

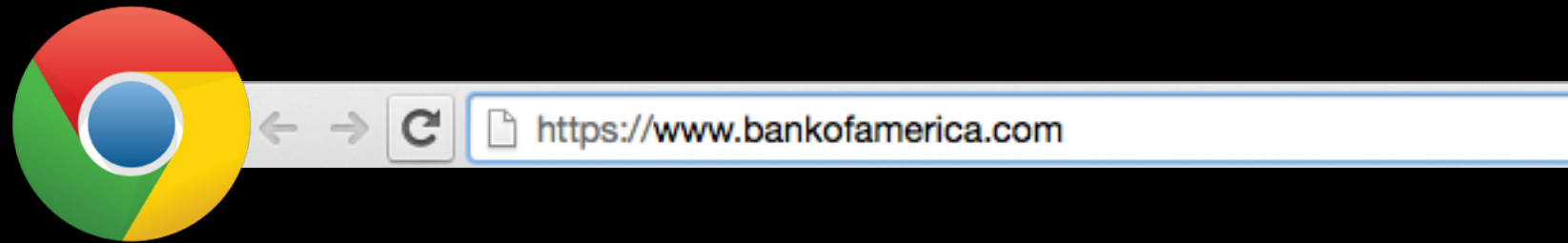
# RevCast: Fast, Private Certificate Revocation over FM radio

**Aaron Schulman**  
Stanford University

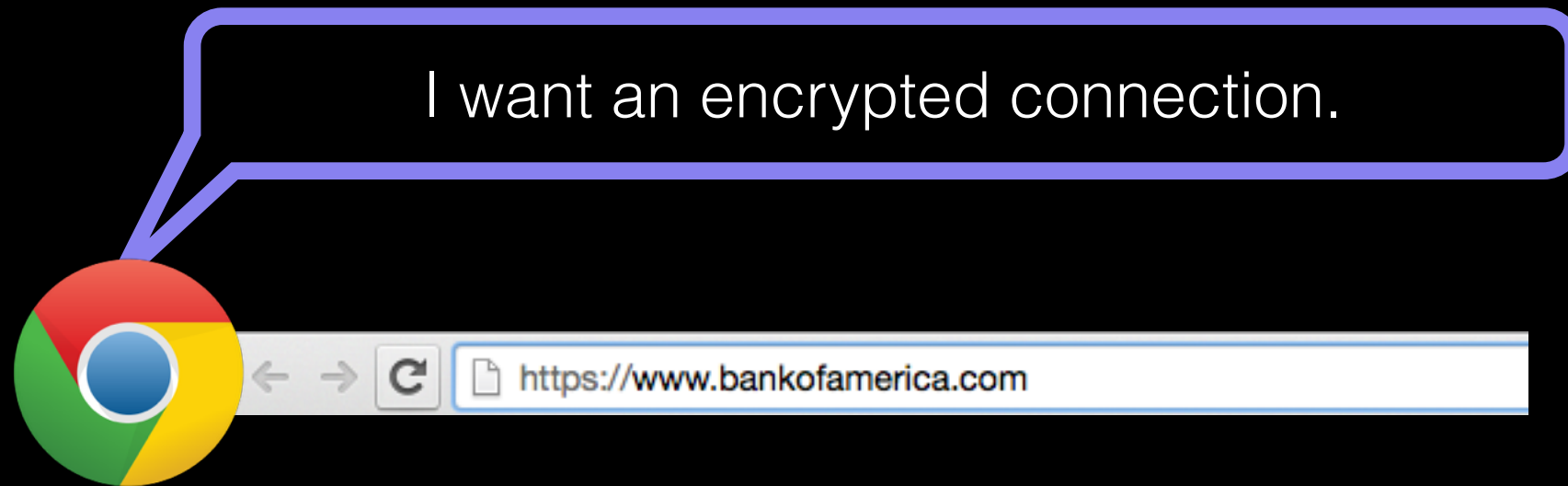
**Dave Levin**  
University of Maryland

**Neil Spring**  
University of Maryland

# Authentication in the PKI



# Authentication in the PKI



# Authentication in the PKI



# Authentication in the PKI



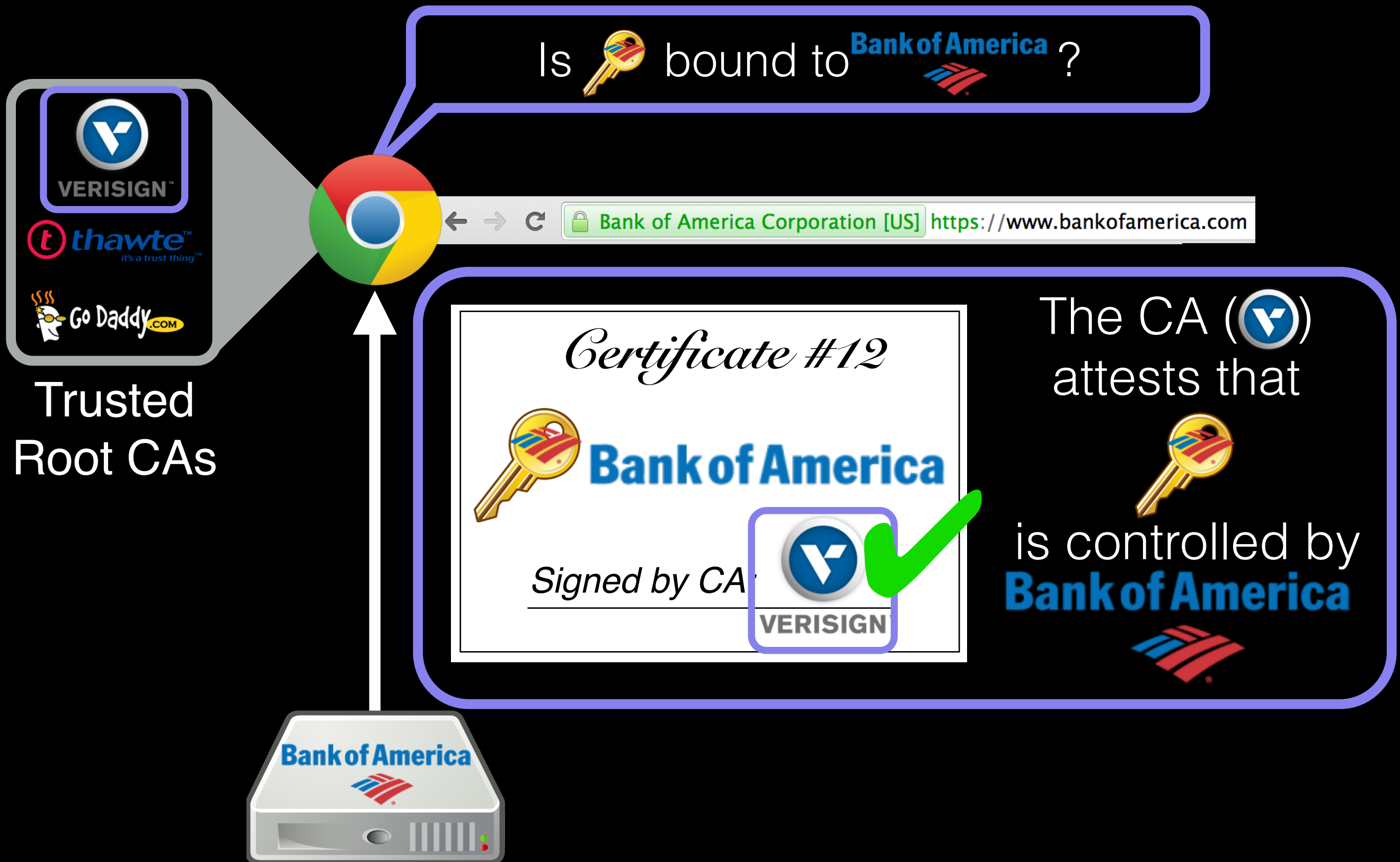
# Authentication in the PKI



# Authentication in the PKI



# Authentication in the PKI

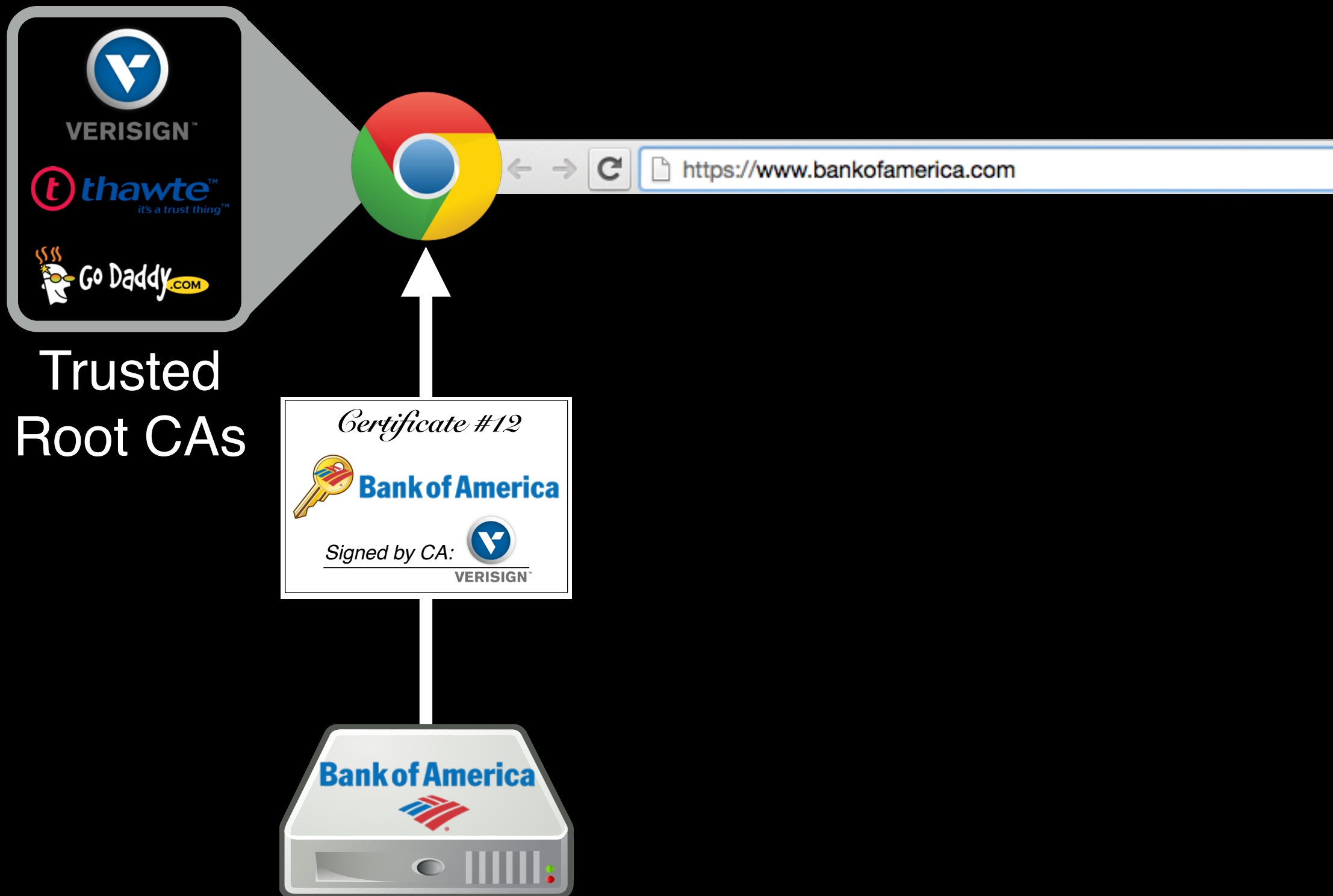




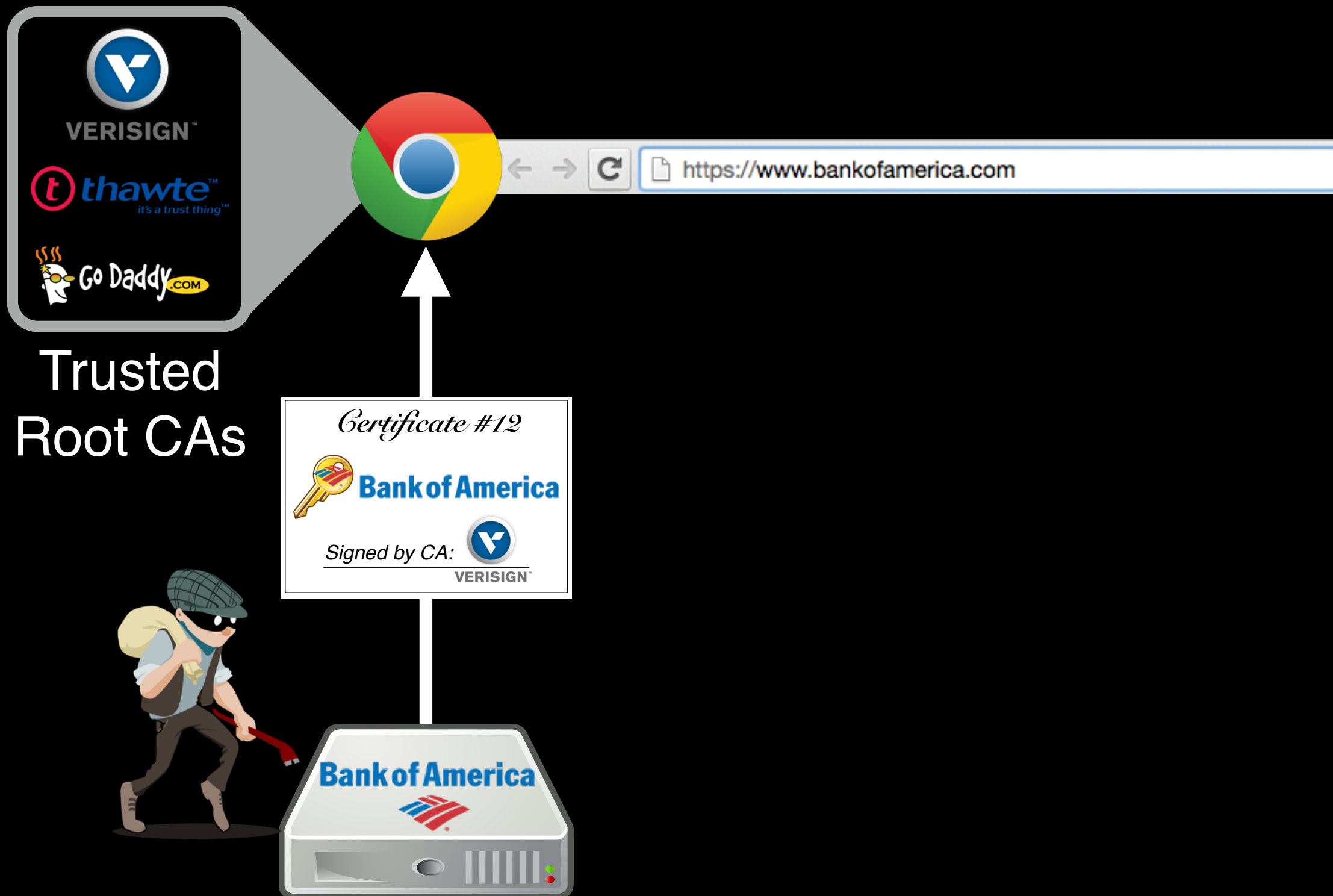
# Revocation in the PKI



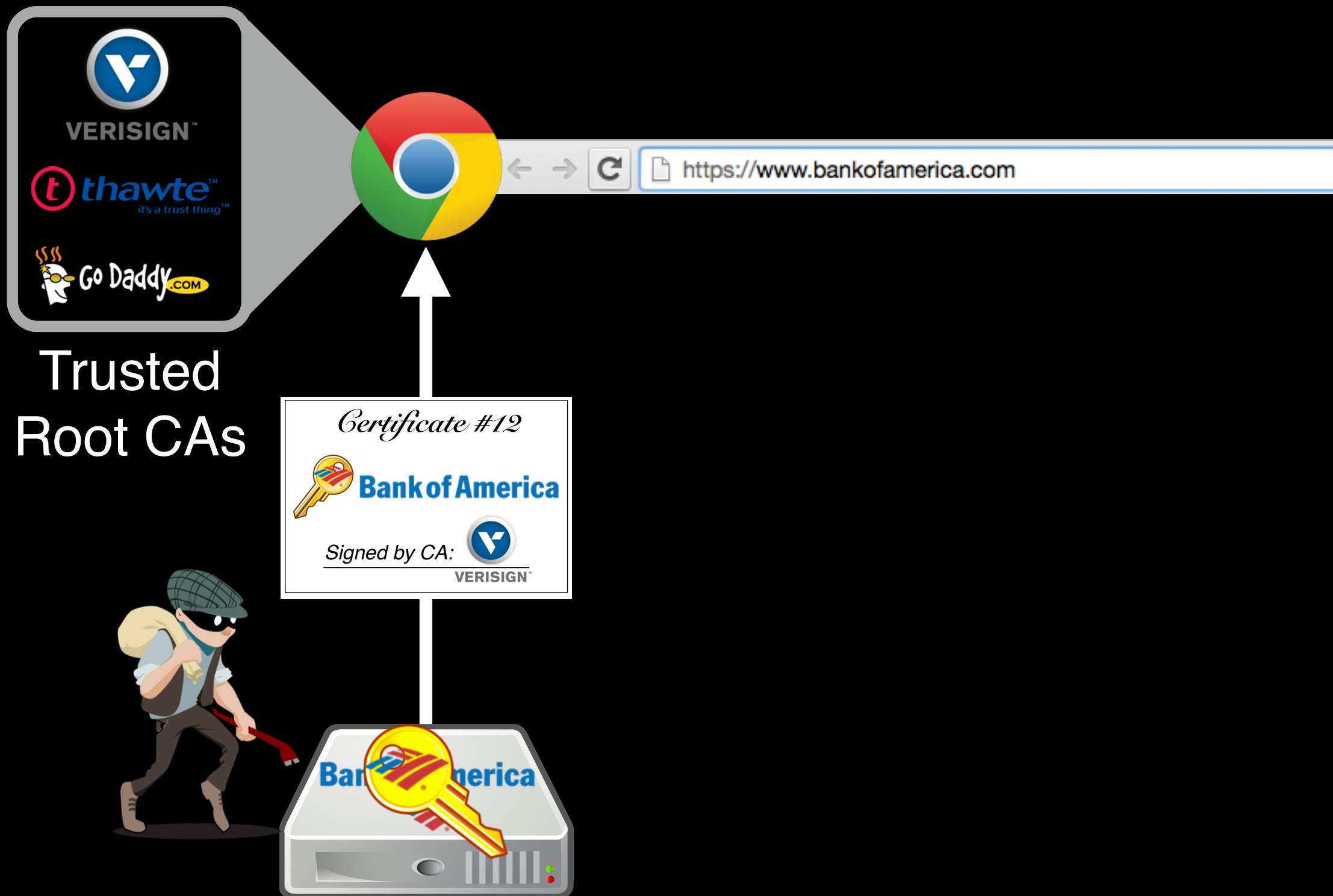
# Revocation in the PKI



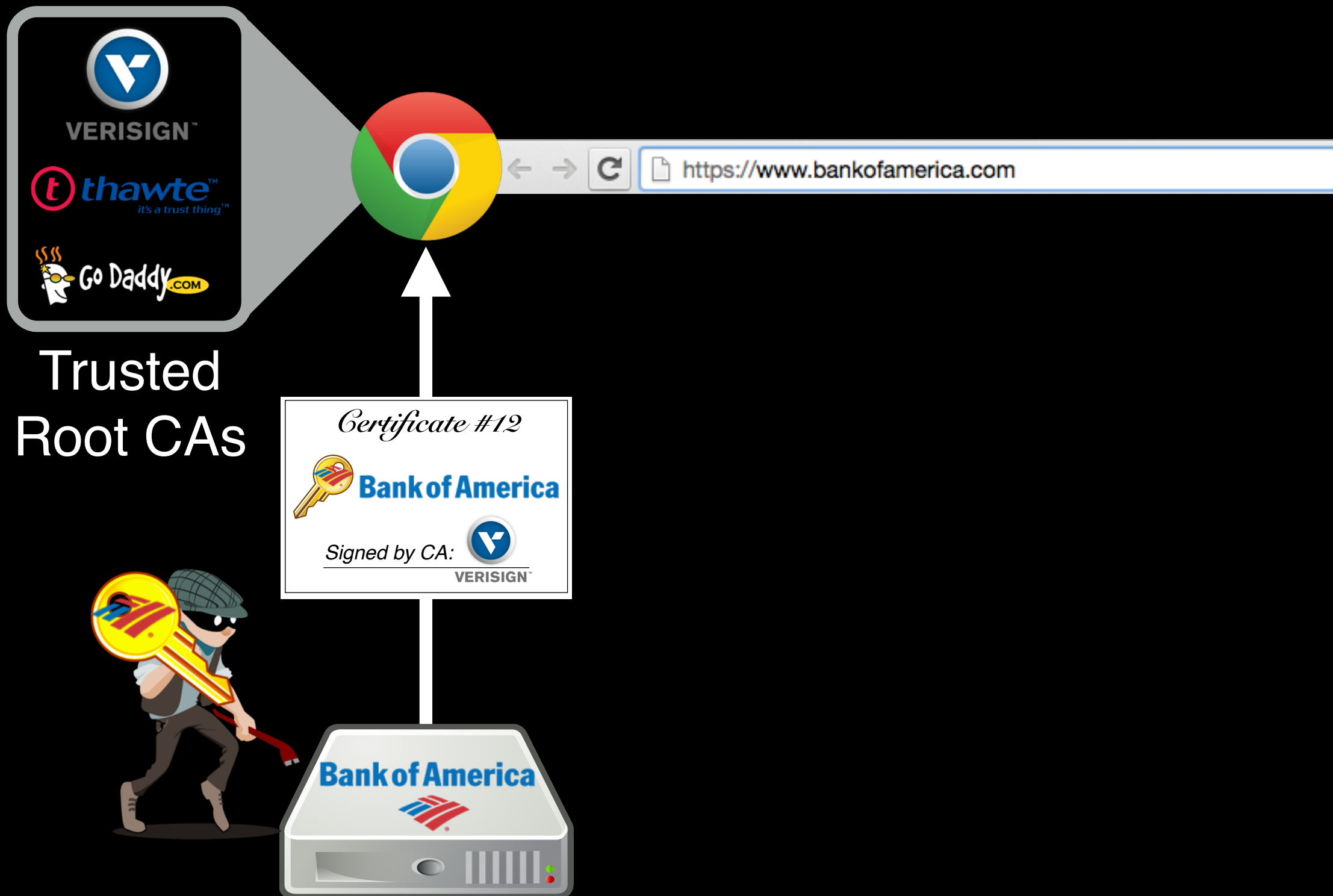
# Revocation in the PKI



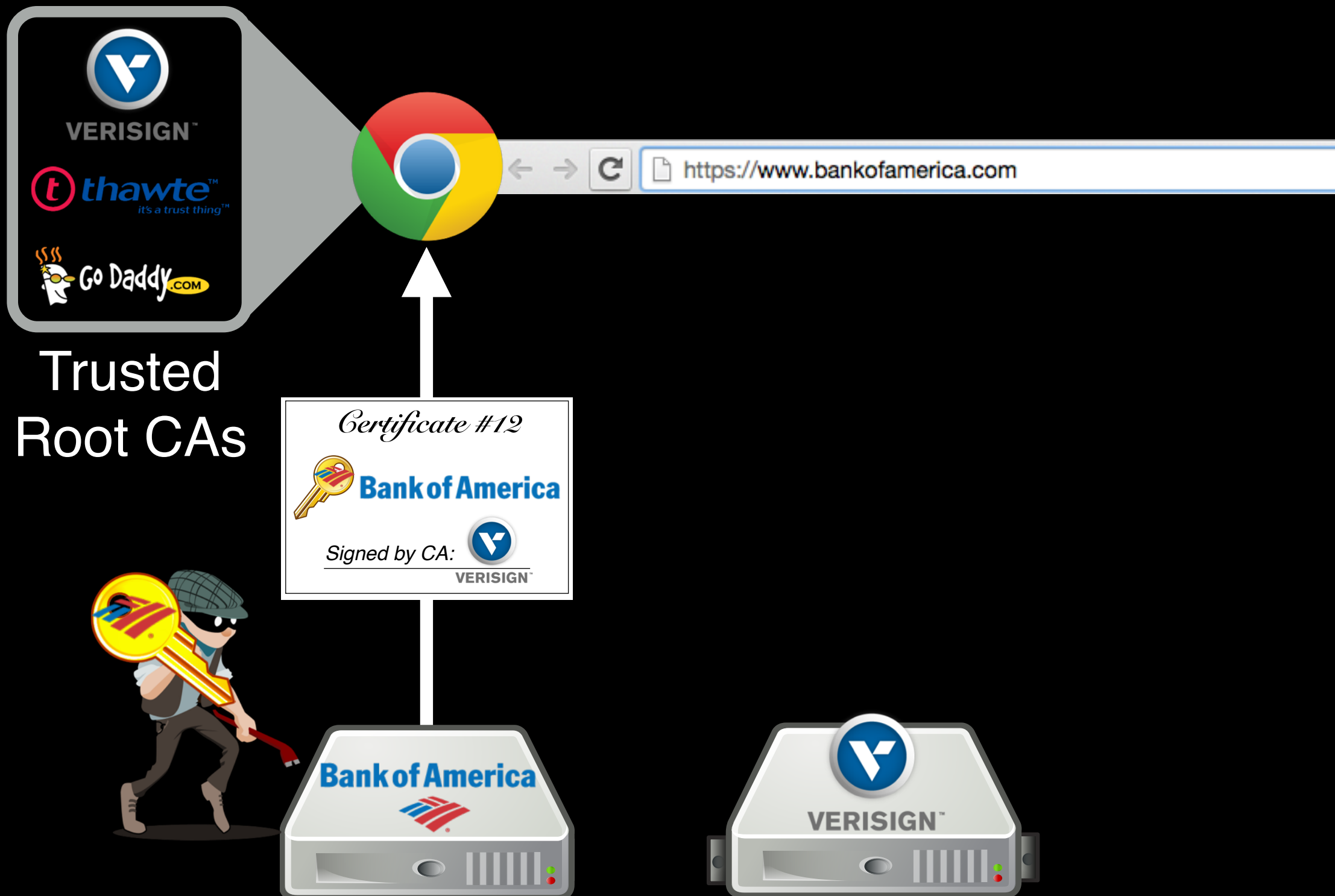
# Revocation in the PKI



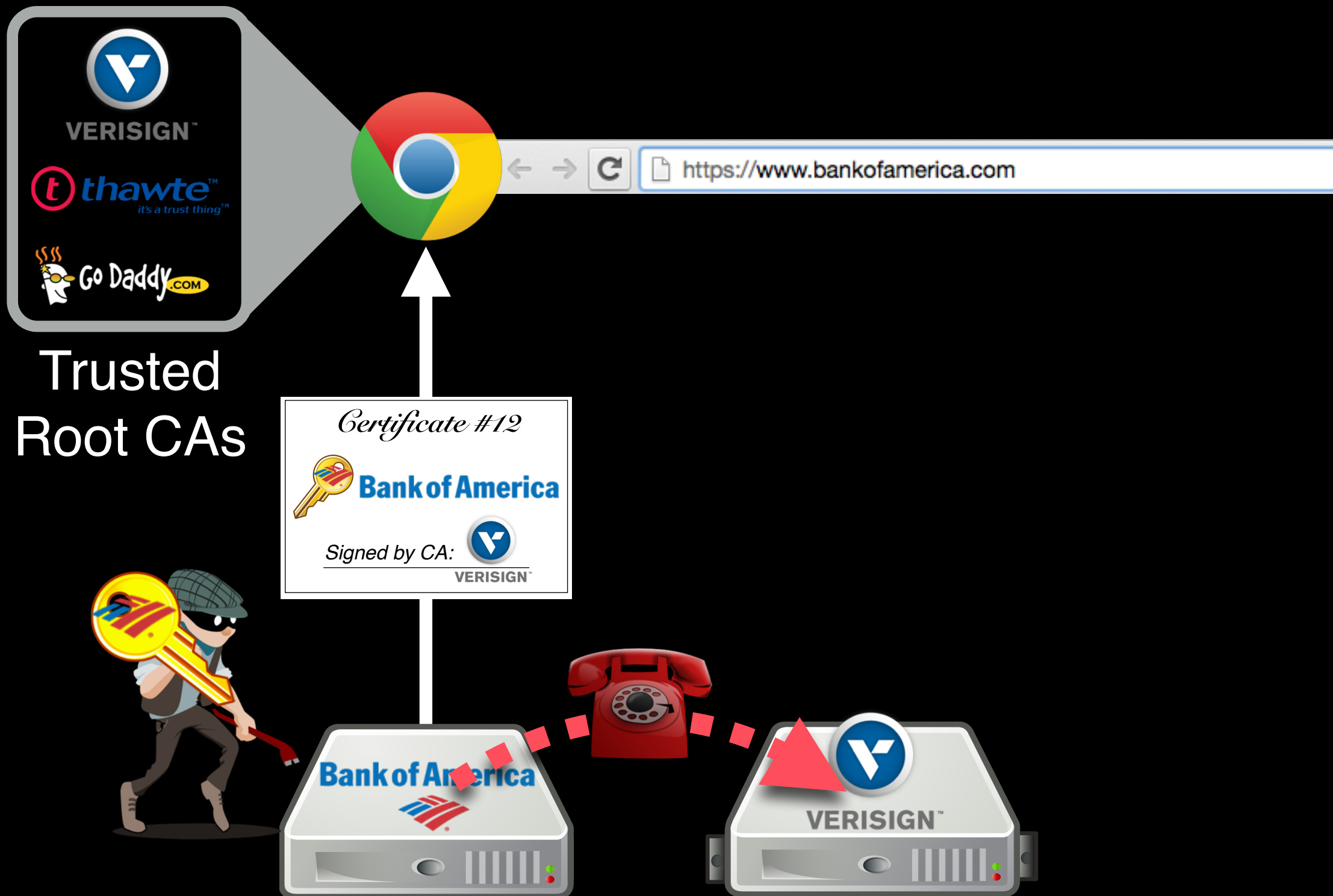
# Revocation in the PKI



# Revocation in the PKI



# Revocation in the PKI

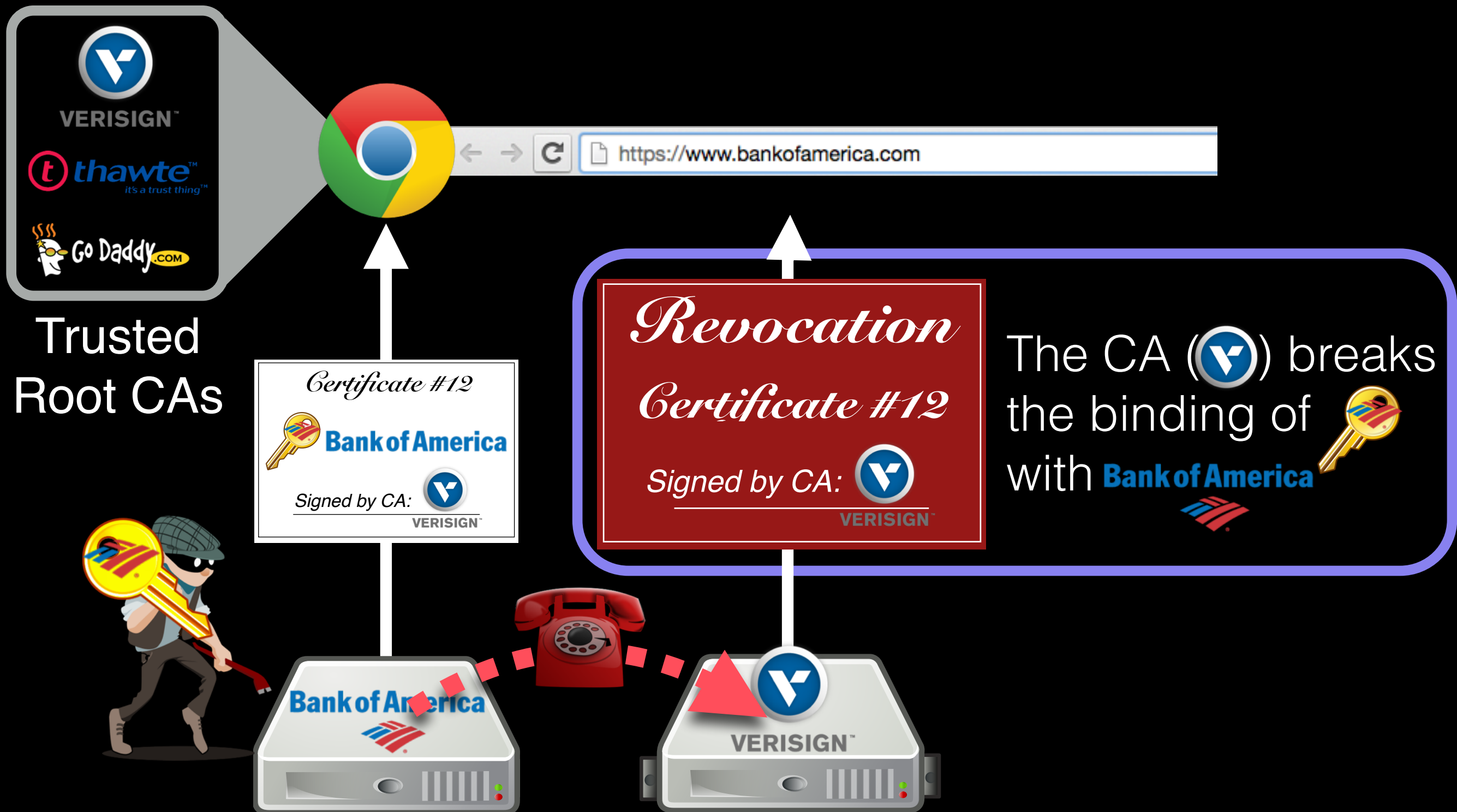


# Revocation in the PKI

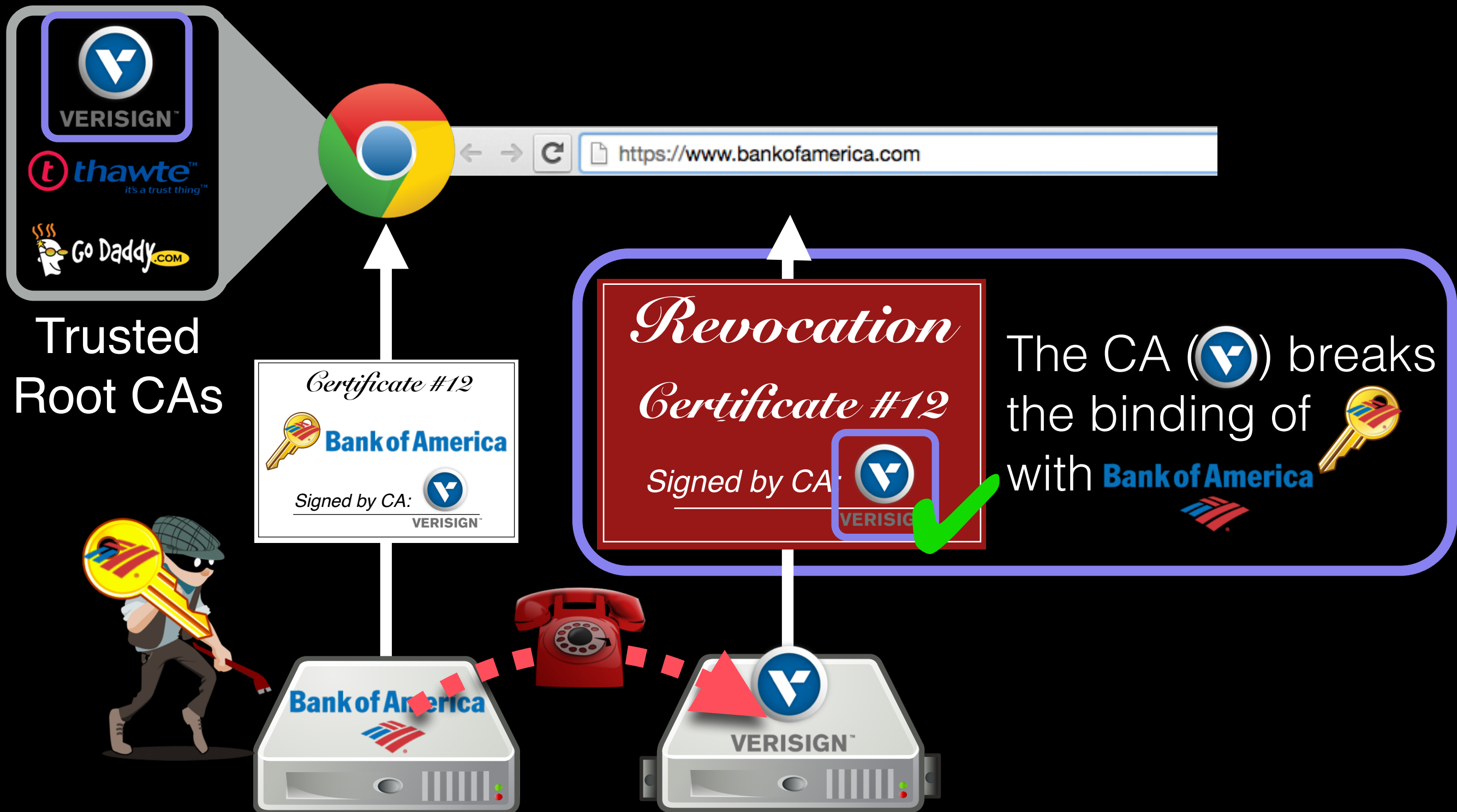




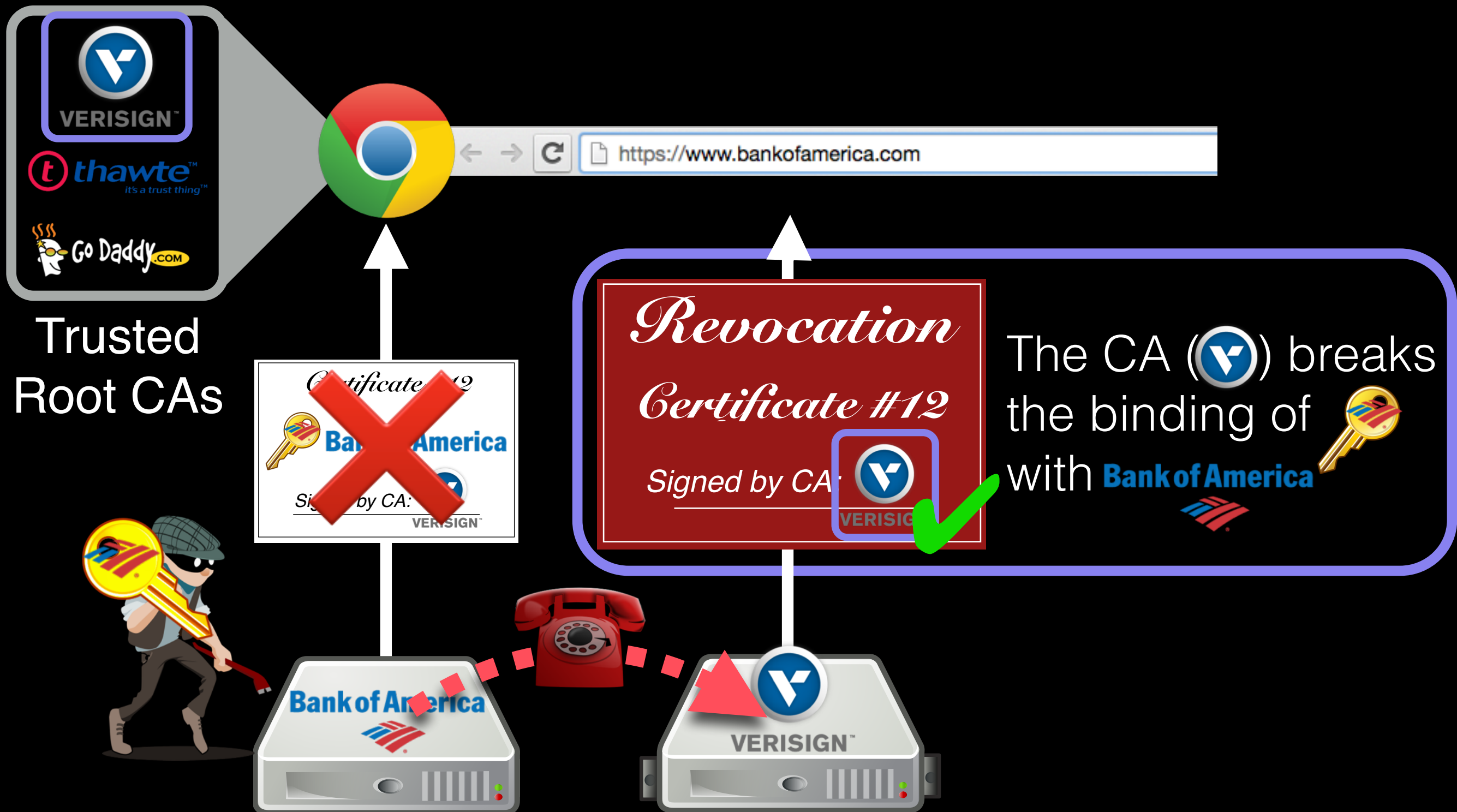
# Revocation in the PKI



# Revocation in the PKI



# Revocation in the PKI



# Revocation in the PKI



# Revocation in the PKI

One revocation every 1.1 seconds for all CAs on the Internet





# Every device needs revocations



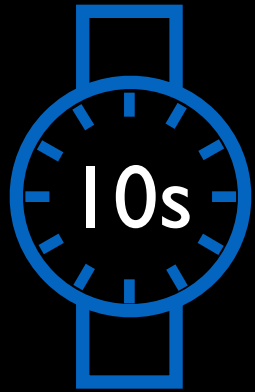
# Every device needs revocations



# Properties of revocation systems



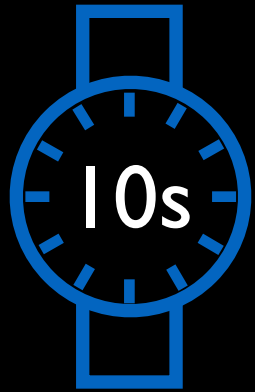
# Properties of revocation systems



## Timeliness

Clients' revocation  
state should be  
up-to-date, ideally  
within 10s of seconds

# Properties of revocation systems



## Timeliness

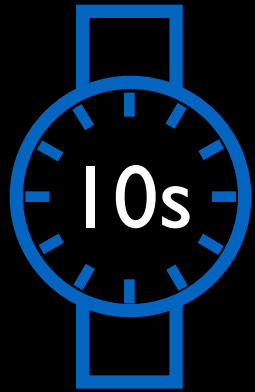
Clients' revocation state should be up-to-date, ideally within 10s of seconds



## Low-cost dissemination

The distribution mechanism must scale with CAs, certificates, and clients

# Properties of revocation systems



## Timeliness

Clients' revocation state should be up-to-date, ideally within 10s of seconds



## Low-cost dissemination

The distribution mechanism must scale with CAs, certificates, and clients

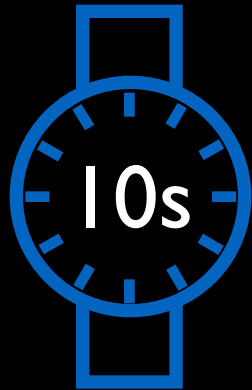


## Privacy

Users' browsing habits should not have to be revealed

# Properties of revocation systems

It is generally regarded that **no system can possibly achieve all three.**



## Timeliness

Clients' revocation state should be up-to-date, ideally within 10s of seconds



## Low-cost dissemination

The distribution mechanism must scale with CAs, certificates, and clients

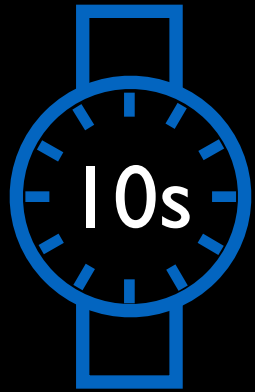


## Privacy

Users' browsing habits should not have to be revealed

# Properties of revocation systems

It is generally regarded that **no system can possibly achieve all three.**



Timeliness



Low-cost dissemination



Privacy



# RevCast

# Existing revocation systems

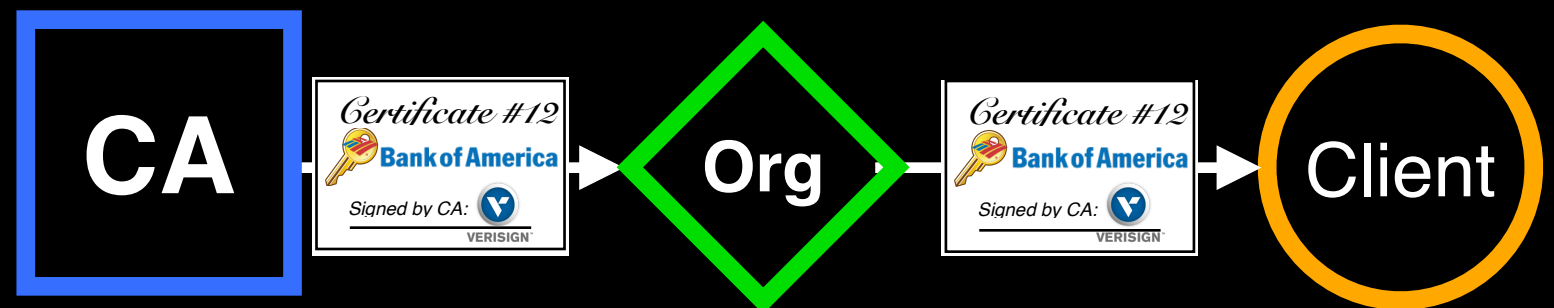
Certificate  
Revocation Lists  
(CRL)



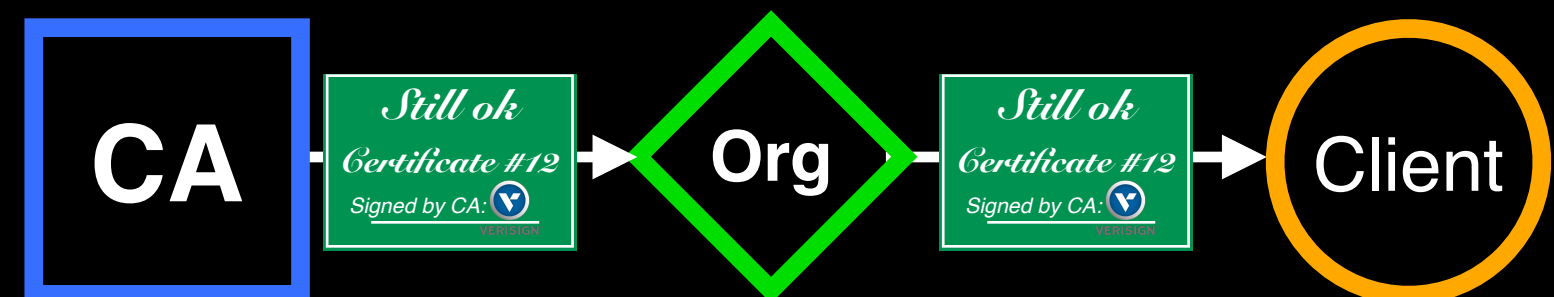
Online Certificate  
Status Protocol  
(OCSP)

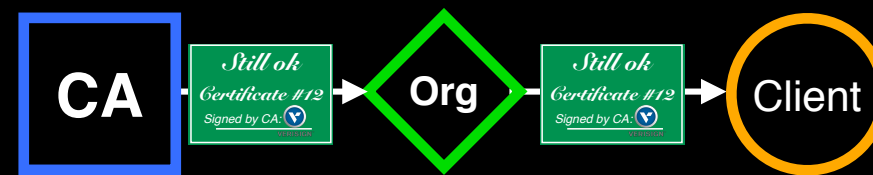
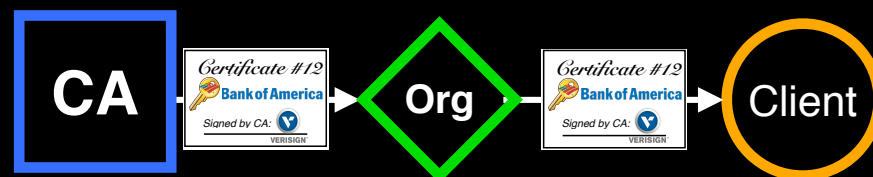


Short lived certs






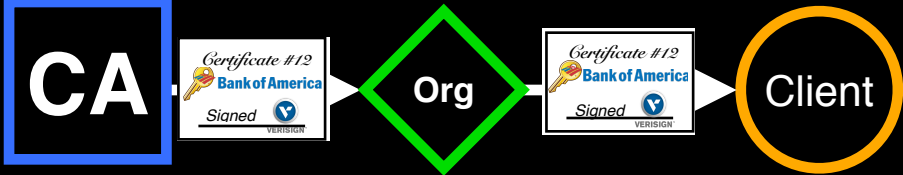
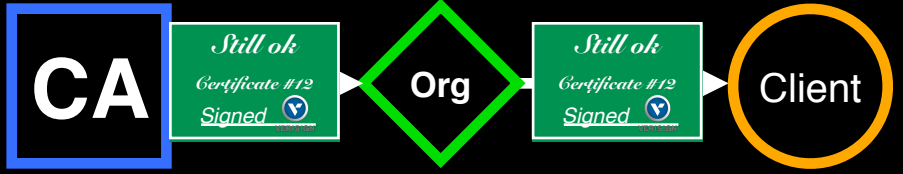


OCSP Stapling








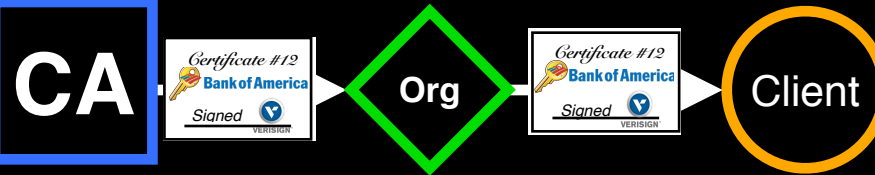
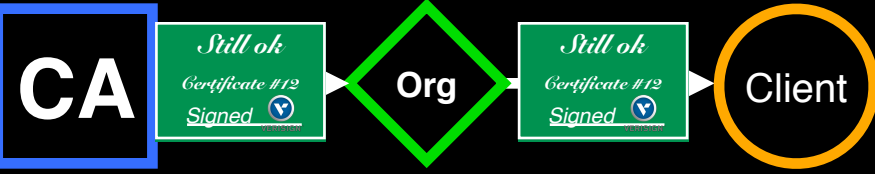


# Existing revocation systems

		 <b>Timeliness</b>	 <b>Low-cost dissemination</b>	 <b>Privacy</b>
CRLs		✗	✗	✓
OCSP		✓	✗	✗
Short lived		✓*	✗	✓
Stapling		✓	✗	✓



# Existing revocation systems

		 Timeliness	 Low-cost dissemination	 Privacy
CRLs		✗	✗	✓
OCSP		✓	✗	✗
Short lived		✓*	✗	✓
Stapling		✓	✗	✓

All of these protocols rely on unicast transmission of revocations

# Unicast is not well suited for distributing revocations

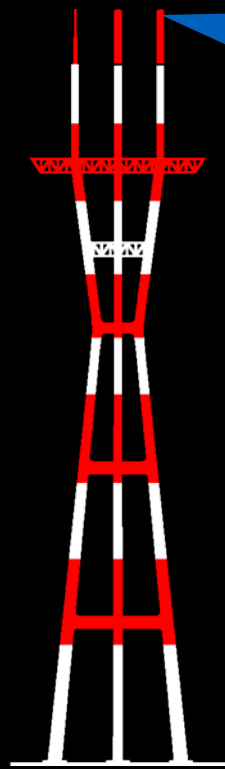
Doesn't **scale** to distributing to every device on the Internet

Failures are **benign** indication of connectivity issues (soft-fail)

*Multicast revocation is also flawed (Sybils, MITM, DoS)*

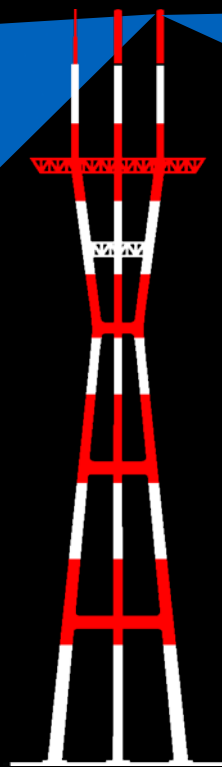
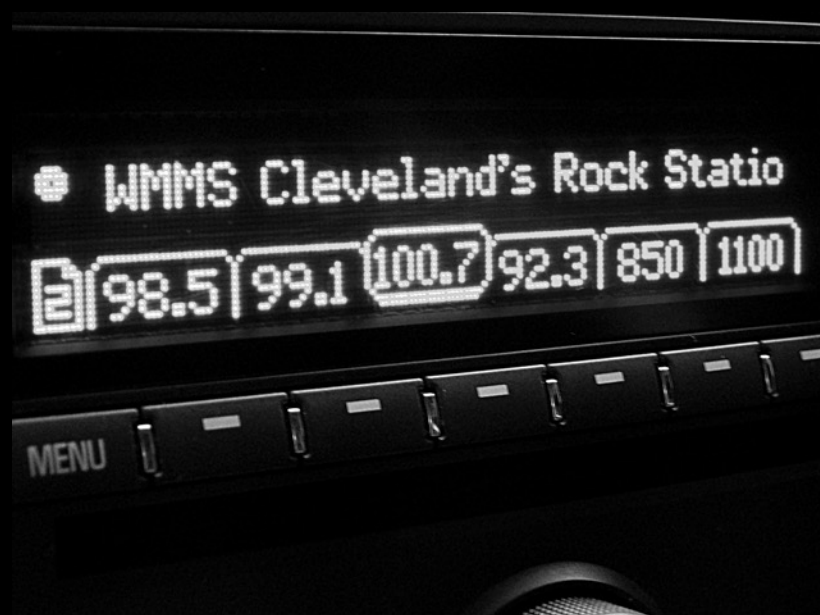
# RevCast

We propose broadcasting  
revocations over FM RDS



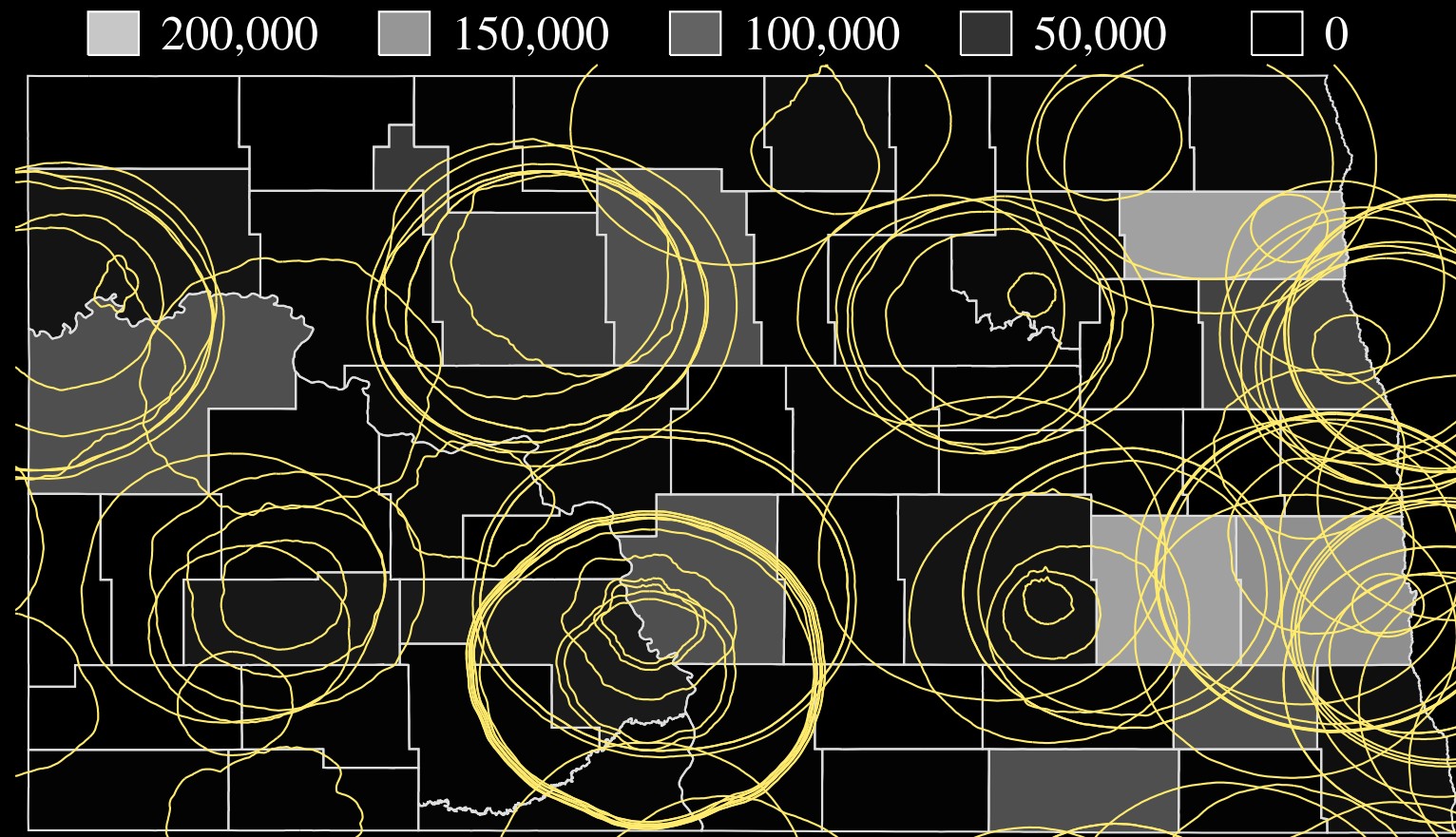
# RevCast

We propose broadcasting  
revocations over FM RDS





# FM RDS coverage is ideal for disseminating revocations



- Transmitters are where people are
- Up to 10 million people per tower

# Properties of revocation systems



## Low-cost dissemination

One transmission  
covers up to 10 million  
& Under-monotized



## Privacy

Radio broadcasts  
are inherently  
receiver anonymous

# Properties of revocation systems



## Low-cost dissemination

One transmission  
covers up to 10 million  
& Under-monotized



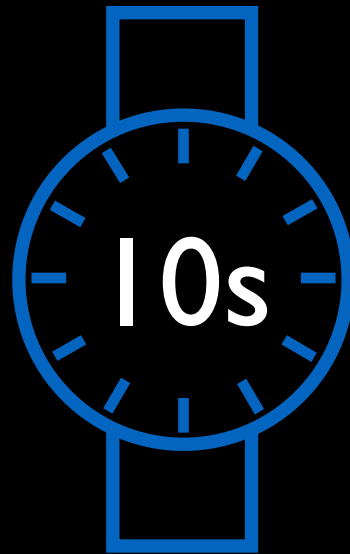
## Privacy

Radio broadcasts  
are inherently  
receiver anonymous

**Solved.** Let's go party like it's 1989!







## Timeliness?

One tiny problem. RDS has an effective bitrate of **421.8 bps**.

# Rest of the talk

RevCast protocol - fitting revocations in 421.8 bps

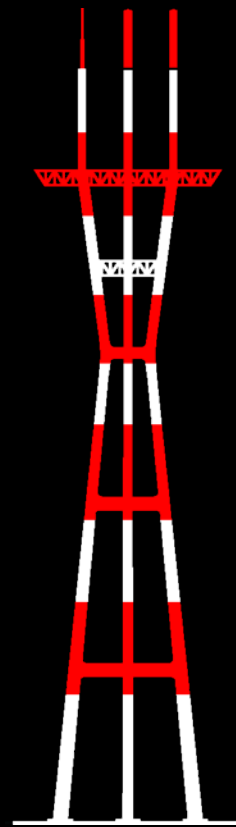
Evaluate RevCast with 2 months of revocations

# Revoking over FM RDS

## CAs



## Radio station



## Receivers

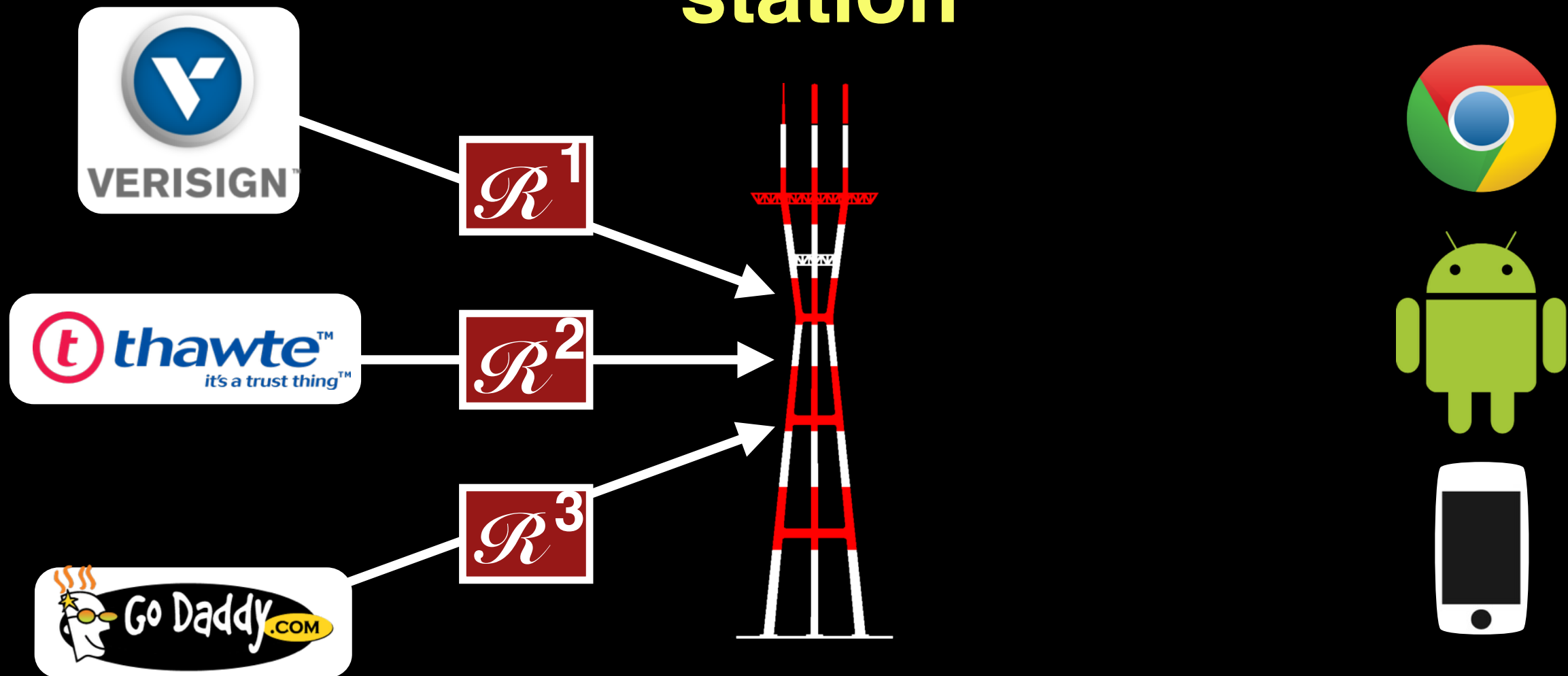


# Revoking over FM RDS

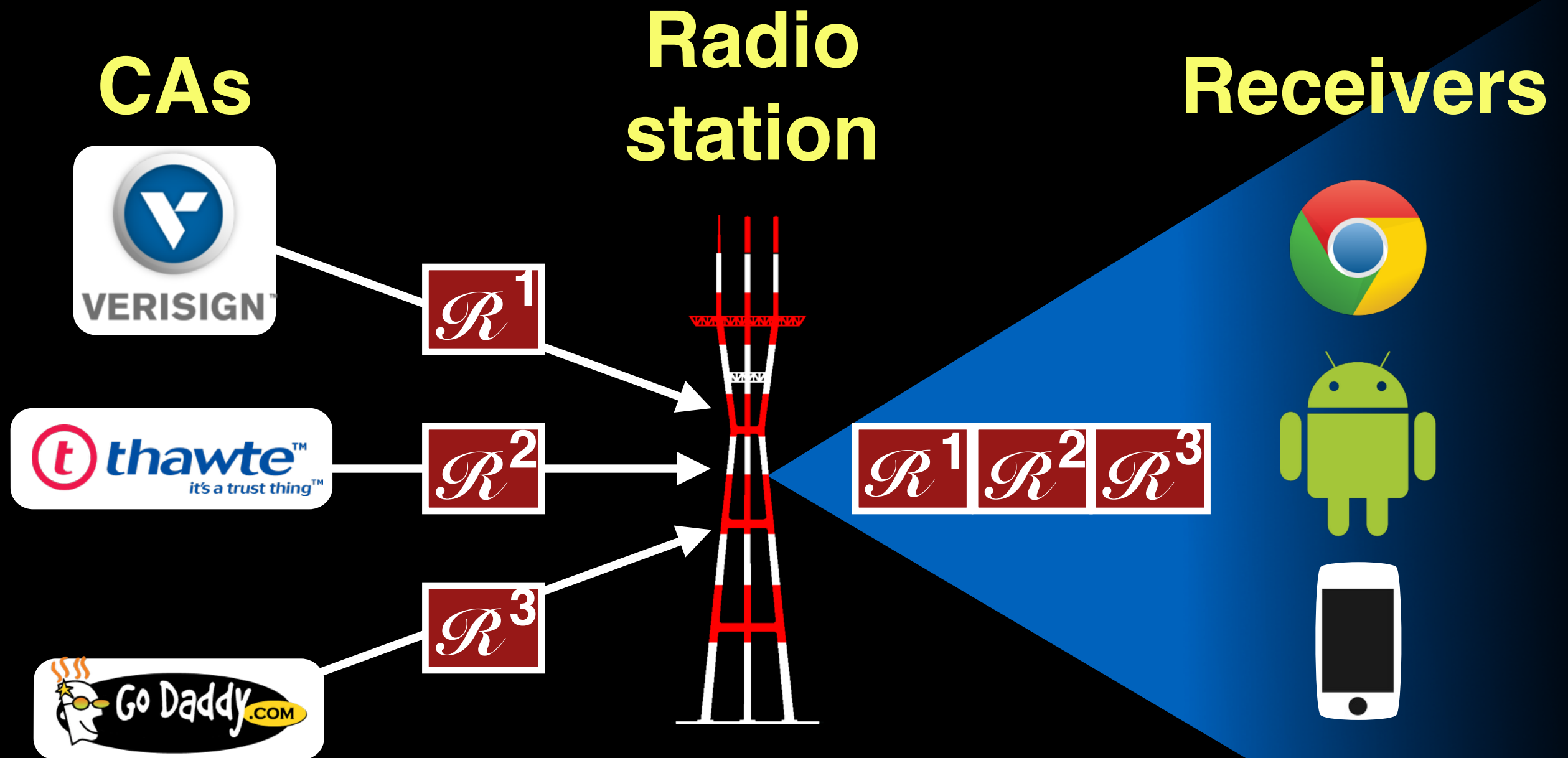
**CAs**

**Radio  
station**

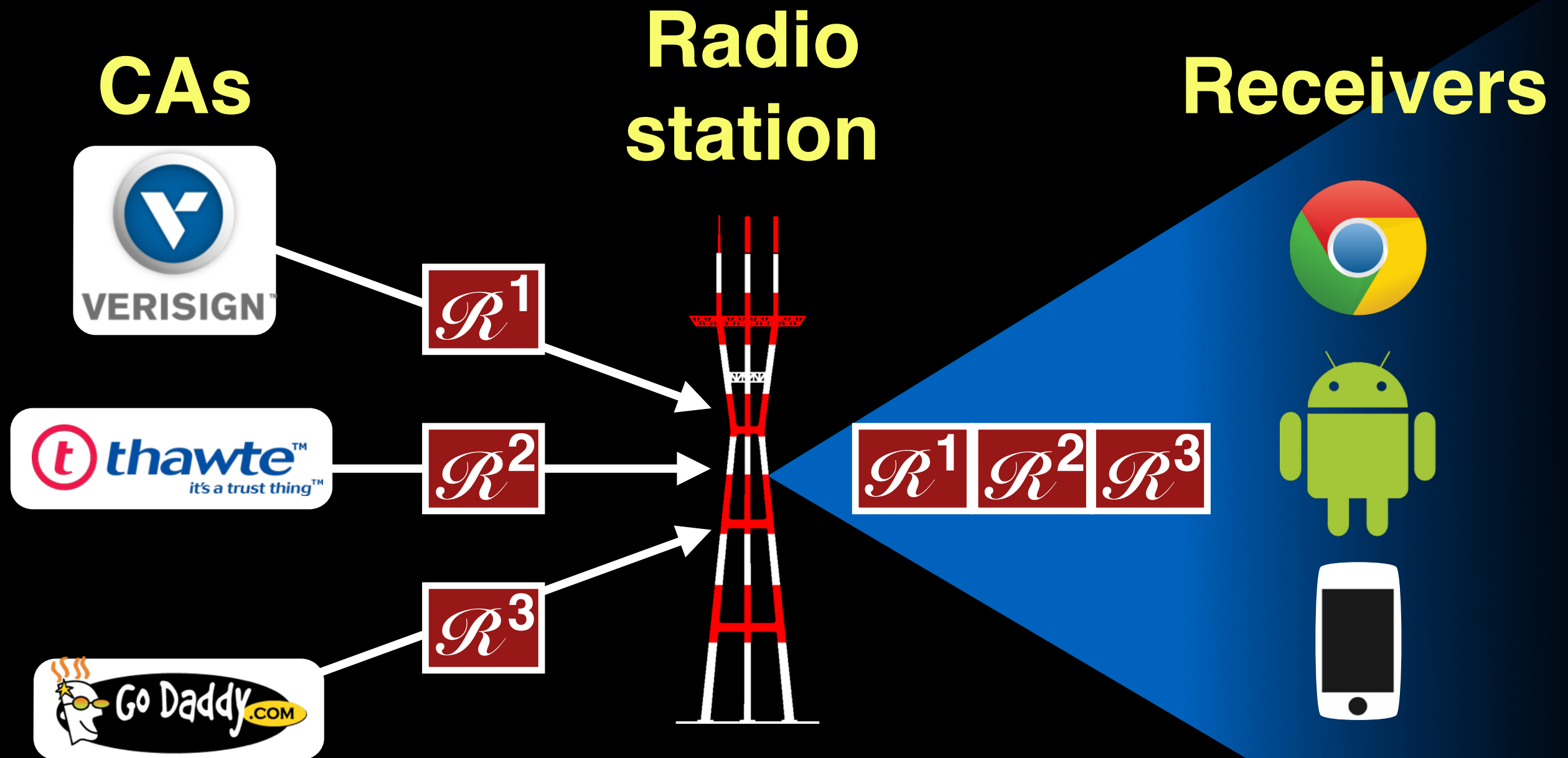
**Receivers**



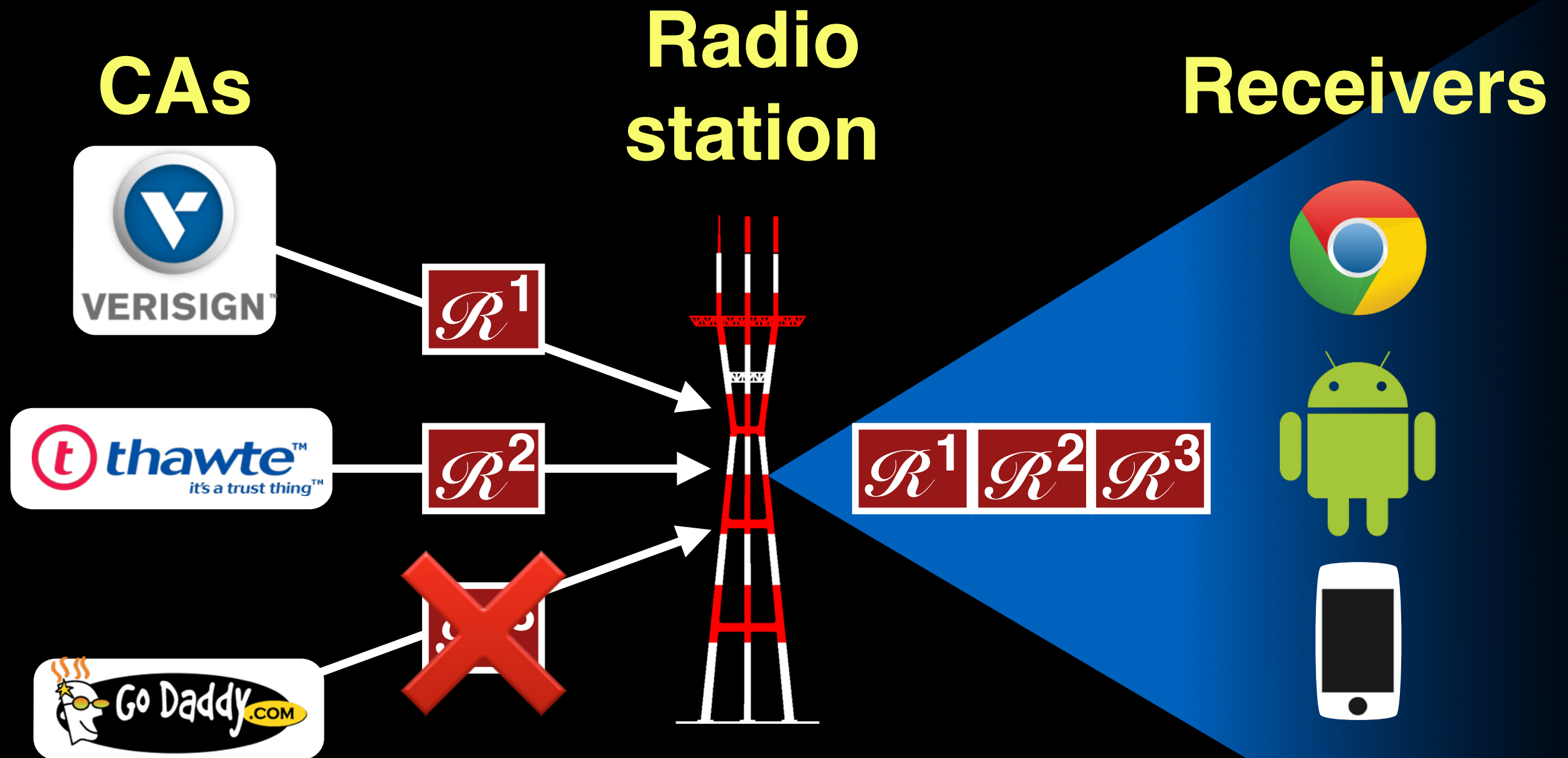
# Revoking over FM RDS



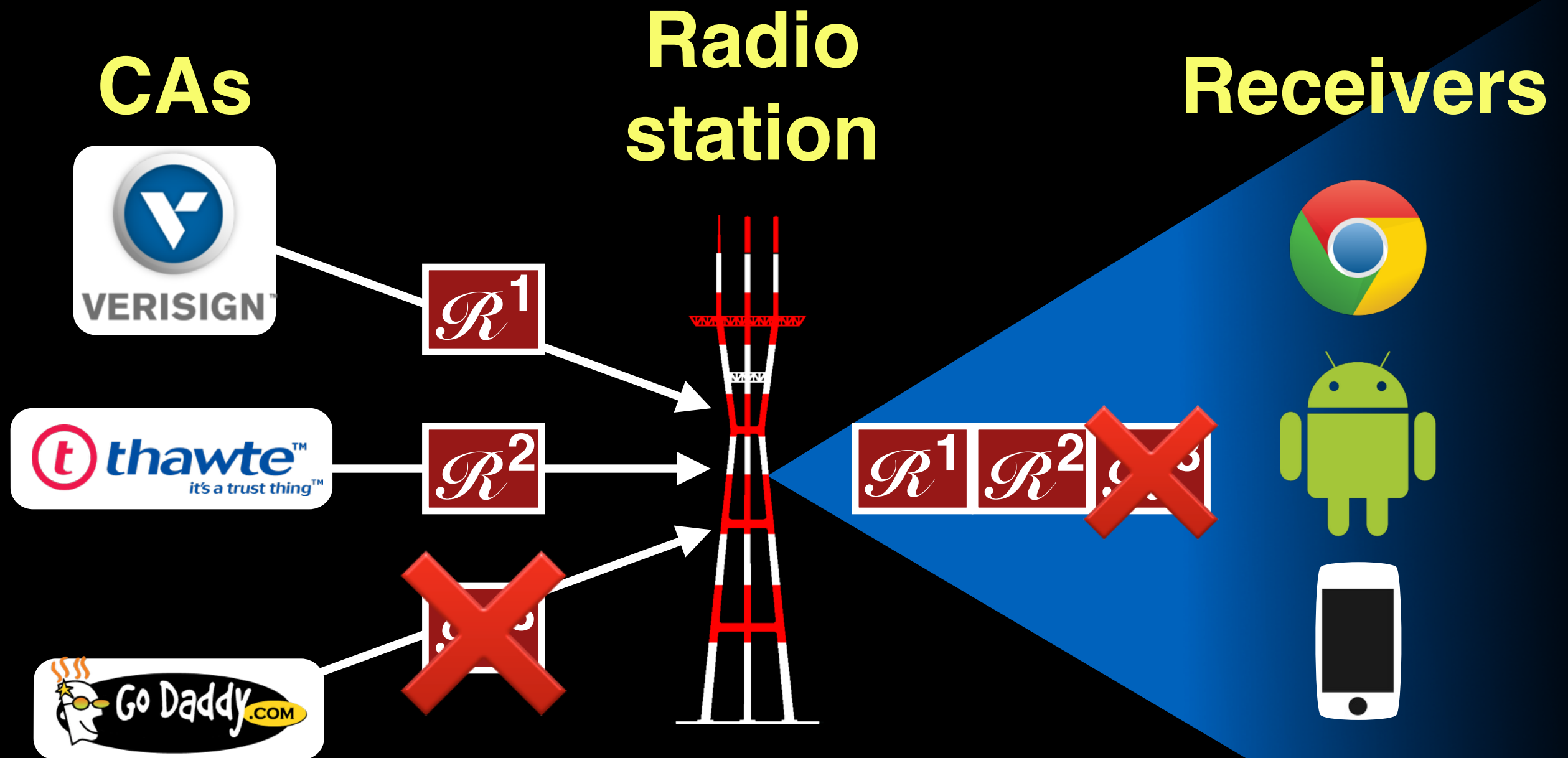
# Losses can go undetected



# Losses can go undetected

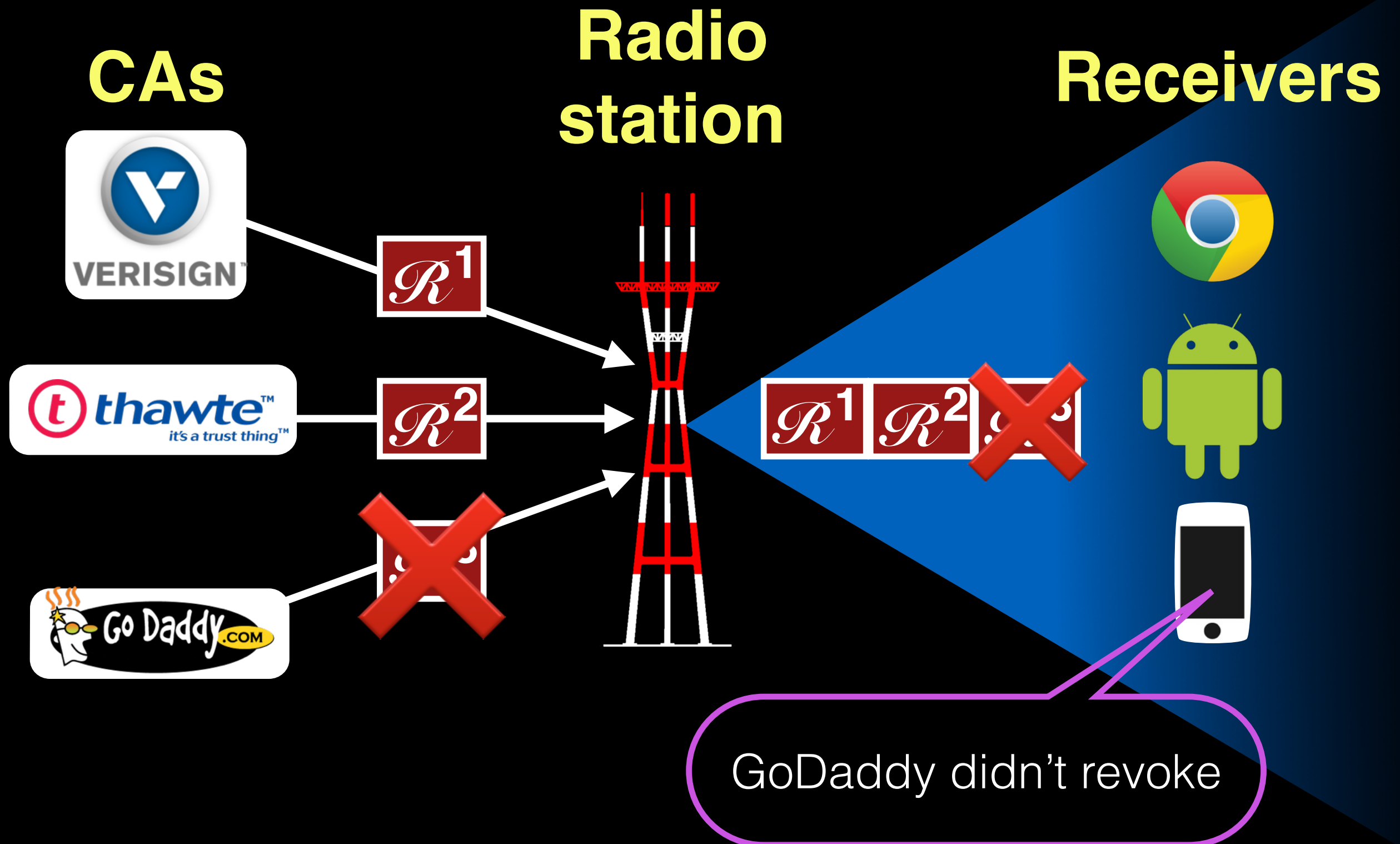


# Losses can go undetected

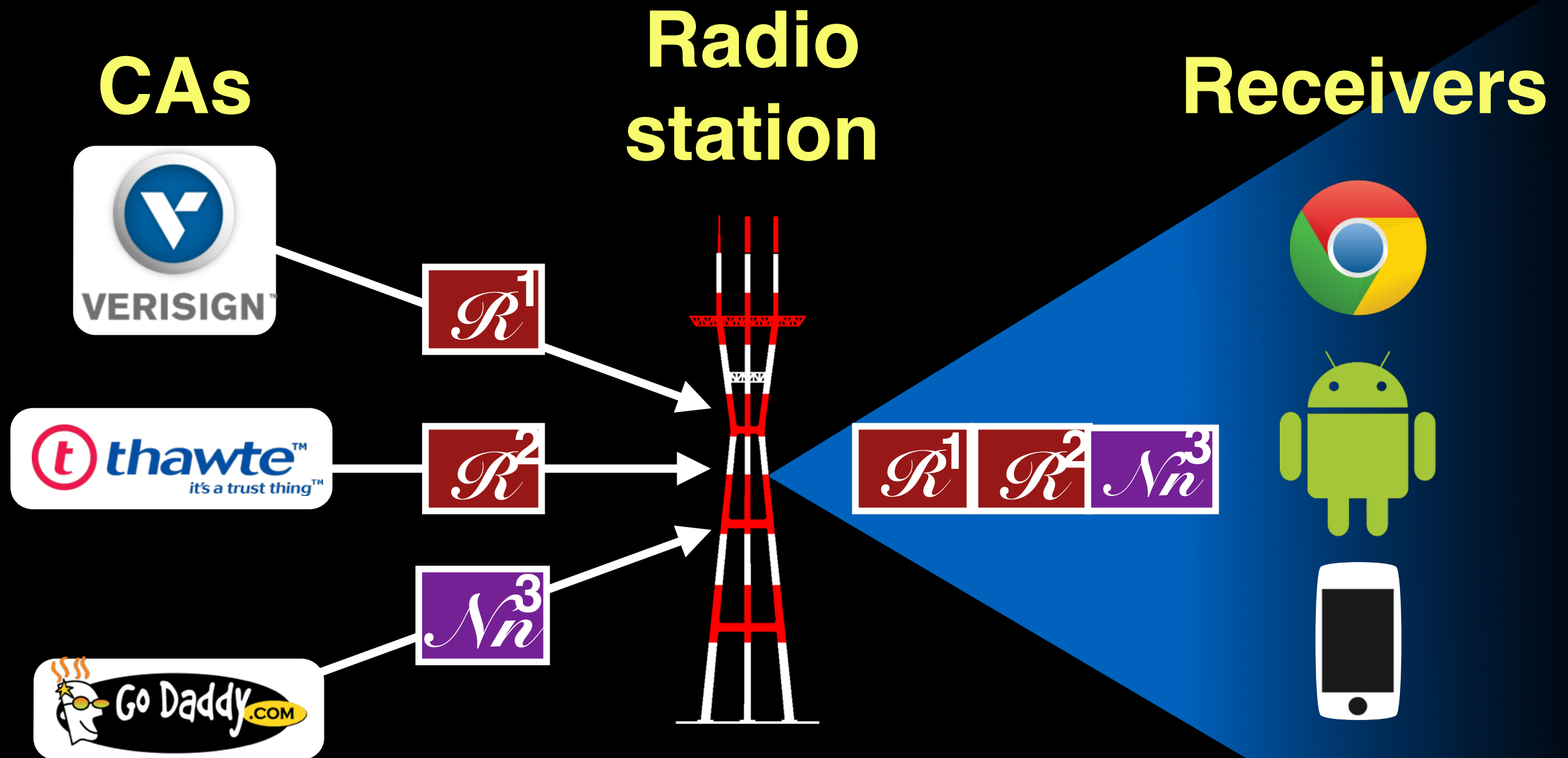




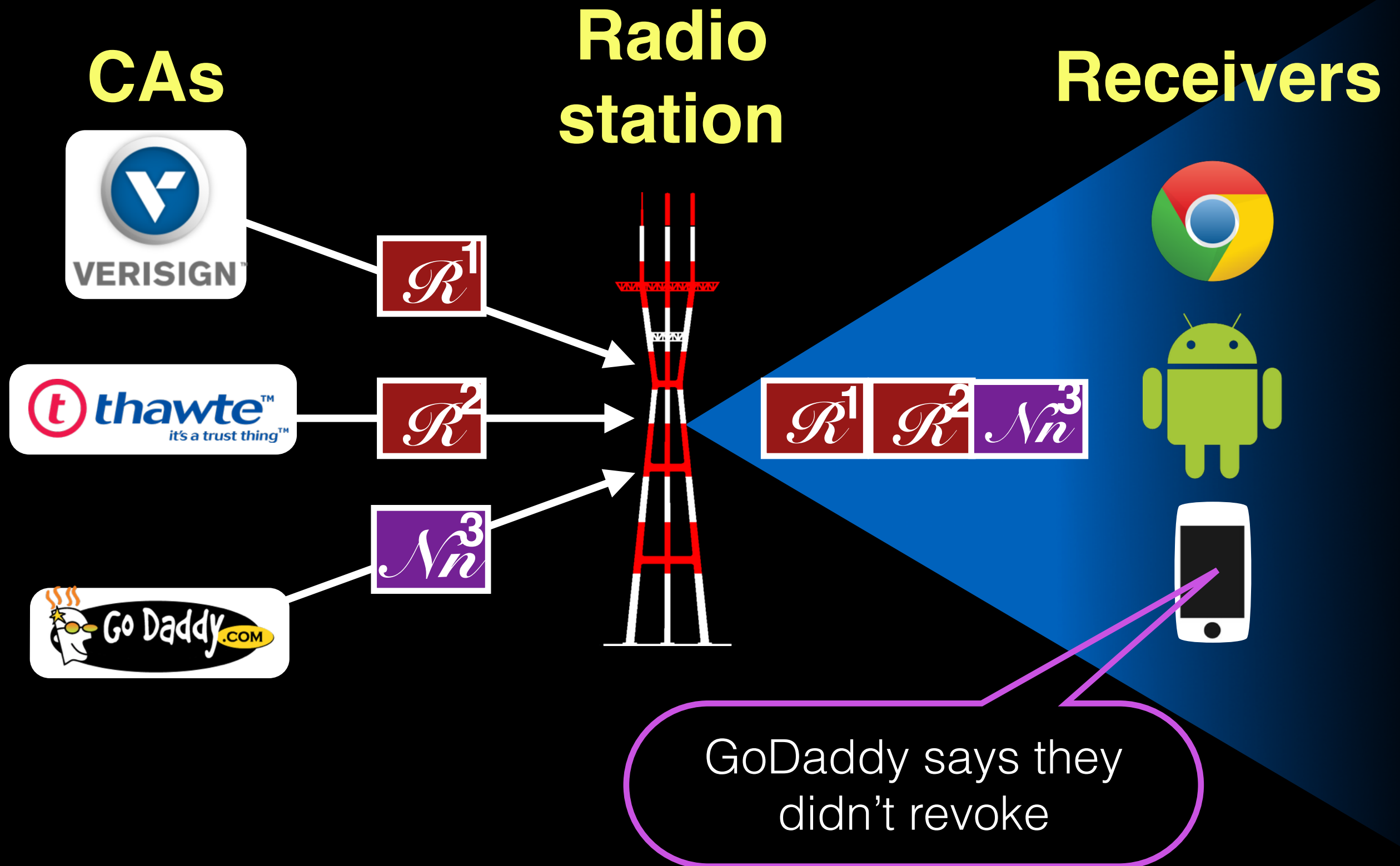
# Losses can go undetected



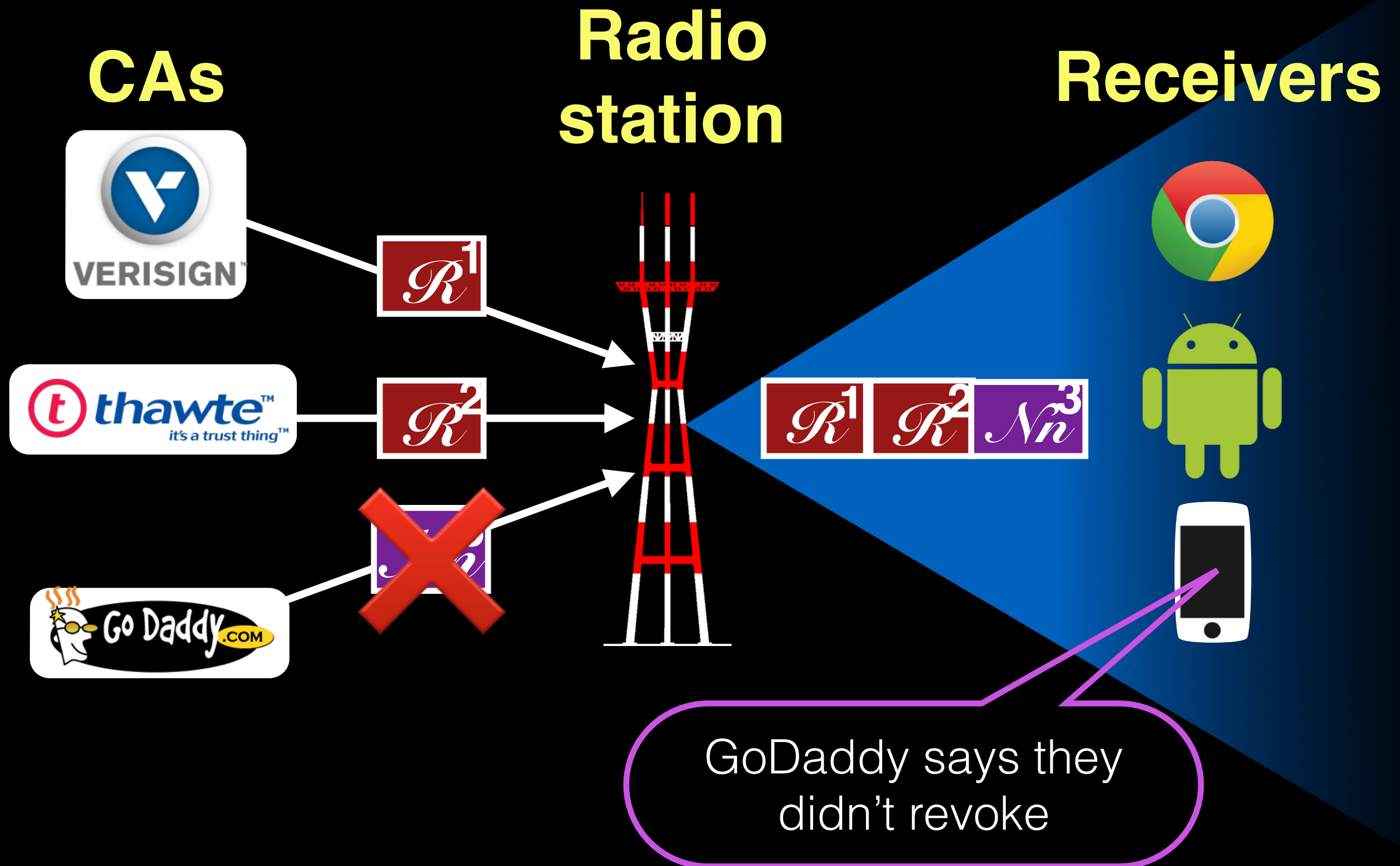
# Making losses detectible with “nothing now”



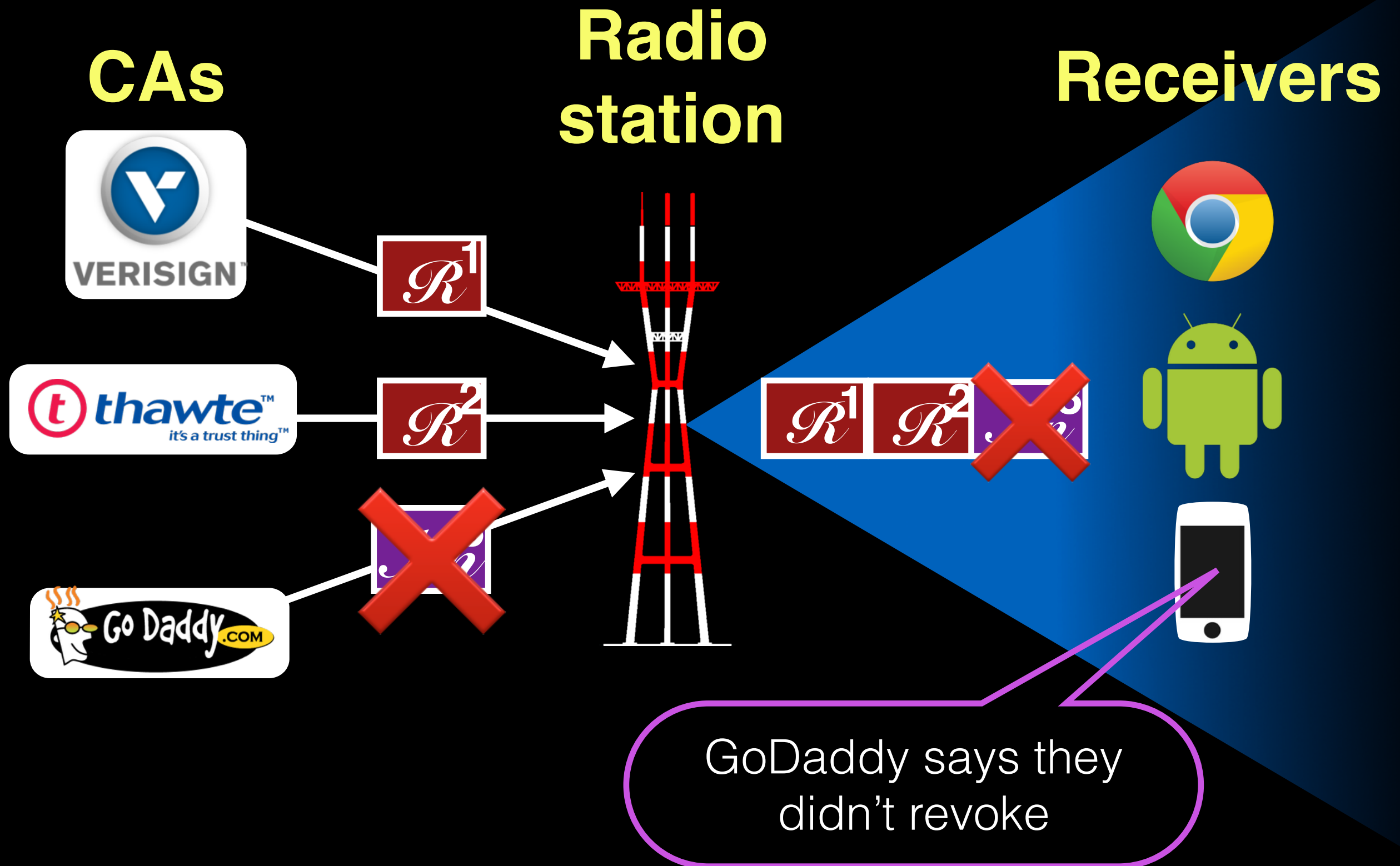
# Making losses detectible with “nothing now”



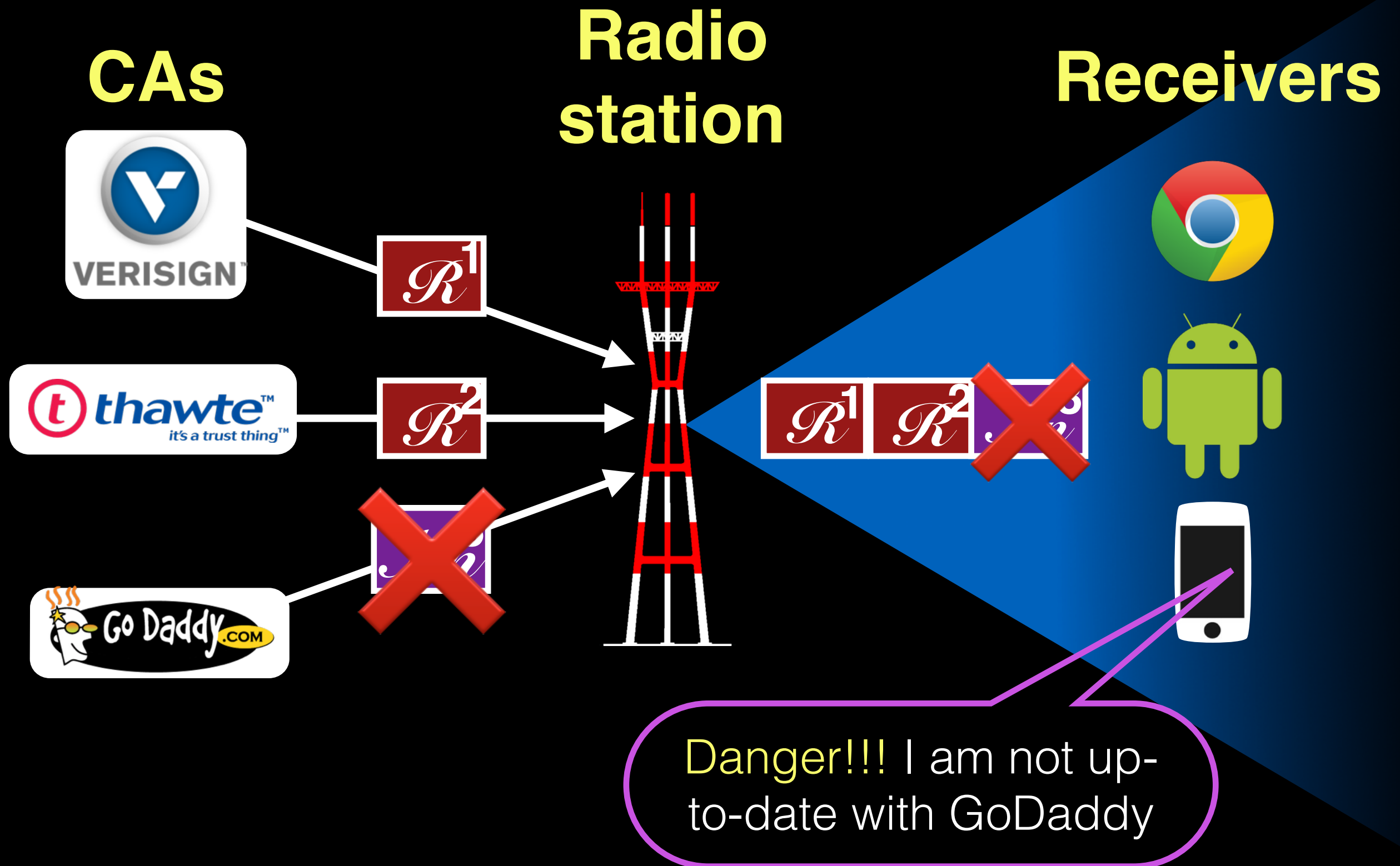
# Making losses detectible with “nothing now”



# Making losses detectible with “nothing now”

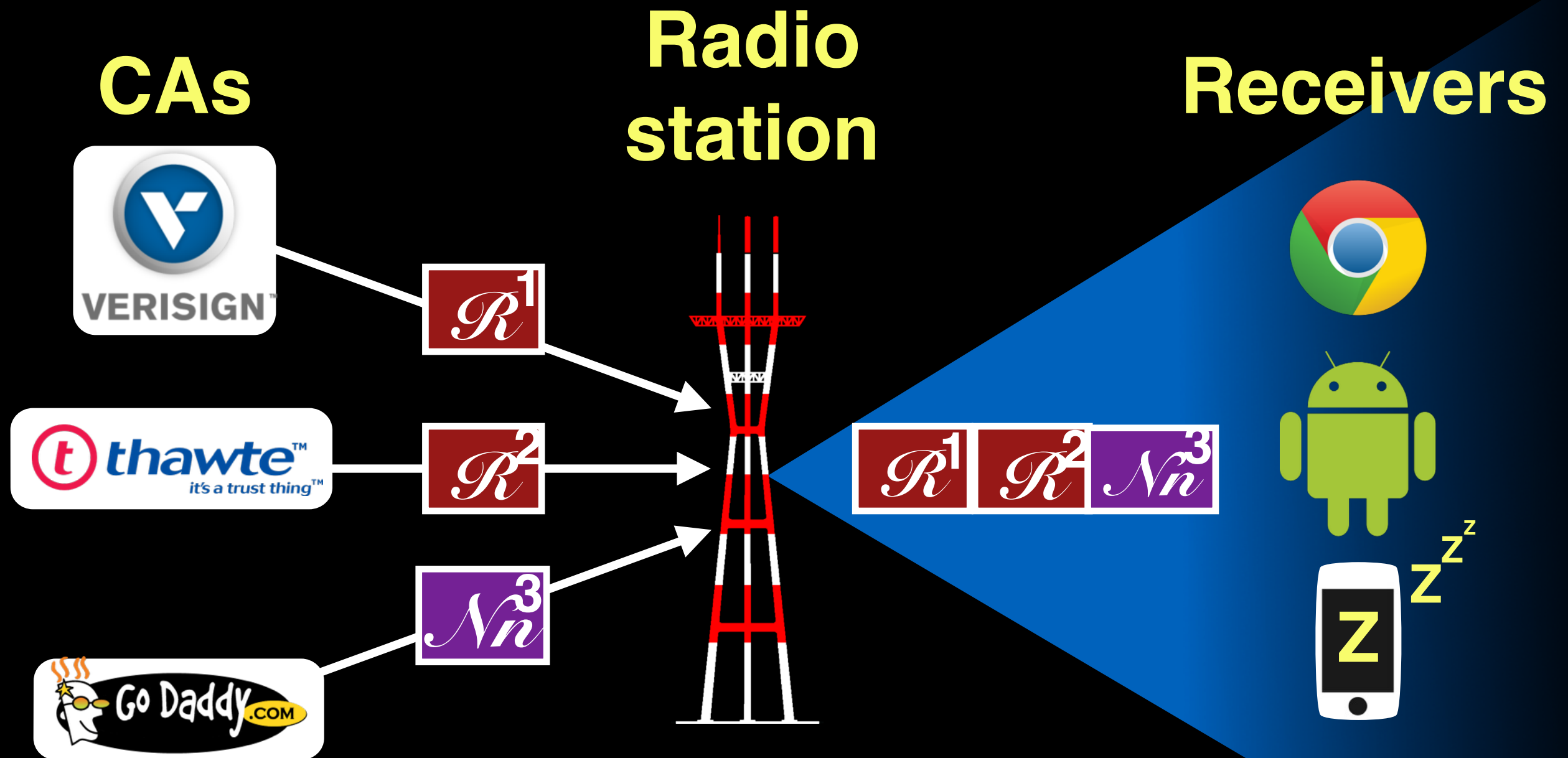


# Making losses detectible with “nothing now”

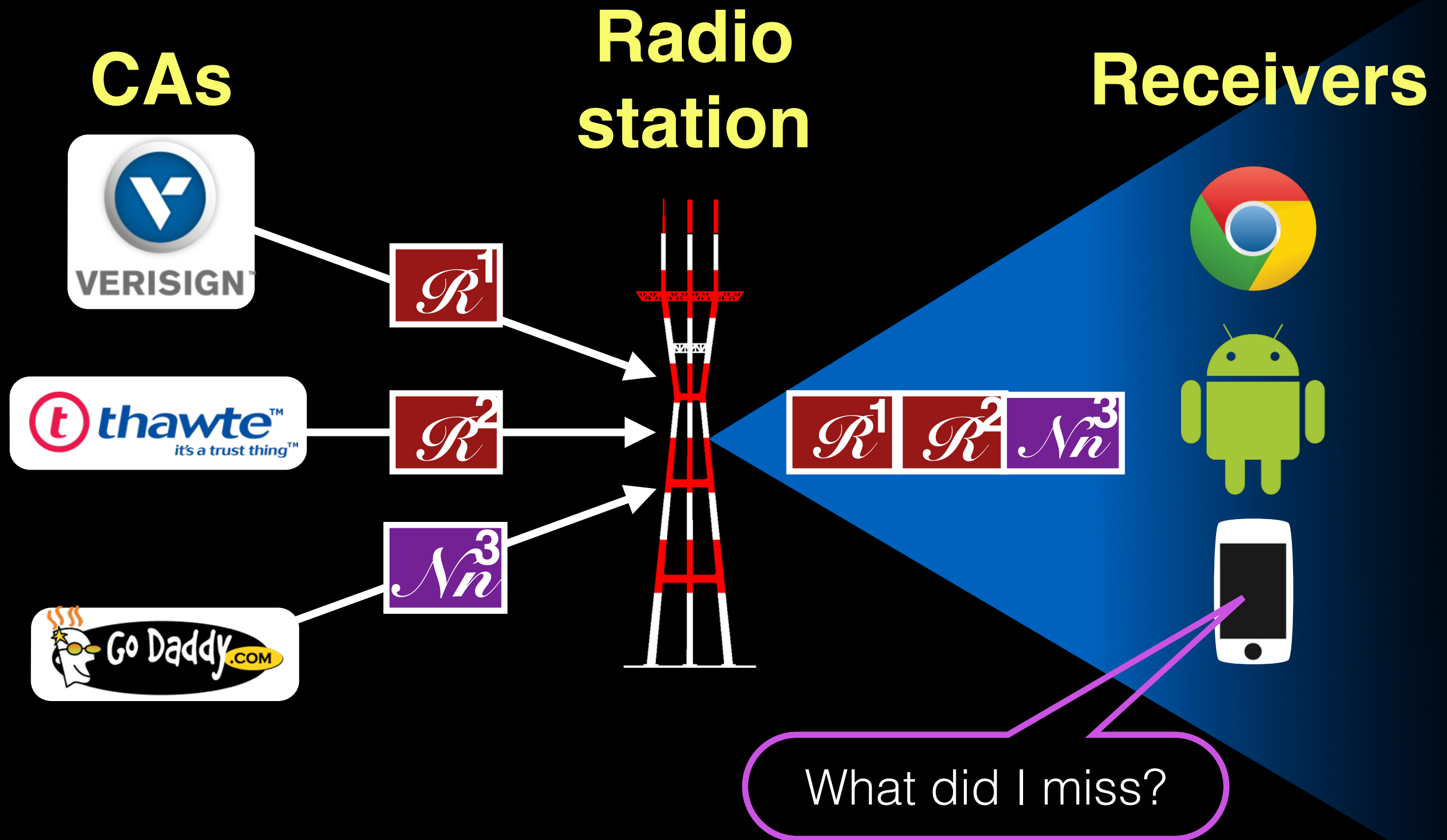




# Sleeping receivers can lose synchronization

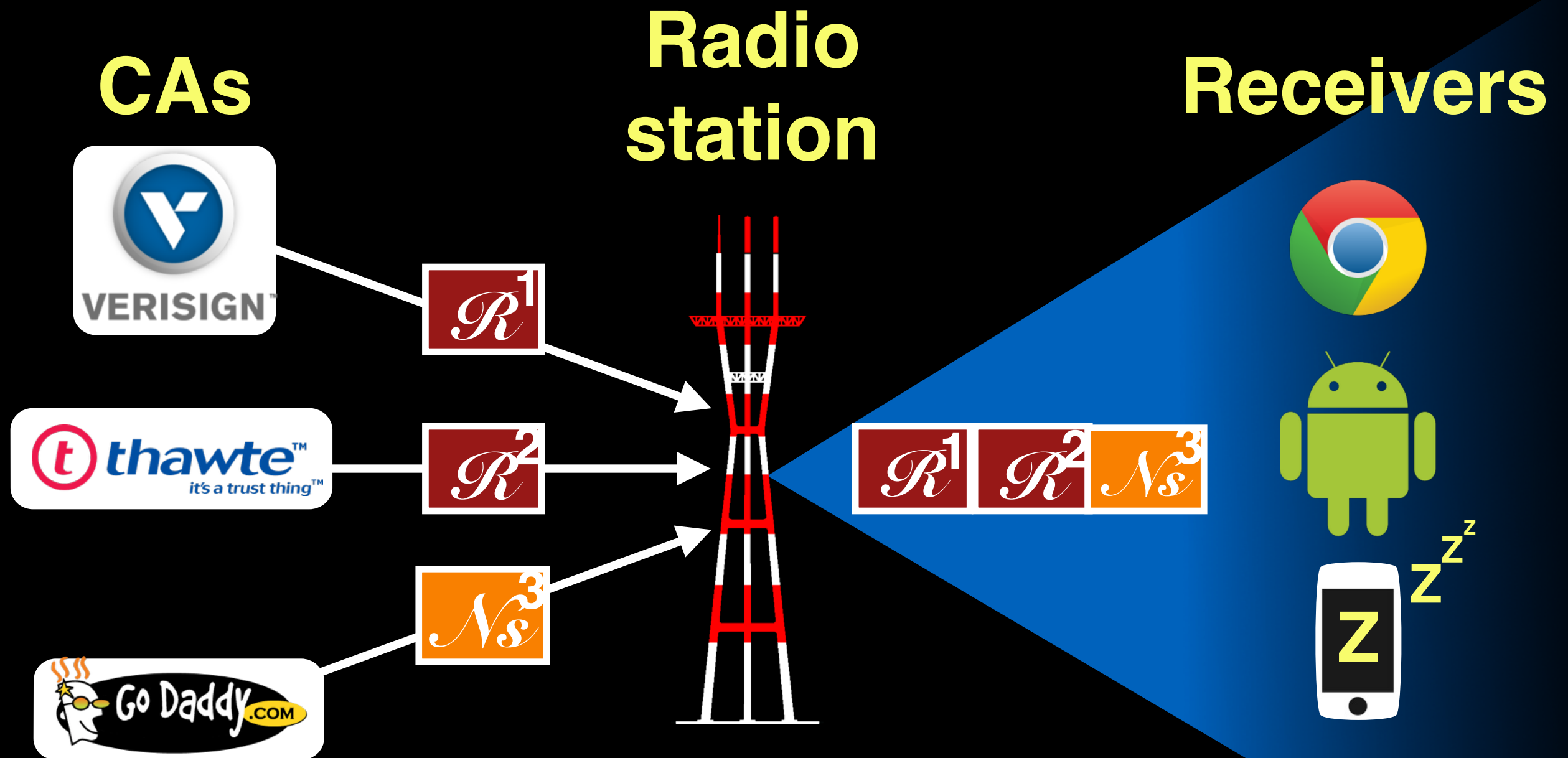


# Sleeping receivers can lose synchronization

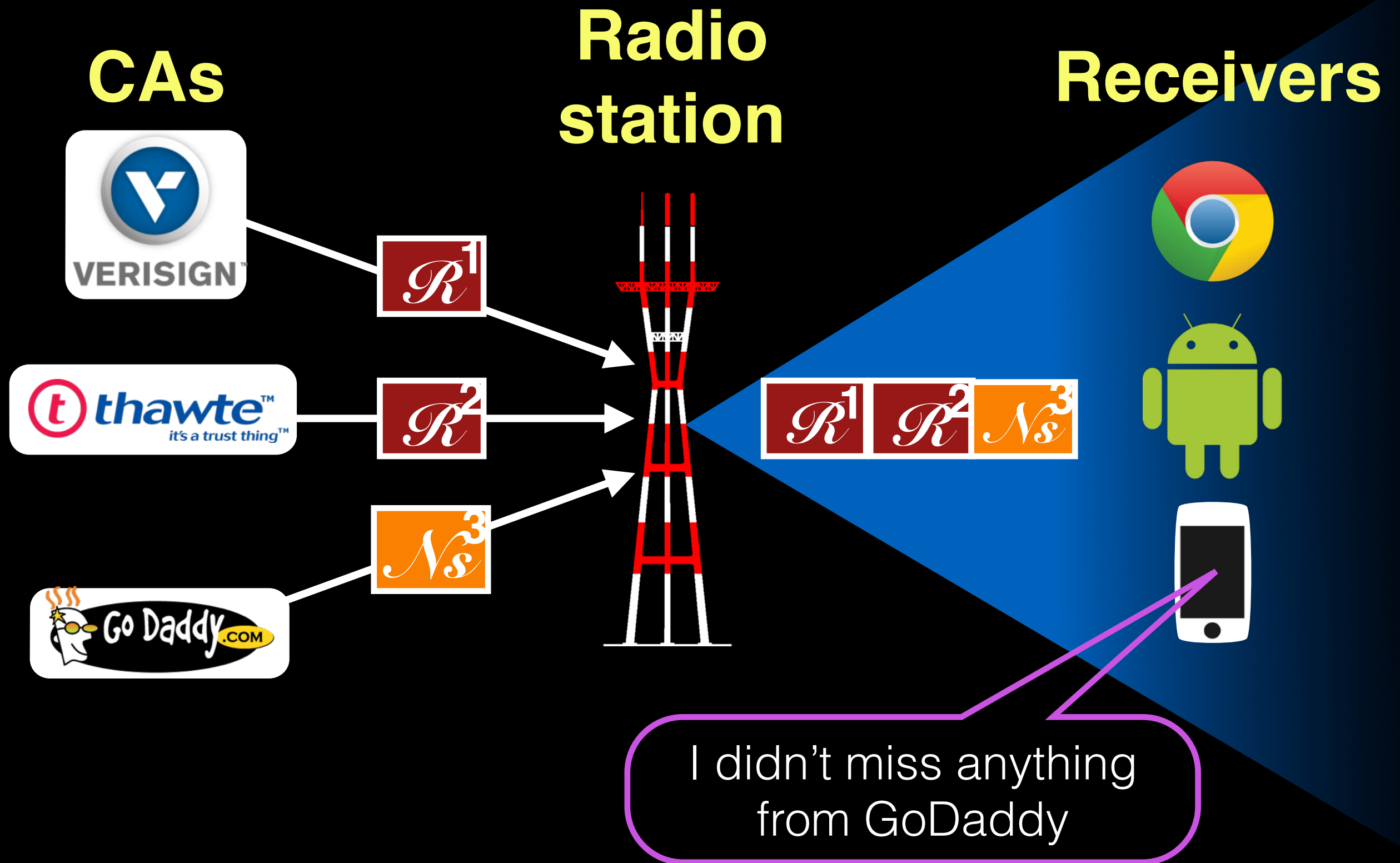




Sleeping receivers stay up-to-date with “Nothing since”



Sleeping receivers stay up-to-date with “Nothing since”



# RevCast messages



Revocation

Revoking  
CAs



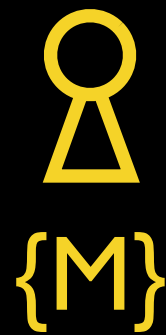
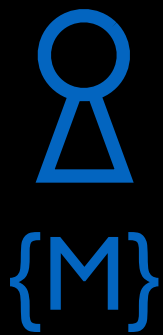
Nothing now



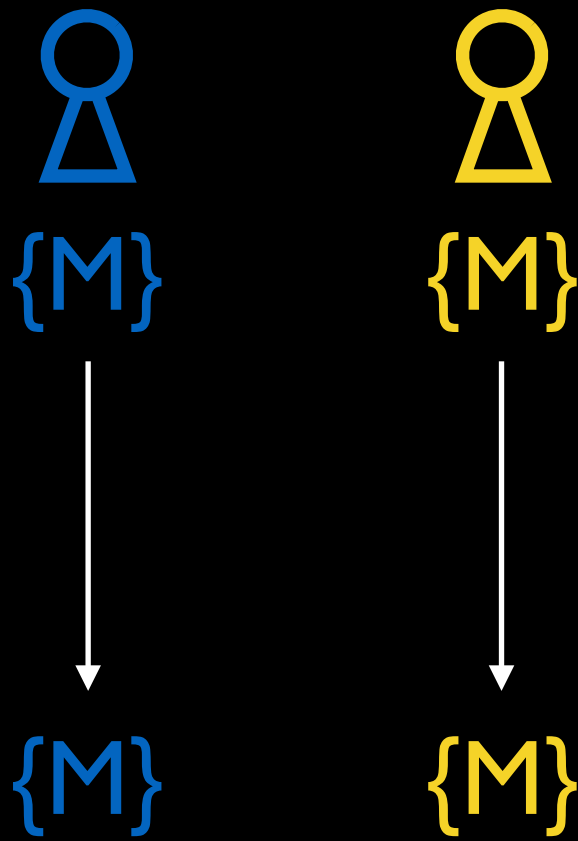
Nothing since

All other CAs  
Must sign every 10s

# Shortening “nothing now” and “nothing since”

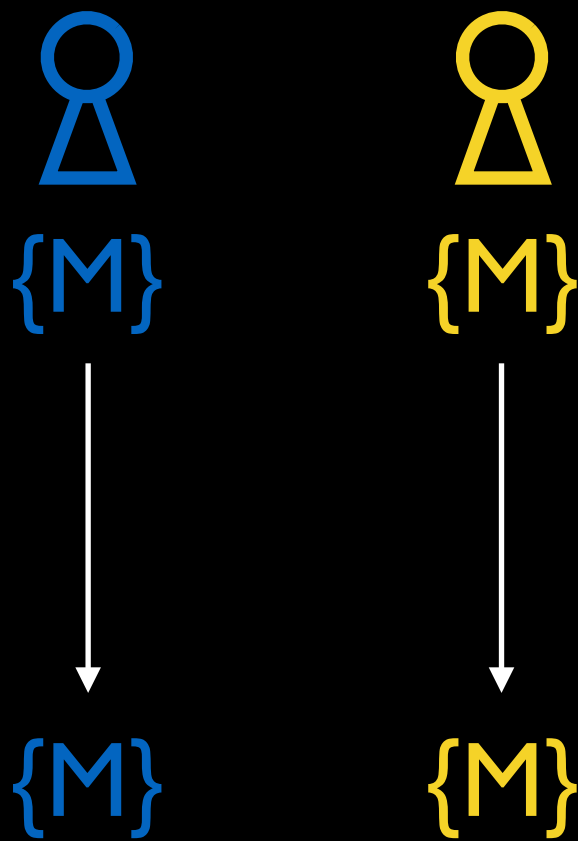


# Shortening “nothing now” and “nothing since”



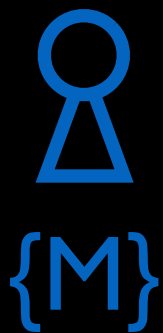
# Shortening “nothing now” and “nothing since”

Problem: FM RDS doesn't scale to ***hundreds of*** signatures



# Shortening “nothing now” and “nothing since”

Problem: FM RDS doesn't scale to ***hundreds of*** signatures

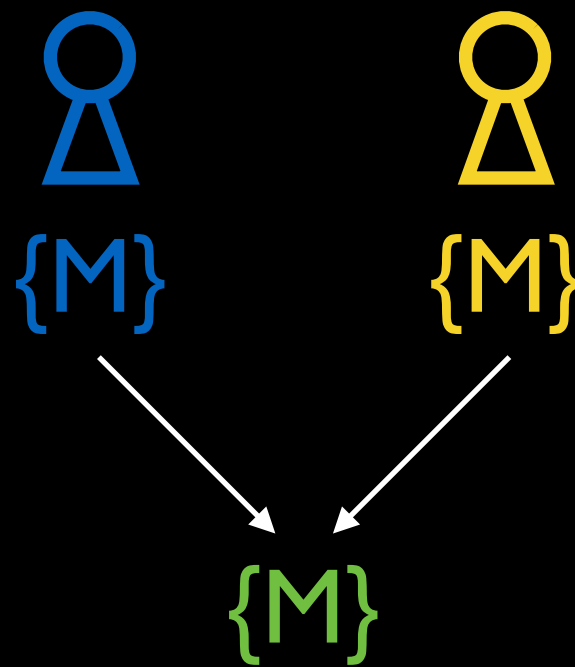


# Shortening “nothing now” and “nothing since”

Problem: FM RDS doesn't scale to *hundreds of* signatures

Multi-signatures: combine multiple CA signatures into one

[Boldyreva 2003]



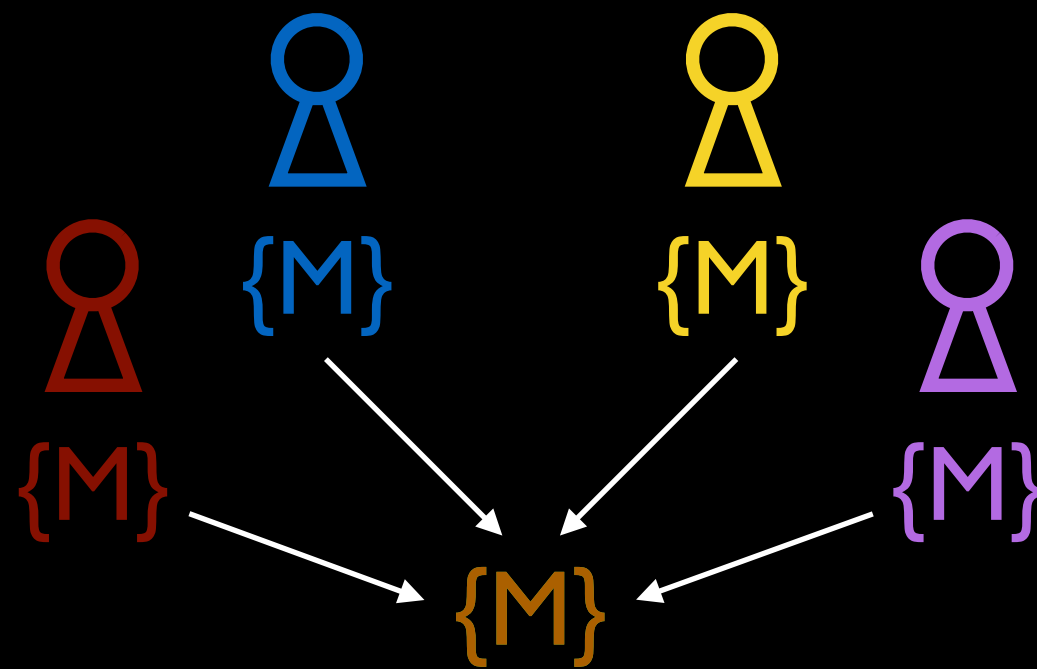


# Shortening “nothing now” and “nothing since”

Problem: FM RDS doesn't scale to *hundreds of* signatures

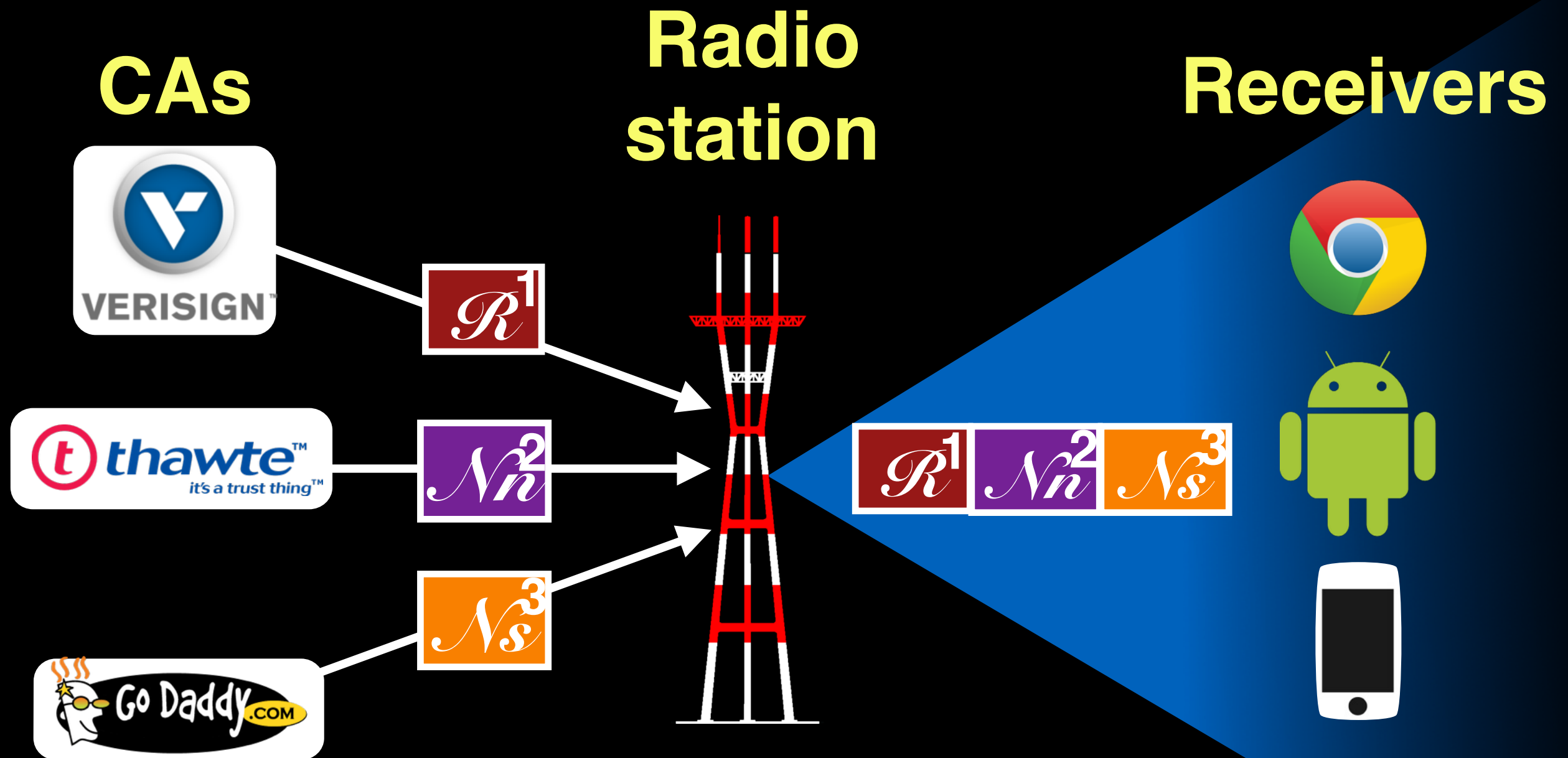
Multi-signatures: combine multiple CA signatures into one

[Boldyreva 2003]



2.89 seconds for both “nothing new” and “nothing since”

# RevCast summary

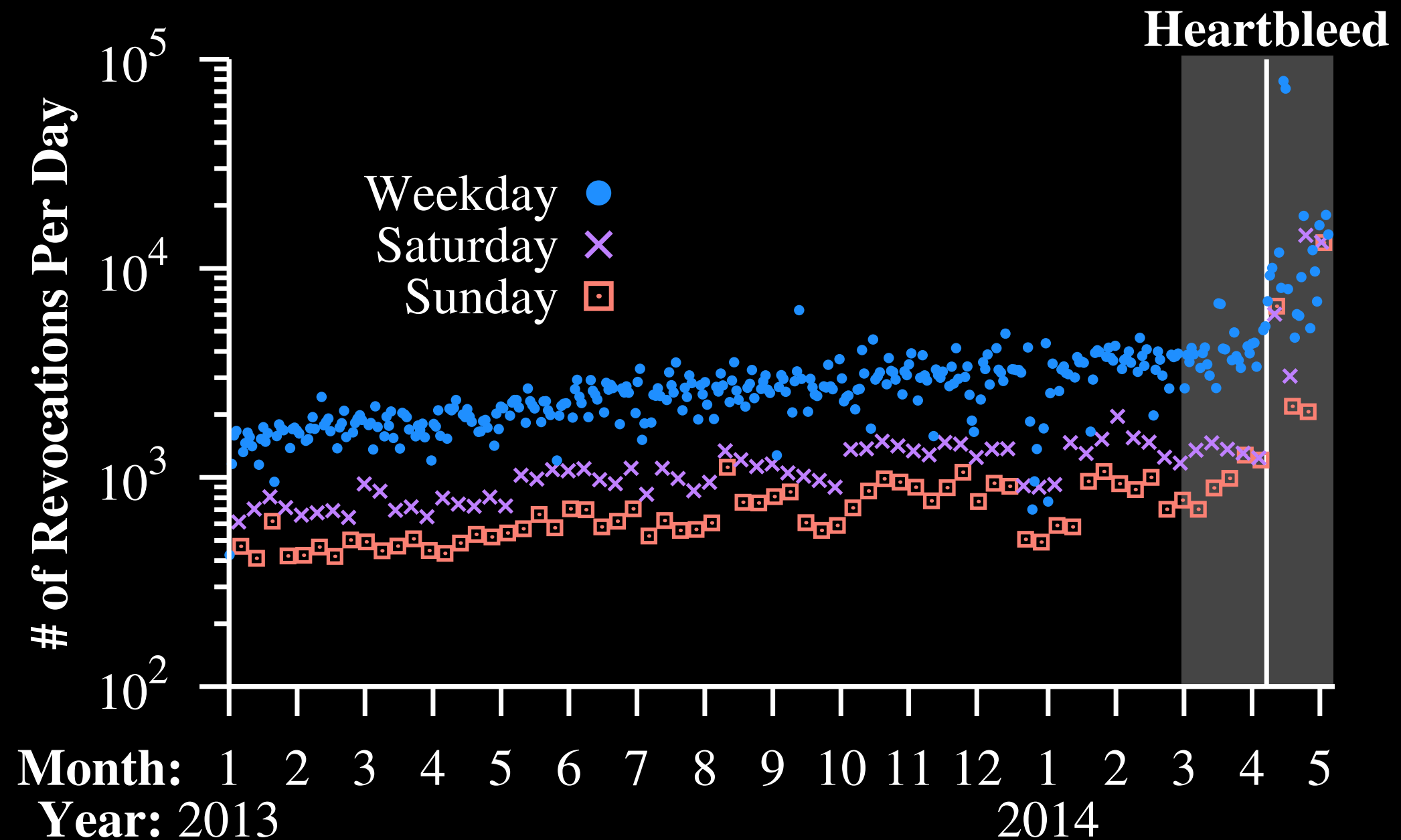


# Evaluation

1. How quickly can RevCast send updates?
2. How would RevCast handle a worst case scenario?
3. Is RevCast practical?

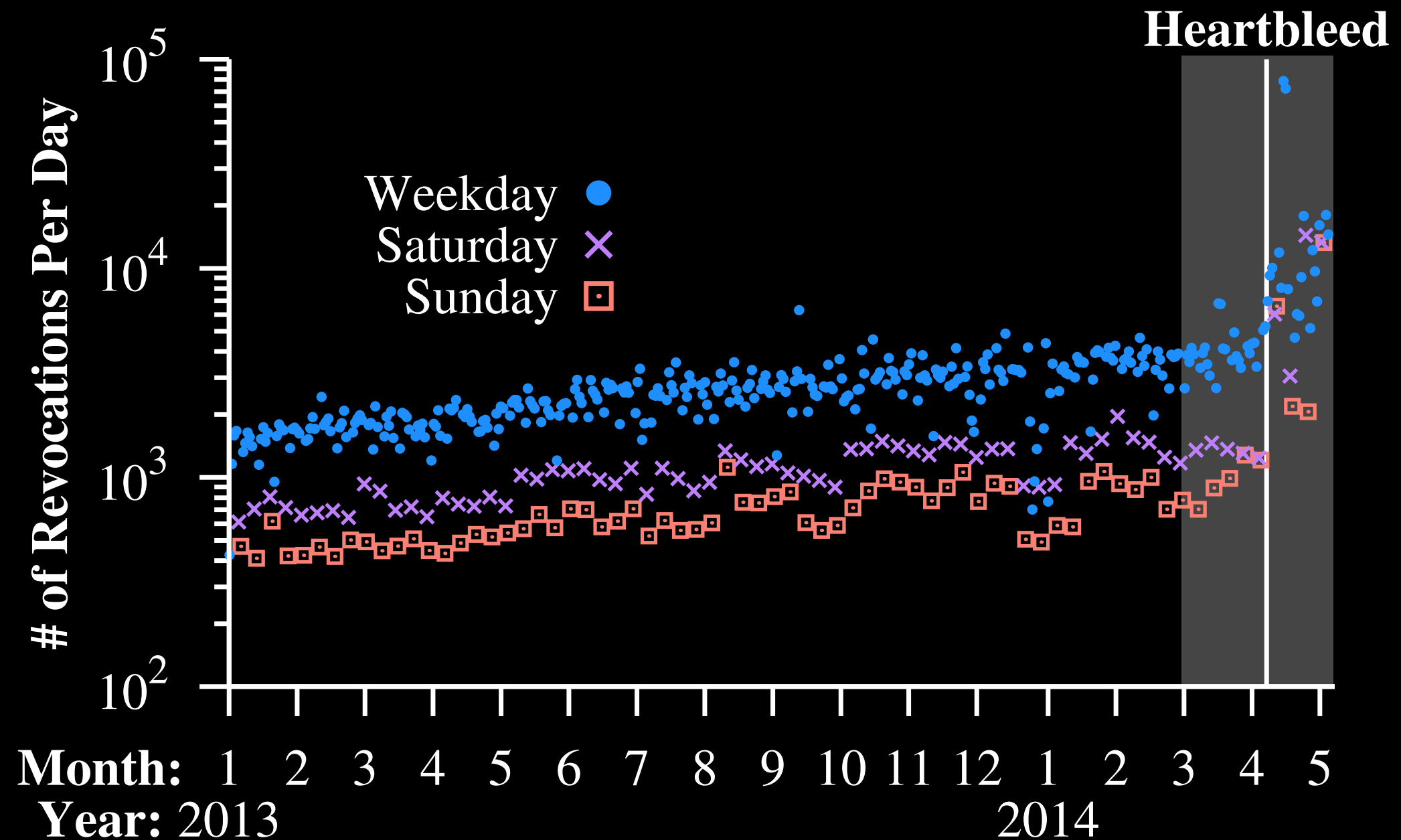
# Evaluation

978 CRLs extracted from Rapid7's scan of the entire IPv4 space



# Evaluation

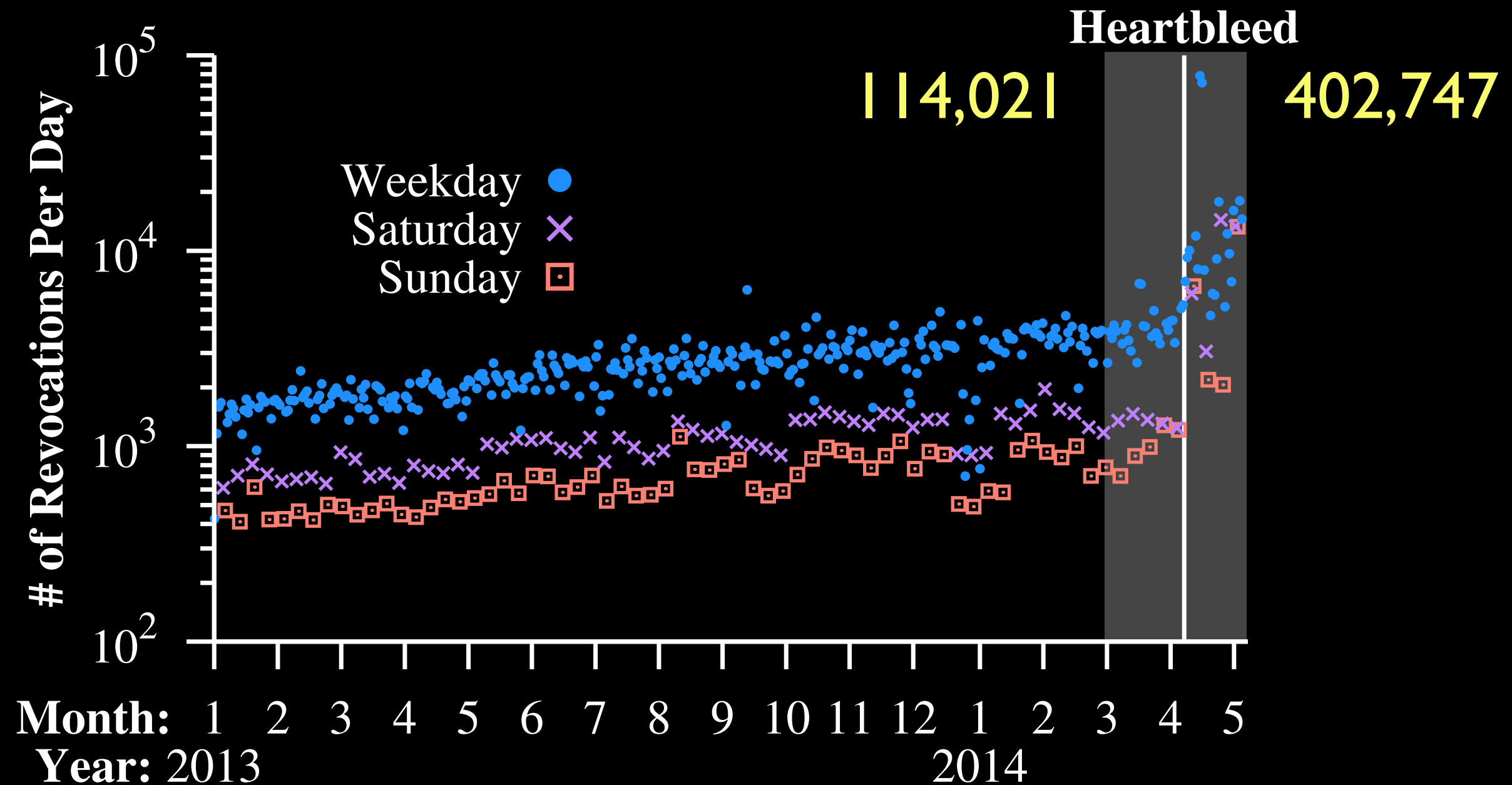
978 CRLs extracted from Rapid7's scan of the entire IPv4 space



Security takes the weekends off

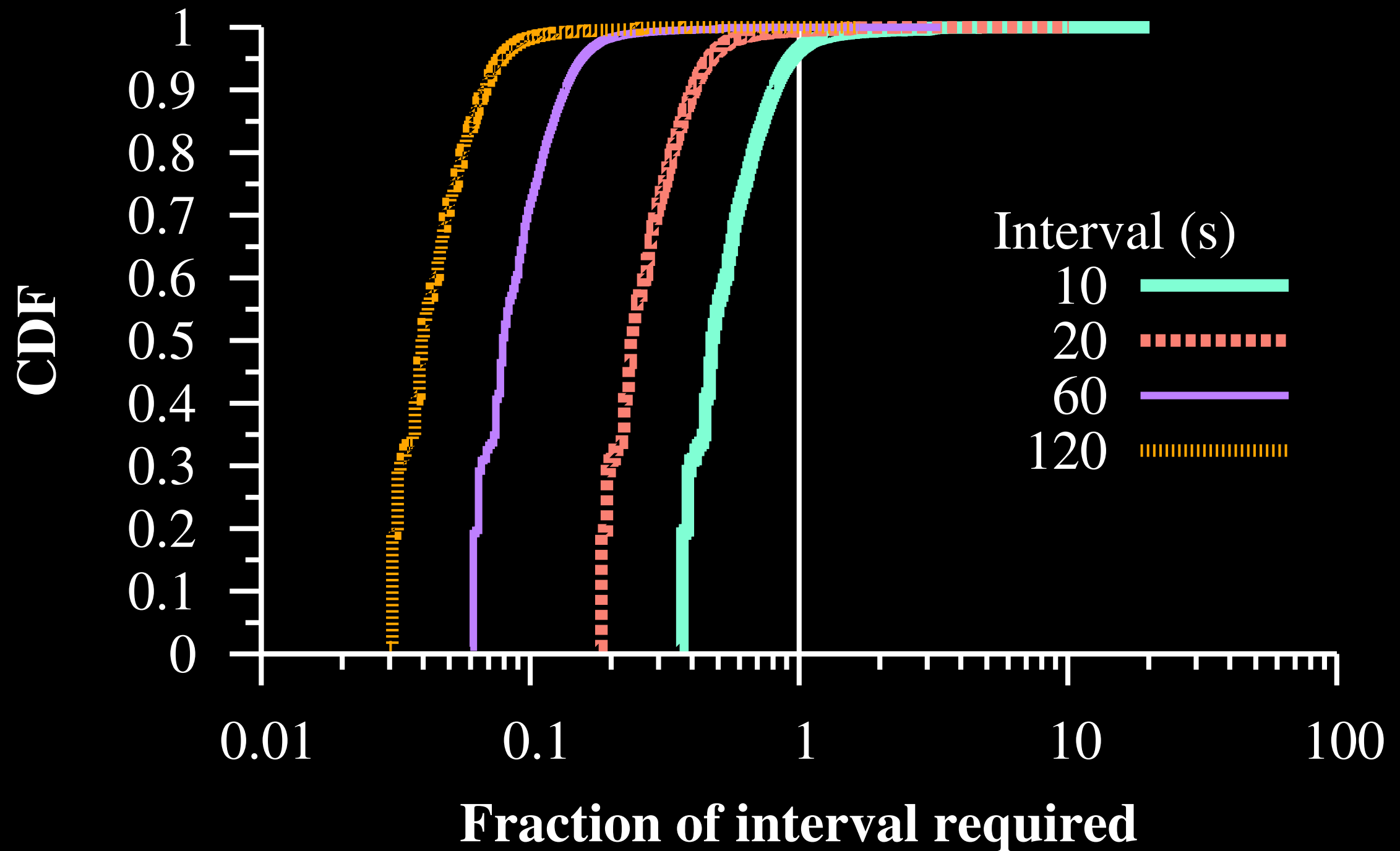
# Evaluation

978 CRLs extracted from Rapid7's scan of the entire IPv4 space



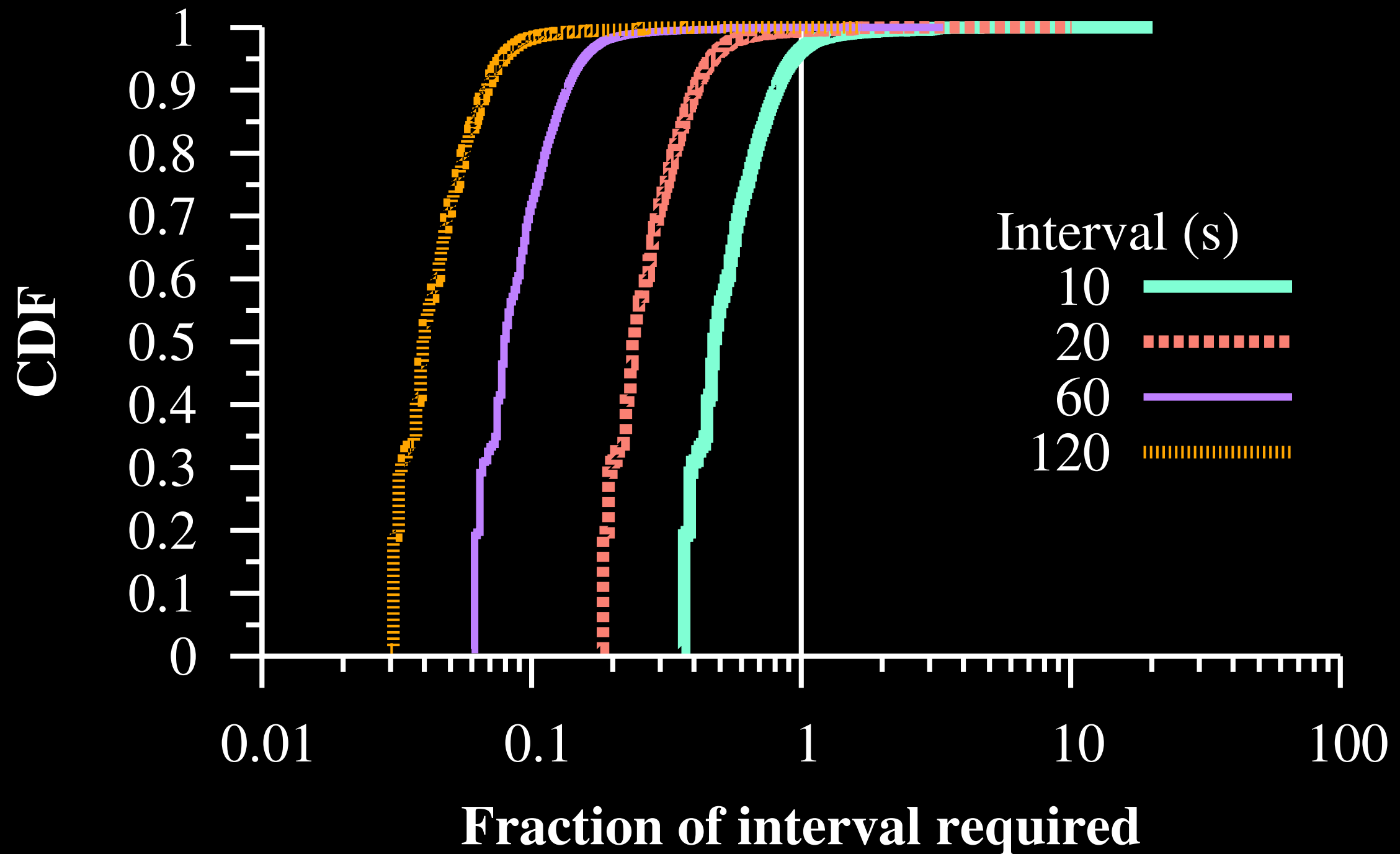
Security takes the weekends off

# How quickly can RevCast update?





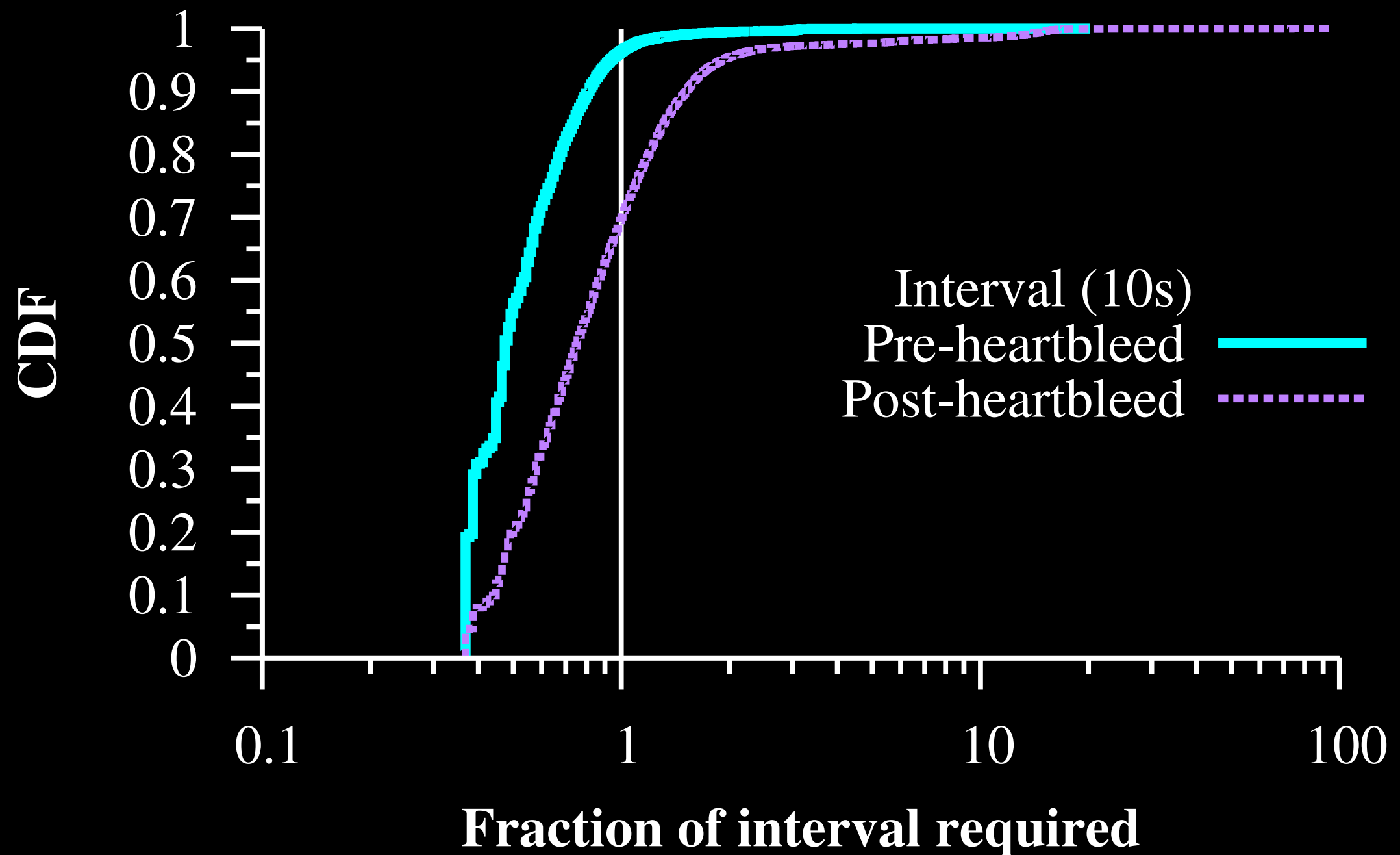
# How quickly can RevCast update?



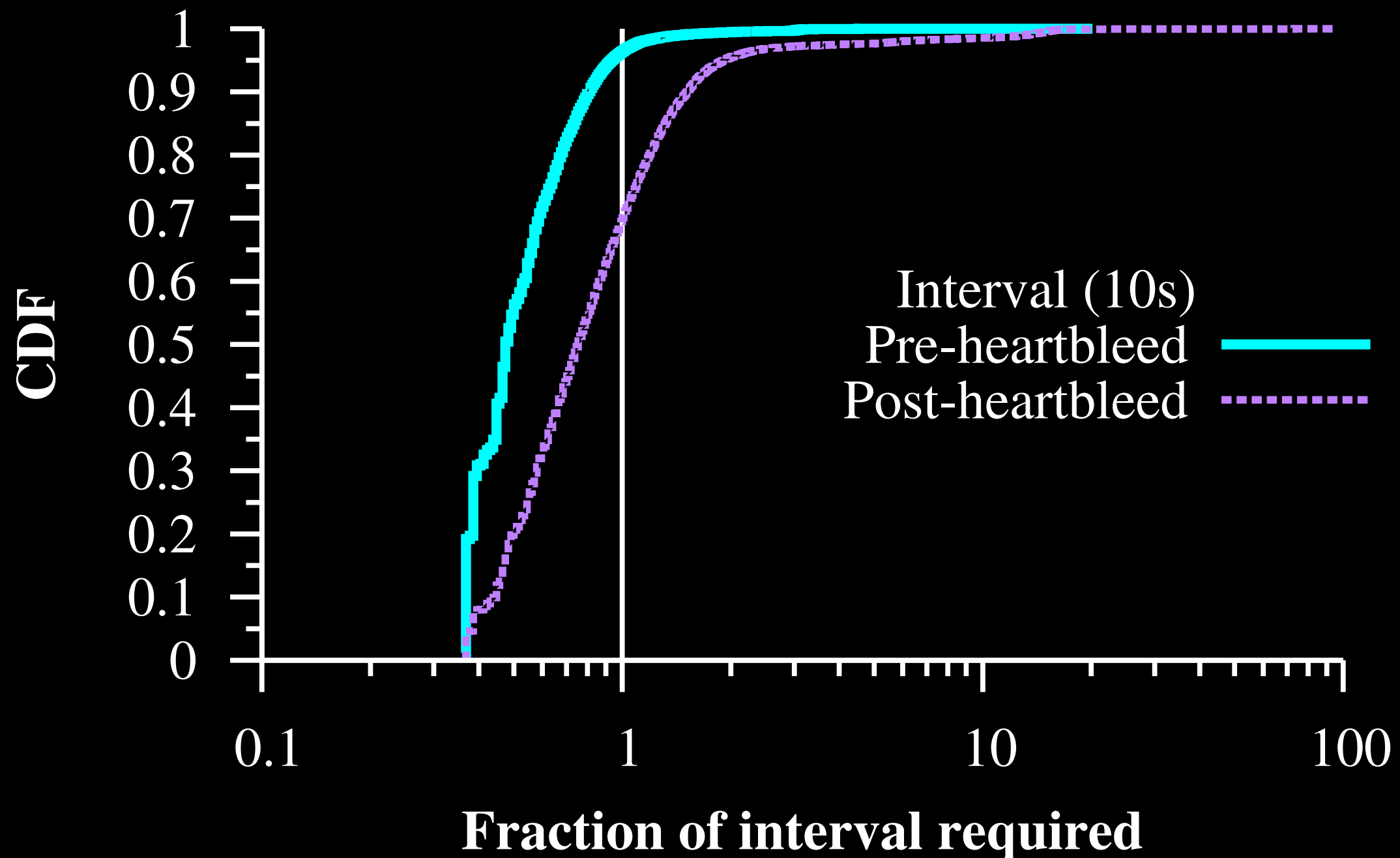
96% of 10sec intervals

99.999% of 2min intervals

# Worst-case scenario

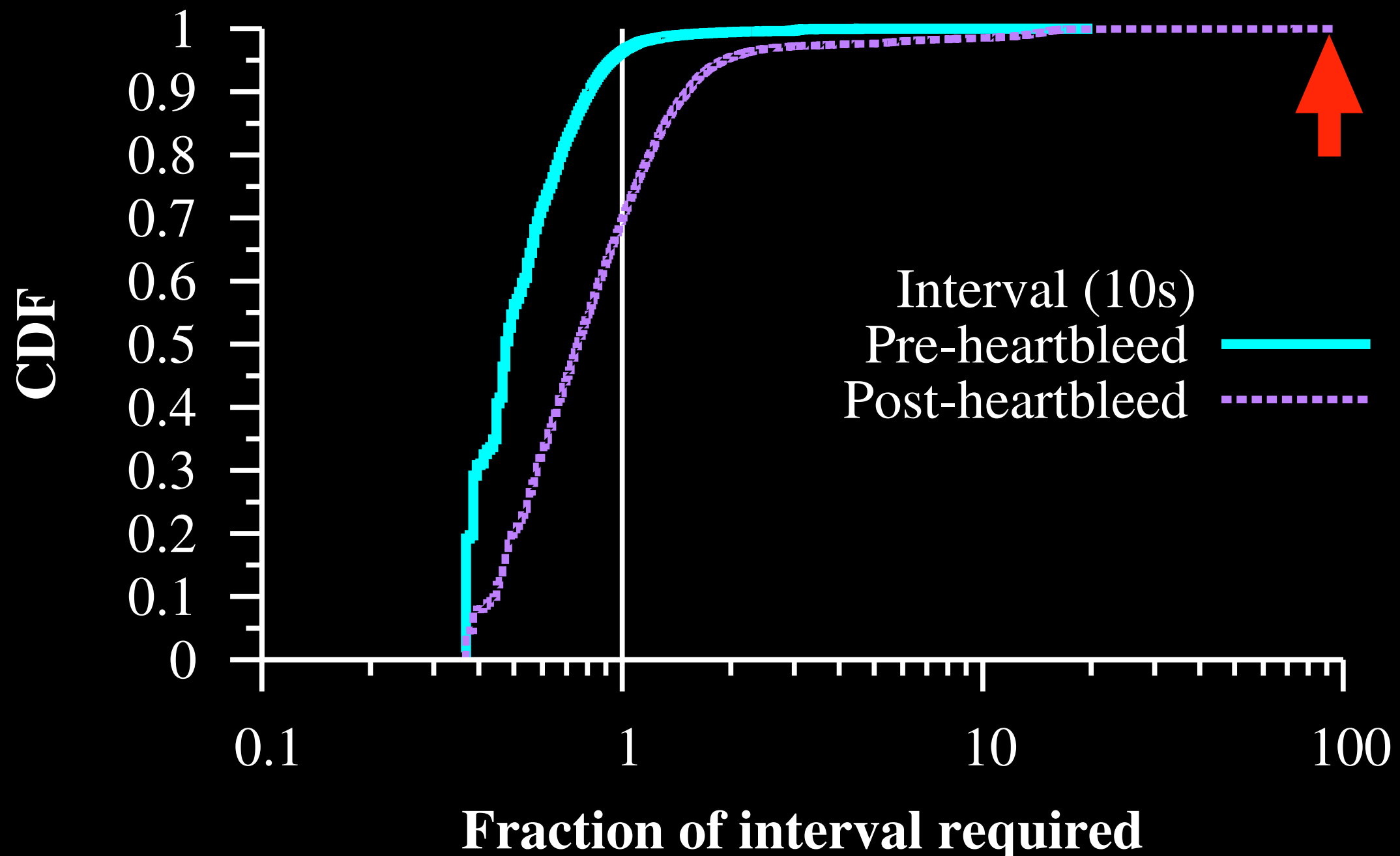


# Worst-case scenario



70% of time, up-to-date within 10 seconds

# Worst-case scenario



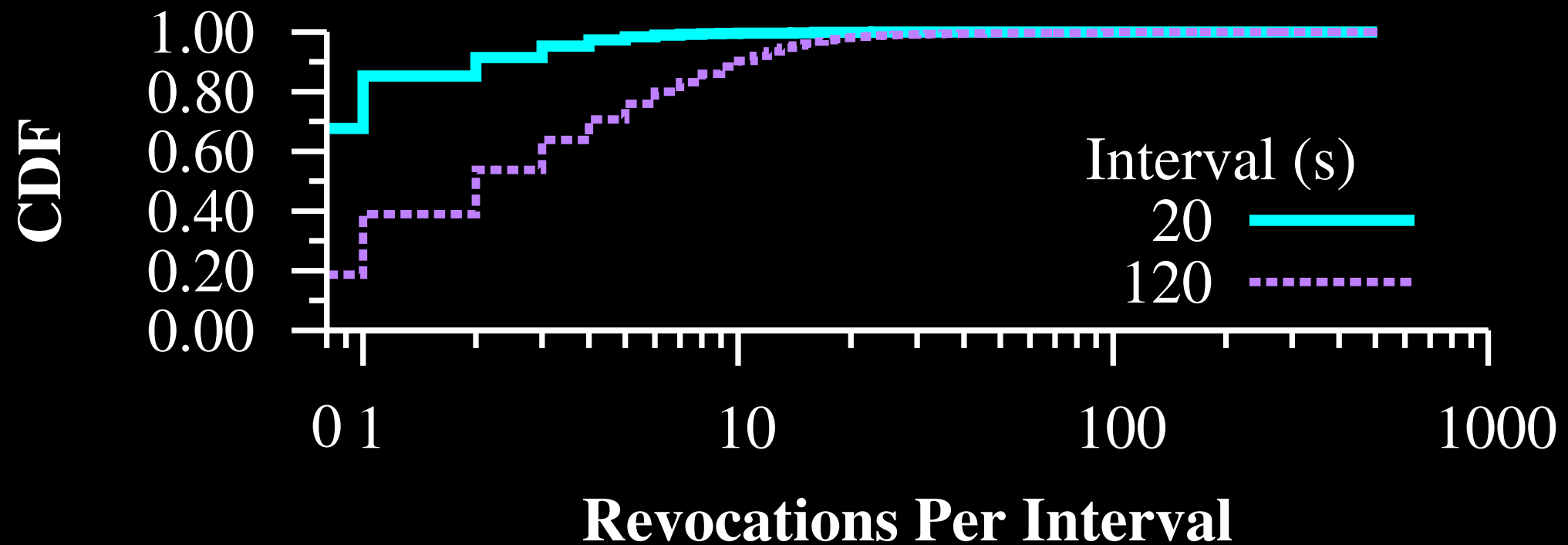
70% of time, up-to-date within 10 seconds

The most extreme takes 15.5 minutes

# Why does RevCast work?

# Why does RevCast work?

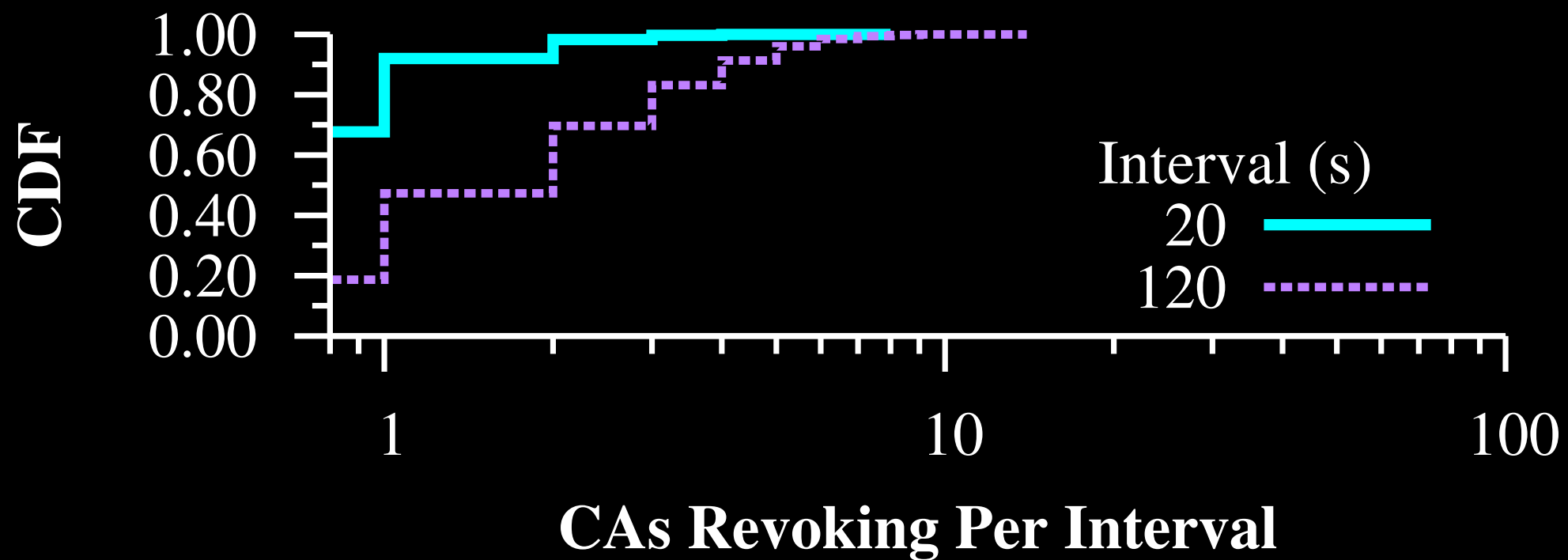
In a small window,  
there are usually  
few revocations



# Why does RevCast work?

In a small window, there are usually few revocations

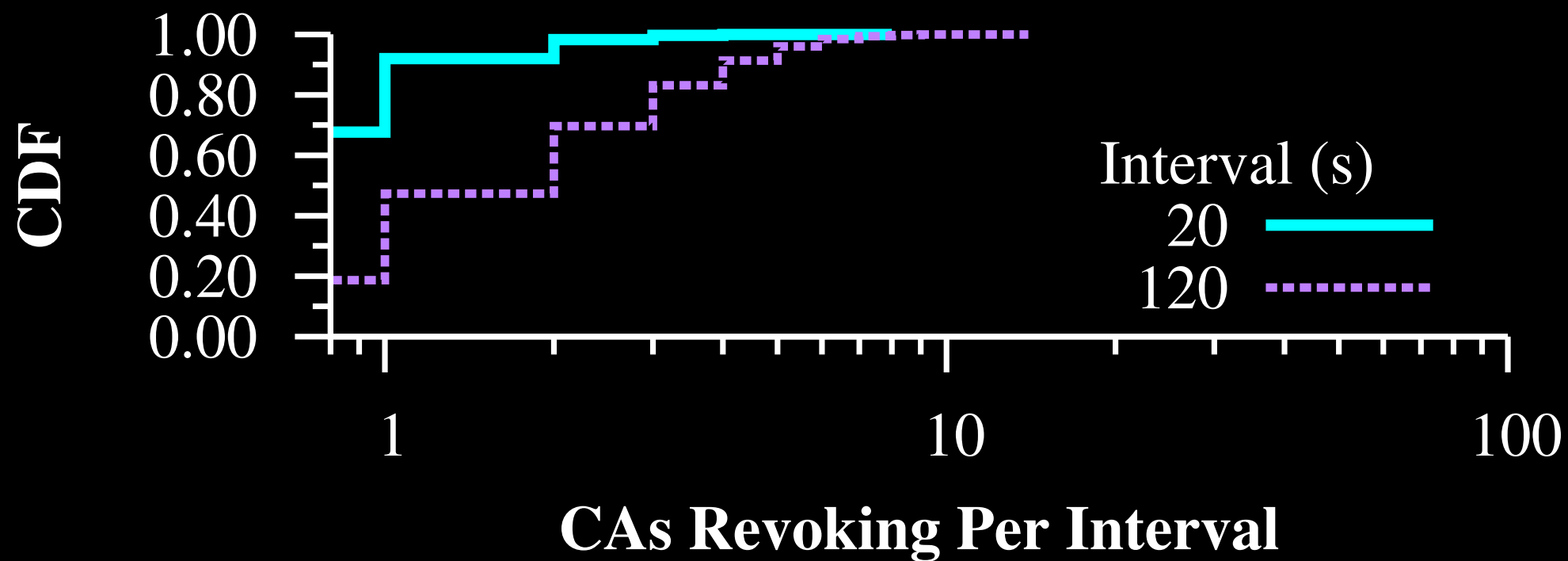
Different CAs rarely revoke within the same window



# Why does RevCast work?

In a small window, there are usually few revocations

Different CAs rarely revoke within the same window



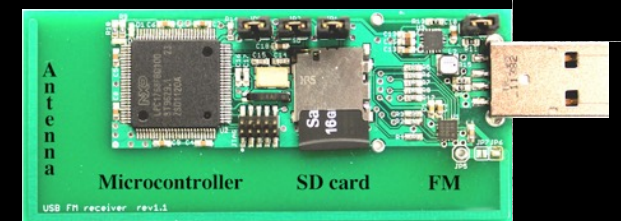
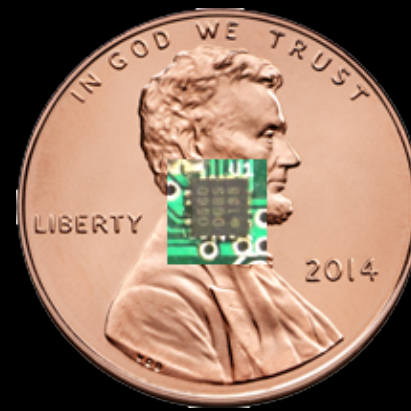
- Most CAs co-sign “nothing now” messages
- When they do have something to revoke, it’s a small list



# FM RDS is ideal for disseminating revocations

## Receivers:

- Tiny and cheap (2.5 x 2.5 mm)
  - Already built into many devices \*
- \*receivers not antennas



## Robustness:

- 10 error correcting bits for every 16 bits
- VHF & FM (same used for emergency weather radio)

# Conclusions

It is possible to design a revocation system that provides **timelines, privacy, and is low cost**.

Broadcasting revocations is a novel application of **multi-signatures**.

Practical in today's Internet, and necessary in tomorrow's.