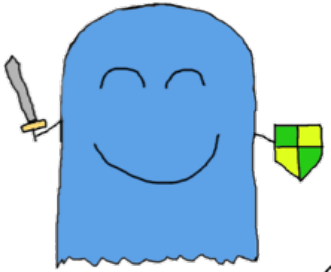
Spearing Superfish with HPKP

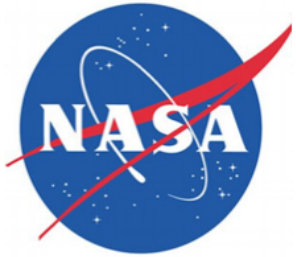
Stuart Larsen
Yahoo Paranoids - Pentest

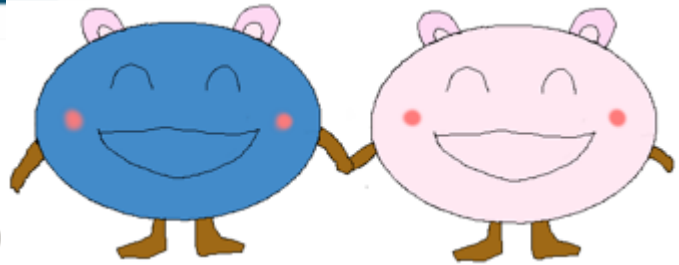
Overview

- The Problem
- HPKP
- Lenovo Superfish Certificate
- Conclusion

whoami

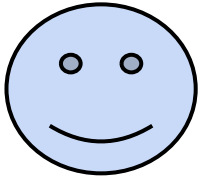




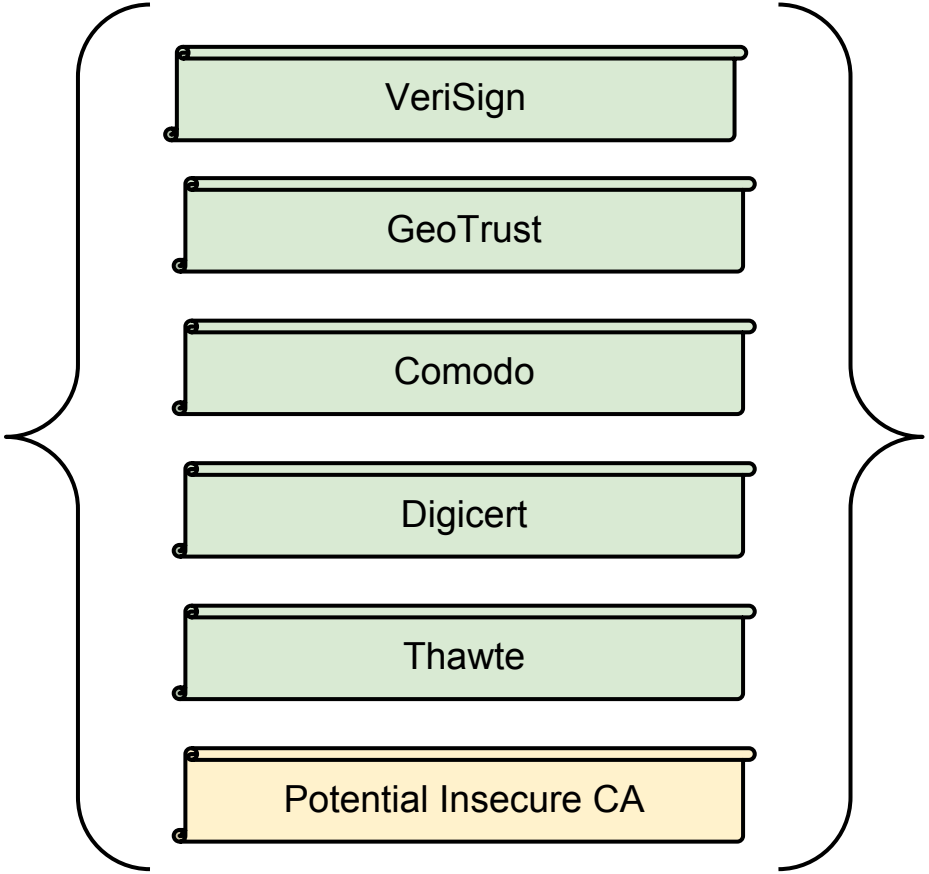


Mom: “Why can’t you read porn like a normal boy?”

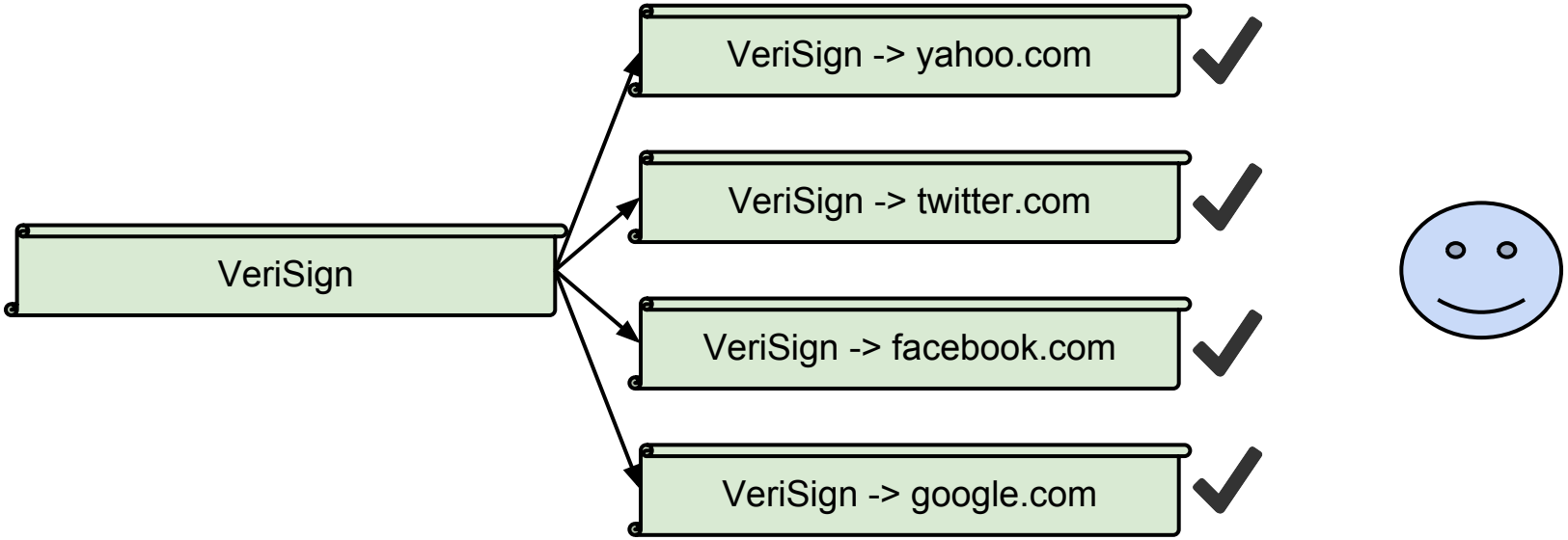
The Problem



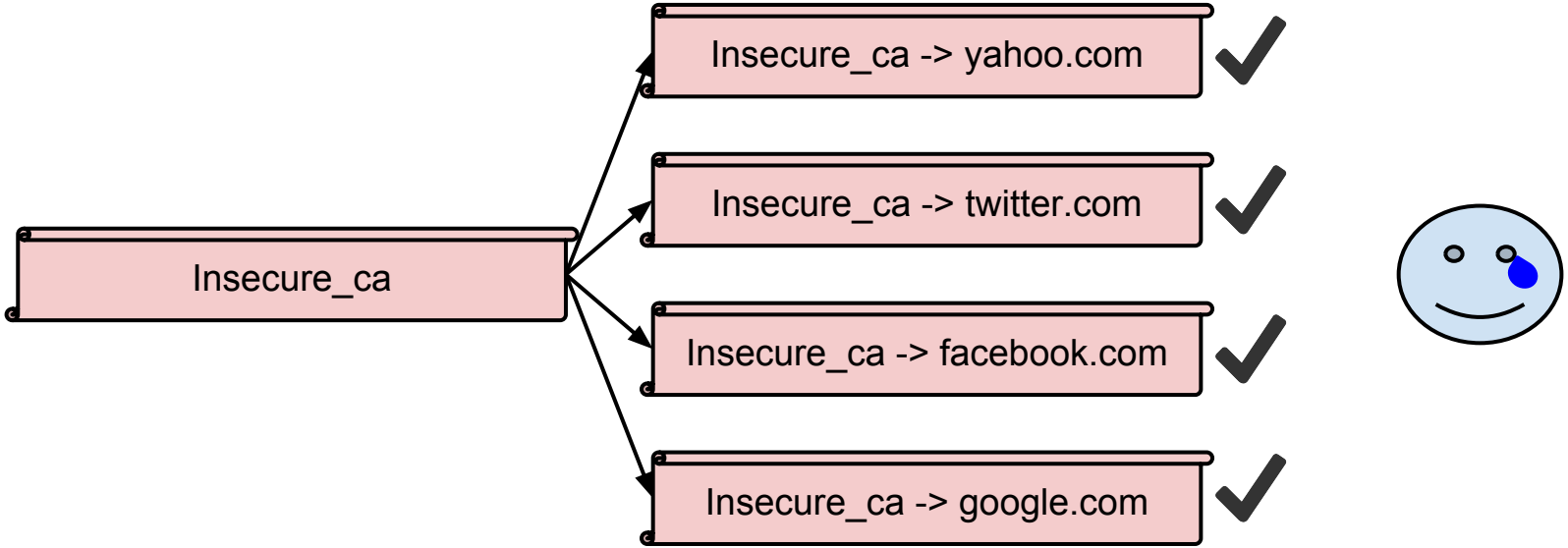
Trusted CAs:



The Problem

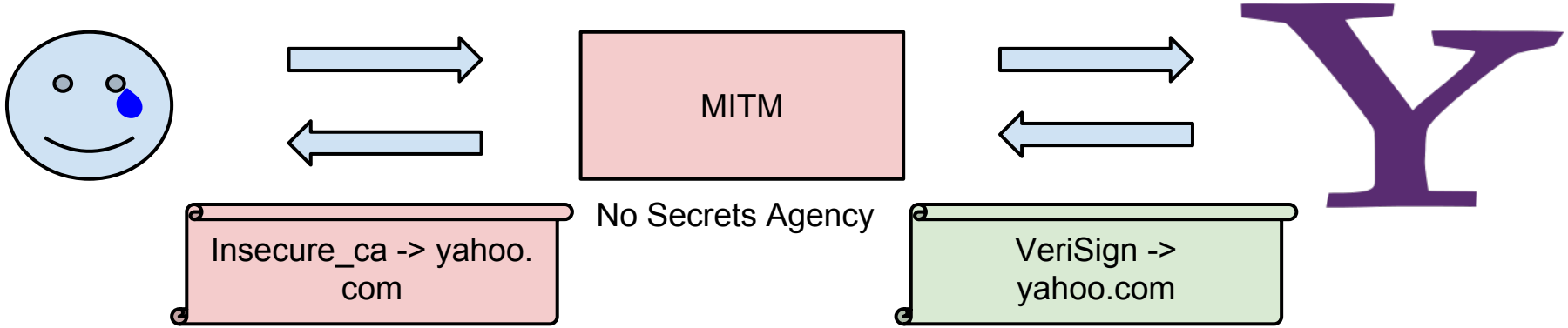

VeriSign
VeriSign -> yahoo.com
VeriSign -> twitter.com
VeriSign -> facebook.com
VeriSign -> google.com

The Problem


Insecure_ca
Insecure_ca -> yahoo.com
Insecure_ca -> twitter.com
Insecure_ca -> facebook.com
Insecure_ca -> google.com

The Problem

To the user, everything looks okay.



Is this a real problem?

- ComodoHacker: http://en.wikipedia.org/wiki/Comodo_Group#Certificate_hacking
- DigiNotar: http://arstechnica.com/security/2011/08/earlier-this-year-an-iranian/
- More?

HTTP Public Key Pinning (HPKP)

“instructs web clients to associate specific cryptographic identities with a certain web server to prevent MITM attacks dues to compromised Certificate Authorities”

Public-Key-Pins Header

Public-Key-Pins:

pin-sha256="klO23nT2ehFDXCfx3eHTDRESMz3asj1muO+4aIdjiuY=";

pin-sha256="IN1y/s/iJ+9dzXOhnh5sMzqPV6gmsYM9tLlO5iaCwSA=";

max-age=30;

includeSubdomains;

report-uri="hpkp_report"

```
Last-Modified: Mon, 11 May 2015 14:56:58 GMT
public-key-pins: pin-sha256="klO23nT2ehFDXCfx3eHTDRESMz3asj1muO+4aIdjiu
Y="; pin-sha256="IN1y/s/iJ+9dzXOhnh5sMzqPV6gmsYM9tLlO5iaCwSA="; max-age=30;
includeSubdomains; report-uri="hpkp_report"
Strict-Transport-Security: max-age=60; includeSubDomains;
X-Powered-By: Express
```

Public-Key-Pins Header

- pin-sha256:
  - base 64 encoding of a hashed Subject Public Key Info
- max-age:
  - number of seconds to save host pinning
- includeSubDomains: (optional)
  - tells the client to apply pinned host to subdomains as well
- report-uri: (optional)
  - If there is a violation, where should it be reported

What is a Pin

Subject: yahoo.com

Issuer: VeriSign

Public Key Algorithm
Subject Public Key

notBefore
notAfter

extensions

….

SPKI: Subject Public Key Identifier

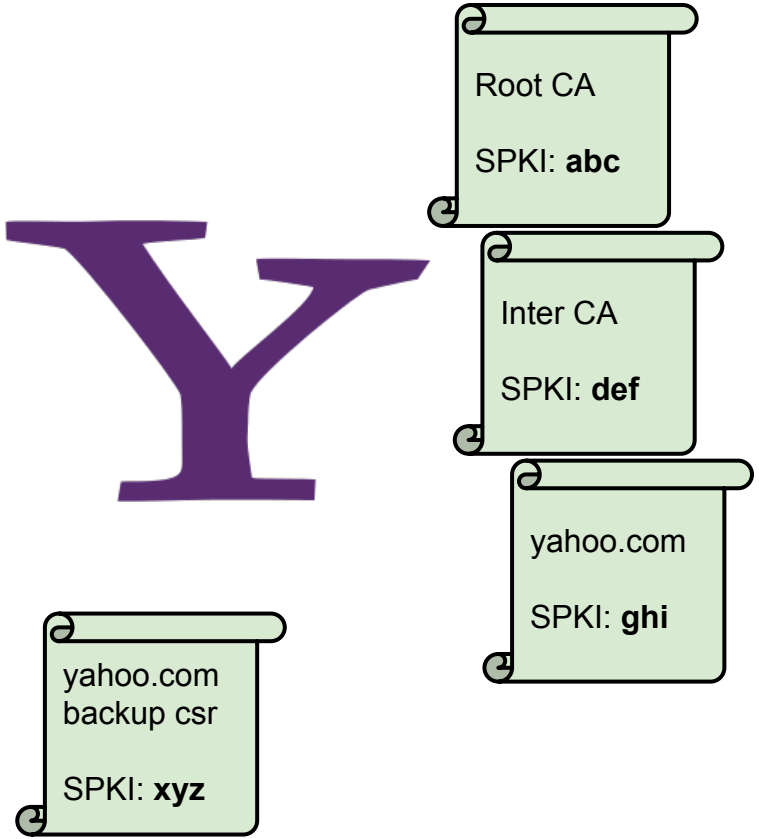
Public Key Algorithm

Subject Public Key

pin-sha256=256klO23nT2ehFDXCfx3eHTDRESMz3asj1muO+4aIdjiuY=

For Examples: pin-sha256=**abc**

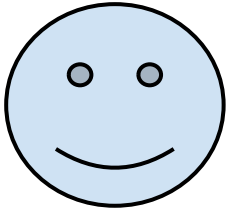
Where to Pin

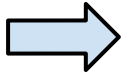


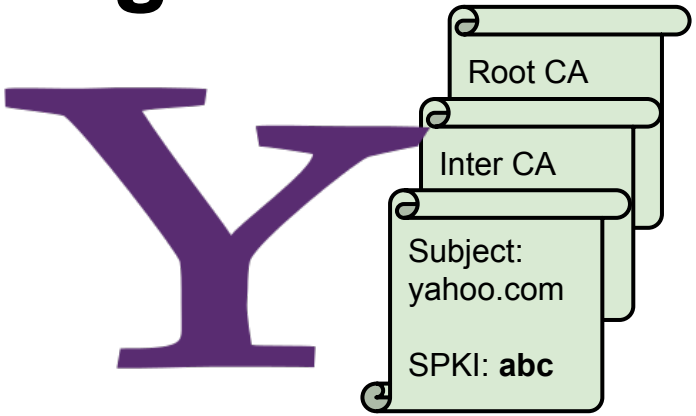
- A pin can be any certificate in the chain
- When publishing a policy, two of the pins must be in different trust chains
- You can publish a pin at different levels of the chain
- Backup CSRs

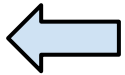
Public Key Pinning

Monday









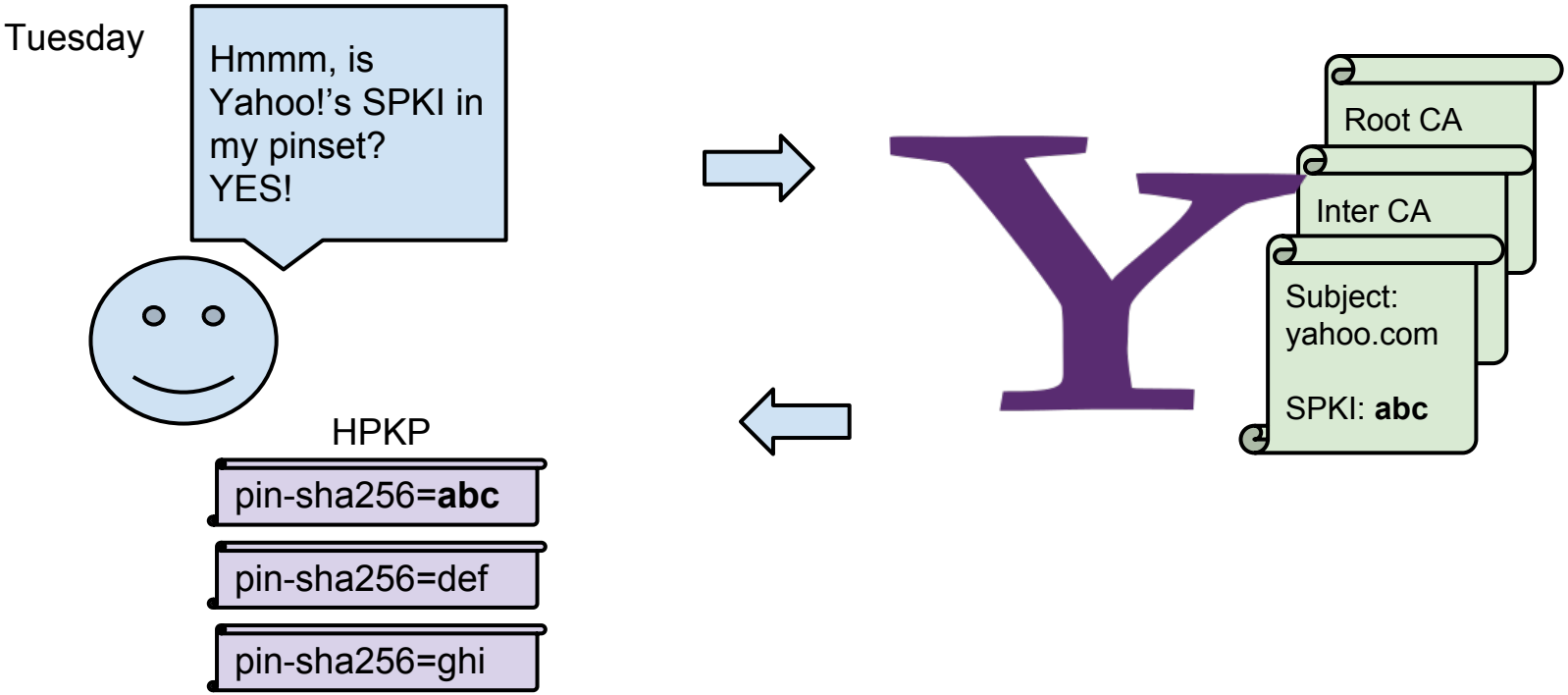
HPKP

pin-sha256=**abc**

pin-sha256=def

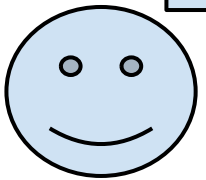
pin-sha256=ghi

Public Key Pinning



Public Key Pinning

Wednesday



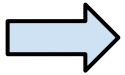
Hmmm, is Yahoo!'s SPKI in my pinset?
NO! STOP CONNECTION

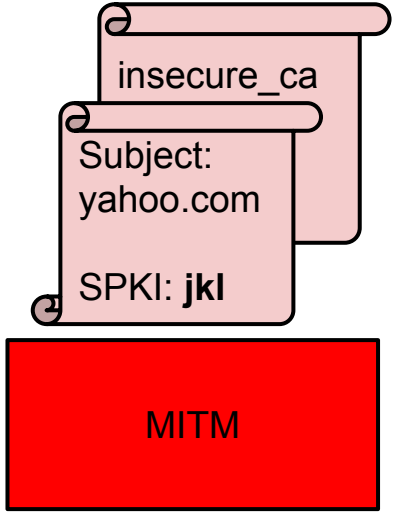
HPKP

pin-sha256=**abc**

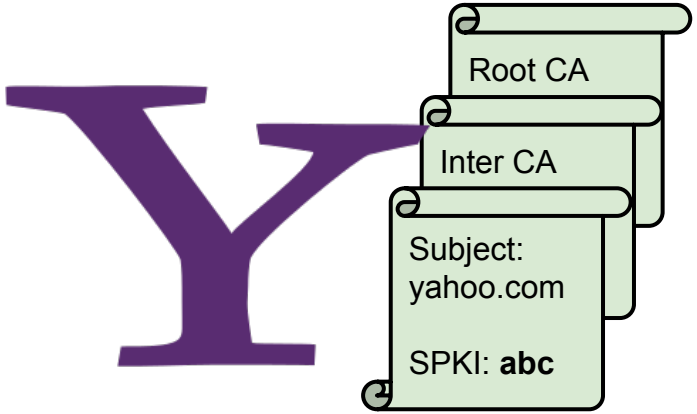
pin-sha256=def

pin-sha256=ghi



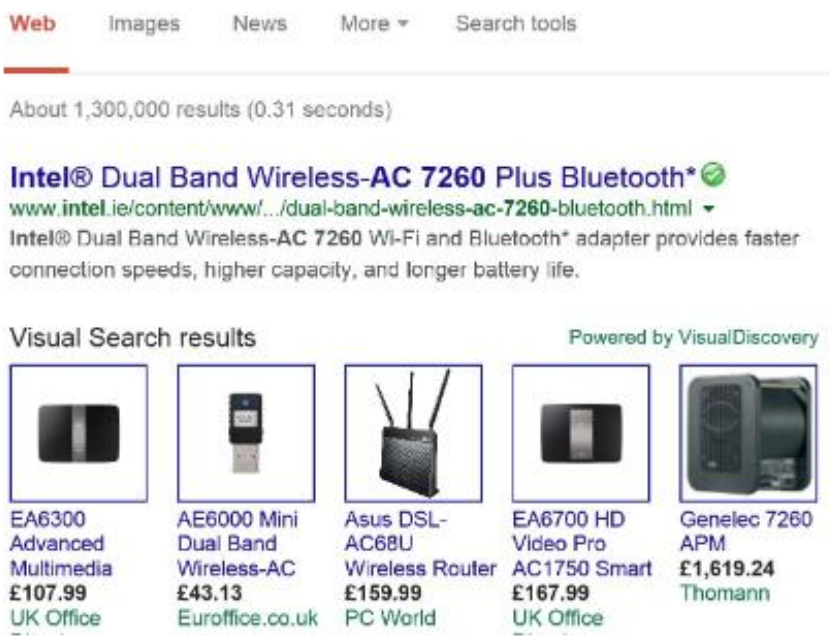


No Secrets Agency



Lenovo and Superfish

- Pre-installed adware for displaying Ads in Google searches
- The adware came from a company called Superfish



The Problem of Superfish

- Google Search uses HTTPS
- So Lenovo pre-installed self signed root certificate
- The same certificate was on all infected machines
- The encryption key was trivially crackable
- Check here: https://superphish.com

Superfish MITM

- Any malicious actor can use this certificate to MITM *any* website.
- Which completely negates HTTPS, meaning passwords, bank statements, emails, messages are visible again
- It also gives nation states, ISPs, backbone providers another vector for information snooping

The Embarrassing Part of the Talk

- Can’t we just apply HPKP to the Superfish certificate?
- The Superfish certificate won’t be in any pinned certificate chains.

- Turns out it doesn’t quite work that way

HPKP: Locally Installed Certificates

What about MITM proxies, Fiddler etc?

There are a number of cases where HTTPS connections are intercepted by using local, ephemeral certificates. These certificates are signed by a root certificate that has to be manually installed on the client. Corporate MITM proxies may do this, several anti-virus/parental control products do this and debugging tools like Fiddler can also do this. Since we cannot break in these situations, user installed root CAs are given the authority to override pins. We don't believe that there will be any incompatibility issues.

HTTP Public Key Pinning (HPKP)

“instructs web clients to associate specific cryptographic identities with a certain web server to prevent MITM attacks dues to compromised Certificate Authorities”

Conclusion

- The Problem
- HPKP
- Lenovo Superfish Certificate

Questions?