InfoSec Summary Notes

Akira Wang

July 2019

0.1 Improving Privacy

This is an improvement, not solution.

- Periodically check privacy settings and update them
- Take note on mobile apps, online accounts, or other software
- Turn off settings that share information, such as location, data, contacts, etc

0.2 Defending Privacy

- Assume you have less anonymity and less privacy when you're doing something electronically
- Only give out as much personal information as you have to
- Ask yourself what they need it for (i.e don't give it to them, give them made up info, find an alternative)
- Use tools that reduce websites ability to track.

1 Cryptography

Ciphertext is the encrypted message.
The coprime is defined as having no integer factors in common apart from 1.

1.1 Before Public-Key Cryptography

- Previously, we had symmetric-key cryptography.
- Both the sender and receiver had to agree on the secret key in advance (i.e agree on a code prior to sending).
- Encrypting and decryption used the exact same key.
- Advanced Encryption Standard (AES) still uses this method since they're fast.

1.2 Public-Key Cryptography

- The receiver generates both a public and private key (pk, sk respectively)
- The public key is used for encrypting messages, whilst the private key is used for decrypting messages.
- *Anyone can encrypt a message, but only you can decrypt it.*
- Symmetric Encryption (such as AES) use secret keys which blend with the plain text of a message to encrypt it. The sender and receiver should both know the secret key that is used to encrypt and decrypt the messages.
- Asymmetric Encryption (public key cryptography) uses two secret keys to encrypt plain text messages. Here, anyone with the private key can decrypt the message and anyone with the public key can encrypt a message.

1.3 RSA

A type of public key cryptography (asymmetric).

- The receiver thinks of two different large prime numbers p, q
- Each one is roughly 300 digits long, and multiplies them to get $N = pq$.
- $\phi(n)$ is the number of integers that are coprime with n. (i.e $\phi(8) = [1, 3, 5, 7]$)
- The public exponent e (for encrypting a coprime to $(p-1)(q-1)$) is generated and the public key (pk) is publicised:
$$pk = (N, e) \tag{1}$$
- To encrypt a message m (**ciphertext**), compute $(m||r)^e \text{mod}(N)$ for r = randomness.
- The receiver can decrypt m because she knows both p and q.
- Useful when there are several people sending messages to the same receiver (i.e in an electronic voting system).
- Attack: Try to decrypt two identical messages.
- Attack: Common modulus attack. Consider:

> MiTM attack where Mike can listen and sabotage transmissions. As the ciphertext is sent, Mike changes the exponent to e' so that Bob receives (e', N) instead of (e, N). When Alice receives e', she encrypts it and sends it back to Bob. Since Bob cannot decrypt it, they retry the procedure. Now, Mike does not interfere this time so the ciphertext is encrypted with the correct public key.
> Since Mike now has two ciphertexts, one with e and another with e', as well as the public modulus, Mike can apply the common modulus attack under the assumption that Alice encrypted the exact same message.

1.4 Diffie-Hellman Key Exchange

A type of public key cryptography (asymmetric).
Procedure:

1. Fix a large prime number with 600 digits
2. Fix an integer g, where $g \in [0, p)$
3. Person 1 (P1) will choose a randint a, where $a \in [0, p)$. Then, the message A is encoded as $A = g^a \text{mod}(p)$.
4. Person 2 (P2) will choose a randint b, where $b \in [0, p)$. Then, the message B is encoded as $B = g^b \text{mod}(p)$.
5. The shared secret key K_{AB} to decode the message is $K_{AB} = g^{ab} \text{mod}(p)$.
6. The equation works since the following holds:
$$B^a \text{mod}(p) = g^{ba} = K_{AB} = g^{ab} = A^b \text{mod}(p) \tag{2}$$
7. Hence, you can solve for shared secret:

For an attacker,

1. The shared secret key can be discovered:
$$DH_g(g^a, g^b) = g^{ab} \text{mod}(p) \tag{3}$$
2. Time Complexity is $\exp(\mathcal{O}(\sqrt[3]{n}))$

1.5 Man-in-the-Middle (MiTM) Attack Prevention

Happens when there is a third party which inserts a bogus key to both sides of the party, which can then be used to read the message without the true values of a and b.

> *Suppose we know some other PK, is it possible to prevent Middle-Man Attack.*

- Use the other PK to encrypt K to double check whether the keys match. Must ensure that the middle-man cannot fake it.
- If person 2 knows person 1's signing key, person 1 can sign A ($\text{sig}_{\text{P1}}A$)
- Use the PK to encrypt A, B to get A_e, B_e, and then key exchange. The middle-man can continue to observe, but will be unable to decrypt the original message since it is encrypted.

2 Encryption Tutorial Notes

2.1 Protocols using RSA

Question: Assuming RSA is secure, what is one way a middle man can intercept the message.

> Middle Man can pretend to be Alice by advertising her Public Key which Bob knows the Private Key for. Then, Bob will encrypt the secret message with a Public Key which is actually the Middle Man's.

Now suppose this scenario:

1. Alice advertises her RSA PK = RSApubKey_A
2. Bob generates a secret key k for a secret-key encryption algorithm (such as AES)
3. Bob encrypts the message m using AES and k, then sends the cipher-text $c_k = \text{RSA}(k, \text{RSApubKey}_A)$ to Alice.

Question: Does the above attack work still work?

> Yes, the middle man will still be able to intercept the message.

Question: Suppose Bob has an alternative way of checking which RSA Public Key truly belongs to Alice. Is there another way of intercepting the message?

> It is now not possible without breaking the encryption of RSA or AES.

Question: Does the protocol provide *forward* secrecy (past) or *future* secrecy against an attacker who learns Alice's RSA Private Key?

> No for both. This is because all past and future messages are still readable using Alice's RSA Public Key (decrypt the value of k and then use AES to decrypt the message).

Question: Does the protocol provide *forward* secrecy (past) or *future* secrecy against an attacker who is able to calculate the short-term secret key k for a single message?

> Yes for both. This is because the attacker can now read the one message, but not any past or future messages (since they will now have different k values).

2.2 Diffie-Hellman Key Exchange

Consider the DH Key Exchange:

1. Alice and Bob agree on public values g and p (large primes). Middle Man also learns of these values.
2. Alice generates a secret a and sends $A = g^a \text{mod}(p)$ to Bob
3. Alice generates a secret b and sends $B = g^b \text{mod}(p)$ to Alice
4. Alice and Bob both compute $k = g^{ab} \text{mod}(p)$ and verify they get the same result
5. Bob sends Alice an encrypted message using their shared key k (for example: $c = AES(m, k)$)

Question: Explain how a Middle Man can read the the message.

> An attacker can insert a bogus key (A' and B') to both sides of the party, which can then be used to read the true message without the values of a and b. To the parties encrypting the messages, it will seem as if they are encrypting the message correctly. However, they are actually encrypting the message with respect to the attacker's bogus key.

Now consider a *signed* version of this problem. Suppose Bob has an independent way of checking which public key for signatures truly belongs to Alice.

1. Alice and Bob agree on public values g and p (large primes). Middle Man also learns of these values.
2. Alice generates a secret a and sends $A = g^a \text{mod}(p)$ to Bob. **She additionally signs A with her private signing key.**
3. Alice generates a secret b and sends $B = g^b \text{mod}(p)$ to Alice.
4. **When Bob receives A from Alice, he checks her signature to make sure A is truly sent by Alice.**
5. Alice and Bob both compute $k = g^{ab} \text{mod}(p)$ and verify they get the same result
6. Bob sends Alice an encrypted message using their shared key k (for example: $c = AES(m, k)$)

Question: Assume the Middle Man *does not* know Alice's private signing key. Does the attack now work?

> No. This is because the Middle Man will not be able to sign A so Bob will be able to verify if it is correct or not.

Question: Suppose Alice and Bob generate new a and b values (and therefore a resulting new k) every time they communicate. Does the protocol provide *forward* secrecy (past) or *future* secrecy against an attacker who learns only the short-term secret key k for one message?

> Yes for both (same as RSA).

Question: Suppose the Middle Man learns Alice's private signing key. Can they decrypt past messages (forward secrecy)?

> No they cannot - even if the Middle Man retains a transcript of the conversation and knows the signing key, it still requires the original secrets to decrypt.

Question: Suppose the Middle Man learns Alice's private signing key. Can they intercept future messages (future secrecy)?

> Yes. The Middle Man will now be able to forge Alice's signature and intercept messages using the same attack method as the RSA..

3 Additional Cryptography Notes

3.1 AES

- The algorithm is based on several substitutions, permutations and linear transformations, each executed on data blocks of 16 byte – therefore the term blockcipher

3.2 RSA

- As opposed to traditional, symmetric encryption systems, RSA works with two different keys: A public and a private one. Both work complementary to each other, which means that a message encrypted with one of them can only be decrypted by its counterpart. Since the private key cannot be calculated from the public key, the latter is generally available to the public.
- The security of RSA itself is mainly based on the mathematical problem of integer factorization. A message that is about to be encrypted is treated as one large number. When encrypting the message, it is raised to the power of the key, and divided with remainder by a fixed product of two primes. By repeating the process with the other key, the plaintext can be retrieved again.

3.3 Key Exchange

- Diffie-Hellman is a key exchange protocol but does nothing about authentication.
- In the raw Diffie-Hellman exchange that you present, you talk to some entity that is supposed to generate a random secret value on-the-fly, and use that. Everybody can do such random generation. At no place in the protocol is there any operation that only a specific Bob can do. Thus, the protocol cannot achieve any kind of authentication – you don't know who you are talking to. Without authentication, impersonation is feasible, and that includes simultaneous double impersonation, better known as Man-in-the-Middle. At best, raw Diffie-Hellman provides a weaker feature: though you do not know who you are talking to, you still know that you are talking to the same entity throughout the session.

- In SSH, a Diffie-Hellman key exchange is used, but the server's public part (its gb mod p) is signed by the server. The client knows that it talks to the right server because the client remembers (from a previous initialization step) the server's public key (usually of type RSA or DSA); in the model explained above, the rightful servers is defined and distinguished from imitators by its knowledge of the signature private key corresponding to the public key remembered by the client. That signature provides the authentication; the Diffie-Hellman then produces a shared secret that will be used to encrypt and protect all the data exchanges for that connection (using some symmetric encryption and MAC algorithms).

4 Cryptography Lecture 3

4.1 Downsides to Diffie-Hellman Exchange

- Exchange only hides the contents of the message, but not the traffic between two parties
- Tor on the other hand, aims to **hide** both the contents of the message, but the parties who are communicating too

4.2 How Tor Solves the Problem

- Suppose Person 1 knows Person 2's encryption key PK_B, then she can prevent the Man-in-the-Middle attack using an RSA to encrypt her message $\text{RSA}(A)$.
- *Assuming that Person 1 has the correct public key and not the Man-in-the-Middle's public key.*
- The Man-in-the-Middle can still intercept and send a fake message (i.e A'), but now they do not know A for $A^{b'}\operatorname{mod}(p)$ and hence cannot decrypt the message.

4.3 Tor

- Tor stands for The Onion Routing
- *Imagine you want to send a letter to someone, you always put an address and a return address - this means any postman can see your address. One way around this is to send your letter to a trusted source, where they will open the letter to find the true letter and post that to the desired address (peeling the onion). Now there is no letter that has your address and connects you to the actual address you are sending to.* **The problem:** *What if the trusted source (i.e proxy server) is malicious? The solution is to go through another layer of trusted sources. This is why it is called "onion routing" since it is a layer of proxies.*
- The strongest property of "onion routing" is that it is secure so long as at least one proxy remains "honest" (there is at least one anonymous link that hides the connection between the "onion layers"). For Tor to be compromised, all proxies need to be colluding.
- The Tor design uses an initial RSA encrypted key, where the layers are encrypted using different AES's for each layer. The layers encrypt and decrypt the information using the Diffie-Hellman Key Exchange.
- The user can control which circuits to use, but still needs to establish a shared secret with the first relay. Then, the first relay establishes a shared secret with the second relay. As a result, the user can have a shared secret *via* the first relay.
- The important factor is that the relays only communicate to their designated relay, but not to any other relay (i.e the relay does not / cannot open the messages in the deeper layer).
- Once the relay has been configured, the message is encrypted using layered AES encryption.
- Protection from interception still applies since the secret key is hashed using AES.

4.4 Law Enforcement

- **Technical Assistance Notice**: might require turning over information or data that the provider already has.
- **Technical Capability Notice**: might require re-engineering the system to provide new data that the provider wouldn't otherwise have. I understand it to include possibly installing software from law enforcement, or possibly re-engineering parts of the provider's system.

5 TOR Tutorial Notes

Question: Explain the main purpose of the TOR network.

Hide communications between parties.

Question: Describe how the circuits are constructed in TOR.

Circuits are designed using multiple layers of AES encrypt ions.

Question: What is the main reason for having multi-step paths rather than using a single intermediary?

The main reason is because if one intermediary is lost / compromised / malicious, then the whole network is compromised and privacy is lost. The multi-step paths distributes trust so that an intermediary does not know the remainder of the network. This means if individual nodes are bad, the network is still guaranteed privacy.

Question: What information might law enforcement gain by issuing a *Technical Assistance Notice* to one TOR relay node? Would it be useful?

Law Enforcement will learn which node incoming messages were sent to. However, this does not say anything outside of traffic since they still do not know the source or destination.

Question: What information might law enforcement gain by issuing a *Technical Assistance Notice* to several TOR relay node? Suppose they manage to read all information from all the nodes along a circuit.

Law Enforcement will be able to learn about the source and destination because they can trace the communication through the network. However, the circuits in a TOR network are always changing, so it is difficult to completely compromise every single node in the circuit without compromising a large fraction of the TOR network.

Question: Suppose law enforcement issue a *Technical Capability Notice* (TCN) that allows them to install software on one TOR relay node. What could they learn / will it be useful?

Same as before, they will not learn anything other than traffic since they do not know the source or destination.

Question: Suppose that an adversary can now undermine Alice's checks on the public key infrastructure of the TOR network. So, when Alice wants to know the public key (**onion key**) of another user, the adversary is able to substitute a bogus key. How can this help the adversary learn who Alice is communication with?

If this happens, then Alice's ability to set a circuit up is completely broken. Whenever Alice initiates the initial DH exchange, the message is encrypted with the public key of the intended recipient to prevent the man in the middle attack. However, if an adversary is able to substitute a bogus key, then her connection can be intercepted and decrypted.

6 Unique in the Crowd: The Privacy Bounds of Human Mobility

The bare minimum of a single carrier tower is still precise in knowing where you are.

- Always know which carrier tower you are connected do, even if you disable location services.
- Phone carrier will always have an approximate location given the location of the tower.
- Aggregations don't hide much, since the bare minimum of location information is enough to identify an approximate target.
- Close to 100% of people are re-identifiable (unique) after 5 numbers of spatio-temporal points. Roughly half of the people are already unique with just 2 spatio-temporal points.
- Spatial and Temporal Resolution: (1 antenna,1 hour) means everyone is re-identifiable.
- Reducing the precision in the time attribute will not increase the privacy of individuals. This is because the antennas are the main identifiers, so reducing the precision with spatial resolution is the best way to increase privacy.

7 BitCoin Blockchain

Refer to EoDP Lecture 17-18 Slides for more detail.

- Distributed e-cash system which maintains the entire history of all transactions and generated coins.
- When a transaction is performed:
  1. You announce it globally
  2. Some participants (minors) compute a proof-of-work and incorporate it into the bitcoin blockchain.

7.1 Proof-of-Work

$$\text{Hash}(B_1, B_2, n) < \text{threshold}, \tag{4}$$

where B_i is the i'th Block in the BlockChain.

- Hash using SHA-256 called the prior block with a randomly-chosen nonce n.
- Succeed when the digest (output of hash) is below some threshold that proves you tried a lot of different (nonce) n values (the proof-of-work is rewarded bitcoin, hence called "mining").
- The threshold may decrease as more participants join the network.
- The final step is the broadcast the new block including the (nonce) n values.
- Anyone can easily test, but it is computationally time expensive to generate the nonce value.
- *When you find the nonce, you tell everyone the value of n. Then, people can test your nonce value by hashing it to see if it is lower than the threshold.*

7.2 BitCoin agreement

- Different versions of the blockchain diverge. These occur during simultaneous updates and network connectivity problems.
- Honest nodes should **always** accept the "longest" version (the one with the largest total work accomplished / total number of blocks).
- *So if there are two different history's floating around, then the node should always accept the history that goes furthest back.*
- Works in practice pretty well, but an attacker with vast computational resources could subvert it.
- *An attacker can build a long chain and hide it if they have a significant amount of computational power. Then, they can push it and it will be accepted.*

7.3 The "Rewriting History" Attack (51% Attack)

Suppose the attacker controls more computation power than everyone else in the network. Let A be the attacker.

- A gets something from B in return for payment, but A would rather keep B's goods and spend the money again.
- So A needs to generate a longer, self-serving different history.
- This needs to be kept in secret until they're well away from B.
- At the end, they reveal it to everyone else as they will adopt it as the truth.
- **There is no prevention as there is no way to distinguish the difference between a legitimate history and a self-serving different history.**
- But, this is unrealistic since the attacker would need 51% of the worlds' total computing power.

8 WiFi Pineapples

Pineapples are a tool used to find wireless security risks by penetration testers in order to test the robustness of organizational security. They are

- Small and unobtrusive with a shape akin to an actual wifi router
- Ultra portable meaning it is easy to move around and plant onto a persons' premise
- Works straight out of the box without the need of installing Linux Kali and dependencies
- Allows you to inject frames which normal access points or wireless dongles will not allow

8.1 Functionalities

The PineAP (Access Points) will continuously listen for SSID's (wifi network identifier which are always a list of remembered networks within a device).

The PineAP collects these recognized SSID's stored on the device in order to infer information about the devices' owner. These include where they might live, work / study, places they eat, etc. Shopping centres use this technique to monitor their customers.

SSID's can be geolocated via https://www.wigle.net which uses collected data from people who roam around to identify networks and their vulnerabilities (wardriving).

8.2 Evil Portal

There is a module called Evil Portal which exploits public wifi and captive portals. THat is, the webpages users are obliged to view and open when connecting to a public wifi before connection is approved. This particular model can disconnect people from legitimate public networks, where the Evil Portal is then used to mimic the network SSID and captive portal to trick these people from reconnecting to the Pineapple.

Similarly, if the attacker has background information on the types of devices you use, they can identify your device, mimic the SSIDs you usually connect to and trick you into connecting. This is possible due to the **Broadcast SSID POOL** which mimics any identified SSID.

8.3 Lessons to Learn

- Public networks are always at risk
- If you decide to connect to public wifi, use a VPN
- Never ever go on HTTP, only on HTTPS
- Try and forget all public networks to prevent your device from broadcasting the SSIDs of networks connected

8.4 Cyber-Security Logic Chain

- What are we trying to protect? *Data, communications, money / finance, lives*
- Who is your **real** adversary? *Cybercriminals, governments, ethical hackers*
- What are your **real threats and vulnerabilities**? *Servers, websites, employees, devices*
- Prioritise your responses and mitigation via the **known weakest links** first
- Balance the mitigation's' relative effectiveness against their cost / inconvenience (look at Equifax / small businesses for examples). Does the cost out-weight security? Is it inconvenient to update / patch?

9 Small Businesses

Likelihood of attackers (1 being most likely):

1. Cyber Criminals
2. Current Employees
3. Ex-Employees
4. Competitors
5. Nation States

Types of attacks that can occur:

- Malware Infections on any device
- Spam / Phishing Emails
- Attacks on websites or servers (via SQL injection)
- Remote network or desktop access
- Local network access (directly onto the wifi)
- Cloud server attacks
- Employees or Ex-Employees maliciously retaining restricted files

Ways to protect your own business:

1. Ensure all OS and applications are up to date. But, you need to consider if it might cause considerable downtime (affecting profits) or if it will break legacy software/
2. Protect workstations by limiting access to the administrator accounts. Local administrators should be disabled as a safe measure.
3. Ninite is an excellent way of updating all applications at once (though it is limited to the list of supported software)
4. Buy software which support enterprise security where possible (such as Office 365 for email services)

Protecting emails is a good way to eliminate base attacks:

- Use enterprise-grade email providers such as Office 365

- Implement spam filtering to block phishing attacks
- Block all dangerous file attachments. Even better, only allow a white list of allowed file-types
- Ensure attackers can't impersonate users by setting up SPF records
- Encourage 2FA and password policies to enforce strong passwords.

9.1 The 3-2-1 Backup Strategy

- **3** copies of your data as backups
- **2** of which are stored on different storage media devices
- and **1** which should be located off-site.

10 High Risk IT Security Environments

- Aid - money from donors (government, private sector) to help the lives of those in developing countries.
- Types of areas:
  1. Cyberpolicy - Regulations for Online Freedom (i.e Net Neutrality).
  2. Cybersensorship - Prevent global censorship of data.
  3. Cybersecurity - Defend people who wish to remain anonymous (i.e journalists).
- China kept a tab on interesting people (i.e if Chinese friends contacted, then they would be brought in for potential questioning).
- Try to introduce technology (i.e VPN, proxies, tor, etc) to those who are living in cybersensorship.
- Extreme examples (Africa):
  - Completely lacks mobile towers (only dial up), but they have internet cafes.
  - 1 hour costs about 50 cents, where one page may take 4 minutes to load.
  - Surprising that there is no cybersensorship. The bandwidth was just very slow.
- Physical aspects: The activists / journalists can be prepared, but their families or relatives may be put in danger.
- In a non-free country (Iran), independent sources are banned. Hence, Exile Media is used (people who work outside of the country to bring sources in). Communication must be secure since once it is exposed, all correspondents can be identified and captured.
- Governments won't come to arrest you for using VPN in countries (like China, Iran), but they do try to block access. *Since there are so many people using VPN, they can't allocate resources to them. So, they prioritise those who may be of a higher risk - i.e the people that run the VPN services.*
- Pirated software don't get updates - can be super vulnerable to exploits and security flaws.
- Most people have insecurity of endpoints (software) and accounts (online).

11 Privacy Infringing Technologies

11.1 Definition of Emerging Technologies

Technology under development which are current unrealized, but may soon become prominent.

11.2 Defining Attributes

So, the five defining attributes of emerging technologies are:

1. Radical Novelty
2. Fast Growth
3. Coherence that persists over time
4. Benefit for a wide range of sectors
5. Prominent impact of the technology lies in the future

11.3 CIA Triad

- **Confidentiality:** Ensuring only those who ought to have access can do so.
  - Risks: *Loss of privacy, unauthorised access to information and identity theft.*
  - Controls: *Encryption, authentication and access controls.*
  - Primary Focus: *Information Security*
- **Integrity:** Ensuring information cannot be modified without detection.
  - Risks: *Information is no longer reliable or accurate and fraud.*
  - Controls: *Quality assurance and audit logs.*
  - Primary Focus: *Operational controls*
- **Availability:** Ensuring information can be accessed when needed.
  - Risks: *Business disruptions, loss of customer confidence and loss of revenue.*
  - Controls: *BCP plans and tests, back-up storage and sufficient capacity.*
  - Primary Focus: *Business continuity and planning (BCP)*

11.4 Triple A

- **Accountability:** The ability of a system to hold users responsible for their actions.
- **Auditability:** Conduct persistent monitoring of all human or machine actions on the system (i.e log files).
- **Authenticity:** Verify and identify a third party with the information it provides.

11.5 Threats to Privacy

- From Businesses you are dealing with
  - Metadata can be collected by online businesses
  - Social media data for the purpose of selling
  - Collect and use information for many purposes
  - Opt-out option provides a false sense of privacy
- From Technologies you are using:
  - When we don't know which data is being collected by who
  - Data is being sold or used by other companies (such as changing prices or products or services)
  - De-identification and re-identification of data
- Societal threats:
  - The right to have privacy
  - Having a choice
- Other:
  - Embarrassment
  - "Past coming back to haunt you
  - Lack of security of information
  - Unwanted marketing
  - Marketing manipulation
  - Irrelevant considerations
  - Collection of profiles
  - Intrusive bio-metrics
  - Repressive state control
  - Unfair decisions on wrong / sensitive info
  - Tracking of movements and locations
  - Interception of communications

11.6 Values of Privacy

- Monetary value as personal data is being sold between companies
- Digital data is closely connected to real-world data and may compromise physical security
- Scamming targets vulnerable people (such as the elderly) who may end up losing personal or monetary valuables
- An individual's links to their networks
- Privacy enhances individual freedom and agency (i.e risk of losing all control over their own data)
- Freedom of thought and creation
- Equal opportunities (i.e shopping)
- Escaping prejudice and discrimination
- Respect for human autonomy
- Psychological need for privacy
- Conduct free from inhibiting surveillance
- "Forgiveness" of past actions
- Avoidance of injustices
- Preventing long-term repression
- Enabling markets (e-commerce)

11.7 Information Management (APP)

- Types of citizen data:
  - Consumer data
  - Medical data
  - Bio-metric data
  - Criminal Records
- Responsibilities of data holders
  - Bio-metric and criminal data should only be used during criminal cases
  - Laws set by parliament must be followed
  - Transparency
  - Only use data for intended / disclosed purposes
  - If data is sold to a third-party, they must be checked for trustworthiness through education and agreements

The **Privacy Act 1998** define personal information as:

> "... information or an opinion, whether true or not, and whether recorded in a material form or or not, about an identified individual, or an individual who is reasonably identifiable."

The GDPR is straight to the point: If the person is identifiable from the data, then it is personal data. Australia's Privacy Act allows for some room of flexibility (and loopholes) with the "reasonably" term.

Common examples of an individual's personal information include:

- Name
- Signature
- Address
- Telephone number
- Date of Birth
- Medical records
- Bank / Financial account details
- Commentary or opinion(s) about a person or body

12 The Big Four (IT Security Audit)

The four sections are:

1. Endpoint Security: Ensure everything is up to date.
2. Online Account Safety: Use MFA or have Password Managers.
3. Encryption of data at rest: Encrypt disk and local data using BitLocker.
4. Encryption of data in transit: e2e encryption for Instant Messaging such as Signal, WhatsApp, Viber.

12.1 Tutorial Questions

Question: Imagine you are planning to travel overseas and require internet access. However, the country you are traveling to charges exorbitant prices for a local SIM card with mobile data, so all you can use is just free public Wi-Fi. Explain how would you keep you and your device safe while using public Wi-Fi.

- Use a good VPN to hide traffic from other people on the network who might be watching.
- Have a good local firewall to block incoming connections.
- Ensure to keep device(s) up to date to protect against attacks that exploit networking vulnerabilities.

Question: Imagine you're the IT administrator of a small business organization and you are responsible for managing the organization's computers. The cybersecurity department has notified you of a vulnerability that is already being exploited in the wild. The impact of the vulnerability is very big and has already impacted the infrastructure of several foreign government organizations. A fix is already available as part of a major operating system upgrade (e.g. Windows 10), but your organization is not running this version of Windows due to the continued use of some legacy software. What are the challenges involved in securing your organization from this threat, and is it worth doing so?

- The biggest challenge is to upgrade to Windows 10. This is because it may be time-consuming and expensive, resulting in significant downtime to upgrade. In this case, any form of downtime will result in a loss of revenue.
- The upgrade will also break legacy software, leading to loss of productivity and revenue. Although it may be possible to procure updated versions of the legacy software, resources will need to be spent in order to re-train employees to use it.
- However, if no measures are taken to prevent more threats, the costs could be more devastating than the combination of upgrading and down time. This is because the nature of the threat may wipe out the existence of your organisation.
- In the end, if the cost to fix the problem does not result in a significant loss of revenue, then it is worth fixing.

13 Notifiable Data Breach (NDB) Scheme

The Privacy Act requires entities to notify individuals and the Commissioner about data breaches that are likely to cause serious harm.

Entities that have an obligation to comply under the NDB scheme are:

1. Entities with current existing obligations
2. Australian Government agencies, business and not-for profit organisations with annual turnover greater than AUD$3 million, private sector health service providers, credit reporting bodies, credit providers, entities that trade in personal information and TFN recipients.

A data breach is eligible when the following three criteria are satisfied:

1. There is unauthorised access to OR unauthorised disclosure of personal information OR a loss of personal information, that an entity holds
2. The data breach is likely to result in serious harm to one or more individuals
3. The entity has not been able to prevent the likely risk of serious harm with remedial actions

14 Thomas Drake Guest Talk

- Trends of censorship by government are concerning.
- The cloud act that allows Australian government to have access to all on-shore technology and software via a backdoor.
- If security takes priority, then society loses all freedom and control of their own privacy.

- Logic - legislation to justify exercise of more security.
- NSA was given special authorization to sweep from the inside out (violated 4th amendment).
- 9/11 was used as an excuse to violate the law.
- Lead attorney under orders from the president abandoned the constitution because of the failure to keep almost 3000 people out of harms way. The attorney general just said *"we just need the data"* and congress will say no if we try to change the law to make it legal.
- Data collection suffers from the same problem as Data Science - too much data gives too many dimensions.
- NSA was unable to gather that much data if it did not have connections with telco companies.
-

1. Having the capacity to collect and analyze data - especially on people is seductively powerful - especially when done without the person's permission and particularly when done in secret - the ultimate form of control.
2. Direct partnership access agreements to pools of data (see Prism)
3. Physical locating at server premises to intercept communications
4. Agreements to access undersea cables
5. Agreements with software manufactures to allow infiltration, including encryption software companies
6. Mapping of key private sector arrangements to access data that flows between them
7. Manipulation of private sector tools (for example, using Google Cookies)
8. Access to Verizon's 120 million customers
9. PRISM (Google, Facebook, Apple, Microsoft, Yahoo, Skype, Paltalk, YouTube and AOL)
10. UPSTREAM - agreements for NSA to directly access fiber optic cables
11. ROYAL CONCIERGE - direct access to luxury hotel databases
12. SQUEEKY DOLPHIN - ability to monitor social media in real time (YouTube, Facebook, etc)
13. Companies will be forced to deal with a clear conflict of interest between the pursuit of profit and fulfilling a regulatory role on behalf of the government
14. A company will find it difficult to maintain the integrity of its paying customers, especially with respect to their privacy
15. Increasing access to and manipulation of data makes it inherently less secure
16. Changing and vague demands from government might make it difficult to build appropriate data security infrastructure

15 Penetration Testing Guest Talk

- **White Hat:** Test from a physical, digital or social POV through ethical means.
- **Black Hat:** Does it illegal for their own motivation - i.e money or self satisfaction.
- There are thousands of pen-testers in Australia. There is no news since they sign disclosure agreements, hence unable to discuss.
- Linux is commonly used since several tools are based off linux.
- Linux Mint works well with the latest generation laptops.
- Executive profiling: Devices, transport, social clubs, addresses, public info.

15.1 Attack Preparations

Waterhole Attack: *Attackers poison a website with the goal of attacking the target, who is expected to visit that particular site. Attackers may break into the website and then modify the website code so that malware is injected to the user. The victim may be directed to download a backdoor as the payload. Advanced waterhole attacks may even redirect users to an external website and then re-redirect them into the true website.*

15.1.1 Phase 1 - Victim Evaluation

- Gather information on target
- Prepare for the actual attack (such as IP ranges, platforms and usage patterns of target)
- Place the right waterholes to filter out unwanted victims from the true targets. This can be achieved by passive information gathering from social media, active scanning and preparing additional waterholes.

15.1.2 Phase 2 - Preparation for Infection

The second phase is about **infecting**. That is, generate fingerprints of the victim in order to find the best suited infection method. These methods can include appropriate software/device exploits or social engineering techniques.

During this time, you need to:

- **Activate waterholes** or send **spearphishing**
- Execute **fingerprinting** usually done with JS
- Given the above conditions and the target, a suitable **exploit** is chosen. If this is not applicable or possible, then **social engineering** issued.

15.1.3 Phase 3 - Active Infection

In this phase, the attacker is already in the network and will want to spread (quantity and quality regarding access to the system).

- **Trojan Supported Reconnaissance:** An initial reconnaissance tool is usually placed to suss out the network of the victim. Generally speaking, the tool doesn't have much capability itself but aims to host a more powerful malware at any time.
- **Gaining Persistence:** If the recon tool is successfully placed and hidden, then the actual malware is released. This malware will have much more functionality and create deeper persistence within the system.
- **Lateral Movement:** Here, the attacker begins to move laterally (on the same level of access) to gain additional information. Lateral movement is often done using normal tools that are used to manage systems. Usually, this step includes collection of credentials and an attempt at elevating privileges on the network.
- **Data Exfiltration:** As soon as the attacker begins to steal data, they will want to export it outside of the network without being discovered. To do so, the attacker will compress the data and send it piece by piece to reduce the bandwidth.

16 Readings

16.1 Unique in the Crowd

A reading about the re-identification of individuals.

- 15 months worth of human mobility data with $n = 500,000$.
- Users were traced anonymously into approximate zones based on the closes k towers
- It was found that 12 points of data was needed to completely uniquely identify a fingerprint.
- Specifically with geolocation (time and space), time does not do much at all. That is, increasing the approximate time gap does not help preserve anonymity. This is because spatial resolution is the largest factor, where most fingerprints were successfully identified based on their location.

16.2 Is Cybersecurity incompatible with digital convenience

This reading discusses privacy vs convenience.

- Contends that companies need to move away from the one-size-fits-all approach. This is because different customers think and feel differently about their own security expectations.
- The research suggests three types of customers; those who prefer convenience, those who prefer security and those who are comfortable with a blended model.
- It was also found that the majority of the population **wanted** to be able to automatically log in without entering credentials, as well having the ability to store all usernames and passwords in some secure vault. However, it was also found that people **wanted** to have extra-secure credit card procedures, as well as the option to have one-time downloaded passwords as a single use login method.

16.3 Petya

A ransomware malware which used EternalBlue

- Was targeted at the Ukraine shipping company "Maersk"
- Was the first batch of Eternal Blue exploit atacks which demanded payments to be made (before WannaCry)

16.4 NotPetya

An attack using EternalBlue (NSA penetration tool) and Mimikatz (proof of concept that passwords were accessible on a computers' memory).

- EternalBlue took advantage of a vulnerability, allowing hackers to remotely execute any code on any unpatched machine.
- Mimiktaz was a tool to pull passwords out of RAM and use them to hack into other machines with the same credentials.
- Even though EternalBlue was patched, the combination of the two was troublesome. *Computers that weren't patched could be infected to grab credentials to then infect computers that were patched.*
- The NotPetya malware resulted in a global total of 10 billion in damages.
- The main lesson learned from this attack is that cyberwarfare knows no boundaries. That is, any country and any organization is vulnerable to cyberattacks.

16.5 Equifax

An example of failing to patch / deciding not to patch

- Equifax was a large credit reporting company which had a data breach exposing 144 million records
- Victims were USA, Canada and even Britain
- The weakness was due to Apache Struts, which was very fixable since the pathc was released
- The breach was actually known 2 - 3 months prior to public declaration in which several executives sold company shares and retired
- The CEO was sentenced to 4 months in prison due to insider trading, though much better as prior years would be no prison time
- Since servers are always full of dependencies and can have vulnerabilities years old, it would be impractical to take them down. Here, this risk did not pay off.

16.6 Olympic Destroyer (2018 Winter Olympics)

A stuxnet (malicious computer worm) attack

- The attack broke the official Olympics website and all wifi at stadiums. Side affect: broadcasts were down.
- The attack was thought to originate from North Korea, though a Kaspersky analysis discovered that it originated from a Russian group APT
- It was difficult to attribute attacks to any party
- The ethical and strategic viability of retaliation needs to be considered. Examples include some Russian attacks during the French election, as well as Chinese attacks on the Australia Parliament.

16.7 Capital One Attack

Human error based on misconfigured servers

- Problem stemmed in part from a misconfigured open-source Web Application Firewall (WAF) that Capital One was using.
- The WAF was deployed with an open-source Apache Web Server to provide protections against several classes of common exploits.
- However, the misconfiguration allowed the intruder to trick the firewall into relaying requests to a key back-end resource on the AWS platform. This resource (known as metadata service), is responsible for handing out temporary information to a cloud server including current credentials sent from a security service to access any resource in the cloud.
- Specific to Capital One, the misconfigured WAF was assigned too many permissions. It was allowed to query any bucket of data and read the contents.
- The attack made was called **Server Side Request Forgery (SSRF)** in which a server can be tricked into running commands it should not be able to, including commands that allow it to talk with metadata services.

16.8 ShadowHammer

A stuxnet (malicious computer worm) attack

- Attackers executed a supply chain attack either prior to game development completion, or had access to the source code
- The attack was payload which gathered usernames, computer specs and operating system versions.
- The main issue from this attack is that the attackers were able to obtain valid certificates to compromise their victims' development
- Software vendors are recommended to introduce additional checks for potential malware injections **even after it is digitally signed**

16.9 WannaCry

A ransomware attack which encrypted data and made it inaccessible.

- Executed through a network worm called "WannaCrypt"
- Utilized EternalBlue (like NotPetya) which was distributed by a group called The Shadow Brokers
- Microsoft released a killswitch which prevented further damage
- Payment did not guarantee the return of data, where a total of $130,000 USD was payed out

16.10 Spyfall

An article explaining the modern day transition of spying.

- Traditional methods of spying relied on deception based on identity. Until recently, profiles that were difficult to crack could be created where spy agencies had no choice but to wait. This fails in modern day as facial recognition has started to become commercially available.
- Counterintelligence is also now much more internet based. Old scans through CCTV footage, social media scans, etc can be used to pull together a true profile.
- Phones nowadays are also less reliant due to their capability of transmitting locations real-time. Even using privacy tools such as VPN, Tor or public wifi hot-spots can arouse suspicions - *why would they need to use this?*
- Essentially you just need to be aware of how traditional methods have become redundant compared to modern day era spying. Examples include "one use" spies who come from a legitimate background and are hired for a single case.

16.11 ANU Data Breach

A significant databreach with several attackers achieved via spearphising emails. Unknown amounts of data dating up to 19 years ago was potentially affected.

- The initial means of infection was through spearphising which did not require any interaction. Here, the attackers tried to steal a broad range of **credentials** for administrator accounts in case some expired or compromised.
- The attackers were able to create a foothold in the network and were able to identify more targets of interest, run tools and compromise several other machines.
- One of the major issues from the breach is the loss of personal identifiable information. ANU is still currently looking online for related stolen data or credentials that may be traded or sold online.
- Post-Breach operations included the complete identification and replacement of all legacy email and legacy devices. 2FA has also now been enforced (at an accelerated deployment).

16.12 Adversarial Threats

A paper summarizing the affects of whistle-blowing (i.e Edward Snowden from the NSA) due to the mass surveillance technologies coming into play. It explores how other countries are using mass surveillance and how common weaknesses are being exploited at both a criminal and government level.

- The PRISM Program which allowed the NSA to essentially scrape metadata from large providers (Amazon, Google, Facebook, Skype, etc)
- The BULLRUN Program which aimed to create back-doors into all telecommunication systems, encryption standards, operating systems, etc. The NSA paid the creators of RSA $10 million to include a weak random number generator which allowed the NSA to decrypt it easier.
- X-KEYSCORE is a program aimed to survey on targeted personals. A deep packet inspection technology was created, which was so powerful that it gave real-time filtering for anything. For example, an analyst could upload a logo and all results would be instantly returned.
- The TURMOIL and TURBINE programs which allowed the NSA to inject packets into a connection, specifically, malware.
- MUSCULAR was a program designed to infiltrate all private optic fibre cables that ran internally between Google and Yahoo datacentres.
- The NSA has power over private companies such as Google and Facebook, where a court order would make it very difficult to be refused.

16.13 This is the way I create my passwords

Essentially discusses about how the normal population will usually reject security advice.

- The paper found evidence for pre-existing routines, change resistance an endowment effect when creating passwords. That is, the normal population may change and follow secure password generating strategies but will eventually fall back to bad habit.

16.14 My Health Records

A system where every Australian (who doesn't opt out) will have their medical records and information pooled into a single digital system hosted by the government.

- There have been 42 data breaches that have occurred, where it is claimed that none of them had any purposeful or malicious attacks compromising the integrity or security of the My Health Record system
- My Health Record system falls under the NDBS system so they have been routinely reported by the Agency and the Department of Human Services which runs the identity scheme which underpins My Health Record to the OAIC.
- According to the NDBS, My Health Record only found suspected fraud against the Medicare program where unauthorised Medicare Claims were submitted, resulting in incorrect records appearing the My Health Record database,
- The data stored goes through a database with access controls, but **is not fucking encrypted and is stored in plain format**.

16.15 SingHealth Data Breach

Here, attackers targeted SingHealth (largest health care institution) and stole personal profiles of 1.5 million patients, along with the details of prescriptions for 160,000 others. From this attack, Singapore's prime minister was claimed to be targeted specifically and repeatedly.

- Apparently there are claims that it was state-sponsored
- As for the 1.5 million patients affected by the attack, the only information lost were their personal profiles. These included their names, addresses, gender, race, date of birth, and national registry numbers, but not medical information.
- The attack was carried out using an advanced persistent threat (APT), where the nature of such attacks are conducted by nation states using very advanced tools

17 Exam Revision

1. **Pineapples**

    (a) Pineapples are security tools which aim to find wireless security risks. They are commonly used by penetration testers to test the robustness of organizational security.

    (b) The most common way a pineapple is used is via the PineAP, which will scan and continuously listen for SSID's. Specifically, the PineAP is able to collect and recognize the SSID's stored on the connected devices in order to infer additional information about the owner (such as where they live, work / study or eat). This inference is possible because SSID's can be geolocated via wigle. Another method is using an Evil Portal which which essentially creates fake websites to steal credentials.

    (c) Wifi pineapples teach us that Public networks are always at risk and to use a VPN if we ever decide to connect to public wifi. They also teach us to never go on HTTP where possible (plain-text credentials), but rather HTTPS.

    (d) One way to thwart an attack is to forget all SSID's on devices to prevent our device from broadcasting additional SSID's. This means that the pineapple is less likely to force your device to connect to an impersonated SSID. In addition, you can disable wifi when not in use (iOS people will have more trouble, but Android users are more safe).

    (e) The defensive actions don't really thwart the attack and aren't really effective in a sense that there is no true way to prevent connecting to a wifi pineapple. However, you can always be secure and vigilant by visiting HTTPS and VPNs if you are in a public area.

    (f) Mainly penetration testers who are hired to purposely break and test the capabilities of an organizations' security procedures, though of course black hat hackers who have malicious intent can also use the wifi pineapples to steal data. Finally, a normal user at home can also use it to test their own wifi security at home.

    (g) The professional ethical constraints on using pineapples depends on the contract. For example, creating a honeypot without consent or previous agreement is illegal, as passerby's will connect to the wifi pineapple where you will be able to essentially see everything being sent through. Strictly speaking, wifi pineapples are ethically legal if they are used with consent and for testing purposes.

2. **What are the key components of what the Access and Assistance Law 2019 does?**

    (a) Specifically for a company in Australia, a *Technical Assistance Notice* will require the company to turn over information or data that the provider already has. In addition, a *Technical Capability Notice* may require some re-engineering to the system in order to provide **new** data that the provider would not otherwise have. This can be installing law enforcement software or to modify key parts of the providers' system in order to allow listening.

    (b) *Unsure, but I recall a hefty fine of up to 7.3 million if they fail to comply.*

    (c) Customers will unknowingly be listened on, even if their messages are truly encrypted. In this case, the privacy is completely lost as any law enforcement is able to read their messages without consent or warrant. In the worst case, the backdoor is compromised and malicious attackers can abuse it to steal information and data.

3. **What is the C.I.A triad and why is it important?**
The CIA triad refers to the model in InfoSec which helps identify problems and provide the required solutions. Specifically,

    - Confidentiality ensures that only those who should have access can access it,
    - Integrity to ensure information cannot be modified without detection or notification, and
    - Availability which ensures information can be accessed when needed.

4. **Make sure you know these readings:**
CapitalOne (bad management), NotPetya (EternalBlue and Mimikatz), WannaCry (TODO), Maersk (TODO), Olympic Destroyer (Stuxnet), ANU (TODO), Equifax (failing to patch).

5. **Consumer privacy matters – but why?**

    (a) There are several risks concerning the loss of digital privacy. The most important is probably the way consumers will be treated during hiring processes, where companies can hire using discrimination based on the digital history of a person. In this scenario, people can be denied before they even apply for jobs.

    (b) *Unsure? We can protect workers of the future by preserving and advocating for personal* privacy.

(c) *Unsure? But I'm sure consumers will be sold different things at different prices if there is a loss of digital privacy. Consider insurance companies that may charge insanely expensive premiums to disabled or elderly people*

6. **Review the Notifiable Data Breach Scheme**

   (a) The NDBS applies to all entities with current existing obligations, as well as government agencies, businesses, not-for profit organizations with an annual turnover greater than 3 million, private sector health service providers, credit reporting bodies and providers, as well as entities that trade in personal information.

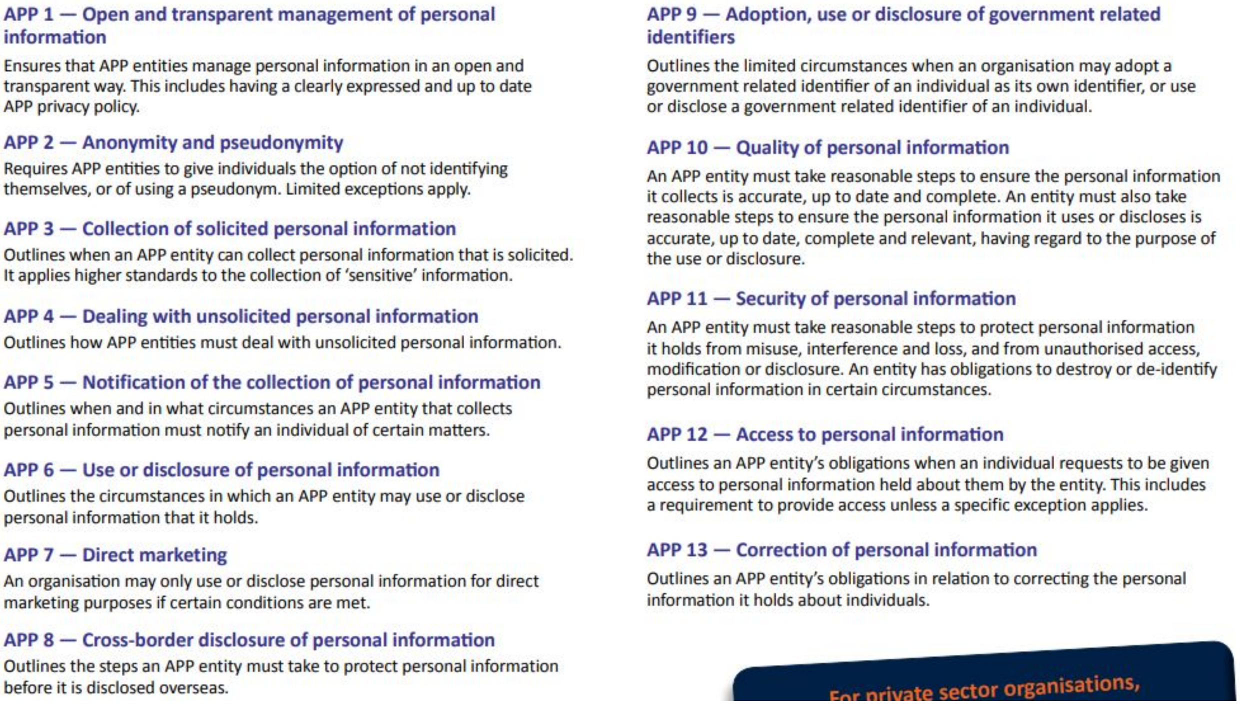
   (b) These must all be reported to the Office of the Australian Information Commissioner (OAIC).

   (c) Organizations must disclose (publicly) if there has been an unauthorised access / unauthorised disclosure of personal information / loss of personal information and if the data breach is likely to result in serious harm to individual(s). **Organizations will have up to 30 days to assess whether or not the breach was harmful.**

   (d) The penalties include fines of $360,000 for individuals and $1.8 million for organisations

7. **Australian Privacy Principles – Please know them**

   (a) The APP's are essentially a list of policies that organizations must adhere to when working with personal information. In total, there are 13 policies which cover the usage of personal information, working with sensitive information and preserving anonymity of persons.



APP 1 — Open and transparent management of personal information

Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

APP 2 — Anonymity and pseudonymity

Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

APP 3 — Collection of solicited personal information

Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

APP 4 — Dealing with unsolicited personal information

Outlines how APP entities must deal with unsolicited personal information.

APP 5 — Notification of the collection of personal information

Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

APP 6 — Use or disclosure of personal information

Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP 7 — Direct marketing

An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP 8 — Cross-border disclosure of personal information

Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP 9 — Adoption, use or disclosure of government related identifiers

Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

APP 10 — Quality of personal information

An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 — Security of personal information

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

APP 12 — Access to personal information

Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13 — Correction of personal information

Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

For private sector organisations,

   (b) **This is APP12 specifically.** Here, individual citizens are only allowed access to *personal information* as defined by the APPs. Citizens may also access personal information of other individuals (marriage certificates if both parties are applicable). Furthermore, citizens are allowed access to their own personal information **even** if it includes information about another individual unless the refuse access applies.

   (c) Organizations must protect and store the latest (hence most correct) details of a citizens' personal information. if the data is stolen or compromised, they have an obligation to destroy or notify the individuals. (works hand in hand with the NDBS)

8. **Privacy – social media and other platforms have many impacts on personal privacy. Be able to describe these, and their secondary impacts.**
   The main target can have all their personal information compromised, with secondary impacts to their relatives and friends.

9. **Openness versus Closedness of information cultures in organisations and societies as a whole is important.**

(a) We should share secret information when it is in the best interest of both parties. These cases can be during war times or for preventing terrorist attacks during special formed treaties. Australia and the US have a particular agreement on the sharing of such defence secrets.

(b) Indeed, data leaks are a common data breach where an inside employee *whistle-blows* in interests of exposing fraudulent activity or crimes against the public. While whistle blowing has exposed several top secret illegal government activities, there is actually little control the public has in seeing the exposed data and procedures undertaken.

10. **Surveillance**

    (a) TODO READING - JK Rowling's Linguistic Footprints, My Health Records, the hack of Sing Health and Paul Farrell's metadata.

11. **Defensive technologies: be able to describe how these provide defense in a technical and practice (end-user) way:**

    (a) Tor is essentially a multi-layer VPN service with no centralised system which guarantees security so long as at least one of the proxies remains honest. This means users can communicate or browse the internet without worrying about 3rd party surveillance or MiTM attacks.

    (b) Panaptoclick is a good website to show how much can be discovered from a device based on its fingerprinting and cookies. In addition, the Brave browser is (at least my recommendation) a chromium based browser which attempts to eliminate all possible tracking and fingerprinting.

    (c) Duck Duck Go is a search engine that provides searches without any tracking. Although there are many other similar search engines like First Page, they are still based off Google and it is much easier to trace it back.