enters into the system $5,000 as the deposit amount. The balance increases by $5,000.

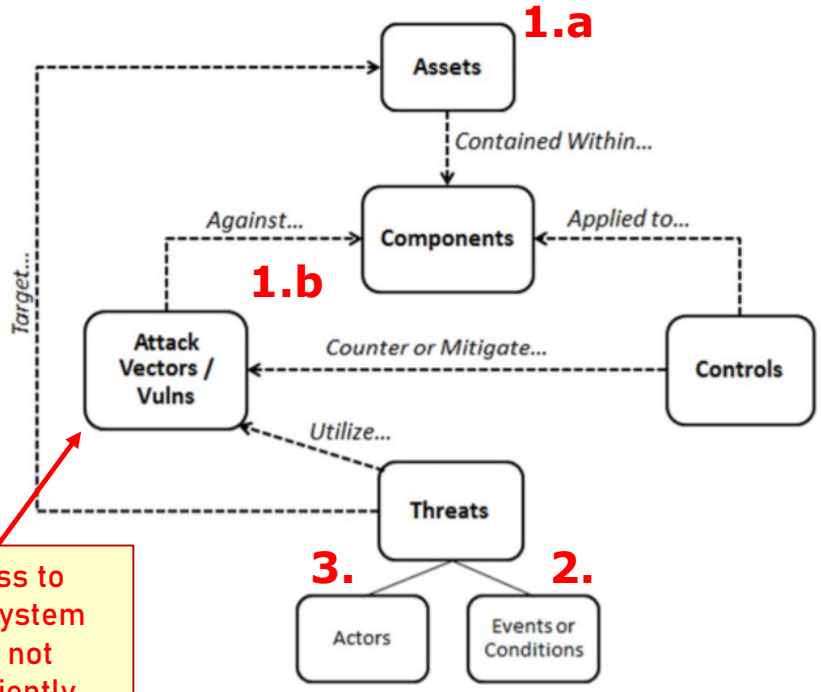
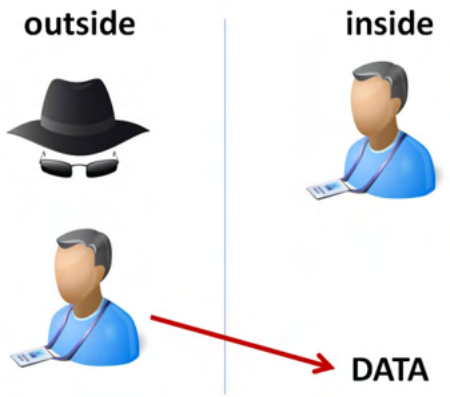


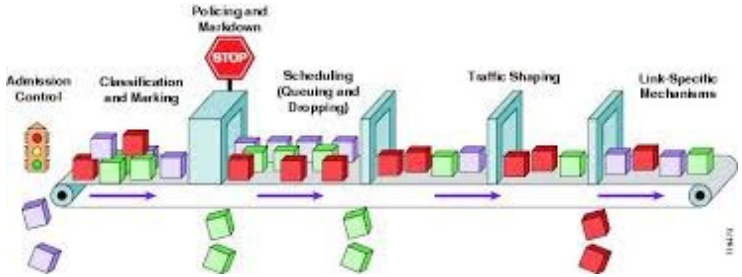
Figure 3 - Threats, Assets and Controls Relationship Model

access to data/system was not sufficiently controlled

Threat Events: Unintentional With Human

- **Deviations in Quality of Service**
  - in organizations that relies on the Internet and Web, irregularities in available bandwidth can dramatically affect their operation
    - e.g., employees or customers cannot contact the system

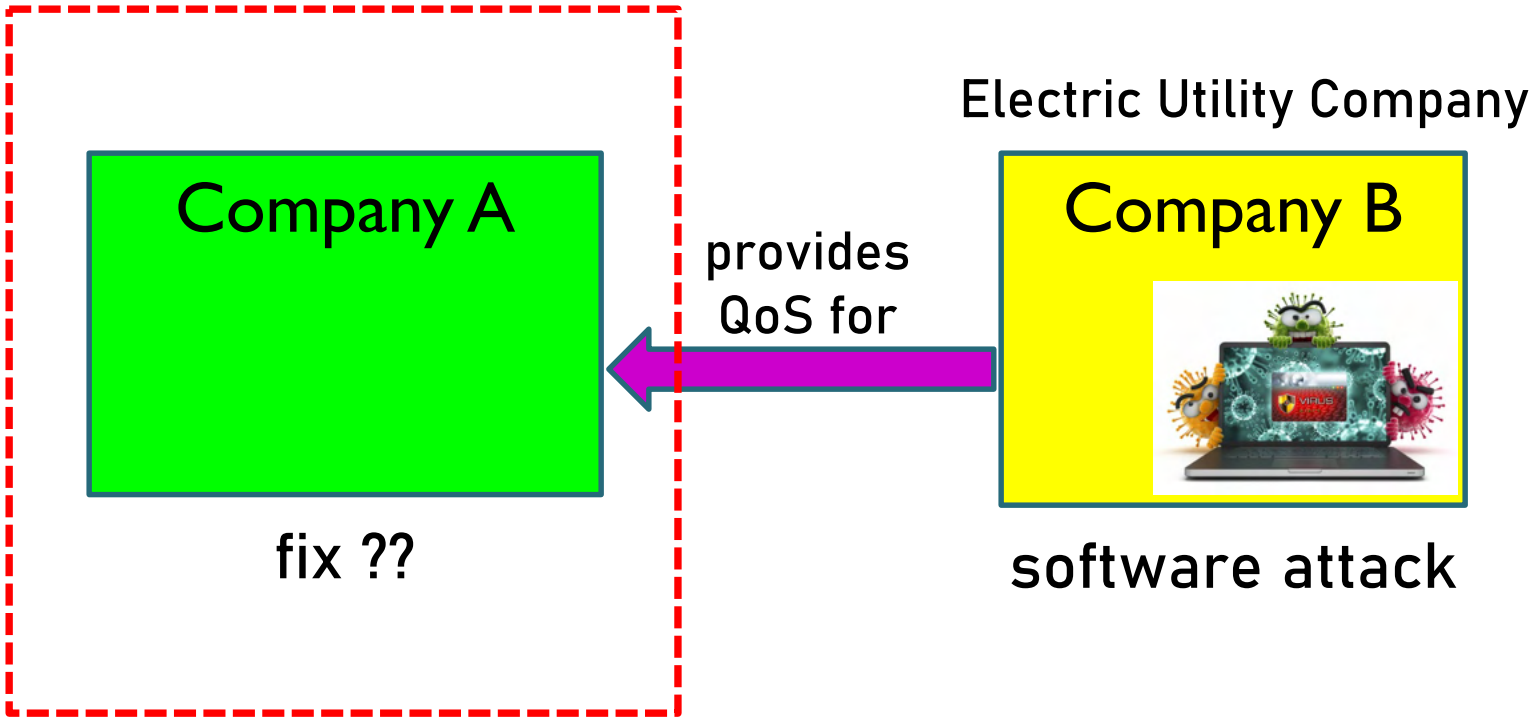




  - possible 'defence': backup ISP or backup power generator

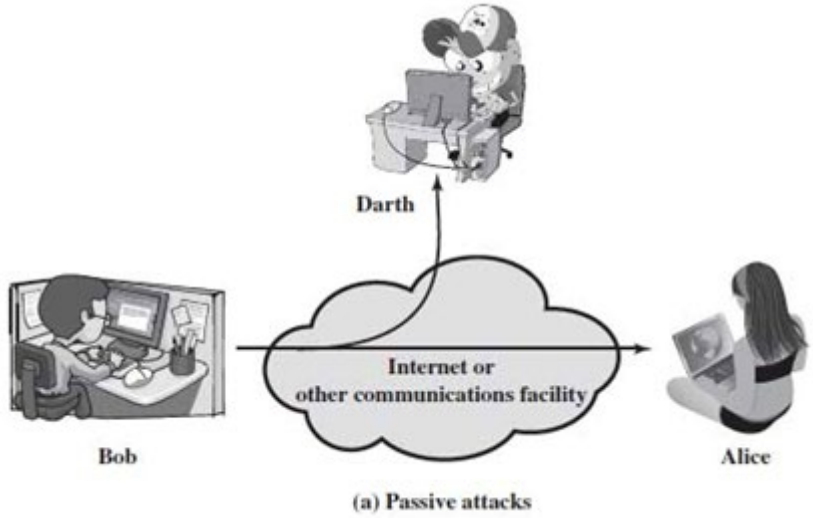
Threat Events: Unintentional With Human

- Deviations in Quality of Service (cont.)



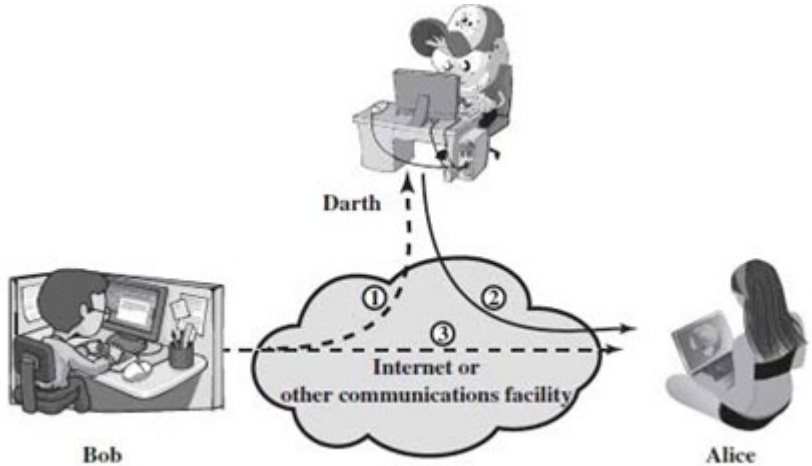
Threat Events: Intentional Attacks

- **Passive Attack** - attempts to learn or make use of info. from the system but does not affect system resources
  - compromises **Confidentiality**
  - **generally hard to detect !!!**
  - examples: traffic sniffing



(a) Passive attacks

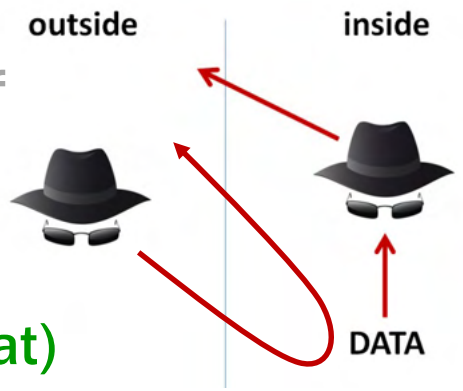
- **Active Attack** - attempts to alter system resources or affect their operation
  - compromises **Integrity** or **Availability**
  - examples: man-in-the-middle, data/packet injection and DoS



(b) Active attacks

Threat Events: Intentional Attacks (cont.)

- **Compromise to Intellectual Property (IP)**
  - IP = any intangible asset that consist of human knowledge & ideas – creations of the mind (copyright, patent, trade secret)
  - any unauthorized use of IP constitutes a security threat (MS Office, Adobe Acrobat)
  - defense measures:
    - use of digital watermarks and embedded code



Example: Peter Morch story – compromise to IP by insider

In 2000, while still employed at Cisco Systems, Morch logged into a computer belonging to another Cisco software engineer, and obtained (burned onto a CD) proprietary information about an ongoing project.

Shortly after, Morch started working for Calix Networks – a potential competitor with Cisco. He offered them Cisco's information.

Morch was sentenced to 3 years' probation.

APPLE \ TECH \ TRANSPORTATION

FBI charges former Apple employee with stealing trade secrets from self-driving car project

The employee was allegedly trying to get a job at Alibaba-backed Xiaopeng Motors

By Sean O'Kane | @sokane1 | Jul 10, 2018, 5:19pm EDT

Xiaolang Zhang, who worked for Apple from December 2015 until May 2018, has been charged in federal court with stealing trade secrets, and faces 10 years imprisonment and a $250,000 fine. Zhang was arrested trying to leave the country this past weekend. The news was first reported by *The Mercury News*.

Once Zhang told his Apple supervisor about his intentions, and after "feeling that he had been evasive," according to the filing, a member of Apple's New Product Security Division joined the meeting and had Zhang turn in his two work phones and his laptop. After the meeting, Apple reviewed Zhang's past network activity, performed a forensic analysis on his work devices, as well as his "activities on the Apple campus," including swipe badge access and closed circuit TV footage.

The company's security team discovered that Zhang's network activity "increased exponentially compared to the prior two years of his employment" in the days before his attempted resignation, and that the majority of that activity was "bulk searches and targeted downloading copious pages of information" from confidential databases that he had access to. The CCTV footage that Apple reviewed showed, according to the complaint, Zhang leaving the company's autonomous vehicle lab on April 28th (during time when he was supposed to be on leave) carrying a "computer keyboard, some cables, and a large box."

https://www.theverge.com/2018/7/10/17556034/fbi-apple-trade-secrets-xpeng-self-driving

Protecting intellectual property from insider threat

How IP gets leaked??

By Josh Lefkowitz June 12, 2019

A company's IP is estimated to represent as much as 70% of its market value.

Unfortunately, the value of IP is often only understood once it has been stolen and commercialised. When copycat products start appearing, or unique features pop up in competitor designs, the loss becomes apparent. By that point, the damage has been done, and recourse is limited to patent infringement courts.

Employees with a grievance against their employer bid to punish them by sharing sensitive information for personal profit. Another scenario might see an employee tempted by a high salary position with a competitor in return for stealing corporate secrets prior to leaving their current role.

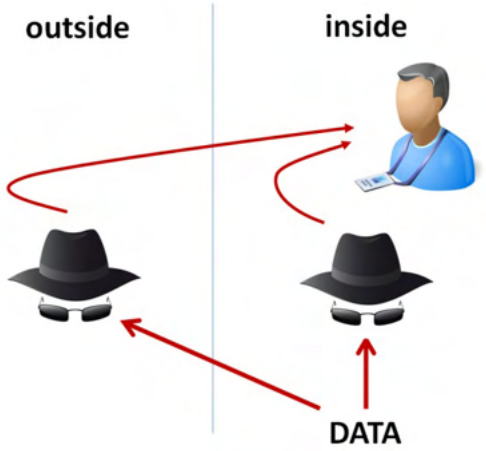
Employees don't always deliberately reveal secrets; they can simply be targets of malicious activity themselves. They may be recruited by bad actors using an apparently legitimate front, such an invitation to an overseas academic conference, and manipulated into divulging trade secrets.

Finally, we see bad actors take roles within target organisations with the sole aim of accessing and exfiltrating trade secrets.

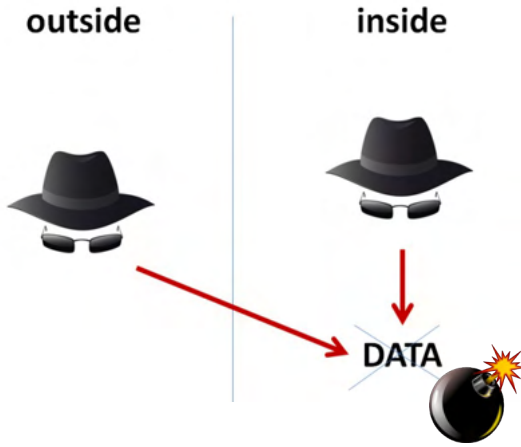
https://www.techradar.com/news/protecting-intellectual-property-from-insider-threat

Threat Events: Intentional Attacks (cont.)

- **Deliberate Act of Info. Extortion / Blackmail**
  - hacker or malicious insider steals information & demands compensation for its return or non-disclosure
  - example:
    - theft of data files containing customer credit card information



- **Deliberate Act of Sabotage or Vandalism**
  - hacker or malicious insider destroys an asset in order to cause financial loss or damage the organization's reputation
  - example:
    - hackers accessing a system and damaging or destroying critical data



Threat Events: Intentional Attacks (cont.)

Example: Two Kazakhstan employees story – info. extortion by insider

In 2002, two employees in a company in Kazakhstan allegedly got access to Bloomberg L.P. financial information database because their company was an affiliate of Bloomberg.

They allegedly demanded $200,000 from Bloomberg to reveal how they got access to the database.

Bloomberg opened an offshore account with $200,000 balance, and invited the pair to London to personally meet with Michael Bloomberg. The meeting was recorded. Soon after the two were arrested ....

In the end, there were sentences to 51 months in prison.

NOTE: finding a vulnerability and requiring payment to learn about it may be considered extortion.

http://www.cybercrime.gov/zezevIndict.htm

Threat Events: Intentional Attacks (cont.)

Example: Domino in France & Belgum – info. extortion by outsider

In 2014, the hacktivist group Rex Mundi is claiming it breached the servers of Domino's Pizza in France and Belgium, downloading approximately 600,000 customer records. In a statement posted on Twitter, Rex Mundi said it was able to download customers' full names, addresses, phone numbers, e-mail addresses and passwords.

"We immediately sent various e-mails to both Domino's Pizza France and Belgium. … We also used the contact forms on their websites to let them know of this vulnerability and to offer them not to release this data in exchange for 30,000 euros." The hackers also said Domino's Pizza has until Monday, June 16, at 8 p.m. CET to pay the ransom. "If they do not do so, we will post the entirety of the data in our possession on the Internet."

In June 2017, five French nationals were arrested by French authorities. The main suspect admitted his role in the extortion scheme but claimed they did not do any of the hacking. Instead, they hired hackers on the Dark Web to carry out the cyberattacks. In October 2017, two other hackers were arrested by French police in France while the final eighth accomplice - also a French national - was arrested in Thailand last month.

https://www.securityweek.com/dominos-pizza-refuses-extortion-demand-after-customer-data-stolen
https://www.databreachtoday.com/ransom-sought-in-dominos-pizza-breach-a-6957
https://cyware.com/news/europol-arrests-eight-alleged-members-of-the-notorious-rex-mundi-hacker-group-1ead3821

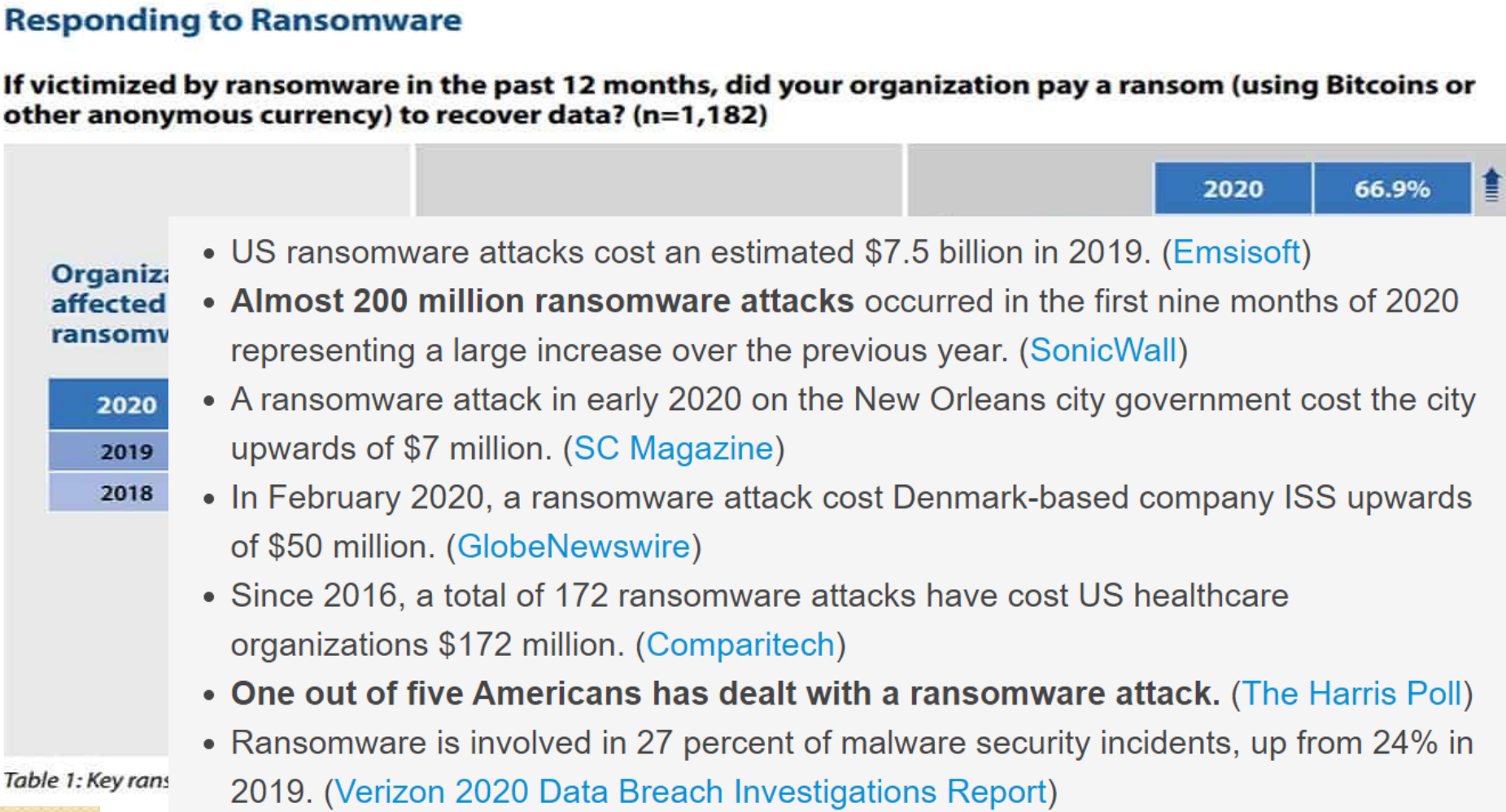
Threat Events: Intentional Attacks (cont.)

Extortion by outsiders are now very common!

Which type of attack is 'ransomware' ???

- ransomware, most commonly, is 'extortion by an outsider'
- though, in some cases it is also a simple act of 'vandalism' or 'sabotage'

Threat Events: Intentional Attacks (cont.)



- US ransomware attacks cost an estimated $7.5 billion in 2019. (Emsisoft)
- **Almost 200 million ransomware attacks** occurred in the first nine months of 2020 representing a large increase over the previous year. (SonicWall)
- A ransomware attack in early 2020 on the New Orleans city government cost the city upwards of $7 million. (SC Magazine)
- In February 2020, a ransomware attack cost Denmark-based company ISS upwards of $50 million. (GlobeNewswire)
- Since 2016, a total of 172 ransomware attacks have cost US healthcare organizations $172 million. (Comparitech)
- **One out of five Americans has dealt with a ransomware attack.** (The Harris Poll)
- Ransomware is involved in 27 percent of malware security incidents, up from 24% in 2019. (Verizon 2020 Data Breach Investigations Report)
- Ransomware payments continued their steep incline in Q3 2020. The average sits at $233,817 which is up 31% over the previous quarter and a whopping 468% over Q3 2019. (Coveware's Q3 2020 Ransomware Marketplace report)

https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/

Threat Events: Intentional Attacks (cont.)

Example: Michael Thomas story – information vandalism by insider

In 2011, Michael Thomas, was an IT operations manager for web hosting company ClickMotive. Upset that a friend had been fired from the IT department, and, as court documents tell it, annoyed that fewer staff would mean more work, Thomas embarked on a weekend campaign of electronic sabotage.

He deleted over 600 files, disabled backup operations, eliminated employees from a group email a client used to contact the company, diverted executives' emails to his personal account, and set a "time bomb" that would result in employees being unable to remotely access the company's network after Thomas submitted his resignation. Once ClickMotive discovered what Thomas did, it incurred over $130,000 in costs to fix these problems.

Thomas was convicted (**under Computer Fraud and Abuse Act**) and sentenced to time served plus three years of supervised release and fined roughly $130,000, the cost of fixing the damage.

https://caselaw.findlaw.com/us-5th-circuit/1882400.html
https://www.theregister.com/2017/12/14/it_admin_cant_claim_authorization_for_vengeful_data_destruction/

Threat Events: Intentional Attacks (cont.)

Example: Michael Thomas story – information vandalism by insider (cont.)

Thomas challenged the application of the law. The CFAA criminalizes anyone who "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage **without authorization**, to a protected computer."

However, the court's ruling stated: "No reasonable employee could think he had permission to stop the system from providing backups, or to delete files outside the normal protocols, or to falsify contact information in a notification system, or to set a process in motion that would prevent users from remotely accessing the network."

https://cybercrimeincidenttracker.com/pages

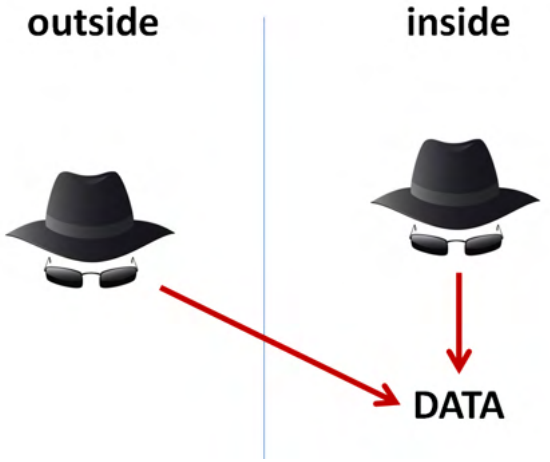
C.C.I.T Home Incidents Relations Login Register Search Search

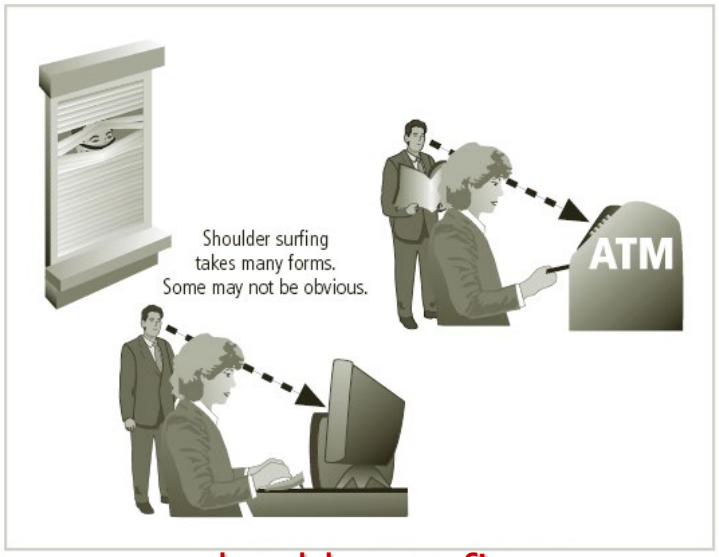
Motovations

Name	Persons
threat	1
fraud	1
threats	1
death threats	1
cyberstalking	1
revebge	0
activisim	9
profit	265
extortion	1
fanatical hobbyism	4
hoarding	1
revenge	31
fun	3
bored	2

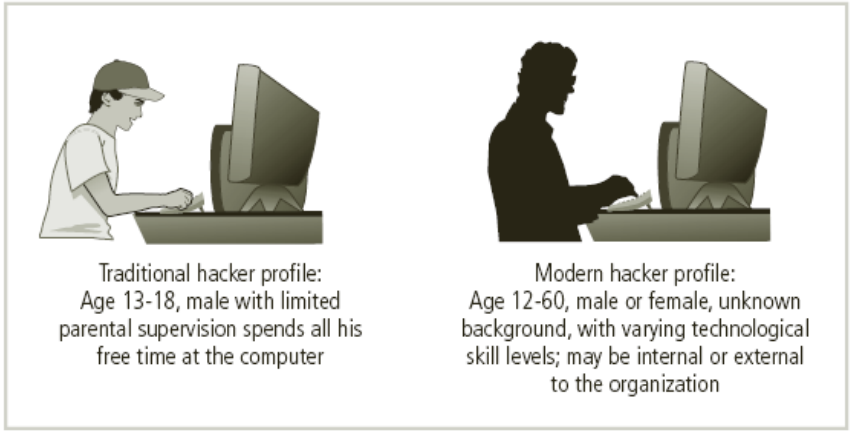
Threat Events: Intentional Attacks (cont.)

- **Deliberate Act of Trespass**
  - unauthorized access to info. that an organization is trying to protect (e.g., through stolen passwords)
  - low-tech e.g.: shoulder surfing
  - high-tech e.g.: hacking



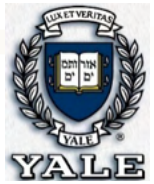


shoulder surfing



hacker profiles

Threat Events: Intentional Attacks (cont.)



Example: Yale vs. Princeton – trespass by outsider

Yale University's admission created a web-based system to enable applicants to check the status of their application on-line. To access the system, the applicants had to prove their identity by answering questions regarding their name, birth date, SIN.

Many of these students also applied to other top universities.

At Princeton, Associate Dean and Director of Admissions - Stephen LeMenager - knew that the private information that Yale used to control access was also in the applications that candidates submitted to Princeton. He used this information to log into the Yale system several times as applicants.

When the word got out, he admitted doing the break-ins but said that he was merely testing the security of the Yale system. Princeton put him on administrative leave.

NOTE: The case emphasizes that information used to control access must not be generally available ...

not-involving specialized software: disgruntled employee uses his system privileges to manually destroy files

involving specialized software: disgruntled employee installs a 'logic-bomb' malware on the system which ends up destroying files on a particular date/event

- **Main Groups of Threat Actions/Events :**

Threat	Example
Act of human error or failure	Accidents, employee mistakes
Compromises to intellectual property	Piracy, copyright infringement
Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
Deliberate acts of information extortion	Blackmail for information disclosure
Deliberate acts of sabotage or vandalism	Destruction of systems or information
Deliberate acts of theft	Illegal confiscation of equipment or information
Deliberate software attacks	Viruses, worms, macros, denial-of-service
Deviations in quality of service by service provides	Power and WAN quality of service issues from service providers
Forces of nature	Fire, flood, earthquake, lightning
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies

Threat Events: Software Attacks

- **Deliberate Software Attacks**
  - a deliberate action aimed to violate / compromise a system's security through the use of specialized software
  - types of attacks base on the type of malicious software:

a) Use of Malware

b) Password Cracking

c) DoS and DDoS

d) Spoofing

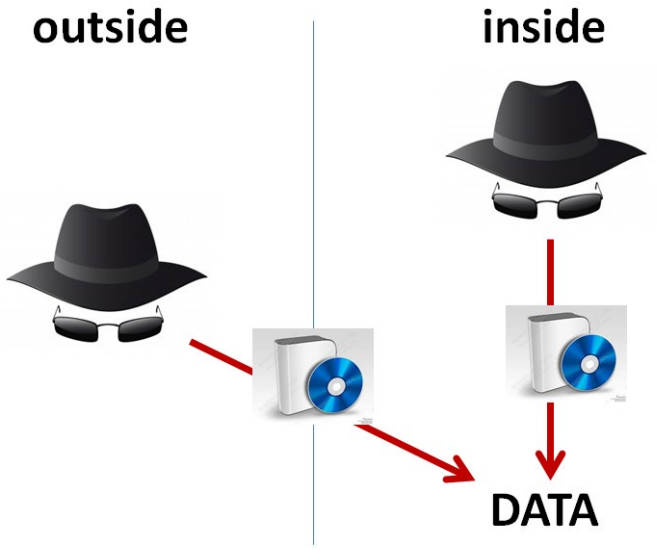
e) Sniffing

f) Man-in-the-Middle

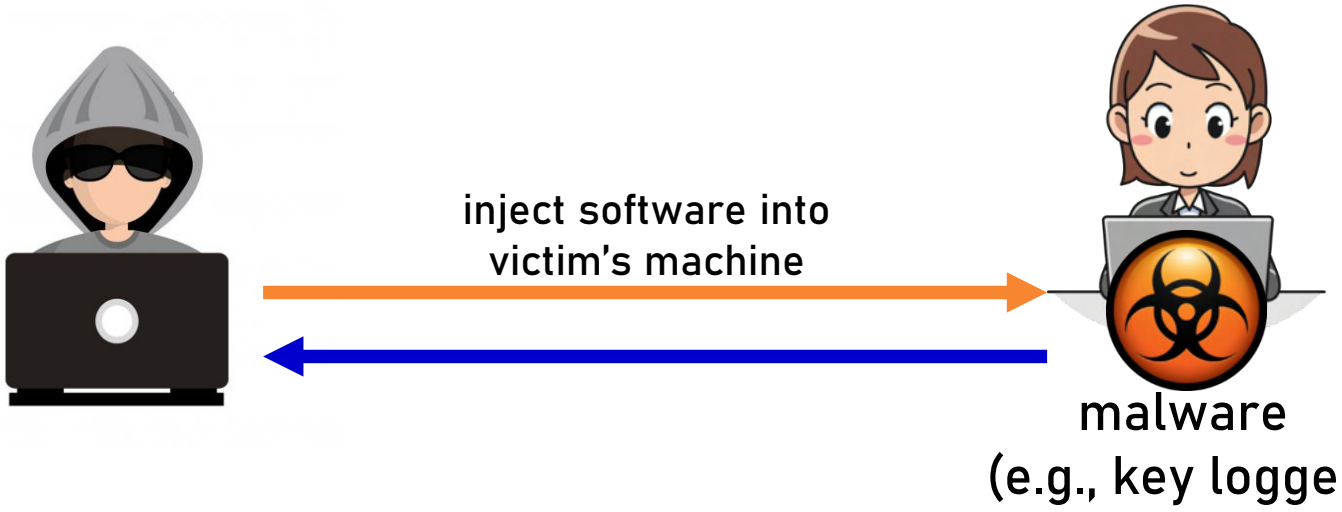
g) Phishing

h) Pharming

Lab 1



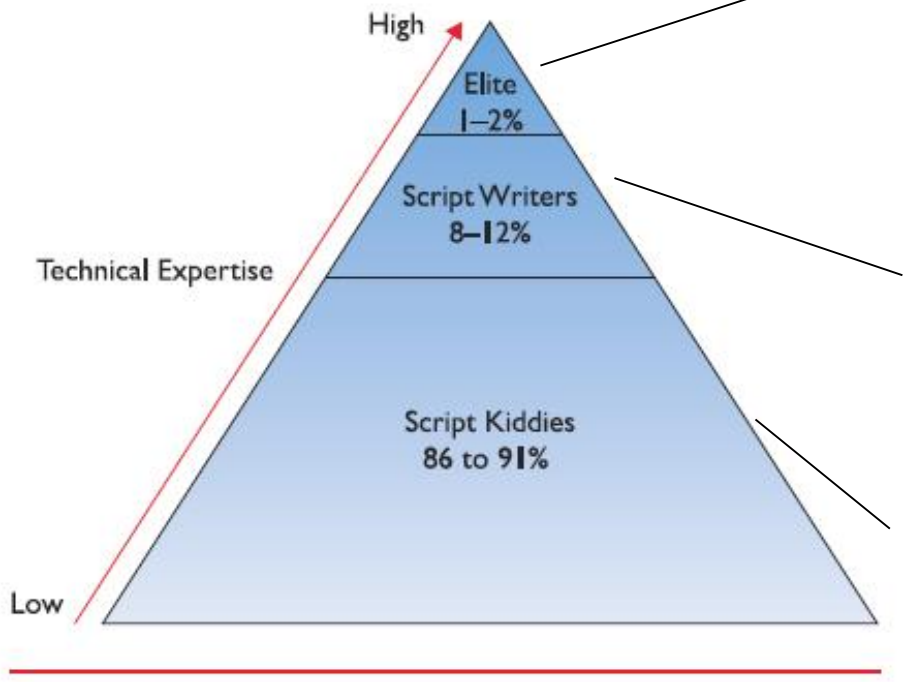
Threat Events: Software Attacks



Threat Events: Software Attacks (cont.)

Hacker = person that conducts a deliberate software attack

(can be distinguished based on their '**skill level**' & their '**mission**')



• Figure 1.1 Distribution of attacker skill levels

Elite Hackers: Individuals capable of **discovering new vulnerabilities** and writing programs (scripts) that exploit those vulnerabilities.

Script Writers: Individuals capable of writing scripts to exploit known vulnerabilities.

Script Kiddies: Individuals with (only) enough understanding of computer systems to be able to download and run scripts that others have developed. Vast majority of attack activity on the Internet is carried out by these individuals.

Lab 1

Threat Events: Software Attacks (cont.)

Hacking

Positive / Negative

Ethical Hacking: Penetration testing focusing on **securing and protecting** IT systems.

WHITE HAT	GRAY HAT	BLACK HAT
'good guys' hired to discover security vulnerabilities in a system	illegally access a system, but generally do not exploit the discovered vulnerability	'bad guys' (criminals) use their skills to conduct malicious activities

Threat Events: Software Attacks (cont.)

Example: Grey Hat Hackers …

October 12, 2018

A Mysterious Russian Grey Hat Vigilante has patch

Hacking

In the interes
first reported
into people's
kind of digita

On a Russia
over 100,00(

- 2014 – A grey hat hacks thousands of Asus routers and planted text warnings about files that were left exposed and reminding users to patch.
- 2015 – A group of grey hats, ironically called the White team, releases a piece of malware that closes security holes in several models of Linux routers.
- 2017 – A grey hat releases a piece of malware that punishes people for not patching their IOT devices by either deleting firmware or bricking them.
- 2017 – A grey hat makes over 150,000 printers print a message to their owners about the dangers of leaving your printer exposed online.
- 2018 – Another grey hat renames thousands of MikroTik and Ubiquiti routers "HACKED" to scare their owners into updating them.

https://www.thesslstore.com/blog/mysterious-russian-grey-hat-vigilante-patched-over-100000-routers/

WHAT IS A CYBER VIGILANTE?

A REBEL WITH GOOD CAUSE

Vigilantism is "a social movement giving rise to premeditated acts of force -or threatened force -by autonomous citizens" Johnston (1996) .

6 key elements of vigilantism, highlighted by Johnston:

- Planning, premeditation, and organization
- Private voluntary agency
- Autonomous citizenship
- The use or threatened use of force
- Reaction to crime and social deviance
- Personal and collective security

Vigilantes are practitioners of vigilantism. On the internet, these cyber vigilantes act outside of the criminal justice system to carry out missions of "good cause".

Cyber vigilantes usually act in response to a perceived and repercussive criminal act. There are many forms of cyber vigilantes including hacktivists, who hack for socio-political purposes.

In IoT, four cyber vigilantes created malwares to reduce vulnerable devices exploited by cyber criminals. All four malwares are explored.

Brickerbot

Silex

Wifatch

Hajime

Threat Events: Software Attacks (cont.)

a) Use of Malware

- **MALWARE** – a program that is **inserted into the victim system, usually covertly**, with the intention to:
  1) compromise the CIA of the victim's data, application(s) or the OS
  2) misuse the resources of the victim computer, or
  3) otherwise annoy or disrupt the victim

  (malware examples: *virus*, *worm*, *trojan*, *key-logger*, ...)

- **Common Malware Targets/Objectives**
  - steal credit card data, passwords, ...
  - destroy files, boot records, ...
  - store illegal music, movies, pirated software, ...

Threat Events: Software Attacks (cont.)

- **Malware Based on What it Does**
  - corruption of system or data files - virus & worms
  - turning the victim into a zombie - bot/botnets for DDoS
  - theft of information (logins, passwords, ...) - keyloggers & spyware
  - hiding of its presence - backdoors & rootkits

local machine harm

remote machine harm

no machine harm

- **Malware Based on How It Spreads/Propagates**
  - carried/spread by 'carriers' + replicate = **virus**
  - spread over a network on their own + replicate = **worms**
  - use 'social engineering' to 'sneak in' = **trojans**

produce copies of themselves

Different categories of malware ...

https://www.youtube.com/watch?v=n8mbzU0X2nQ

Threat Events: Software Attacks (cont.)

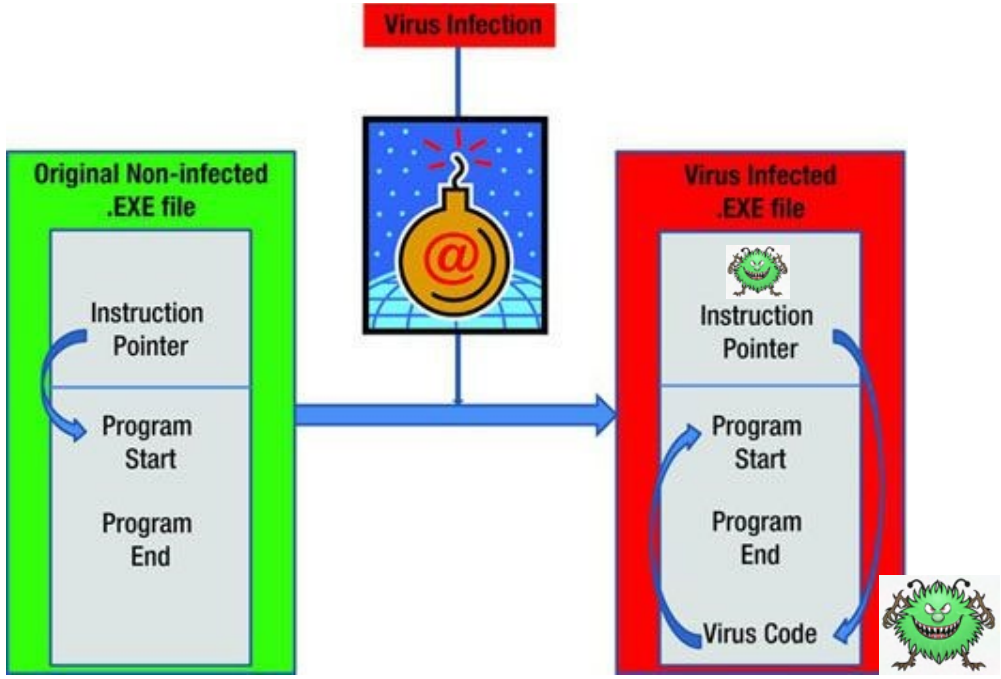
- **Malware Types**
  - Virus
  - Worm
  - Trojan horse
  - Logic Bomb
  - Rootkit
  - Information Stealer
  - Ransomware
  - Scareware
  - Spyware
  - Adware

Threat Events: Software Attacks (cont.)

- **VIRUS** – piece of software that 'infects' other host programs (executable) by modifying them

  - once a virus attaches to an executable, it can do anything that the executable is permitted to do (e.g., erase files & programs, change settings, etc.)

When viruses attach themselves to the executable files, they alter the instruction pointer of the executable programs in such a way that the virus code gets executed first before the actual executable code.



https://link.springer.com/chapter/10.1007/978-1-4302-6383-8_7

Threat Events: Software Attacks (cont.)

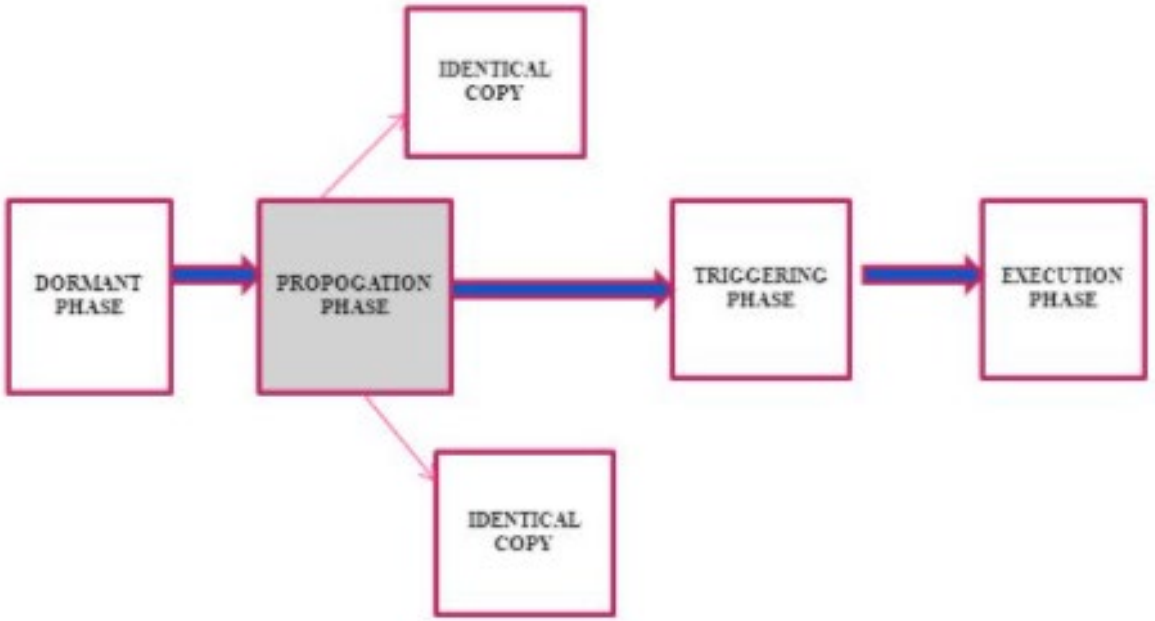
- VIRUS

✶ **phases of virus lifetime**

1) dormant phase - the virus is idle and eventually gets activated by some event (date, presence of another program or file, ...) - not always present
2) propagation/infection phase - the virus places a copy of itself into other programs - each infected program will contain a clone of the virus which itself will enter a propagation/replication phase
3) triggering phase - the virus is activated to perform the function for which it was intended - again, it can be caused by a variety of system events (e.g., number of times that the virus has replicated)
4) execution phase - the malicious function is performed and can be
   - harmless, (e.g.) a message on the screen
   - harmful, (e.g.) destruction of programs or files

Lifecycle of virus

1. **Dormant phase:** The virus is idle and activated by some event.
2. **Propagation phase:** It places an identical copy of itself into other programs or into certain system areas on the disk.
3. **Triggering phase:** The virus is activated to perform the function for which it was intended.
4. **Execution phase:** The function of virus is performed.



✶ **IMPORTANT: viruses need '2 factors' to replicate -**
carrier = document or host program, and
user = to initiate the propagation/triggering phase

Threat Events: Software Attacks (cont.)

- VIRUS

To infect the victim machine, virus must be executed!
Different viruses rely on different tech. to be executed.

- **classification of viruses by target /** means of execution

  a) boot sector infector - infects a master boot record and spreads when a system is booted from the disk containing the virus - nowadays rare

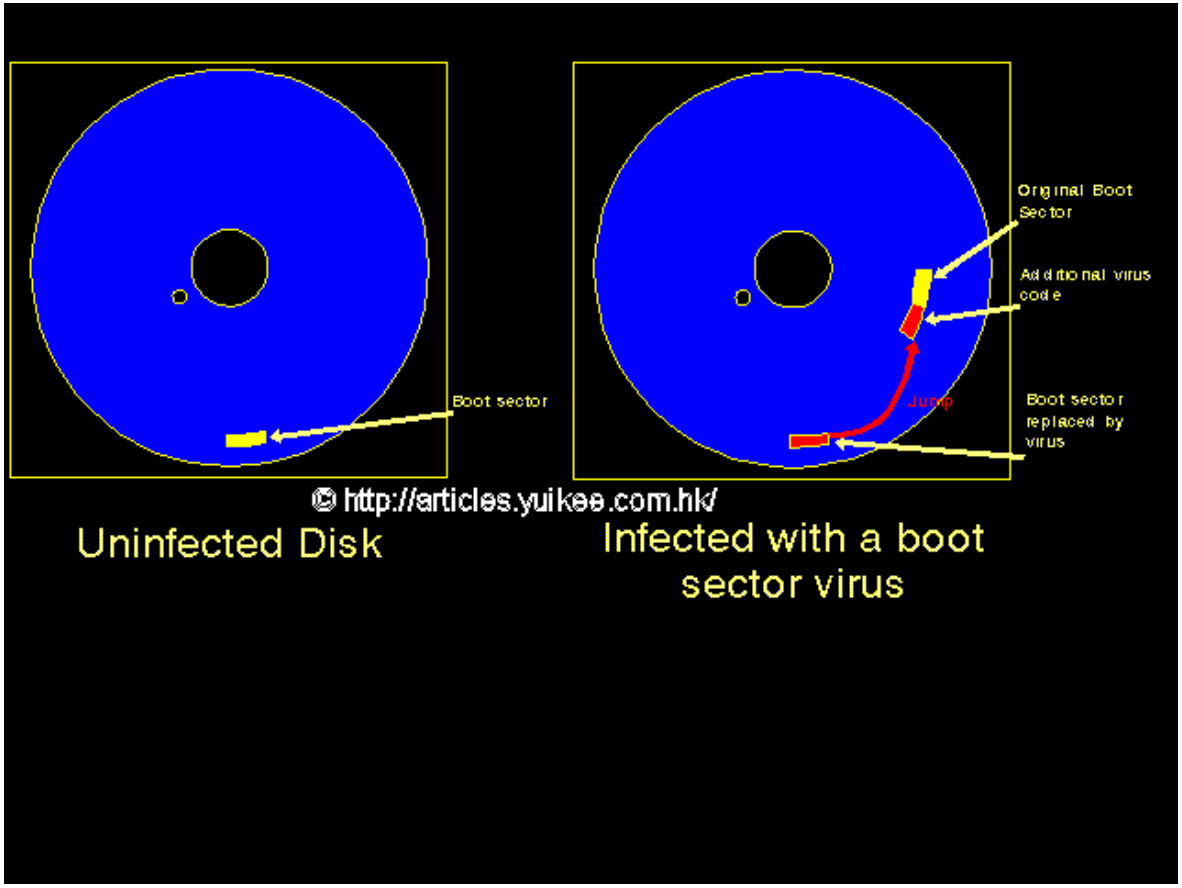
  b) file infector - infects executable files (.exe, .com)

  c) macro virus - infects files with macro or scripting code that are interpreted by an application -
  - easily spread, as 'documents', not applications are commonly exchanged among users today

  d) multipartite virus - uses multiple 'attack vectors', e.g., both boot sector and executable files on hard drive - most difficult to eradicate

Threat Events: Software Attacks (cont.)

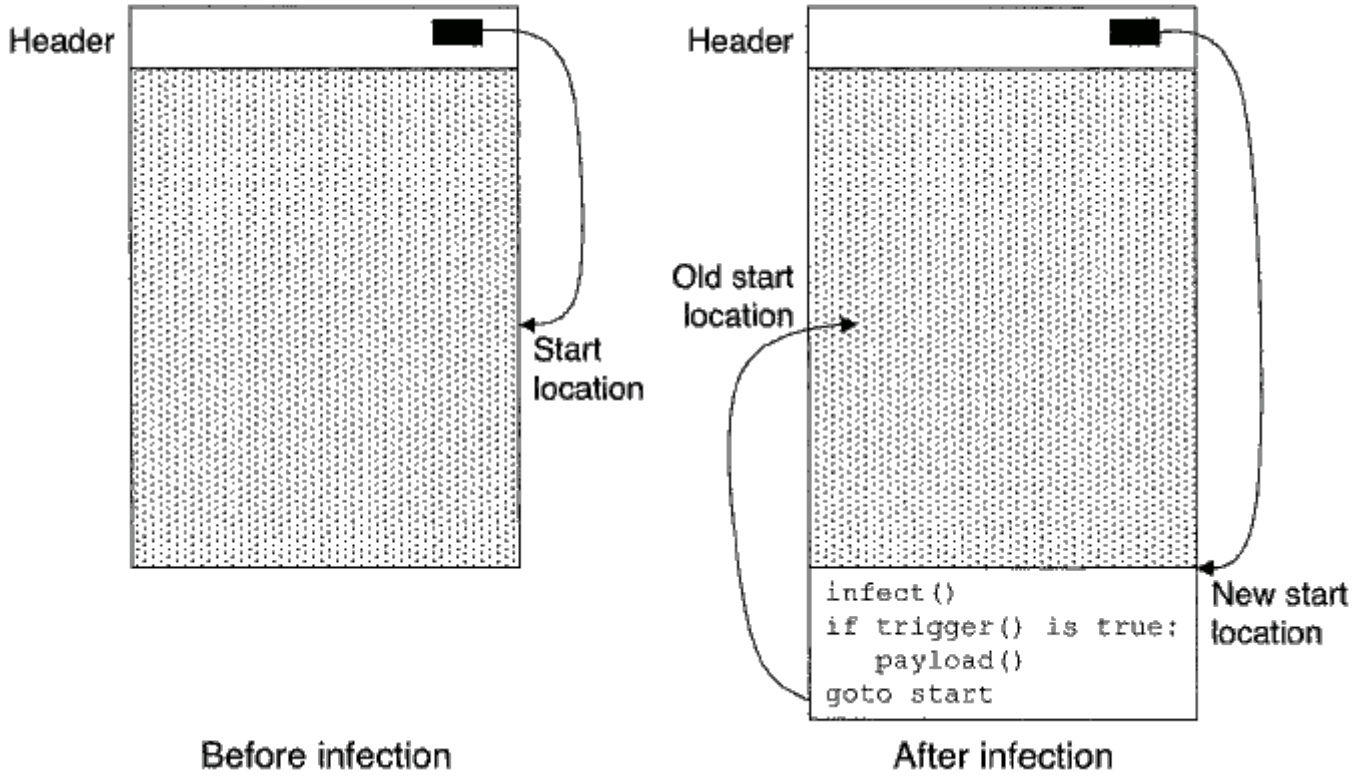
Boot Sector Virus



The Master Boot Record (MBR) is **the information in the first sector of any hard disk or diskette** that identifies how and where an operating system is located so that it can be boot (loaded) into the computer's main storage or random access memory.

Threat Events: Software Attacks (cont.)

File Infector Virus [found in .exe, .com programs]



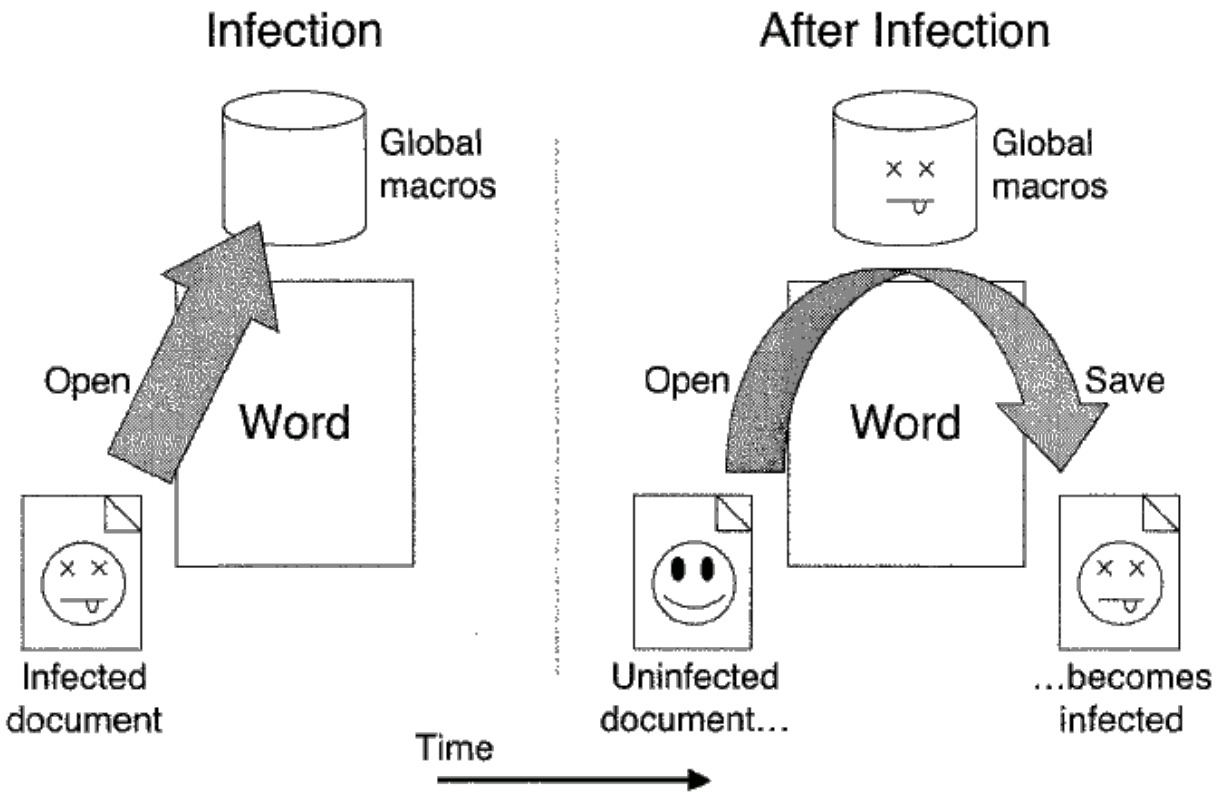
https://www.slideshare.net/hoangnamnguyen1694/ceh-v5-module-16-virus-and-worms

Threat Events: Software Attacks (cont.)

Macro Virus [found in .doc, .pdf files that get interpreted by MSWord and Acrobat]

macro - list of 'shortcut instructions' in a document (e.g., in Visual Basic)

Infect data files rather than programs !!!



https://www.slideshare.net/lastlinesecurity/introduction-to-malware-part-1

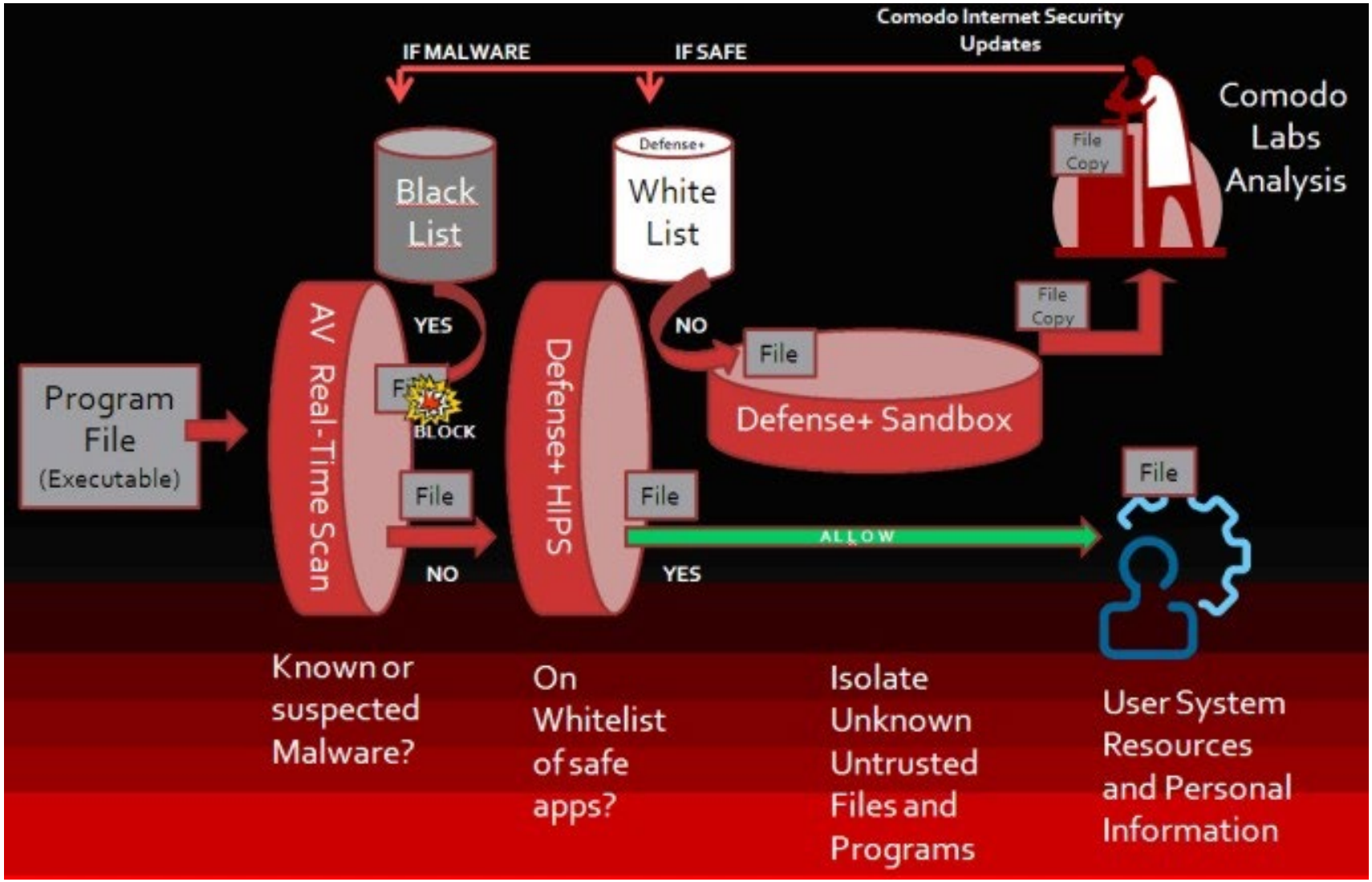
Threat Events: Software Attacks (cont.)

TYPES OF VIRUS CONTROLS. A computer virus may be categorized with one or more of the following four designations:

Boot sector infector	Master Boot Record (MBR) infector	File infector infector	Macro infector
•Boot sector viruses infect the boot record on hard disks, floppy disks, and theoretically also on CD's and DVD's. A boot sector virus does not need to be able to successfully boot the victims computer to infect it. Because of this, even non-bootable media can spread a boot sector virus.these viruses have become less common as floppy disks have become rarer.	•Master Boot Record (MBR) viruses are very similar to boot sector viruses, except that they infect the MBR (Master Boot Record) instead of the boot sector.	•File infector viruses infect files which contain executables code, such as .EXE and .COM files. Some file infectors are memory resident. This means that the virus will stay in memory and continue to infect other programs. Other file infector viruses only infect other files when they are executed.	•They infect certain types of data files, such as Word Documents, Excel Spreadsheets, PowerPoint Presentations, and Access Databases. Macro viruses typically use the Visual Basic macro language which is built into Microsoft Office applications.

How does ‘anti-virus’ work ??

All instances of anti-virus software are updated with latest ‘**signatures**’ of all known viruses.



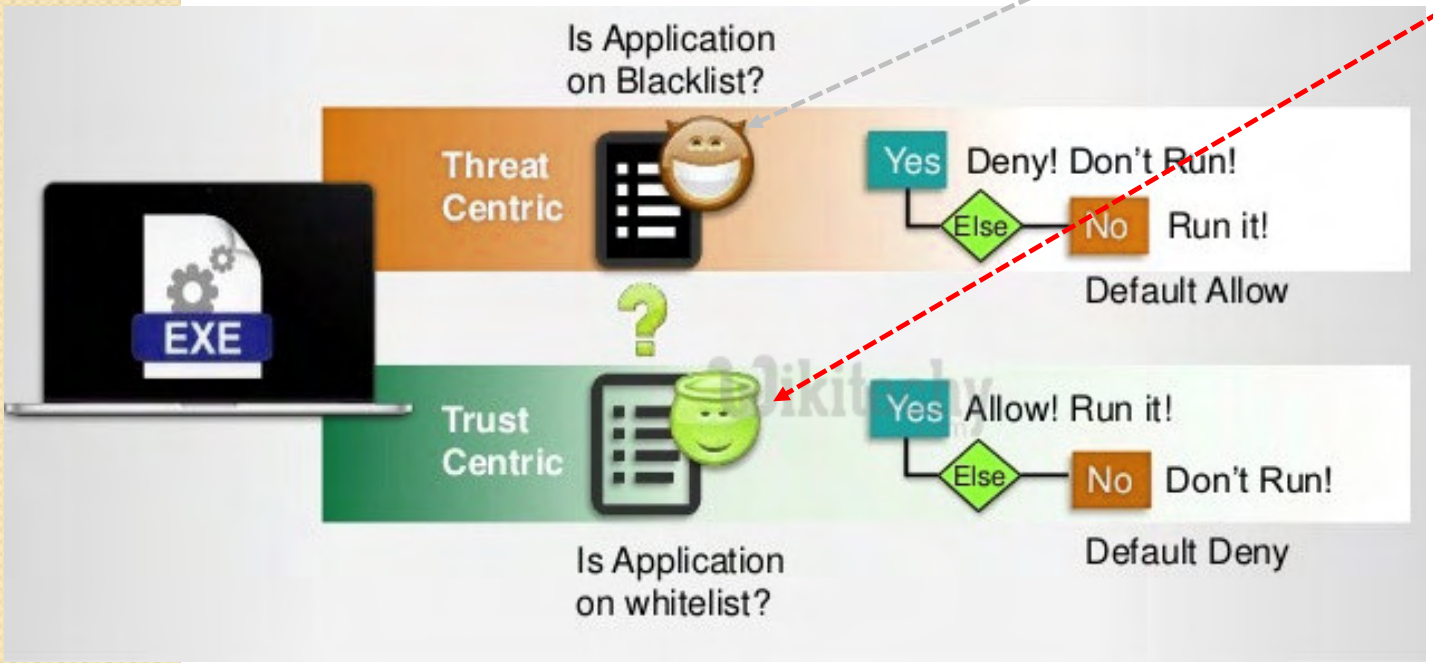
https://antivirus.comodo.com/faq/how-antivirus-works.html

Threat Events: Software Attacks (cont.)

Blacklisting vs. Whitelisting

Whitelisting and blacklisting prevent malware but they do this in opposite ways.

blacklisting vs. whitelisting – which is faster, which is stricter ?!?



Blacklisting:
allow everything
block some
good for detecting yesterday's (known) threats

Whitelisting:
block everything
allow some –
aka "zero trust"
good for detecting zero-day threats

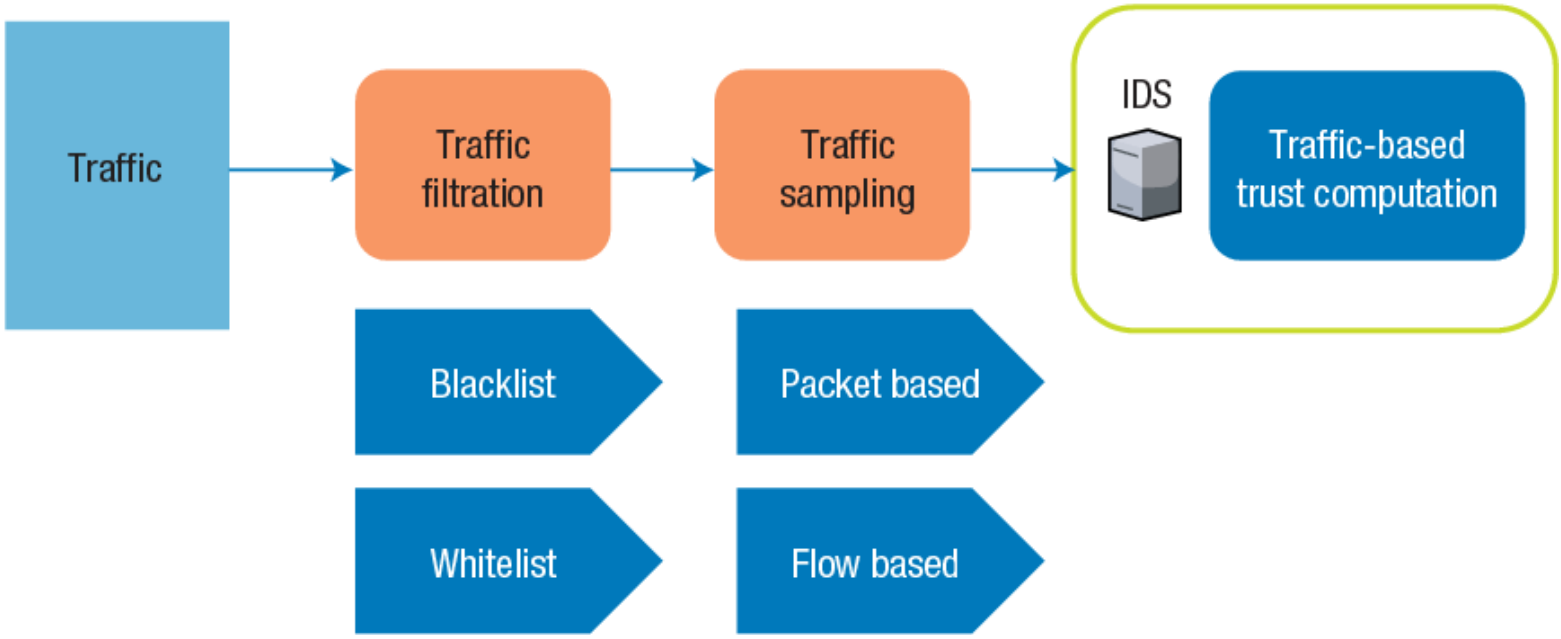
https://www.wikitechy.com/interview-questions/networking/what-is-whitelist

Threat Events: Software Attacks (cont.)

Example: Blacklisting / Whitelisting

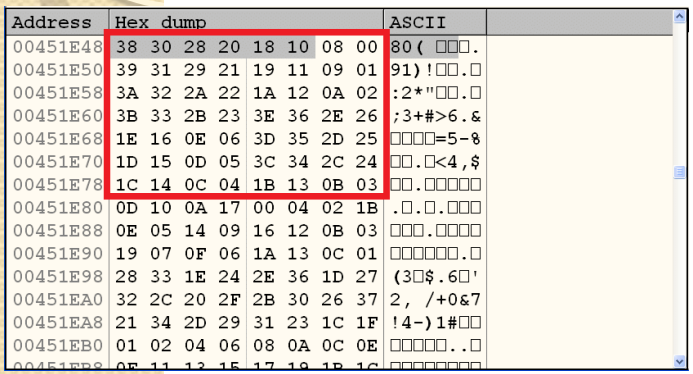
The concept also applies to:

- Web Domains (in a browser)
- IP addresses (in a firewall)
- email addresses (in email client)
- Intrusion Detection System (IDS) signatures …

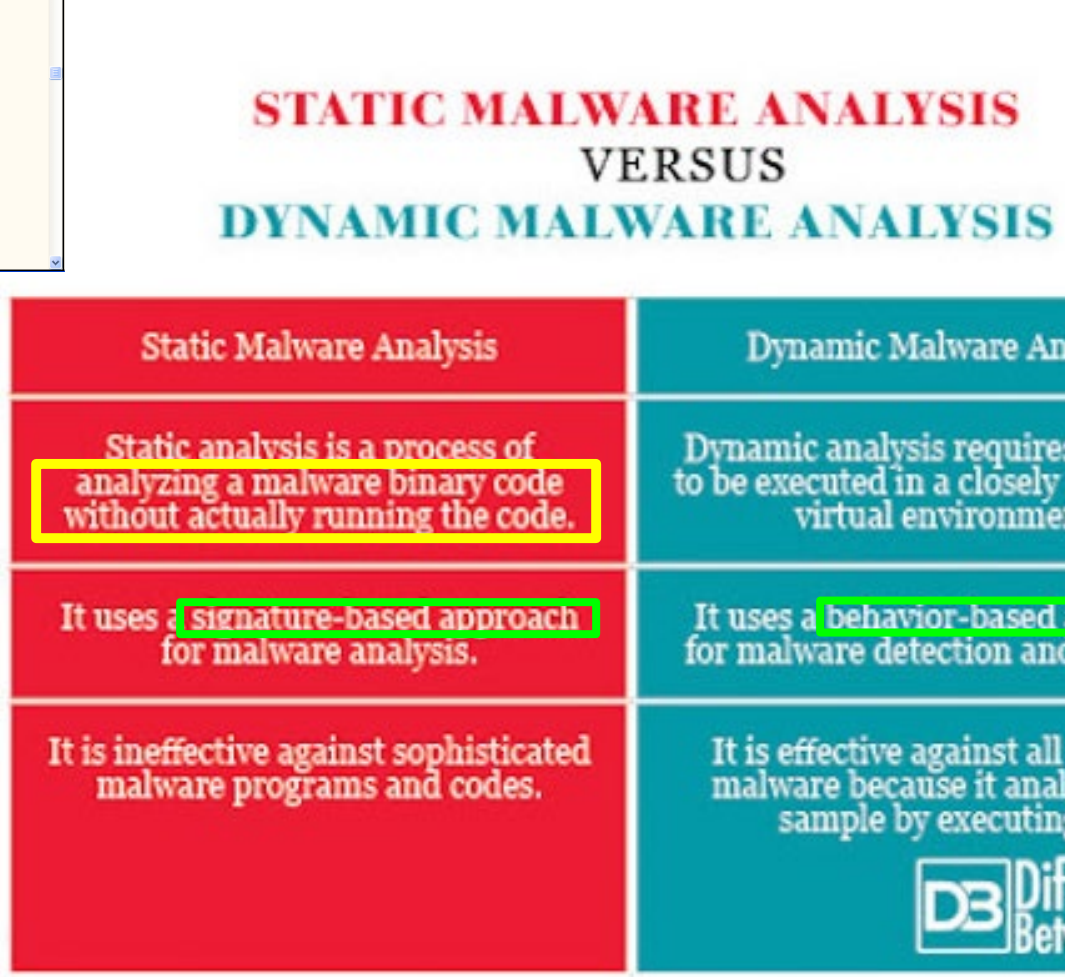


Threat Events: Software Attacks (cont.)

Types of Virus/Malware Analysis: Static vs. Dynamic

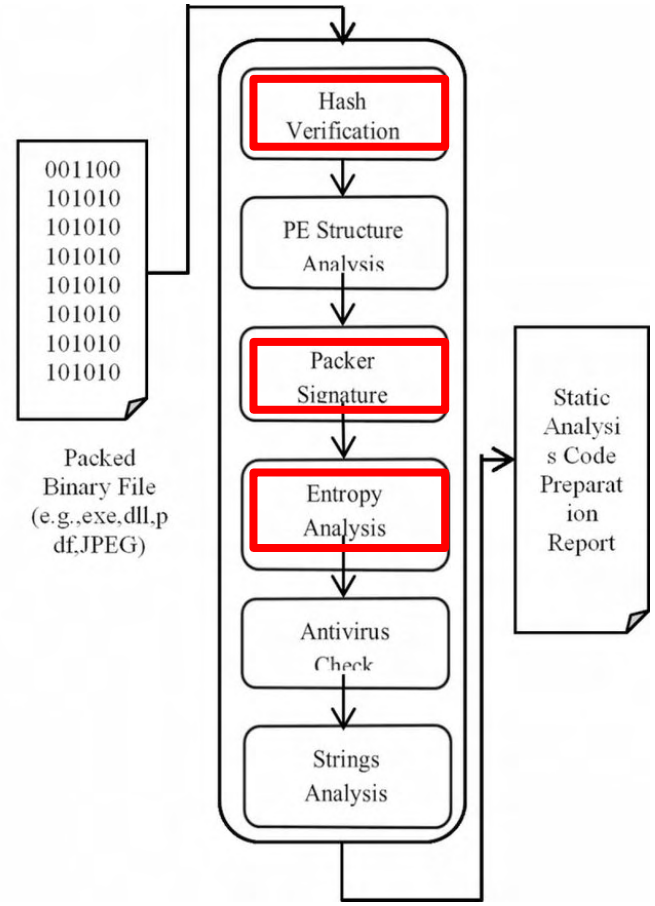


Address	Hex dump	ASCII
00451E48	38 30 28 20 18 10 08 00	80(□□□.
00451E50	39 31 29 21 19 11 09 01	91)!□□.□
00451E58	3A 32 2A 22 1A 12 0A 02	:2*"□□.□
00451E60	3B 33 2B 23 3E 36 2E 26	;3+#>6.&
00451E68	1E 16 0E 06 3D 35 2D 25	□□□□=5-%
00451E70	1D 15 0D 05 3C 34 2C 24	□□.□<4,$
00451E78	1C 14 0C 04 1B 13 0B 03	□□.□□□□□
00451E80	0D 10 0A 17 00 04 02 1B	.□.□.□□□
00451E88	0E 05 14 09 16 12 0B 03	□□□.□□□□
00451E90	19 07 0F 06 1A 13 0C 01	□□□□□□.□
00451E98	28 33 1E 24 2E 36 1D 27	(3□$.6□'
00451EA0	32 2C 20 2F 2B 30 26 37	2, /+0&7
00451EA8	21 34 2D 29 31 23 1C 1F	!4-)1#□□
00451EB0	01 02 04 06 08 0A 0C 0E	□□□□□..□



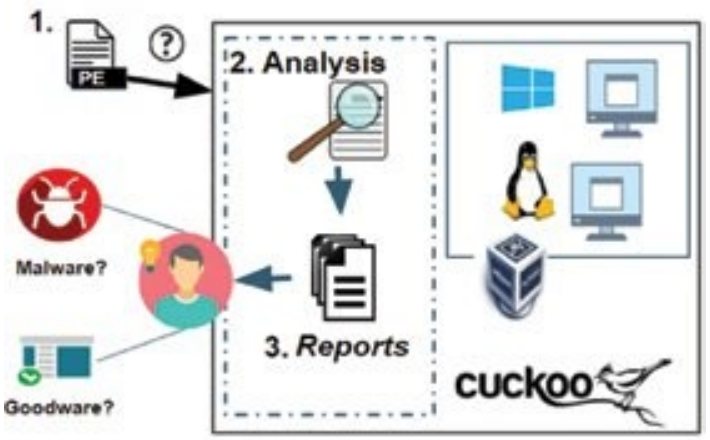
Threat Events: Software Attacks (cont.)

Static Malware Analysis



https://www.researchgate.net/publication/332215777_A_Mathematical_Model_of_HMST_Model_on_Malware_Static_Analysis/figures?lo=1

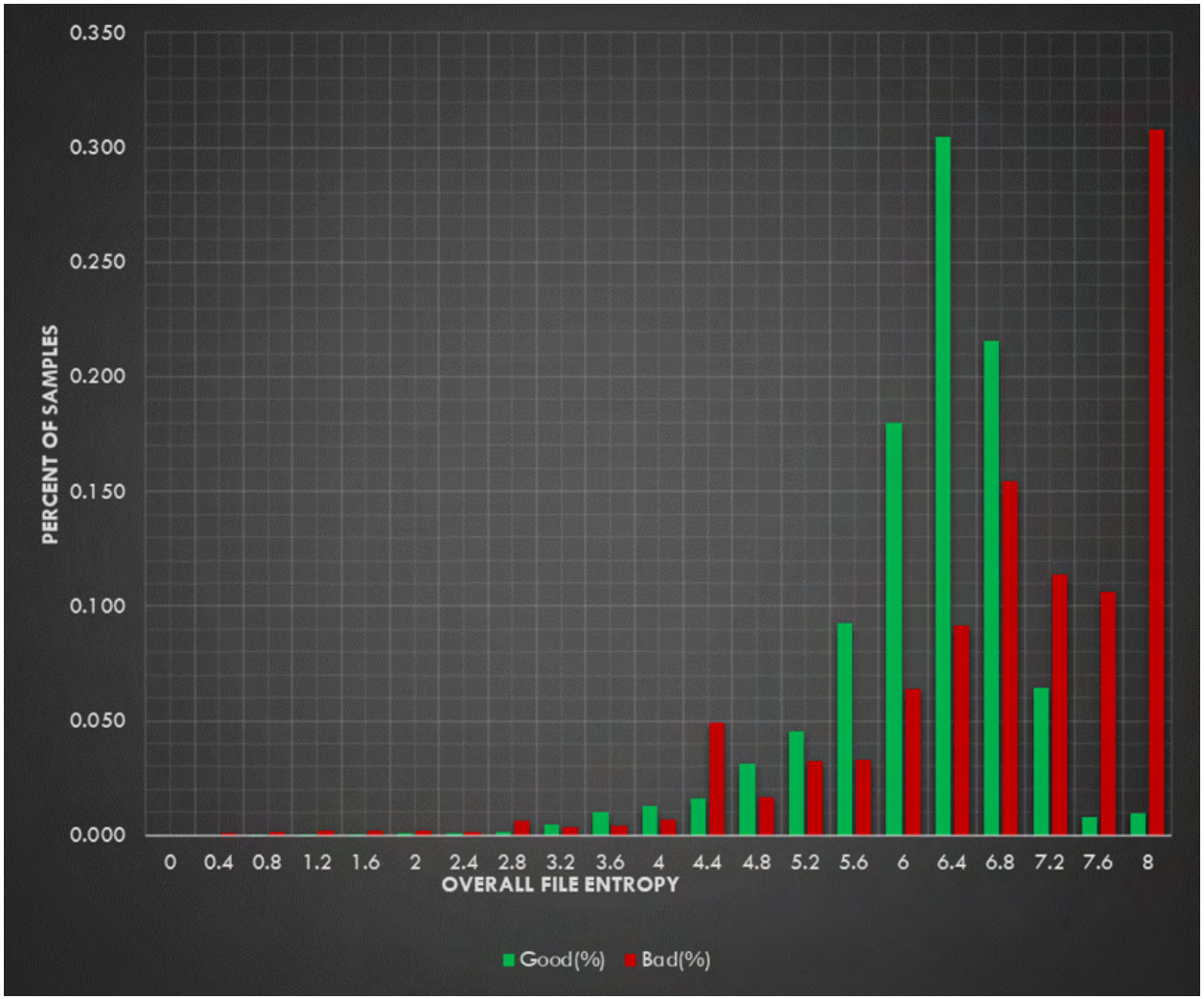
Dynamic Malware Analysis



A sandbox typically provides a tightly controlled set of resources for guest programs to run in. **Network access, the ability to inspect the host system or read from input devices are usually disallowed or heavily restricted.**

https://www.researchgate.net/publication/329496012_Building_malware_classificators_usable_by_State_security_agencies/figures?lo=1

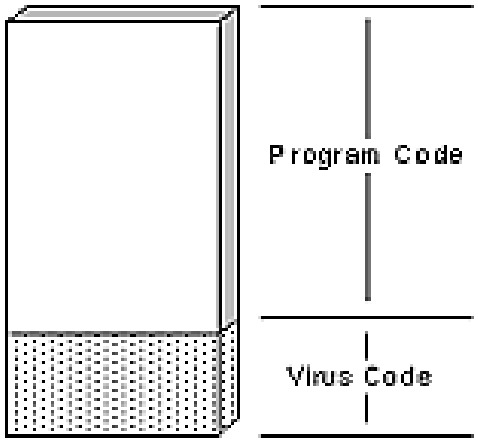
Threat Events: Software Attacks (cont.)



https://practicalsecurityanalytics.com/file-entropy/

Threat Events: Software Attacks (cont.)

- VIRUS



✶ **classification of viruses by concealment strategy**

i) **polymorphic virus** – mutates (changes its appearance) with every infection to avoid 'signature' (bit pattern) detection — avoids static detection

iv) **metamorphic virus** - mutates (changes its behavior dynamic binary/opcode/) with every infection while remaining 'functionally equivalent' — avoids dynamic detection

ii) **encrypted virus** - a portion of the virus creates a random key and encrypts the remainder - special case of polymorphic virus

iii) **stealth virus** - uses special techniques to conceal its presence on the OS

- makes sure that 'last modified' date of host file remains unchanged
- makes sure that the size of host file appears/ stays the same - aka cavity viruses

IMPORTANT:

Definition of polymorphic vs. metamorphic malware are very different in different books/papers.

The papers that supports the definition provided in these slides are:

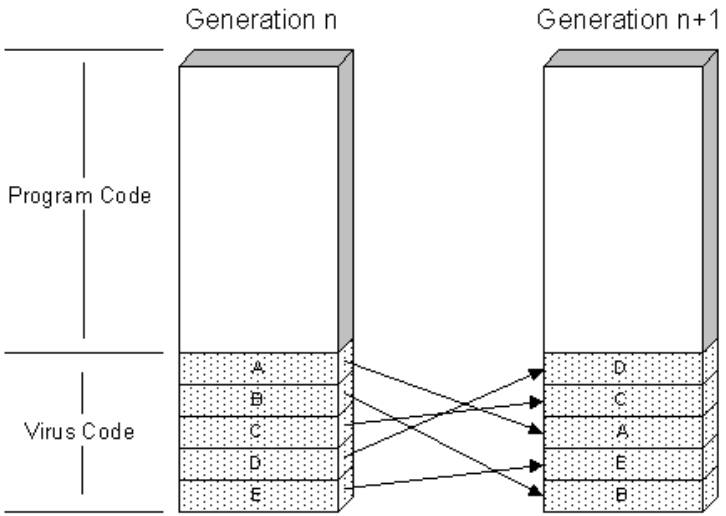
Philip OKane, Sakir Sezer, and Kieran McLaughlin. Obfuscation: The Hidden Malware. IEEE Security and Privacy, 9(5):41 – 47, September 2011
https://ieeexplore-ieee-org.ezproxy.library.yorku.ca/stamp/stamp.jsp?tp=&arnumber=5975134

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.728.3123&rep=rep1&type=pdf

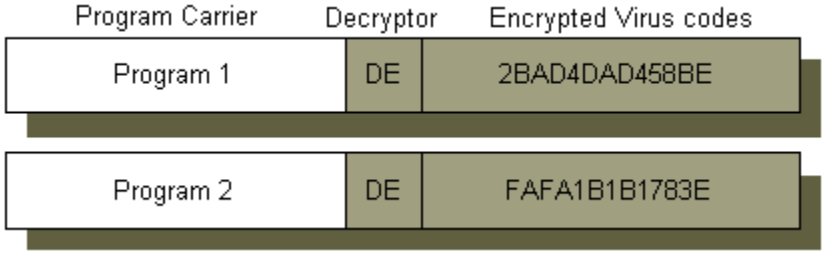
Metamorphism is a technique that mutates the dynamic binary code to avoid detection. It changes the opcode with each run of the infected program and does not use any encryption or decryption. The malware never keeps the same sequence of opcodes in the memory. This is also called *dynamic code obfuscation*. There are two kinds of metamorphic malware defined in [21] based on the channel of communication used: *Closed-world malware*, that do not rely on external communication and can generate the newly mutated code using either a binary transformer or a metalanguage. *Open-world malware*, that can communicate with other sites on the Internet and update themselves with new features.

Threat Events: Software Attacks (cont.)

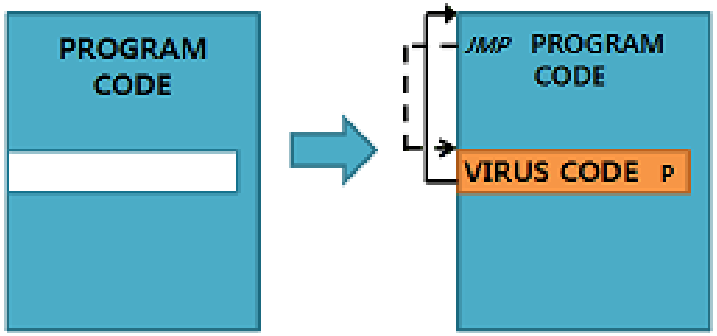
Polymorphic Virus



Encrypted Virus



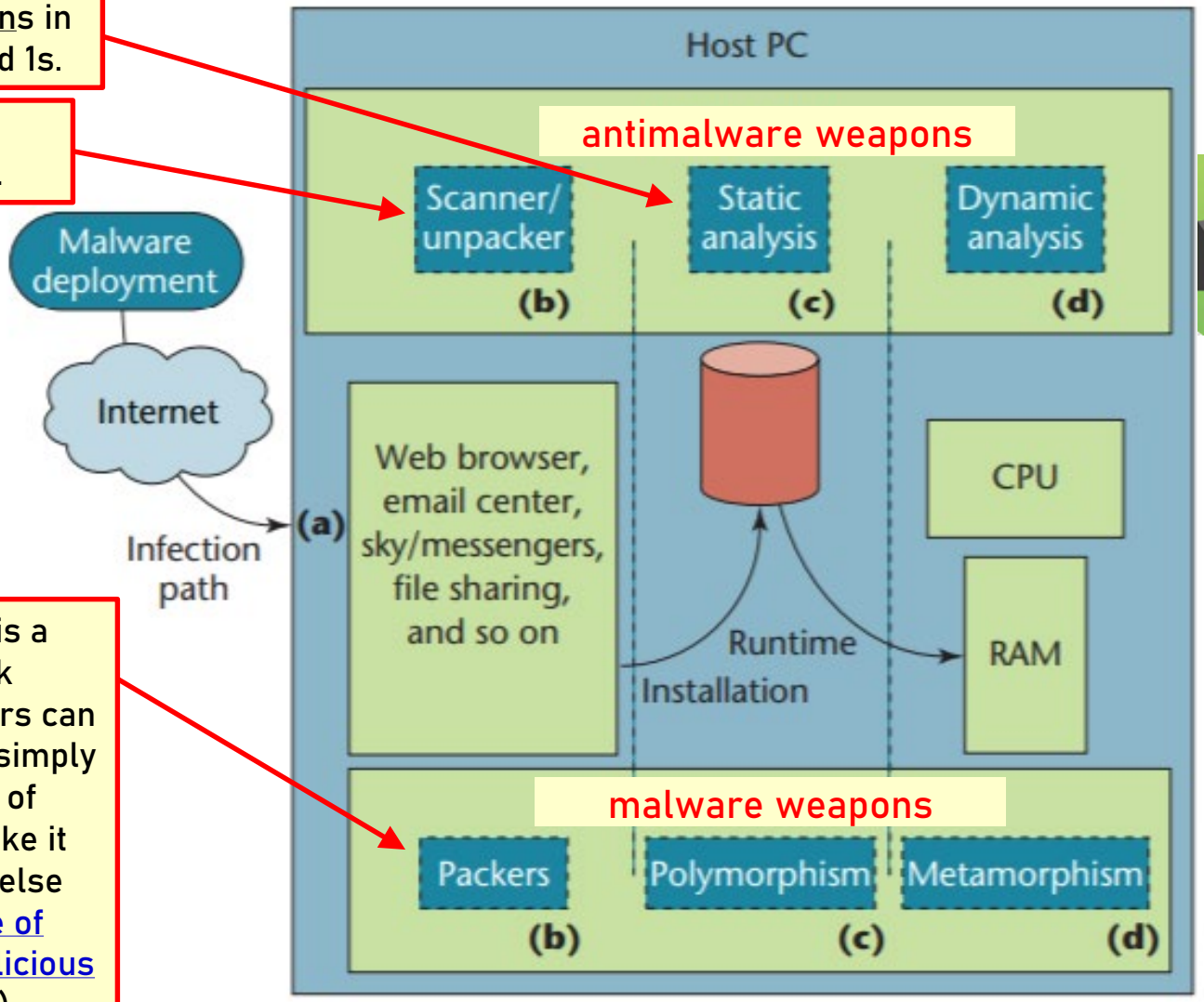
Stealth (Cavity) Virus



Different generations of anti-malware / malware weapons

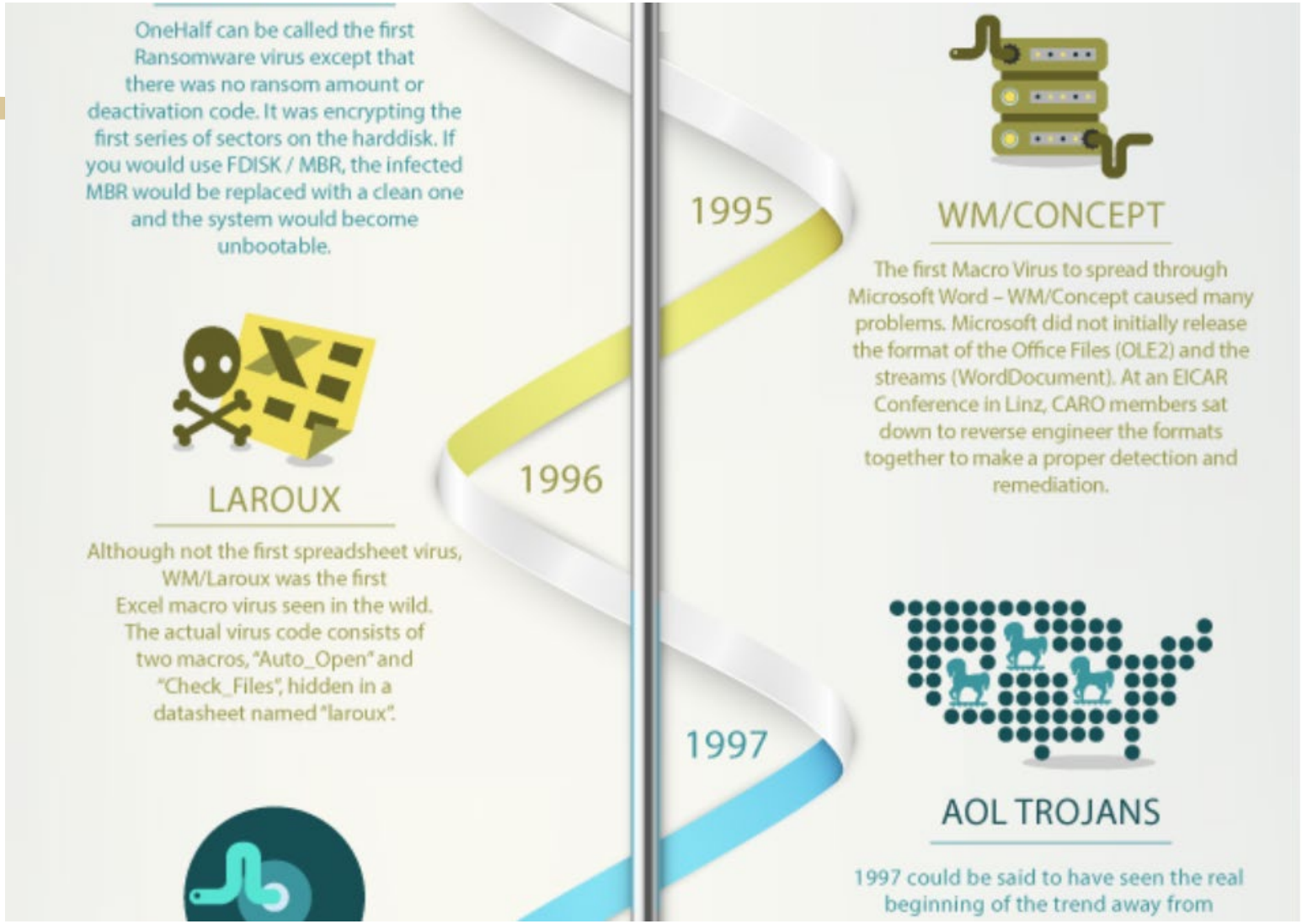
Look for some variations in the sequence of 0s and 1s.

Look for an identical sequence of 0s and 1s.



A malware packer is a tool used to mask a malicious file. Packers can encrypt, compress or simply change the format of a malware file to make it look like something else entirely. (Sequence of instructions in the malicious code unchanged.)

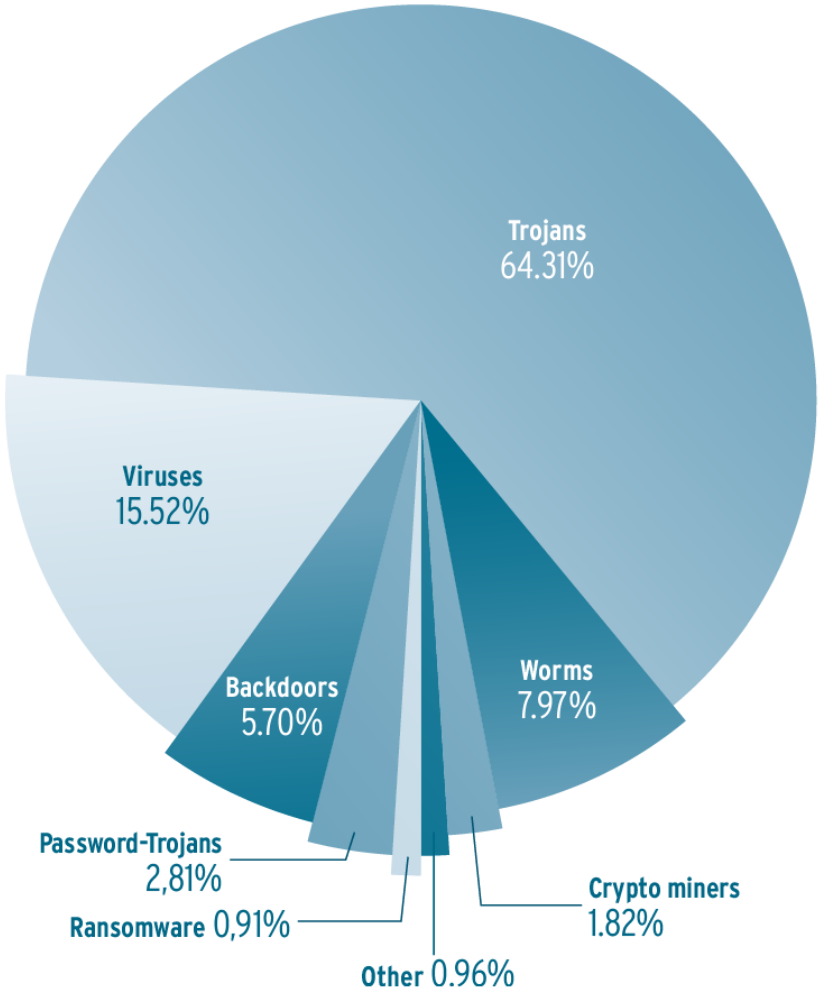
Figure 1. The antimalware-malware weapons race's four phases. (a) Systems were infected from various sources. (b) Signature scanners were countered by malware packing. (c) Static analysis was countered by polymorphic malware. (d) Dynamic analysis was countered by metamorphic malware.



https://www.welivesecurity.com/2014/10/17/infographic-brief-history-of-malware/

Distribution of malware under Windows in 2019

AV-TEST
The Independent IT-Security Institute



https://www.pcmag.com/news/windows-computers-account-for-83-of-all-malware-attacks-in-q1-2020

Threat Events: Software Attacks (cont.)

- **WORM** – malware **actively** seeks out more machines to infect and then each infected machine serves as an automated launching pad for attacks on other machines

  - worms exploit software vulnerabilities in **client or server** programs to gain access to a new system

    (worm = power of virus + **convenience of Internet**)

  - IMPORTANT: viruses vs. worms

    - viruses need a carrier medium (document or program to 'attach' itself to) and then require user action to propagate
    - worms do not always need a carrier or human action to move (can some times 'move' on their own), are typically **spread through the Internet**, does not always rely on user to replicate/infect

BASIS FOR COMPARISON	VIRUS	WORMS
Meaning	The Virus attaches itself to executable files and transfers from one system to the other.	A Worm is a malicious program that replicates itself and can spread to different computers via Network.
Human Action to infect !	Needed	Not Required
Speed of Spreading	Slower as compared to Worm	Fast
Requirement of host	Host is needed for spreading.	It doesn't need a host to replicate from one computer to another.
Removing Malware	Antivirus, formatting	Virus removal tool, formatting
Protect the System using	Antivirus software	Antivirus, firewall
Consequences	Corrupt and erase a file or program.	Consumes system resources and slows down it, and can halt the system completely.

carrier

Threat Events: Software Attacks (cont.)

- **WORM**

  - ✶ classification of worms by replication strategy

Infects email client; propagates on its own, but requires user action to activate. →

1) electronic mail or instant messaging - worm emails a copy of itself to other systems, or sends itself as an attachment via an instant message service

Propagates and activates on its own, but needs a carrier. →

2) file sharing - worm copies itself on removable media such as USB drives; it, then, executes when the drive is connected to another system

3) remote login capability - worm logs onto a remote system as a user and then uses commands to copy itself from one system to another

4) remote file access or transfer capability - worm uses a remote file access or transfer service to another system to copy itself

etc. ....

Threat Events: Software Attacks (cont.)

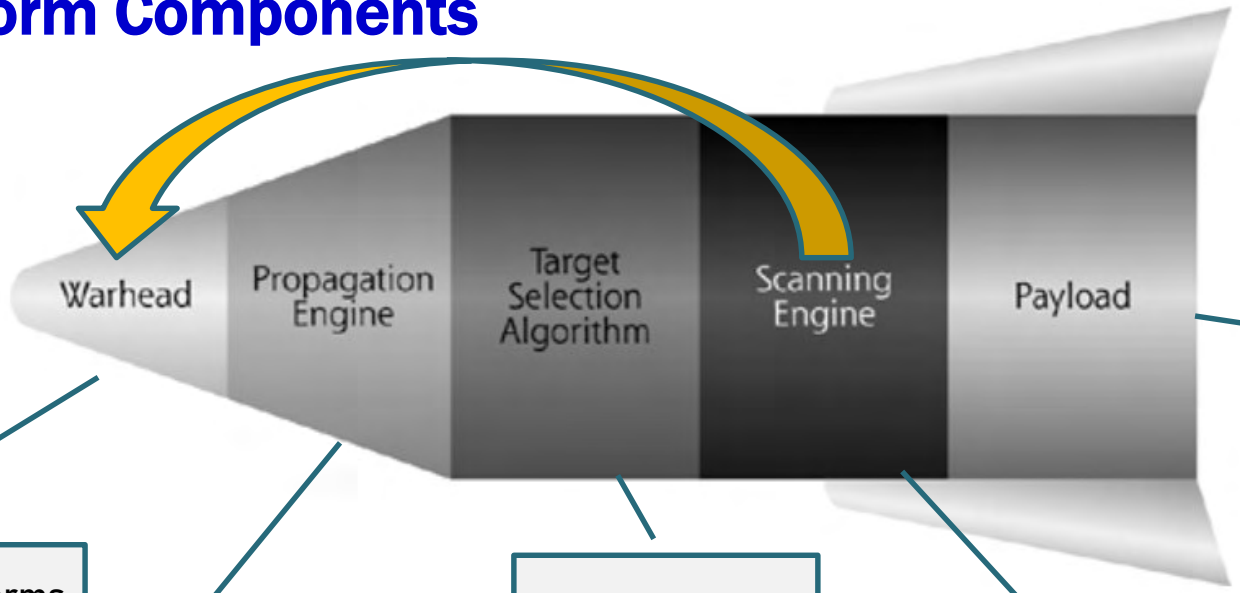
Example: USB Virus vs. USB Worm

VIRUS: Malware 'sits' inside a 'carrier' (program/document) and requires the user to manually move the carrier 'onto' a USB (on one computer) and 'from' a USB (to another computer) and to click on it.

Worm: Malware on its own infects the USB (copies itself as autoran.inf); when plugged into a new host, automatically executed & infects the new machine.

Threat Events: Software Attacks (cont.)

Worm Components



Methods worms use to first gain access to the victim machine:
- drive-by-download
- email
- file sharing

etc.

Methods worms use to transfer the rest of its body to the target:
- file transfer
- HTTP

etc.

Once the worm is running on the victim machine it starts looking for new victims to attack
- email address
- host lists
- different IPs targets

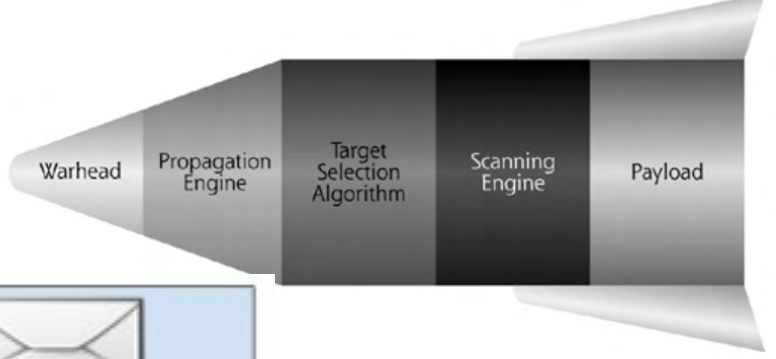
etc.

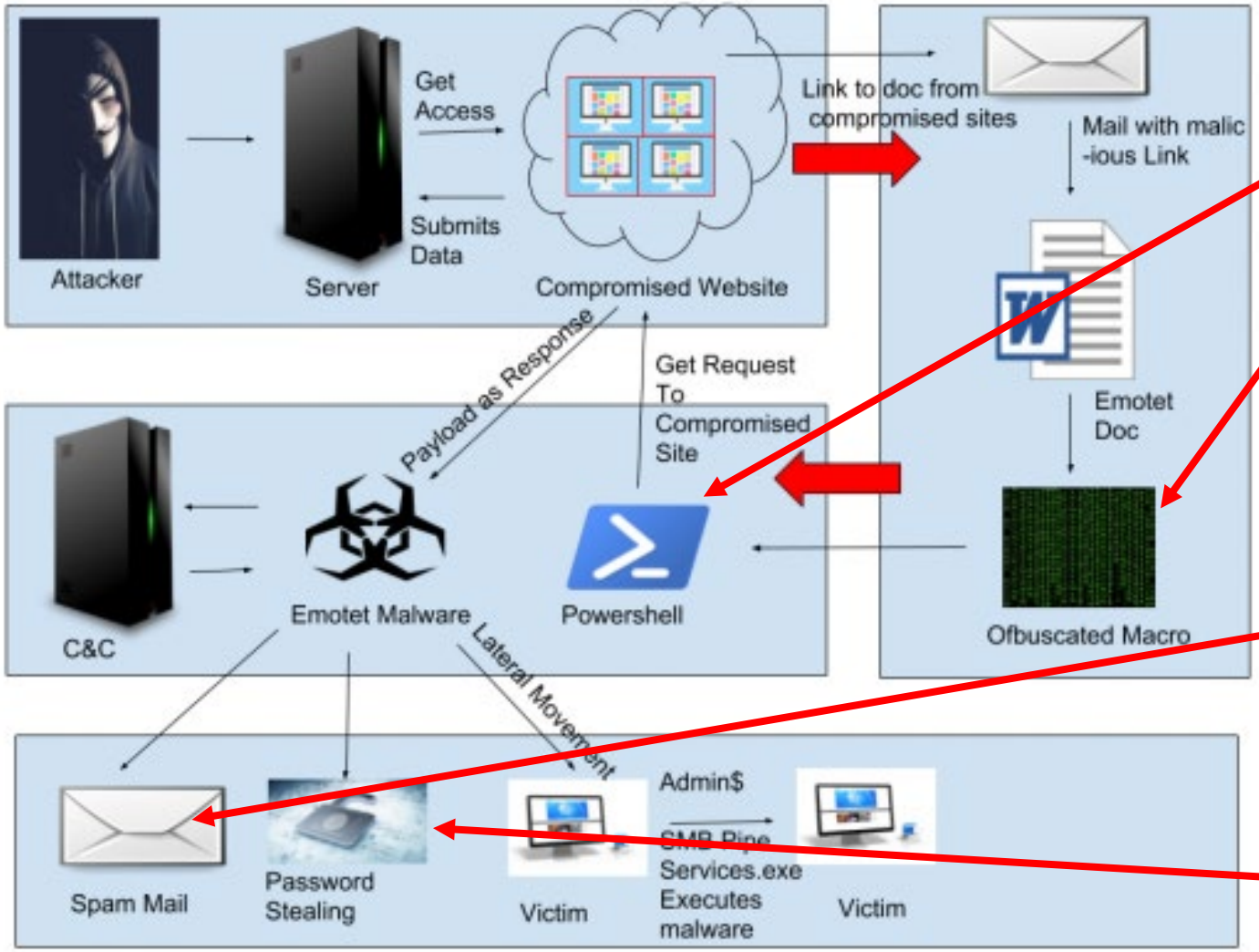
Using addresses generated by the target engine, the worm actively scans across the network to determine suitable victims

Chunk of code designed to implement some specific action on behalf of the attacker on a target system. It is what the worm does when it gets to a target …
- opening a backdoor
- planting a DDoS bot
- performing a complex math operation (e.g., cryptominer)

https://userpages.umbc.edu/~dgorin1/432/worms.htm

Emotet





Propagation Engine

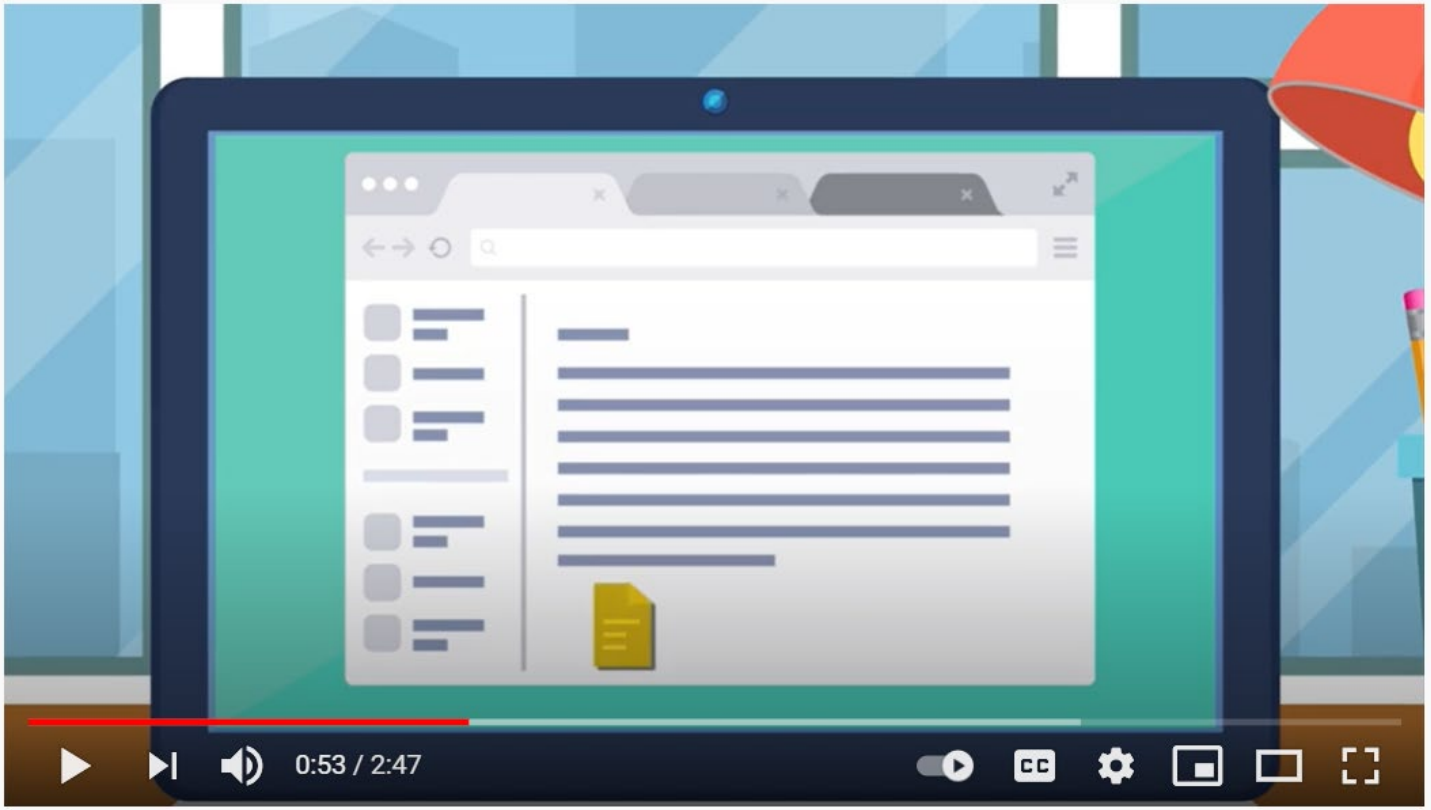
Warhead - small hard-to-detect piece of code

Target Selection Algorithm + Scanning Engine

Payload

https://blogs.quickheal.com/beware-your-website-might-be-delivering-emotet-malware/

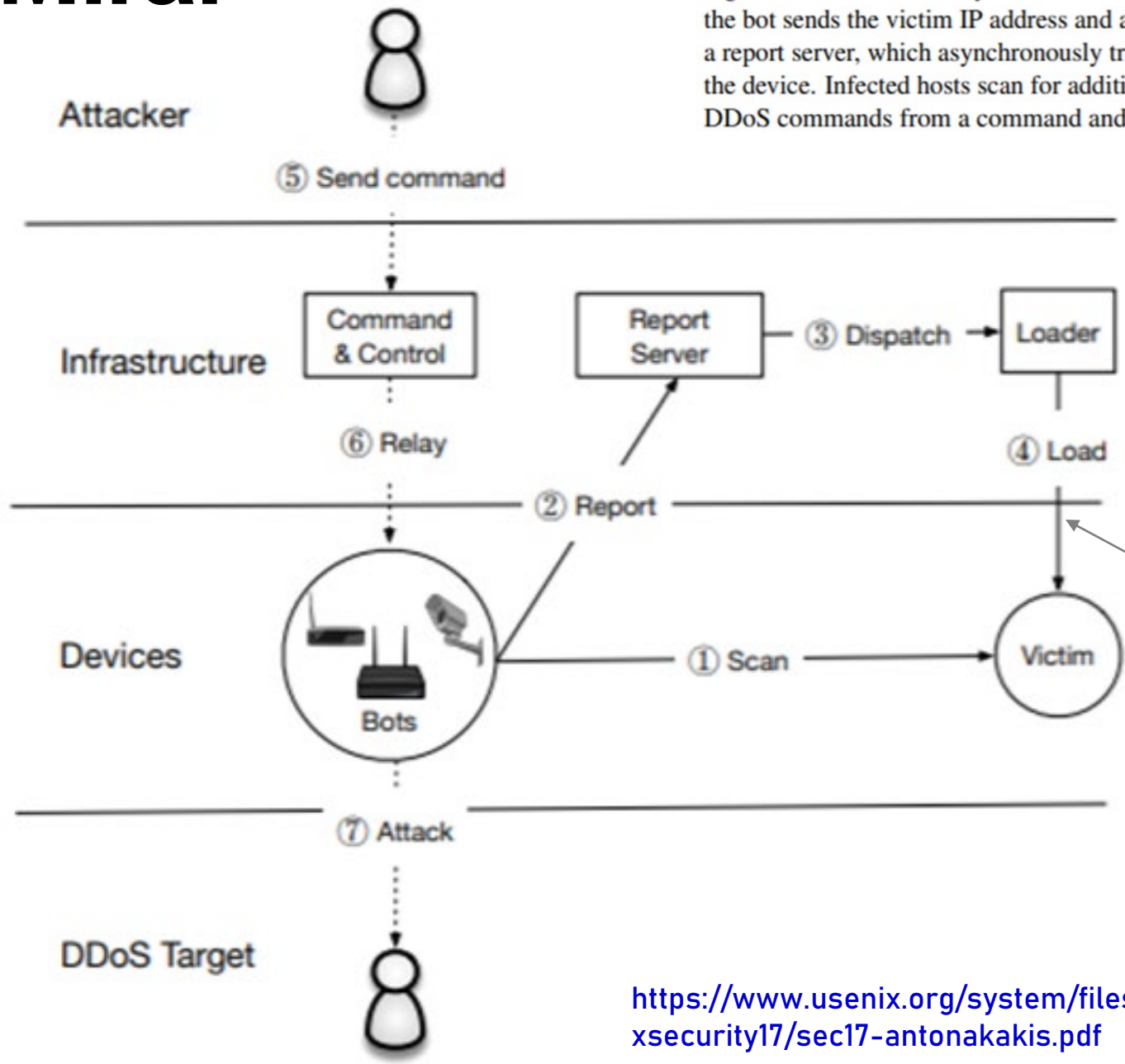
Emotet



https://youtu.be/CkwKTBifXJg

Mirai

Figure 2: **Mirai Operation**—Mirai bots scan the IPv4 address space for devices that run telnet or SSH, and attempt to log in using a hardcoded dictionary of IoT credentials. Once successful, the bot sends the victim IP address and associated credentials to a report server, which asynchronously triggers a loader to infect the device. Infected hosts scan for additional victims and accept DDoS commands from a command and control (C2) server.



After step 4, the victim becomes a fully infected 'bot'.

https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf

Threat Events: Software Attacks (cont.)

- **WORM**
  - ✶ classification of worms by target discovery
    - a) random - each compromised host probes random addresses in IP addr. space - fast development, but 1) unknown results (many machines may not be vulnerable), 2) some machine may already infected
    - b) hit list - the attacker pre-compiles a long list of potentially vulnerable machines, each infected machine uses a part of this list - time consum. devel.
    - c) topological - worm uses information contained on the infected machine to find more hosts to scan - e.g., worms infecting/exploiting P2P applications
    - d) local subnet - worm uses the subnet address to find other vulnerable machine on the same network (works well against firewall-protection)

Threat Events: Software Attacks (cont.)

Ideally, we would want to 'catch' a worm while in Slow Start phase ...

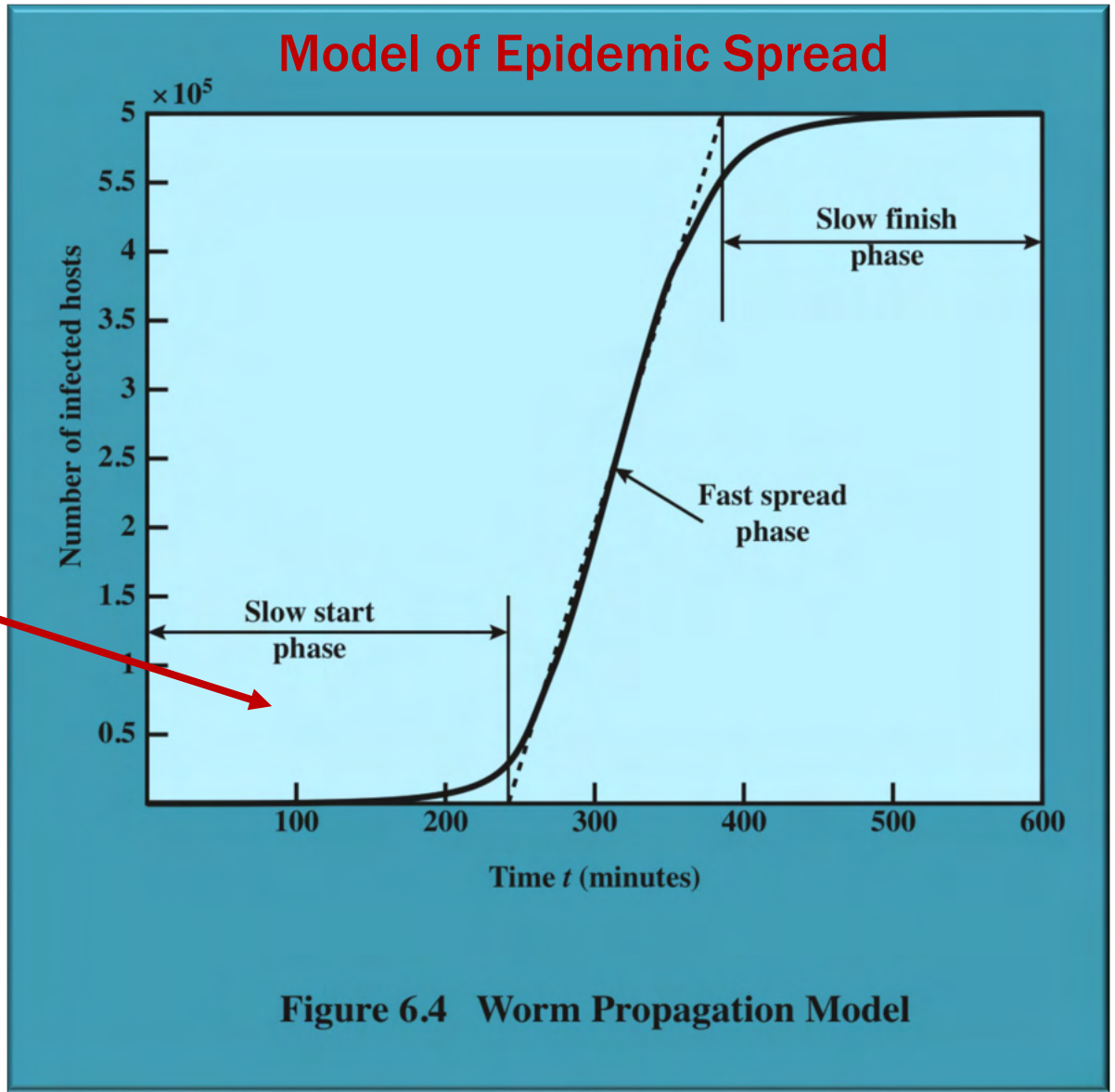


Figure 6.4 Worm Propagation Model

SLOW FINISH: most vulnerable machines have been infected

Threat Events: Software Attacks (cont.)

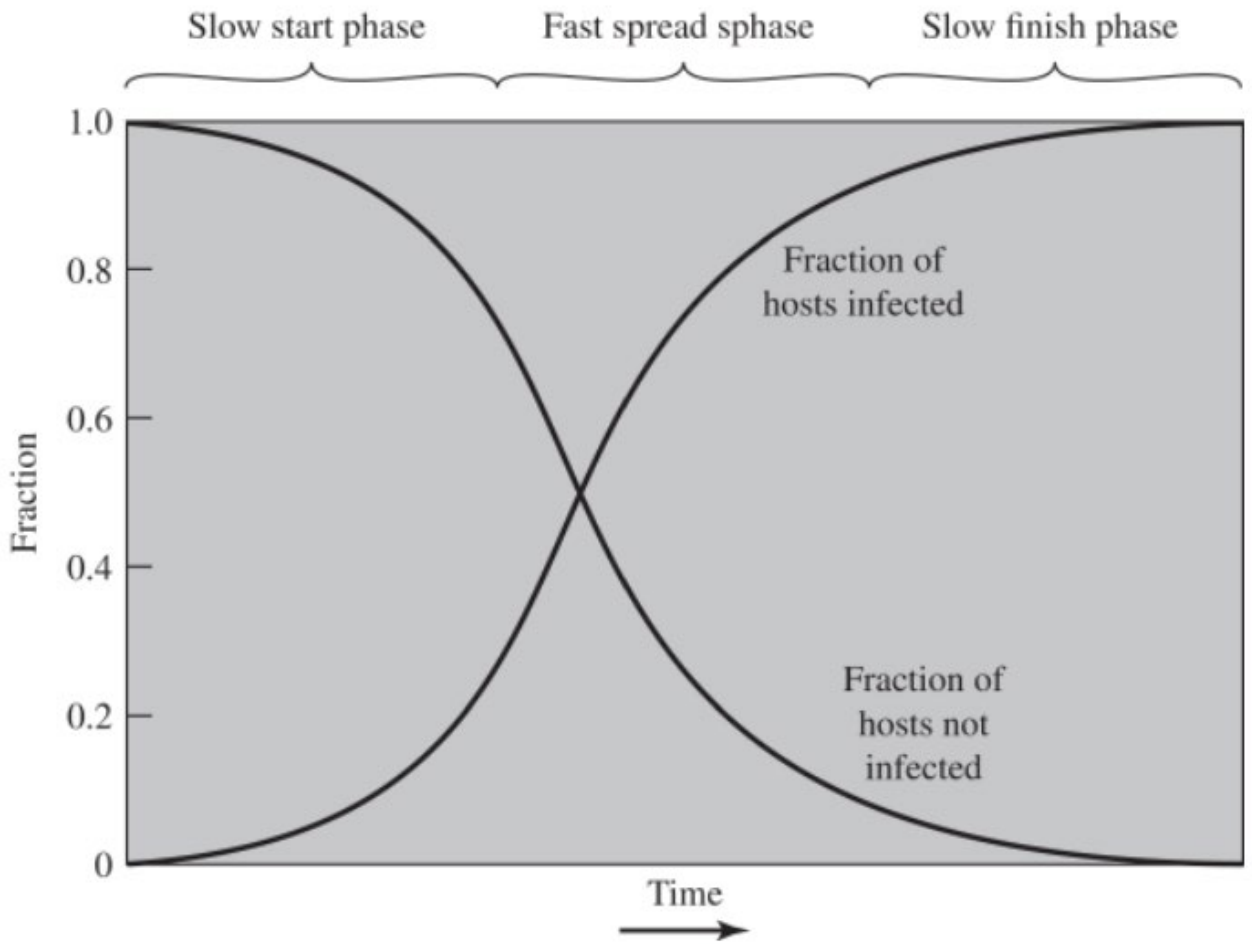
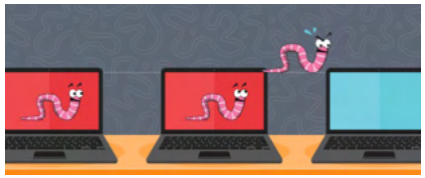


Figure 6.2 Worm Propagation Model

Example: Worm propagation …



Consider a network consisting of N machines and a worm that uses 'local network' propagation model. In particular, at time t=0, the worm has infected only 1 machine. In each subsequent minute, every infected machine contacts and successfully infects k=2 other machines on the same network. (You can also ssume:

1) All the machines in this network are 'vulnerable' to the given worm.
2) The worm is 'smart' so that an infected machine never tries to infect another infected machine.)

If N = 200, how many minutes does it take to infect all the machines in the system?

Solution

1st minute: 1 old + 2 new infected = 3 infected machines

2nd minute: 3 old + 3*2 new infected = 9 infected machines

3rd minute: 9 old + 9*2 new infected = 27 infected machines

4th minute: 27 old + 27*2 new infected = 81 infected machines

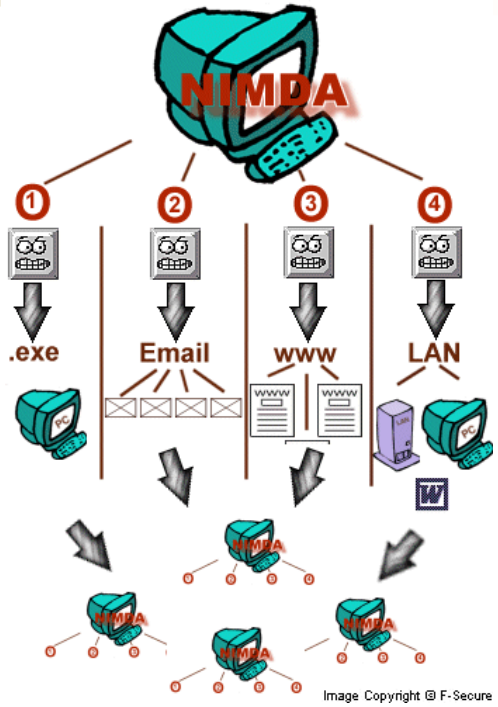
5th minute: 81 old + 81*2 new infected = 243 infected machines

Threat Events: Software Attacks (cont.)

- **WORM**
  - ✶ state of worm technology
    - i) multi-platform / cross-platform - target a variety of platforms / OSs
    - ii) multi-exploit - penetrate systems in a variety of ways (through email, browsers, file sharing, ...)
    - iii) ultrafast spreading - use various techniques to to identify as many vulnerable machines in a short period of time
    - iv) polymorphic
    - v) metamorphic
    - vi) multi 'transport vehicle' - can carry a variety of payloads (rootkits, spam generators, bots, etc.)
    - vii) zero-day exploit - try to exploit new/unknown vulnerabilities

Threat Events: Software Attacks (cont.)

- **Nimda (2001)** – first multi-exploit worm – used 5 different infection paths:
  - * via email
  - * via browsing of compromised web sites – an injected java-script would allow the downloading of Nimda
  - * via open network shares on LANs
  - * via exploiting of vulnerabilities in Microsoft's IIS server
  - * via back doors left behind by the Code Red



Nimda cost an estimated $635 million in damages.

Nimda itself does not contain a destructive payload beyond modification of Web content to continue to propagate itself.

DoS may occur because of the volume of e-mail traffic triggered by this worm, but it doesn't appear to be targeting specific systems with a DoS attack.

http://www.f-secure.com/v-descs/nimda.shtml

https://www.techrepublic.com/article/learn-what-nimda-worm-does-and-how-to-combat-it/

https://www.eweek.com/security/nimda-takes-over-the-net/

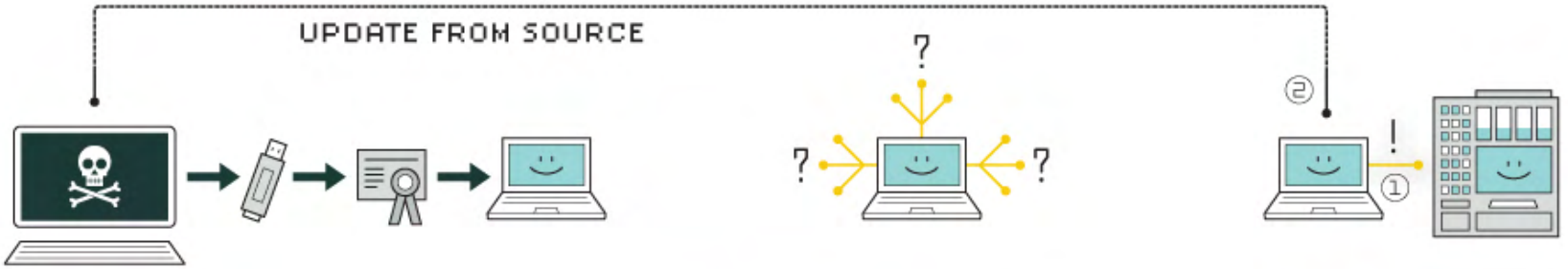
Threat Events: Software Attacks (cont.)

- **Stuxnet (2010)** – a highly sophisticated worm that used a variety of advanced techniques to spread, including:
  - by the use of shared infected USB drives (spreads even between computers that are not connected to the Internet);
  - by connecting to systems using a default SQL database password;
  - by searching for unprotected administrative shares of systems on the LAN; …

While it was programmed to spread from system to system, it was actually searching for a very specific type of system to execute – programmable logic controller (PLC) system made by Siemens and run on devices that control and monitor industrial processes. When it found such a system, it executed a series of actions designed to destroy centrifuges attached to the Siemens controller.

multi-exploit | multi-platform | targeting CPS

HOW STUXNET WORKED



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

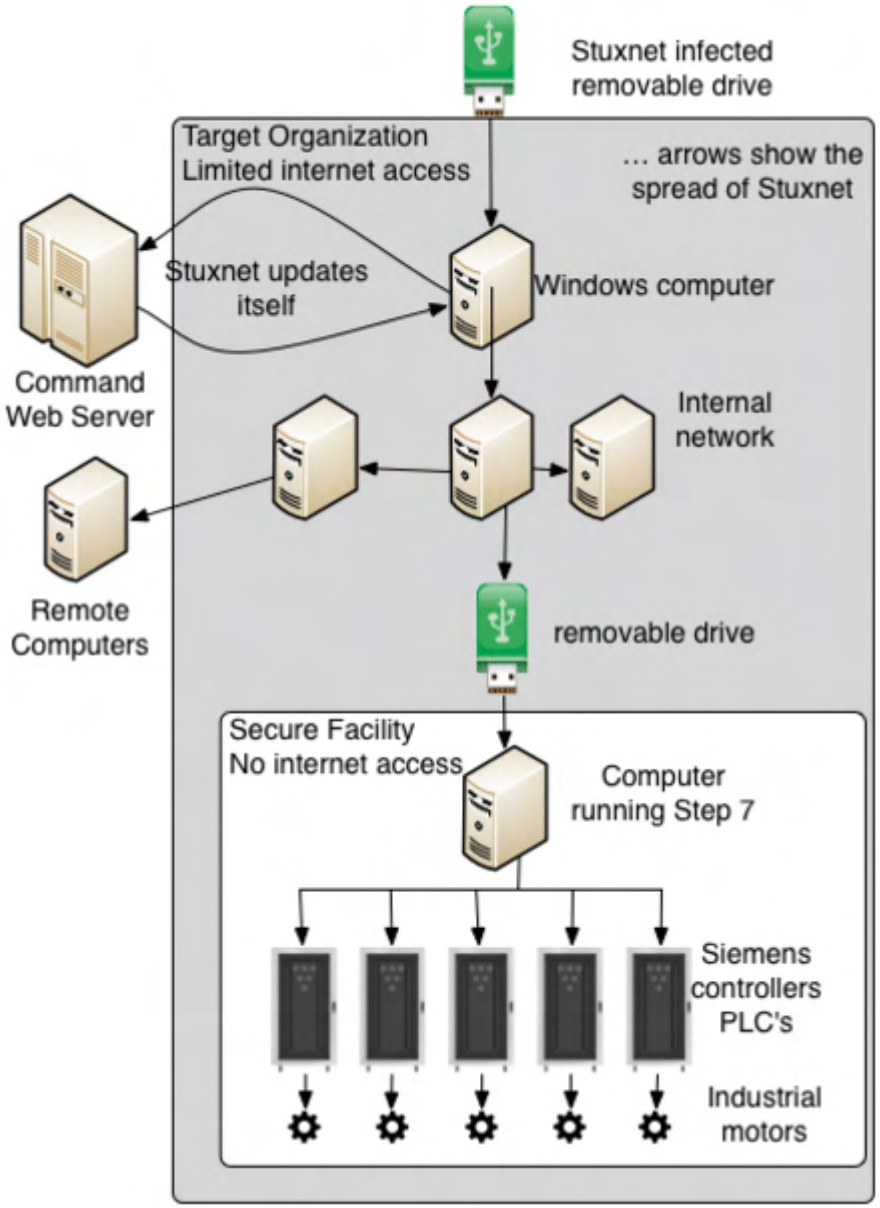
3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet


Stuxnet infected
removable drive
Target Organization
Limited internet access
… arrows show the
spread of Stuxnet
Stuxnet updates
itself
Windows computer
Command
Web Server
Internal
network
Remote
Computers
removable drive
Secure Facility
No internet access
Computer
running Step 7
Siemens
controllers
PLC's
Industrial
motors

Stuxnet

https://www.youtube.com/watch?v=nEsNnwZpXrk

https://www.youtube.com/watch?v=LqDqD1tpl_E

OPTIONAL:

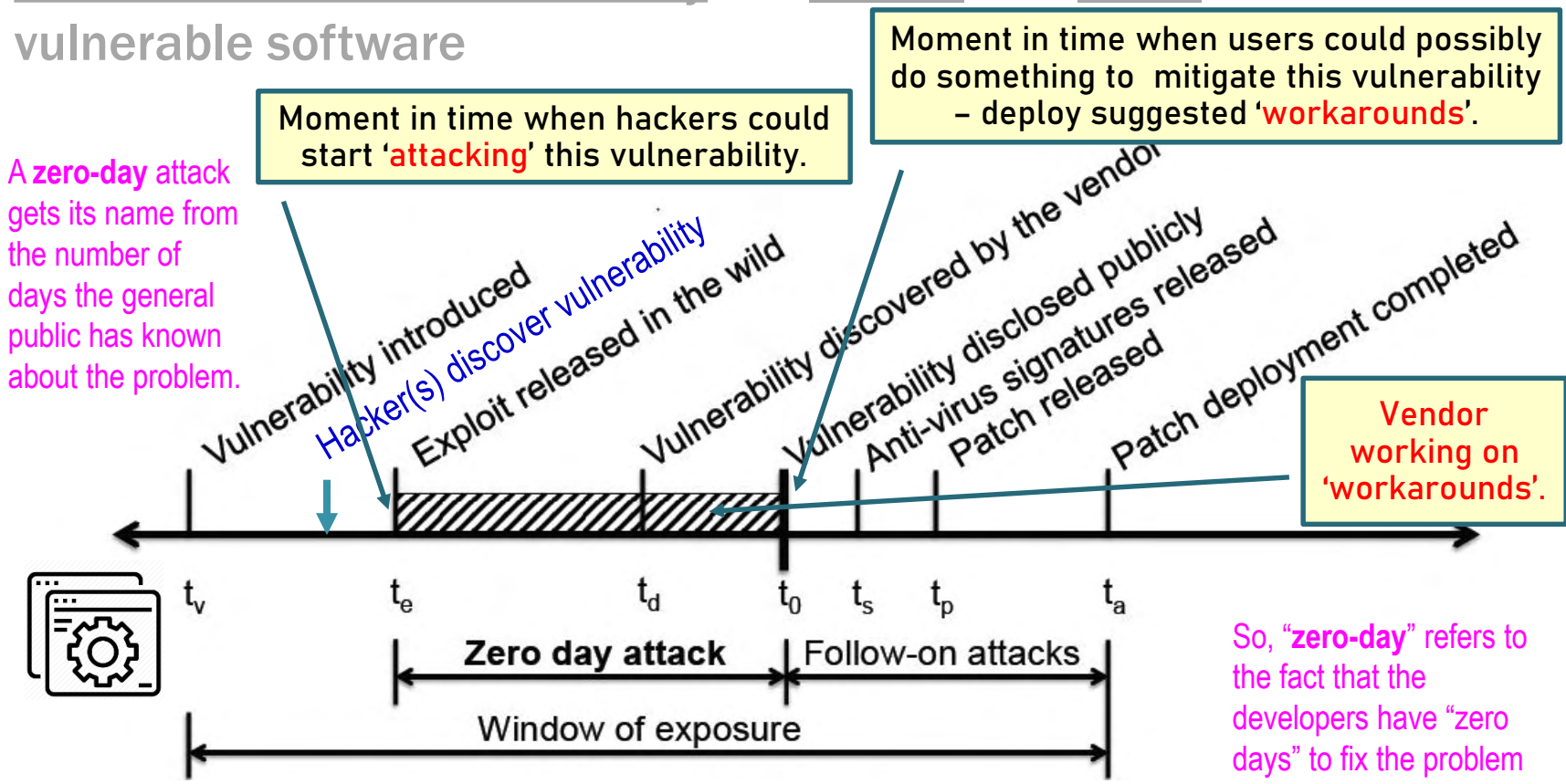
https://www.youtube.com/watch?v=oz585G-6NBA

https://www.youtube.com/watch?v=SAy46DhWW8Y

Threat Events: Software Attacks (cont.)

Zero-Day Vulnerability – a computer-software vulnerability NOT known to or addressed by the vendor and users of the vulnerable software

A **zero-day** attack gets its name from the number of days the general public has known about the problem.



http://users.ece.cmu.edu/~tdumitra/public_documents/bilge12_zero_day.pdf

http://securityaffairs.co/wordpress/9566/hacking/wrong-response-to-zero-day-attacks-exposes-to-serious-risks.html

So, "**zero-day**" refers to the fact that the developers have "zero days" to fix the problem that has just been exposed — and perhaps already exploited by hackers.

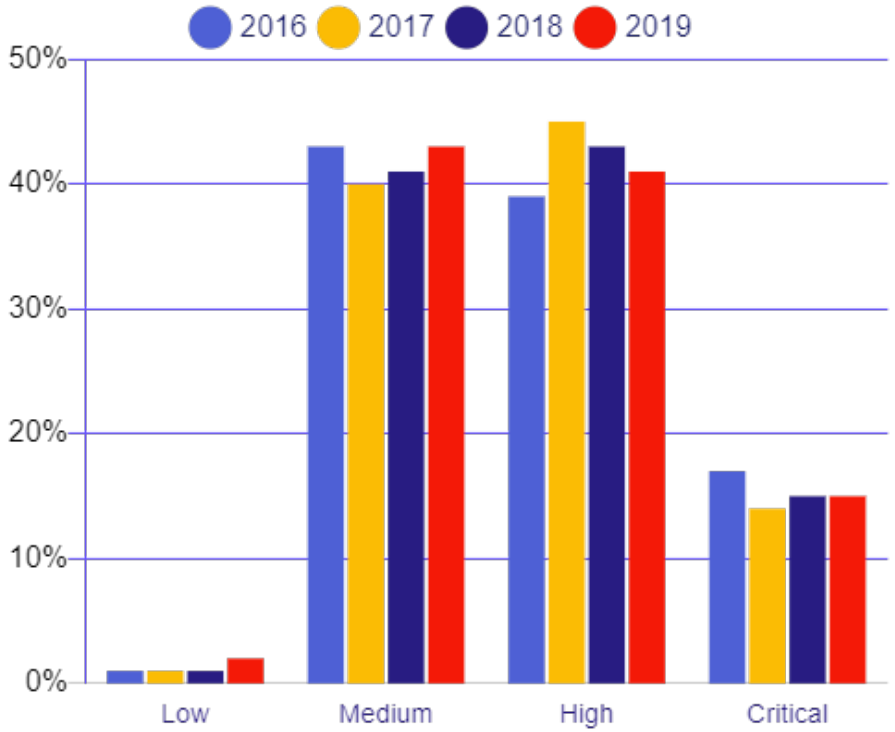
Threat Events: Software Attacks (cont.)

Common Vulnerability Exposure (CVE) – program launched in 1999 by MITRE to identify and catalog vulnerabilities in software and firmware

- MITRE – US non-profit funded by Cybersecurity and Infrastructure Security Agency, part of the US Department of Homeland Security
- CVE database – list of publicly disclosed computer security flaws
- CVE entry/report – brief description of a reported vulnerability – does not include technical data or information about risk and fixes
- CVE reports can come from anywhere: a vendor, a researcher, a clever user …
- CVSS = CV Scoring System - set of open standards for assigning a number/score to a vulnerability to assess its severity
  [scores range from 0 to 10]

CVSS v2.0 Ratings	
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10.0

CVSS v3.0 Ratings	
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0



https://www.darkreading.com/vulnerabilities---threats/is-cvss-the-right-standard-for-prioritization/a/d-id/1337712

Threat Events: Software Attacks (cont.)

New CVE ID Syntax

The new CVE ID syntax is variable length and includes:

CVE prefix + Year + Arbitrary Digits

Vulnerability Details : CVE-2021-41773

A flaw was found in a change made to path normalization in Apache HTTP Server 2.4.49. An attacker could use a path traversal attack to map URLs to files outside the directories configured by Alias-like directives. If files outside of these directories are not protected by the usual default configuration "require all denied", these requests can succeed. If CGI scripts are also enabled for these aliased pathes, this could allow for remote code execution. This issue is known to be exploited in the wild. This issue only affects Apache 2.4.49 and not earlier versions. The fix in Apache HTTP Server 2.4.50 was found to be incomplete, see CVE-2021-42013.

Publish Date : 2021-10-05 Last Update Date : 2021-10-16

Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

– CVSS Scores & Vulnerability Types

CVSS Score	4.3
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	None (There is no impact to the integrity of the system)
Availability Impact	None (There is no impact to the availability of the system.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code Directory traversal
CWE ID	22

https://www.cvedetails.com/cve/CVE-2021-41773/

https://threatpost.com/microsoft-zero-day-actively-exploited-patch/152018/

Common Vulnerability and Exposure

Microsoft Zero-Day Actively Exploited, Patch Forthcoming

Author:
Tara Seals

January 21, 2020 / 9:58 am

CVE-2020-0674 s a critical flaw for most Internet Explorer versions, allowing remote code execution and complete takeover.

An unpatched remote code-execution vulnerability in Internet Explorer is being actively exploited in the wild, Microsoft has announced. It's working on a patch. In the meantime, workarounds are available.

The bug (CVE-2020-0674) which is listed as critical in severity for IE 11, and moderate for IE 9 and IE 10, exists in the way that the jscript.dll scripting engine handles objects in memory in the browser, according to Microsoft's advisory, issued Friday.

The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user – meaning that an adversary could gain the same user rights as the current user.

While Microsoft is aware of "limited targeted attacks," a patch won't be released until next month's Patch Tuesday, according to the computing giant.

"Our standard policy is to release security updates on Update Tuesday, the second Tuesday of each month. This predictable schedule allows for partner quality assurance and IT planning, which helps maintain the Windows ecosystem as a reliable, secure choice for our customers,

Microsoft Releases Advisory on Zero-Day Vulnerability CVE-2020-0674, Workaround Provided

January 20, 2020

Suggested workaround

While users are waiting for a patch to address CVE-2020-0674, Microsoft has published a workaround that restricts access to Jscript.dll:

For those using 32-bit systems, the following command should be entered at a command prompt as an administrator:

takeown /f %windir%\system32\jscript.dll

cacls %windir%\system32\jscript.dll /E /P everyone:N

On the other hand, those using 64-bit systems should enter the following command via a command prompt as an administrator:

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/microsoft-releases-advisory-on-zero-day-vulnerability-cve-2020-0674-workaround-provided

Home › News › Security › Microsoft's February 2020 Patch Tuesday Fixes 99 Flaws, IE 0day

Microsoft's February 2020 Patch Tuesday Fixes 99 Flaws, IE 0day

By Lawrence Abrams

February 11, 2020 01:39 PM

Fix for Internet Explorer zero-day vulnerability released

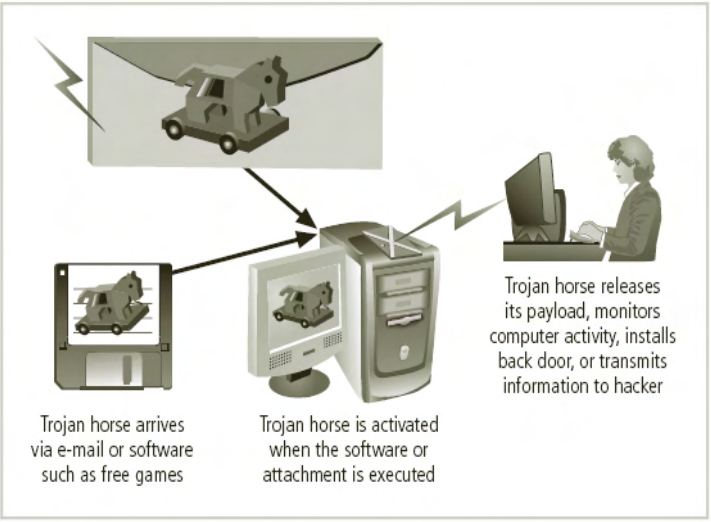
In the middle of January 2020, Microsoft released an advisory about an Internet Explorer zero-day vulnerability (CVE-2020-0674) that was publicly disclosed and being actively exploited by attackers.

With today's Patch Tuesday updates, Microsoft has released a formal security update for the 'CVE-2020-0674 | Scripting Engine Memory Corruption Vulnerability' that fixes the vulnerability without having to use the previously recommended mitigations.

https://www.bleepingcomputer.com/news/security/microsofts-february-2020-patch-tuesday-fixes-99-flaws-ie-0day/

Threat Events: Software Attacks (cont.)

- **TROJAN HORSE** – malware that looks legitimate and is advertised as performing one activity but actually does something else; it does NOT self-replicate
  - example: **AOL4Free** - advertised free access to AOL Internet Service; would delete hard drive
  - common types of Trojans:
    - destructive – designed to destroy data or kill the system – not common today
    - **remote access** – designed to give an attacker control over the victim's system (client-server model)
    - **data sending** – designed to capture and redirect data (keystrokes, passwords, …) to an attacker



Threat Events: Software Attacks (cont.)

- common types of Trojans (cont.)
  - **Denial of Service** – designed to conduct a DoS attack on a predefined IP address
  - **FTP** – designed to set up the infected system to serve as an FTP server for illegal software, pirated movies and music, etc.

Example: 'Legitimate' Trojans

spread through social media (MySpace) – a message contains a link claiming to offer a useful program

FBI Spyware Could Look Like Your Average Trojan

By: Larry Seltzer | April 23, 2009

OPINION: For years the FBI has been using a Trojan horse program to spy on suspects' computers.

> The FBI's bespoke surveillance malware—called Computer and IP Address Verifier (CIPAV)—is designed to track criminal suspects by logging their IP address, MAC address, computer programs running, operating system details, browser details, and other identifying computer information.

https://www.eweek.com/web/index.php/news/fbi-spyware-could-look-like-your-average-trojan

Threat Events: Software Attacks (cont.)

Port	Trojans
1080	MyDoom.B, MyDoom.F, MyDoom.G, MyDoom.H
2283	Dumaru.Y
2535	Beagle.W, Beagle.X, other Beagle/Bagle variants
2745	Beagle.C through Beagle.K
3127	MyDoom.A
3128	MyDoom.B
3410	Backdoor.OptixPro.13 and variants
5554	Sasser through Sasser.C, Sasser.F
8866	Beagle.B
9898	Dabber.A and Dabber.B
10000	Dumaru.Y
10080	MyDoom.B
12345	NetBus
17300	Kuang2
27374	SubSeven
65506	various names: PhatBot, Agobot, Gaobot

Most Trojans do not 'damage' the host computer, but instead use its resources for illegal purposes through a client-server connection.

How can we detect a Trojan?!

- most Trojan 'exfiltrate' or 'infiltrate' data to/from remote machines (over the Internet)
- common techniques of Trojan detection:
  - on the infected computer – run netstat and look for unusual ports and connections
  - from the infected network – scan the network with nmap and look for systems with unusual open ports

Threat Events: Software Attacks (cont.)

- **LOGIC BOMB** – malware typically installed by an authorized user; lies dormant until triggered by a specific logical event; once triggered, it can perform any number of malicious activities
  - trigger events:
    1) a certain date reached on the calendar – check for organization payroll data;
    2) a person was fired – files deleted once his account got disabled

Description	Reason for Attack	Results
A logic bomb was planted in a financial services computer network that caused 1,000 computers to delete critical data.	A disgruntled employee had counted on this causing the company's stock price to drop and he would earn money when the stock dropped.	The logic bomb detonated yet the employee was caught and sentenced to 8 years in prison and ordered to pay $3.1 million in restitution.
A logic bomb at a defense contractor was designed to delete important rocket project data.	The employee's plan was to be hired as a highly paid consultant to fix the problem.	The logic bomb was discovered and disabled before it triggered. The employee was charged with computer tampering and attempted fraud and was fined $5,000.
A logic bomb at a health services firm was set to go off on the employee's birthday.	None was given.	The employee was sentenced to 30 months in a federal prison and paid $81,200 in restitution to the company.

Threat Events: Software Attacks (cont.)

Example: Roger Duronio story – logic bomb

In 2002, disgruntled system administrator for UBS Investment Bank was accused of planting a logic bomb shortly before quitting his job. The bomb had been designed to wipe out 2,000 files on the main servers for UBS, and cripple the company.

His plan was to drive down the company's stock, and eventually profit from that (*put option contract*).

During the downtime caused by the **logic bomb**, brokers could not access the UBS network or make trades. According to one employer: *"Every branch was having problem. Every single broker was complaining. They couldn't log onto their desktops and [get to] their applications because the servers were down. ..."*

In 2006, Duronio was convicted and sentenced to 8 years and 1 month in prison as well as $3.1 million restitution to UBS.

http://www.theregister.co.uk/2006/12/13/ubs_logic_bomber_sentenced/

Threat Events: Software Attacks (cont.)

- **ROOTKIT** – stealthy software with root/administrator privileges – aims to modify the operation of the OS in order to facilitate a nonstandard or unauthorized functions
  - unlike virus, rootkit's goal is not to damage computer directly or to spread, but to hide the presence and/or control the function of other (malicious) software
  - since rootkits change the OS, the only safe and foolproof way to handle a rootkit infection is to reformat the hard drive and reinstall the OS

Example: Sony story – rootkit

In 2005, Sony included a rootkit program Extended Copy Protection (**XCP**) on many of its music CDs in an attempt to limit the user's ability to access the CD and prevent illegal copying.
The software was automatically installed on Windows desktop computers (in a hidden directory + modified the OS) when customers tried to play the CD.

XCP (Extended Copy Protection) and MediaMax - software for copy protection and digital rights management used by Sony

Problems with XCP Security researchers have shown that the XCP technology was designed to have many of the qualities of a "rootkit." It was written with the intent of concealing its presence and operation from the owner of the computer and once installed it degrades the performance of the machine opens new security vulnerabilities and installs updates through an Internet connection to Sony BMG's servers. The nature of a rootkit makes it extremely difficult to remove often leaving reformatting the computer's hard drive as the only solution. When Sony BMG offered a program to uninstall the dangerous XCP software researchers found that the installer itself opened even more security vulnerabilities in users' machines.

Problems with MediaMax The MediaMax software which is included on over 20 million Sony BMG CDs has different but similarly troubling problems. It installs on the users' computers even if they click "no" on the EULA and does not include a way to uninstall the program. The security issue involves a file folder installed on users' computers by the MediaMax software that could allow malicious third parties who have localized lower-privilege access to gain control over a consumer's computer running the Windows operating system. The software also transmits data about users to SunnComm through an Internet connection whenever purchasers listen to CDs allowing the company to track listening habits -- even though the EULA states that the software will not be used to collect personal information and SunnComm's website says "no information is ever collected about you our your computer."

https://www.eff.org/cases/sony-bmg-litigation-info

Sony settles 'rootkit' class action lawsuit

The record label agrees to offer U.S. customers money and free downloads to encourage them to replace CDs that secretly install software.

In the settlement filing, Sony states that it will immediately recall all XCP CDs and replace them with non-content-protected CDs. It has also agreed to offer incentives to U.S. customers to "ensure that XCP CDs are promptly removed from the market." Sony first released details about its CD recall scheme in late November.

Customers who exchange their XCP CD can either download three albums from a list of over 200 titles, or claim a cash payment of $7.50 and a free download of one album. To claim this compensation, customers must return their XCP CDs to Sony or provide the company with a receipt showing they returned or exchanged the CD at a retailer after Nov. 14.

https://www.cnet.com/news/sony-settles-rootkit-class-action-lawsuit/

Microsoft will wipe Sony's 'rootkit'

Security tools will detect and remove part of the copy protection tools installed on PCs when music CDs are played.

By Joris Evers | November 13, 2005 -- 08:15 GMT (00:15 PST) | Topic: Windows

Microsoft will update its security tools to detect and remove part of the copy protection tools installed on PCs when some music CDs are played.

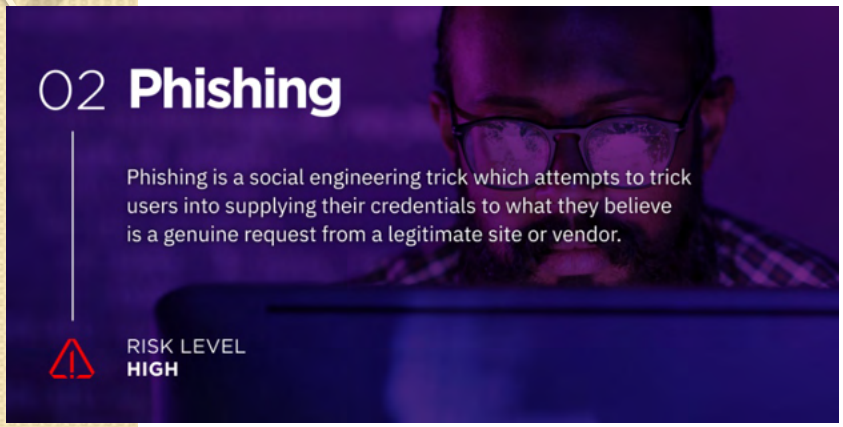
To protect Windows users, Microsoft plans to update Windows AntiSpyware and the Malicious Software Removal Tool as well as the online scanner on Windows Live Safety Center to detect and remove the Sony BMG software, the software maker said in its blog.

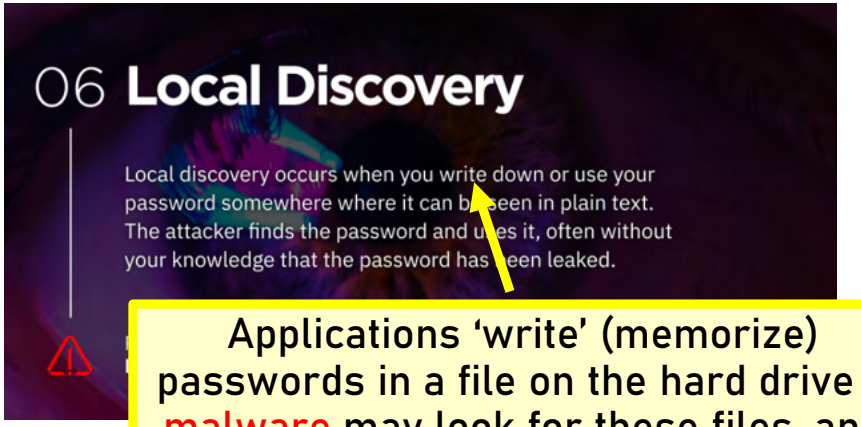
> Windows AntiSpyware is Microsoft's spyware-fighting software that is currently available as a test version and used by millions of people worldwide. Microsoft provides weekly updates for Windows AntiSpyware. The Windows Malicious Software Removal Tool is updated monthly and is part of Microsoft's monthly patch releases.

Detection and removal of the rootkit component will also be in Windows Defender, the forthcoming update to Windows AntiSpyware that will also be part of Windows XP successor Windows Vista, Microsoft said.

https://www.zdnet.com/article/microsoft-will-wipe-sonys-rootkit/

How could Mallory steal Alice's Gmail / Online-Banking password ??





Does phishing involve the use of malware ?

Applications 'write' (memorize) passwords in a file on the hard drive – malware may look for these files, and exfiltrate them.

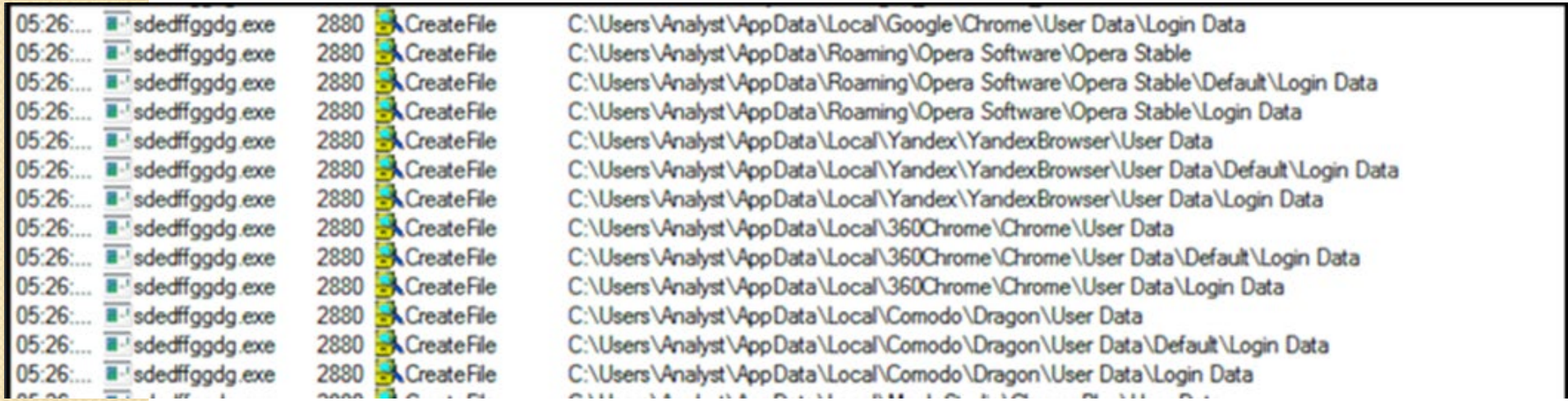
However, most applications nowadays pt stored passwords.

https://www.sentinelone.com/blog/7-ways-hackers-steal-your-passwords/

BluStealer Malware

BluStealer is a new information-stealing malware that contains the functionality to **steal login credentials**, credit card data, cryptocurrency and more. This harvested data is returned to the attacker via SMTP and the Telegram Bot API.

ChromeRecovery begins by scanning the infected machines for any potential login credentials for web browsers, FTP clients and email clients. In the screenshot below, the malware can be seen searching through the directories of various well known web browsers, including Chrome™ and Opera.



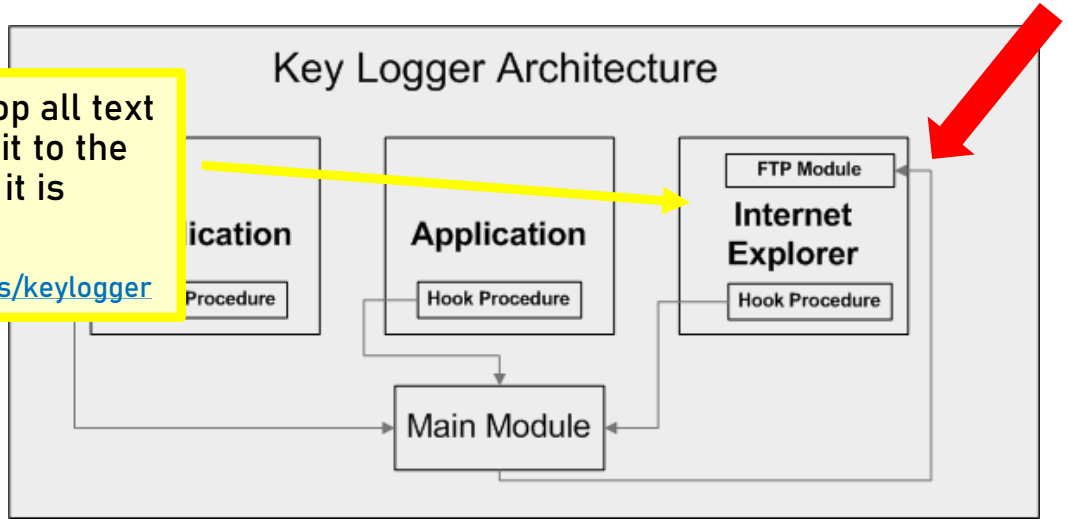
https://blogs.blackberry.com/en/2021/10/threat-thursday-blustealer-infostealer

Threat Events: Software Attacks (cont.)

- **INFORMATION STEALER** – malware that steals information such as: passwords, financial credentials, intellectual property … that resides in volatile memory (i.e., are not stored on the hard drive)
  - subcategories of information stealers, based on their implementation, include:
    1) Software Keylogger – captures keystrokes in a compromised system

"Form grabbing"-based keyloggers eavesdrop all text entered into website forms once you send it to the server. Data is recorded locally before it is transmitted to the hacker …

https://www.kaspersky.com/resource-center/definitions/keylogger



http://www.codeproject.com/Articles/10272/Keyboard-Spy-implementation-and-counter-measures

Threat Events: Software Attacks (cont.)

Example: Hardware Keylogger

Not 'classical' malware – does not require any software or drivers to be installed on the victim machine.

Logger is plugged in between USB keyboard (connector) and USB port. All keyboard activity is logged to its internal memory.

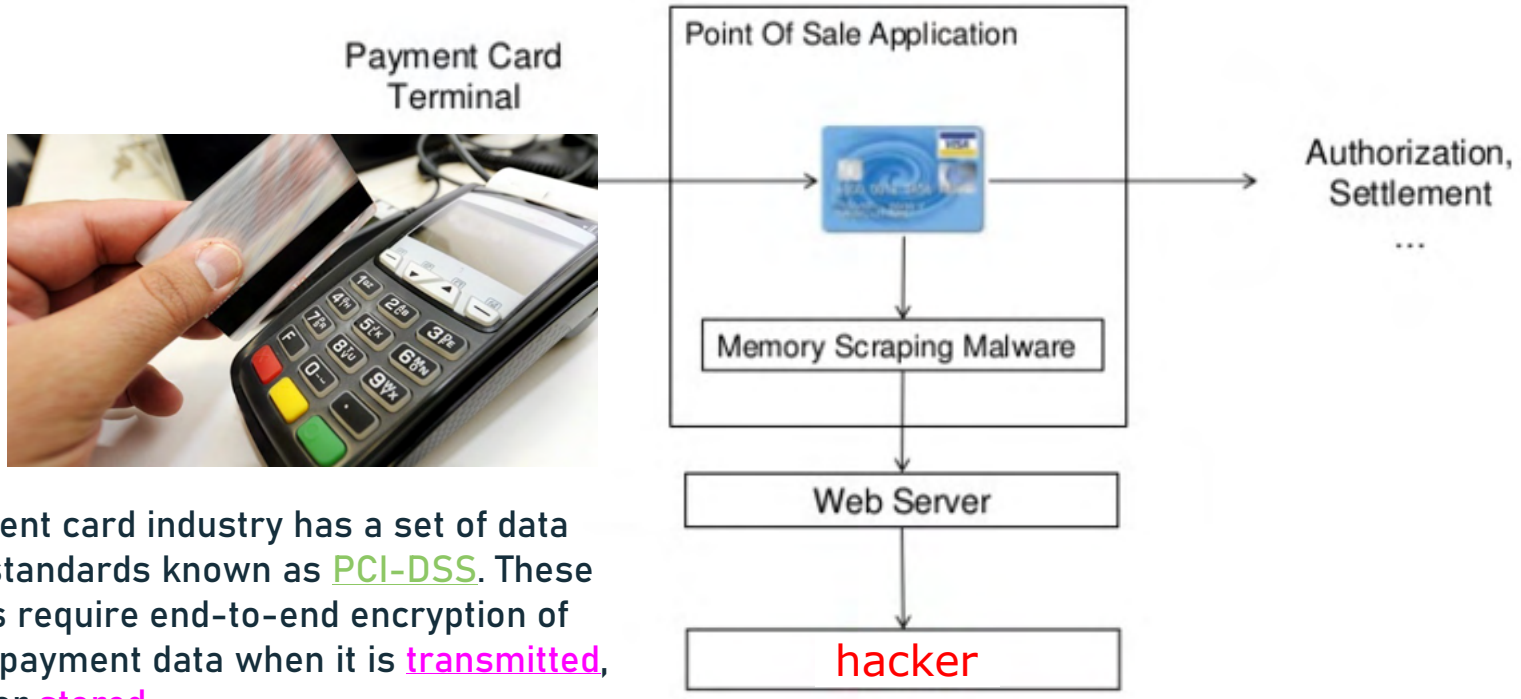
Effective against antivirus protection; no 'physical trace' stays on the victim machine => challenge for forensics analysis!

Threat Events: Software Attacks (cont.)

- **INFORMATION STEALER** – cont.

2) **Memory (RAM) Scraper** – steals data when processed in memory

- best place to steal data - everything is decrypted



The payment card industry has a set of data security standards known as PCI-DSS. These standards require end-to-end encryption of sensitive payment data when it is transmitted, received or stored.

Threat Events: Software Attacks (cont.)

- **INFORMATION – cont.**
  STEALER

3) **Desktop Recorder** – takes screenshots of the desktop (e.g.) when mouse clicked or keyboard pressed

   - disadvantage: amount of that that needs to be stored / transmitted

Threat Events: Software Attacks (cont.)

- **RANSOMWARE** – holds data or access to systems containing data until the victim pays a ransom
  - subcategories of ransomware based on implementation

1) **CryptoLockers** – encrypts victim's data or entire hard-drive get encrypted

2) **ScreenLockers** – user is locked out and denied login to the system

Your computer has been locked due to suspicion of illegal content downloading and distribution.
Mentioned illegal content (414 Mb of video files) was automatically classified as child pornographic materials. Such actions, in whole or in part, violate following U.S. Federal Laws:

18 U.S.C. § 2251- Sexual Exploitation of Children (Production of child pornography)
18 U.S.C. § 2252- Certain activities relating to material involving the sexual exploitation of minors (Possession, distribution and receipt of child pornography)
18 U.S.C. § 2252A- certain activities relating to material constituting or containing child pornography

Any individual who violates, or attempts to violate, or conspires to violate mentioned laws shall be sentenced to a mandatory term of imprisonment from 4 to 30 years and shall be fined up to $250,000.

Technical details:
Involved IP address: [redacted]
Involved host name: [redacted]
Source or intermediary sites: http://pornerbros.com

All suspicious files from your computer were transmitted to a special server and shall be used as evidences. Don't try to corrupt any data or unblock your account in an unauthorized way.

Your case can be classified as occasional/unmotivated, according to title 17 (U. S. Code) § 512. Thus it may be closed without prosecution. Your computer will be unblocked automatically.

In order to resolve the situation in an above-mentioned way you should pay a fine of $300.

HOW TO UNLOCK YOUR COMPUTER:

1 $ Take your cash to one of this retail locations:
Walmart, Kmart, Sears, 7-Eleven, CVS/pharmacy, Walgreens

2 Get a MoneyPak and purchase it with cash at the register
MoneyPak

3 Come back and enter your MoneyPak code to unlock your computer (5 attempts available)

Code: Submit

1	2	3
4	5	6
7	8	9
Delete	0	Enter

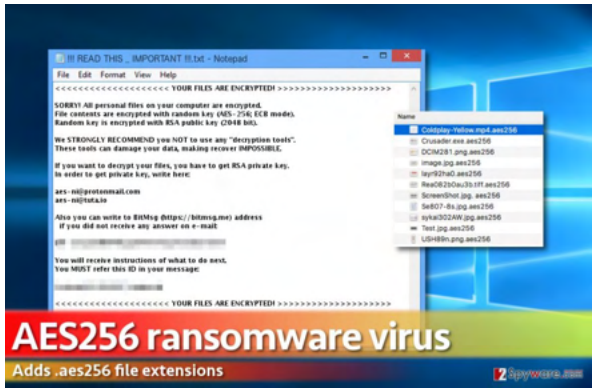
Table 1: Ransomware collection (CryptoLockers)

Family	First seen	Most recent	Encryption algorithm	C&C
Gpcode	2004	2014	AES - ECB	~ HTTP
CryptoLocker	2013	2014	AES	~ HTTP
CryptoWall	2014	2016	AES - CBC	Tor
CTB-Locker	2014	2016	AES - ECB	Tor
TorrentLocker	2014	2016	AES - CTR|CBC *	Tor
TeslaCrypt	2015	2016	AES - ECB|CBC *	Tor
CrypVault	2015	2016	RSA - OAEP	
Locky	2016	-	AES - CTR|ECB *	~ HTTP
Petya	2016	-	Salsa20	No

* Samples variation.

https://www.semanticscholar.org/paper/Ransomware-and-the-Legacy-Crypto-API-Palisse-Bouder/f80a0b39974fa70bc96f7054953629ebb0b8322d

Why TOR ??



Ryuk, Doppelpaymer, Conti, …

Threat Events: Software Attacks (cont.)

- **SCAREWARE** – malicious programs that aim to scare users into installing a program and sometimes even paying for it
  - program is 'supposed' to solve a problem that does not exist!

Threat Events: Software Attacks (cont.)

- **SPYWARE** – software that spies on users by gathering information without their consent, thus violating their privacy
  - example: Zango – transmits detailed information to advertisers about Web sites you visit
  - legal spyware – parental monitoring of Internet usage by children

- **ADWARE** – software that delivers advertising content in a manner that is unexpected and unwanted by the user

Featured Article

A new Android spyware masquerades as a 'system update'

The malware can take complete control of a victim's device

scareware

Zack Whittaker @zackwhittaker / 10:00 AM EDT • March 26, 2021

Comment

The malware was found bundled in an app called "System Update" that had to be installed outside of Google Play, the app store for Android devices. Once installed by the user, the app hides and stealthily exfiltrates data from the victim's device to the operator's servers.

classical malware

spyware

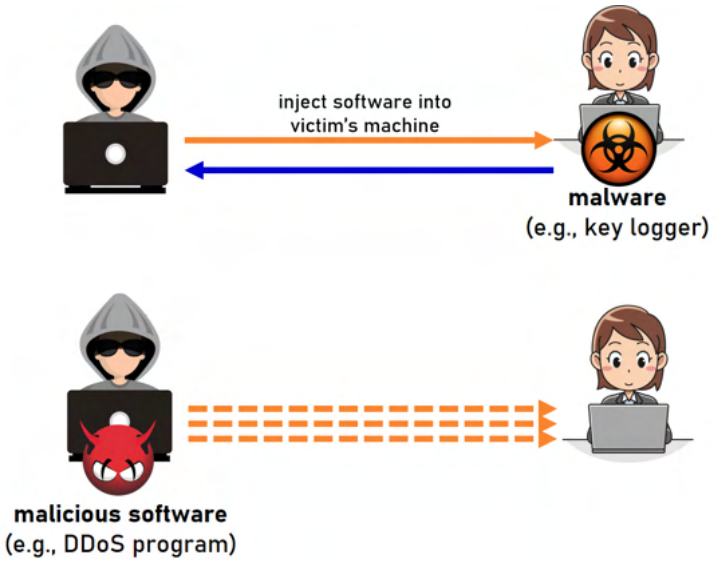
information stealer

The spyware can steal messages, contacts, device details, browser bookmarks and search history, record calls and ambient sound from the microphone, and take photos using the phone's cameras. The malware also tracks the victim's location, searches for document files and grabs copied data from the device's clipboard.

https://techcrunch.com/2021/03/26/android-malware-system-update/

- **Deliberate Software Attacks**
  - a deliberate action aimed to violate / compromise a system's security through the use of specialized software
  - types of attacks base on the type of malicious software:

1. a) Use of Malware
2. b) Password Cracking
   c) DoS and DDoS
   d) Spoofing
   e) Sniffing
   f) Man-in-the-Middle
   g) Phishing
   h) Pharming



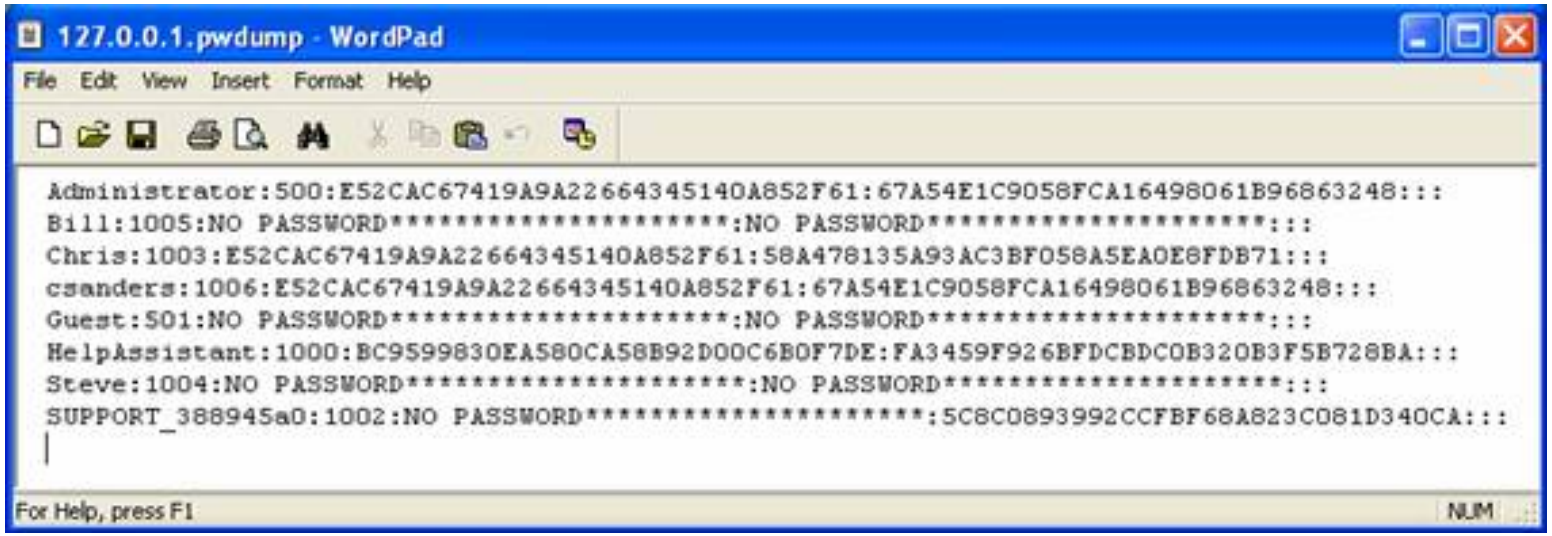
Threat Events: Software Attacks (cont.)

b) Password Cracking

1. Cain & Abel
2. John the Ripper
3. Medusa
4. OphCrack …

- can be 'on-line' and 'off-line'
- off-line crackers attempt to reverse-calculate a password
- requires that a copy of Security Account Manager (SAM) - a registry data file - be obtained
  - SAM file (c:\windows\system32\config\SAM) contains the hashed representation of the user's password – LM or NTLM hash algorithms are used
  - cracking procedure: hash any random password using the same algorithm, and then compare to the SAM file's entries
  - SAM file is locked when Windows is running: cannot be opened, copied or removed (unless pwdump is run by the administrator)
  - off-line copy of SAM's content can be obtained (e.g.) by booting the machine on an alternate OS such as NTFSDOS or Linux

Threat Events: Software Attacks (cont.)



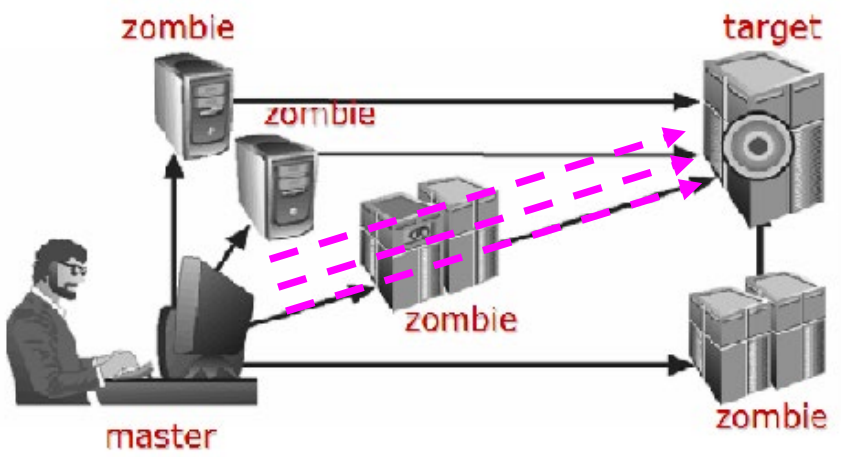
- types of password cracking attacks
  - **brute force** – every possible combination/password is tried
  - **dictionary** – a list of commonly used passwords (the dictionary) is used
  - **guessing** – the attacker uses his/her knowledge of the user's personal information and tries to guess the password

Threat Events: Software Attacks (cont.)

c) Denial of Service (DoS)

- attacker sends a large number of requests to a target
  - target gets overloaded and cannot respond to legitimate requests
- distributed DoS = DDoS - a coordinated stream of requests is launched from many locations (zombies) simultaneously
  - **zombie/bot** – a compromised machine that can be commanded remotely by the **master** machine
  - **botnet** – network of bots + master machine

1. Scapy
2. LOIC, …



overwhelm the bandwidth or CPU

Threat Events: Software Attacks (cont.)

- DDoS 'as a service'

"Given the ready availability of DDoS-as-a-service offerings and the increasing affordability of such services, organizations of all sizes and industries are at a greater risk than ever of falling victim to a DDoS attack that can cripple network availability and productivity."

Service Name	Service Pricing (USD)
Xakepy.cc	1 hour starts at $5 24 hours starts at $30 1 week starts at $200 1 month starts at $800
World DDoS Service	1 day starts at $50 1 week starts at $300 1 month starts at $1,200
King's DDoS Service	1 hour starts at $5 12 hours starts at $25 24 hours starts at $50 1 week starts at $500 1 month starts at $1,500
MAD DDoS Service	1 night starts at $35 1 week starts at $180 1 month starts at $500
Gwapo's Professional DDoS Service	1-4 hours at $2 per hour 5-24 hours at $4 per hour 24-72 hours at $5 per hour 1 month at $1,000 fixed
PsyCho DDoS Service	1 hour for $6 1 night for $60 1 week for $380 1 month for $900
DDoS Service 911	1 night for $50
Blaiz DDoS Service	1 day for $70 1 week starts at $450
Critical DDoS Service	1 day starts at $50 1 week starts at $300 1 month starts at $900
No. 1* DDoS_SERVICE	1 day starts at $50 1 week starts at $300 1 month starts at $1,000

http://securityaffairs.co/wordpress/33916/cyber-crime/verisign-ddos-attacks-as-a-service.html

Threat Events: Software Attacks (cont.)

Example: Mafiaboy story - DDoS

In 2000, a number of major firms were subjected to devastatingly effective distributed denial-of-service (DDoS) attack that blocked each of their e-commerce systems for hours at a time. Victims of this series of attacks included: CNN.com, eBay, Yahoo.com, Amazon.com, Dell.com, ZDNet, and other firms.

The Yankee Group estimated that these attacks cost $1.2 billion in 48 hours:
$100 million from lost revenue
$100 million from the need to create tighter security
$1 billion in combined market capitalization loss.

At first, the attack was thought to be the work of an elite hacker, but it turned to be orchestrated by a 15-year-old hacker in Canada.

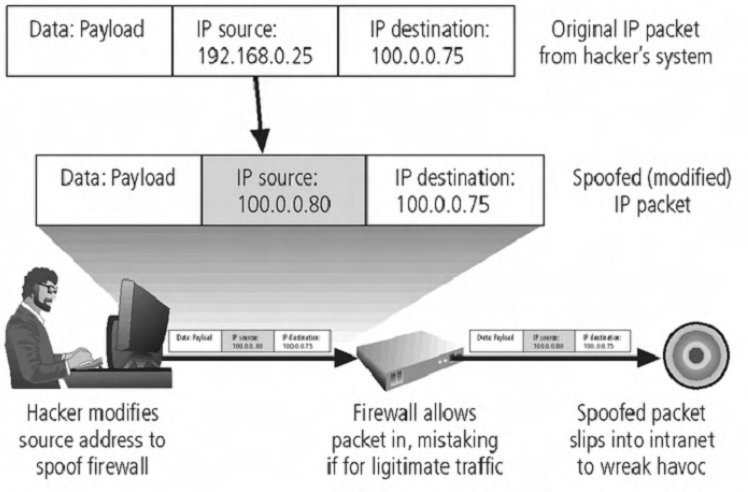
He was sentenced to eight months detention plus one year probation and $250 fine.

http://journal.fibreculture.org/issue9/issue9_genosko.html

Threat Events: Software Attacks (cont.)

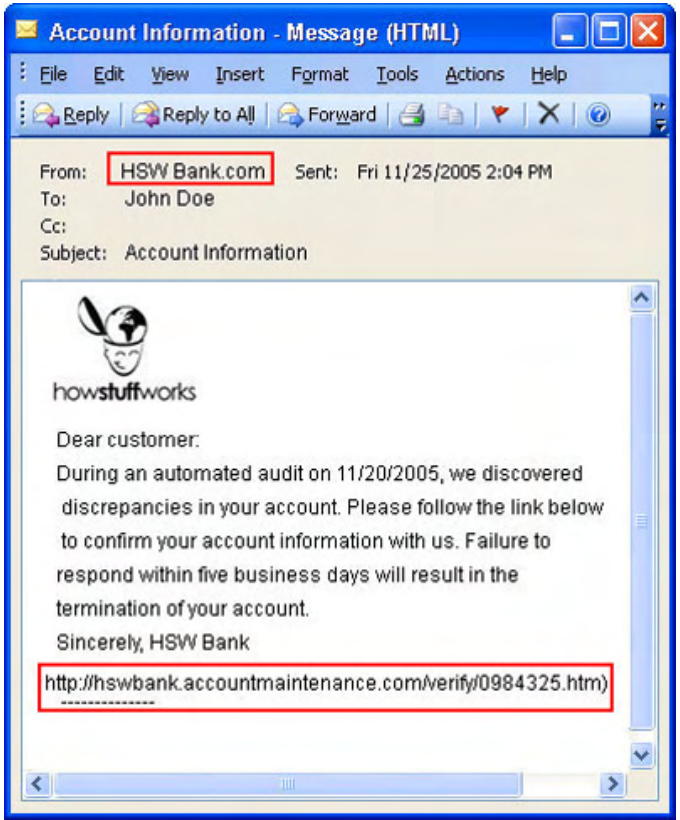
d) Spoofing

- insertion of forged Internet identification data in order to gain an illegitimate advantage (in packets, web-requests, emails)
- types of spoofing
  - IP Spoofing – creation of IP packets with a forged source IP address, e.g. for the purpose of 'passing through a firewall'



Threat Events: Software Attacks (cont.)

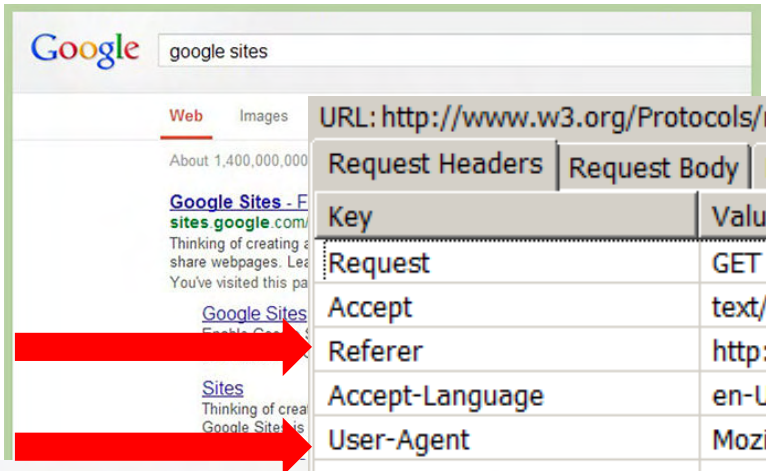
- types of spoofing (cont.)
  - **Email Address Spoofing** – creation of email messages with a forged sender address, e.g. for the purposes of social engineering and data phishing

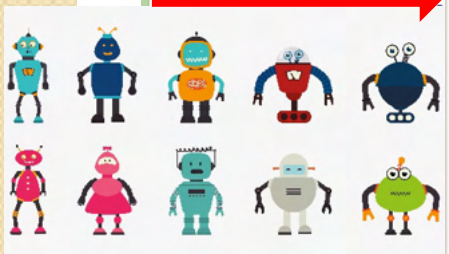


Threat Events: Software Attacks (cont.)

- types of spoofing (cont.)
  - **Referrer or User Agent Spoofing** – creation of HTTP requests with forged fields in order to gain access to a protected web-site

    * some sites allow access to their material only from certain approved (login) pages and/or only to humans





URL: http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html

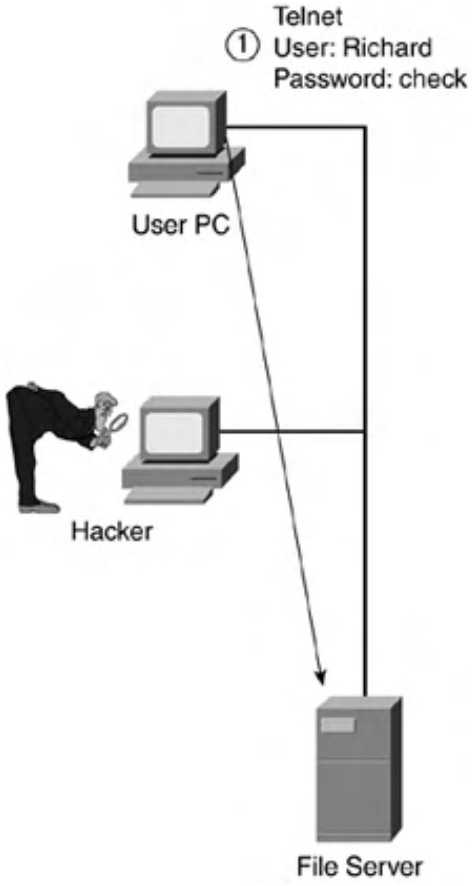
Request Headers	Request Body	Response Headers	Response Body	Cookies	Initiator	Timings

Key	Value
Request	GET /Protocols/rfc2616/rfc2616-sec14.html HTTP/1.1
Accept	text/html, application/xhtml+xml, */*
Referer	http://www.google.com/url?sa=t&source=web&cd=3&ved=0CC4QFjAC8
Accept-Language	en-US
User-Agent	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5
Accept-Encoding	gzip, deflate
Host	www.w3.org
If-Modified-Since	Wed, 01 Sep 2004 13:24:52 GMT
If-None-Match	"1edec-3e3073913b100"
Connection	Keep-Alive

Threat Events: Software Attacks (cont.)

e) Sniffing

- use of a program or device that can monitor data traveling over a network
  - unauthorized sniffers can be very dangerous – they cannot be detected, yet they can sniff/extract critical information from the packets traveling over the network
  - wireless sniffing is particularly simple, due to the 'open' nature of the wireless medium
  - popular sniffers:
    Wireshark – wired medium
    Cain & Abel – wireless medium
    Kismet – wireless medium

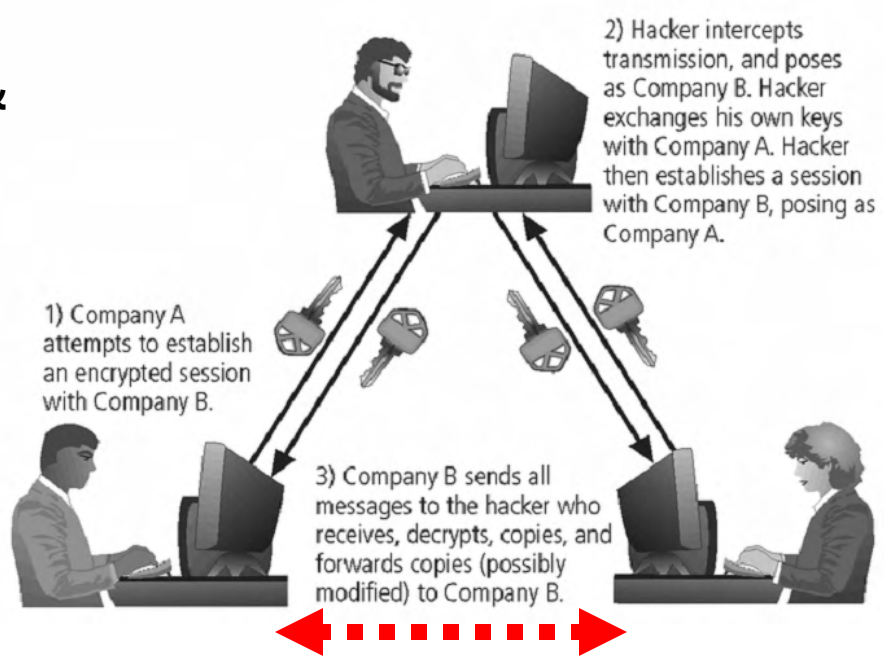


Threat Events: Software Attacks (cont.)

f) Man-in-the-Middle Attacks

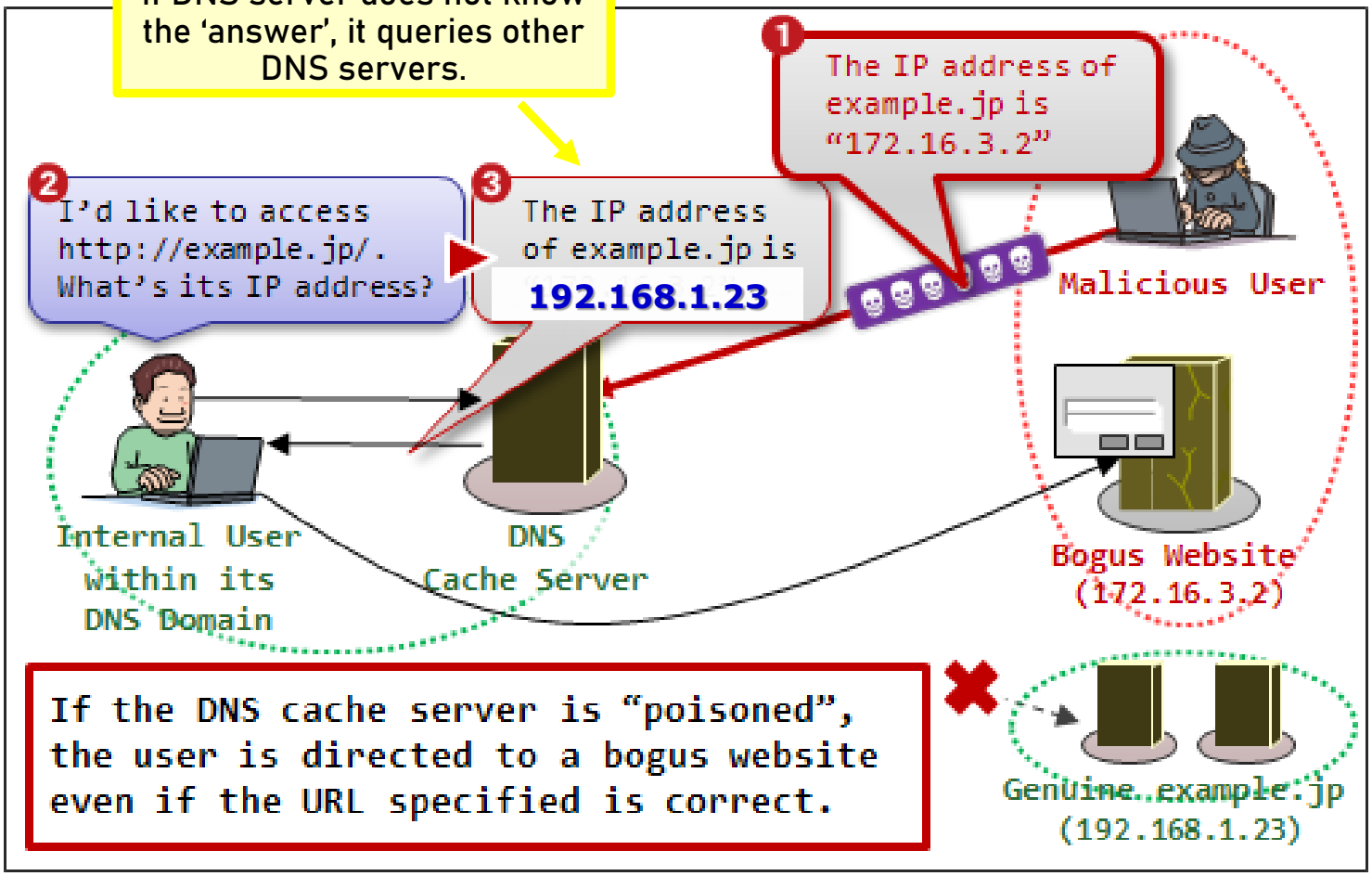
- gives an illusion that two computers are communicating with each other, when actually they are sending and receiving data with a computer between them
  - spoofing and/or sniffing can be involved

- examples:
  - passive – attacker records & resends data at a later time (acts as a signal/packet repeater)
  - active – attacker intercepts, alters and sends data before or after the original arrives to the recipient



Threat Events: Software Attacks (cont.)

Example: DNS Poisoning (active Man-in-the-Middle attack)



http://hackingplayground.blogspot.ca/2012/01/hacking-facebookgmailhotmail-using-set.html

Threat Events: Software Attacks (cont.)

Social Engineering

- process of using social skills to manipulate people into revealing vulnerable information
  - either by believing that an email came from a legitimate person or believing that a web-site is the real web-site, or both!

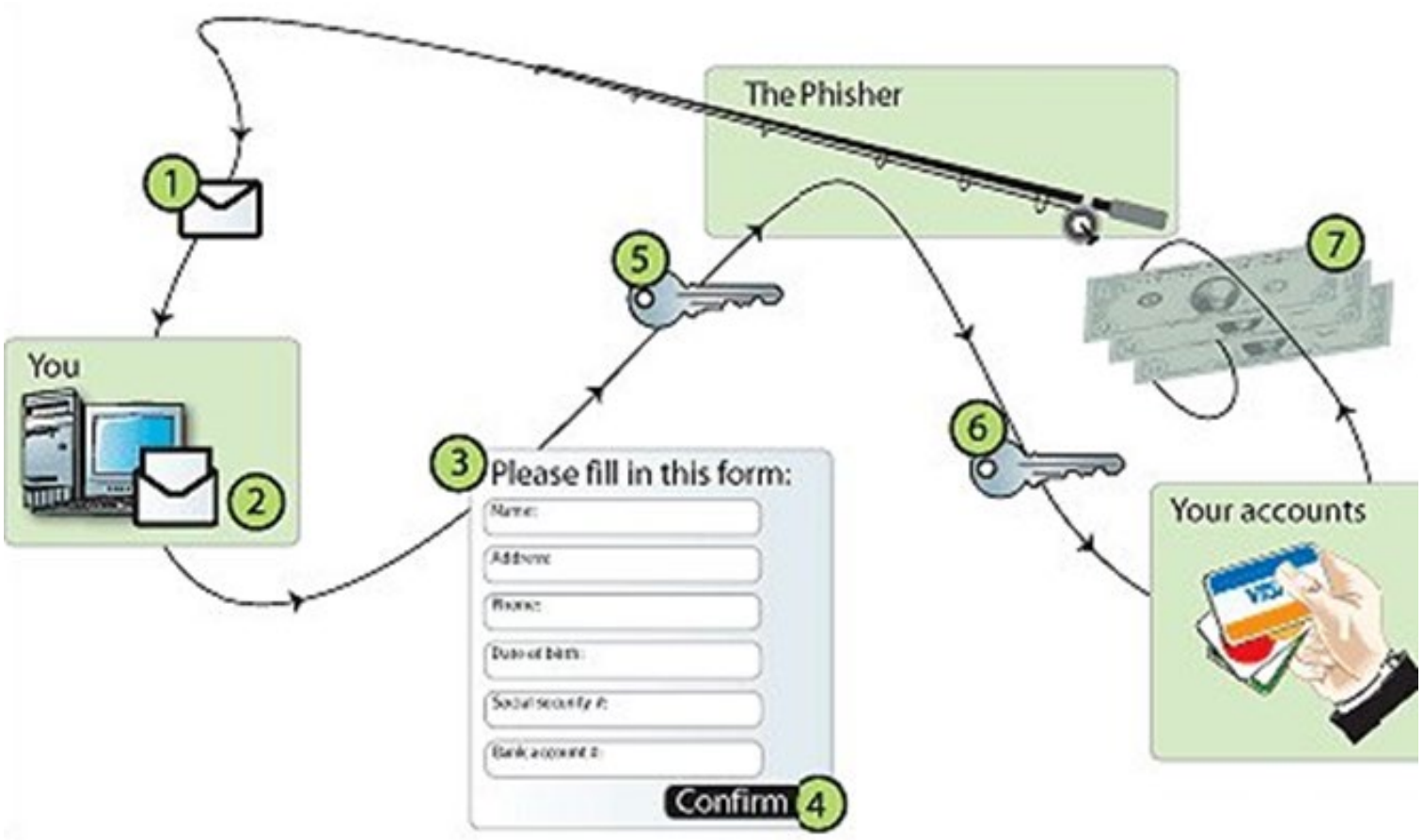
g) Phishing – involves fake/spoofed emails + …

- attempt to gain sensitive personal information by posing as a legitimate entity
  - SIMPLE PHISHING: an email is sent to the victim informing them of a problem (e.g. with their email or banking account) and asking them to provide their username, password, etc.;

    'From' email address is spoofed to look legitimate, 'Reply To' email address is an account controlled by the attacker

Threat Events: Software Attacks (cont.)

Example: Simple Phishing

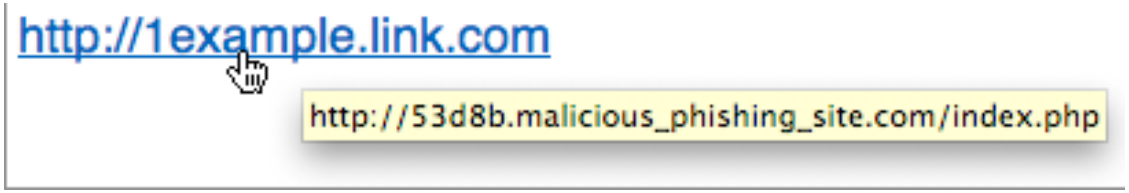


http://www.itknowingness.com/page/2/

Threat Events: Software Attacks (cont.)

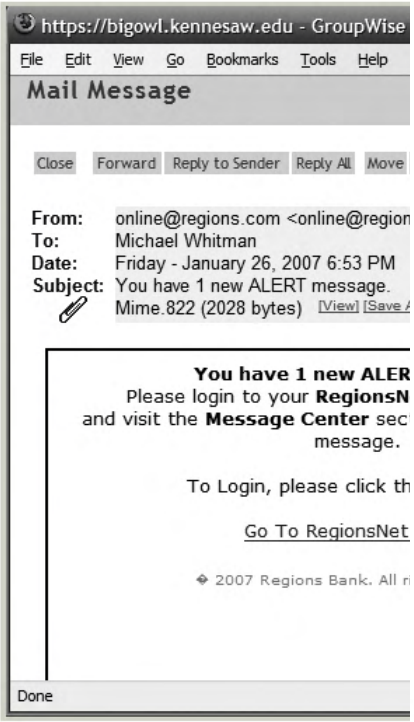
- **SOPHISTICATED PHISHING**: an email is sent to the victim containing a link to a bogus website that looks legitimate

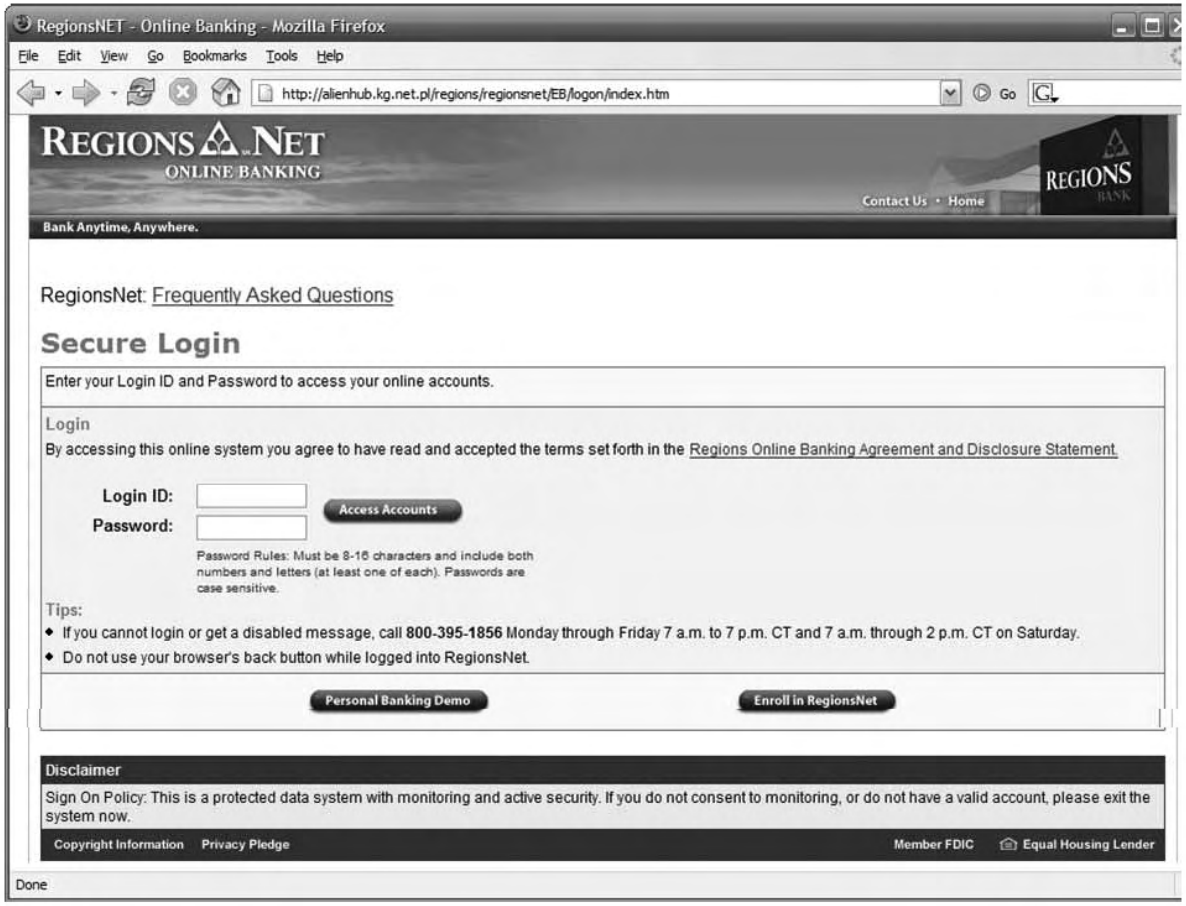
Example: Phishing using URL Links Embedded in HTML-based Emails



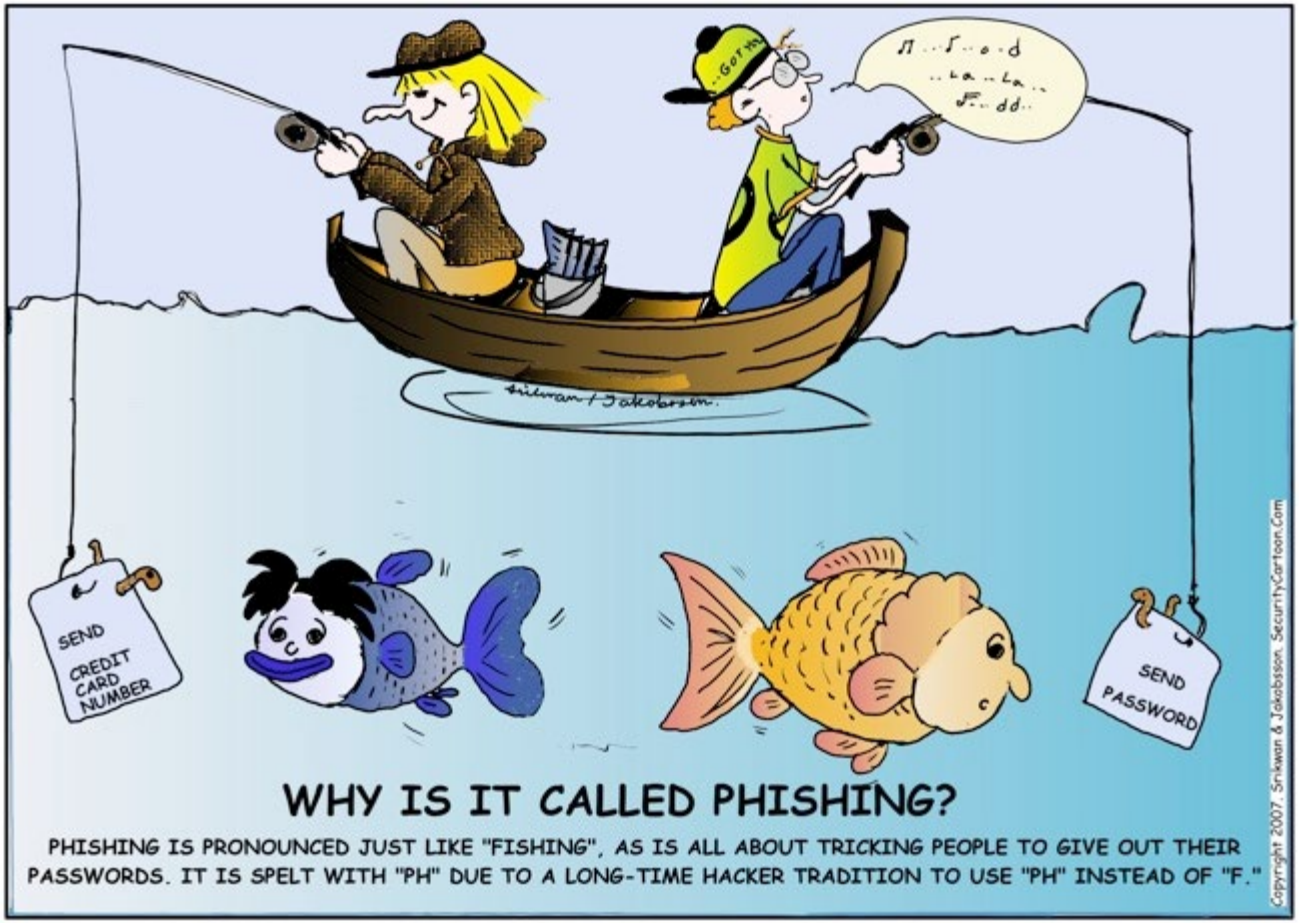
Threat Events: Software Attacks (cont.)

Example: Phishing using URL Links Embedded in HTML-based Emails (cont.)





Threat Events: Software Attacks (cont.)

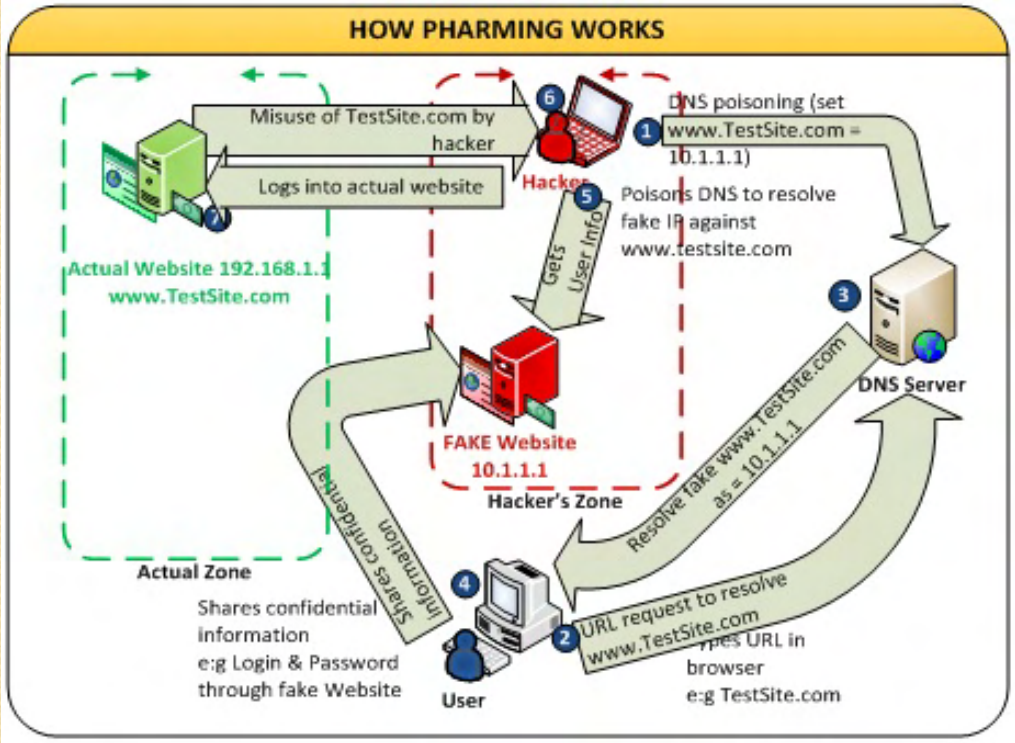


http://www.informacija.rs/Clanci/Phishing-Obmanjivanje-korisnika.html

Threat Events: Software Attacks (cont.)

i) Pharming – involves a fake Web-site (remember Lab 1)

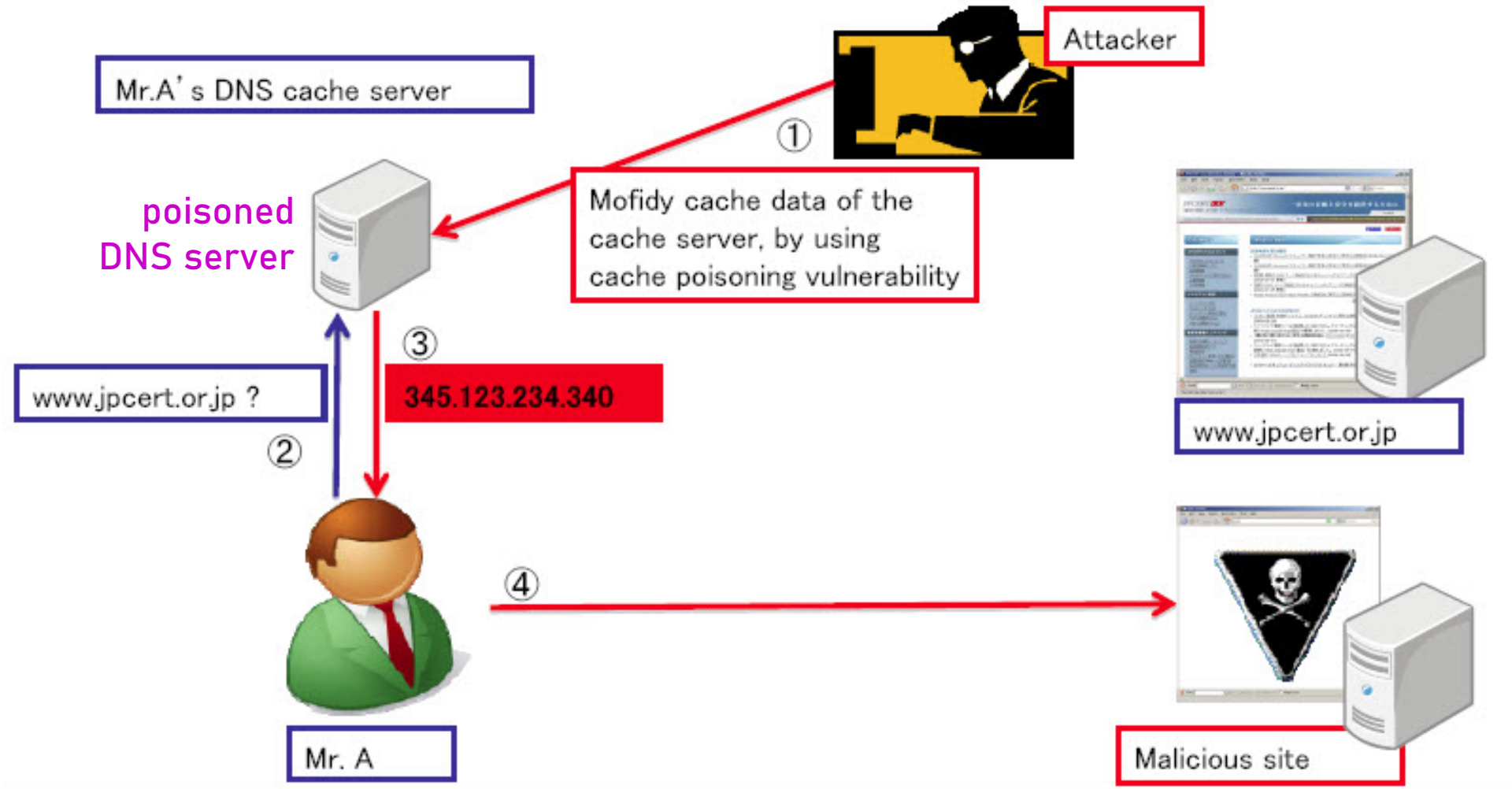
- phishing is accomplished by getting users to type in or click on a bogus URL
- pharming redirects users to false website without them even knowing it – typed in or clicked on URL looks OK



- performed through DNS poisoning – user's local DNS Cache or DNS server are 'poisoned' by a virus

http://www.itmatrix.com/FraudManagement/AntiPharming.html

Overview of DNS cache poisoning vulnerability
What is DNS cache poisoning



Copyright© 2008 JPCERT/CC All rights reserved.

Threat Events: Software Attacks (cont.)

- **Biggest Challenge of Information Security** – How much security?!

Information security should balance protection & access - a completely secure information system would not allow anyone access!

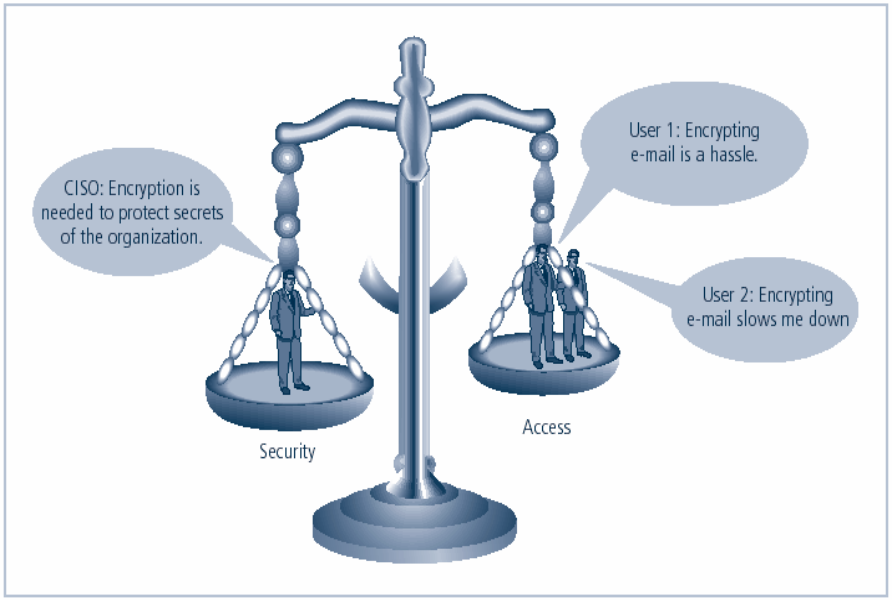


FIGURE 1-7 Balancing Information Security and Access