Cats? In My Certificate Transparency Logs?

It's More Likely Than You Think.

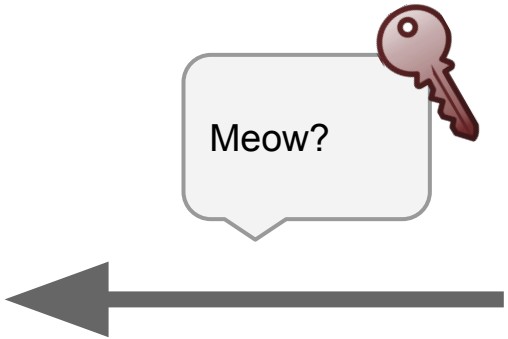
Ian Haken, Scott Behrens, Rekha Bachwani
BSidesSF 2019

NETFLIX

What is Certificate Transparency?

Public Key Primer

Alice

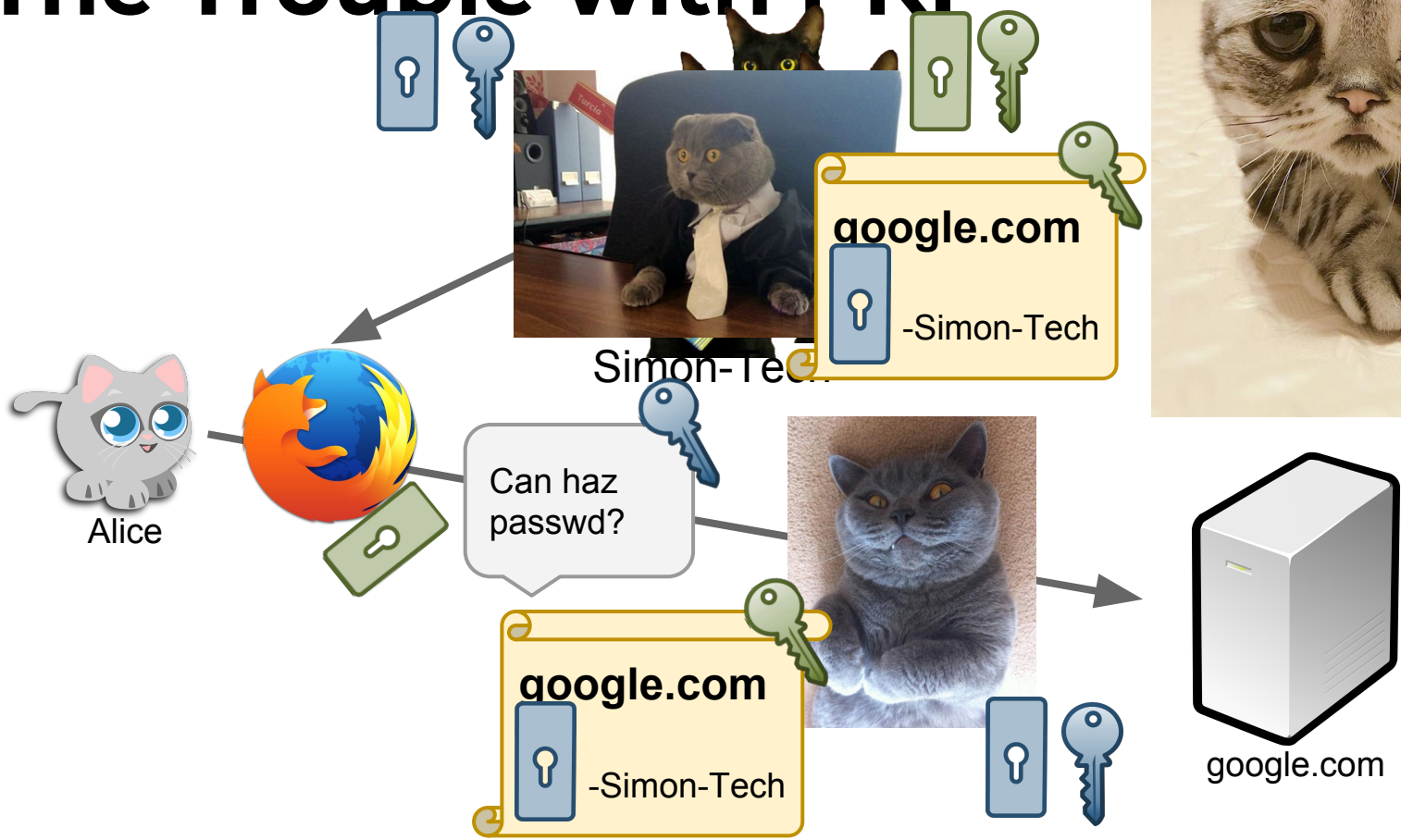


Bob

Public Private

PKI On the Web

The Trouble with PKI



What is Certificate Transparency?

Certificate Transparency (CT) aims to remedy certificate-based threats by making the issuance and existence of SSL certificates open to scrutiny. CT has three main goals:

1. Make it impossible for a CA to issue a SSL certificate for a domain without the certificate being visible to the owner of that domain.
2. Provide an open auditing and monitoring system that lets any domain owner or CA determine whether certificates have been mistakenly or maliciously issued.
3. Protect users from being duped by certificates that were mistakenly or maliciously issued.

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

What is a CT Log?

A CT log is a simple network service that maintains a record of SSL certificates. CT logs have three important qualities:

- They're append-only: certificates can only be added to a log; certificates can't be deleted, modified, or retroactively inserted into a log.
- They're cryptographically assured: logs use "Merkle Tree Hashes" to prevent tampering and misbehavior.
- They're publicly auditable: anyone can query a log and verify that it's well behaved.

There are many CT logs, e.g. Google, Digicert, Comodo, and Cloudflare

Chrome SCT Requirements

- Chrome now requires Signed Certificate Timestamps (SCT) be present with certificates in order to trust them.
  - An SCT is a “promise” signed by a CT log that the certificate will be included in the log.
- “Chrome may check that an SCT has been honoured by the CT log that issued it. This is so that a CT log cannot issue an SCT but then never publish the certificate, thereby hiding its existence. … If the log cannot provide a proof, or the proof cannot be verified, then Chrome learns that the log has misbehaved.”

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

TL;DR: How does CT work?

- Certificates must have an SCT for Chrome to trust them
- An SCT is a signature from a CT log guaranteeing the certificate will show up in the log.
  - Chrome will notice if it doesn't get added to the log.
- Because of crypto, a CT log can never remove or alter entries.
  - The crypto of the CT log would fail, this would be detected, and Chrome would remove non-compliant logs would no longer be trusted.

Abusing Certificate Transparency

Infrastructure Reconnaissance

Enumerate internal (or external) domain names, or search for potentially interesting targets, e.g. `%admin%.microsoft.com`

Capture the delta of domains which have interesting names and don't respond externally

527686753	2018-06-15	2017-09-19	2019-09-19	billingadminconsole.co1.cp.microsoft.com	C=US, ST=Washington, L=Redmond, O=Microsoft Corporation, OU=Microsoft IT, CN=Microsoft IT TLS CA 5
527686753	2018-06-15	2017-09-19	2019-09-19	billingadminconsole.cp.microsoft.com	C=US, ST=Washington, L=Redmond, O=Microsoft Corporation, OU=Microsoft IT, CN=Microsoft IT TLS CA 5
527686753	2018-06-15	2017-09-19	2019-09-19	billingadminconsole.dm2.cp.microsoft.com	C=US, ST=Washington, L=Redmond, O=Microsoft Corporation, OU=Microsoft IT, CN=Microsoft IT TLS CA 5
527686753	2018-06-15	2017-09-19	2019-09-19	billingfrsadminconsole.co1.cp.microsoft.com	C=US, ST=Washington, L=Redmond, O=Microsoft Corporation, OU=Microsoft IT, CN=Microsoft IT TLS CA 5
527686753	2018-06-15	2017-09-19	2019-09-19	billingfrsadminconsole.cp.microsoft.com	C=US, ST=Washington, L=Redmond, O=Microsoft Corporation, OU=Microsoft IT, CN=Microsoft IT TLS CA 5
527686753	2018-06-15	2017-09-19	2019-09-19	billingfrsadminconsole.dm2.cp.microsoft.com	C=US, ST=Washington, L=Redmond, O=Microsoft Corporation, OU=Microsoft IT, CN=Microsoft IT TLS CA 5
527683858	2018-06-15	2018-06-	2020-06-	jitadminuatpr.one.microsoft.com	C=US, ST=Washington, L=Redmond, O=Microsoft Corporation

Finding Domains with Weak Keys

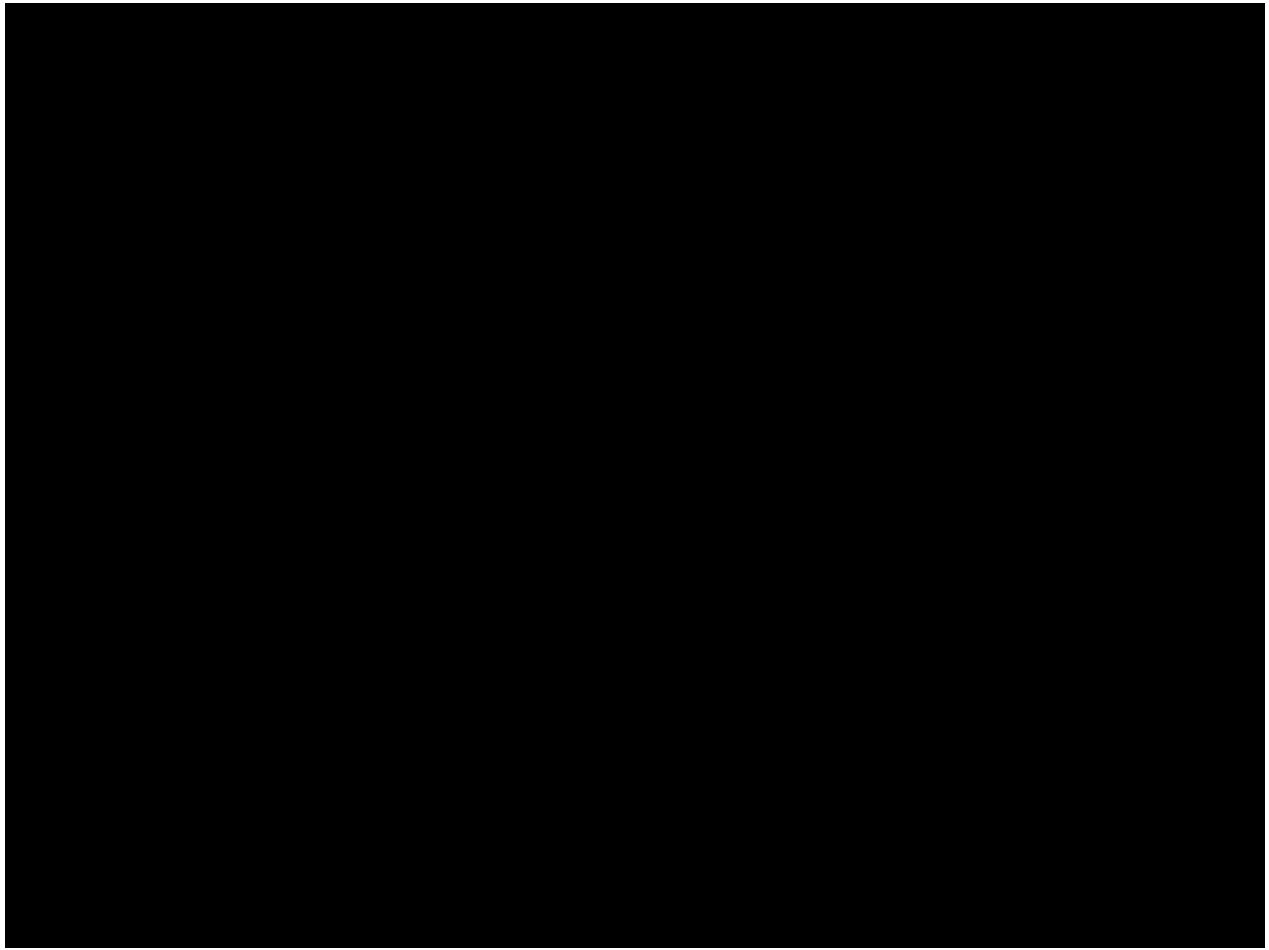
Reaping and Breaking Keys at Scale: When Crypto Meets Big Data[1]

“We’ve run our custom distributed batch-gcd algorithm on our dataset made of over 340 million keys and have found that on average, 1 key out of 1600 is vulnerable to batch-gcd in our dataset. We broke over 210k RSA keys in total. Out of these vulnerable keys, 207k are X.509 certificates.”

[1] https://research.kudelskisecurity.com/2018/10/16/reaping-and-breaking-keys-at-scale-when-crypto-meets-big-data/

Persistent Data Storage

- CAs must publish certs to CT logs so that SCTs can be included in the cert.
- CT logs must actually add the cert entry to the log after signing an SCT.
- CT logs must be available and can never have entries removed or altered.



https://crt.sh/?id=391676432

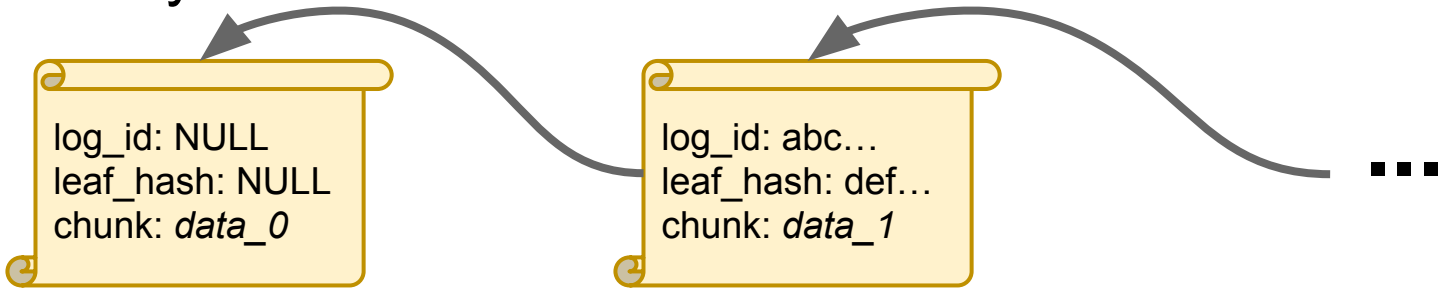
SAN Packing

- Let’s Encrypt allows for up to 100 SANs per certificate
- 1 SAN can be up to 230 characters (minus “dots”)
- A character in a SAN can be alphanumeric (plus hyphen)
- Given a 6 character domain name suffix...

$$\frac{(230\text{-}4\text{-}6)\ \text{characters}}{\text{SAN}} \times \frac{99\ \text{SAN}}{\text{cert}} \times \frac{5\ \text{bytes}}{8\ \text{char}} = 13612.5\ \text{bytes/cert}$$

Data Chunking

- When we mint a cert, that cert includes a SCT
- From a SCT we know how to look up that cert in the CT logs
- In the next cert we mint, we can include a pointer to that CT log entry



catlog

It puts the cat in ctlog

catlog

- https://github.com/JackOfMostTrades/catlog
- Abstracts CT logs as a data storage provider.
  - Provides “push” command to put a file in CT logs
  - Provides “pull” command to get files from CT logs
- Provides an “box” abstraction for putting your ~~files~~ cat pics into.
  - Run “catlog init mycats.mydomain.net”
  - Push a few files…
  - Run “catlog commit” to put your box (list of files) into CT logs
  - Later “catlog clone mycats.mydomain.net” to checkout the box on someone else’s machine.

Catlog Demo

- `catlog clone demo.catlog.pw`
- `catlog pull cat-1151519 1920.jpg`
- `catlog pull yelling_cat.webm`

Who’s Abusing CT?

Evidence Hypothesis

- Large Certs with many SANs
  - Check entropy for evidence of encryption
  - Check for magic numbers*

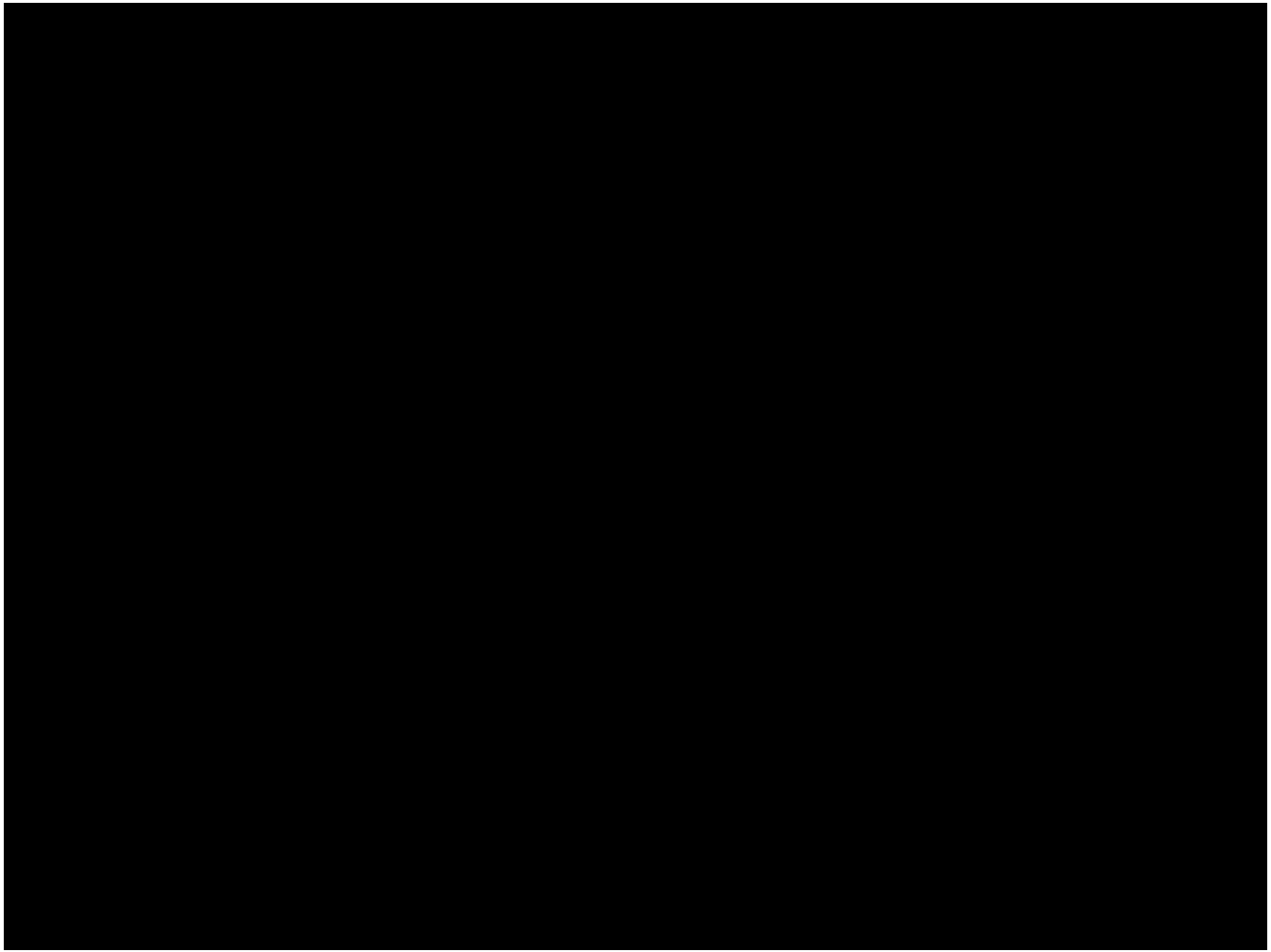
Quick Primer: Magic Numbers

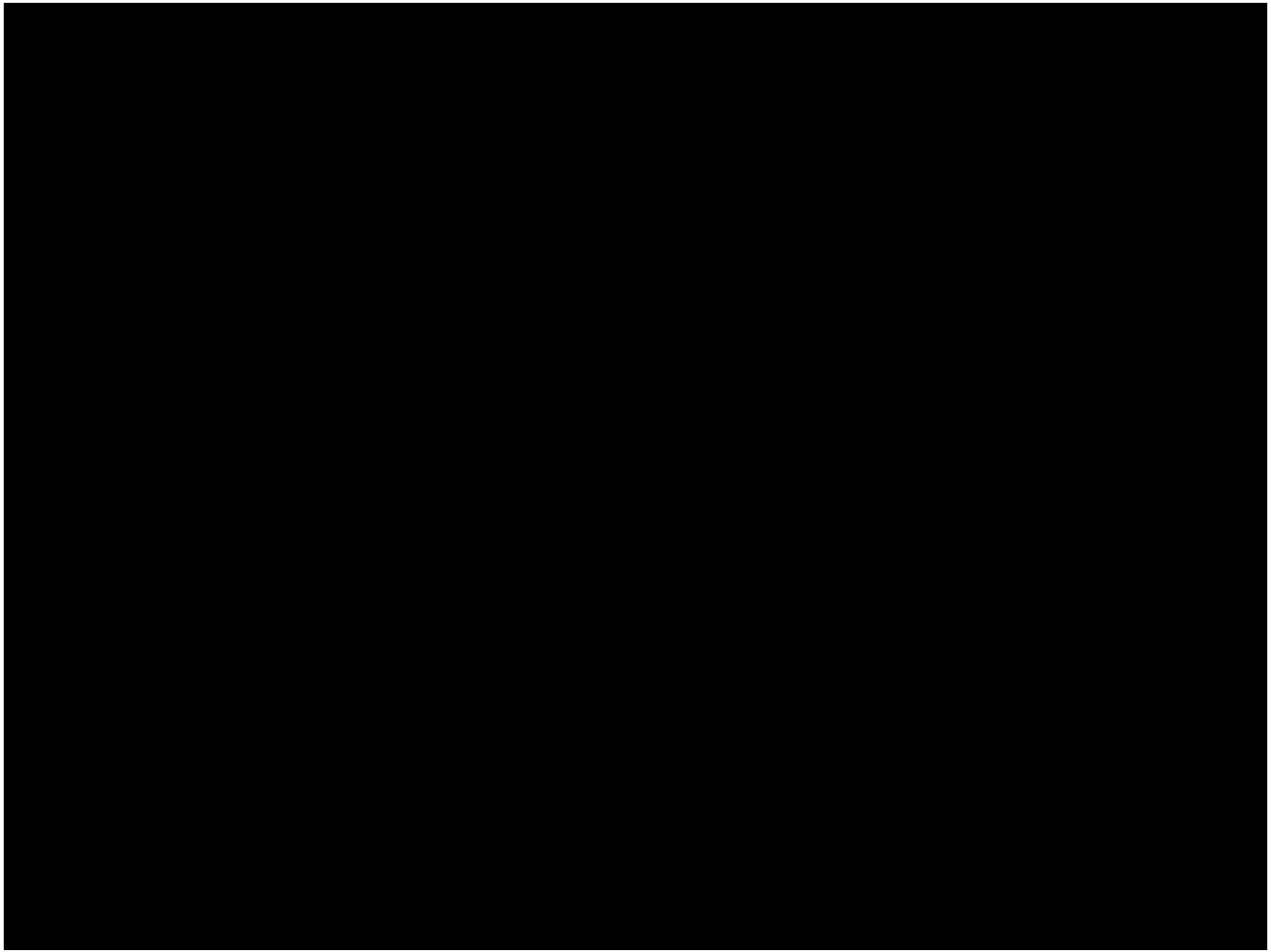
- Constant number used to identify a file format
  - Gif: “GIF89a” 47 49 46 38 39 61
  - Jpeg: “Exif” 45 78 69 66
  - Elf: 7F E L F

https://github.com/CaliDog/Axeman

Modifications to Axeman

- Wrote Icarus certs to Hive
- Calculated entropy
- Plucked out public key
- Stored cert size in bytes for filtering
- Looked for magic numbers in SANs





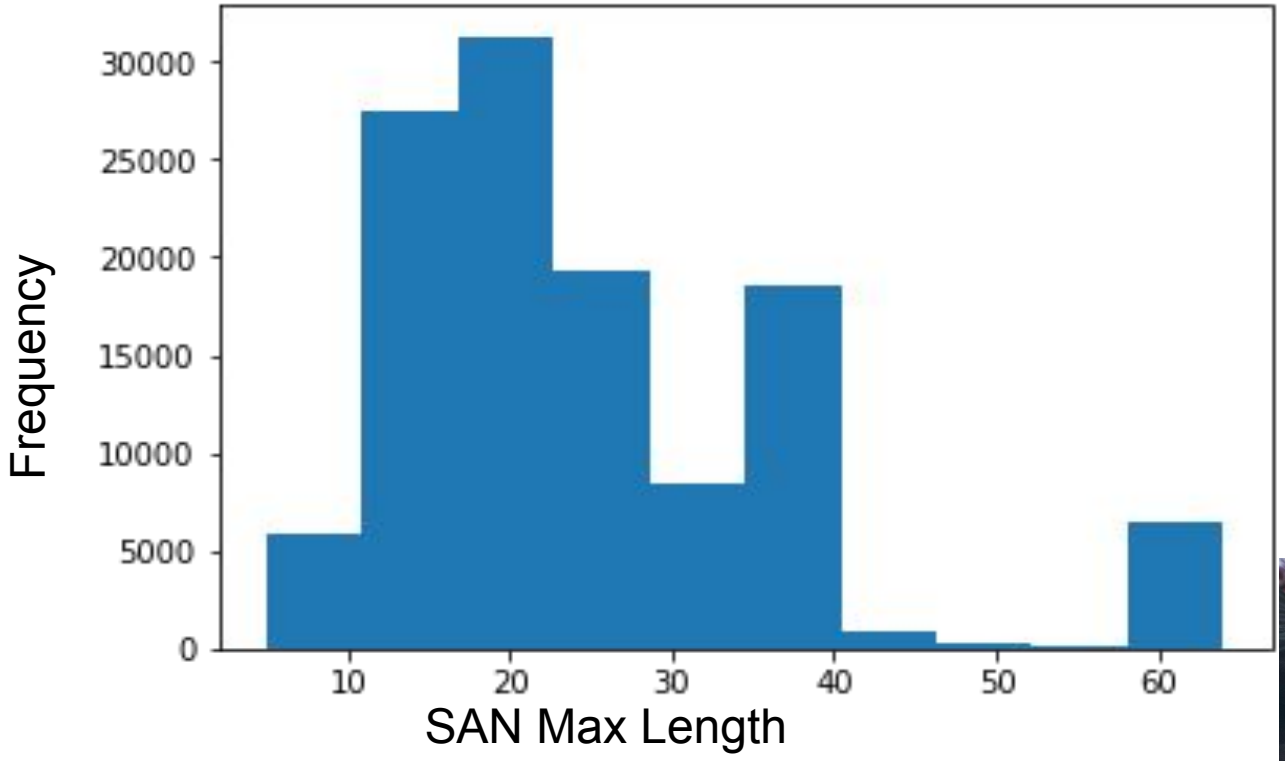
Raw WHOIS Record

```
Domain Name: WEHAVETHE.TECH
Registry Domain ID: D55509083-CNIC
Registrar WHOIS Server: whois.dotserve.com
Registrar URL:
Updated Date: 2018-03-09T00:14:10.0Z
Creation Date: 2017-11-10T19:25:21.0Z
Registry Expiry Date: 2027-11-10T23:59:59.0Z
Registrar: Dotserve Inc
Registrar IANA ID: 1913
Domain Status: clientTransferProhibited
https://icann.org/epp#clientTransferProhibited
Registrant Organization: Privacy Protection Service INC d/b/a PrivacyProtect.org
Registrant State/Province: Queensland
Registrant Country: AU
Registrant Email: Please query the RDDS service of the Registrar of Record
```

wehavethe.tech

- https://crt.sh/?q=%25wehavethe.tech
  - Something with numbers/text
  - Binary data (possibly encrypted)

Cert Length of Certs with >= 100 SAN Certs



Select * Where San Certs >= 75 and at Least 1 SAN Length >= 200

baltic-oil.emerald-grp.com

bbb.derp.fish

box.rahulprasad.com

cat.jpeg.wehavethe.tech

cloud.jefflau.hk

digital.foreantech.com

dreamconmerce.com

enugui4giy20854h35hg4yg4ghyeyhrg4gbyubyu4gnui.grado.cz

for-the-love-of-god.ml

foreantech.com

glok23.com

jefflau.hk

lol-all-day-long.ga

mail.sedrills.com

mail.swastikenterprise.com

numbers.jpg.wehavethe.tech

p.o.c.wehavethe.tech

Thuijo1ief0c.p0m.fr

tocreate.life

tocreate.life

didyoueverhearthetragedyofdarthplagueisthewise.ithoughtnot.itsnotastorythejediwouldtellyou.itsasithlegend.darthplagueiswasadarklordofthesithsopowerfulandsowise.hecouldusetheforcetoinfluencethemidichlorians.tocreate.life

Did you ever hear the tragedy of darth plague is the wise i thought not its not a story the jedi would tell you its a sith legend darth plague is was a darklord of the sith so powerful and so wise he could use the force to influence the midichlorians to create life

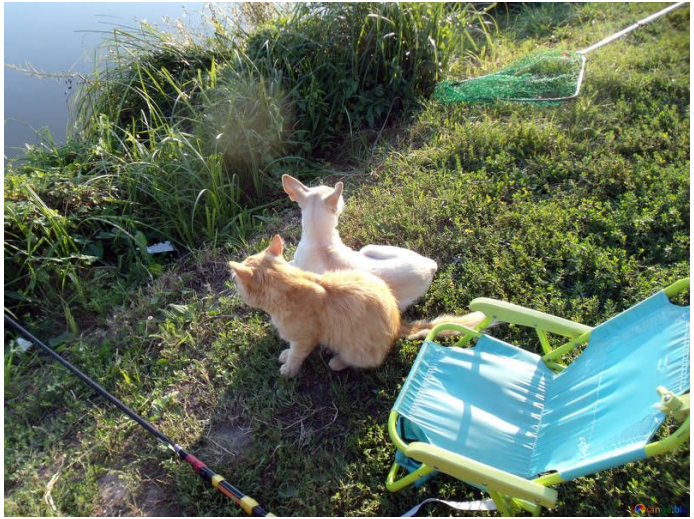
https://crt.sh/?id=166391179

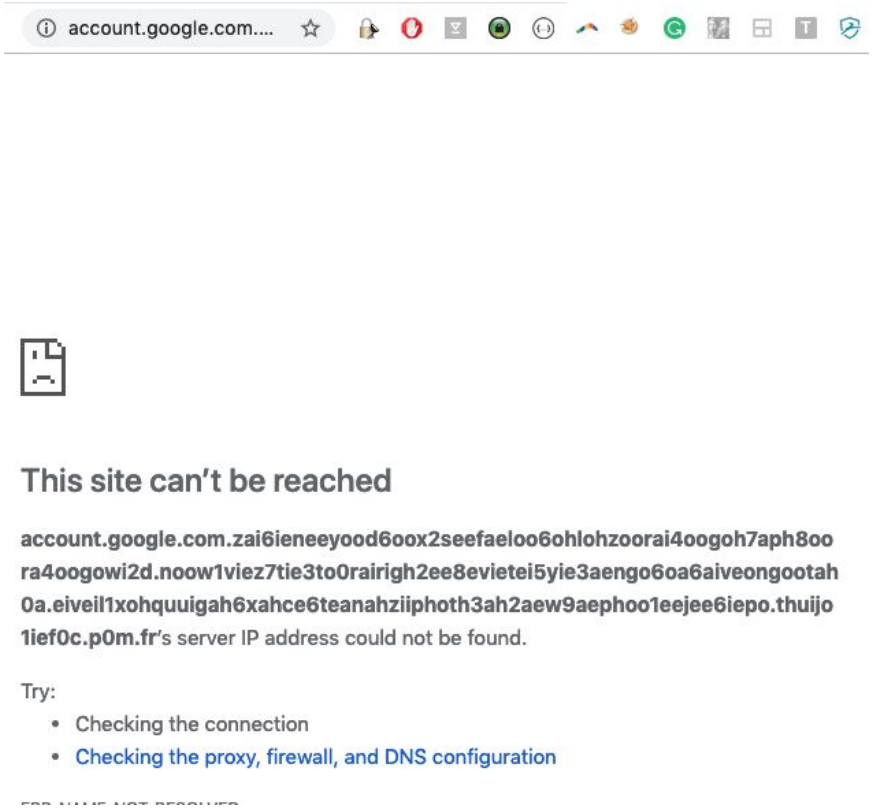
Large Certs with Good Entropy

- P.o.c.wehavethe.tech
- Entropy: 5.03, highest entropy for >= 75 SANS
- Looks like binary data, not sure how to sort it...

Large Certs with Good Entropy

- Thuijo1ief0c.p0m.fr
- Convincing phishing for low-res displays





Large Certs with Good Entropy

- Multidomain-prober.mdp .certsbridge.com
- Cert prober
- Many SANS

Scott Behrens • 1:55 PM
Hi Marcin,

I work on the Application Security team at Netflix, and I'm currently doing some research against the Certificate Transparency logs. I'd love to pick your brain a bit more on what the domain-prober service is you have built and its use, as the certs keep showing up in my analysis.

Marcin Walas • 1:55 PM
Hi Scott,
indeed you got us here :) The probing may be somewhat chatty in CTs.

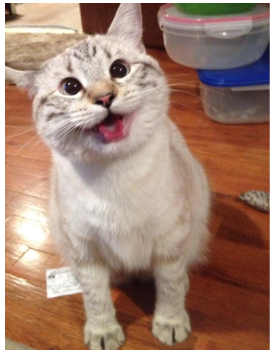
For public docs on the features powered by the system see:
https://cloud.google.com/blog/products/gcp/introducing-managed-ssl-for-google-app-engine
https://cloud.google.com/load-balancing/docs/ssl-certificates#managed-certs

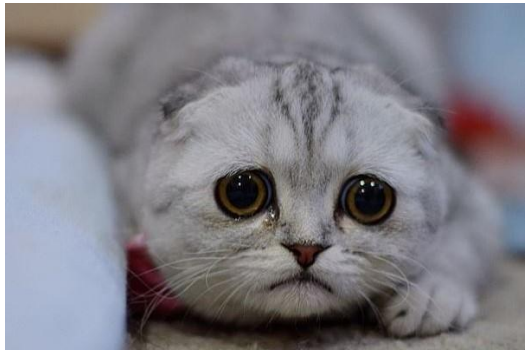
Marcin Walas is now a connection.

Final Thoughts

Summary

- Certificate Transparency is awesome!
- But it puts all your internal domain names on display
- And it puts all your weak crypto on display
- And it’s a non-redactable, unmodifiable, append-only public data store that anyone can write to.
    - And changing any of these properties would significantly weaken the benefit of having this system.



Special Thanks

- Rekha Bachwani - Netflix Dig Data Wizard
- Everyone who has posted pictures of cats on the Internet
- Google, CT log owners, and Let’s Encrypt
  - Sorry!

Like This Talk? Download the Slides!

$> catlog clone slides.catlog.pw