



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



- 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



THE UNIVERSITY OF
MELBOURNE

Making things secure is hard





Meltdown and Spectre - Mozilla Firefox

Meltdown and Spectre x +

https://meltdownattack.com 67%

Most Visited Getting Started Sign In

Meltdown and Spectre

Vulnerabilities in modern computers leak passwords and sensitive data.

Meltdown and Spectre exploit critical vulnerabilities in modern processors. These hardware vulnerabilities allow programs to steal data which is currently processed on the computer. While programs are typically not permitted to read data from other programs, a malicious program can...

DATA CENTRE SOFTWARE SECURITY TRANSFORMATION DEVOPS BUSINESS PERSONAL TECH

Meltdown and Spectre work on personal c infrastructure, it might be possible to steal r

New "Freak" SSL exploit may be a major threat to online security - Mozilla Fir... - x

New "Freak" SSL exploit x +

blog.gsmarena.com/new-freak-ssl

Most Visited Getting Started Sign In

POSTED IN: Online Services, Various, Web browsers

New "Freak" SSL exploit may be a major threat to online security

March 4th, 2015, 18:18 by Victor 72 comments

bleed" will ring a bell to almost anyone. It was center stage in a quite significant security its essence, it was a fault that plagued the widely-used TLS (Transport Layer Security) protect HTTP connections. That problem was quickly dealt away with by an emergency mnSSL cryptography library which contained the vulnerability.

Security

Cloudbleed: Big web brands 'leaked crypto keys, personal secrets' thanks to Cloudflare bug

Heartbleed-style classic buffer overrun blunder

Meltdown

Meltdown breaks the most fundamental is between user applications and the operati This attack allows a program to access the thus also the secrets, of other programs ar operating system.

If your computer has a vulnerable process unpatched operating system, it is not safe t sensitive information without the chance c information. This applies both to personal c well as cloud infrastructure. Luckily, there a patches against Meltdown.



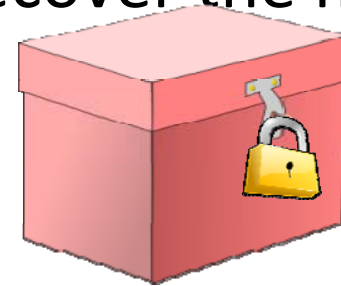
24 Feb 2017 at 01:47, Iain Thomson



today that researchers have found another vulnerability in the same package, which n, expose a lot of critical and personal data to malicious attacks. Just like Heartbleed, the ped "FREAK attack" targets the SSL/TLS protocol, widely used for securing online s new exploit, however is not solely limited to servers, but could put browsers at risk as



- 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





- 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.
 - $d \cdot e = 1 \bmod \Phi(N)$
 - 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





- 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



Not end-to-end encrypted: WA Internet voting

The screenshot shows the iVote website interface on the left and a Certificate Viewer window on the right. The website header includes the Western Australian Electoral Commission logo and navigation links: About Us, Enrol, Vote, and Electorates. The main content area is titled 'iVote' and contains a list of links: 'What is iVote', 'How to use iVote', 'Register now for iVote', 'Practice iVote is now unavailable', 'Voting Instructions', 'Voting has now closed', and 'Verify'.

The Certificate Viewer window, titled 'Certificate Viewer: "incapsula.com"', shows the following details:

- General** tab selected.
- Certificate Hierarchy:**
 - GlobalSign Root CA
 - GlobalSign CloudSSL CA - SHA256 - G3
 - incapsula.com
- Certificate Fields:**
 - Authority Information Access
 - Certificate Policies
 - Certificate Basic Constraints
 - Certificate Subject Alt Name
 - Extended Key Usage
 - Certificate Subject Key ID
 - Certificate Authority Key Identifier
 - Certificate Signature Algorithm
- Field Value:**
 - DNS Name: *.directvla.com.ec
 - DNS Name: *.doublestarcasino.com
 - DNS Name: *.elections.wa.gov.au
 - DNS Name: *.everygame.com
 - DNS Name: *.golddiadem.com
 - DNS Name: *.gutegutscheine.ch
 - DNS Name: *.hays.com.au
 - DNS Name: *.hays.net.nz
 - DNS Name: *.hayscareer.net

A blue arrow points to the 'DNS Name: *.elections.wa.gov.au' entry in the Field Value list.



- **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



- 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



- 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



- “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



- 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



- 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



- [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]



- 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.



- 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?