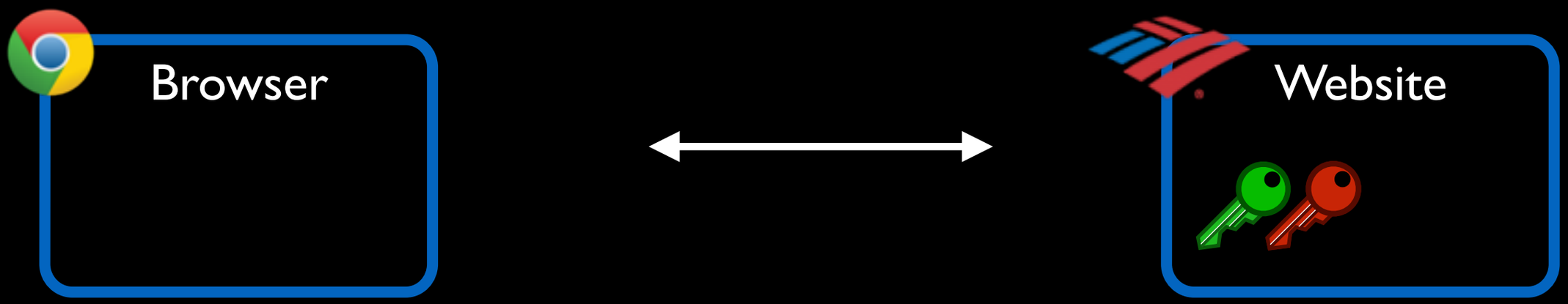
Analysis of SSL certificate reissues and revocations in the wake of Heartbleed

Liang Zhang*, David Choffnes*, Tudor Dumitras†, Dave Levin†,
Alan Mislove*, Aaron Schulman‡, Christo Wilson*

*Northeastern University †University of Maryland ‡Stanford University

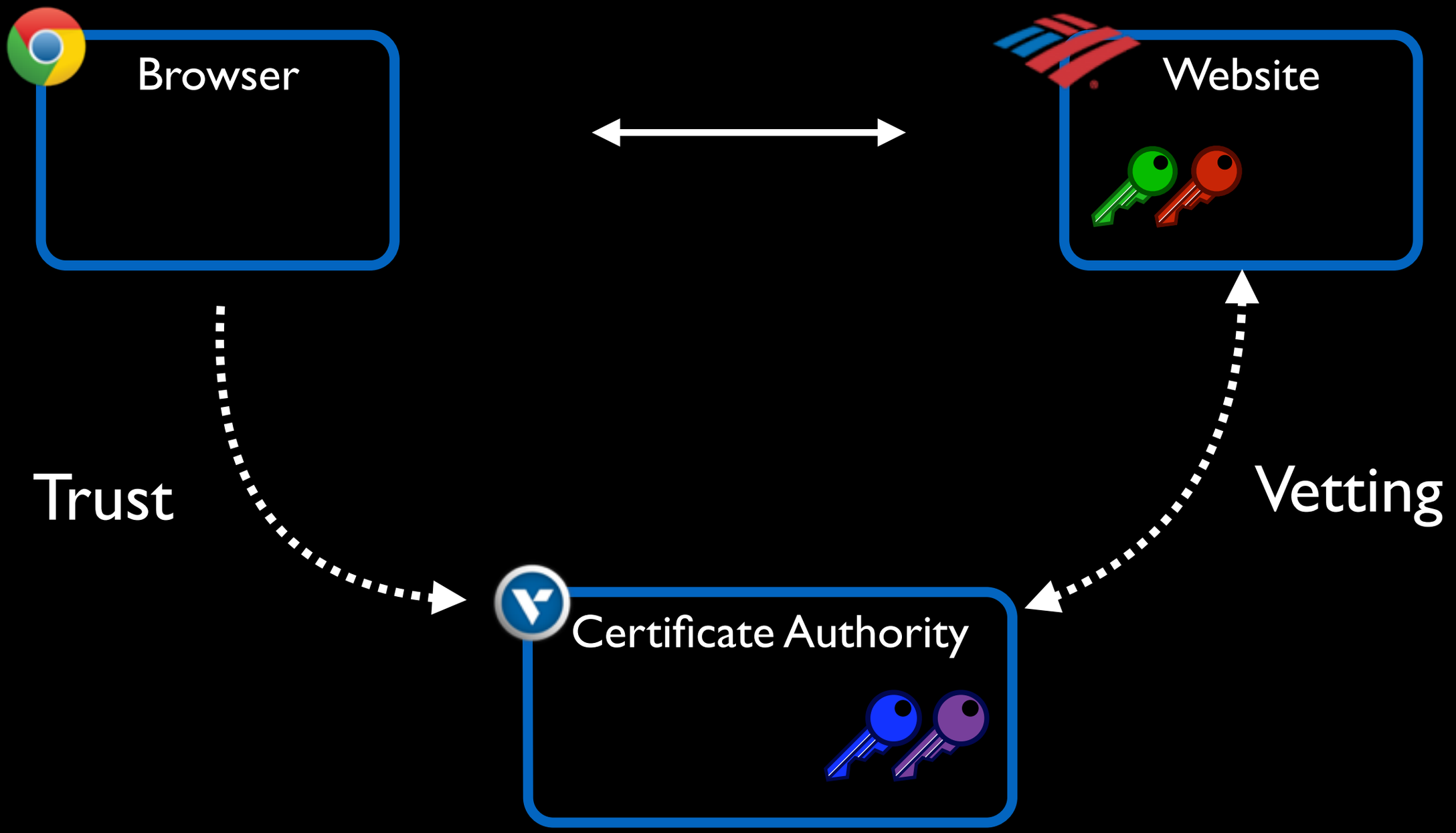
Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?



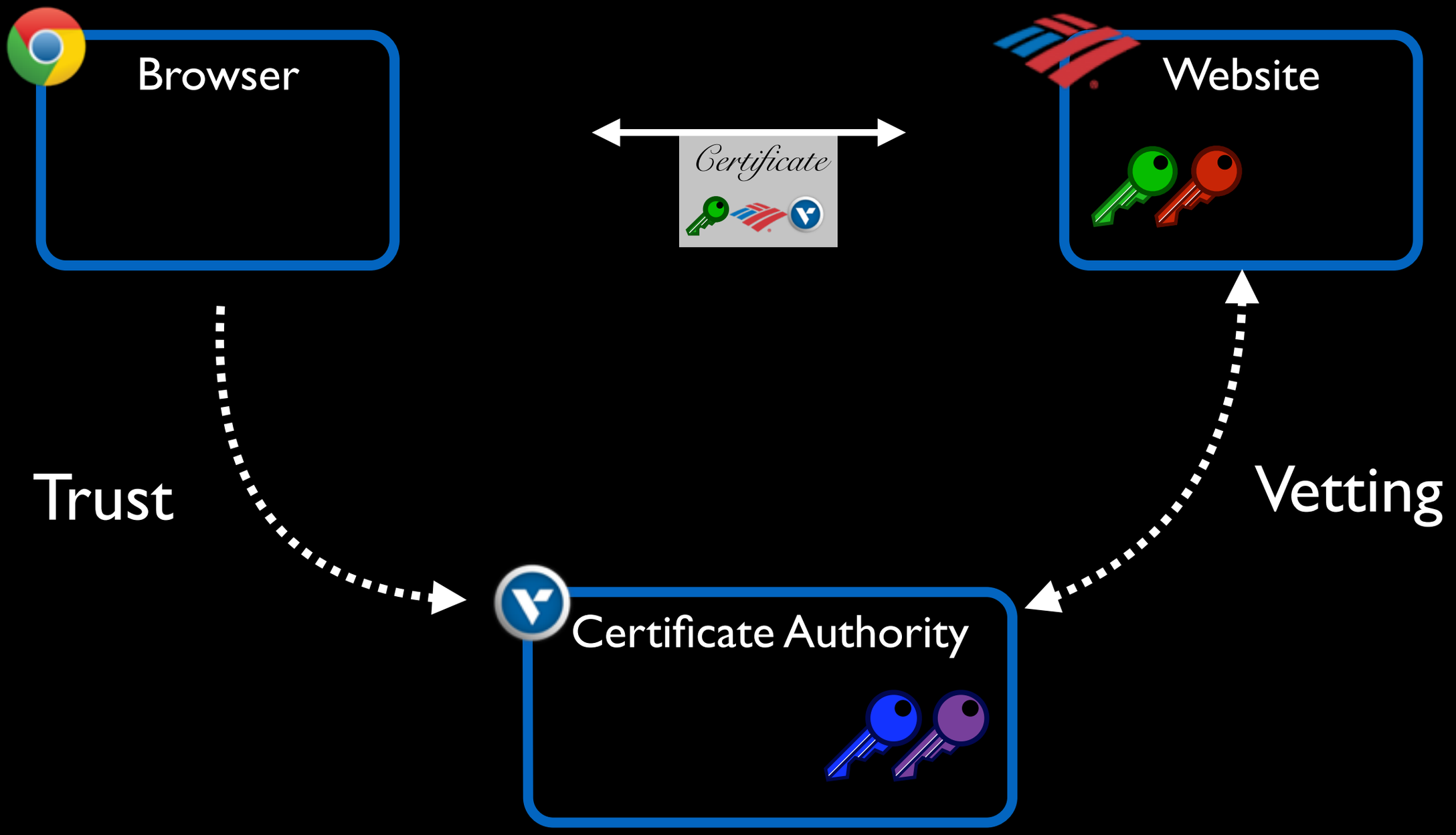
Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?

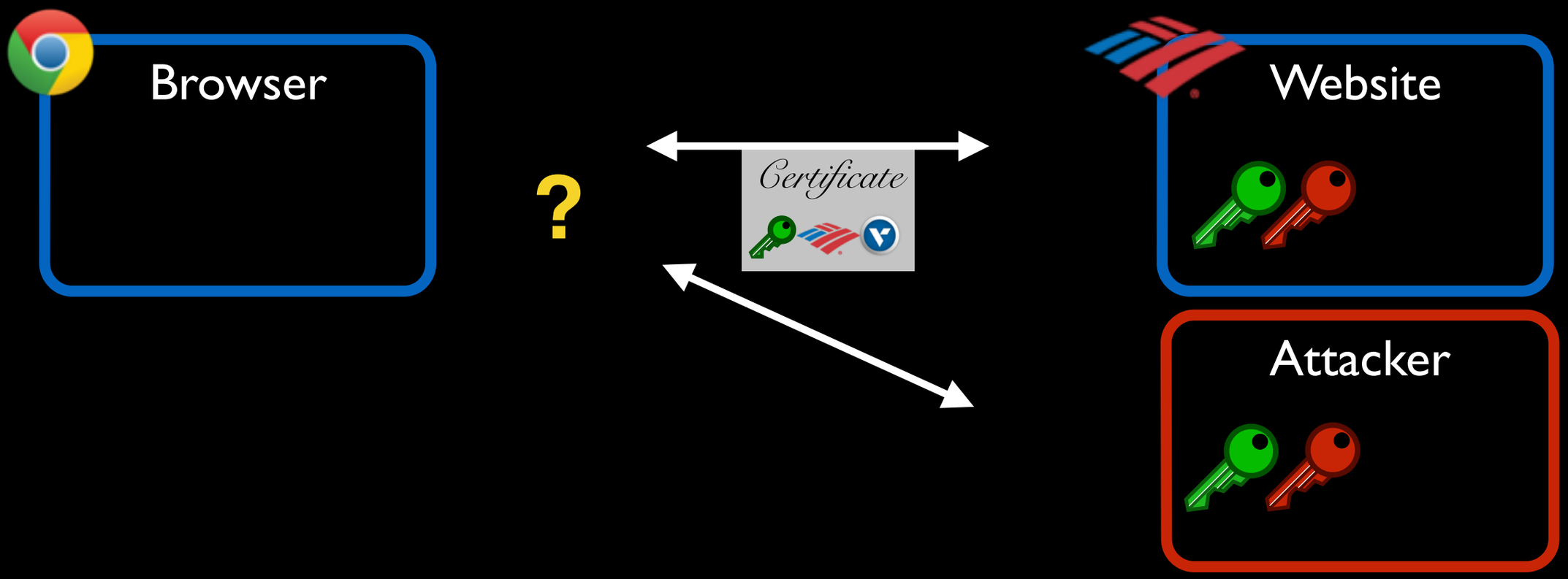


Public Key Infrastructures (PKIs)

How can users truly know with whom they are communicating?



Public Key Infrastructures (PKIs)



What needs to do when a certificate is no longer valid?

Certificate revocation
is a critical part of any PKI

Certificate revocation
is a critical part of any PKI

Administrators must revoke and reissue as quickly as possible

Certificate revocation
is a critical part of any PKI

Administrators must revoke and reissue as quickly as possible

Authority publish revocations via CRL as quickly as possible

Certificate revocation
is a critical part of any PKI

Administrators must revoke and reissue as quickly as possible

Authority publish revocations via CRL as quickly as possible

Browsers should obtain revocations as often as possible

Certificate revocation
is a critical part of any PKI

Administrators must revoke and reissue as quickly as possible

Authority publish revocations via CRL as quickly as possible

Browsers should obtain revocations as often as possible

In practice:

How quickly and thoroughly do administrators act?

Heartbleed

Allows attackers to extract up to 2^{16}-1 bytes of memory with a single heartbeat message

Heartbleed

Allows attackers to extract up to 2^{16}-1 bytes of memory with a single heartbeat message

April 7

Every vulnerable website should have:

1. Patched
2. Revoked
3. Reissued

Heartbleed

Allows attackers to extract up to 2^{16}-1 bytes of memory with a single heartbeat message

April 7 → *Every* vulnerable website should have:

1. Patched
2. Revoked
3. Reissued

Heartbleed is a natural experiment:
For studying SSL certificate reissues and revocations

Outline

1. ~~Motivation~~
2. Data and methodology
3. Analysis

Dataset

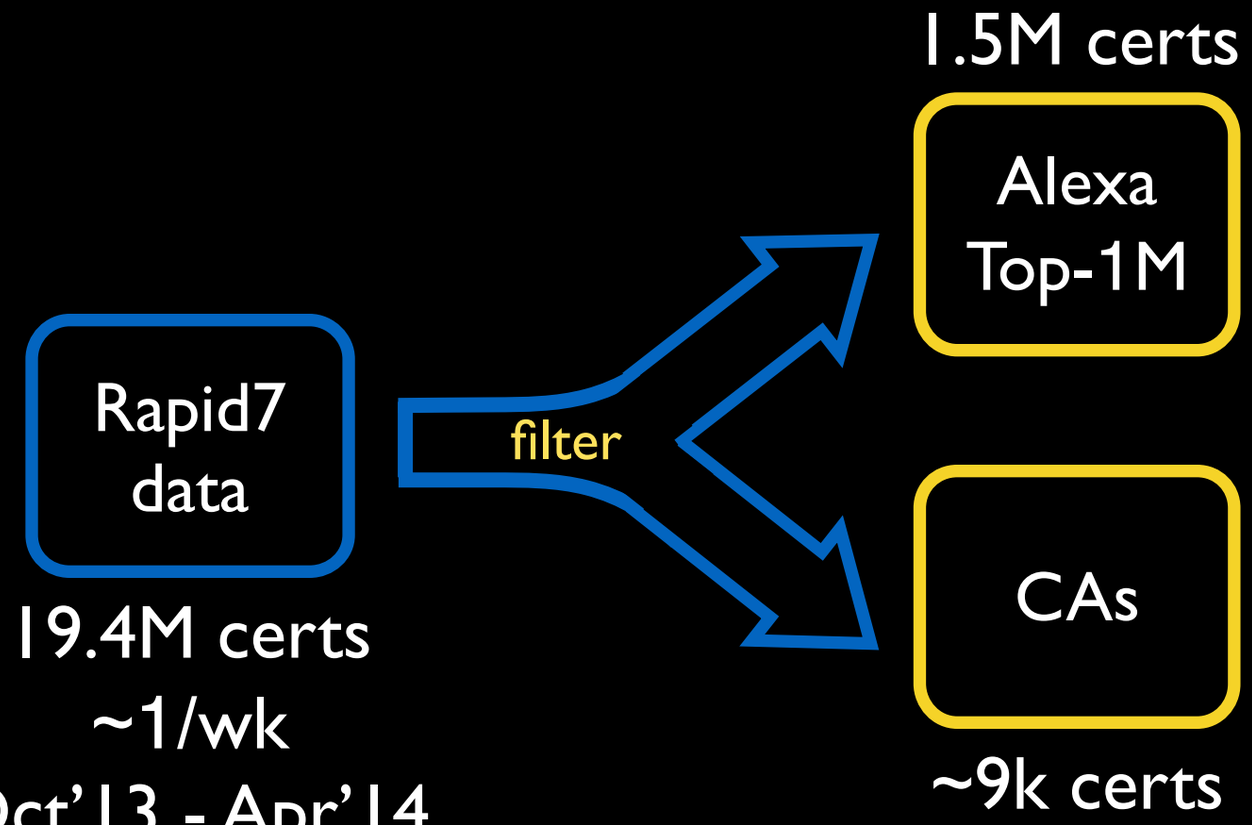
Rapid7
data

19.4M certs

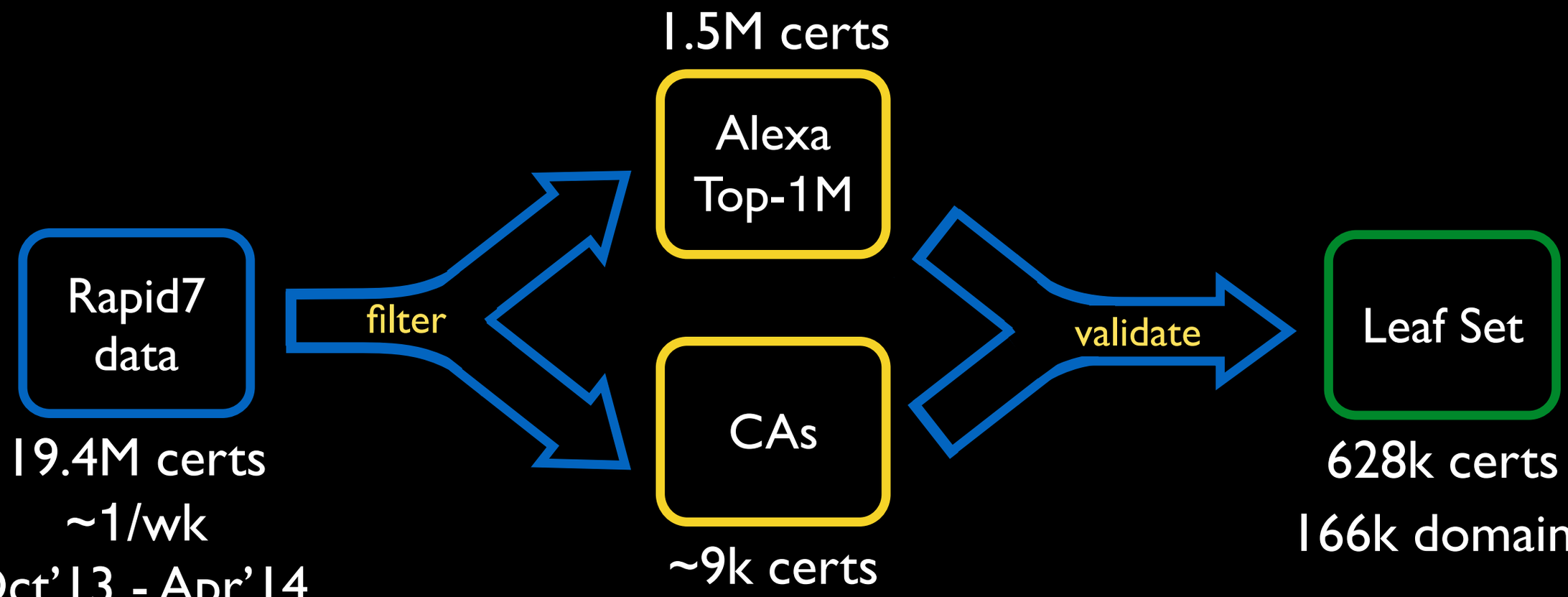
~1/wk

Oct'13 - Apr'14

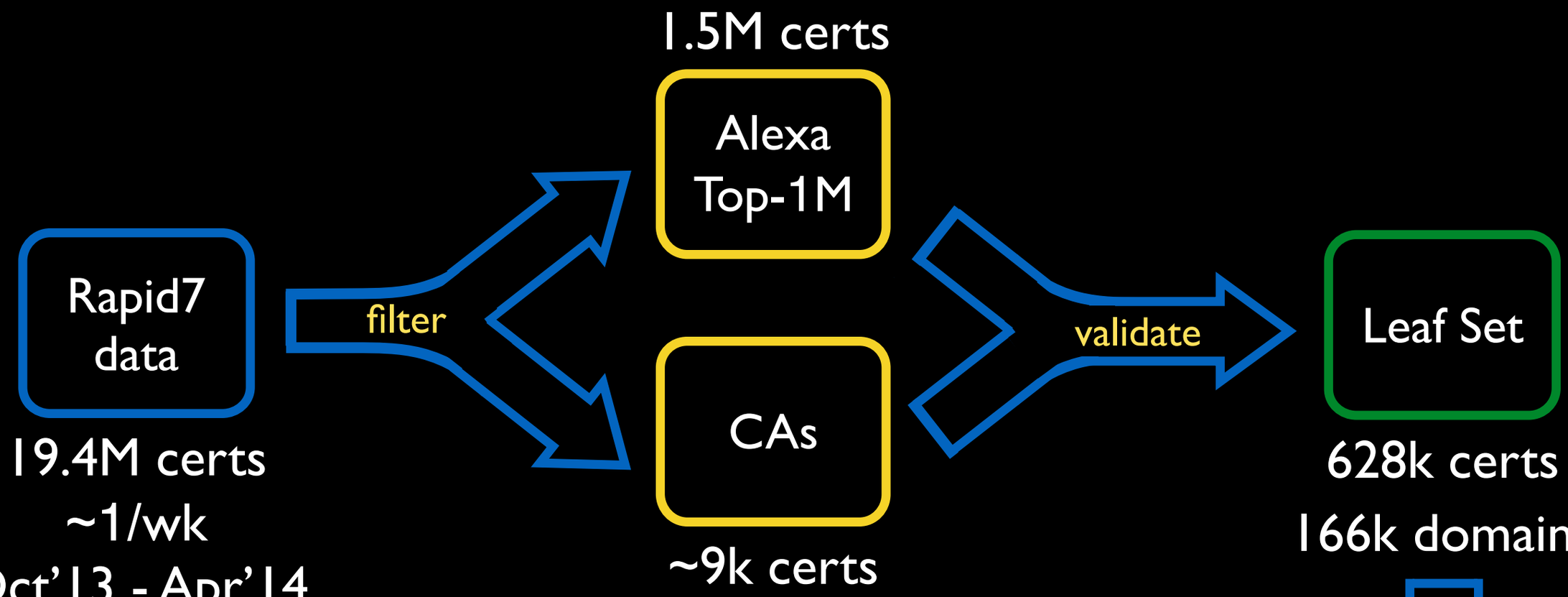
Dataset


1.5M certs
Alexa
Top-1M
Rapid7
data
filter
CAs
19.4M certs
~1/wk
Oct'13 - Apr'14
~9k certs

Dataset


1.5M certs
Alexa Top-1M
Rapid7 data
filter
CAs
validate
Leaf Set
19.4M certs
~1/wk
Oct'13 - Apr'14
~9k certs
628k certs
166k domains

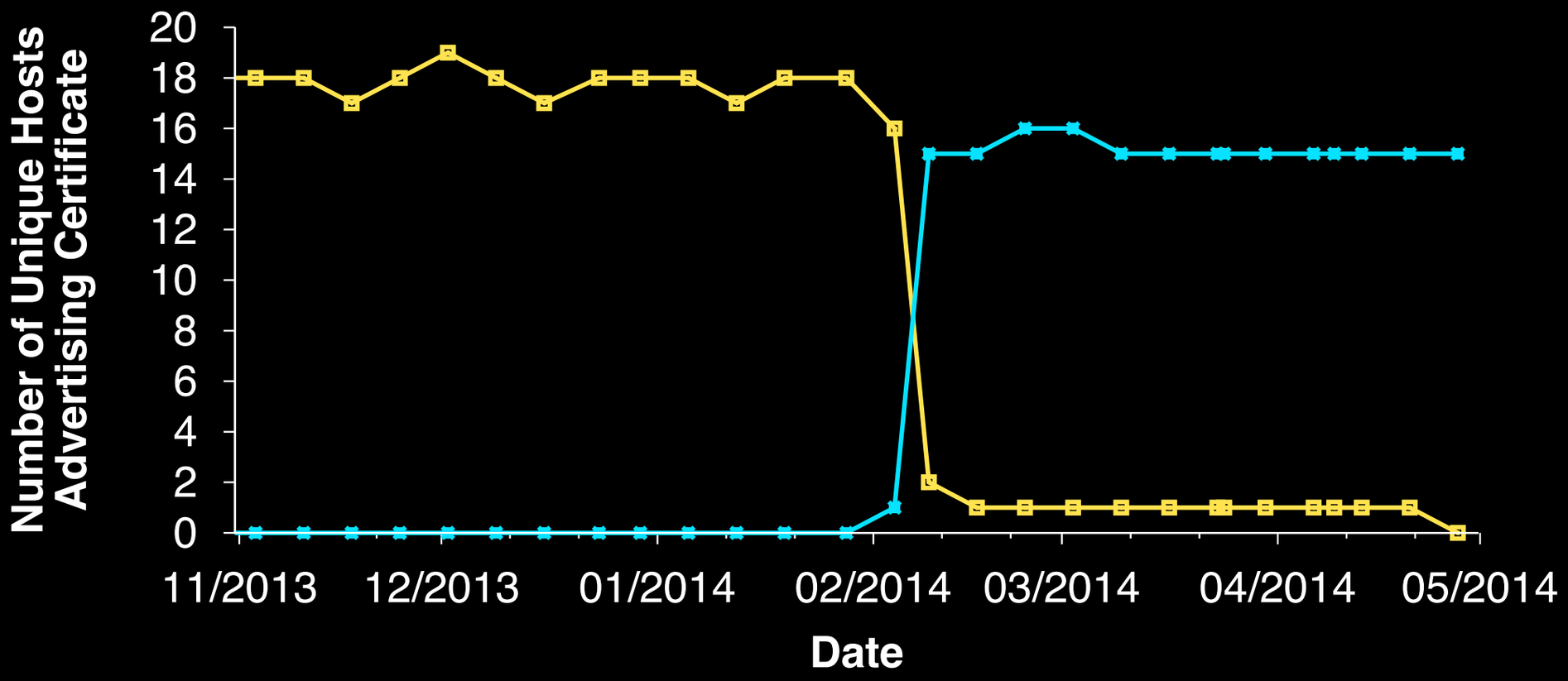
Dataset



- Download CRLs
- Detect Heartbleed vulnerability

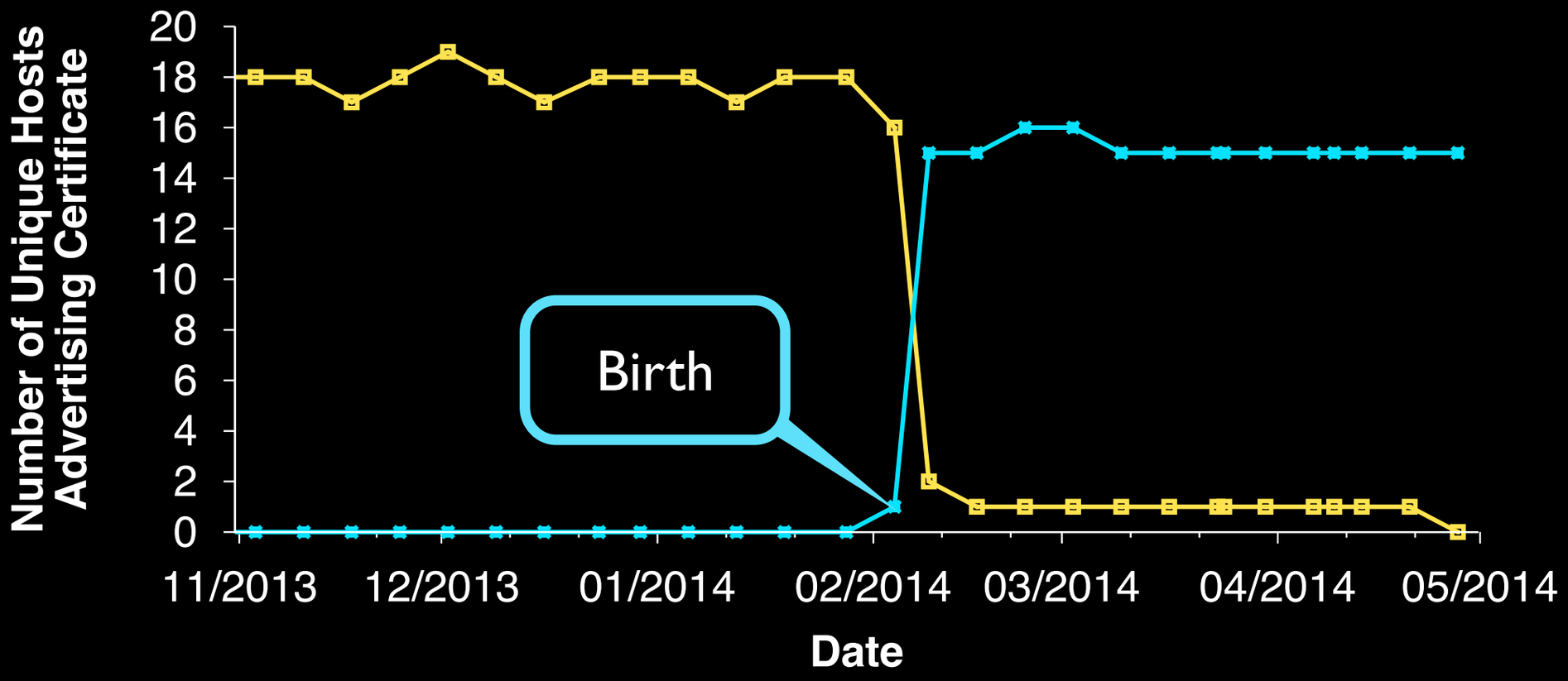
Identifying reissues

m.scotrail.co.uk



Identifying reissues

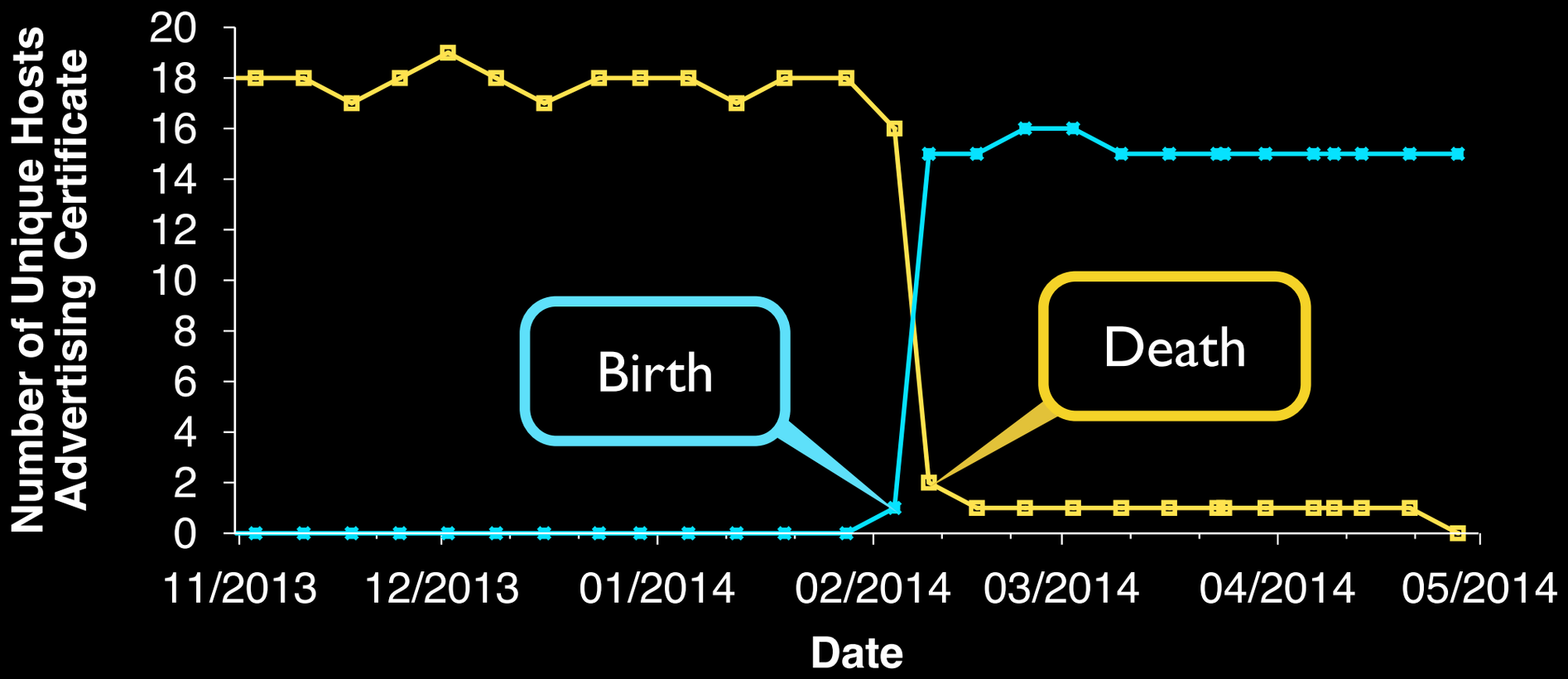
m.scotrail.co.uk



Birth — First crawl we see it announced

Identifying reissues

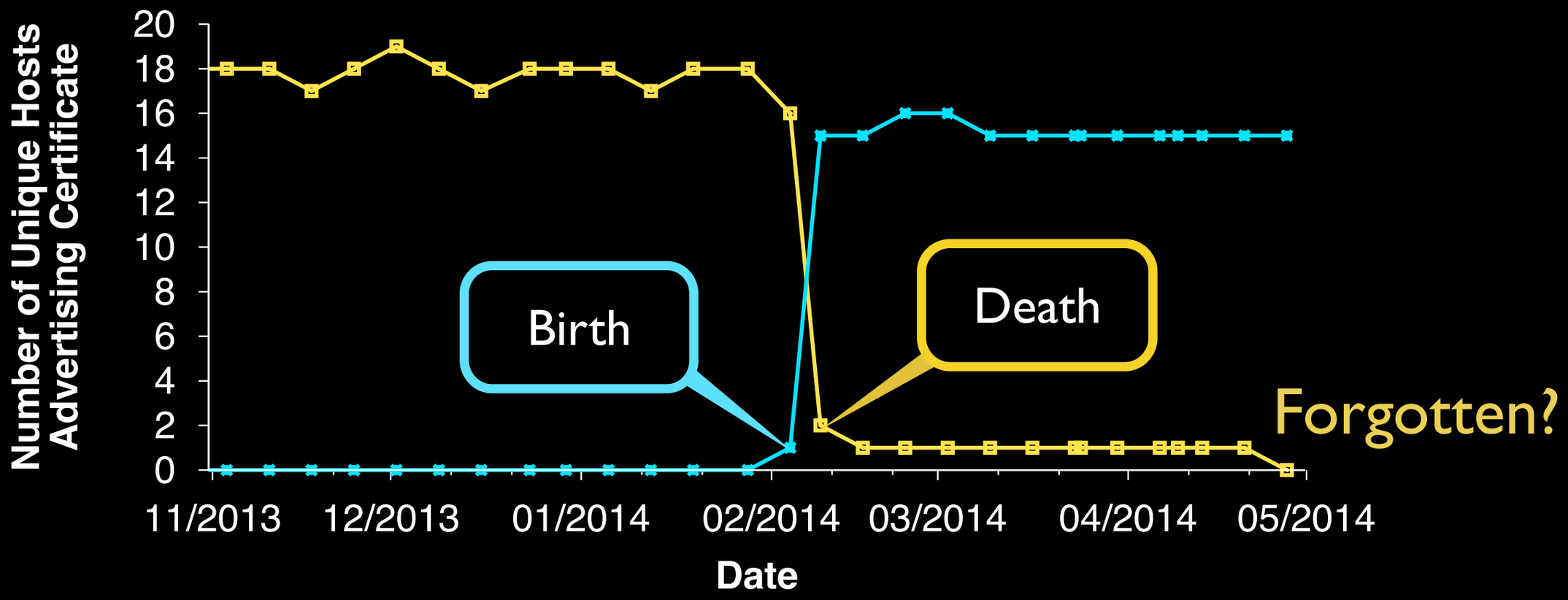
m.scotrail.co.uk



Death — First crawl with ≤10% still announcing it

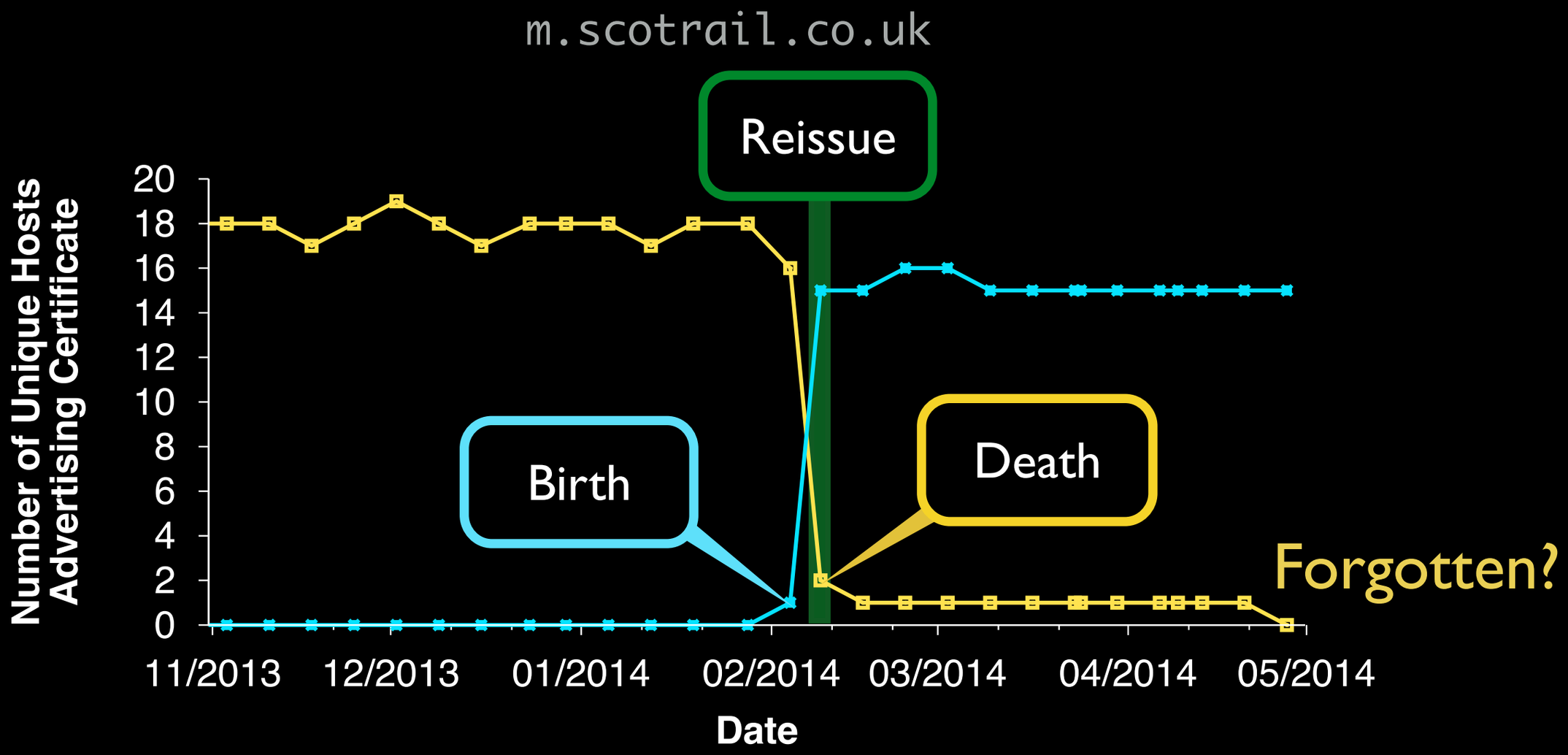
Identifying reissues

m.scotrail.co.uk



Death First crawl with ≤10% still announcing it

Identifying reissues



Reissue — Birth + death + we see a host swap

Attributing reissues to Heartbleed

Attributing reissues to Heartbleed

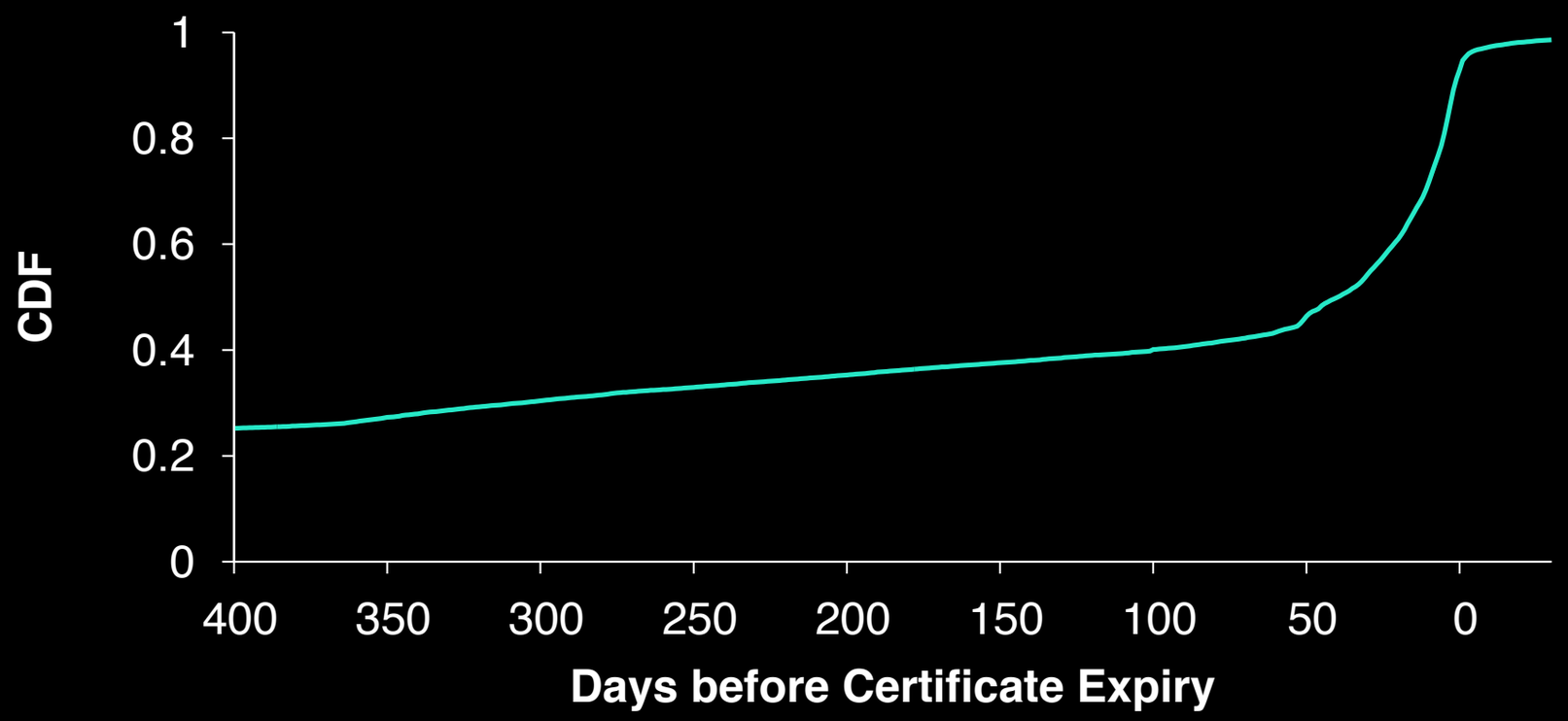
1. Reissued on or after April 7

Attributing reissues to Heartbleed

1. Reissued on or after April 7
2. Expiration date >60 days away

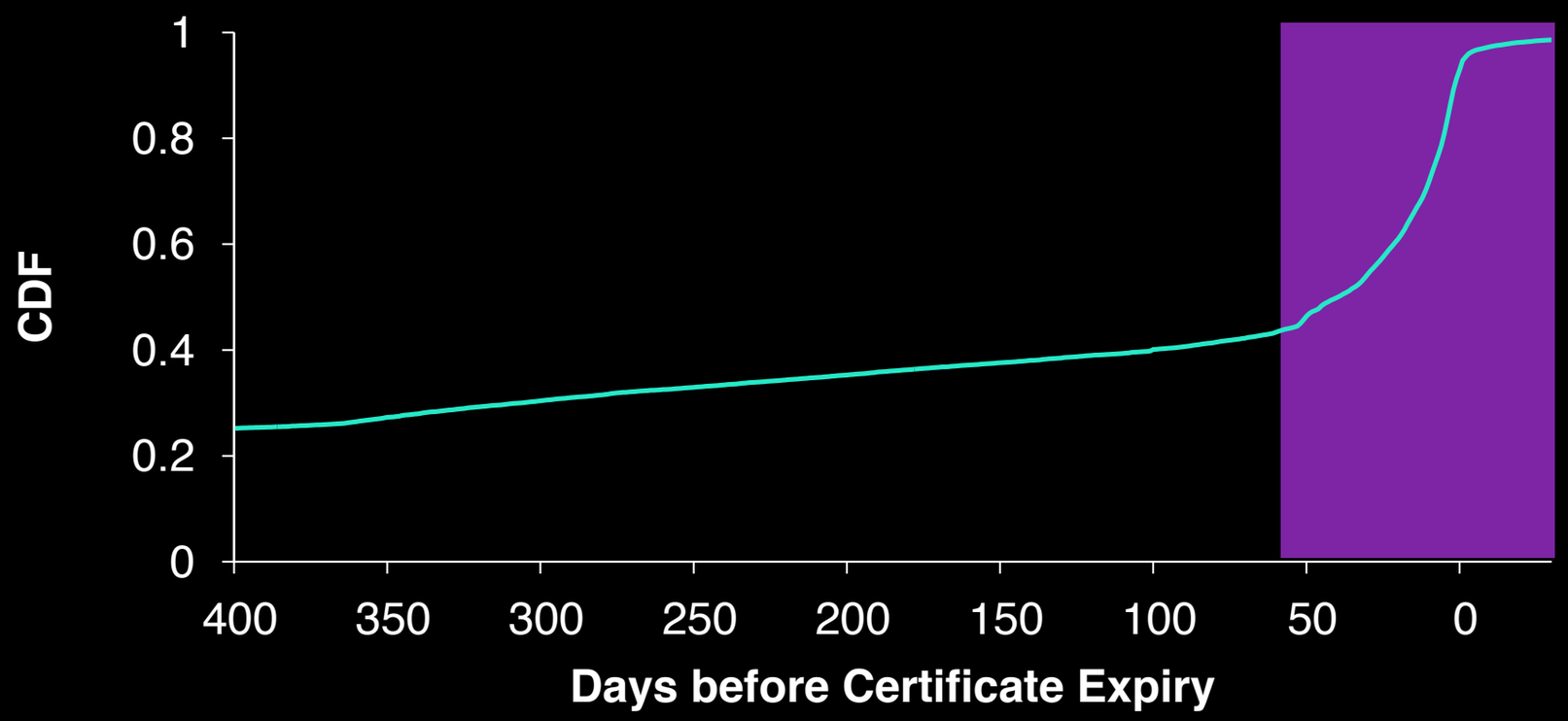
Attributing reissues to Heartbleed

1. Reissued on or after April 7
2. Expiration date >60 days away



Attributing reissues to Heartbleed

1. Reissued on or after April 7
2. Expiration date >60 days away

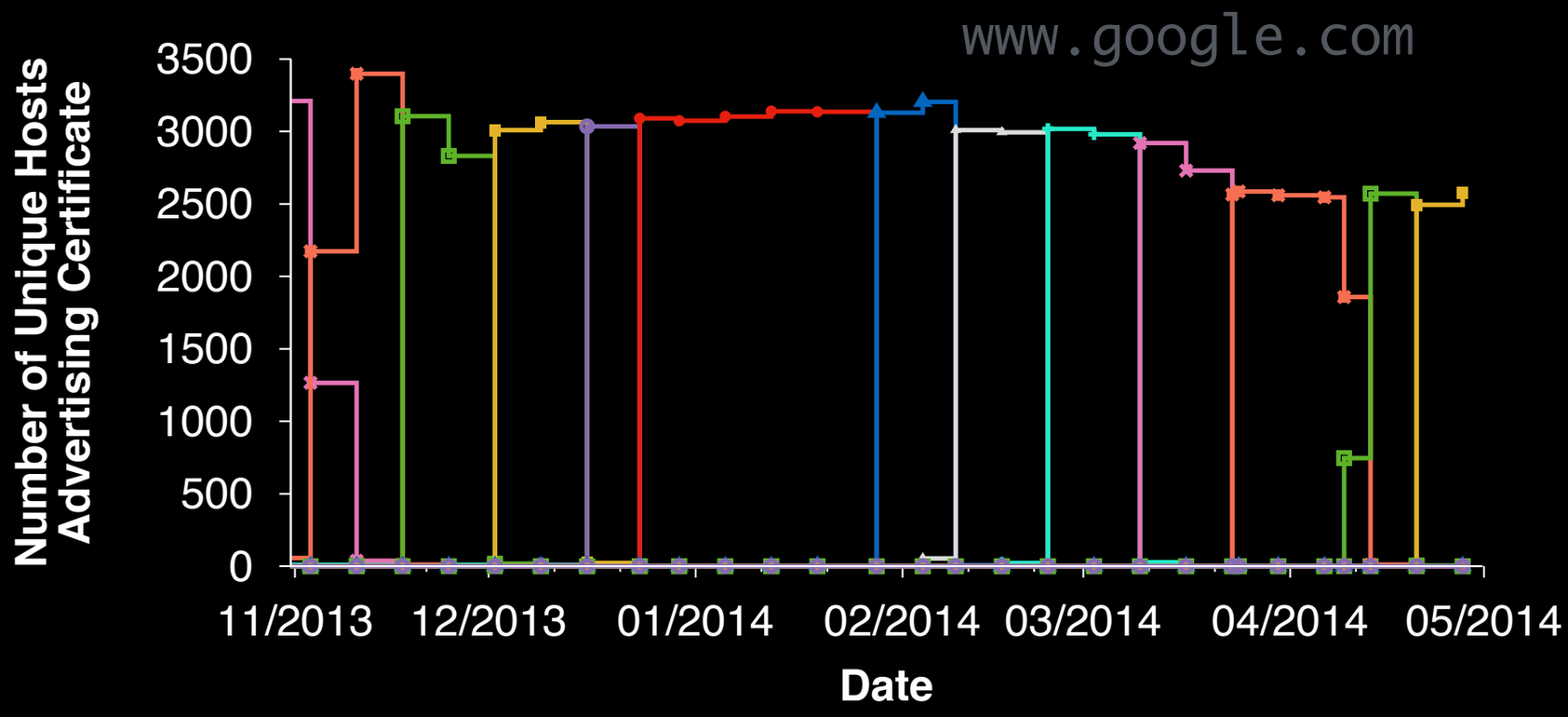


Attributing reissues to Heartbleed

1. Reissued on or after April 7
2. Expiration date >60 days away
3. Domain reissues <1 time per 2mos

Attributing reissues to Heartbleed

1. Reissued on or after April 7
2. Expiration date >60 days away
3. Domain reissues <1 time per 2mos



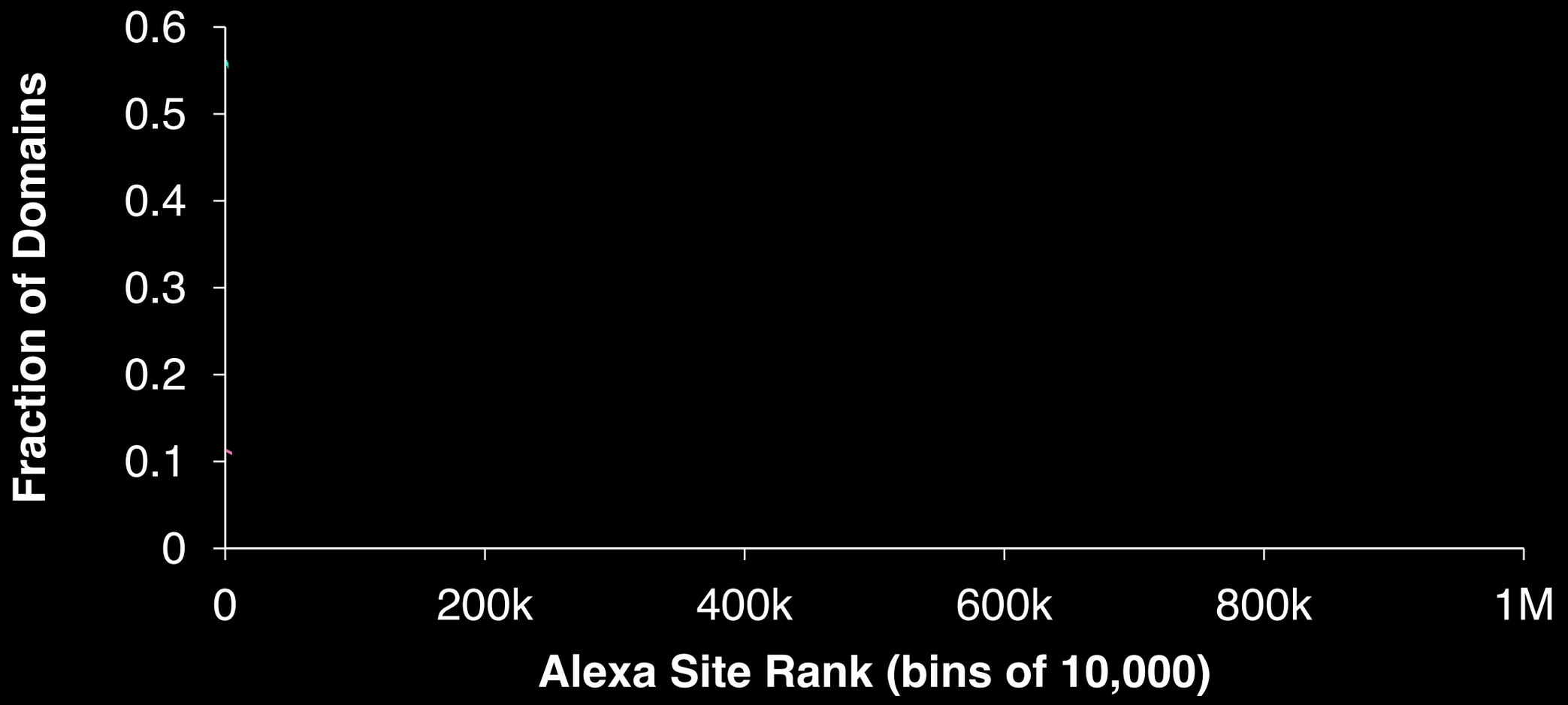
Outline

1. ~~Motivation~~
2. ~~Data and methodology~~
3. Analysis

Outline

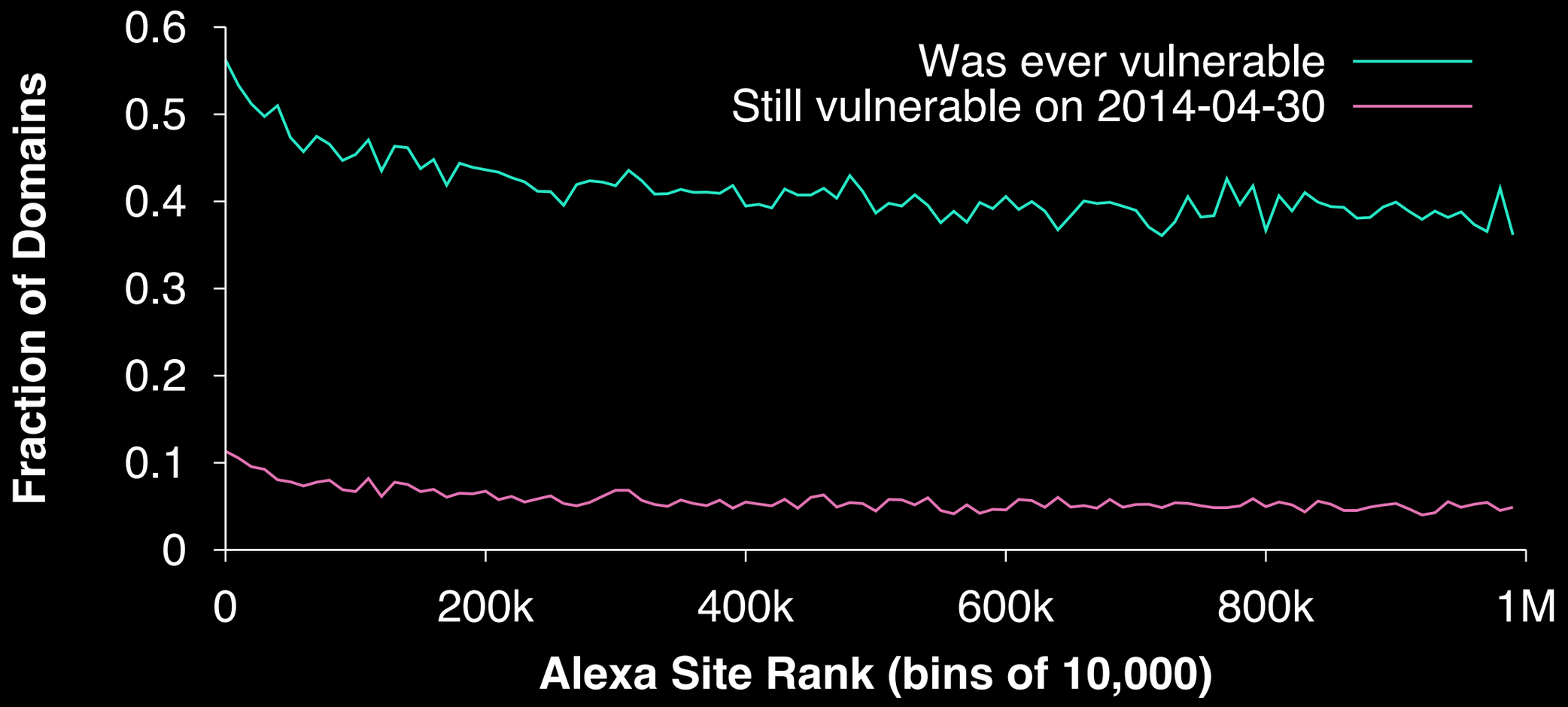
1. ~~Motivation~~
2. ~~Data and methodology~~
3. Analysis

Prevalence and patch rates



Prevalence and patch rates

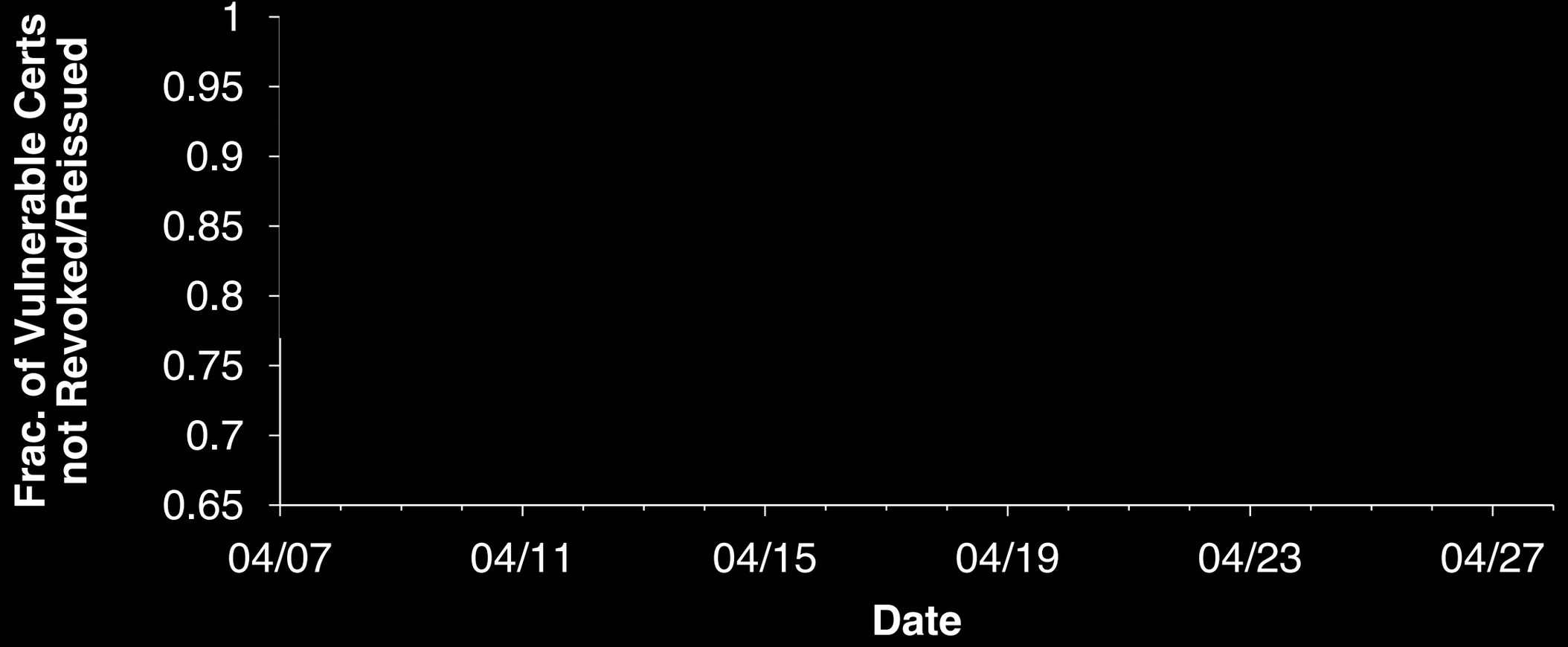
Prevalence and patch rates



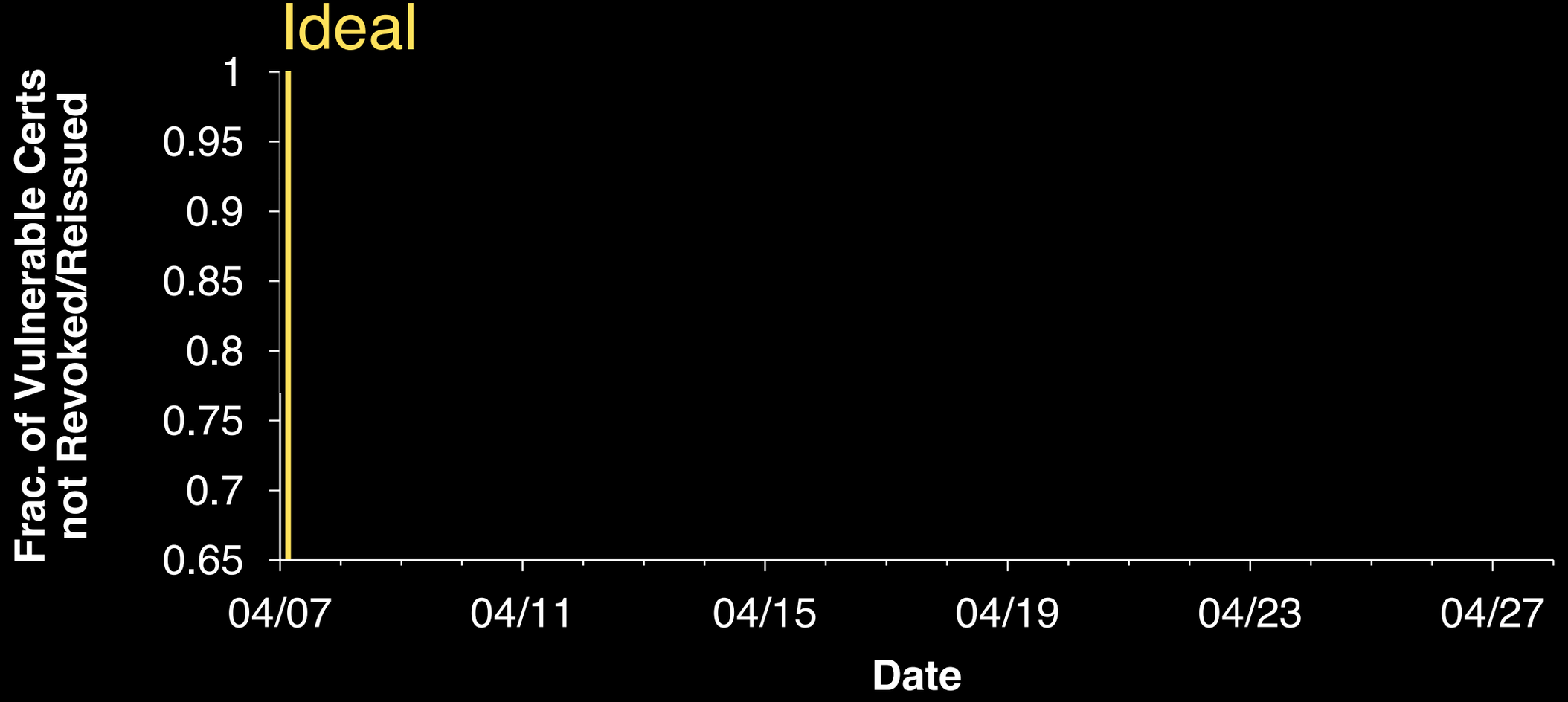
Patching rates are mostly positive

~6% still vulnerable after 3 weeks

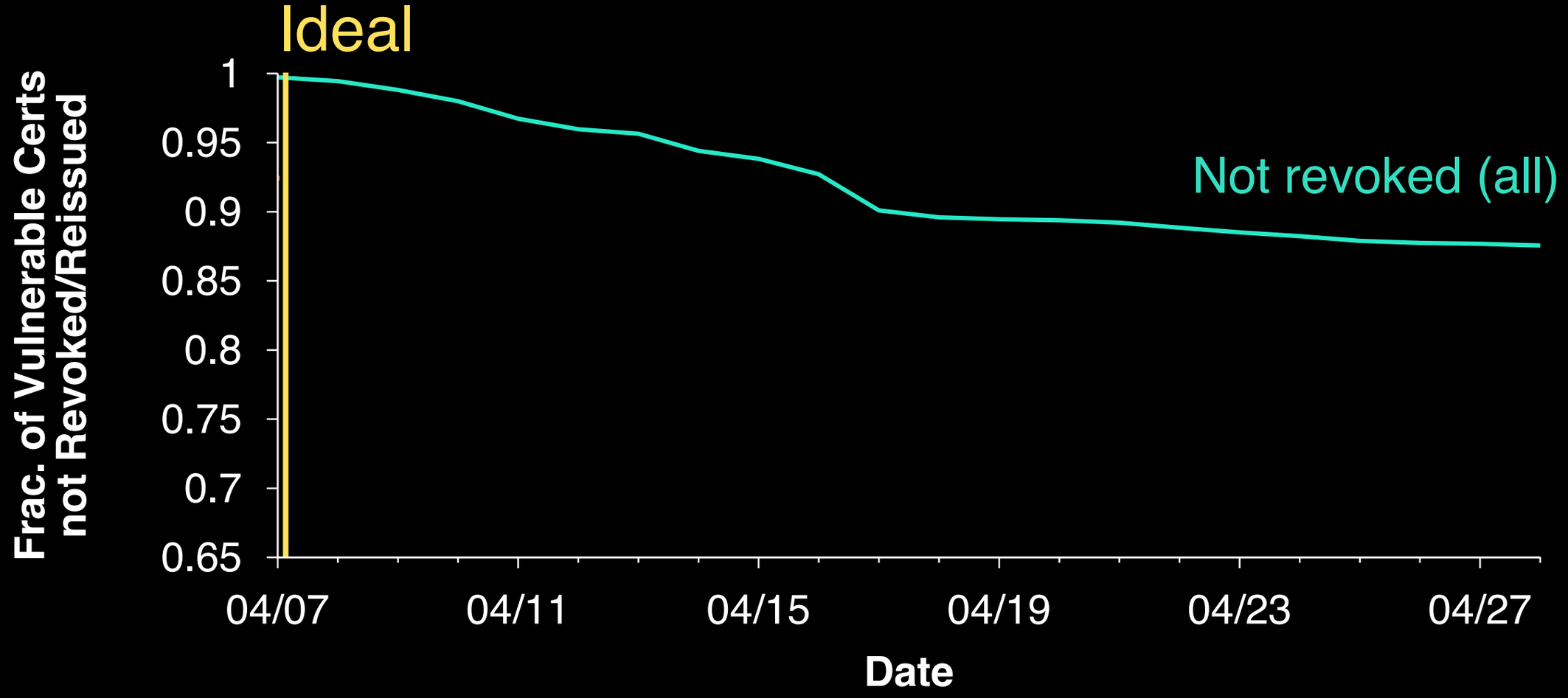
Certificate revocation rates



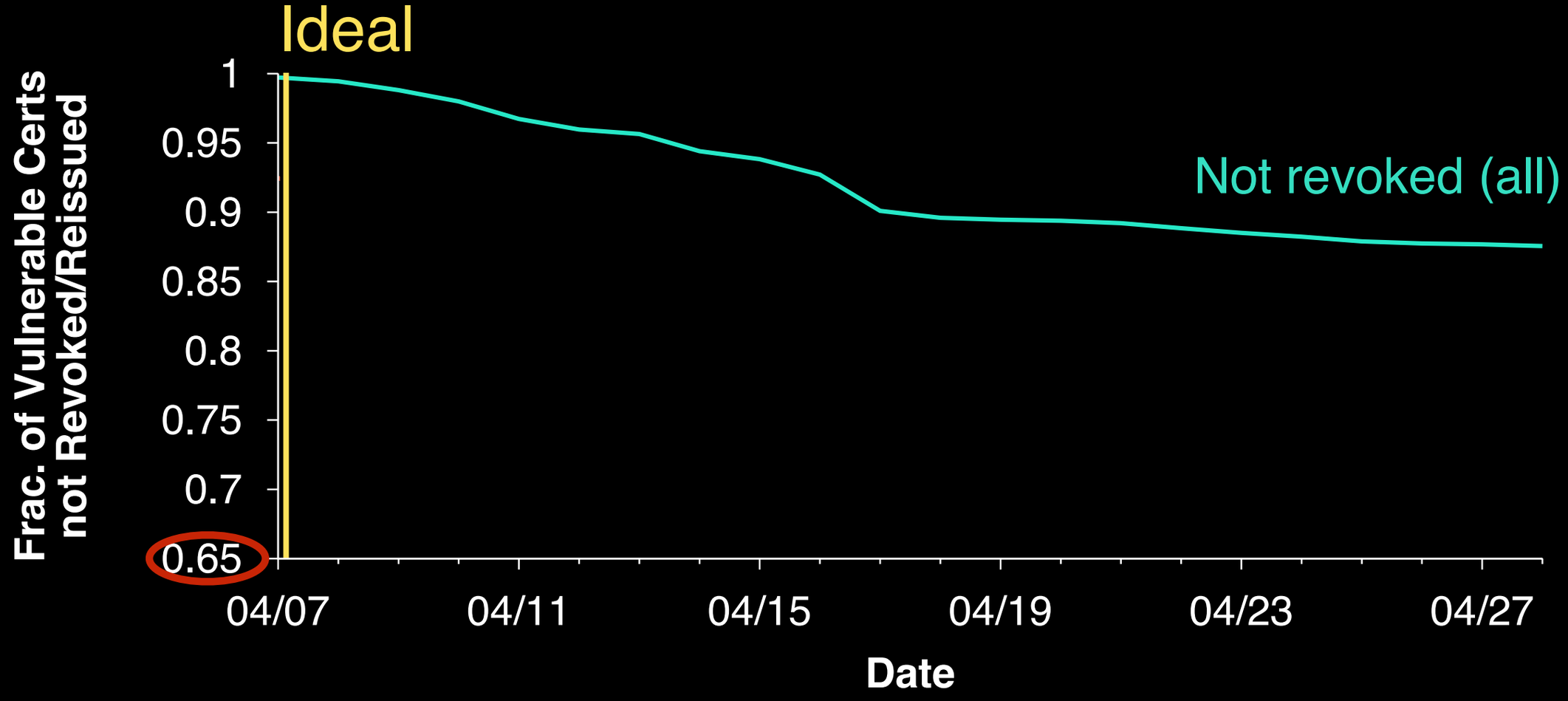
Certificate revocation rates



Certificate revocation rates



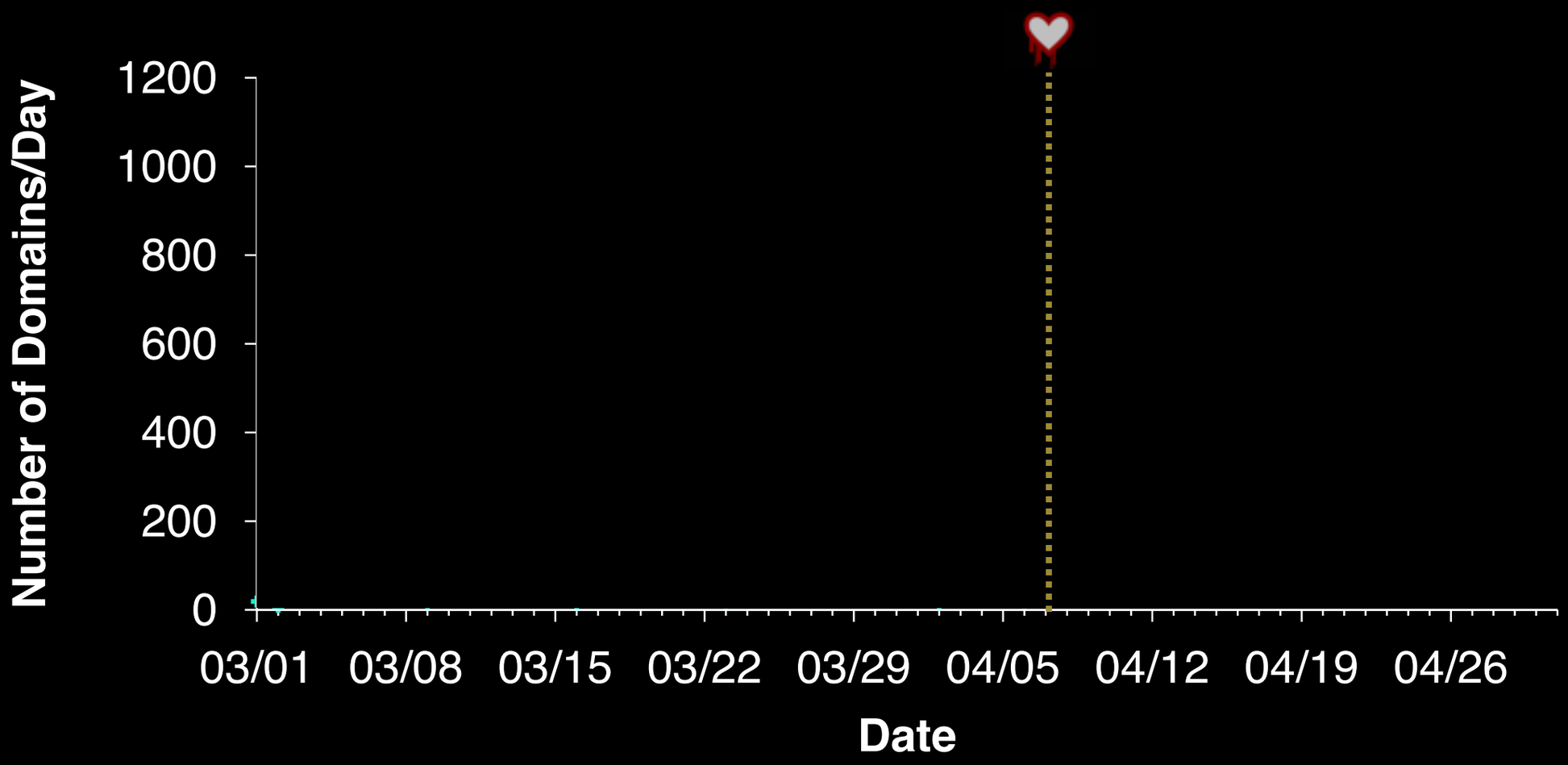
Certificate revocation rates



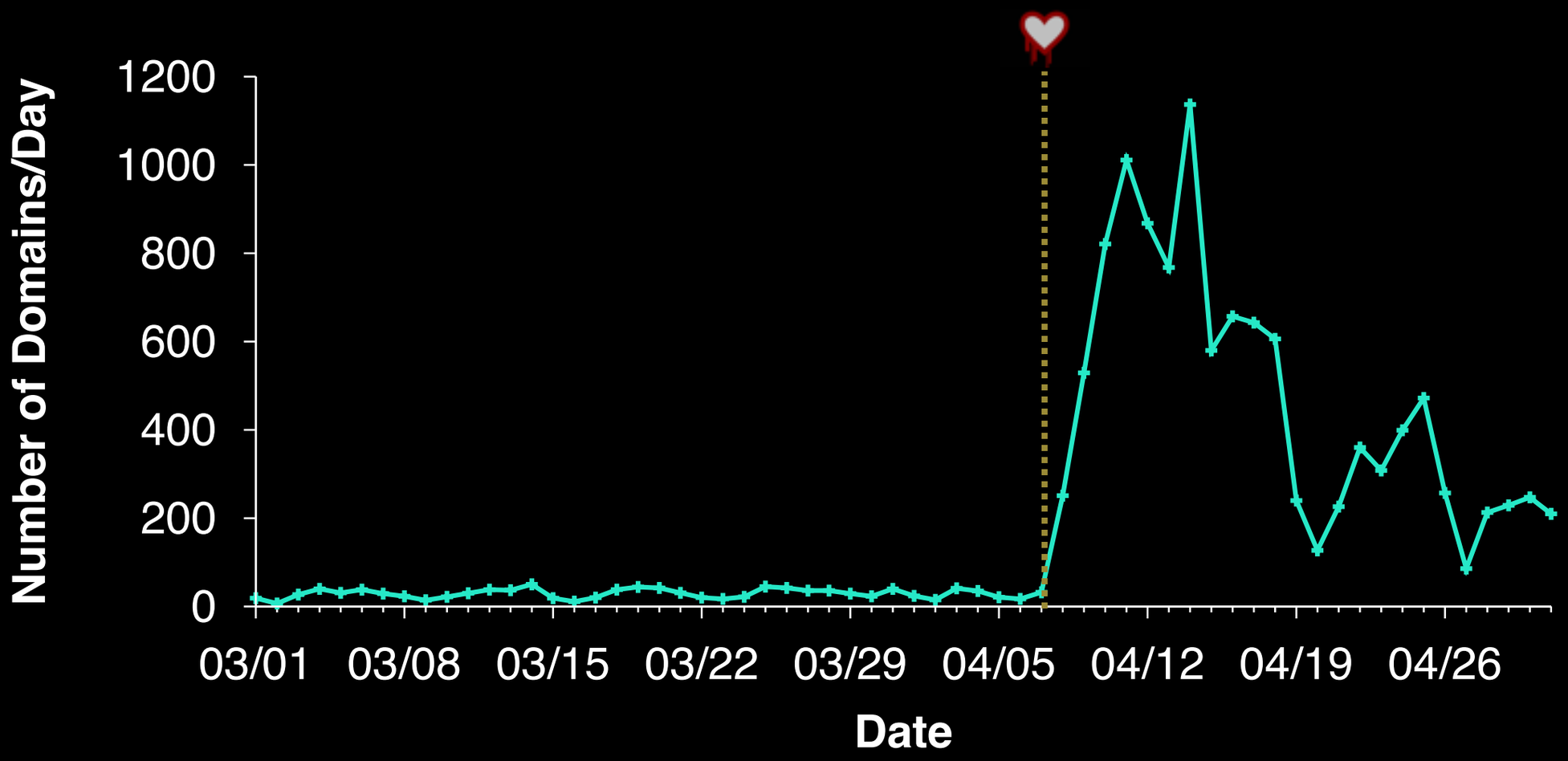
Exponential drop-off, then levels out

After 3 weeks: 13% Revoked

How quickly were certs revoked?

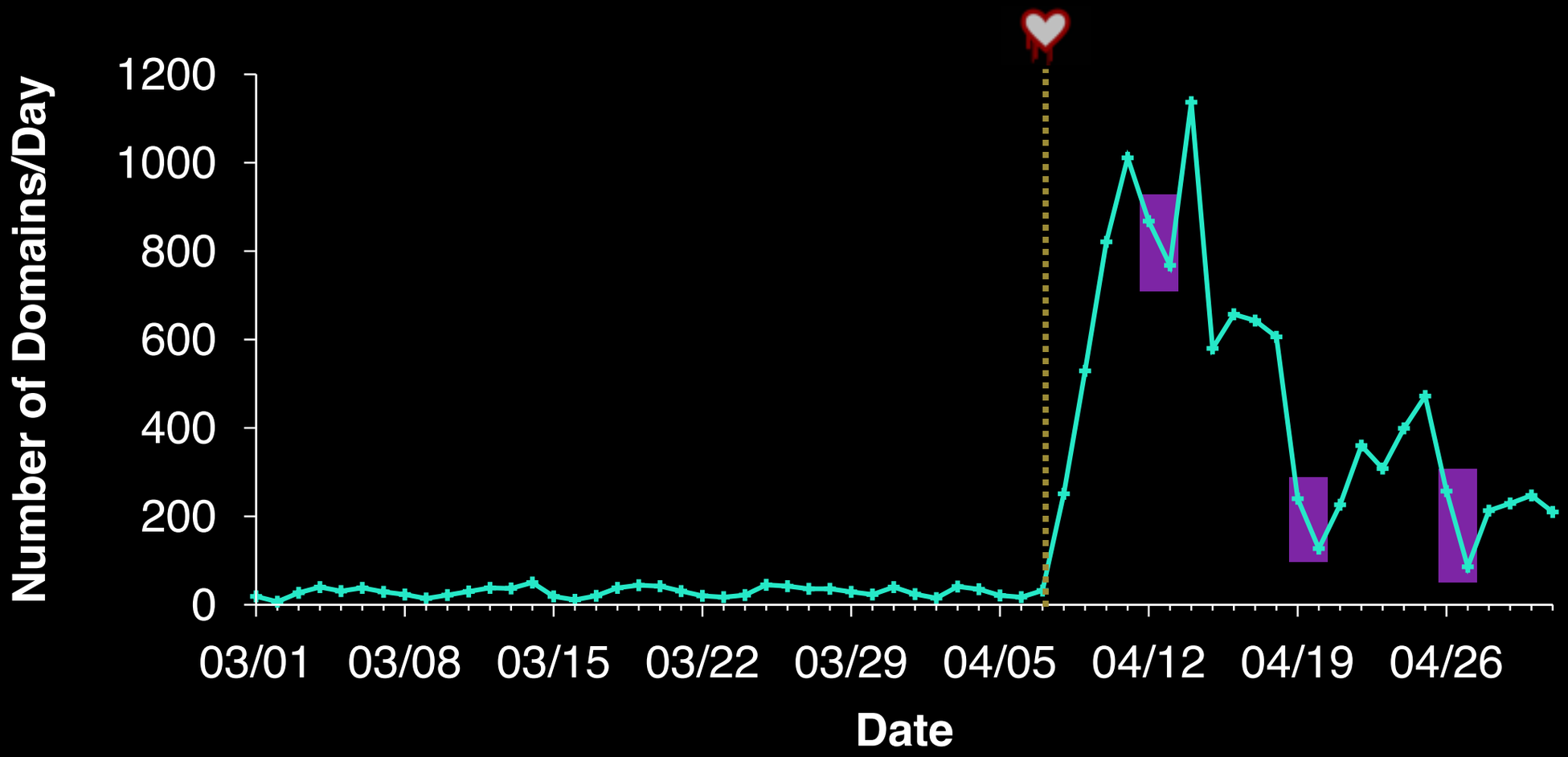


How quickly were certs revoked?



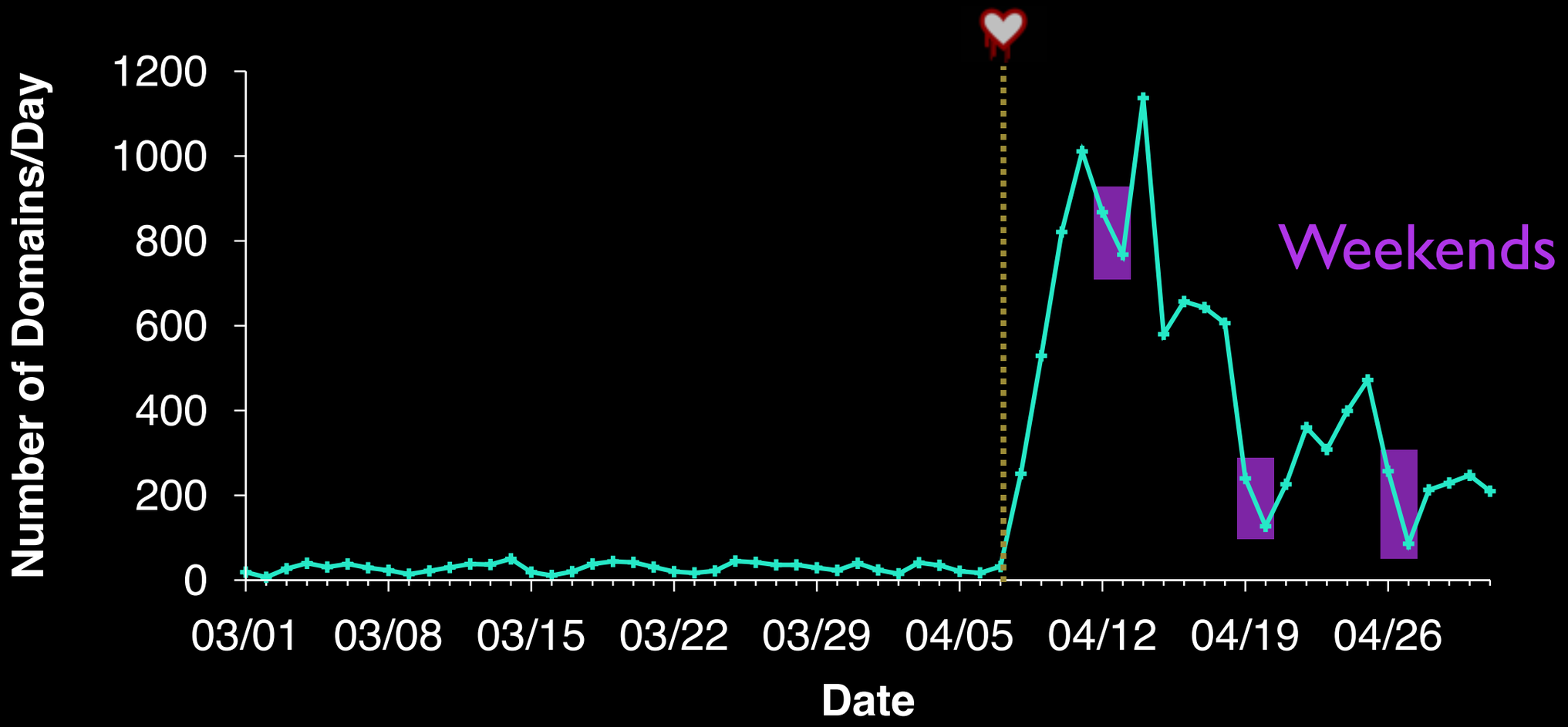
Reaction ramps up quickly

How quickly were certs revoked?



Reaction ramps up quickly

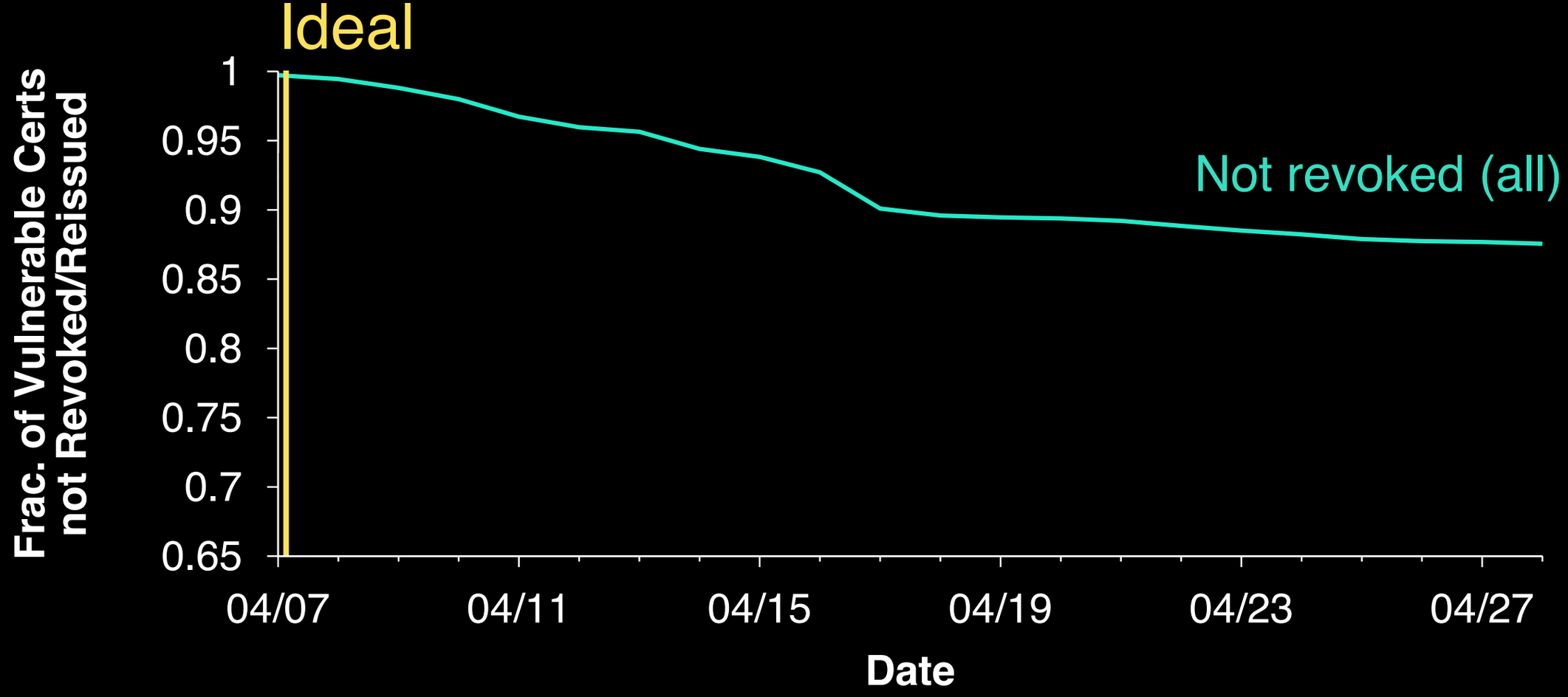
How quickly were certs revoked?



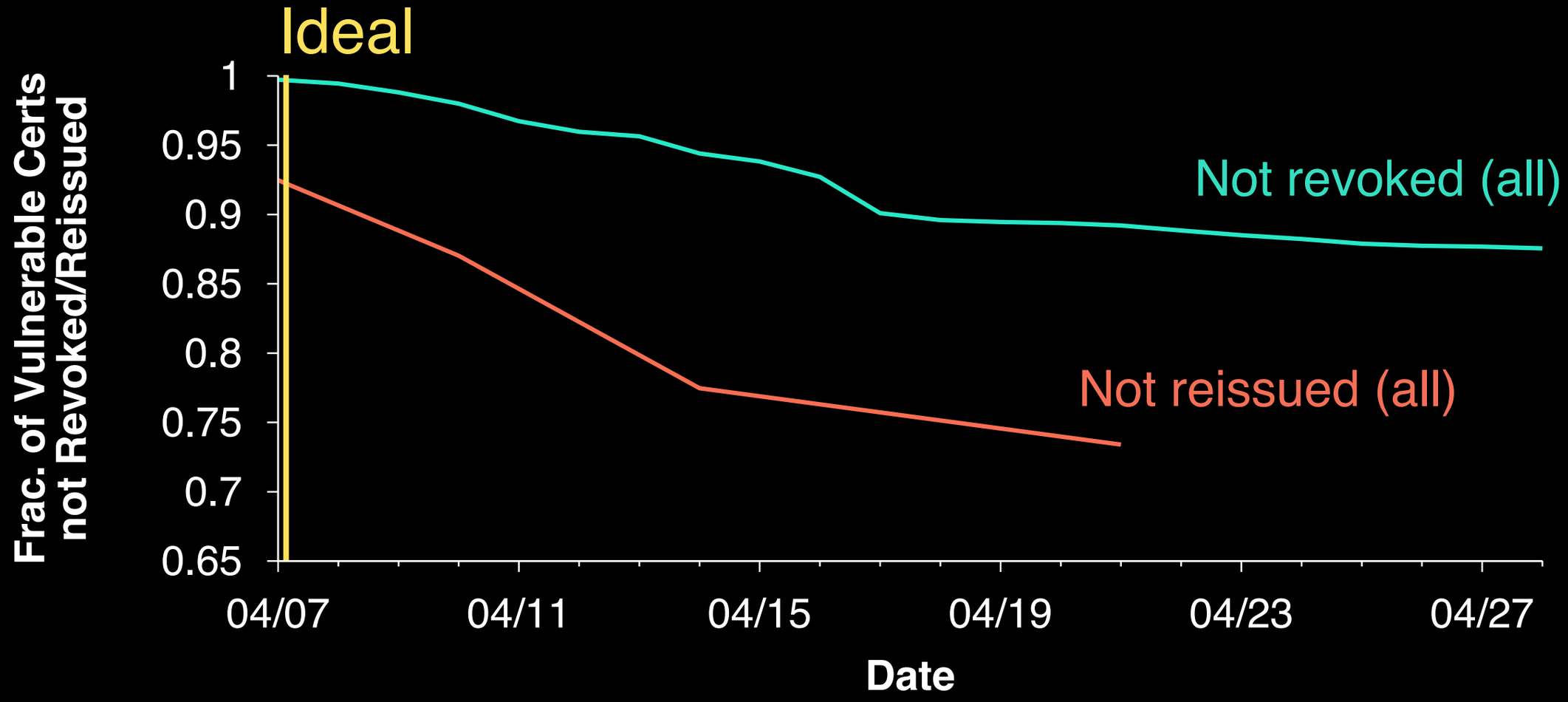
Reaction ramps up quickly

Security takes the weekends off

Certificate reissue rates



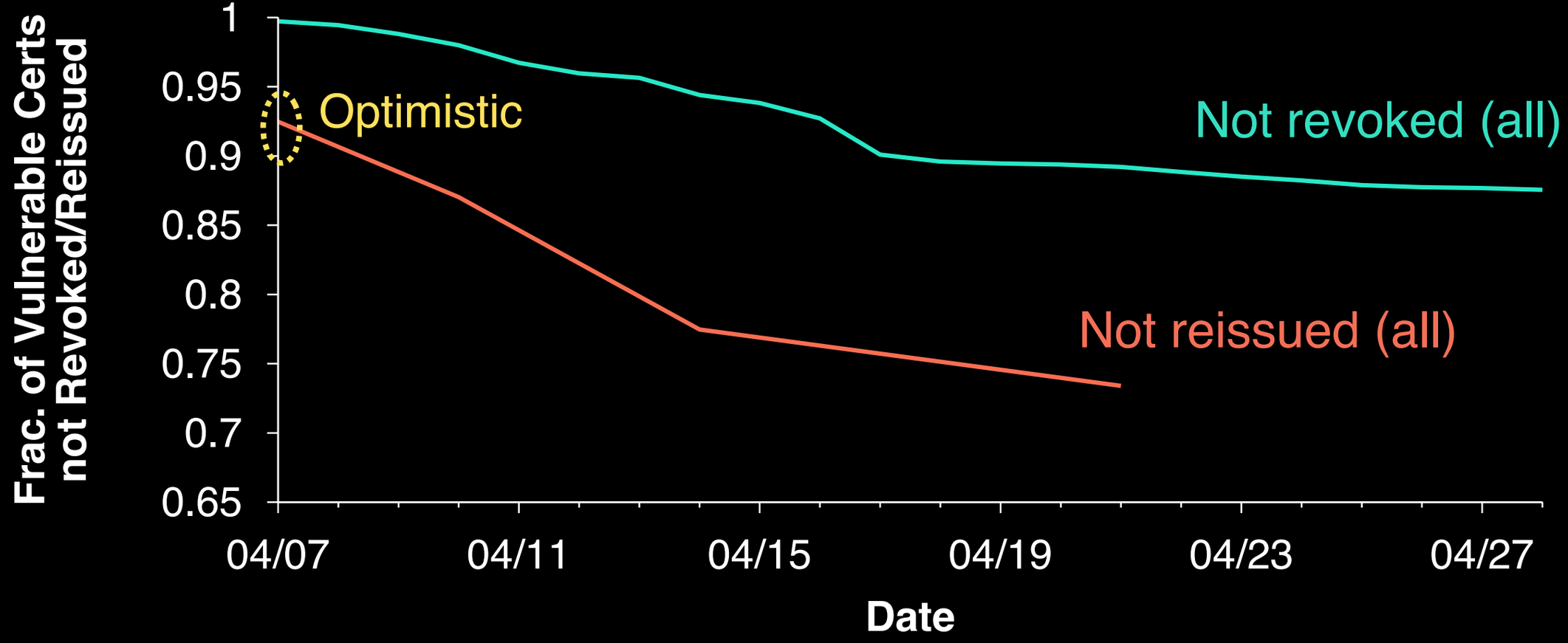
Certificate reissue rates



Compared to revocations:
Similar pattern but better reissue rate

After 3 weeks: 27% Reissued

Certificate reissue rates

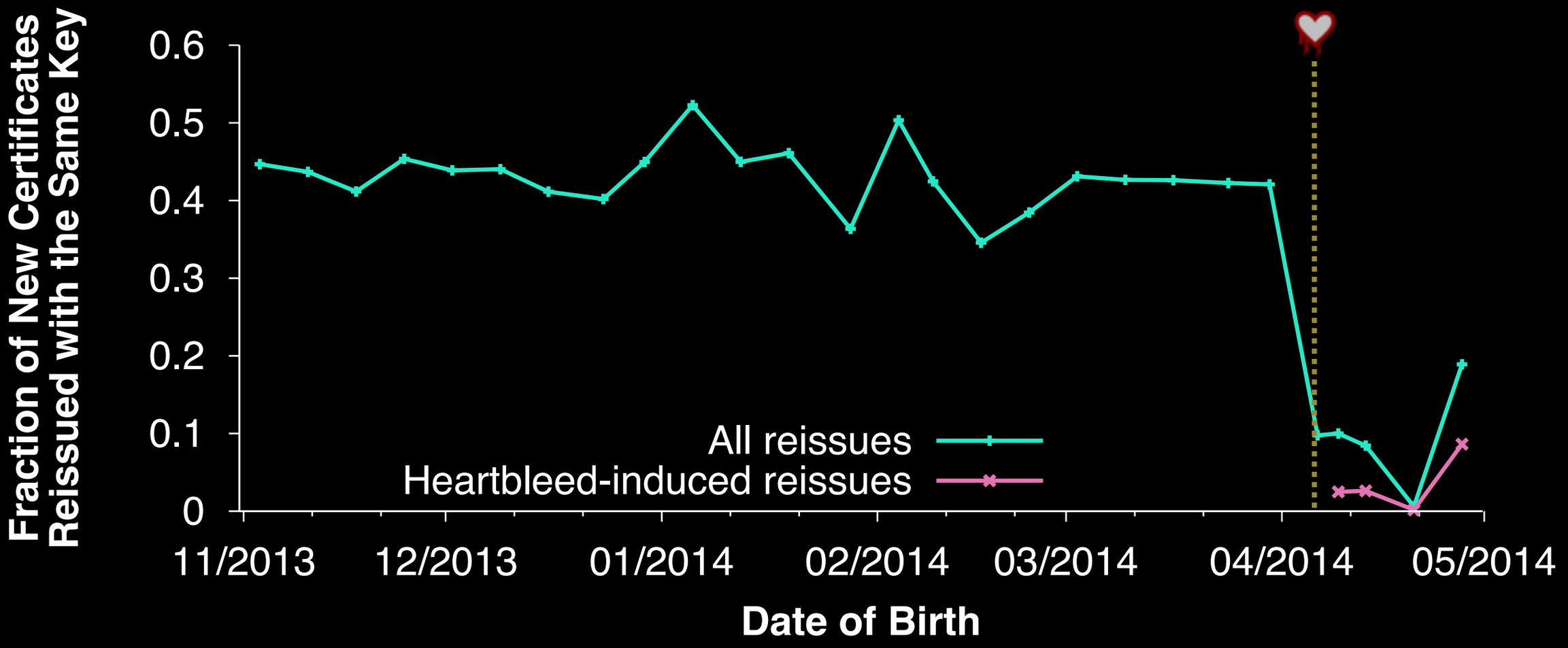


Compared to revocations:
Similar pattern but better reissue rate

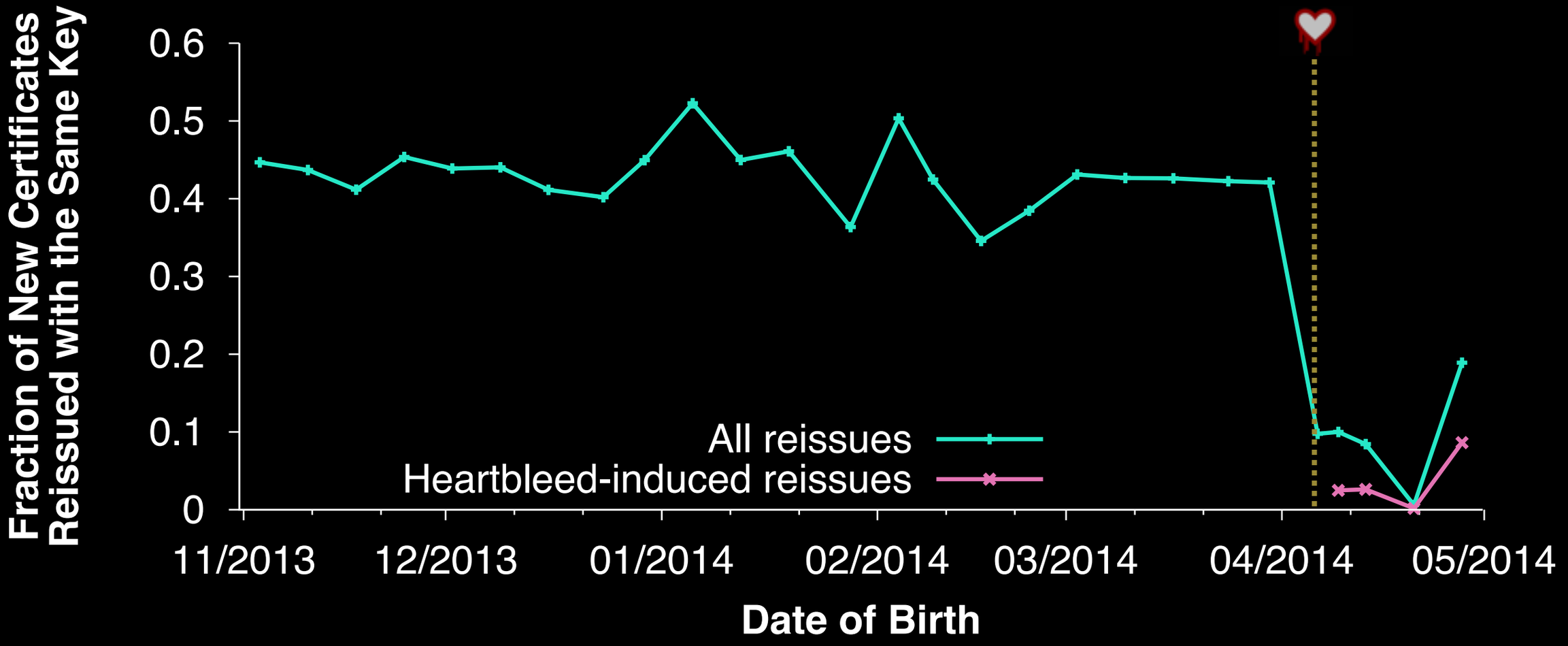
After 3 weeks: 27% Reissued

Reissue ⇒ New key?

Reissue ⇒ New key?



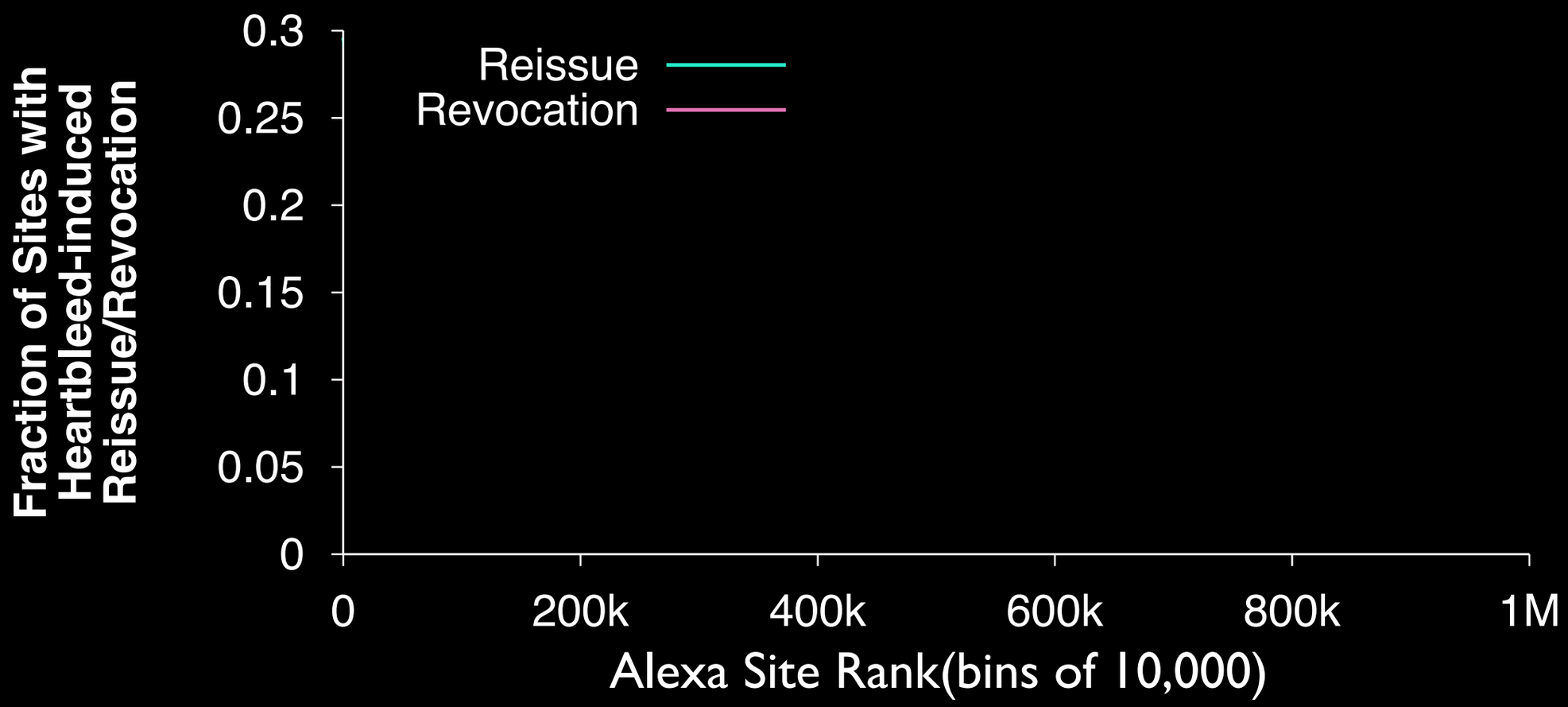
Reissue ⇒ New key?



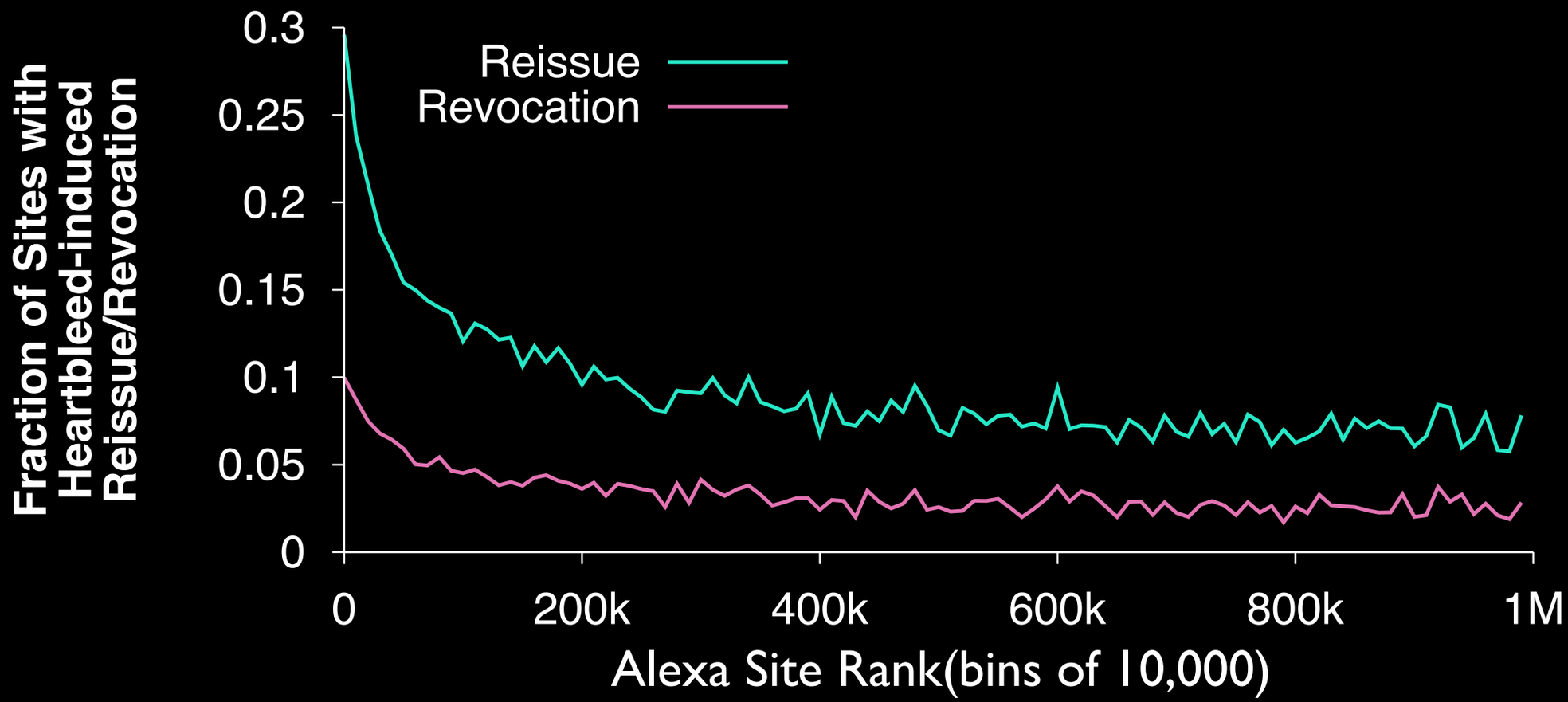
Reissuing the same key is common practice

4.1% Heartbleed-induced with same key

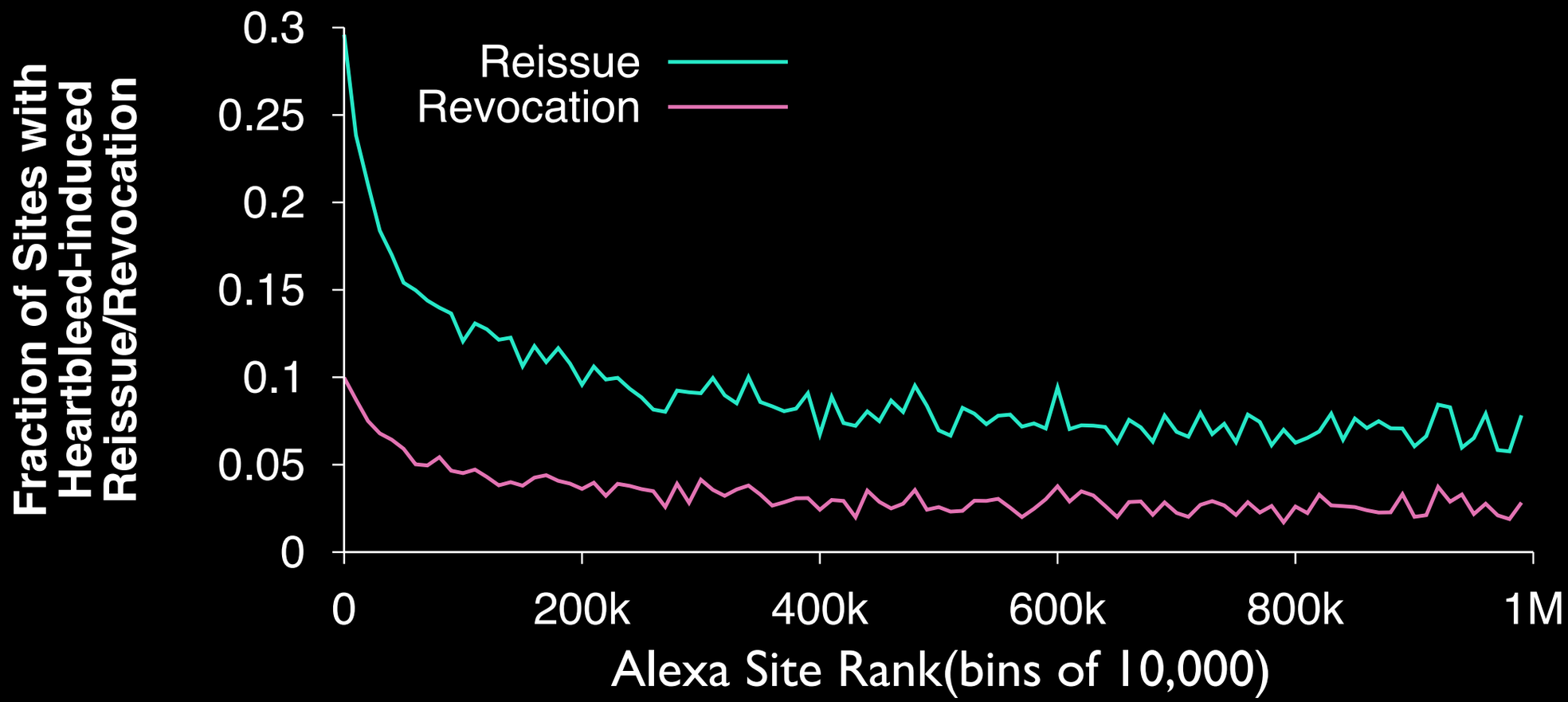
Popularity ⇒ Better reaction?



Popularity ⇒ Better reaction?



Popularity ⇒ Better reaction?



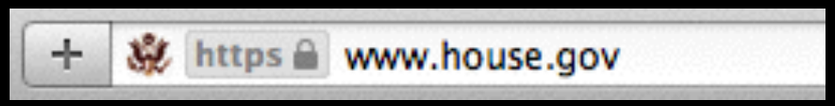
Administrators of even highly popular websites aren't doing what the PKI needs them to do

EV Certificates

More thorough vetting process of CAs and clients

Extended Validation

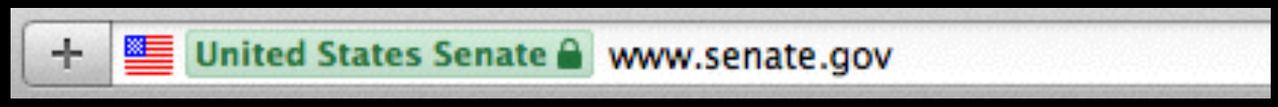
Normal



EV Certificates

More thorough vetting process of CAs and clients

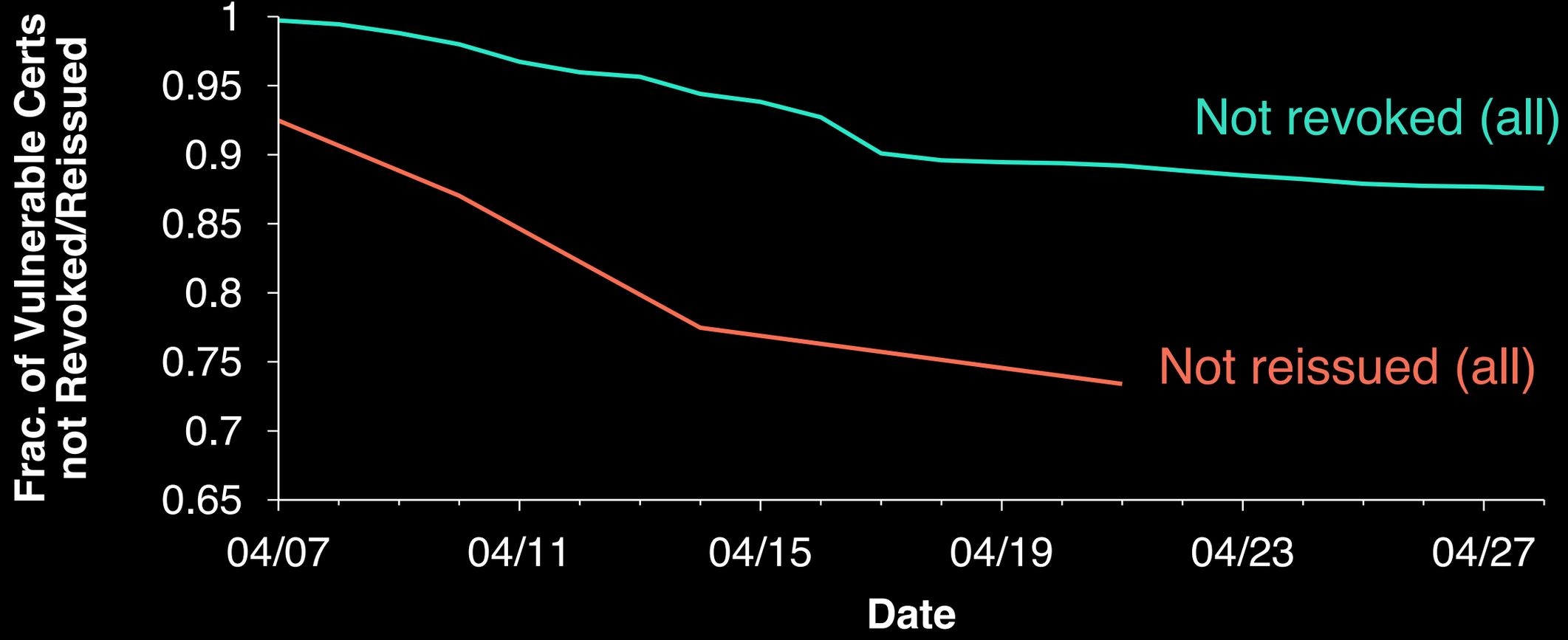
Extended Validation



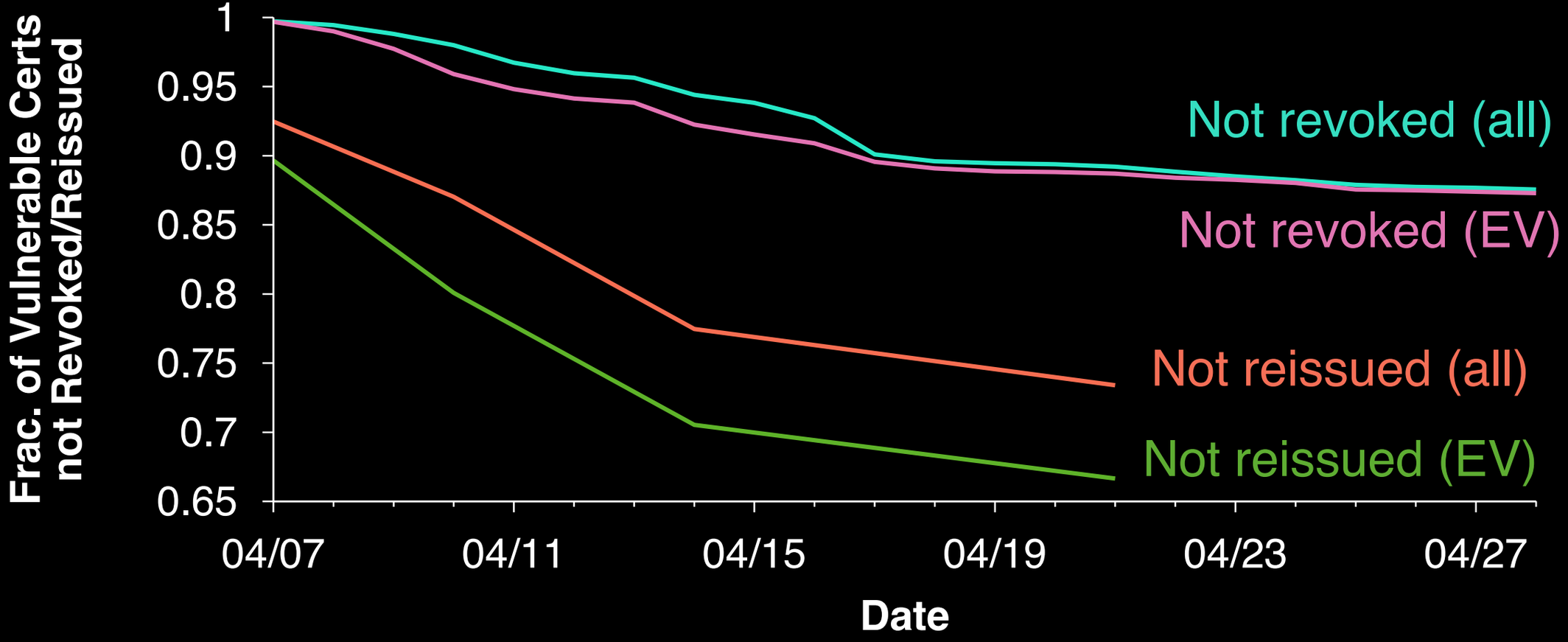
Normal

Does the more thorough vetting process translate into better *security practices*?

Are EV certs better managed?

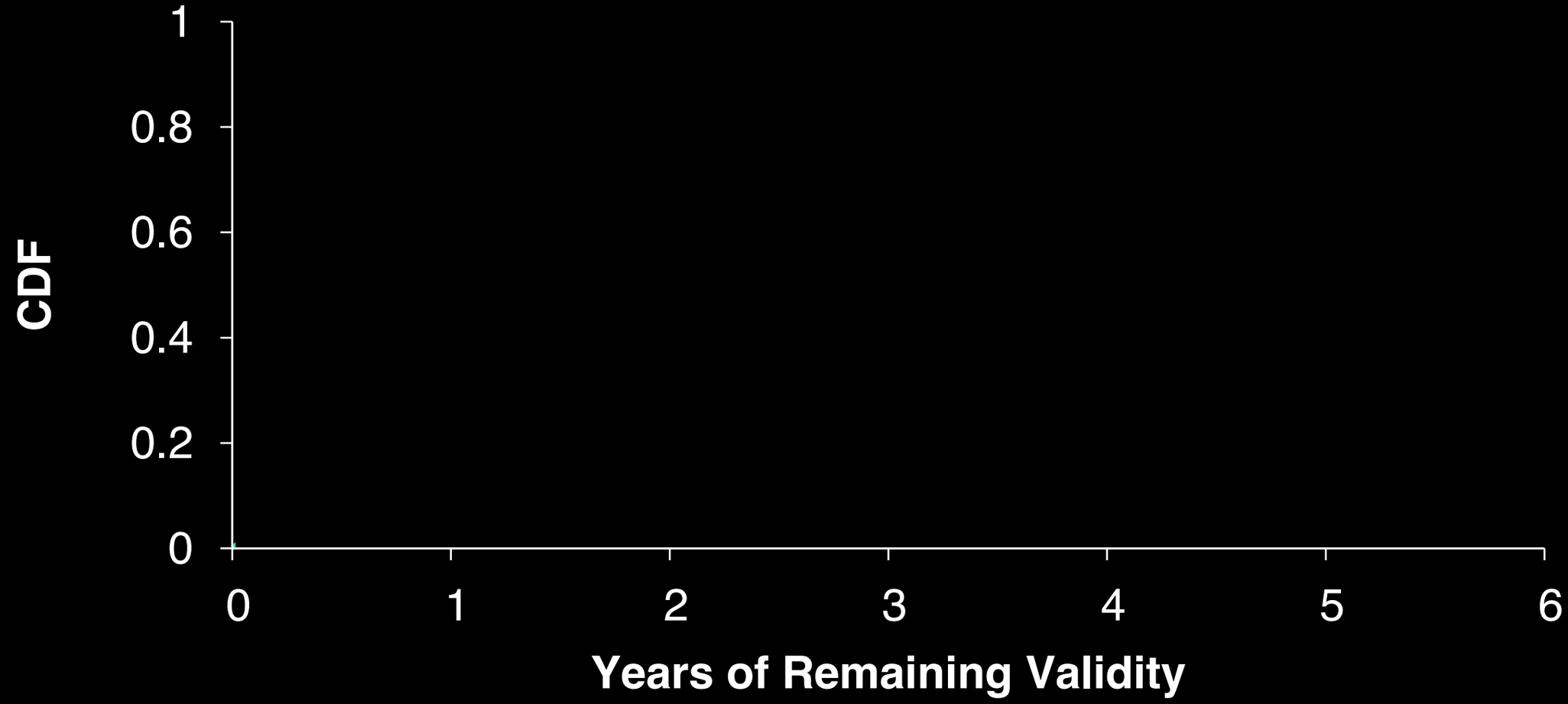


Are EV certs better managed?



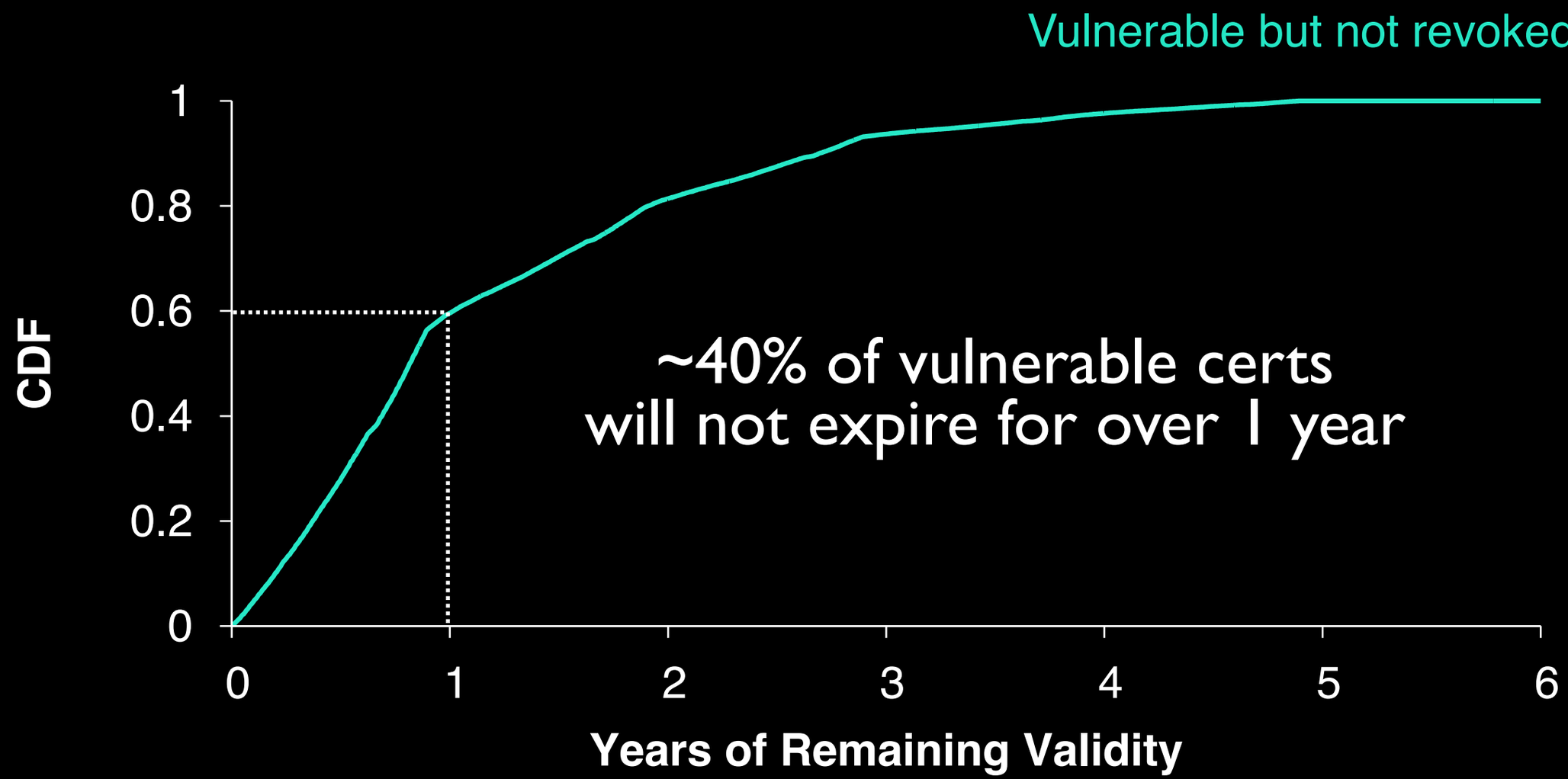
EV certs exhibit slightly better rates (8% reissue)

Can we wait for expiration?

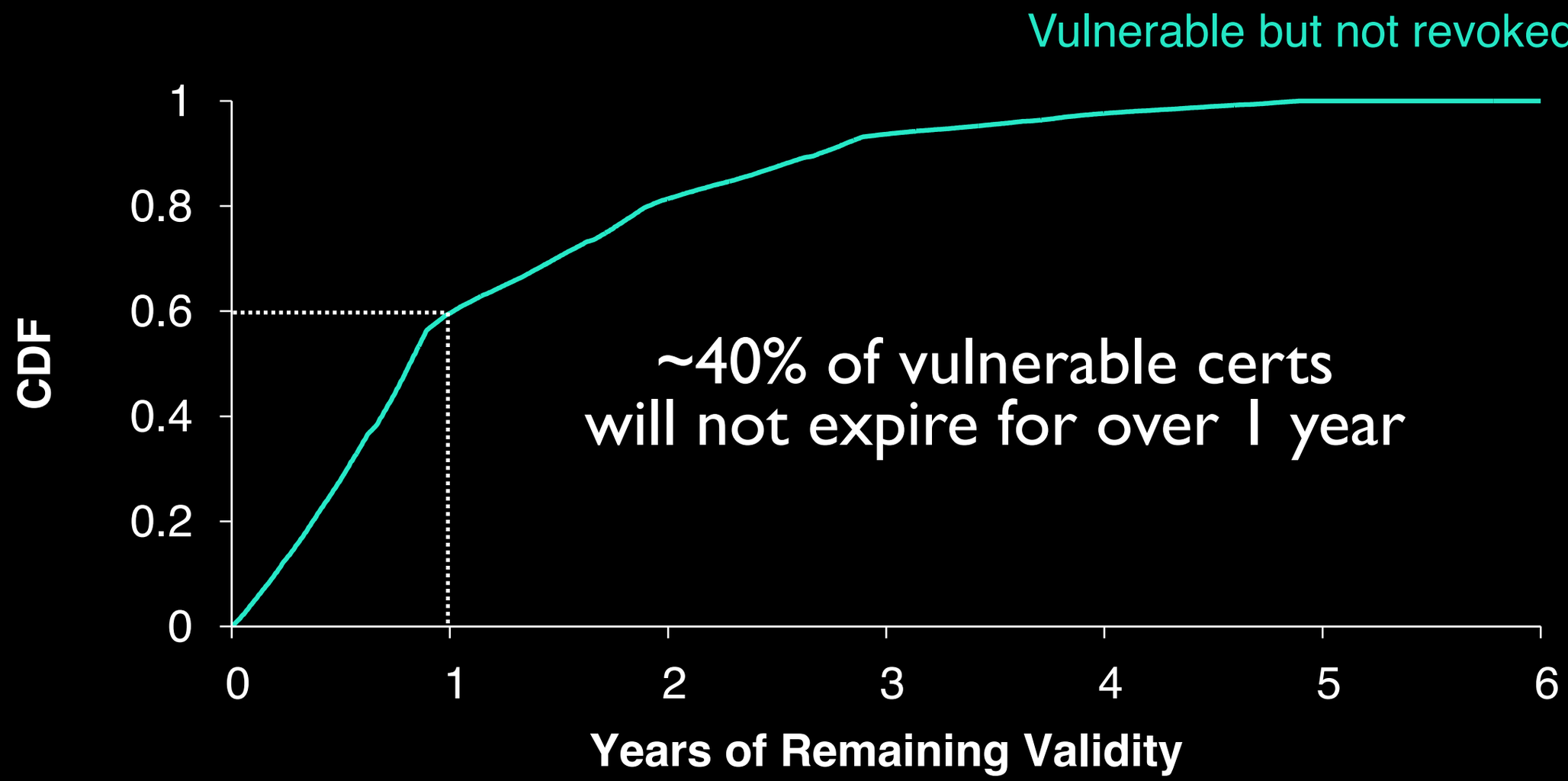


Can we wait for expiration?

Can we wait for expiration?



Can we wait for expiration?



We may be dealing with Heartbleed for *years*

In the paper

- Most reason codes are incorrect
- Revocation and reissue are not simultaneous
- CAs update CRLs in hours
- Heartbleed induce more retired certificates revocations

  and more …

Summary

- First study focus on certificates reissues and revocations
  - Large-scale measurements
  - Developed new methodologies and heuristics

- Key findings
  - After three weeks, only 13% revoked and 27% reissued
  - Security takes the weekends off
  - Live with Heartbleed for years

- Problem: low revocation rates and long expiration dates
  - Techniques for automate revocation
  - Set reasonably short certificate expiration dates

Summary

- First study focus on certificates reissues and revocations
  - Large-scale measurements
  - Developed new methodologies and heuristics

- Key findings
  - After three weeks, only 13% revoked and 27% reissued
  - Security takes the weekends off
  - Live with Heartbleed for years

- Problem: low revocation rates and long expiration dates
  - Techniques for automate revocation
  - Set reasonably short certificate expiration dates

Questions?

securepki.org