11. Incident Response, Privacy and Red Teaming

COMP6441 • KC Notes

11.1 Incident Response

- There are often capable people who respond to incidents.
  - People are affected by **emotions, stress, lack of information**
  - These people at the scene **should not be blamed** for the outcome
  - In the Lindt siege, there were uncertainties, anger from families and from the police
- Incidents like the Lindt siege do not go perfectly
  - In hindsight, there was bad planning right when the incident started
  - People should be **training** immediately for the event
  - **Plans** to be put in place
  - **Thinking** to be done in advance
- **Wisdom in hindsight**: we make systematic and thorough reports **after** an incident, but we tend to not carry out the information in future incidents
  - We should **learn from mistakes** from both in and outside of the cyber world

11.2 Privacy

11.2.1 OVERVIEW

- Secrets and information in the public usually **go one way** – they **spread**, and rarely can be **removed or put back** from the public
- **Project Angelfire**: plane with a camera can reconstruct what happens when an IED explodes
  - Plane flies there, **roll film backwards** to find the car and find who planted the bomb
  - Also works with robbery, assassinations – **roll the tape back, then roll the tape forward.**
- Benefits to information
  - Knowing more information helps police, security
  - Helps companies target products
- Risks to information
  - Protests: Chinese students gone missing
  - Women in abusive relationships tracked down
  - Other dissonant group information, like ethnic genocide
    - But can work the other way – driving Jewish people out of Denmark by looking at surnames in the phone book
- **“Nothing to hide”**
  - It may be easy to say it now when you trust the government, but **how about later**? The information would still be accessible and stays with the new government later.

11.2.2 WHO OWNS YOUR DATA?

- **Henrietta Lacks**: the owner of HeLa cells that helped **significantly in the medical field**
    - It is good that it is out there, but could be **abused**, and does not respect her privacy
- **Big Data**: primarily **personal data about individuals**
    - Who should control this data? Maybe governments, but companies?
    - Google NDA – the **intellectual property belonged to Google**, and ideas/IP had to be handed back
    - Two sides: **companies are glad to hold data** but **do not want to share it themselves**
- Individuals should **be more empowered**
    - Users should be able to have more control over their phones, and what sort of data it releases (e.g. MAC addresses, Wi-Fi access, EMF waves)
- **Perfect forward privacy**: where data from the past is safe

11.2.3 GUEST SPEAKER: NSW PRIVACY COMMISSIONER ELIZABETH COOMBS

- Privacy Commissioner:
    - Has no definitive power, but can ask for information, and has power of the Royal Commission
    - Is a regulator but **works with people** to prevent privacy breaches
    - Not a public servant, is independent – can **question government legislation**
- NSW Laws:
    - 1998 Privacy and Personal Information Protection Act (PPIPA)
    - 2002 Health Records and Information Privacy Act (HRIPA)
        - **Health information** is more sensitive and important
- Laws have no definition of privacy.
    - PIPPA: information used to reasonably **identify you**, including **images, fingerprints and an opinion about an individual**
    - HRIPA: personal (name, address) and physical functions
    - Not a black and white definition, and is **very contextual**
- There are separate laws for state and national levels – state can look at both public and private healthcare information
- **Privacy has transitioned from law based** to involving psychology, IT, engineering, maths
    - People are more aware of privacy and are asking more questions
    - People make assumptions until it starts affecting themselves – when they are in risk
    - Privacy **matters** when they are **a parent** (child info) or **getting a job**
    - No universal manners or etiquette for privacy on Facebook

11.3 Red Teaming (Guest Speakers: Westpac)

- **Red Teaming** involves testing **security controls** and **their effectiveness**
    - They **identify, improve and block** infrastructure and applications
    - Red Teams involve a lot of social engineering
- **Technology and protocols change**, but hacking has remained relatively the same
    - Is usually a cat and mouse game
- Red teaming involves:
    - **Diversity and community**
        - Different ways of interpreting and thinking outside the box
        - There are no hard rules, look through different angles
    - **Preparation**
        - People may unknowingly pass on emails, or call the police
        - Homework is very important, recon makes it become personal
        - Google is usually the first step in recon
    - **A Purple Team**
        - The team is an interface between the red and blue
        - Creates learning, uplifts monitoring
- Some tips:
    - Don’t click on dodgy links
    - Check your Facebook privacy settings
    - Make sure everything is patched