Encryption & Data

Technology, choice, and whether we're making ourselves more secure or not

For The Police Security Conference
May 2018

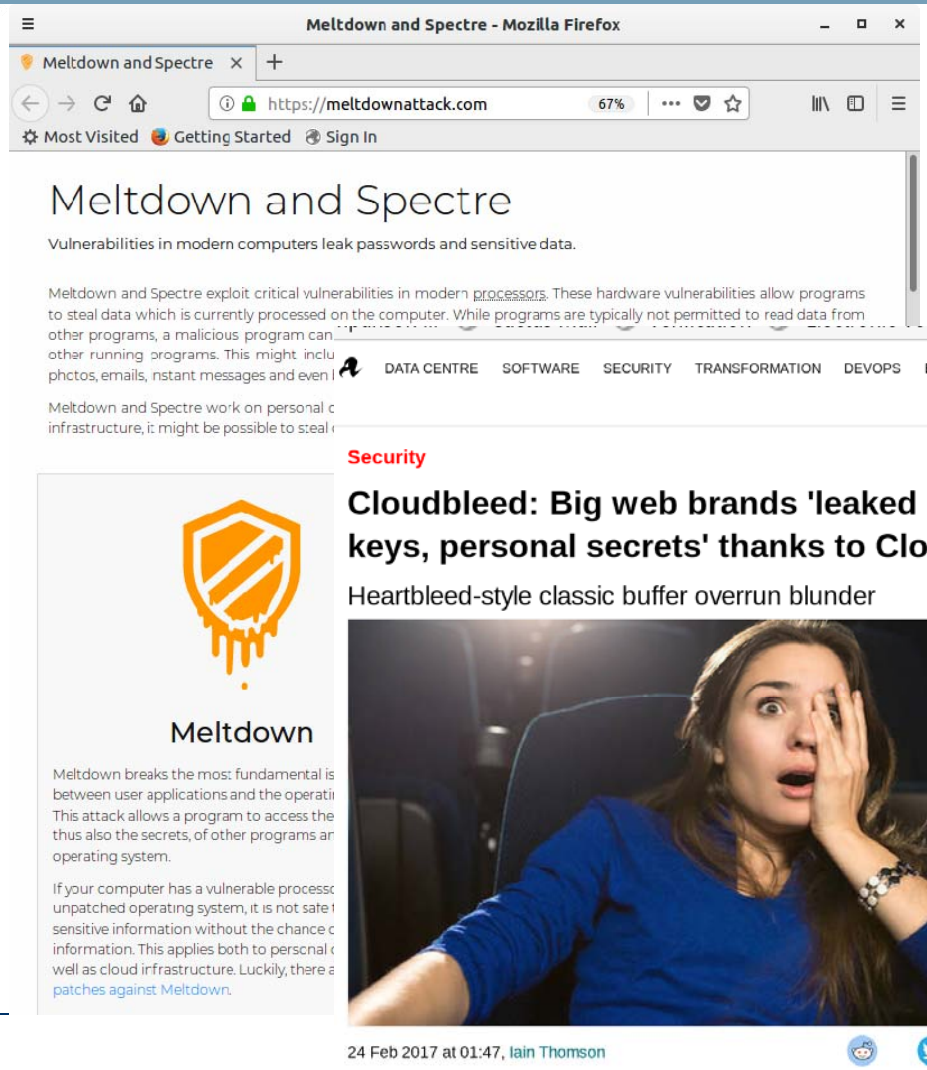
Dr Vanessa Teague
School of Computing and Information Systems,
The University of Melbourne
vjteague@unimelb.edu.au

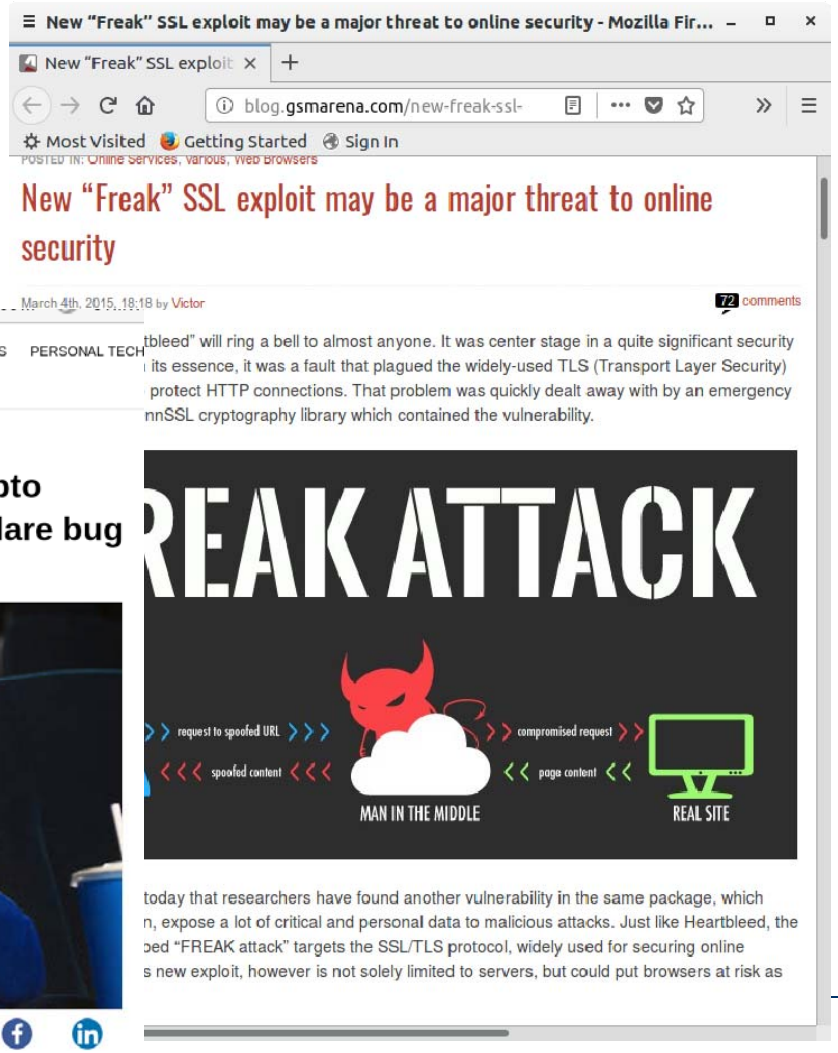
Roadmap

- Encryption
  - End-to-end encryption
    - For sms/email/cloud storage
  - Non-end-to-end encryption
    - And the privacy implications
  - What information is available now?
    - Content
    - Metadata
  - Things to consider when making changes
    - Will it work?
    - Will it make other things less secure?
  - Example: storage for police body camera video
- Data ethics: some questions about body cameras

Making things secure is hard

And often broken





What's encryption?

- Sending messages that are secret from everyone but the intended recipient
- The sender has to "hide" the message for sending, so nobody else can understand it
  - This is called **encrypting**
  - It uses a key, i.e. a big number
- The receiver has to "un-hide" and recover the message
  - This is called **decrypting**
  - Needs the right key

Modern encryption looks something like this

- two large prime numbers p,q
  - $N=pq$
  - Ciphertext $c = (m \,||\, r)^e \bmod N$
    - ($||$ just write the randomness after m)
- The receiver can decrypt because she knows p and q
  - Let $\Phi(N) = (p-1)(q-1)$
  - She generates a private key d s.t.
    - $d.e = 1 \bmod \Phi(N)$
    - e.g. using Euclid's Algorithm
  - Theorem (Euler): for all x coprime with N,
    - $x^{\Phi(N)} = 1 \bmod N$.
- Decryption: compute c^d
  - $c^d = (m \,||\, r)^{ed} \bmod N$
  - $= (m \,||\, r)^{k\Phi(N)+1} \bmod N$, for some k
  - $= (m \,||\, r) \bmod N$
  - Delete r, retrieve m.

What's end-to-end encryption?

- I'd call it "normal" encryption
  - In which the intended recipient is the only one with the decryption key

What's not end-to-end encryption?

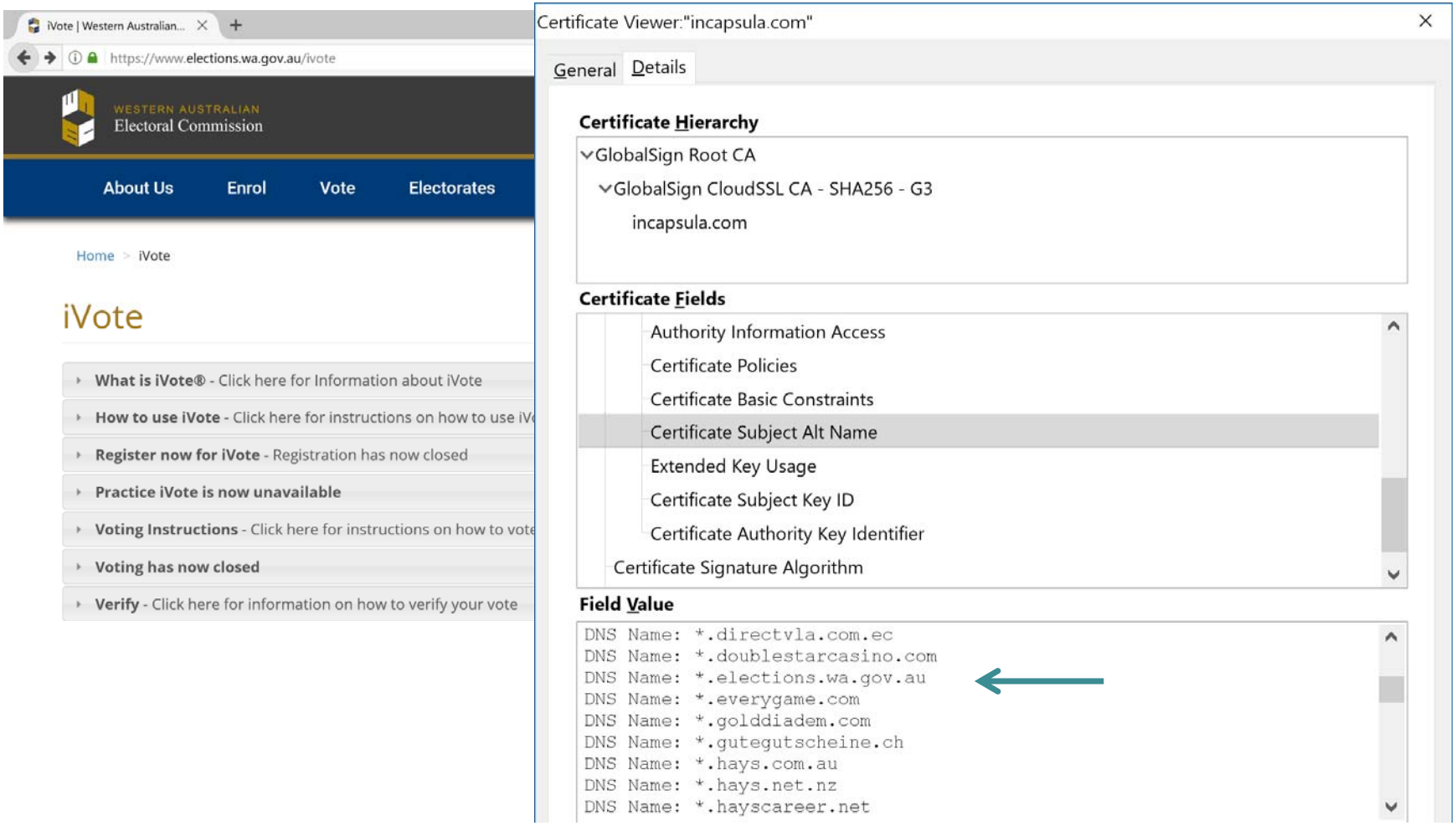
- So what's non-end-to-end encryption?
  - When the holder of the decryption key isn't the person you feel you're talking to
  - e.g. ordinary Facebook posts, Skype, Hangouts, Gmail…
  - Your message is decrypted by the company, then re-encrypted and sent to the next person

Intermediaries / service providers

- These intermediaries get a lot of information
- Better processes for accessing (with a warrant) the information they already have would be great
  - And wouldn't do any harm to anyone's security
- Often they get metadata for end-to-end encrypted services
  - Who communicated with whom when

THE UNIVERSITY OF MELBOURNE

Not end-to-end encrypted: WA Internet voting



Recommendations

- **Use end-to-end encryption whenever you can**
- For SMS use Signal/Wikr/WhatsApp *etc*
  - Check you've got a valid version
  - check the public keys of your friends
- Mac: iMessage, faceTime
- Use encrypted cloud storage
  - Encrypted by you

Weakening / backdooring encryption has opened opportunities for others to exploit it

- Clipper
  - A malicious party could trick the police into decrypting an innocent person's key
- Restrictions on key size for "export grade" crypto
  - FREAK / logjam
    - Including NSW iVote
- The DUAL-EC-DRBG
  - A weak(ened) random number generator, observed with a rekeyed backdoor
- Wannacry
  - An NSA tool redeployed as ransomware

Forced entry into devices?

- a.k.a. the Apple/FBI controversy
- The FBI asked Apple for a special software update, signed with Apple's key, for extracting data from just that phone
- Apple argued that that software in the wrong hands could become a wider security risk
- And that suspects would turn off updates

Further reading

- “Decrypting the encryption debate: a framework for decisionmakers”
- https://www.nap.edu/catalog/25010/decrypting-the-encryption-debate-a-framework-for-decision-makers

- Making it easier to catch criminals without making it easier to commit crime

Example: storage of police body camera videos

- Don’t store unencrypted videos on other people’s cloud servers
- Use end-to-end encryption
  - For privacy
- And digital signatures for integrity
  - To prove they haven’t been altered

Speculations and questions about body cameras

- Police Minister Lisa Neville said the cameras would be good for the community and police.
- [1] “It helps with early guilty pleas, it helps with quicker prosecutions, it reduces the paperwork for Victoria Police members.”
- [2] “It is also really critical for improving police accountability and behaviour,” she said.

- Jeff Gray, Orlando Florida.

- https://www.youtube.com/watch?v=jD6sige9ZYI
- Note that I am not endorsing or judging, just pointing out that this story raises some interesting questions

Information Imbalance

- [1] “It helps [police] with…”
- [2] “It is also really critical for improving police accountability…”

- Is it acceptable for other people to video their interactions with police?
- Should police have discretion about when to turn the camera on or off?
- Should a person have the right to view/download police video of them?

- Information imbalance is generally good for aim [1] but bad for aim [2]

Not always the consequences we expect

- From the police car
- Officer 2: Hey, do you want me to go straight to BRC [booking and release centre] or do anything special?
- Officer 1: [Unintelligible]
- Officer 2: I'm sorry?
- Officer 1: Frankie's on his way over there, and we're going to find the L. T. [lieutenant] to see if there's anything else we need to do. You're not recording right now while you're talking?
- Officer 2: I'm sorry?
- Officer 1: Are you still recording yourself?
- Officer 2: Uh, I only have same-car right now, but the mic is running.

Speculations and questions about body cameras

- Police Minister Lisa Neville said the cameras would be good for the community and police.
- “It helps with early guilty pleas, it helps with quicker prosecutions, it reduces the paperwork for Victoria Police members. It is also really critical for improving police accountability and behaviour,” she said.
- “We know it gets rid of a lot of frivolous complaints about Victoria Police members so we know if there are issues, it is all recorded.”

Questions?