THE UNIVERSITY OF QUEENSLAND
AUSTRALIA

CREATE CHANGE

BISM3205: Business Information Security

Week 02:

Part 1: The Need for Security (Ch. 2)

Part 2: Legal, Ethical, Professional Issues (Ch. 3)

Dr Alex Pudmenzky

Semester 1, 2023

Clickjacking - Live Demo

Logon to our BISM3205 Bank to check our account balance (using Chrome browser):

https://alexpudmenzky.com/BISM3205/bank.php

Oh dear - we have been hacked!

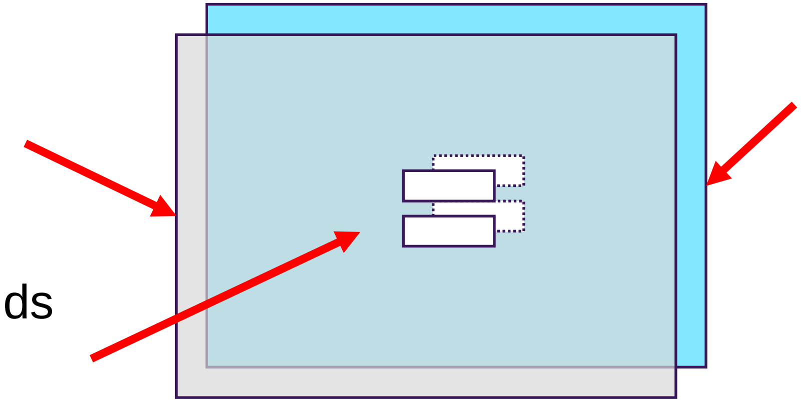
Let's inspect the source code of the web page from the browser!

Clickjacking - How it is done

The real web site is embedded in the hacker's web site with the <iframe> tag.

An iframe is normally used to include another web page such as a YouTube video in one's own web page as demonstrated here:

https://www.youtube.com/embed/tgbNymZ7vqY (original video)
https://www.w3schools.com/html/tryit.asp?filename=tryhtml_youtubeiframe (video embedded in page)



Hacker's website (fully transparent)

Hacker's form fields (visible & overlap real fields on top)

Bank website containing original form fields (now inaccessible) in full page iFrame of hacker's website

Clickjacking - Protection

Clickjacking attacks can be prevented by including this directive in a web page's HTTP return header:

header("X-Frame-Options: DENY");
or
header("Content-Security-Policy: frame-ancestors 'none'", false);

You can test a site for the presence of this protection here:
https://geekflare.com/tools/x-frame-options-test

If you find this line in the returned message:

:
X-Frame-Options: DENY
:

it will force the browser NOT to render the page in an iframe!

Clickjacking - Check if a site is protected

Check if this protection exists for the following websites:

- https://www.facebook.com/login
- https://login.anz.com/internetbanking

Clickjacking - But how did I get onto the hacker's website?

This is another trick that was once exploited by registering the malicious site http://www.paypal.com in 2005 (the first *a* character in "paypal" is replaced by a Cyrillic *a*).

It is called a **homoglyph** attack.

The attacker uses letters from another alphabet (like Cyrillic) that look like Roman letters and registers this text as a URL.

Here is a website that demonstrates how you can form such a URL https://www.irongeek.com/homoglyph-attack-generator.php

Some browsers are now displaying those URLs in Punycode to warn the user (see https://en.wikipedia.org/wiki/Punycode).

When security needs and business needs collide, business wins

Information security performs four important functions for an organization:

1. Protects ability to function
2. Enables safe operation of applications implemented on its IT systems
3. Protects data (stored and transmitted) that the organization collects and uses
4. Safeguards technology assets in use

Protecting the functionality of an organization

Decision makers in organizations must set policy and operate their organizations in compliance with the complex, shifting legislation that controls the use of technology.

We need **information security** when we

store,

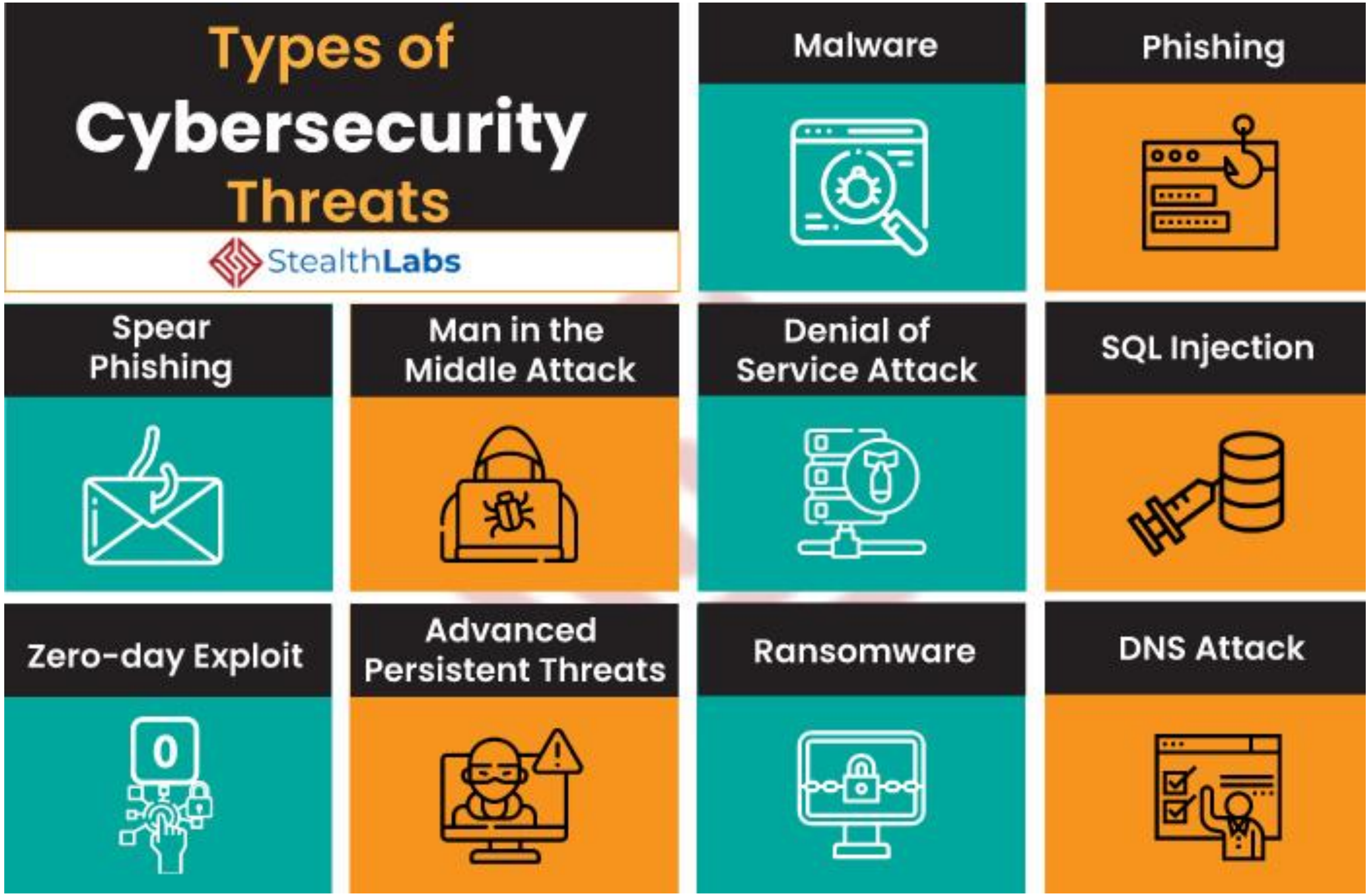
process,

transmit information

Some definitions – we encountered these in week 1:

- Threat
- Attack
- Exploit
- Vulnerability
- Risk

Threat: a potential risk to an asset, a loss of value, usually targeting a weakness/vulnerability in an asset



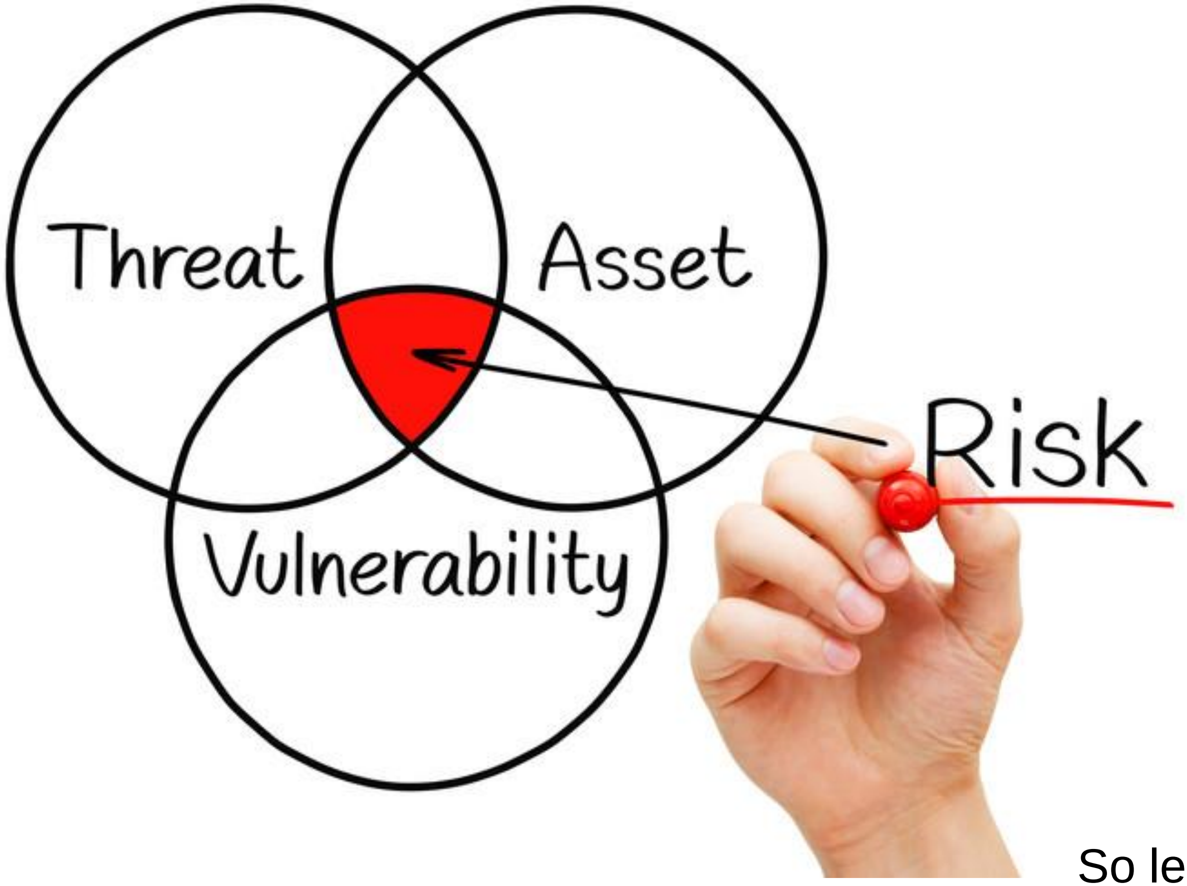
Attack: An intentional or unintentional act that can damage or otherwise compromise information and/or the systems that support it

Exploit: A technique used to compromise a system, we also speak of an attack vector (e.g. a phishing email)

Vulnerability: A (potential) weakness in an asset or its defensive control system(s)

OpenSSL 3 Critical Vulnerability | What Do Organizations Need To Do Now?

Management must know about the threats so the risks can be evaluated



So let's look at some threats now...

Threat #1: Deviations in Quality of Service

- Includes **situations where products or services are not delivered as expected.**
- Internet service, communications, and power irregularities dramatically affect **availability** of information and systems.
- **Internet service issues**
  - Internet service provider (ISP) failures can considerably undermine availability of information
  - Outsourced Web hosting provider assumes responsibility for all Internet services as well as hardware and Web site operating system software
- **Communications and other service provider issues**
  - Other utility services affect organizations: telephone, water, wastewater, trash pickup, etc.
- **Power irregularities**
  - Commonplace, organizations with inadequately conditioned power are susceptible, controls can be applied to manage power quality, fluctuations (short or prolonged)

Threat #2: Espionage or Trespass

- **Access of protected information by unauthorized individuals**
- Competitive intelligence (legal) vs. industrial espionage (illegal)
- **Shoulder surfing** can occur anywhere a person accesses confidential information
- **Controls let trespassers know they are encroaching on organization's cyberspace**
- Hackers use skill, guile, or fraud to bypass controls protecting others' information

Shoulder surfing

Image source: Michael E. Whitman and Herbert J. Mattord, *Principles of Information Security*, 7th Edition. © 2022 Cengage. All Rights Reserved.

Threat #3: Forces of Nature

- Forces of nature are among the most dangerous threats
- Disrupt not only individual lives, but also storage, transmission, and use of information
- **Organizations must implement controls to limit damage and prepare contingency plans for continued operations**

Threat #4: Human Error or Failure

- **Includes acts performed *without* malicious intent**
- Causes include:
  - **Inexperience**
  - **Improper training**
  - Incorrect assumptions
- **Employees are among the greatest threats to an organization’s data**
- Again, we need to consider the appropriate controls

Human Error or Failure (cont‘d.) - Social Engineering

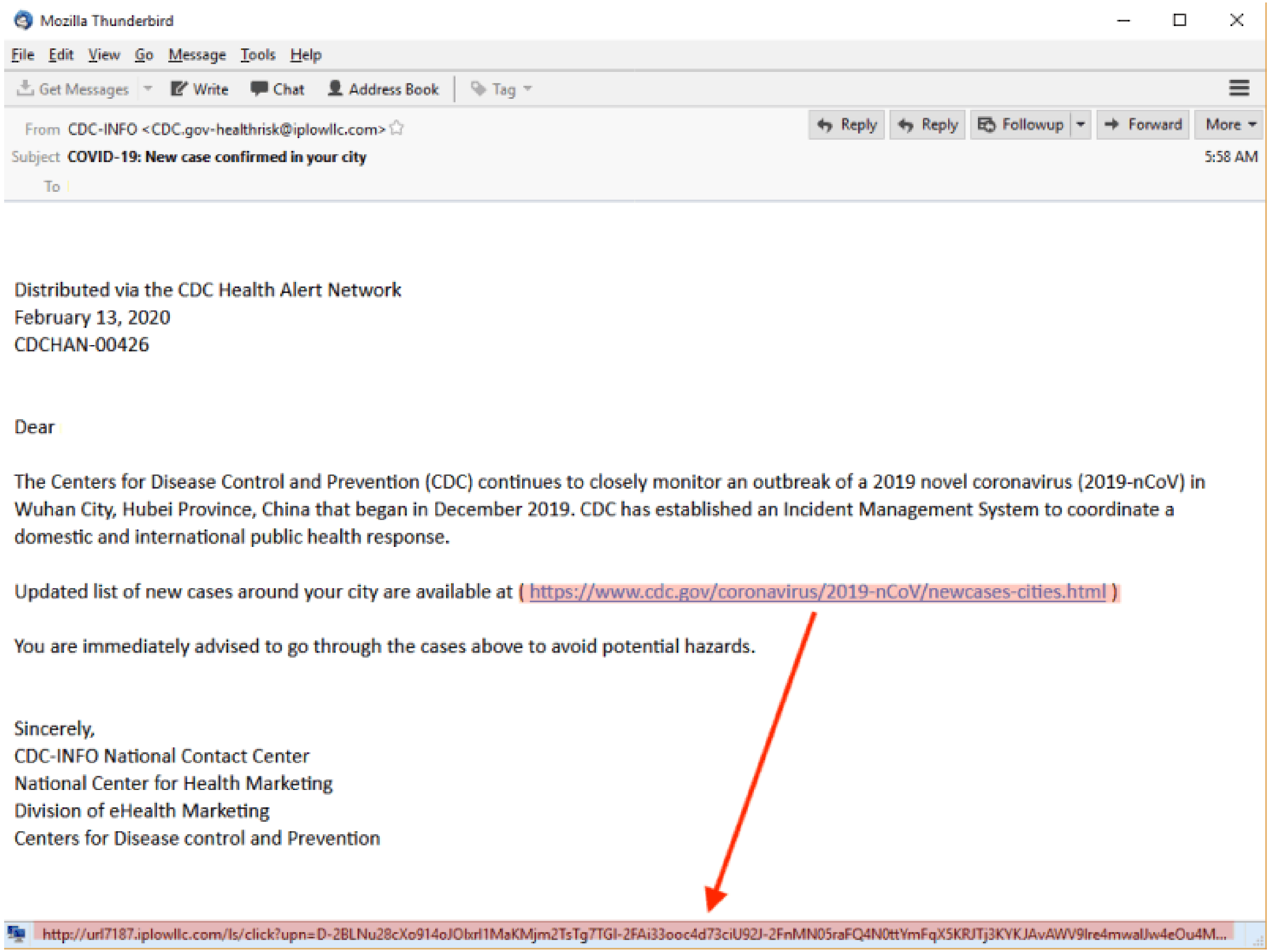
> “***<u>People are the weakest link</u>***. *You can have the best technology; firewalls, intrusion-detection systems, biometric devices ... and somebody can call an unsuspecting employee. That's all she wrote, baby. They got everything.”** — *Kevin Mitnick*

- **<u>Social engineering</u>:** using social skills to convince people to reveal access credentials or other valuable information to an attacker.
- **<u>Phishing</u>**: attempt to gain personal/confidential information; apparent legitimate communication hides embedded code that redirects user to third-party site
- Other types:
  - Business e-mail compromise
  - Advance-fee fraud

*The phrase "That's all she wrote" is a colloquial expression that means "that's all there is" or "there is nothing more to say." It is often used to indicate the end of something, such as a story or a situation. The addition of "baby" to the phrase is simply a colloquialism that adds emphasis or emotion to the statement.

Phishing Example

- Cybercrime up **600%** due to Covid-19 pandemic
- Increased security risk from **remote working**
- **18 million** COVID-related daily phishing emails



From CDC-INFO <CDC.gov-healthrisk@iplowllc.com>

Subject COVID-19: New case confirmed in your city

5:58 AM

To

Distributed via the CDC Health Alert Network
February 13, 2020
CDCHAN-00426

Dear

The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

You are immediately advised to go through the cases above to avoid potential hazards.

Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention

http://url7187.iplowllc.com/ls/click?upn=D-2BLNu28cXo914oJOlxrl1MaKMjm2TsTg7TGl-2FAi33ooc4d73ciU92J-2FnMN05raFQ4N0ttYmFqX5KRJTj3KYKJAvAWV9lre4mwalJw4eOu4M...

https://purplesec.us/resources/cyber-security-statistics/

Information Security Statistics & Phishing

- By the end of 2022, cybercrime is expected to cost the world **$6 trillion**.
- The global information security market is forecasted to grow to **$170.4 billion** in 2022.
- The average annual cost of a phishing scam in 2021 is **$14.8 million** for a 9,600-employee organization.

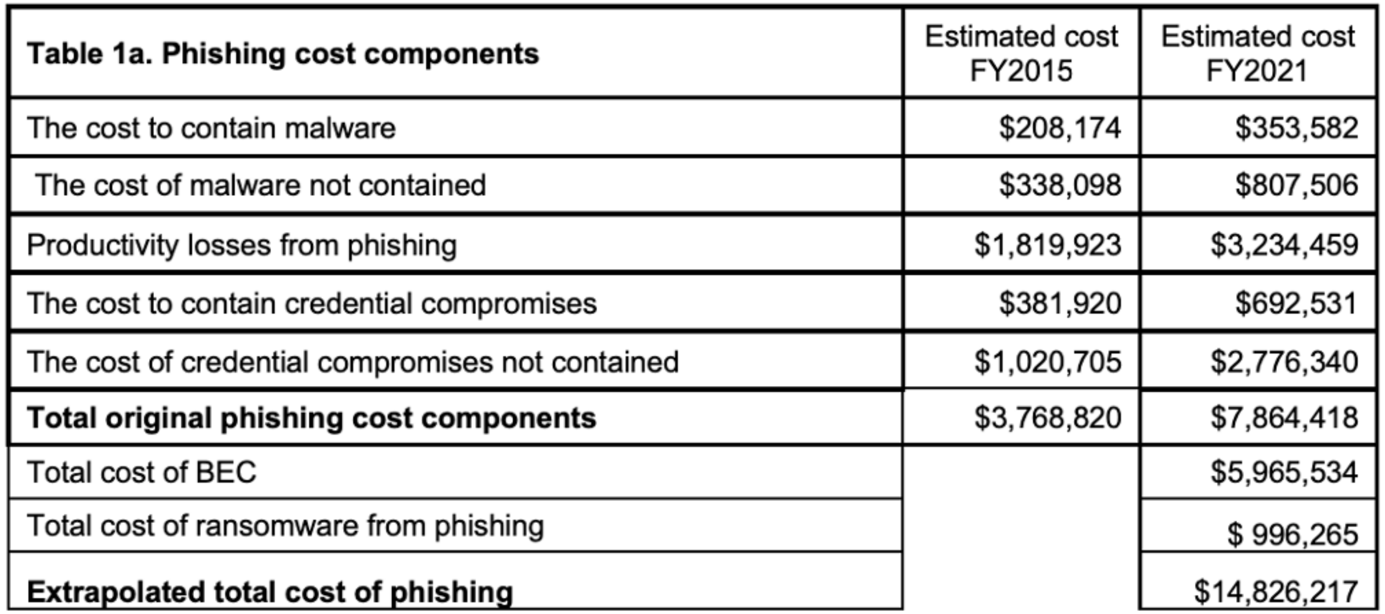
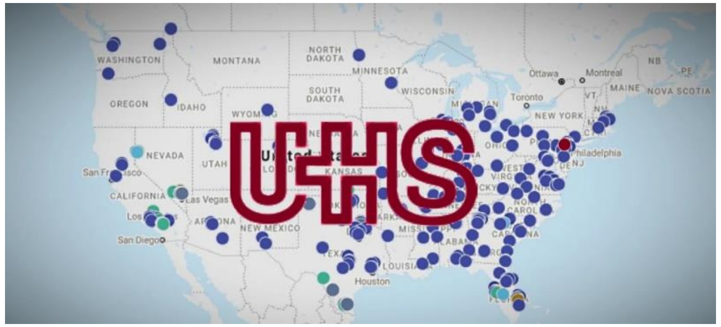


Table 1a. Phishing cost components	Estimated cost FY2015	Estimated cost FY2021
The cost to contain malware	$208,174	$353,582
The cost of malware not contained	$338,098	$807,506
Productivity losses from phishing	$1,819,923	$3,234,459
The cost to contain credential compromises	$381,920	$692,531
The cost of credential compromises not contained	$1,020,705	$2,776,340
Total original phishing cost components	$3,768,820	$7,864,418
Total cost of BEC		$5,965,534
Total cost of ransomware from phishing		$ 996,265
Extrapolated total cost of phishing		$14,826,217

Note: BEC = Business Email Compromise

Cybersecurity Ventures 2020; Google 2020; Ponemon Institute (2021)

Impact on People and Society



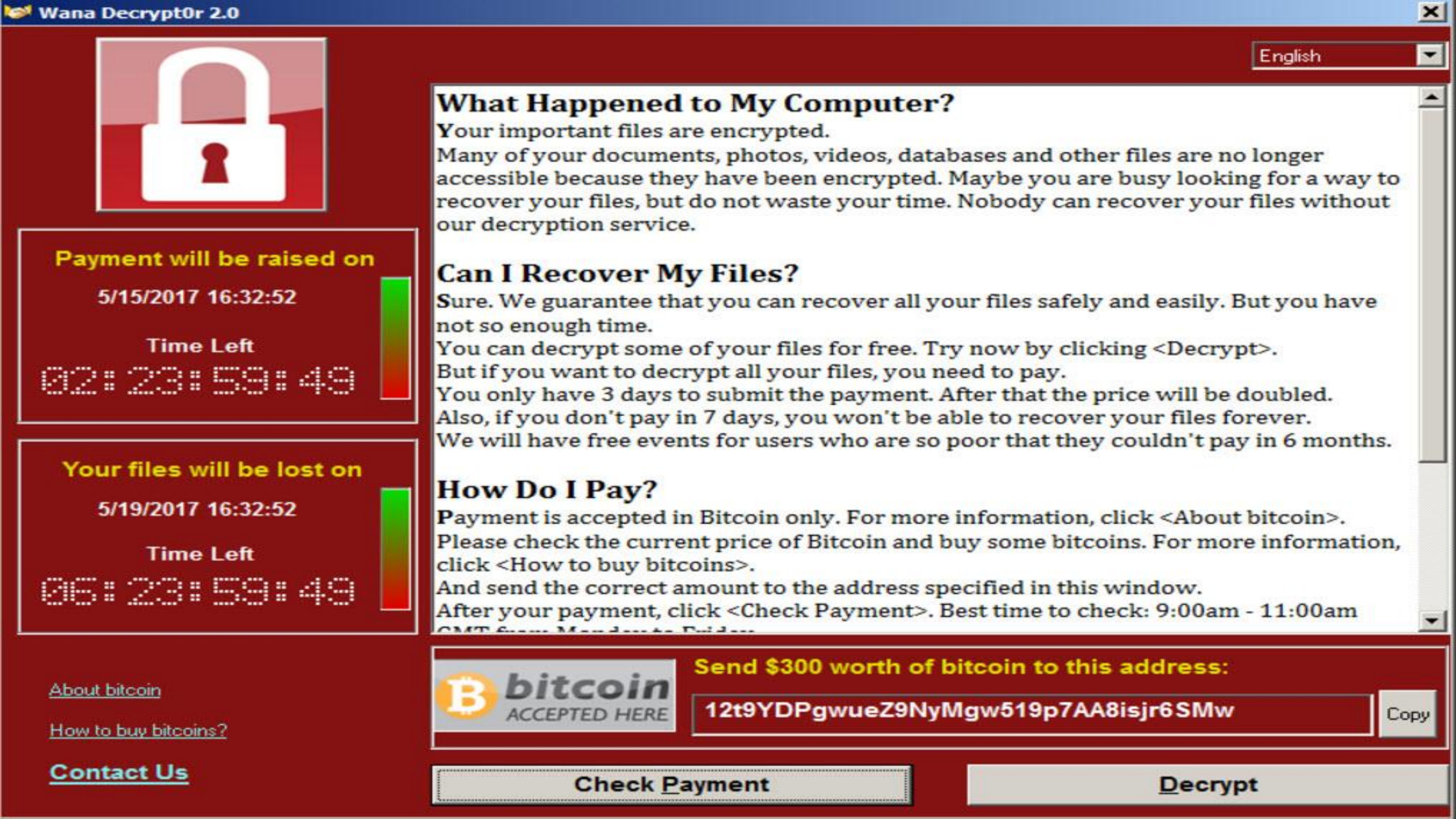
© picture-alliance/dpa/J. Güttler

Disturbances in public transportation

Threat to a hospital‘s ability to provide patient care

Potential manipulation of federal elections

...And many more. How do you think phishing impacts you?



Payment will be raised on

5/15/2017 16:32:52

Time Left

02:23:59:49

Your files will be lost on

5/19/2017 16:32:52

Time Left

06:23:59:49

What Happened to My Computer?

Your important files are encrypted.

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

Can I Recover My Files?

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

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

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

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

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

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

How Do I Pay?

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

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

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

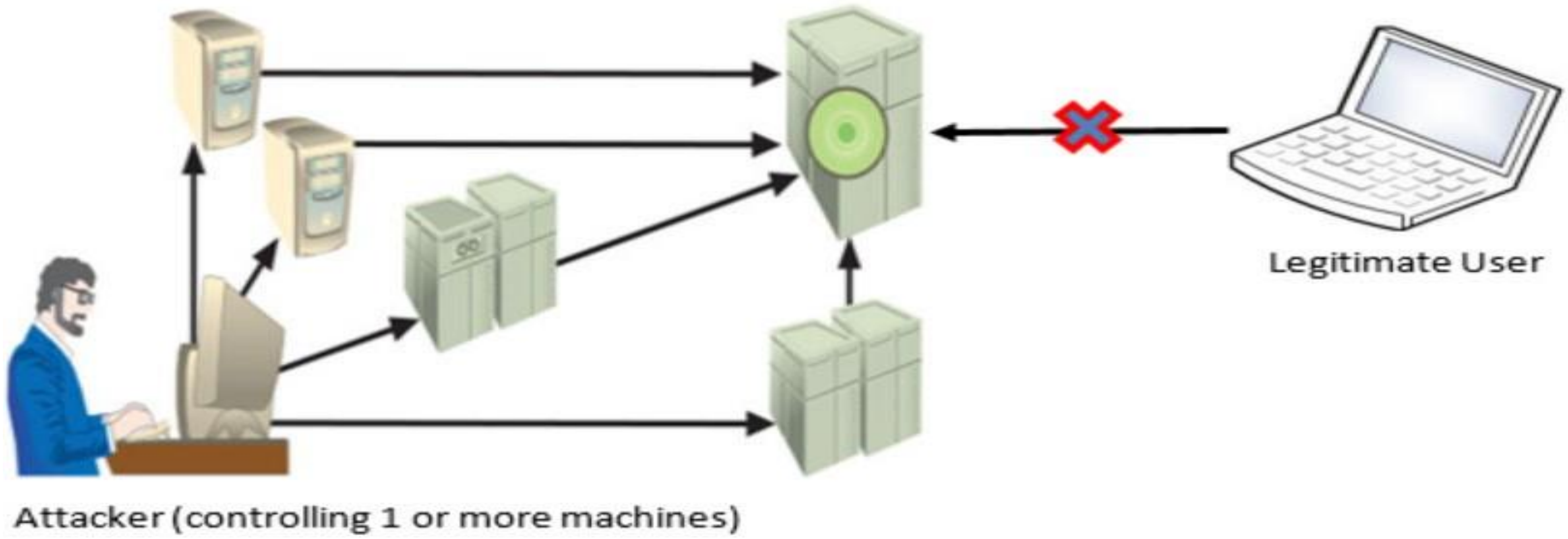
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Threat #5: Denial of Service

- **Denial-of-service (DoS):** attacker sends large number of connection or information requests to a target
  - Target system cannot handle successfully along with other, legitimate service requests
  - May result in system crash or inability to perform ordinary functions
- **Distributed denial-of-service (DDoS)**: coordinated stream of requests is launched against target from many locations (*zombies* or *bots* – compromised machines) simultaneously

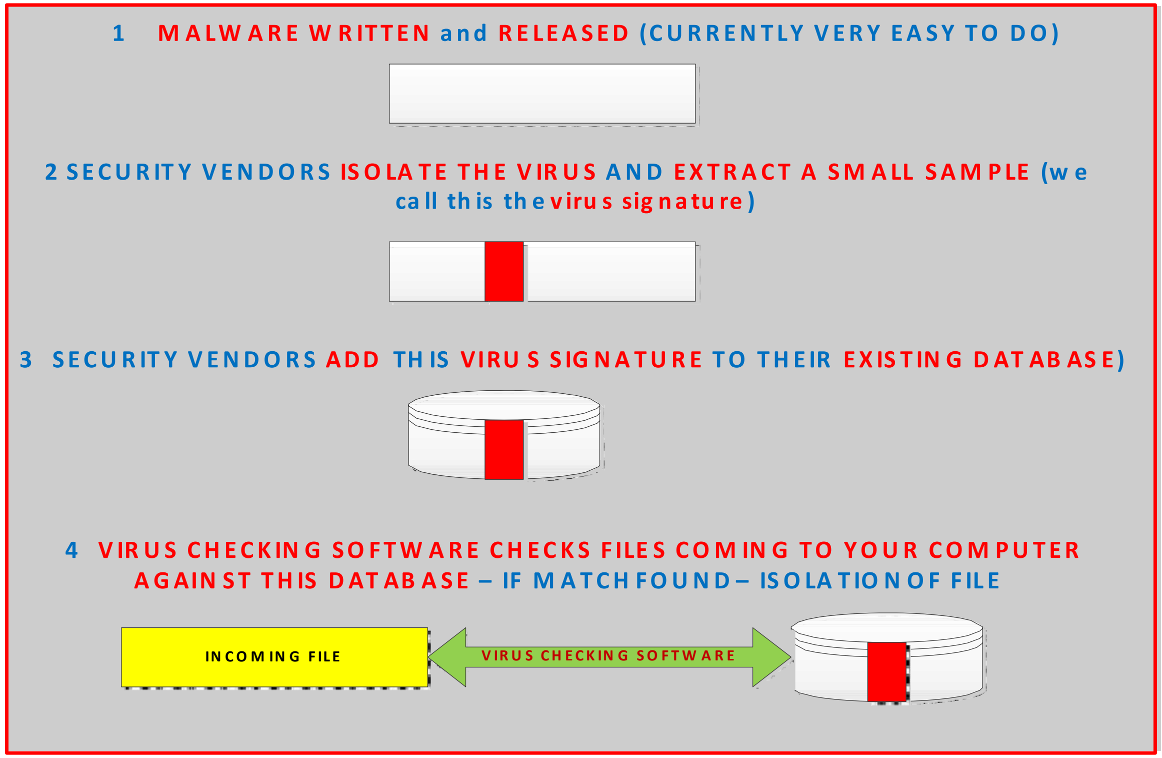


Threat #6: Deliberate Software Attacks

- **Malicious software (malware)** designed to damage, destroy, or deny service to target systems

- Includes the following malware attack vectors:
  - **Viruses & Worms** (self-replicating)
  - **Trojan horses & backdoors** (non-replicating)
  - **Logic bombs**
  - **Polymorphic threats**
  - **Worm hoaxes**

Malware Control Strategy (Generic)



1 MALWARE WRITTEN and RELEASED (CURRENTLY VERY EASY TO DO)

2 SECURITY VENDORS ISOLATE THE VIRUS AND EXTRACT A SMALL SAMPLE (we call this the virus signature)

3 SECURITY VENDORS ADD THIS VIRUS SIGNATURE TO THEIR EXISTING DATABASE)

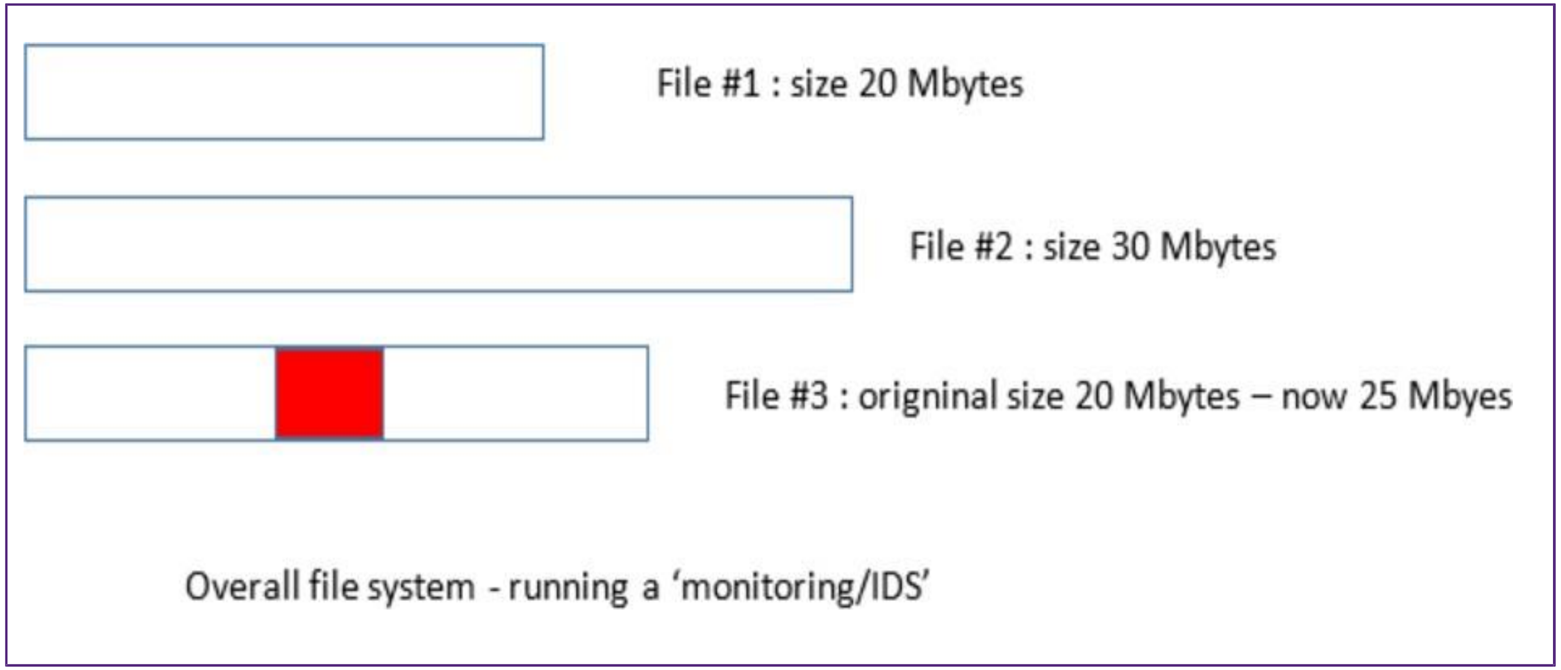
4 VIRUS CHECKING SOFTWARE CHECKS FILES COMING TO YOUR COMPUTER AGAINST THIS DATABASE – IF MATCH FOUND – ISOLATION OF FILE

INCOMING FILE

VIRUS CHECKING SOFTWARE

- This is essentially ‘**pattern matching**’ – there are obvious conclusions!
- If a virus comprises **NEW CODE**, it cannot be ‘caught’ in the above model **until it has been included in the SIGNATURE DATABASE**
- **If the SIGNATURE DATABASE is not kept up to date**, the control strategy quickly degrades.

Malware Control Strategy (more specific)



File #1 : size 20 Mbytes

File #2 : size 30 Mbytes

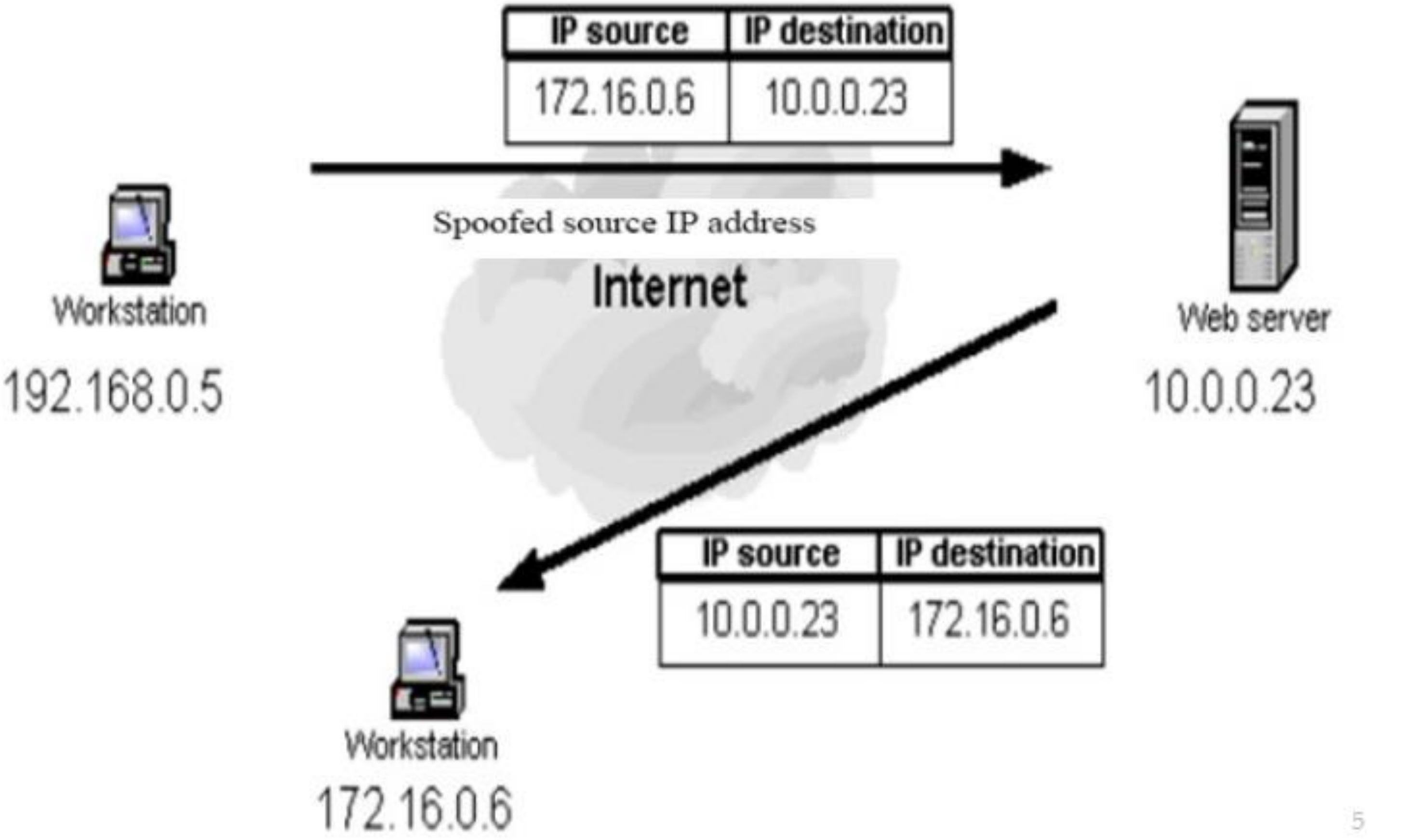
File #3 : orignal size 20 Mbytes – now 25 Mbyes

Overall file system - running a ‘monitoring/IDS’

- *We shall look later in the course at ‘Intrusion Detection Systems’ or IDS*
- There is one type of IDS that can monitor files systems – especially ‘critically important’ files within those systems
- **Any changes in those critical files – the IDS reports the ‘anomaly’ and this should then be investigated**.

Threat #7: IP Spoofing

Technique used to gain unauthorized access by replacing real IP address with a trusted IP address



IP source	IP destination
172.16.0.6	10.0.0.23

IP source	IP destination
10.0.0.23	172.16.0.6

Also caller ID spoofing: https://en.wikipedia.org/wiki/Caller_ID_spoofing

GPS position can also be spoofed.Tesla GPS hack: https://www.gpsworld.com/two-years-since-the-tesla-gps-hack/

GPS position spoofing

Scenario 1. Exiting the highway at the wrong location

Scenario 2. Enforcing an incorrect speed limit

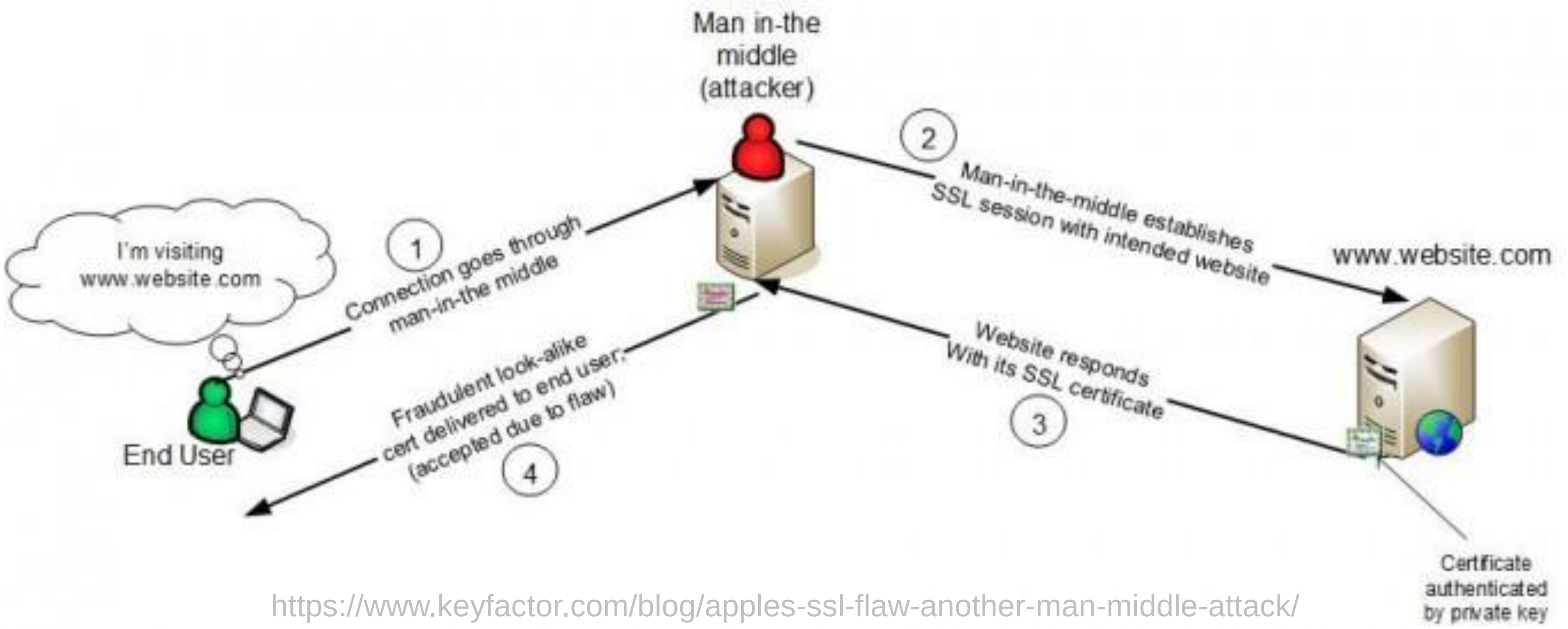
Scenario 3. Turning into incoming traffic

Tesla GPS hack: https://www.gpsworld.com/two-years-since-the-tesla-gps-hack/

Threat #8: Man-in-the-middle

Attacker monitors network packets, modifies them, and inserts them back into network

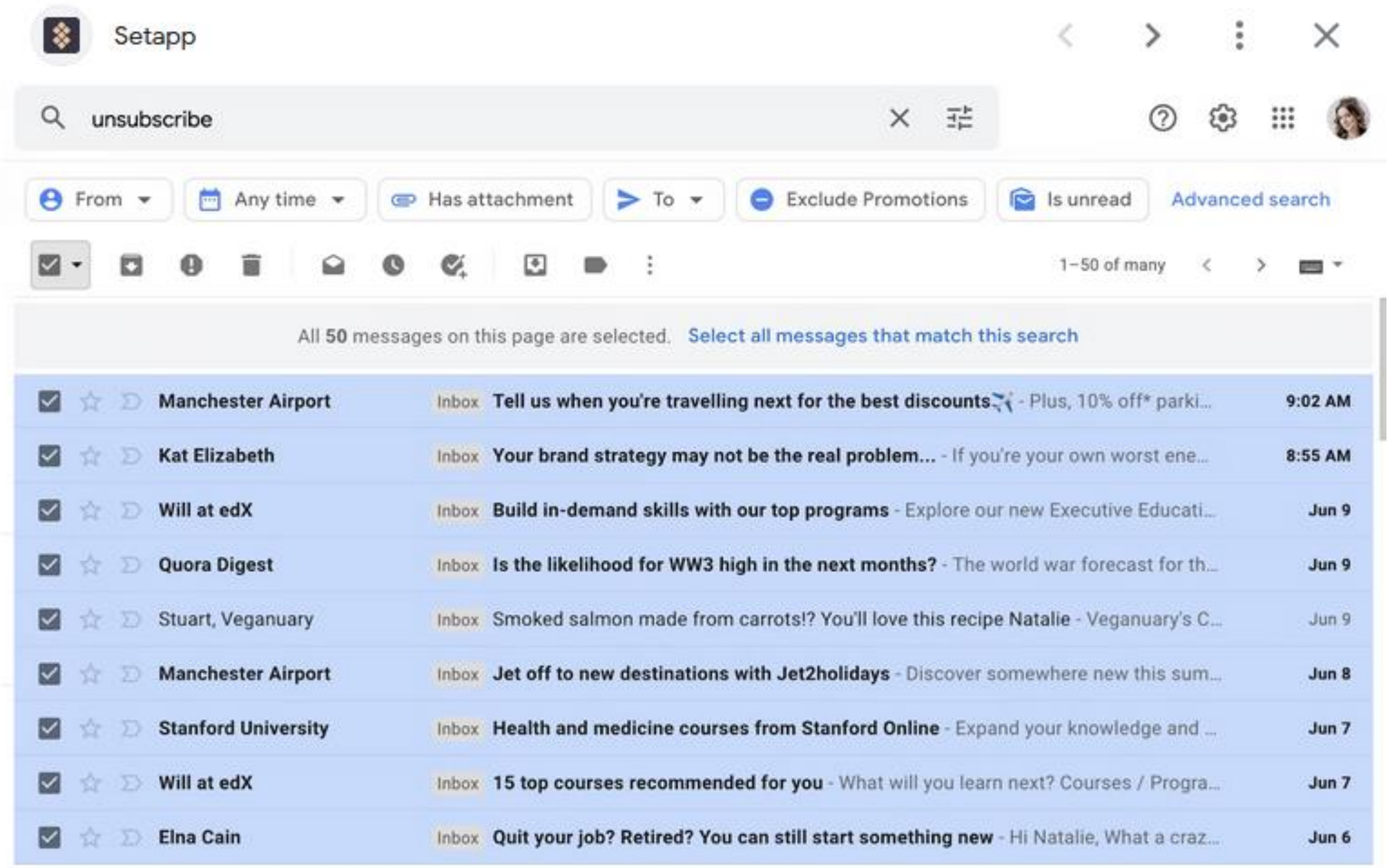
Example: Apple’s SSL Bug: Another Man-in-the-Middle Attack (February 22, 2014)


Man in-the middle (attacker)
I'm visiting www.website.com
End User
1
Connection goes through man-in-the middle
2
Man-in-the-middle establishes SSL session with intended website
www.website.com
3
Website responds With its SSL certificate
4
Fraudulent look-alike cert delivered to end user, (accepted due to flaw)
Certificate authenticated by private key

https://www.keyfactor.com/blog/apples-ssl-flaw-another-man-middle-attack/

Threat #9: Spam

Unsolicited commercial e-mail; more a nuisance than an attack, though is emerging as a vector for some attacks



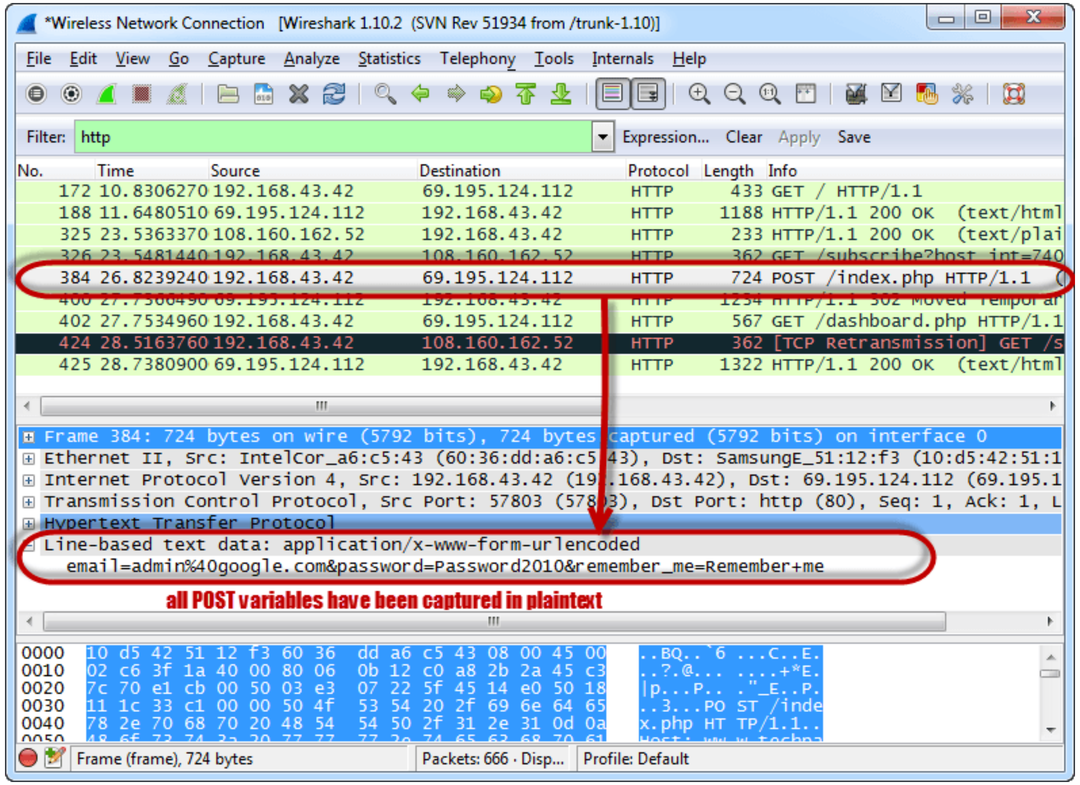
All **50** messages on this page are selected. Select all messages that match this search

Manchester Airport	Inbox	**Tell us when you're travelling next for the best discounts✈️** - Plus, 10% off* parki...	9:02 AM
Kat Elizabeth	Inbox	**Your brand strategy may not be the real problem...** - If you're your own worst ene...	8:55 AM
Will at edX	Inbox	**Build in-demand skills with our top programs** - Explore our new Executive Educati...	Jun 9
Quora Digest	Inbox	**Is the likelihood for WW3 high in the next months?** - The world war forecast for th...	Jun 9
Stuart, Veganuary	Inbox	Smoked salmon made from carrots!? You'll love this recipe Natalie - Veganuary's C...	Jun 9
Manchester Airport	Inbox	**Jet off to new destinations with Jet2holidays** - Discover somewhere new this sum...	Jun 8
Stanford University	Inbox	**Health and medicine courses from Stanford Online** - Expand your knowledge and ...	Jun 7
Will at edX	Inbox	**15 top courses recommended for you** - What will you learn next? Courses / Progra...	Jun 7
Elna Cain	Inbox	**Quit your job? Retired? You can still start something new** - Hi Natalie, What a craz...	Jun 6

Threat #10: Sniffer

Program or device that monitors data packets traveling over a network; can be used both for legitimate diagnostic purposes and for stealing information from a network

Download Network Sniffer *Wireshark* from here: https://www.wireshark.org/download.html


*Wireless Network Connection [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http
Expression... Clear Apply Save

```
No.    Time       Source          Destination      Protocol Length Info
   172 10.8306270 192.168.43.42   69.195.124.112   HTTP      433 GET / HTTP/1.1
   188 11.6480510 69.195.124.112  192.168.43.42    HTTP     1188 HTTP/1.1 200 OK  (text/html
   325 23.5363370 108.160.162.52  192.168.43.42    HTTP      233 HTTP/1.1 200 OK  (text/plai
   326 23.5481440 192.168.43.42   108.160.162.52   HTTP      362 GET /subscribe?host_int=740
   384 26.8239240 192.168.43.42   69.195.124.112   HTTP      724 POST /index.php HTTP/1.1  (
   400 27.7306490 69.195.124.112  192.168.43.42    HTTP     1234 HTTP/1.1 302 Moved Temporar
   402 27.7534960 192.168.43.42   69.195.124.112   HTTP      567 GET /dashboard.php HTTP/1.1
   424 28.5163760 192.168.43.42   108.160.162.52   HTTP      362 [TCP Retransmission] GET /s
   425 28.7380900 69.195.124.112  192.168.43.42    HTTP     1322 HTTP/1.1 200 OK  (text/html
```

```
⊞ Frame 384: 724 bytes on wire (5792 bits), 724 bytes captured (5792 bits) on interface 0
⊞ Ethernet II, Src: IntelCor_a6:c5:43 (60:36:dd:a6:c5:43), Dst: SamsungE_51:12:f3 (10:d5:42:51:1
⊞ Internet Protocol Version 4, Src: 192.168.43.42 (192.168.43.42), Dst: 69.195.124.112 (69.195.1
⊞ Transmission Control Protocol, Src Port: 57803 (57803), Dst Port: http (80), Seq: 1, Ack: 1, L
⊞ Hypertext Transfer Protocol
⊟ Line-based text data: application/x-www-form-urlencoded
    email=admin%40google.com&password=Password2010&remember_me=Remember+me
```

all POST variables have been captured in plaintext

```
0000  10 d5 42 51 12 f3 60 36  dd a6 c5 43 08 00 45 00   ..BQ..`6 ...C..E.
0010  02 c6 3f 1a 40 00 80 06  0b 12 c0 a8 2b 2a 45 c3   ..?.@... ....+*E.
0020  7c 70 e1 cb 00 50 03 e3  07 22 5f 45 14 e0 50 18   |p...P.. ."_E..P.
0030  11 1c 33 c1 00 00 50 4f  53 54 20 2f 69 6e 64 65   ..3...PO ST /inde
0040  78 2e 70 68 70 20 48 54  54 50 2f 31 2e 31 0d 0a   x.php HT TP/1.1..
```

Frame (frame), 724 bytes | Packets: 666 · Disp... | Profile: Default

Tutorial at: https://www.guru99.com/wireshark-passwords-sniffer.html

Global reports (1): 2021 SANS Cyber Threat Intelligence (CTI) survey

From Executive Summary of report – key takeaways:

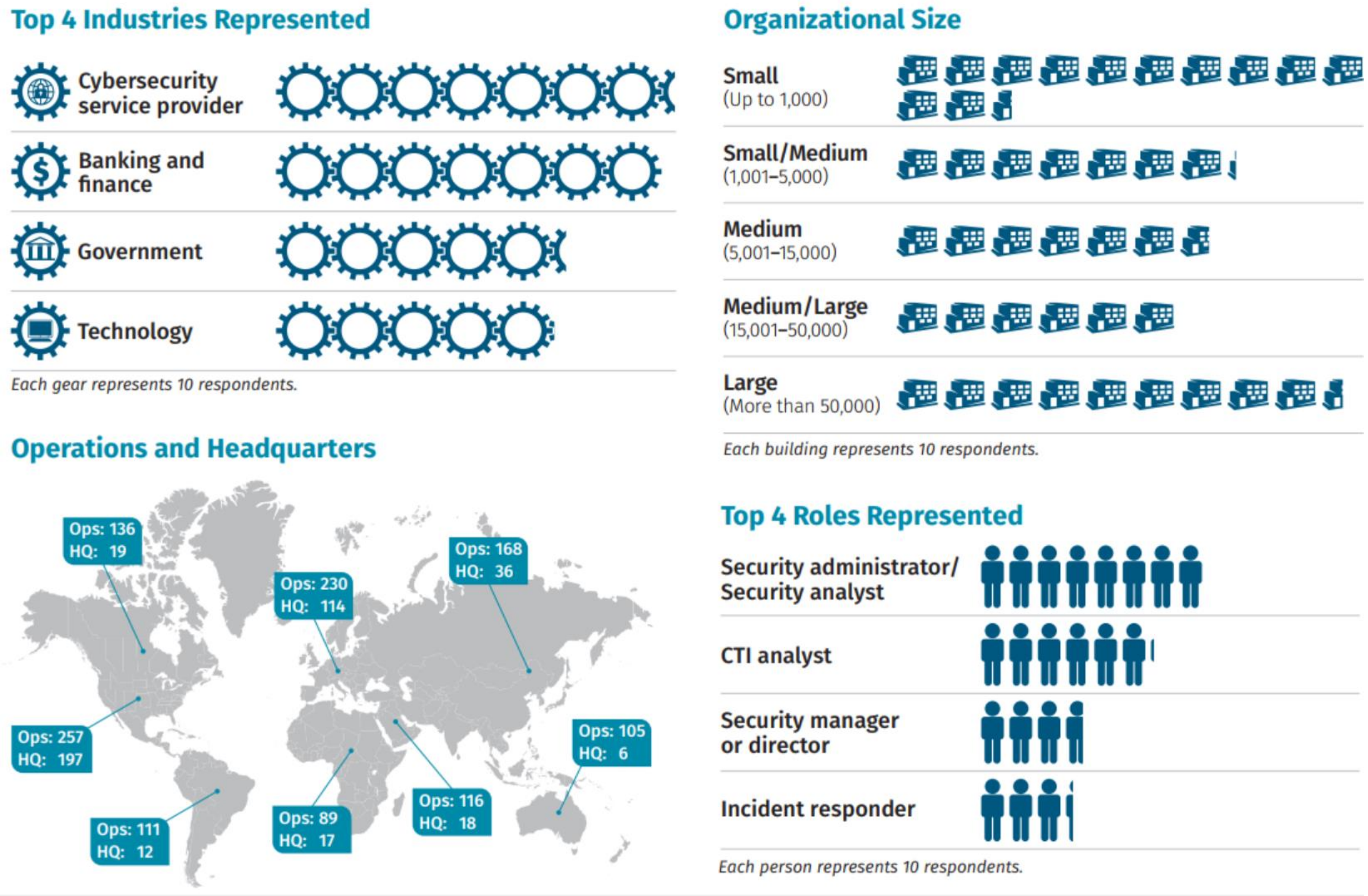
- **The way CTI analysts operate has changed due in large part to the coronavirus**
  - Analysts disseminate information more asynchronously (emails, dashboards) rather than in-person
  - Analysts work more on their own (home office!)
- **CTI is not just for the top 1% of organizations**
  - Increase of small organizations with CTI programs
  - CTI provides improved support for security at all levels and benefits organizations of all sizes
- **CTI tools are becoming more automated**
  - Analysts more time for higher-level analytic activities rather than repetitive collection and processing tasks
  - More information from government security bulletins and media reporting in analysis

SANS = System Administration, Networking and Security Institute

Global reports (1): 2021 SANS Cyber Threat Intelligence (CTI) survey

From page 3 of report:

The survey participants



Top 4 Industries Represented

Each gear represents 10 respondents.

Organizational Size

Each building represents 10 respondents.

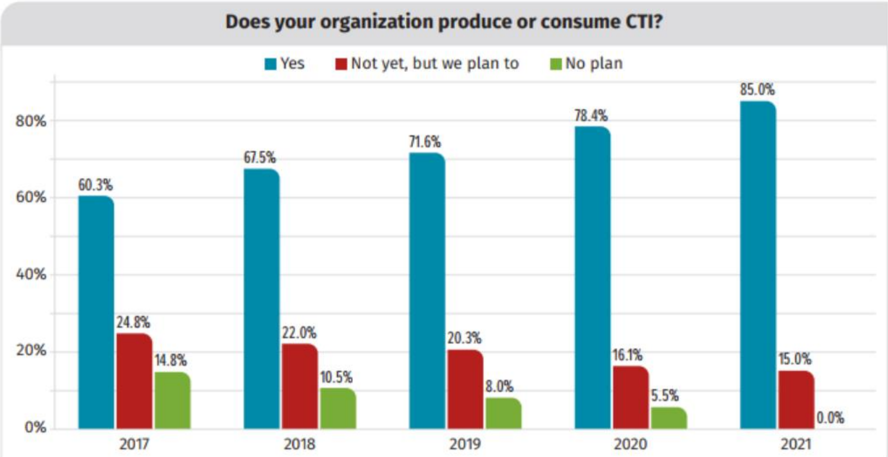
Operations and Headquarters

Top 4 Roles Represented

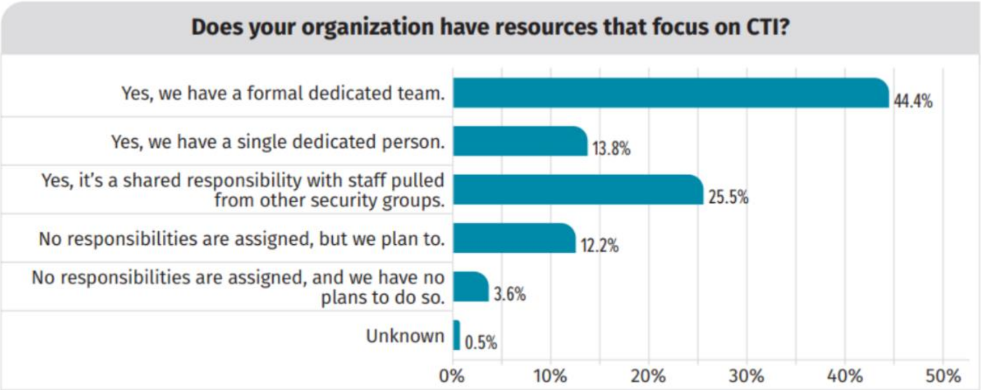
Each person represents 10 respondents.

Global reports (1): 2021 SANS Cyber Threat Intelligence (CTI) survey

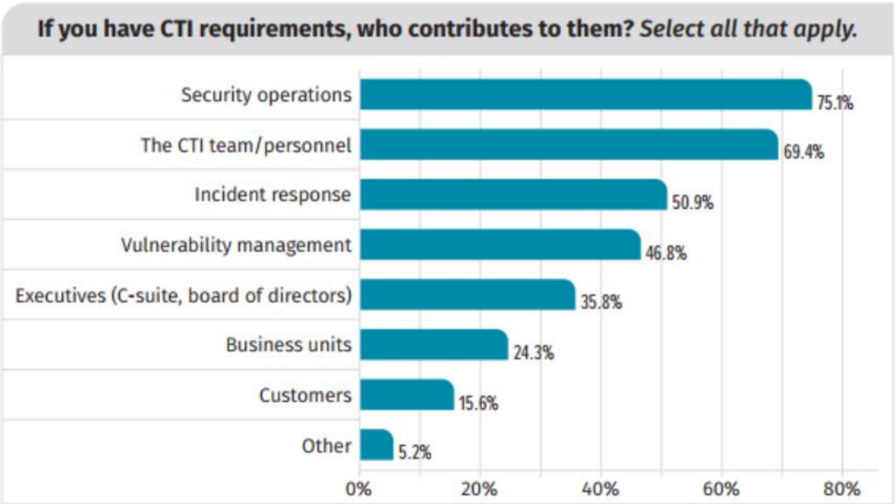
From the report: Some questions



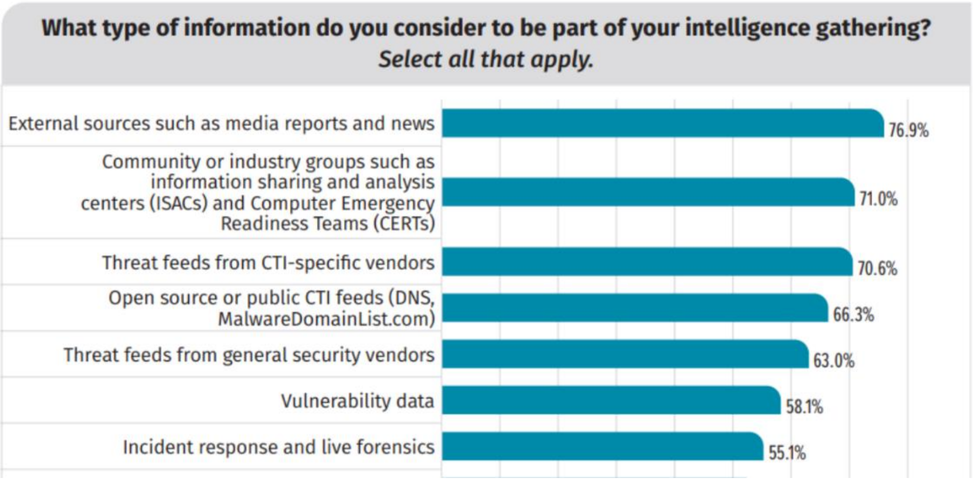
Does your organization produce or consume CTI?



Does your organization have resources that focus on CTI?



If you have CTI requirements, who contributes to them? *Select all that apply.*

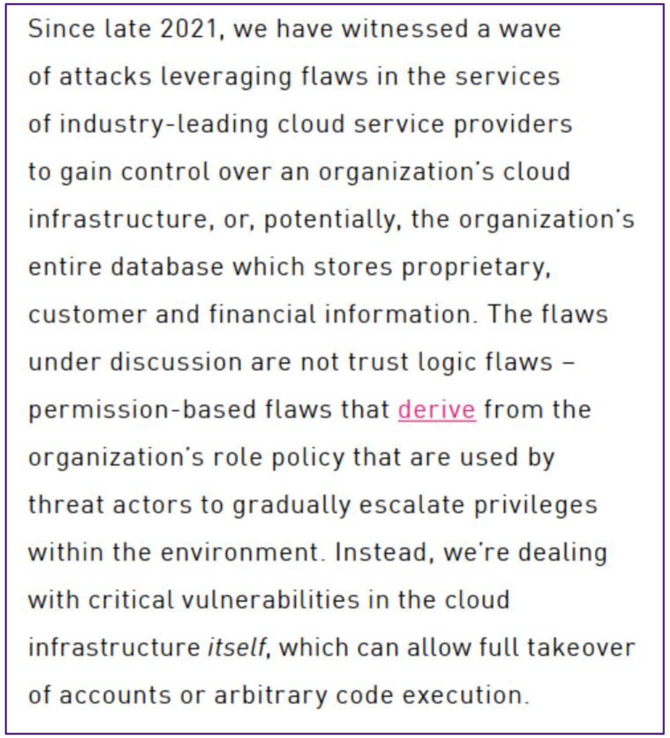


What type of information do you consider to be part of your intelligence gathering? *Select all that apply.*

Global reports (2): Check Point 2022 Cyber Security Report

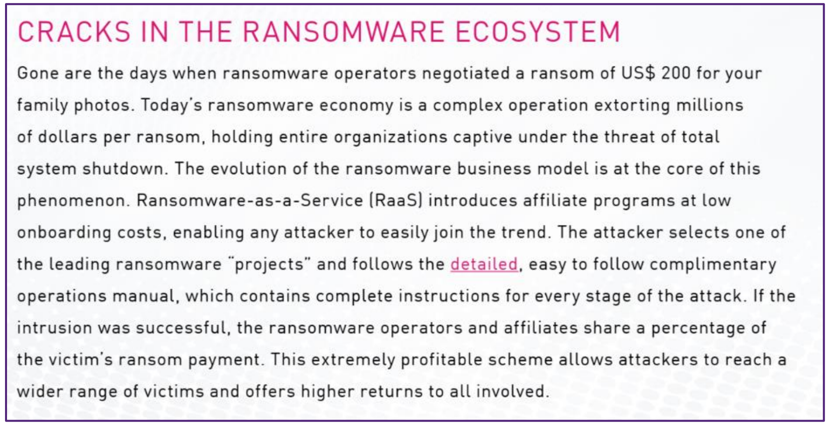
(Check Point is an American-Israeli multinational provider of software and combined hardware and software products for IT security.

Cloud services under attack (p. 21)



Since late 2021, we have witnessed a wave of attacks leveraging flaws in the services of industry-leading cloud service providers to gain control over an organization's cloud infrastructure, or, potentially, the organization's entire database which stores proprietary, customer and financial information. The flaws under discussion are not trust logic flaws – permission-based flaws that derive from the organization's role policy that are used by threat actors to gradually escalate privileges within the environment. Instead, we're dealing with critical vulnerabilities in the cloud infrastructure *itself*, which can allow full takeover of accounts or arbitrary code execution.

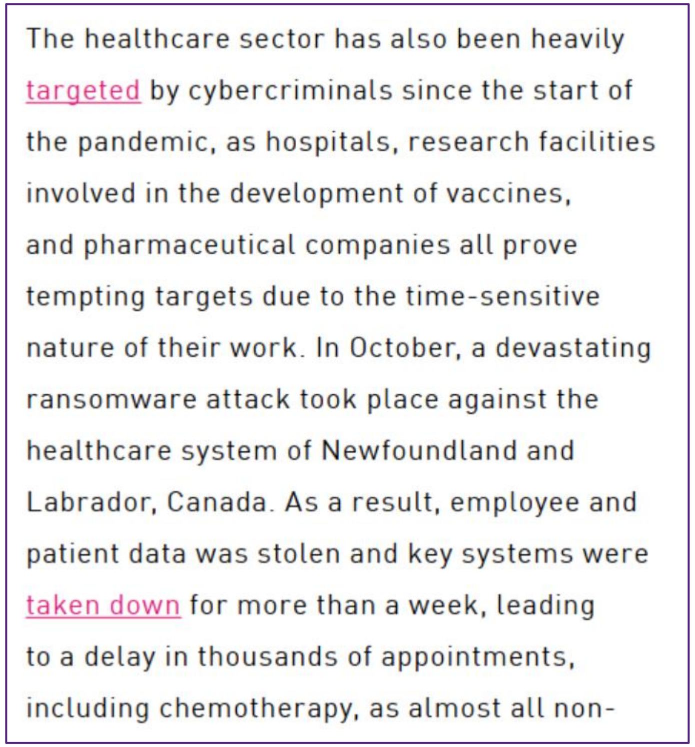
Ransomware-as-a-Service (RaaS) (p. 28)



CRACKS IN THE RANSOMWARE ECOSYSTEM

Gone are the days when ransomware operators negotiated a ransom of US$ 200 for your family photos. Today's ransomware economy is a complex operation extorting millions of dollars per ransom, holding entire organizations captive under the threat of total system shutdown. The evolution of the ransomware business model is at the core of this phenomenon. Ransomware-as-a-Service (RaaS) introduces affiliate programs at low onboarding costs, enabling any attacker to easily join the trend. The attacker selects one of the leading ransomware "projects" and follows the detailed, easy to follow complimentary operations manual, which contains complete instructions for every stage of the attack. If the intrusion was successful, the ransomware operators and affiliates share a percentage of the victim's ransom payment. This extremely profitable scheme allows attackers to reach a wider range of victims and offers higher returns to all involved.

Healthcare sector under attack (p. 19)



The healthcare sector has also been heavily targeted by cybercriminals since the start of the pandemic, as hospitals, research facilities involved in the development of vaccines, and pharmaceutical companies all prove tempting targets due to the time-sensitive nature of their work. In October, a devastating ransomware attack took place against the healthcare system of Newfoundland and Labrador, Canada. As a result, employee and patient data was stolen and key systems were taken down for more than a week, leading to a delay in thousands of appointments, including chemotherapy, as almost all non-

Summary (Part 1)

- Information security performs **four important functions** to ensure information assets remain safe and useful
- **Management must be informed about threats** to its people, applications, data, and information systems, and the attacks they face.
  - Threats**:** any events or circumstances that have the potential to adversely affect operations and assets.
  - Attack**:** an intentional or unintentional act that can damage or otherwise compromise information and the systems that support it.
  - Vulnerability**:** a potential weakness in an asset or its defensive controls.
- Threats can fall into 10 categories *(Note: we did not cover all of them today, see also textbook)*
  - *Important to remember*: internal/external origin; malicious/accidental origin

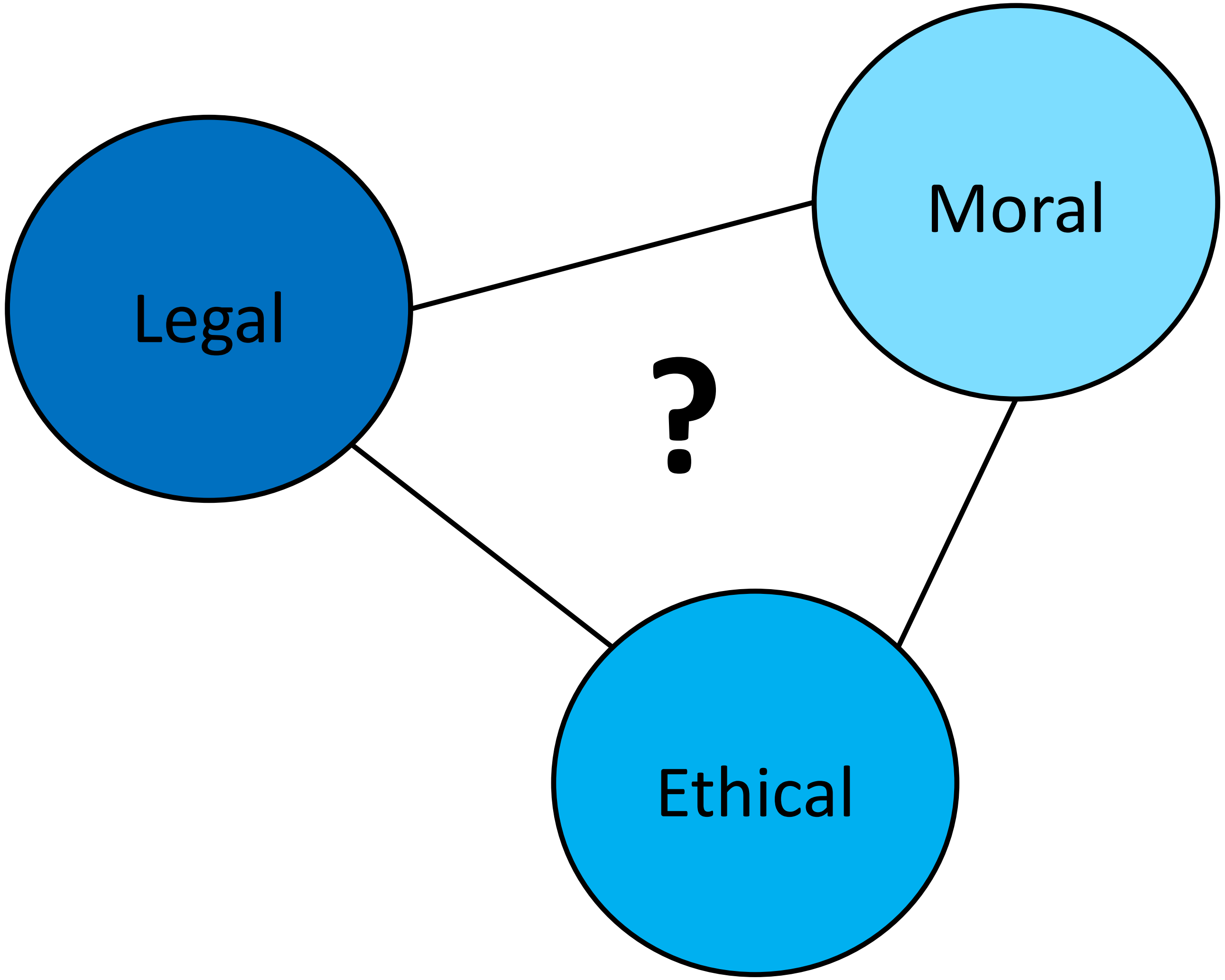
Ethics

The branch of philosophy that involves systematizing, defending, and recommending concepts of right and wrong conduct.

http://en.wikipedia.org/wiki/Ethics

Ethics
Not just “Good vs. Evil”

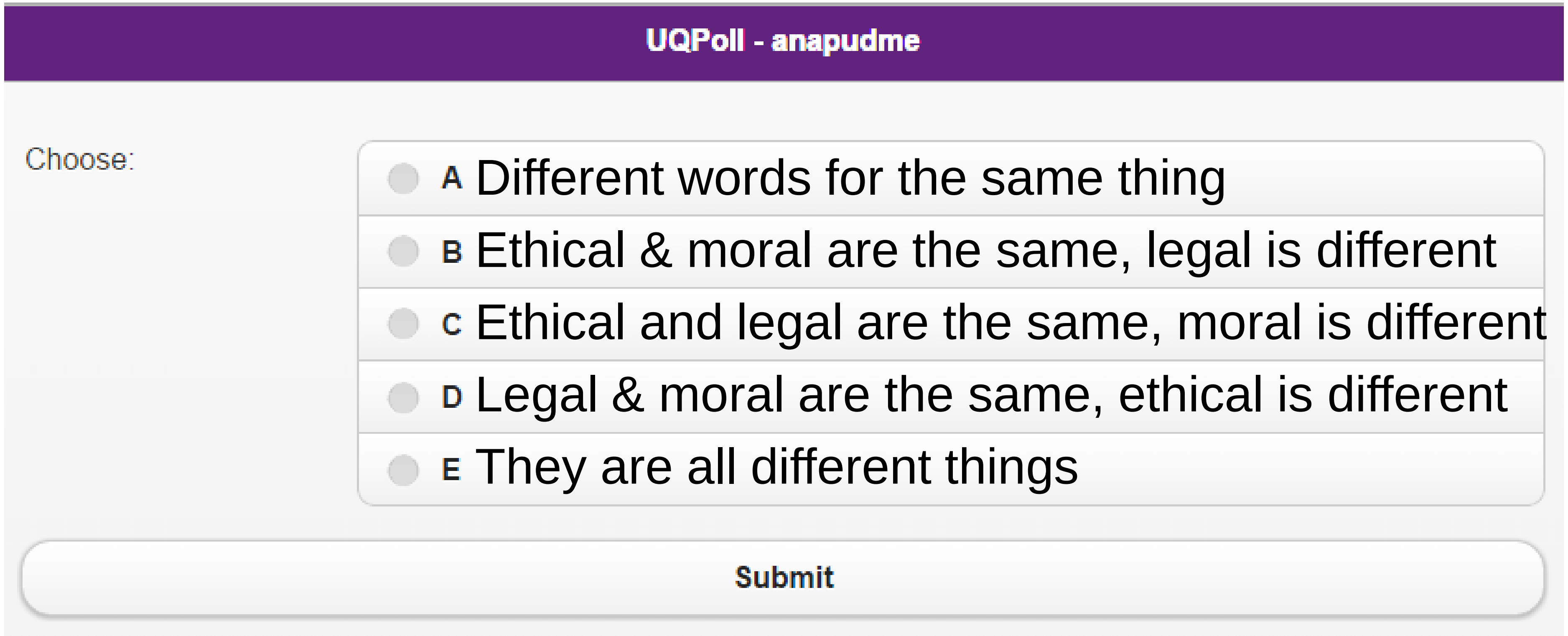
What is their relationship?



Navigate to this URL in your browser please to submit your answer:

apps.elearning.uq.edu.au/poll/71682

What is the difference between: Ethical, moral and legal?



UQPoll - anapudme

Choose:

- ○ A Different words for the same thing
- ○ B Ethical & moral are the same, legal is different
- ○ C Ethical and legal are the same, moral is different
- ○ D Legal & moral are the same, ethical is different
- ○ E They are all different things

Moral vs. Ethical

Morals define personal character, while **ethics** stress a social system in which those **morals** are applied.

In other words, **ethics** point to standards or codes of behaviour expected by the group to which the individual belongs (national ethics, social ethics, company ethics, professional ethics, family ethics). So while a person’s **moral** code is usually unchanging, the **ethics** he or she practices can be other-dependent.

Legal vs. Ethical

Legality is a society's application of **ethics** to the structure of society.

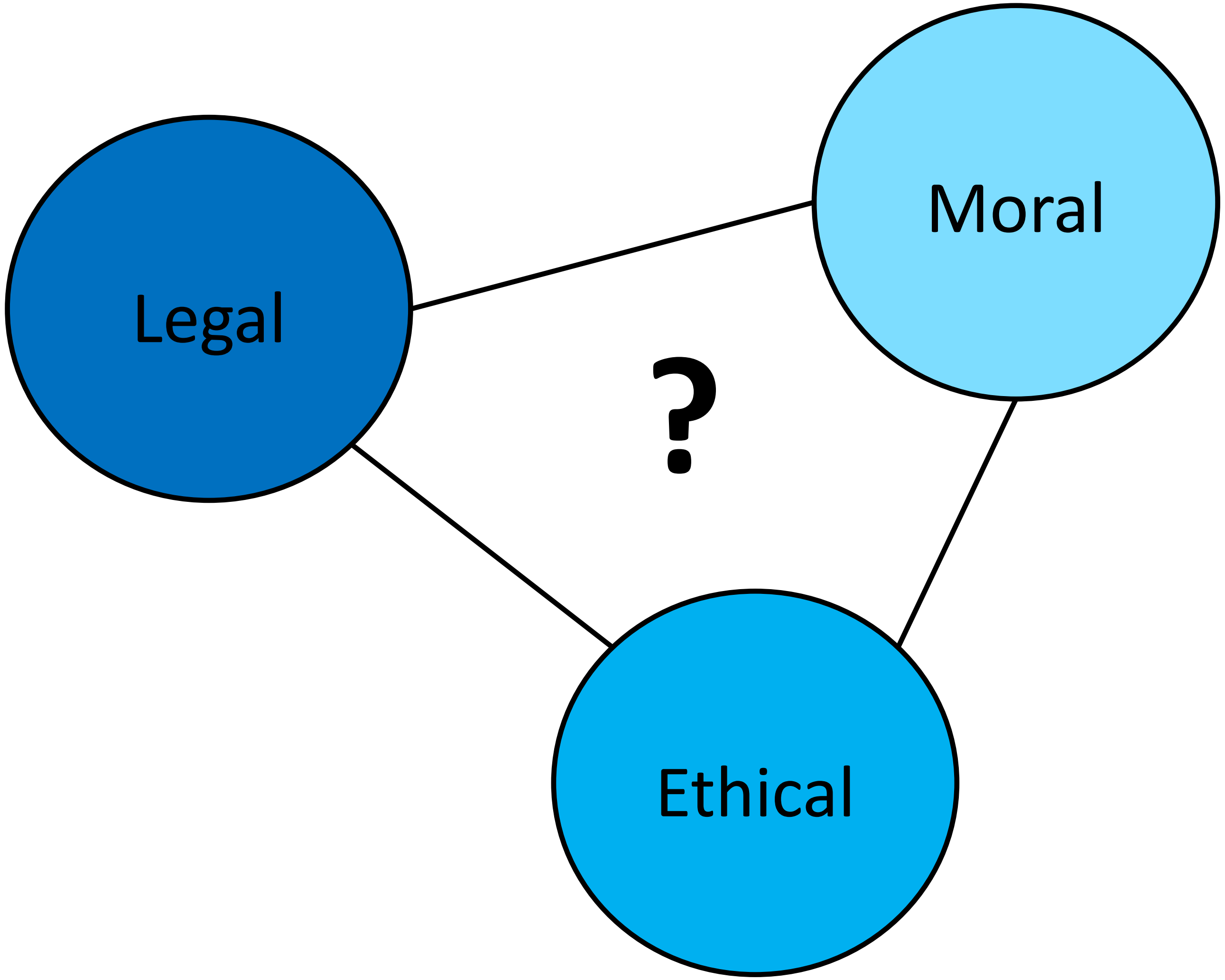
An act is **legal** if it complies to governing laws and regulations whereas an act is also **ethical** if it complies to **ethical** policies of an organisation and it is also **moral** if it is correct in your opinion.

Example:

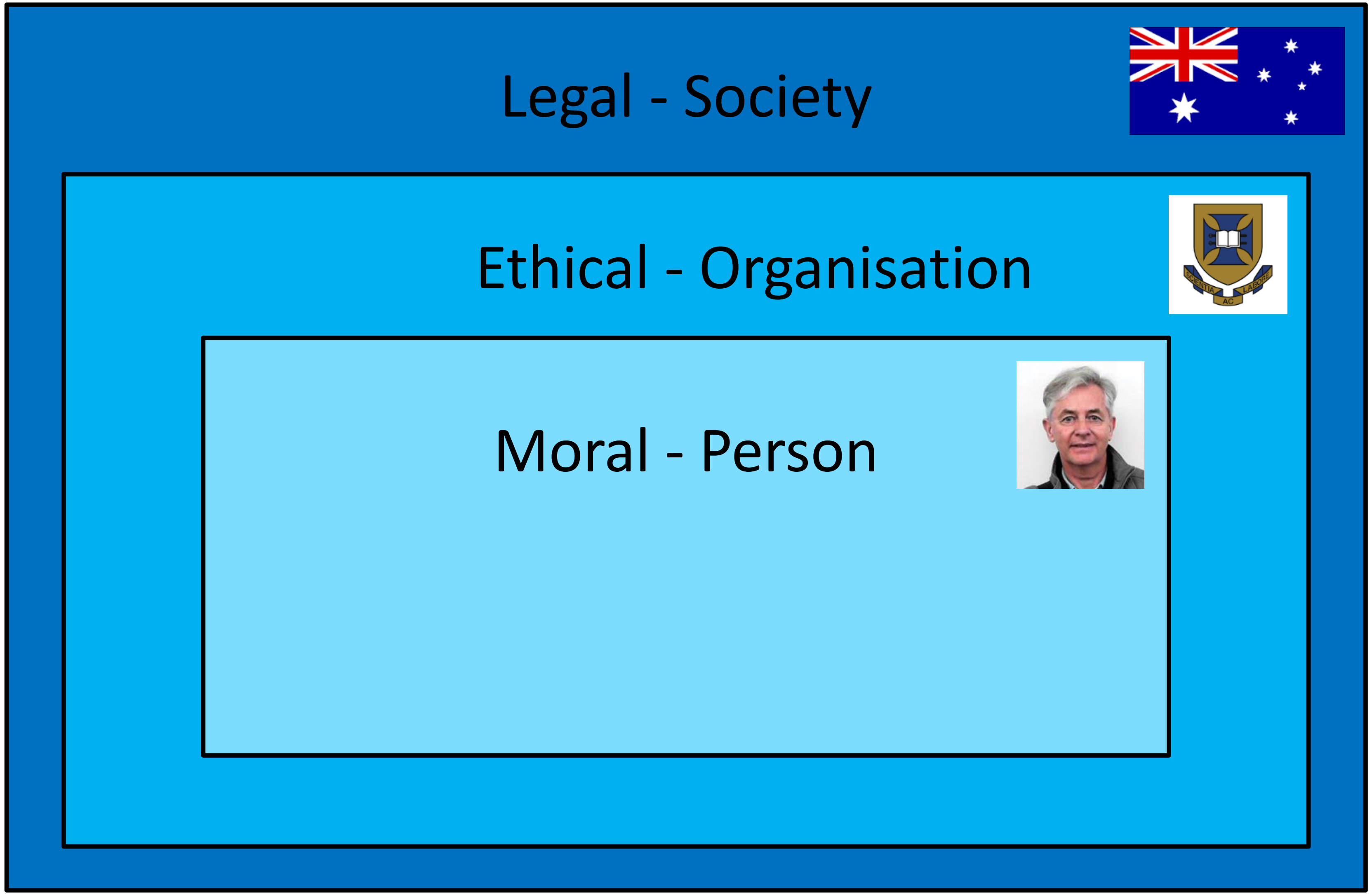
Abortion is **legal*** and therefore medically **ethical**, while many people find it personally **immoral**.

* If necessary to preserve the woman from a serious danger to her life or health - different state laws apply in Australia (http://en.wikipedia.org/wiki/Abortion_in_Australia).

Solution: ?



Solution: Nested levels



Legal - Society

Ethical - Organisation

Moral - Person

Why do we talk about “Ethics”?

Most of us, day to day, have a firm ethical compass

So why talk about ethics at all?

Essentially, it’s not always clear, particularly in technology work, what is ‘right’ or ‘wrong’ in a particular situation

Professional ethics provides frameworks to support ethical decisions in uncertain scenarios

Ethics and Standards Bodies

Professional Societies providing ethical standards documents:

- The Australian Computer Society (ACS) has a Code of Ethics
- Engineers Australia (EA) has a Code of Ethics
- Australian Institute of Computer Ethics (AICE) runs conferences and discussion groups on ethical topics
- The Australian Institute of Project Management (AIPM) has a Code of Ethics and Professional Conduct
- APES 110 Code of Ethics for Professional Accountants†

† https://www.cpaaustralia.com.au/professional-resources/accounting-professional-and-ethical-standards/apes-110-code-of-ethics-for-professional-accountants

The Australian Computer Society (ACS)[†]

“The ACS was established in 1966 as a result of the merger of then existing State based computer societies. It has become the recognised association for IT professionals, attracting a large and active membership from all levels of the IT industry, and providing a wide range of services and opportunities for networking and career enhancement.

It is the public voice of the IT professional; the guardian of professional ethics and standards in IT; with a commitment to the wider community to ensure the beneficial use of IT.”

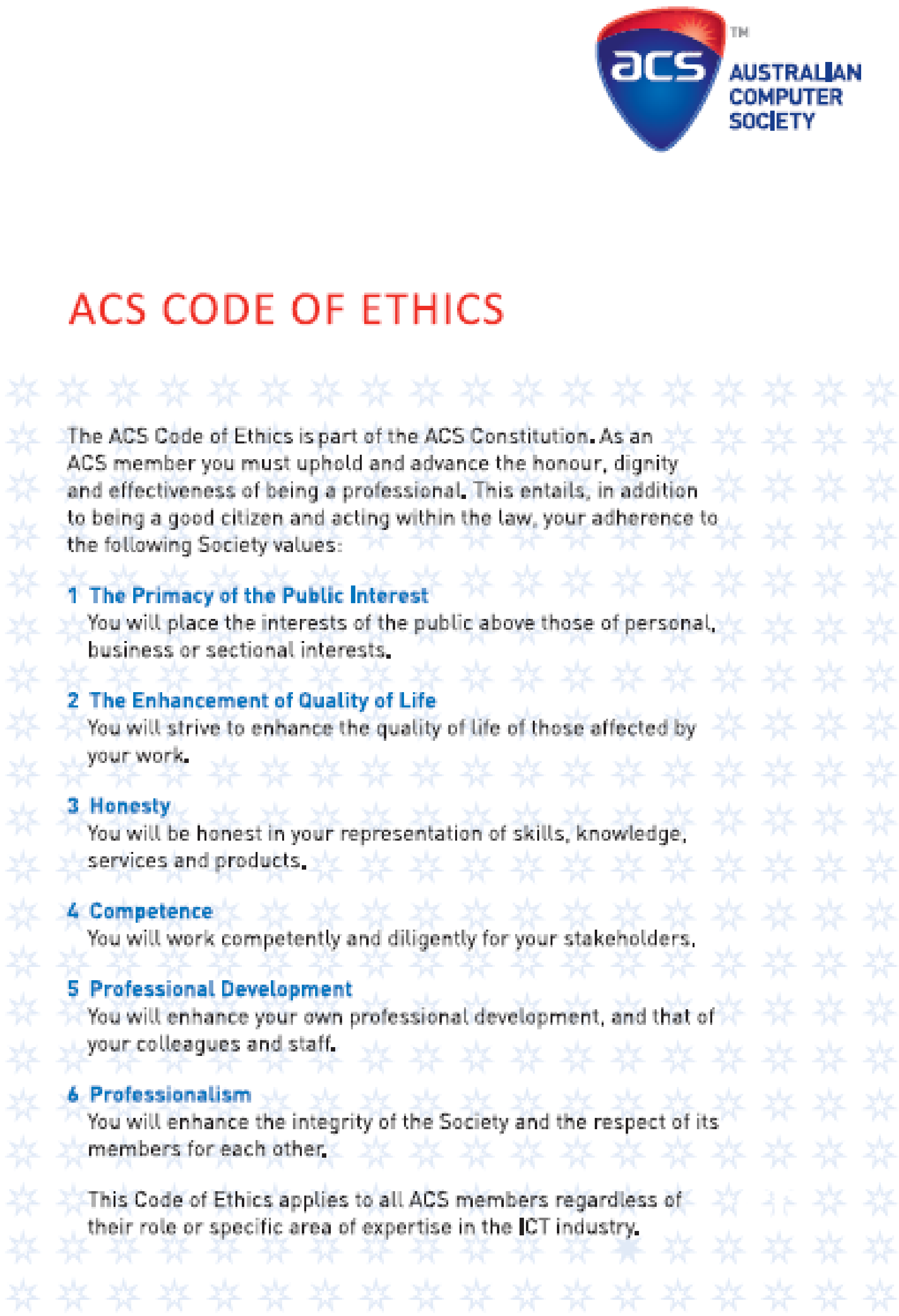
[†] https://www.acs.org.au/

ACS and Ethics

The Australian Computer Society Code of Ethics

The code is part of the Society's Regulations

The Society requires its members to subscribe to a set of values and ideals which uphold and advance the honor, dignity and effectiveness of the profession of information technology



AUSTRALIAN COMPUTER SOCIETY

ACS CODE OF ETHICS

The ACS Code of Ethics is part of the ACS Constitution. As an ACS member you must uphold and advance the honour, dignity and effectiveness of being a professional. This entails, in addition to being a good citizen and acting within the law, your adherence to the following Society values:

1 **The Primacy of the Public Interest**
You will place the interests of the public above those of personal, business or sectional interests.

2 **The Enhancement of Quality of Life**
You will strive to enhance the quality of life of those affected by your work.

3 **Honesty**
You will be honest in your representation of skills, knowledge, services and products.

4 **Competence**
You will work competently and diligently for your stakeholders.

5 **Professional Development**
You will enhance your own professional development, and that of your colleagues and staff.

6 **Professionalism**
You will enhance the integrity of the Society and the respect of its members for each other.

This Code of Ethics applies to all ACS members regardless of their role or specific area of expertise in the ICT industry.

https://www.acs.org.au/content/dam/acs/rules-and-regulations/Code-of-Ethics.pdf

ACS Code of Ethics

- It is a standard of behaviour
- Not exhaustive
- Is meant to be illustrative
- Written in terms of specific behaviour
- May conflict with standards from other sources
- The delineation between ethical and unethical has some element of subjectivity
- Members are expected to take into consideration the spirit of the code in resolving contentious issues

Policy, Law and Ethics in Information Security

- **Policies**: Most organizations develop and formalize a body of management views/expectations called policy. Policies serve as organizational laws – the view of management.
- To be enforceable, policy must be **distributed**, **readily available**, **easily understood**, and **acknowledged by employees** – **and assessed from a legal viewpoint**.

- The **Code of Ethics** provides a framework for ethical decision-making, while policies provide specific guidance on how to implement that framework in practice.

Privacy

- One of the hottest topics in information security:
- Privacy is a “*state of being free from unsanctioned intrusion*”

- Ability to aggregate data from multiple sources allows creation of information databases previously unheard of
- Many types of privacy issues: spamming, fraud, government intrusion.

- Information Privacy: ”***the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others*”.**

(Alan Westin – Columbia University 1967)

- Is *privacy* the same as *confidentiality*?

iPhone Privacy Ad

https://www.youtube.com/watch?v=FbRUQRmvC4U

iPhone Privacy

In 2016, the Federal Bureau of Investigation (FBI) asked Apple to help them unlock the iPhone of one of the San Bernardino shooters, who had killed 14 people in a terrorist attack. The FBI was unable to access the phone's data due to its strong encryption and the passcode protection. The agency requested that Apple create a new version of its iOS software that would bypass the iPhone's security features and allow the FBI to access the data.

Apple refused to comply with the request, stating that creating such a software would undermine the security and privacy of all iPhone users. The company argued that once such a tool was created, it would be nearly impossible to keep it from falling into the wrong hands and being used for malicious purposes.
The case quickly became a highly publicized legal battle between Apple and the US government. The FBI eventually dropped the case after finding a third-party solution to access the iPhone's data, but the incident sparked a wider debate over the balance between national security and individual privacy.

Apple's refusal to create a backdoor to the iPhone's security features has since been hailed by privacy advocates as a victory for digital rights, while some law enforcement officials have criticized the move as hindering their ability to prevent and investigate criminal activities.

In comparison: TOLA Act in Australia

In 2018, the Australian government passed the Telecommunications and Other Legislation Amendment (TOLA) Act, which requires technology companies to provide law enforcement and security agencies with access to encrypted communications when requested.

The law has been criticized by privacy advocates, who argue that it undermines the security and privacy of users and could potentially weaken overall cybersecurity.

See ***GOING-DARK-Kopsias.pdf*** on Blackboard.

Australian IT/Privacy Law

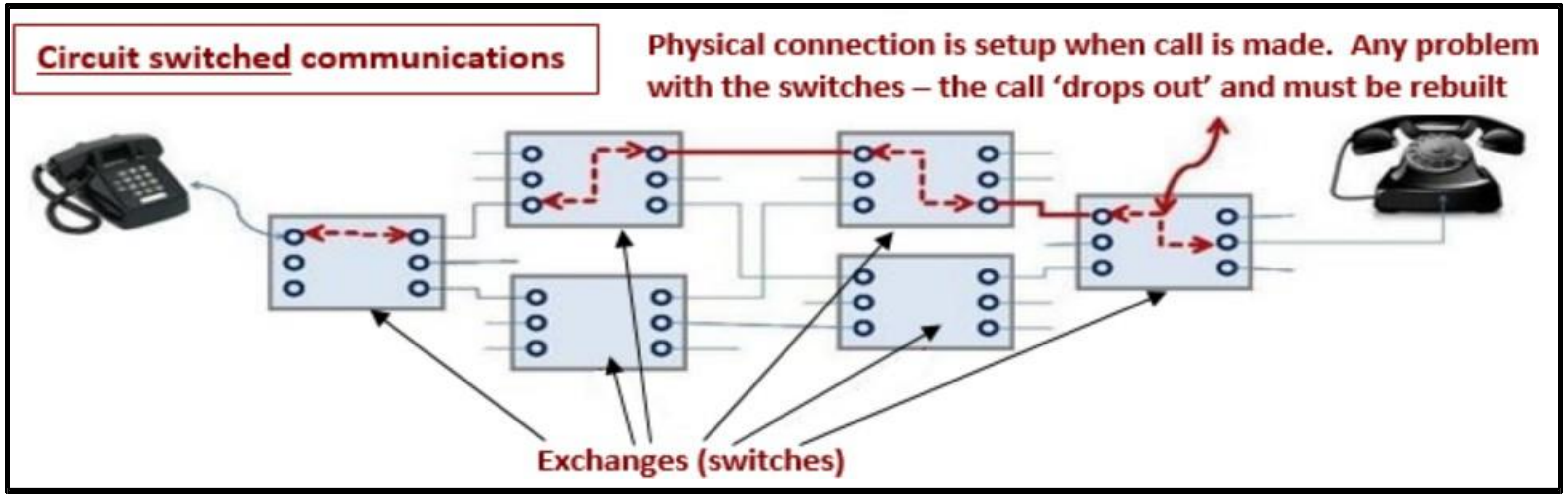
- **Telecommunications Act 1997:**
  - Prohibits breaches of privacy in telecoms traffic. Exemptions made for police – with judicial approval – obligations on internet service providers (ISPs)
- **Cybercrime Act 2001:**
  - Unauthorised access, modification or impairment with intent to commit a serious offence (Section 477), Possession or control of data with intent to commit a computer offence (Section 478), Producing, supplying or obtaining data with intent to commit a computer offence (Section 478)
- **Spam Act 2003:**
  - Three steps (**Consent, Identity, Unsubscription**)
- **Privacy Act 1988:**
  - 10 principles: Collection, Use and disclosure, Data quality, Data Security, Openness, Access and correction, Identifiers, Anonymity, **Transborder data flows**, Sensitive information.
  - Targets public sector. **Private sector coverage introduced in 2001.**
- **Privacy Amendment (Notifiable Data Breaches) Act 2017:**
  - Established the NDB scheme in Australia - applies to all agencies and organisations with existing personal information security obligations under the Australian *Privacy Act 1988* (Privacy Act) **from 22 February 2018**.
- **TOLA (Access and Assistance) Bill 2018**
  - "Going dark" – *see next slides*
- **Surveillance Legislation Amendment (Identify and Disrupt) Bill 2021**
  - Extends TOLA bill – "Unprecedented powers for online surveillance, data interception and **altering data**"

    passed both houses of the Australian Parliament on 25 August 2021 and is now known as the **Surveillance Legislation Amendment (Identify and Disrupt) Act 2021.**

"the decryption laws"

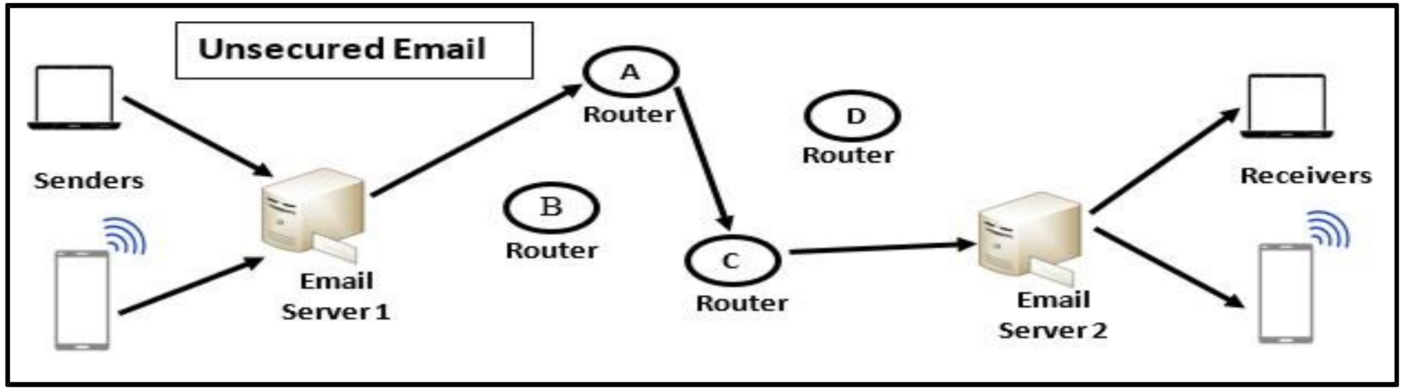
“Going Dark” #1

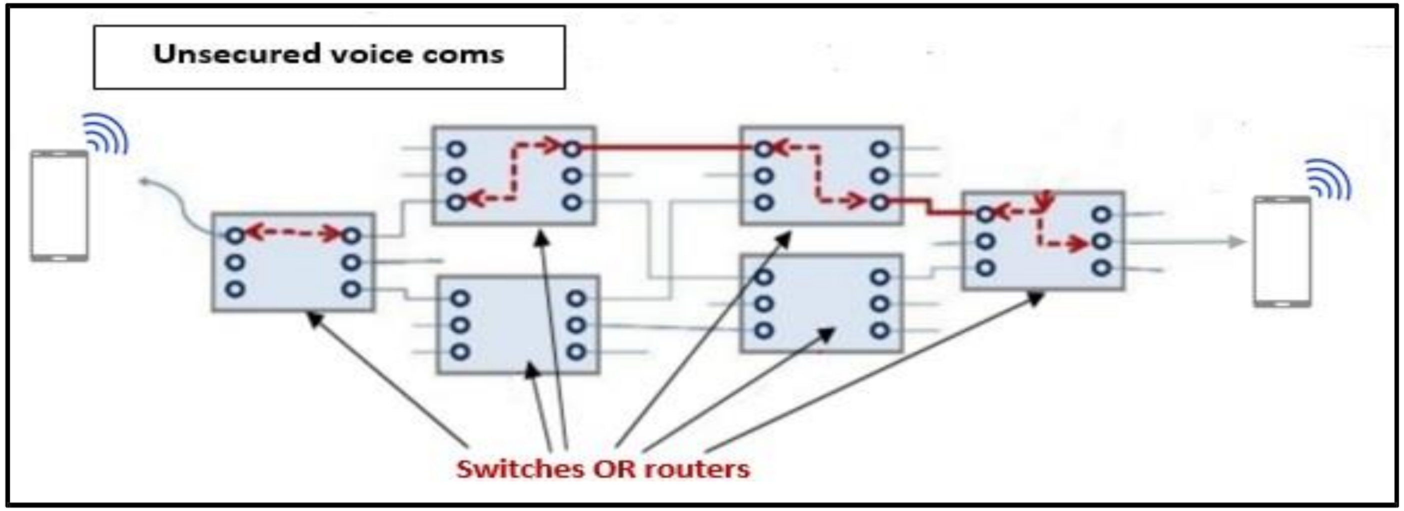
- **<u>Traditional ‘person-to-person</u>’** communications – who could access the communicated ‘information’?
- Traditionally, these (telephone) communications (telephone and ‘snail mail’) have allowed police/law enforcement to ‘listen-in’ (*<u>subject to judicial approval</u>*)


Circuit switched communications
Physical connection is setup when call is made. Any problem with the switches – the call ‘drops out’ and must be rebuilt
Exchanges (switches)

“Going Dark” #2

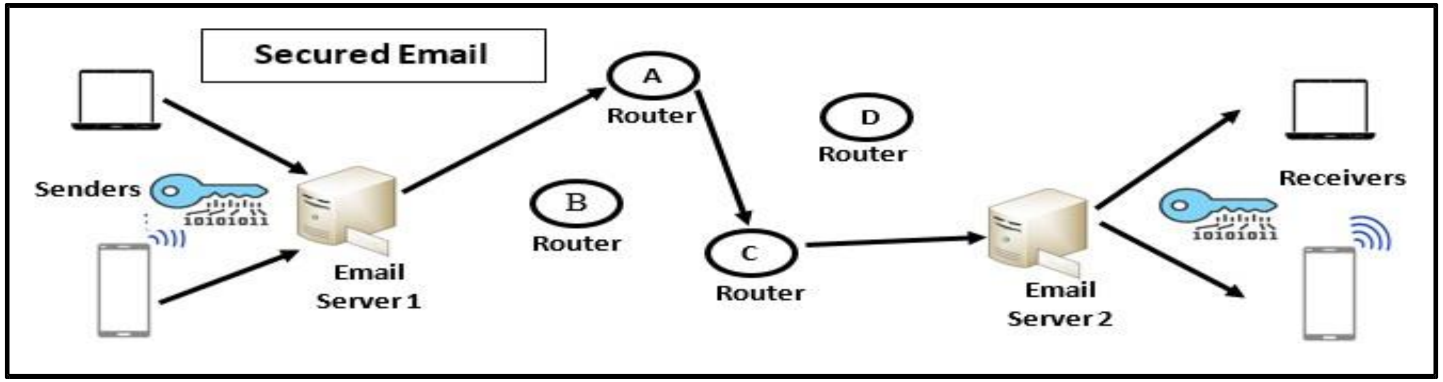
- **Modern unsecured ‘person-to-person’** communications – who can access the communicated ‘information’?
- Email – can be copied at work or in private (with judicial approval). Work calls can be monitored (at work) and can be monitored in private (with judicial approval)

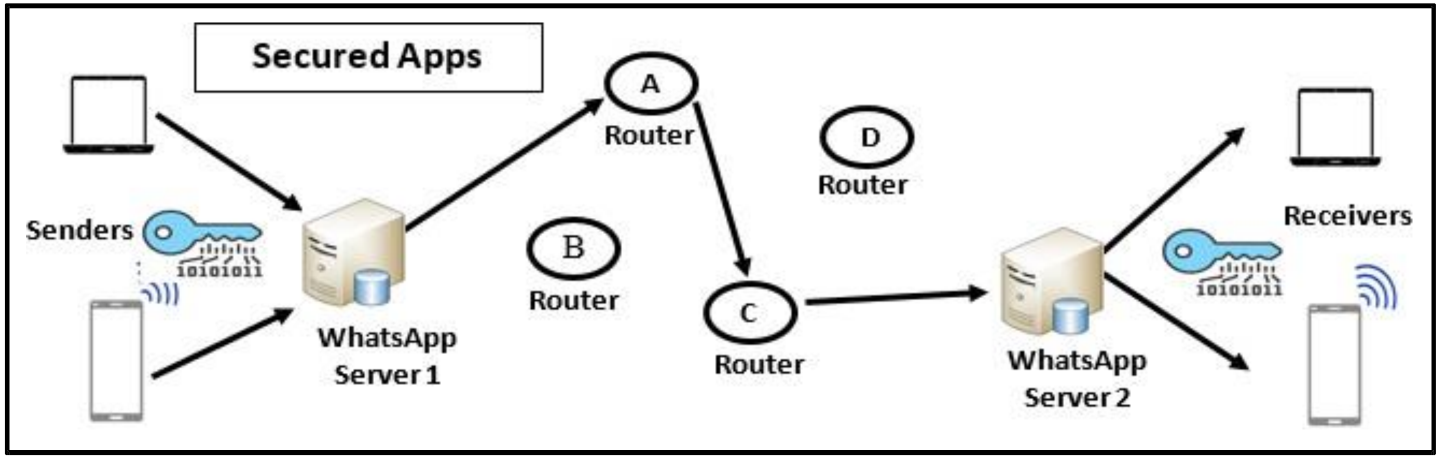




“Going Dark” #3

- **<u>Modern secured ‘person-to-person</u>**’ communications – who can access the communicated ‘information’?
- Secure email, secure digital apps (e.g. WhatsApp) <u>cannot</u> (in theory) <u>be copied at any intermediate point</u> (‘end-to-end’ communication). This is quite different to routine ‘secured’ digital communications (e.g. between me and my bank – *this is explained later in the course in some detail*)

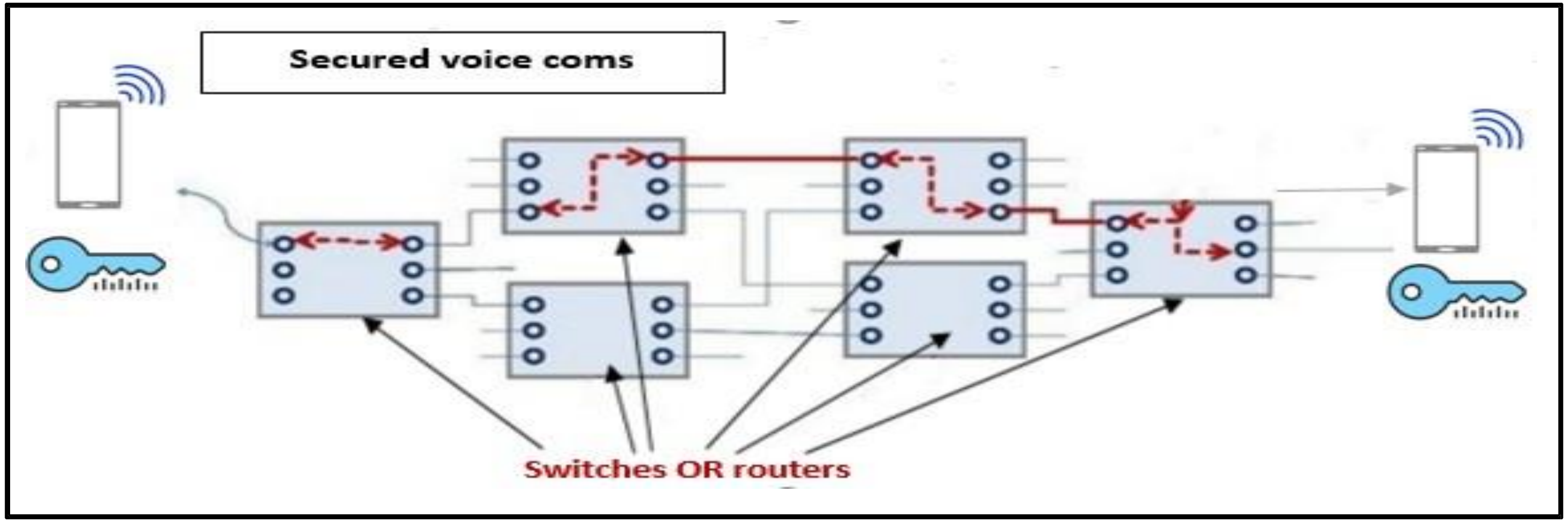




Some services use Transport Layer Security (TLS) to encrypt email messages in transit between servers. Some email services also offer end-to-end encryption, which encrypts the content of the email message from the sender's device all the way to the recipient's device, so that only the sender and recipient can read the message.

"Going Dark" #4

- **<u>Modern secured 'person-to-person</u>**' communications – who can access the communicated 'information'?
- Secure telephony <u>cannot</u> (in theory) <u>be copied at any intermediate point</u> ('end-to- end' communication)



‘**Going dark**’ – a term first introduced by the FBI (US)

- Short paper: *‘Going dark’: the unprecedented government measures to access encrypted data* – Arthur Kopsias – Feb, 2019 (**On course Blackboard site)**

“The greatest benefit of encryption also creates the biggest problem. Secure, encrypted communications are being used by terrorist groups and organised criminals to avoid detection, and the inability of law enforcement agencies to read or even partially understand encrypted communications has presented real challenges for these agencies worldwide.”

- The trust created by secure communications is essential for digital business.
- ‘End-to-end’ encryption – incorporated into **email** two decades ago
- ‘End-to-end’ encryption – since approximately 2015 incorporated into **mobile telephony services** and various **apps**. This has been developed into a very powerful marketing concept by corporate communication companies *(see video from Apple on next slide)*
- Over 90 percent of telecommunications information being lawfully intercepted by the Australian Federal Police now uses some form of encryption.
- End to end security (i.e. digital privacy) now a very significant marketing discourse for the corporate telcos

‘**Going dark**’ – Australian government response

The Telecommunications and Other Legislation Amendment Act 2018 (TOLA Act)

- Also known as the Assistance and Access Act 2018
- Became law on 8 December 2018 – first law of its type! *(but not the last!)*

- TOLA is an attempt to counter the ‘***going dark***’ problem faced by Australian law enforcement agencies

- **TOLA creates a new operational framework for Australian law agencies seeking access to data and content held by designated communications providers within or outside the Australian jurisdiction.**

- TOLA has implications for the operation of the US CLOUD Act 2018. This US law enables US federal law enforcement to compel US-based technology companies via warrant or subpoena to provide requested data stored on servers regardless of whether the data are stored in the U.S. or on foreign soil.

TOLA Act – overview – it is designed to be ‘cooperative’

- Schedule 1 of the TOLA Act inserts a new ‘**Industry Assistance**’ section into the Telecommunications Act 1997.
  - A new operational protocol by which Carriers/Carriage Service Providers (‘**CSP**s’) will provide assistance to law enforcement and security agencies.

- This ‘Industry Assistance’ framework contains three distinct new powers which allow an agency head to issue:
  - ‘**technical assistance request**’ (TAR) for voluntary assistance from the CSP
  - ‘**technical assistance notice**’ (TAN) for compulsory assistance from the CSP – this power is used in cases where the CSP is already capable of providing the assistance.
  - ‘**technical capability notice**’ (TCN) for new capabilities. This notice can only be used by the Australian Attorney-General and requires a CSP to create a specific capability where the CSP is not currently able to assist.

TOLA Act – overview – carriers/carriage service providers

- The term ‘Carriers/Carriage service providers (CSPs)’ is broadly defined in the Act so that it includes the wide range of entities integral to the 21st century Australian communications operational environment. The main descriptors are as follows:
  - CSPs that are based in Australia, and those providers based offshore who operate or supply communications services, devices or products for use within Australia.
  - Anyone who facilitates the services of CSPs.
  - Electronic service providers (with at least one end-user in Australia) and anyone who facilitates the services of electronic service providers, e.g. Facebook, Google, and Amazon Web Services; and
  - Manufacturers of electronic equipment and anyone who facilitates the manufacture of electronic equipment used in Australia, e.g. Samsung, Apple.

TOLA Act – overview – what kind of assistance?

- Section 317E sets out, in some detail, the types of assistance that may be specified. These types include (but not limited to):
  - **Providing** technical information.
  - **Facilitating** access to services and equipment.
  - **Removing** one or more forms of electronic protection.
  - **Modifying** technology.
  - **Concealing** that the company has done any of the above.
- Example: The assistance may require the issue (to a specific criminal suspect) of a notice to update messaging software – when in fact the 'update' will then allow access to the messages of that suspect.
- **No introduction of systemic weaknesses and vulnerabilities** (also know as 'backdoors' for encryption mechanisms)
- Civil immunity is available for CSPs acting in good faith to ensure that they are protected from any legal risk.

TOLA Act – overview – other relevant details

- **Organisations**: The use of the powers has been restricted to the Australian Federal Police, the Australian Criminal Intelligence Commission, the Australian Security Intelligence Organisation, the Australian Secret Intelligence Service, the Australian Signals Directorate, and State and Territory Police forces.
- **Responsible officer**: A TAR or a TAN may be issued by the head (or delegate) of each agency above. A TCN may only be issued by the Attorney-General
- **Suspected offence**: The use of the powers is connected to the safeguarding of national security or (for State/Territory/Commonwealth Police) the enforcing of criminal law so far as it relates to serious Australian or foreign offences (defined as punishable by a maximum term of 3 years imprisonment, or more, or for life'.
- **Enforcement**: The framework is not intended to be adversarial – it intends to engender a spirit of cooperation. However – civil penalty for contravention is $10 million for corporate entities and $50,000 for private individuals.
- **Oversighting and reporting**: The Commonwealth Ombudsman or Inspector- General of Intelligence and Security. The use of industry assistance powers is subject to annual reports to the Home Affairs Minister.

TOLA Act – overview – other relevant details

- The TOLA Bill was introduced to the Australian Parliament on 20 September 2018.
- **The Bill created significant interest (here and abroad) – the main concerns were:**
  - **Perceived privacy implications**
  - **Withdrawal of international corporate investment in Australia,**
  - **Loss of public confidence in Internet trust levels.**

- The Bill was subsequently referred to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) for inquiry and report.
- The PJCIS then received a very large number of submissions expressing concerns with the Bill (from the Law Society of NSW, the Law Council of Australia, carrier industry providers, law enforcement/security agencies, and a large number of other commercial and private legal institutions.
- The Bill became law on 8 December 2018. The reason given for the rapid passage of these complex reforms: a heightened risk of terrorist incidents over the Christmas and New Year period (2018)

Fast forward to 2021 – Surveillance Legislation Amendment (**Identify and Disrupt**) Bill 2021

- Updates Surveillance Devices Act 2004 and Telecommuications Act 1979/1997

Three new powers:

1. "**data disruption warrants**": allow authorities to "**disrupt data**" by copying, deleting or modifying data as they see fit
2. "**network activity warrants**": permit the collection of intelligence from devices or networks that are used, or likely to be used, by subject of the warrant
3. "**account takeover warrants**": let agencies take **control of an online account** (such as a social media account) to gather information for an investigation.

What's different to previous laws?

- Telecommunications Act 1997: only permits to **intercept** or **access** communications and data under certain circumstance.
- Identity and Disrupt Bill 2021: unprecedented interception or "*hacking*" powers (access can be gained to encrypted data which could be **copied**, **deleted**, **modified**, and analysed even before its relevance can be determined).

What are the privacy concerns?

What are the security issues and impact?

Privacy concerns & security issues

- The bill may **impact third parties who are not suspected** in the investigation of criminal activities.
  - The bill can authorize access to third party computers, communication and data.
- Broad powers can potentially **compel** any individual with relevant knowledge of the targeted computer or network **to conduct hacking activities**.

- Law enforcement could modify potential evidence in criminal proceedings (**Integrity** of data)
- In lawful hacking, authorities also depend on **zero-day exploits**.
  - Ethical issues? *Think how you'd feel if your government would put its citizens at risk by not reporting software vulnerabilities to software manufactures so that they can be patched.*
  - Security issues? In 2016, CIA's secret stash of hacking tools itself was stolen and published
    - (https://www.washingtonpost.com/national-security/elite-cia-unit-that-developed-hacking-tools-failed-to-secure-its-own-systems-allowing-massive-leak-an-internal-report-found/2020/06/15/502e3456-ae9d-11ea-8f56-63f38c990077_story.html)

Codes of Ethics & Professional Organizations

(next 5 slides – overview only, important for professionals in those areas)

- **ACM** established in 1947 as “*the world's first educational and scientific computing society*”. Membership approx. 100000. Web: www.acm.org

- **IEEE** established in 1963 to advance theory and application and facilitate innovation in *engineering, computer science* and *electronics*. Currently publishes nearly one third of all research literature in those disciplines. Membership approx. 420000. Web: www.ieee.org

- Both promote a code of ethics contains references to *protecting information confidentiality*, *causing no harm*, *protecting others’ privacy*, and *respecting others’ intellectual property*

- **Sources of information**: ***www.ieee.org*** *and* ***www.acm.org***

International Information System Security Certification Consortium (ISC2)

- Non-profit organization focusing on development and implementation of information security certifications and credentials (CISSP – Certified Information Systems Security Professional)
- Membership approx. 140000. Web: www.isc2.org
- Code primarily designed for information security professionals who have certification from (ISC)²
- Code of ethics focuses on four mandatory canons:
  - Protect society and infrastructure; act honorably/honestly/justly/responsibly/legally; provide diligent and competent service to principals; advance and protect the profession.

System Administration, Networking and Security Institute (SANS)

- SANS is a founding organization of the Center for Internet Security
- Professional organization with a large membership dedicated to protection of information and systems
- SANS offers set of certifications called Global Information Assurance Certification (GIAC)
- Website: **www.sans.org**

Information Systems Audit and Control Association (ISACA)

- Professional association with focus on auditing, control, and security (i.e. a focus on IT governance). Formed in 1967.

- Current membership: 140,000.

- Concentrates on providing IT control practices and standards (**COBIT**) – Control Objectives for Information and Related Technologies – a framework for IT management governance.

- ISACA has code of ethics for its professionals

Australian Computer Society (ACS)

- Founded 1966.
- Membership: 45,000.
- Focus: computer and information processing technology

- As the Professional Association and peak body representing Australia's ICT sector, ACS' mission is to deliver authoritative independent knowledge and insight into technology, build relevant technology capacity and capability in Australia and to be a catalyst for innovative creation and adoption of technology for the benefit of commerce, governments and society.

- Web: **www.acs.org.au**

Australian Cyber Security Centre

- The **Australian Cyber Security Centre** (ACSC) is the Australian Government lead agency for cybersecurity.
- The ACSC was established in 2014 replacing the Cyber Security Operations Centre.

The role of the Australian Cyber Security Centre is to:

- lead the Australian Government's operational response to cyber security incidents
- organize national cyber security operations and resources
- encourage and receive reporting of cyber security incidents
- raise awareness of the level of cyber threats to Australia
- study and investigate cyber threats.

The **ASCS integrates cyber security** capabilities across the **Australian Signals Directorate**, the **Digital Transformation Agency**, the **Defence Intelligence Organisation**, the **Computer Emergency Response Team**, the **Cyber Security Policy Division of the Department of Home Affairs**, **Australian Security Intelligence Organisation** cyber and telecommunications specialists, **Australian Federal Police** cyber crime investigators, and Australian Criminal Intelligence Commission cyber crime threat intelligence specialists. The Centre is also a hub for collaboration and information sharing with the private sector and critical infrastructure providers.

AusCERT

- **AusCERT** is a leading Cyber Emergency Response Team (CERT) for Australia and provides information security advice to its members, including the higher education sector. It is a single point of contact for dealing with cyber security incidents affecting or involving member networks.

- **AusCERT** provides members with proactive and reactive advice and solutions to current threats and vulnerabilities. We'll help you prevent, detect, respond and mitigate cyber-based attacks.

- **AusCERT** monitors and evaluates global cyber network threats and vulnerabilities, and remains on-call for members after hours. AusCERT publishes the Security Bulletin Service, drawing on material from a variety of sources, with recommended prevention and mitigation strategies.

- **AusCERT**'s Incident Management Service can be an effective way to halt an ongoing cyber attack or, provide practical advice to assist in responding to and recovering from an attack.

- Web site: ***www.auscert.org.au***

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA

CREATE CHANGE

© Randy Glasbergen
www.glasbergen.com

“I’m applying for the Information Security position.
Here is a copy of my resumé, encoded, encrypted and shredded.”

```
                                    func, std::vect
          end;

       write(Endtext);
end.
CREATE TABLE product(
       class MultinomialNB(object):
       def __init__(self):
2})
          self.X = None
          self.y = None
       def __loading(self):
          self.list_labels = cl.Counter(se
int acc(std::function<int(int, int)> fun
       auto it = operands.begin();
       int result = func(*it, *(++it));
       if (operands.size() > 2) {
          for (++it; it!=operands.end(); +
             result = func(result, *(it));
          }
       }
       return result;      CDog& operator=(c
```

Thank you