Stopping Exfiltration

Mark S. Miller, Agoric
tc39 May 2018, NYC

Exfiltration

- Covert and Side Channels
  - “Normal” cache timing attacks
  - Meltdown & Spectre, all variants
- Overt theft
  - Electron shock
  - “Vetted” libraries. Walgreens, 8000 others

Unworkable “advice”

“Only origin boundaries are security boundaries.”

implies

Use only 3rd party libraries you’ve fully vetted.

Shedding Liability vs. Safety

"Only origin boundaries are security boundaries."

implies

Use only 3rd party libraries you've fully vetted.

"Pinto blew up because of operator error."

Cars became more forgiving of realistic behavior.

Shedding Liability vs. Safety

"Only origin boundaries are security boundaries."

implies

Use only 3rd party libraries you've fully vetted.

"Pinto blew up because of operator error."

Cars became more forgiving of realistic behavior.

We should too.

“Drive-by Key Extraction Cache Attacks from Portable Code”

“… side-channel attack … extract ElGamal, ECDH and RSA decryption keys from various cryptographic libraries.

… implementations of **supposedly-secure constant-time algorithms** … are vulnerable to our attack.”

[emphasis added]

From 2017 frozen-realm proposal

"… computation that is limited to fail-stop implementation-defined determinism ***cannot read covert channels and side channels*** …

Nothing can practically prevent signaling on covert channels and side channels, but approximations to determinism can practically prevent confined computations from perceiving these signals."

[emphasis added]

But Meltdown, Spectre, and variants? Still true!

"… computation that is limited to fail-stop implementation-defined determinism ***<u>cannot read covert channels and side channels</u>*** …

Nothing can practically prevent signaling on covert channels and side channels, but approximations to determinism can practically prevent confined computations from perceiving these signals."

[emphasis added]

Overt theft

Electron shock

“Severe Electron framework vulnerability impacts apps like Skype and Slack

… critical **remote code execution** vulnerability”

[emphasis added]

Brendan tweets

"Some Electron app vulns … could pwn via **Function.prototype.apply** override.

Without **POLA** and **sandboxing**, very hard to fix or *a priori* rule out. Hence **Win10 store ban**."

[emphasis added]

Brendan tweets

"Some Electron app vulns … could pwn via **Function.prototype.apply** override.

Without **POLA** and **sandboxing**, very hard to fix or *a priori* rule out. Hence **Win10 store ban**."

[emphasis added]

POLA === Principle of Least Authority

Princeton "**No Boundary**" series

"… third-party trackers exfiltrating personal information from web pages, browser password managers, and inputs typed into forms."

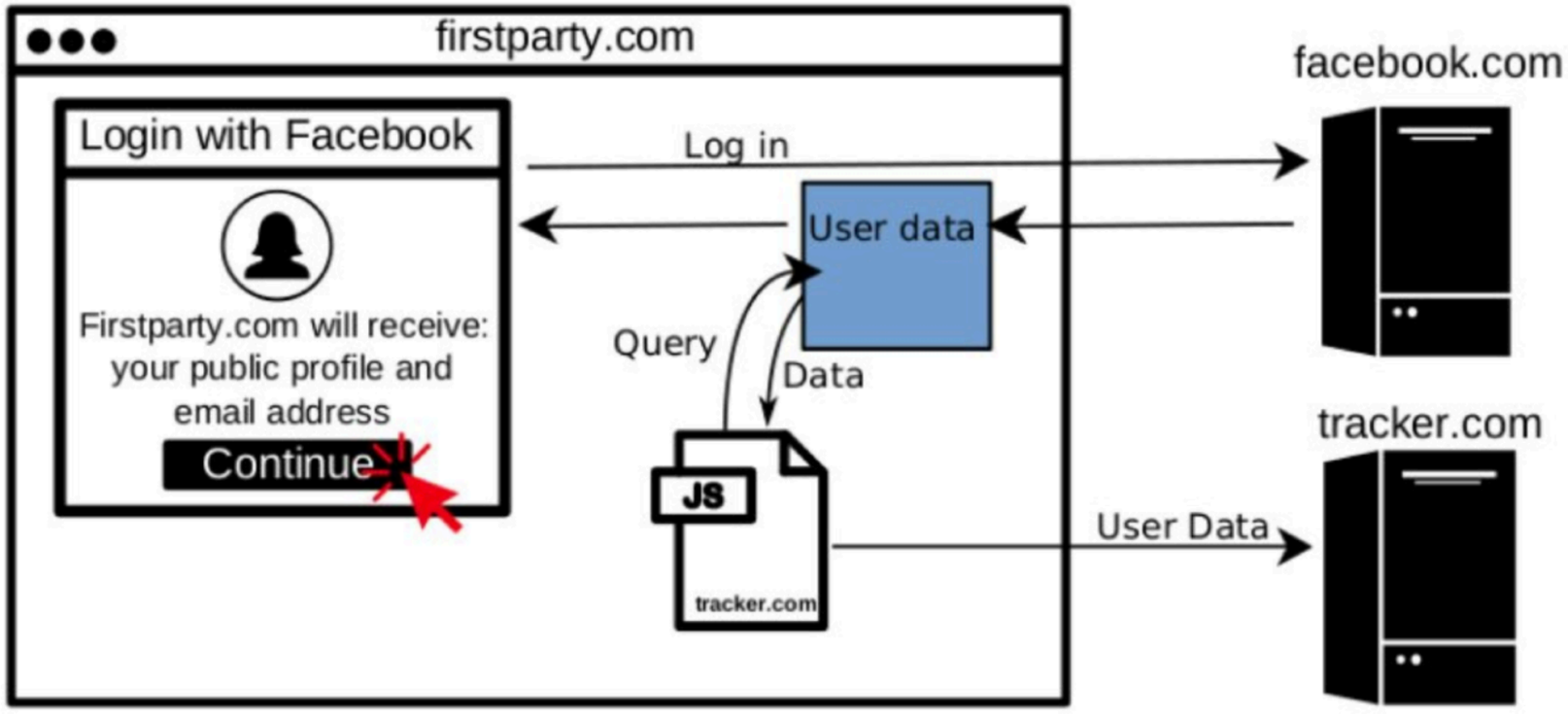
"Website operators are in the dark about privacy violations by **third-party scripts**"

[emphasis added]

Princeton "**No Boundary**" series

"… third-party trackers wait for users to 'Login with Facebook', then exfiltrate user identifiers from Facebook by abusing the **access that Facebook grants** to the website."

[emphasis added]



Princeton "**No Boundary**" series

"… **8,000 sites** on which we observed session-replay scripts recording user data.

… health conditions and prescription data being exfiltrated from walgreens.com. These are considered **Protected Health Information under HIPAA**."

[emphasis added]

Princeton "**No Boundary**" series

"… used for grading assignments, … student names and emails, student grades, and instructor comments on students were being sent to FullStory … **Student Data under FERPA** (US educational privacy law).

Ironically, Princeton's own Information Security course was also affected."

[emphasis added]

Brendan tweets

"I asked in 2012 'why not **add boundaries**?' It's time.

Better isolation, OCap membranes reduce attack surface."

[emphasis added]

Political Challenge

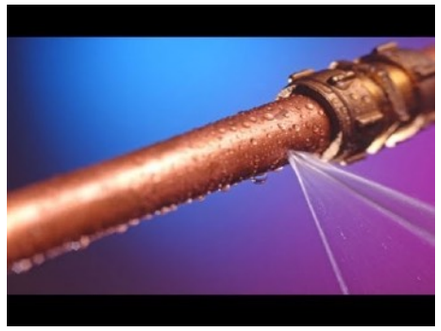
Brendan tweets:

“if Apple, Brave, and Mozilla allied in W3C, we could move the needle.”

Littledan tweets:

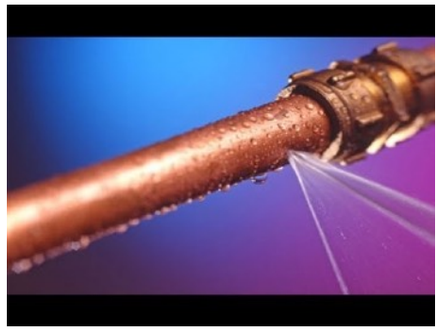
“I prefer this plan of working through the W3C to provide a web-wide solution to building OCap in TC39 alone.”

Exfiltration anatomy



Leaky secrets

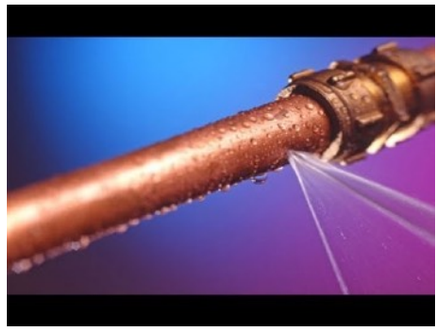
Exfiltration anatomy



Leaky secrets

Internal channel

Exfiltration anatomy

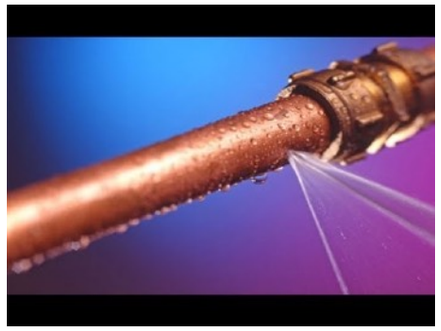


Leaky secrets

Internal channel

Spy in the machine

Exfiltration anatomy



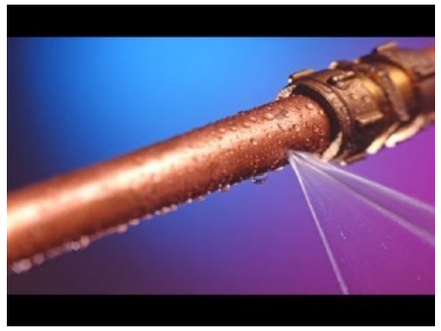
Leaky secrets

Timers (fantastic or not)

Spy in the machine

Internal channel

Exfiltration anatomy



Leaky secrets

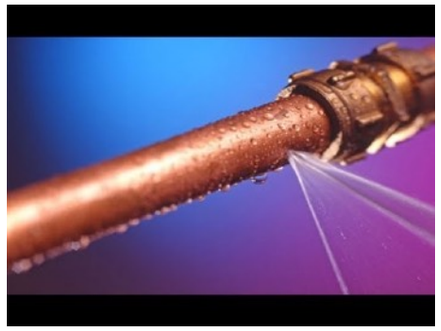
Timers (fantastic or not)

Internal channel

Spy in the machine

External channel

Exfiltration anatomy



Leaky secrets

Timers (fantastic or not)

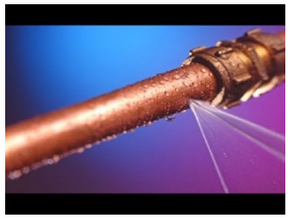
Internal channel

Spy in the machine

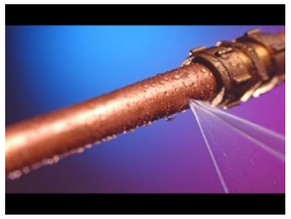
External channel

Lair

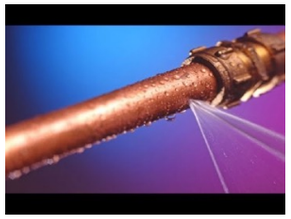
Exfiltration

		Coarse boundaries	
	**Leaky secrets**	Variable timing Cache effects Speculative execution	
	**Internal channel**	Side channels Covert channels	
	**Spy in the machine**	Bad page, origin	
	**Timers**	Essential	
	**External channel**	Overt channels	
	**Lair**	Origin, elsewhere	

Exfiltration

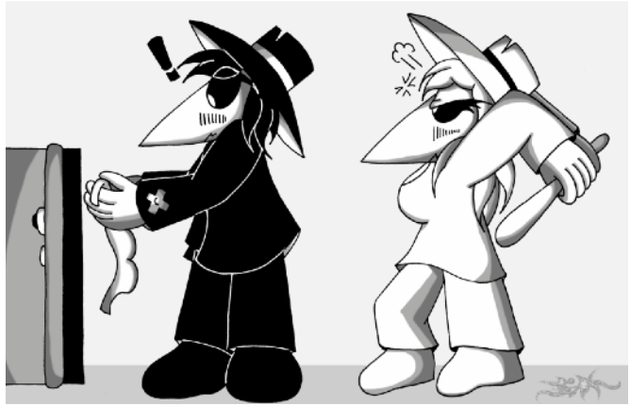
		Coarse boundaries	Fine boundaries
	**Leaky secrets**	Variable timing Cache effects Speculative execution	Reachable objects
	**Internal channel**	Side channels Covert channels	Overt corruption Prototype poison
	**Spy in the machine**	Bad page, origin	Bad library, plugin, mashup
	**Timers**	Essential	Often helpful
	**External channel**	Overt channels	Overt channels
	**Lair**	Origin, elsewhere	Origin, elsewhere

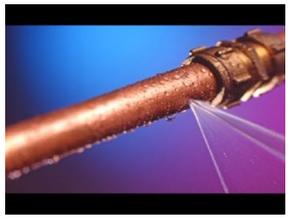
Mitigations

		Coarse	
	**Leaky secrets**	Variable timing Cache effects Speculative execution	
	**Internal channel**	Side channels Covert channels	
	**Spy in the machine**	Bad page, origin	
	**Timers**	Essential	
	**External channel**	Overt channels	
	**Lair**	Origin, elsewhere	

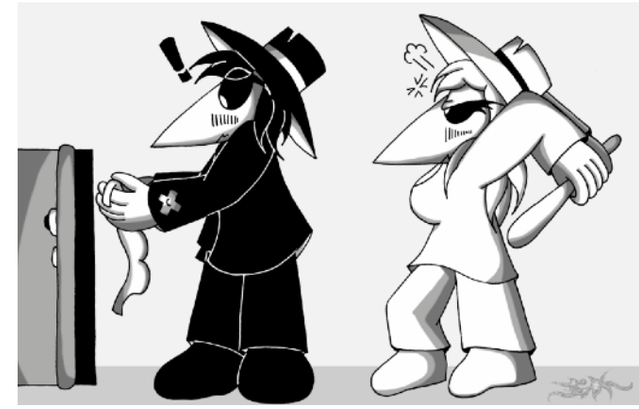
Mitigations

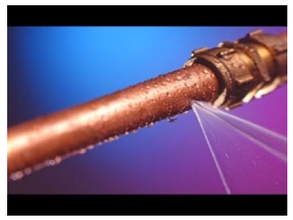
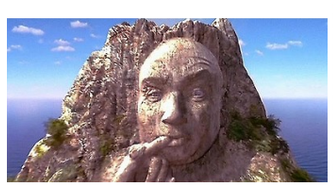
Coarse



	**Leaky secrets**	Variable timing Cache effects Speculative execution	Constant time algs (Doesn't work)
	**Internal channel**	Side channels Covert channels	Anti-speculation (cost *vs.* benefit)
	**Spy in the machine**	Bad page, origin	Site isolation (We'll see)
	**Timers**	Essential	No SABs, JS Zero (Temp, ineffective)
	**External channel**	Overt channels	Always provided (Only limit response)
	**Lair**	Origin, elsewhere	Sometimes foiled (But when?)

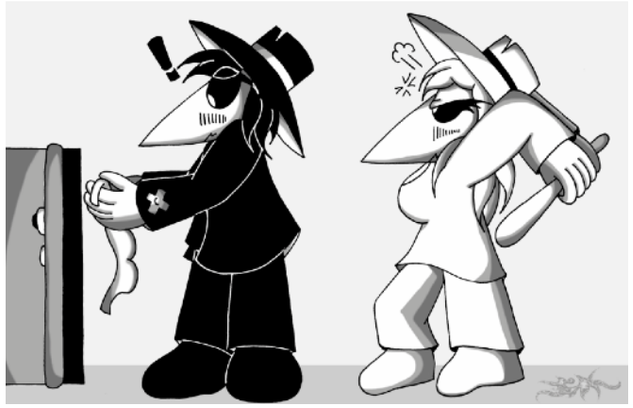
Mitigations

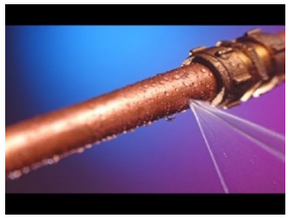


	**Leaky secrets**		
	**Internal channel**		
	**Spy in the machine**		
	**Timers**		
	**External channel**		
	**Lair**		

Mitigations

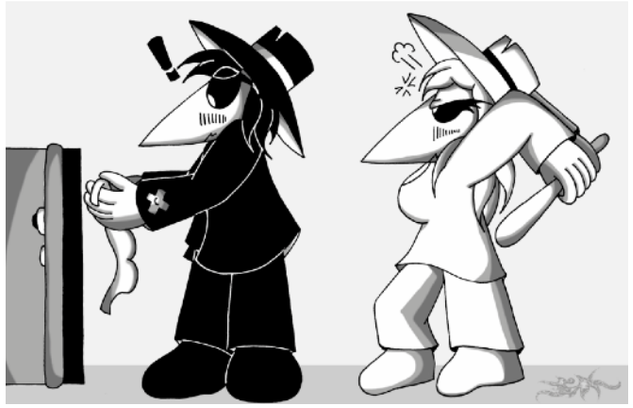
Fine

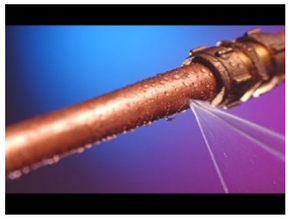


	**Leaky secrets**	Reachable objects	
	**Internal channel**	Overt corruption Prototype poison	
	**Spy in the machine**	Bad library, plugin, mashup	
	**Timers**	Often helpful	
	**External channel**	Overt channels	
	**Lair**	Origin, elsewhere	

Mitigations

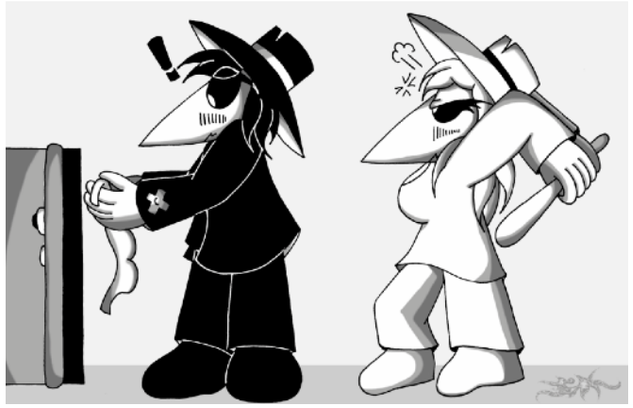
Fine

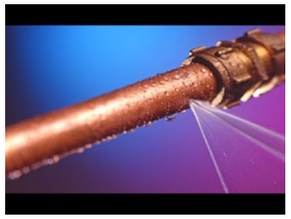


	**Leaky secrets**	Reachable objects	Realms Compartment scope
	**Internal channel**	Overt corruption Prototype poison	Frozen Realms Protect primordials
	**Spy in the machine**	Bad library, plugin, mashup	Module keys POLA linkage
	**Timers**	Often helpful	Deny when possible
	**External channel**	Overt channels	Deny when possible
	**Lair**	Origin, elsewhere	Darn, foiled again! (when possible)

Mitigations

Fine



	**Leaky secrets**	Reachable objects	Realms Compartment scope
	**Internal channel**	Overt corruption Prototype poison	Frozen Realms Protect primordials
	**Spy in the machine**	Bad library, plugin, mashup	Module keys POLA linkage
	**Timers**	Often helpful	Deny **when possible**
	**External channel**	Overt channels	Deny **when possible**
	**Lair**	Origin, elsewhere	Darn, foiled again! (**when possible**)

Transformational Libraries

parser, compiler, pattern matcher

parser generator, pretty printer

linear algebra, constraint solver

Date arithmetic, geometry, image synthesis

collection classes*, machine learning*

Transformational Libraries

parser, compiler, pattern matcher
parser generator, pretty printer
linear algebra, constraint solver
Date arithmetic, geometry, image synthesis
collection classes*, machine learning*

POLA would deny them
XHR, DOM, Sockets, fetch, files, Error.prototype.stack,
Math.random()*, new WeakRef()*
Date.now(), new Date(), postMessage(),
Timers, fantastic or not.

Let’s clean up our mess

Civilization now rests on infrastructure we made.

Its pervasive insecurity puts civilization at risk.

Reducing risks amplifies benefits.

We know how.

References

https://www.cs.tau.ac.il/~tromer/drivebycache/

https://www.cyberscoop.com/electron-vulnerability-skype-slack/

https://freedom-to-tinker.com/tag/noboundaries/

https://twitter.com/BrendanEich/status/992812041441193985

https://twitter.com/BrendanEich/status/987350364474126339

https://twitter.com/littledan/status/990172845434077184

https://github.com/tc39/proposal-frozen-realms

http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2018/02/ndss2018_07A-3_Schwarz_paper.pdf

https://gruss.cc/files/fantastictimers.pdf

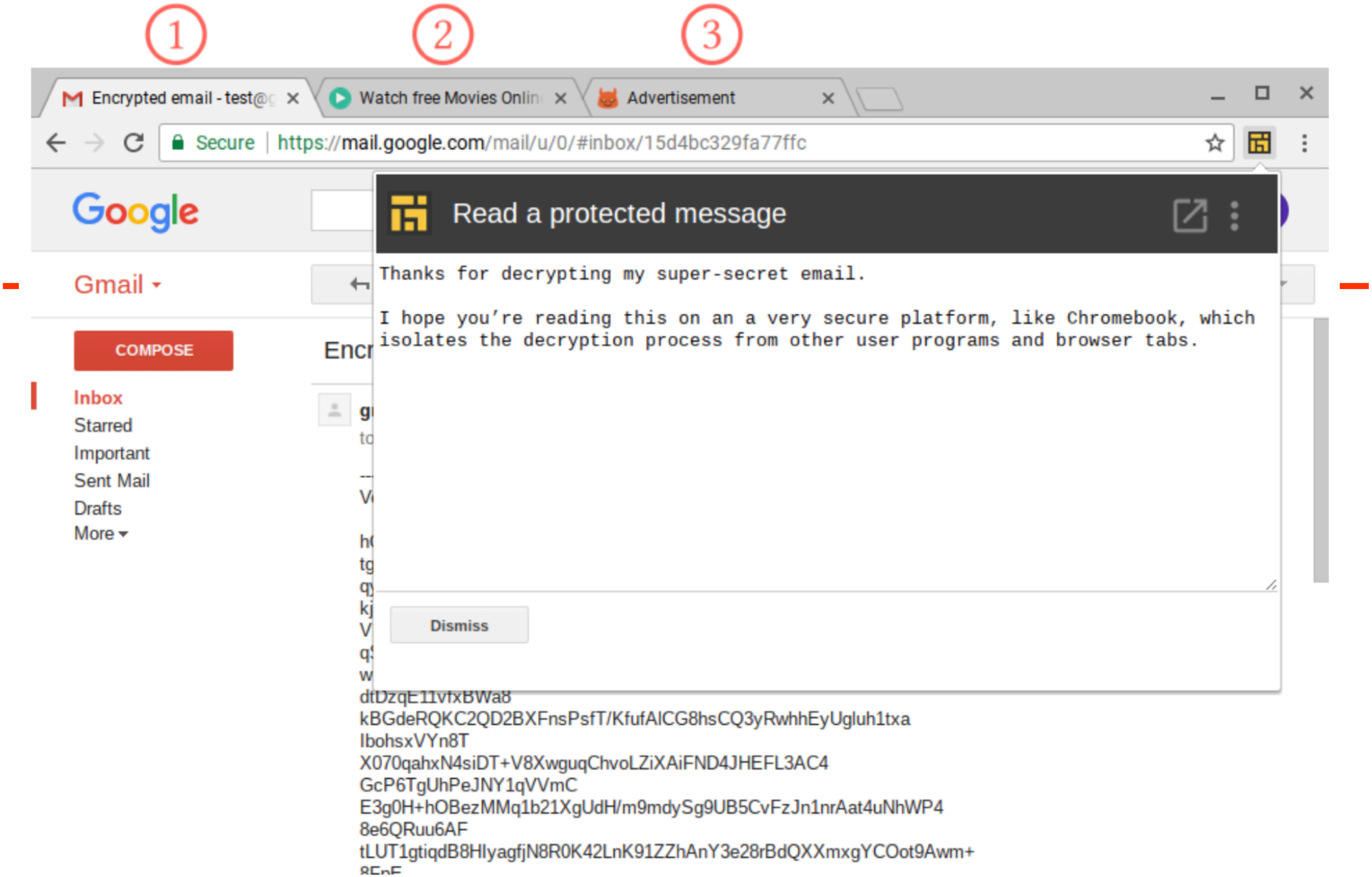
https://ai.google/research/pubs/pub46290

Discuss

Previous talk

Meltdown & Spectre worst case

Safety, Integrity, Consistency	Local integrity unaffected. Frozen realms unaffected. Distributed: Must protect crypto. Dr. SES plans must change
Liveness, Availability, Progress	Unaffected
Confidentiality, Privacy, Secrecy	In process, none among time sensers. ***Frozen Realms & "deterministic" libraries.*** Suspect between processes. Defensible between machines.



Screenshot of the attack scenario. The target user opens an online streaming web-site in Tab ②. Pressing somewhere in this tab (for example to start a movie), causes a pop-under to open up as Tab ③. The malicious advertisement in Tab ③ then monitors the cache activity on the target machine. When an encrypted email is received and decrypted using Google's encrypted email extension (in Tab ①), the malicious advertisement in Tab ③ learns information about the user's secret key.