Intelligent Security Systems

Chapter 1

Computer security with artificial intelligence, machine learning and data science combination:

What? How? Why? and Why now and together?

Abstract

The chapter discusses the basic concepts of computer security as well as the taxonomy and classification of the fundamental algorithms in the domains of artificial intelligence, machine learning and data science in relation to their applications in computer security.

It reviews the sources of security threats and the attacks, using the area of IoT and wireless devices as an example, as well as examines the possible protection mechanisms and tools.

The module provides a general classification of intelligent approaches and their relationship to various computer security fields. It focuses on an introduction of the major intelligent techniques and technologies in computer security, such as expert systems, fuzzy logic, machine learning, artificial neural networks and genetic algorithms.

While presenting multiple techniques, the text emphasizes their advantage in comparison to each other as well as the obstacles in their further progress. Short algorithm descriptions and code examples are included.

Learning outcomes

Upon completion of this topic, students will be able:

- to understand and use a professional terminology in the field of computer security
- to analyze the reasons of computer security current and future developments
- to understand the importance of the computer security tools and protection mechanisms

Contents

Required Reading

- L.Reznik **Intelligent Security Systems:** How artificial intelligence, machine learning, and data science work for and against computer security. IEEE-Wiley, 2022, **Chapter 1**

Recommended Reading

- Report 'State of the Practice of Intrusion Detection Technologies', 1999 available at https://resources.sei.cmu.edu/asset_files/TechnicalReport/2000_005_001_16796.pdf (accessed March 30, 2018)
- NIST Guide to Intrusion Detection and Prevention Systems, 2006 available at http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf (accessed March 30, 2018)
- SANS glossary of terms used in computer security and intrusion detection available at http://www.sans.org/resources/glossary.php (accessed March 30, 2018)
- Threat predictions report. McAfee Labs, 2016 available at https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2017.pdf (accessed March 30, 2018)

Recommended Reading, part 2

- 2018 Cisco Cybersecurity report, available at https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf (accessed August 30, 2018)
- M-trends 2018 attacks report available at https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf (accessed August 30, 2018)
- State of cybersecurity. An ISACA and RSA Survey available at https://cybersecurity.isaca.org/state-of-cybersecurity (accessed March 30, 2018)
- Key Findings from Symantec's 2017 Internet Security Threat Report at https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf (accessed March 30, 2018)

Part 1:

Current security landscape

Intelligent Security Systems

Chapter 1

Computer security with artificial intelligence, machine learning and data science combination

Why is security important? Why now?

We Have Gone From This ….

Introductory: From the primordial ooze

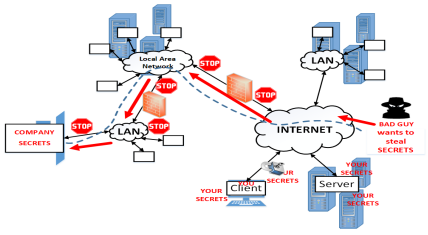
In the beginning, there was no computer security problem. There was no external threat. There was no intrusion problem.

You could ask almost anyone who used or operated computers in those days of yesteryear.

Source: Marvin Schaefer, "If A1 is the Answer, What was the Question?", Annual Computer Security Applications Conference, Tucson, Arizona, December 2004, http://www.acsac.org/2004/papers/ClassicPaperSchafer.pdf

Source: https://image.flaticon.com/icons/svg/469/69734.svg

To this: Think of security as a layered structure



Severity of Cyber Attacks

- US-CERT[1]
  - Activity count beyond a million in 2003
  - 4882 vulnerabilities reported in 2005
    - 79% are launched remotely
    - 62% leads to disruption of service
  - 6604 vulnerabilities reported in 2006
    - 85% are launched remotely
    - 65% leads to disruption of service
- FBI / CSI Survey[2]
  - 80% of 2002 survey respondents indicated financial loss as a result of a computer breach
  - 25% of 2006 survey respondents reported computer intrusions to law enforcement

[1] http://www.us-cert.gov
[2] Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn and Robert Richardson 2006 CSI/FBI Computer Crime and Security Survey, Computer Security Institute, 2006 available online at http://gocsi.com/files/2006.pdf

Big data: new data production-consumption model

New technologies and applications, such as self-driving cars dramatically increase the amount of data produced and consumed as well as the requirements to data quality – see the sensor rotation platform on the car roof

Images taken at CES 2018 @ I.Khokhlov and L.Reznik

Big data: new requirements to data security and privacy protection

New technologies and applications, such as self-driving cars and bikes dramatically increase the data security and privacy protection requirements

Images taken at CES 2018 @ I.Khokhlov and L.Reznik

New fields and opportunities for malicious hacking

New digital devices, such as locks, sensors, kitchen appliances, connected to internet, replace mechanical parts and can open up new fields and opportunities for hacking attacks

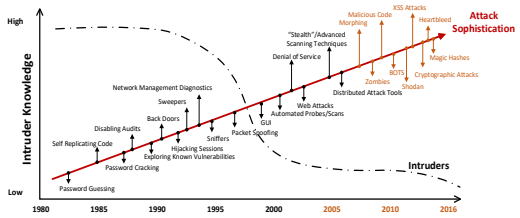
Images taken at CES 2018 @ I.Khokhlov and L.Reznik

Novel protection and intrusion detection for new living environment

Robots, drones, self-driving cars and other digital systems require novel protection and malware detection

Images taken at CES 2018 @ I.Khokhlov and L.Reznik

Is it difficult to intrude?



Attack sophistication vs. Intruder knowledge – courtesy of @L.Reznik and I.Khokhlov. Modified from source: https://www.eleceng.adelaide.edu.au/students/wiki/projects/images/c/cd/Fig2.png.

Severity of Cyber Attacks

- DECEMBER 2006 **NASA was forced to block emails with attachments** before shuttle launches out of fear they would be hacked.
- APRIL 2007 Estonian government networks were harassed by a denial of service attack by unknown foreign intruders, following the country's spat with Russia over the removal of a war memorial. Some government online services were temporarily disrupted and online banking was halted.
- JUNE 2007 The US Secretary of Defense's unclassified email account was hacked by unknown foreign intruders as part of a larger series of attacks to access and exploit the Pentagon's networks

Source: https://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm

Severity of Cyber Attacks

- OCTOBER 2007 China's Ministry of State Security said that foreign hackers, which it claimed 42% came from Taiwan and 25% from the US, had been stealing information from Chinese key areas. In 2006, when the China Aerospace Science & Industry Corporation (CASIC) intranet network was surveyed, spywares were found in the computers of classified departments and corporate leaders.
- SUMMER 2008 The **databases of both Republican and Democratic presidential campaigns were hacked** and downloaded by unknown foreign intruders.
- JULY 2011 In a speech unveiling the Department of Defense's cyber strategy, the US Deputy Secretary of Defense mentioned that a defense contractor was hacked and 24,000 files from the Department of Defense were stolen.

Source: https://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm

Severity of Cyber Attacks (2012-2014)

- Sony Hackers orchestrated multiple breaches of Sony's PlayStation Network knocking it offline for 24 days and costing the company an estimated $171 million.
- Egyptian Government Websites Responding to Hosni Mubarak's decision to block social media sites within the country, on January 27 Anonymous hacked or slowed down sites affiliated with the Egyptian Ministry of Information and the Interior Ministry.
- Google became the target of a phishing campaign originating in Jinan, China, and aimed at gaining access to the accounts of senior officials in the U.S., Korea and other governments, as well as those of Chinese activists. The attack worked by sending the victims spoofed emails, often from accounts that appeared to belong to coworkers, family or friends. Those emails contained links to the spoofed Gmail sites, which harvested the usernames and passwords of anyone fooled by their realistic appearance.

Source: https://www.forbes.com/pictures/mhl45hdje/sony-4/#2068dab54fe1

Privacy violations: Who is spying on you?

- In July 2014 Russian crime ring CyberVog made cybersecurity history by amassing the largest known collection of stolen Internet credentials, including 1.2 billion user name and password combinations and more than 500 million email addresses.
- In 2013 Target theft netted credit and debit card information from 40 million customers and personal information, including email addresses and phone numbers, from up to an additional 70 million customers.

Source: https://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html

Privacy violations: Who is spying on you?

- In 2013 Ed Snowden copied and leaked classified information from NSA without prior authorization. His disclosures revealed numerous global surveillance programs, many run by the NSA and the Five Eyes Intelligence Alliance with the cooperation of telecommunication companies and European governments.
- Who else? Your insurance company? Your boss?

Source: https://blogs.worldbank.org/publicsphere/quote-week-edward-snowden

Severity of Cyber Attacks (2017)

Massive Equifax Breach

By now we're all probably very aware of the massive Equifax hack that exposed 143 million Americans social security numbers, birth dates, addresses and drivers' licenses. There was also a small subset of credit cards and personal identifying documents released with limited personal information to an uncertain amount of Canadian and UK citizens being accessed as well.

According to a statement released by Equifax the breach occurred from mid-May through July 2017. They discovered the breach on July 29th, which means attackers were actively working well over a month, if not more, at exhilarating this treasure trove of data. Equifax also stated that criminals exploited a vulnerability in their web application to gain access to sensitive data as the means of compromising their site.

Source: https://www.ccsinet.com/blog/equifax-breach-what-now/ (accessed March 30, 2018)

Severity of Cyber Attacks (2017)

Massive Equifax Breach -2

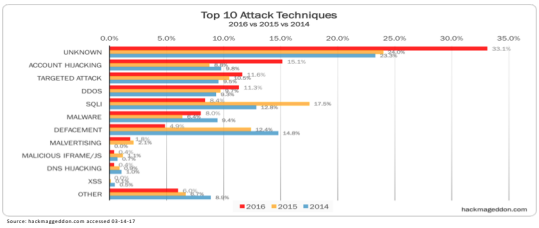
News roundup: Does the blame lie with Equifax or Apache?
Posted by Dan Swinhoe
on September 15 2017

Apache vs. Equifax

Was Apache at fault for the recent Equifax hack? Equifax was quick to place the blame on a vulnerability within Apache Struts – a framework for developing Java EE web applications. The Apache Foundation quickly rebutted this claim.
Turns out that it was a Struts vulnerability that allowed hackers in, but one that was already disclosed and saw a patch issued in March. So the blame still lies at Equifax's door for failure to plug a gaping hole months ago.
Also, the password on Equifax's Argentina employee portal was 'Admin'.

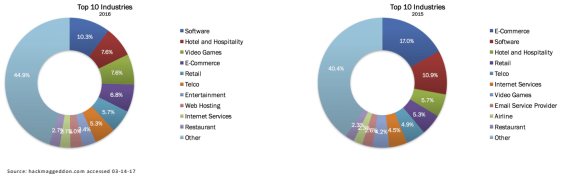
Source: http://www.idgconnect.com/blog-abstract/27958/news-roundup-does-blame-lie-equifax-apache (accessed March 30, 2018)

Attacks techniques



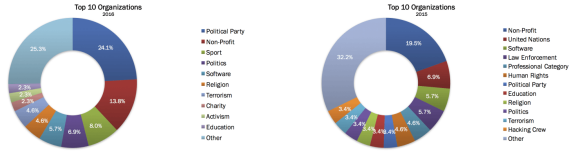
Source: hackmageddon.com accessed 03-14-17

Attacks: target industries



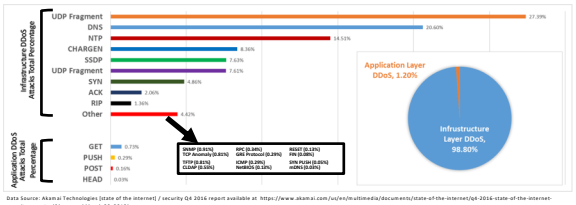
Source: hackmaggeddon.com accessed 03-16-17

Attacks: target organizations



Source: hackmaggeddon.com accessed 03-16-17

DDoS Attack Vector Frequency, Q4 2016



Data Source: Akamai Technologies [state of the internet] / security Q4 2016 report available at https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2016-state-of-the-internet-security-report.pdf (accessed March 30, 2018)

Attacks geography: Top source countries for DDoS attacks

Q1 2016		Q2 2016		Q3 2016		Q4 2016	
Country	Percentage Source IPs	Country	Percentage Source IPs	Country	Percentage Source IPs	Country	Percentage Source IPs
China	16% 115,478	China	40% 306,627	China	19% 81,276	U.S.	24% 180,652
U.S.	10% 72,598	U.S.	12% 95,004	U.S.	14% 59,350	U.K.	10% 72,949
Turkey	6% 43,400	Taiwan	4% 28,546	U.K.	10% 44,460	Germany	7% 49,408
Brazil	5% 36,472	Canada	3% 20,601	France	6% 23,980	China	6% 46,783
South Korea	4% 31,692	Vietnam	3% 20,244	Brazil	3% 13,502	Russia	4% 33,211

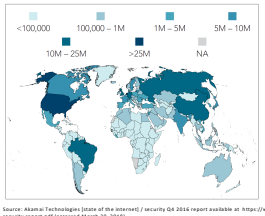
Data Source: Akamai Technologies [state of the internet] / security Q4 2016 report available at https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2016-state-of-the-internet-security-report.pdf (accessed March 30, 2018)

Attacks geography: Top source countries for DDoS attacks Q4 2016

Source Country	Percentage	IP Source Count
U.S.	24%	180,652
U.K.	9.7%	72,949
Germany	6.6%	49,408
China	6.2%	46,763
Russia	4.4%	33,211
Italy	3.1%	23,365
Spain	3.0%	22,645
Brazil	3.0%	22,582
Netherlands	2.8%	21,115
France	2.8%	20,707
Other	34%	258,498

Data Source: Akamai Technologies [state of the internet] / security Q4 2016 report available at https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2016-state-of-the-internet-security-report.pdf (accessed March 30, 2018)

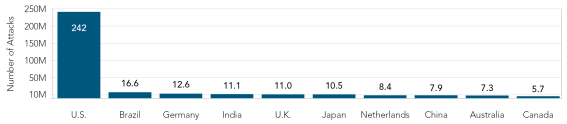
Global Web Application Attack Source Countries, Q4 2016



Country	Attacks Sourced	Percentage
U.S.	97,918,896	28%
Netherlands	61,499,919	17%
Germany	32,384,205	9.2%
Brazil	19,379,729	5.5%
Russia	16,643,150	4.7%
China	14,275,358	4.0%
U.K.	11,908,055	3.4%
Lithuania	9,793,507	2.8%
France	8,772,176	2.5%
India	8,638,666	2.4%

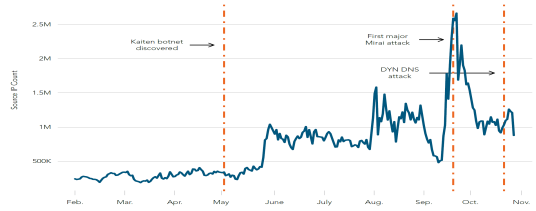
Source: Akamai Technologies [state of the internet] / security Q4 2016 report available at https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2016-state-of-the-internet-security-report.pdf (accessed March 30, 2018)

Top 10 Target Countries for Web Application Attacks, Q4 2016



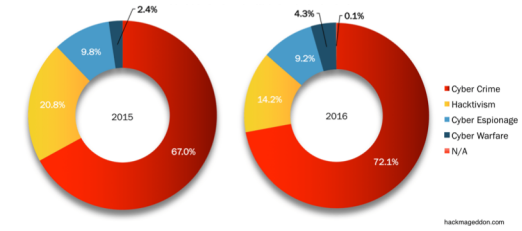
Source: Akamai Technologies [state of the internet] / security Q4 2016 report available at https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2016-state-of-the-internet-security-report.pdf (accessed March 30, 2018)

IP Scanning on Ports 23 and 2323



Source: Akamai Technologies [state of the internet] / security Q4 2016 report available at https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2016-state-of-the-internet-security-report.pdf (accessed March 30, 2018)

Motivations Behind Attacks 2015 vs 2016



Dark web

- The Dark Web is a term that refers specifically to a collection of websites that exist on an encrypted network and cannot be found by using traditional search engines or visited by using traditional browsers[1].
- Almost all sites on the so-called Dark Web hide their identity using the Tor encryption tool. You may know Tor for its ability to hide your identity and activity. You can use Tor to spoof your location so it appears you're in a different country to where you're really located, making it much like using a VPN service[1].
- Last year was a very active year for the dark web. The general offerings of the dark web markets shifted significantly, especially with new cryptocurrencies in use. A few high-profile hacker forums and underground marketplaces disappeared, with new ones popping up in their place[2].
- Nowadays: Huge shift in dark web market offerings, from a focus on illicit drugs, malware offerings, compromised credentials, personally identifiable information (pii), medical records, financial services accounts, hacking tutorials, credit card numbers, and a glut of compromised digital accounts for a wide range of services. Single and bulk compromised account logins are readily available across the top five dark web markets, and the prices are falling as more enter the market[2]

Sources:
1. M Egan What is the dark web and deep web, 19 July 2017, TechAdvisor accessed at http://www.techadvisor.co.uk/how-to/internet/what-is-dark-web-deep-web-3593569/ on August 26, 2017
2 Akamai's [state of the internet] / security Q4 2016 report accesed at https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2016-state-of-the-internet-security-report.pdf on August 1, 2017

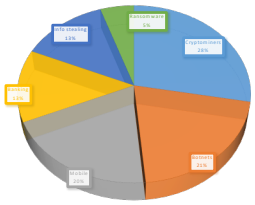
Recent data

In 2019 Mandiant professionals observed that:

- - 7% originated with or used compromised third party access,
- - 15% had multiple attackers,
- - Less than 1% involved an insider,
- - 22% had data theft likely in support of intellectual property or espionage end goals,
- - 29% were likely for direct financial gain. This includes extortion, ransom, card theft, and illicit transfers,
- - 3% of these targeted attacks were for the purpose of reselling access gained in the intrusion,
- - 4% likely served no purpose except for creating compromised architecture to further other attacks
- Eleven percent of all Mandiant engagements in this period were for responses or assessments in environments with a significant cloud component.

Source: M-trends 2020, FIREEYE MANDIANT SERVICES, SPECIAL REPORT

Cyber attacks category rates - 2019



build from data given in Source: Checkpoint Security report 2019

Scale of cyber crime operation

1. Data breaches resulted in 36 billion records being exposed in the first three quarters of 2020, according to RiskBased Security research. Despite this, the number of publicly reported breaches decreased by 51% compared to the same time last year.
2. The use of malware increased by 358% through 2020, and ransomware usage increased by 435% compared to the previous year, according to a study by Deep Instinct. July 2020 alone saw a 653% increase in malicious activity compared to the same month in 2019.
3. More than 90% of healthcare organizations suffered at least one cybersecurity breach in the previous three years, according to the U.S. Healthcare Cybersecurity Market 2020 report.

Source: https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics

Cost of cyber crime operation

1. Cyber crime costs organizations $2.9 million every minute, and major businesses lose $25 per minute as a result of data breaches, according to RiskIQ research.
2. According to research by IBM, it takes 280 days to find and contain the average cyberattack, while the average attack costs $3.86 million.
3. The global cybersecurity market will be valued at $403 billion by 2027 with a compound annual growth rate (CAGR) of 12.5%, according to Brand Essence Research. The firm states the cybersecurity market was worth $176.5 billion in 2020.
4. The U.S. has the world's highest data breach costs, with the average attack costing $8.6 million, according to IBM's Cost of a Data Breach report.

Source: https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics

Proportion of Email Traffic Identified as Malicious - by Geographic Location, 2015

Country	Rate of malicious emails
Hungary	1 in 86
UK	1 in 112
Austria	1 in 124
Netherlands	1 in 140
Brazil	1 in 162
Hong Kong	1 in 176
UAE	1 in 199

Data Source: Internet Security Threat Report, volume 21, April 2016, Symantec

Network Security Issues

- Information must be protected when travelling across the network
- Only authorized access is allowed to a node
- Nodes handle security appropriately within node itself
- Firewalls don't provide complete protection.
- "Whoever thinks his problem can be solved using cryptography, doesn't understand his problem and doesn't understand cryptography ." —— Attributed by Roger Needham and Butler Lampson to each other – source: Ross J. Anderson Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd edition, Wiley, 2008

- 30 Worrying Cybersecurity Statistics for 2021
https://www.youtube.com/watch?v=APOkulJOPPg
Time: 4:44

15 Alarming Cybersecurity Facts and Stats
https://www.youtube.com/watch?v=4gDgEovmTlg
Time: 1:24

Answer the questions:

Is computer security worth studying now for me?

Who is guilty? And What to do?

- **Automated, distributed attacks present a global problem.** The majority of the compromised devices in recent noteworthy botnets have been geographically located outside the US.
- **Effective tools exist, but are not widely used.** However, they do not form the common practices for product development and deployment in many other sectors for a variety of reasons, including (but not limited to) lack of awareness, cost avoidance, insufficient technical expertise, and lack of market incentives.
- **Products should be secured during all stages of the lifecycle.** Devices that are vulnerable at time of deployment, lack facilities to patch their vulnerabilities after discovery, or remain in service after vendor support ends make assembling automated, distributed threats far too easy.

Source: Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats , US Department of Commerce and Department of Homeland Security, May 22, 2018 accessed at https://csrc.nist.gov/CSRC/media/Publications/white-paper/2018/05/30/enhancing-resilience-against-botnets--report-to-the-president/final/documents/eo_13800_botnet_report_-_finalv2.pdf on November 22, 2020

Who is guilty? And What to do? - 2

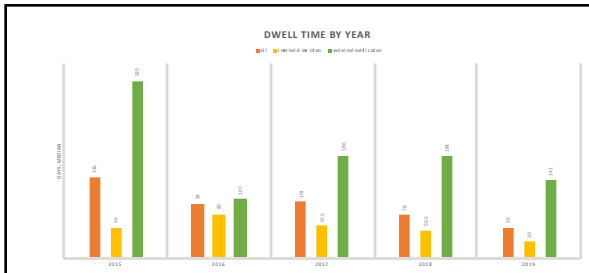
- **Awareness and education are needed.** Home users and some enterprise customers are often unaware of the role their devices could play in a botnet attack and may not fully understand the merits of available technical controls. Product developers, manufacturers, and infrastructure operators often lack the knowledge and skills necessary to deploy tools, processes, and practices that would make the ecosystem more resilient.
- **Market incentives should be more effectively aligned.** They do not currently appear to target at dramatically reducing threats perpetrated by automated and distributed attacks. Market incentives must be realigned to promote a better balance between security and convenience when developing products.
- **Automated, distributed attacks present the world wide challenge.** No single stakeholder community can address the problem in isolation.

Source: Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats , US Department of Commerce and Department of Homeland Security, May 22, 2018 accessed at https://csrc.nist.gov/CSRC/media/Publications/white-paper/2018/05/30/enhancing-resilience-against-botnets--report-to-the-president/final/documents/eo_13800_botnet_report_-_finaly2.pdf on November 22, 2020

Computer security priorities?

- Tom Bossert, the White House homeland security and counterterrorism advisor, told that 'protecting federal networks and data as well as the critical infrastructure are the Trump administration's top two cyber priorities … the administration's third priority is to protect the nation and the American people in cyberspace'.
- Bossert added that the administration has already waded through 15 recent reports on cybersecurity -- from the CSIS Cyber Policy Task Force report to the Commission on Enhancing National Cybersecurity -- and 175 recommendations.

Source: C.D. Carberry "Trump's cyber job #1: protecting federal networks and data", March 15, 2017 accessed at https://fcw.com/articles/2017/03/15/trump-cyber-priority-carberry.aspx?s=fcwdaily_160317 on March 16, 2017



Median dwell time (how long it takes to detect an intrusion) build from data given in Source: M-trends 2020, FIREEYE MANDIANT SERVICES, SPECIAL REPORT

Part 2:

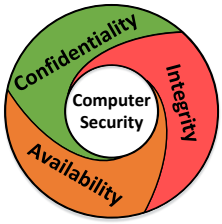
Computer security basic concepts

Intelligent Security Systems

Chapter 1

Computer security with artificial intelligence, machine learning and data science combination

What is Computer Security?

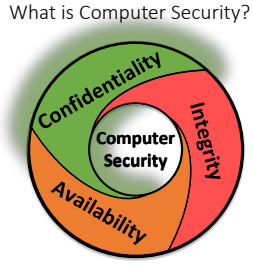


Computer Security = CIA

CIA =

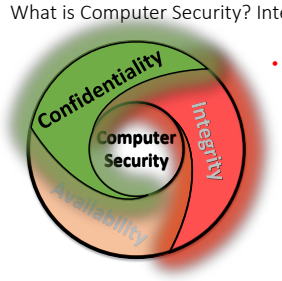
Confidentiality + Integrity + Availability

What is Computer Security? Confidentiality



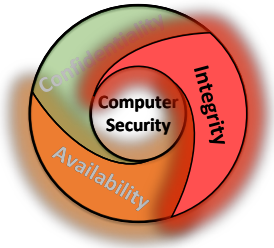
- *Confidentiality*: The protection of information from unauthorized disclosure
  - need to know
  - sample mechanisms: access controls, cryptography, resource hiding
  - existence of data as well as content

What is Computer Security? Integrity



- *Integrity:* The protection from unauthorized modification of information
  - *data* integrity and *origin* integrity (authentication)
    - Prevention mechanisms block unauthorized access
    - Detection mechanisms report when information is no longer trustworthy

What is Computer Security? Availability

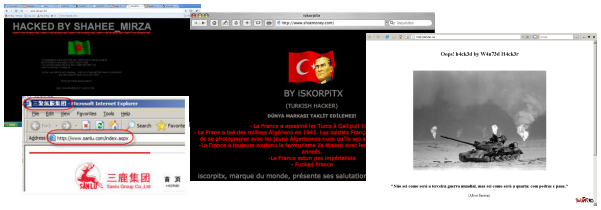


- *Availability:* Resources and services are usable or operational during a given time period despite attacks or failures.

Threats against Assets

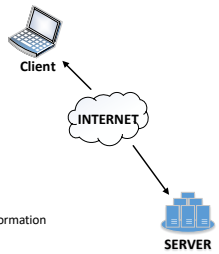
	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.		Parts are replaced with no authorization
Software	Code, programs are removed	An unauthorized copy of software is made and could be executed	A code is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted or hidden, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or replace with new files.
Communication channels	Messages are destroyed or deleted. Communications lines or networks are rendered unavailable.	Messages are copied and/or read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Website Attack



Web Security

- **Client side**
  - Privacy protections
  - Integrity protections
- **Server side**
  - Protection from break in
  - Protection from vandalism
  - Protection from denial of service
- **Both**
  - Confidentiality and integrity of transmitted information



Threats, Vulnerabilities, Risks, Attacks

- A *Threat* is a potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm [1].
- A *Vulnerability* is a weakness in a product that could allow an attacker to compromise the integrity, availability, or confidentiality of that product [2].
- A *Risk* is the product of the level of threat with the level of vulnerability. It establishes the likelihood of a successful attack [1].
- An *Attack* is an attempt to exploit a vulnerability to make a threat a reality.

[1] https://www.sans.org/security-resources/glossary-of-terms/
[2] https://msdn.microsoft.com/en-us/library/cc751383.aspx

Malicious activities

Symantec categorizes malicious activities as follows:

- **Malicious code.** This includes programs such as viruses, worms, and Trojans that are covertly inserted into programs. The purposes of malicious code include destroying data, running destructive or intrusive programs, stealing sensitive information, and compromising the security or integrity of a victim's computer data.
- **Spam zombies.** These are remotely controlled, compromised systems specifically designed to send out large volumes of junk or unsolicited email messages. These email messages can be used to deliver malicious code and phishing attempts.
- **Phishing hosts.** Phishing hosts are computers that provide website services in order to illegally gather sensitive user information while pretending that the attempt is from a trusted, well-known organization by presenting a website designed to mimic the site of a legitimate business.

Source: Internet Security Threat Report, volume 21, April 2016, Symantec

Malicious activities

Symantec categorizes malicious activities as follows:

- **Bot-infected computers.** Malicious programs have been used to compromise computers to allow an attacker to control the targeted system remotely. Typically, a remote attacker controls a large number of compromised computers over a single reliable channel in a botnet, which can then be used to launch coordinated attacks.
- **Network attack origins.** This measures the originating sources of attacks from the Internet. For example, attacks can target SQL protocols or buffer overflow vulnerabilities.
- **Web-based attack origins.** This measures attack sources that are delivered via the web or through HTTP. Typically, legitimate websites are compromised and used to attack unsuspecting visitors.

Source: Internet Security Threat Report, volume 21, April 2016, Symantec

Fundamental Threats

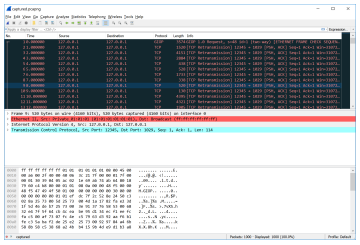
- *Disclosure or Compromise:* Unauthorized disclosure of information.
  - Has received the most attention in R&D over the past 30 years.
- *Deception*: Acceptance of false data
- *Disruption:* interruption or prevention of correct operation
- *Usurpation:* unauthorized control of some part of the system

Snooping

- Unauthorized viewing
- Disclosure threat
- Passive
- Example: Wiretapping, or *passive wiretapping*
- Counter with confidentiality mechanisms

Sniffer

Sniffer is a computer software or computer hardware that can intercept and log traffic passing over a digital network or part of a network.



Screenshot of our computer display running Wireshark software

What is Modification or Alteration?

- Active unauthorized tweaking
- Could be deception threat
- May involve disruption or usurpation if controls are modified
- Example: *Active wiretapping*
- Possible mitigation with integrity mechanisms

What is Masquerading or Spoofing?

- Could be passive or active (examples are below)
- Target: impersonation, misleading user
- Could be deception and usurpation threat
- Passive attacks:
  - user falls into trap with no overt actions by spoofer
  - spoofer gives a user a different file than I asked for. The user does not ask for authentication of file.
- Active attacks:
  - spoofer intentionally misleads user
  - mitigation with authentication mechanisms

Is Delegation an Attack?

- Delegation Can Lead to a Masquerade
- One user is authorized to act on behalf of another.
- Can be used appropriately
- Can be used inappropriately to become a masquerade

Brute Force Attack and Social Engineering

- **Social engineering** is the act of manipulating people into performing actions or divulging confidential information.
- **Brute Force** is a cryptanalysis technique or other kind of attack method involving an exhaustive procedure that tries all possibilities, one-by-one.

Source: https://www.sans.org/security-resources/glossary-of-terms/ (accessed March 30, 2018)

Repudiation of Origin

- Denial that you sent or created something
- Deception threat
- Counter with integrity mechanisms

Denial of Receipt

- User claims messages were not received.
- Deception threat
- Counter with integrity and availability mechanisms

Delay

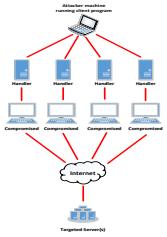
- Temporarily inhibit a service.
- Usurpation threat
  - Can support deception in the form of masquerading
- Counter with availability mechanisms

Denial of Service

- Long term inhibition of service
- Usurpation and sometimes deception
- Counter with availability mechanisms.

Distributed Denial of Service

- A distributed attack occurs when multiple compromised systems attack the target in parallel way.
- These systems are compromised by attackers using a variety of methods.



15 Cybersecurity Terms You Should Know
- https://www.youtube.com/watch?v=wRQorGs2HUw
- Time: 4:04

Answer the questions:

What computer security terms have you learned in this class? Name and briefly describe their meanings.

Part 3:

Sources of security threats

Intelligent Security Systems

Chapter 1

Computer security with artificial intelligence, machine learning and data science combination

Sources of security threats

- **Weakness in the computer and network infrastructure and protocols**
- **Design and implementation problems**
- **Vulnerabilities in software systems and tools**
- **Hackers' activity**
- **Social engineering**
- **Physical theft**

Weakness in the computer and network infrastructure and protocols

- **Policy Level weakness**. Security risks exist if the policies are not followed or if there are no strictly defined guidelines. A security policy must meet certain goals. Among others, it must state how to audit or configure the systems to verify whether the system follows the network policy, it should specify the steps through which requirements are met and finally it should provide proper guidelines to the staff and users for protecting the information and resources. If certain important areas are not covered or misunderstood, the security mechanisms that are set up based on the policies might have loopholes in organization system protection.
- **Technological weakness** depends on technical factors and solutions such as chosen network and communication equipment, protocols, operating systems. Using certain older protocols, for example, telnet might result in weakening security as hackers might get a better chance to exploit the vulnerabilities in the computer systems.
- **Configuration weakness** occurs due to incorrect configurations of systems or applications. It might result in unauthorized accounts, unsecured settings, misconfigured network equipment. All of these factors may lead to vulnerabilities, which could be captured and exploited by the hackers.

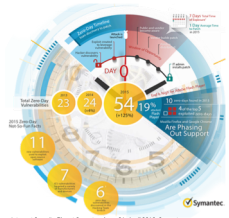
Design and implementation problems

- may include inadequate logging of security relevant events, incorrect or incomplete access controls, insecure default setup conditions, failure to address security issues from external sources.

Vulnerabilities in software systems and tools

- **Design Flaws**
  - Inadequate logging of security relevant events
  - Incorrect or incomplete access controls.
- **Programming Flaws**
  - Improper array bounds allowing buffer overflow.
- **Operational Flaws**
  - Insecure default setup conditions
  - Failure to address security issues from external sources.

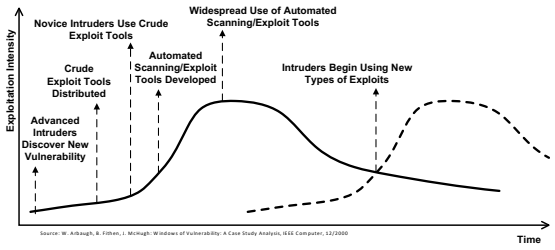
A New Zero-Day Vulnerability Discovered Every Week in 2015



Source: Internet Security Threat Report, volume 21, April 2016, Symantec

- Advanced attack groups continue to profit from previously undiscovered flaws in browsers and websites plugins.
- In 2015, **54 zero-day vulnerabilities** were discovered.

Vulnerability Exploit Cycle

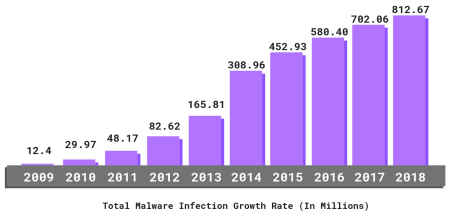


Source: W. Arbaugh, W. Fithen, J. McHugh: Windows of Vulnerability: A Case Study Analysis, IEEE Computer, 12/2000

Hackers' activities

- *Eavesdropping* = intercepting messages , which results in violating confidentiality
- *Inserting* messages, which results in violating of integrity
- *Impersonation = faking* (spoofing) source address in a packet (or any field in packet) , which results in violating of integrity
- *Hijacking* = taking ongoing connection by removing sender or receiver and inserting themselves in place, which results in violating of integrity, confidentiality and availability
- *Denial of service*= preventing service from being used by others (e.g., by overloading resources), which results in violating of availability

Malware statistics



Total Malware Infection Growth Rate (In Millions)

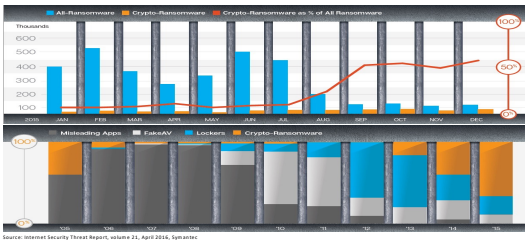
Siurce: **2021 Cyber Security Statistics The Ultimate List Of Stats, Data & Trends - https://purplesec.us/resources/cyber-security-statistics/**

Malware statistics

- 92% of malware is delivered by email.
- Mobile malware on the rise with the number of new malware variants for mobile increased by 54% in 2018.
- Third-party app stores host 99.9% of discovered mobile malware.
- 98% of mobile malware target Android devices.
- Over the last year, MacOS malware has increased by 165%.
- Malware is still the preferred distribution model, used 71.14% of the time over the last 12 months.
- The United States continues to host the most botnet control servers in the world. Over the last year, 36% of these servers were hosted in America, while 24% were hosted in undefined countries.
- Trojans make up 51.45% of all malware.
- 230,000 new malware samples are produced every day — and this is predicted to only keep growing.

Siurce: 2021 Cyber Security Statistics The Ultimate List Of Stats, Data & Trends - https://purplesec.us/resources/cyber-security-statistics/

Ransomware



Source: Internet Security Threat Report, volume 21, April 2016, Symantec

Ransomware statistics

- Ransomware attacks worldwide rose 350% in 2018.
- Ransomware attacks are estimated to cost $6 trillion annually by 2021.
- 50% of a surveyed 582 information security professionals do not believe their organization is prepared to repel a ransomware attack.
- 81% of cyber security experts believe there will be more ransomware attacks than ever in 2019.
- 75% of companies infected with ransomware were running up-to-date endpoint protection.
- Ransomware costs businesses more than $75 billion per year.
- The NotPeyta ransomware attack losses could exceed $1 billion.

Siurce: 2021 Cyber Security Statistics The Ultimate List Of Stats, Data & Trends - https://purplesec.us/resources/cyber-security-statistics/

Social engineering

- 98% of cyber attacks rely on social engineering.
- 43% of the IT professionals said they had been targeted by social engineering schemes in the last year.
- New employees are the most susceptible to socially engineered attacks, with 60% of IT professionals citing recent hires as being at high risk.
- 21% of current or former employees use social engineering to gain a financial advantage, for revenge, out of curiosity or for fun.
- Social engineering attempts spiked more than 500% from the first to second quarter of 2018.
- 56% of IT decision makers say targeted phishing attacks are their top security threat.
- 83% of global infosec respondents experienced phishing attacks in 2018, an increase from 76% in 2017.
- Business email compromise (BEC) scams cost organizations $676 million in 2017.

Siurce: 2021 Cyber Security Statistics The Ultimate List Of Stats, Data & Trends - https://purplesec.us/resources/cyber-security-statistics/

Legal Classification

- **Cyber Crime and Espionage:**

Any crime that encompasses a network or a computer can be deemed as **cyber crime**. The practice of gathering secrets without the consent of the information holder using a Computer System or Network is termed as **cyber espionage**.

- **Cyber Terrorism:**

Instances of terrorism in the cyberspace domain are classified under **cyber terrorism**.

Sources of Cybersecurity Threats - Common Cyber Attacks sources

https://www.youtube.com/watch?v=tS9WXWyALCw

- Time: 4:00

Answer the questions:

What computer security threat source do you consider the most dangerous? Why?

Part 4:

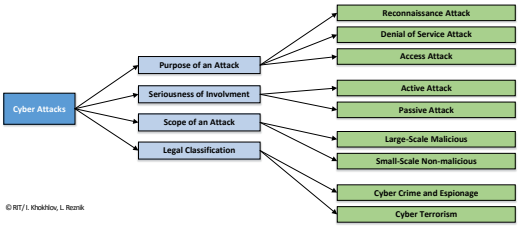
Attacks against IoT and wireless sensor networks

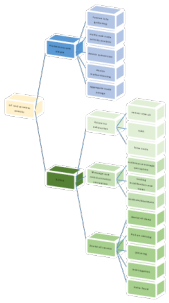
Intelligent Security Systems

Chapter 1

Computer security with artificial intelligence, machine learning and data science combination

Classification of Cyber Attacks





Purpose of Attack

- **Reconnaissance attack** is an attempt to gather sensitive information about network services and system
  - **Packet Sniffers**
  - **Ping Sweep**
  - **Port Scan**
  - **Queries Regarding Internet information**
- **Denial of Service Attack** is a network attack devised to slow down or crash a system by flooding it with useless traffic.
  - **Ping of Death**
  - **Teardrop Attack**
- **Access Attacks** is when an attacker may try to uncover exploits and vulnerabilities in FTP, Web Services and Network Authentication in order to get access to a system's network.
  - **Password Attack**
  - **Trust Exploitation Attack**
  - **Man in the middle**

Seriousness of Involvement

- An **active attack** allows the attacker to block the communication channel between participants on a network or permits him to send data to all the parties at once.
- **Passive attack** is when an intruder with unauthorized network access actively eavesdrops a communication between two participants.

Attack Scope

- **Malicious Large-Scale Attack:**

Malicious attack is an offensive attempt or an intent to inflict harm, such attacks aim at creating chaos and disrupting services.

- **Non-Malicious Small-Scale Attack:**

An unintentional attack or an accidental damage due to a human operational error that might cause a system crash, deletion of data, is a non-malicious attack.

watch video

8 Basic Cyber Attacks … and How to Avoid Them
https://www.youtube.com/watch?v=Ym00-RJnFsk
• Time: 4:50

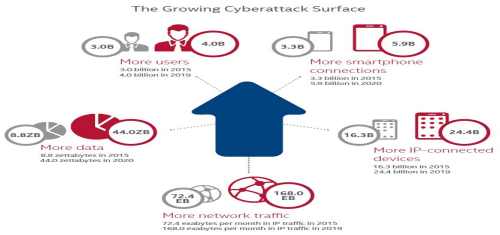
Answer the questions:

Classify attacks presented in this video based on the scheme given in the previous slides

Cybersecurity and privacy protection future development

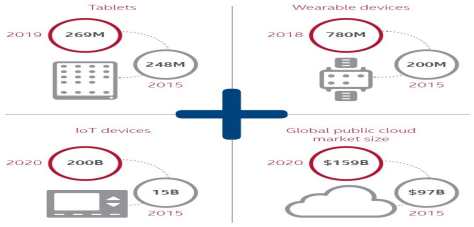
New technologies and applications, such as self-driving cars and bikes dramatically increase the data security and privacy protection requirements
Images taken at CES 2018 @ I.Khokhlov and L.Reznik

Future predictions: infrastructure



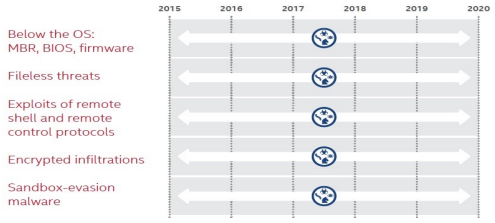
Source: Threat predictions report. McAfee™ Labs, 2016

Future predictions: device diversity



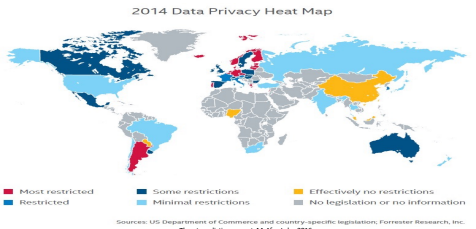
Source: Threat predictions report. McAfee Labs, 2016

Future predictions: difficult to detect attacks



Source: Threat predictions report. McAfee Labs, 2016

Future predictions: Privacy protection legislation



Sources: US Department of Commerce and country-specific legislation; Forrester Research, Inc.
Threat predictions report. McAfee Labs, 2016

EU General Data Protection Regulation (GDPR) – 2018 – Key changes

- This is the most important change in data privacy regulation in 20 years
- After four years of preparation and debate the GDPR was **finally approved** by the EU Parliament on **14 April 2016**. Enforcement date: **25 May 2018** - at which time those organizations in non-compliance may face heavy fines.
  Increased Territorial Scope (extra-territorial applicability)
  it applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location
- **Penalties**
  Under GDPR organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater).
  Consent
  The conditions for consent have been strengthened, and companies will no longer be able to use long illegible terms and conditions full of legalese, as the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent.

Source: https://www.eugdpr.org/key-changes.html

EU General Data Protection Regulation (GDPR) – 2018 – Data subject rights

- **Breach Notification** Under the GDPR, breach notification will become mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.
- **Right to Access** Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to data transparency and empowerment of data subjects.
  Right to be Forgotten Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in article 17, include the data no longer being relevant to original purposes for processing, or a data subjects withdrawing consent.

Source: https://www.eugdpr.org/key-changes.html

EU General Data Protection Regulation (GDPR) – 2018 – Data subject rights

Data Portability
GDPR introduces data portability - the right for a data subject to receive the personal data concerning them, which they have previously provided in a '*commonly use and machine readable format*' and have the right to transmit that data to another controller.

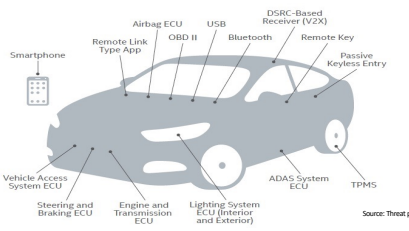
Privacy by Design
Privacy by design as a concept has existed for years now, but it is only just becoming part of a legal requirement with the GDPR. At its core, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. More specifically - *'The controller shall implement appropriate technical and organizational measures in an effective way.. in order to meet the requirements of this Regulation and protect the rights of data subjects'.* Article 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimization), as well as limiting the access to personal data to those needing to act out the processing.

Source: https://www.eugdpr.org/key-changes.html

California's Consumer Privacy Act of 2018

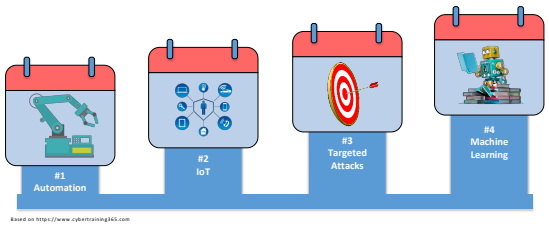
- took effect on January 1, 2020. The law gives California residents the right to know what data companies collect about them and how that information is shared. Consumers will also have the authority to prohibit companies from selling their data.
- The bill bears similarities to the EU's General Data Protection Regulation (GDPR) but it is no clone, so even if you currently must comply with GDPR, the CCPA will be different.
- And, by the way, it's not the only privacy law at the state level.

Future predictions: most exposed attack surfaces on a car



Source: Threat predictions report. McAfee Labs, 2016

The Big 4: 2017 Cyber Security Predictions



based on https://www.cybertraining365.com