RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: DSP-T10

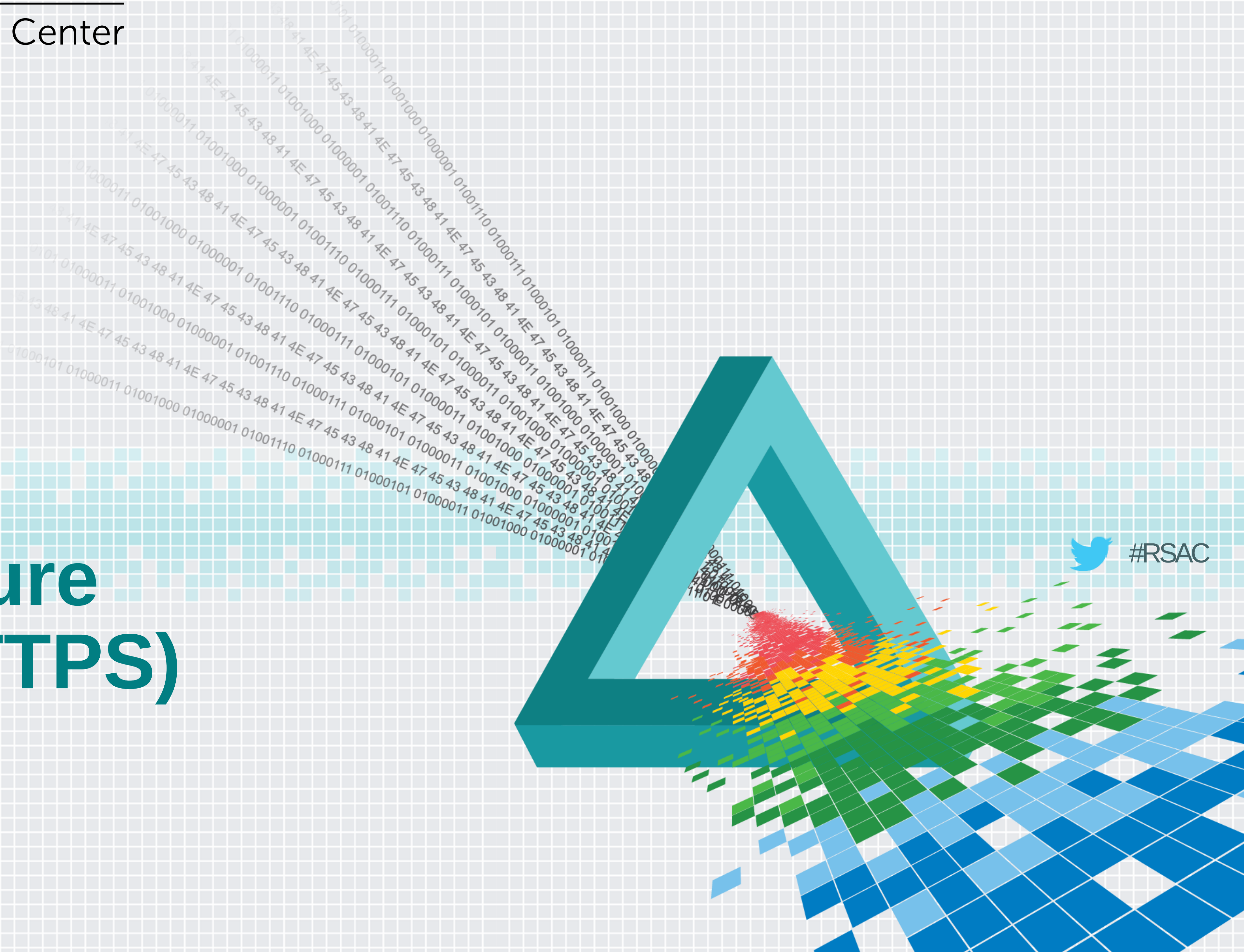
The Long Road to a Secure Web

Andy Ellis

CSO
Akamai
@csoandy

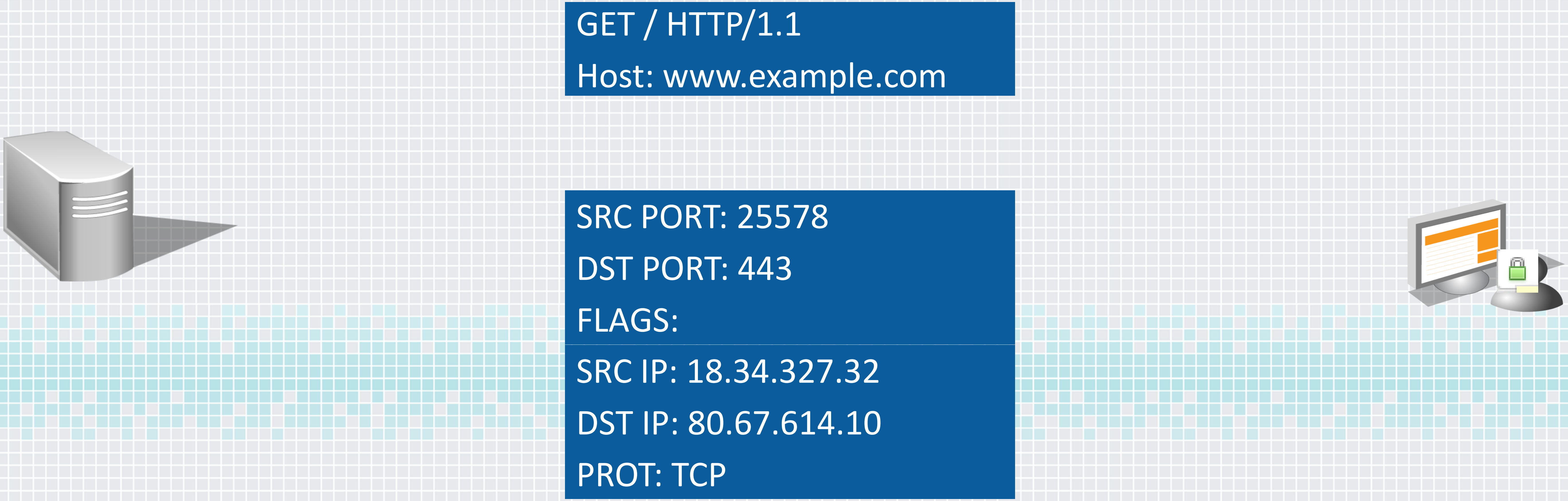
#RSAC

Some Nomenclature (Or, TLS is not HTTPS)



#RSAC

HTTP



GET / HTTP/1.1

Host: www.example.com

SRC PORT: 25578

DST PORT: 443

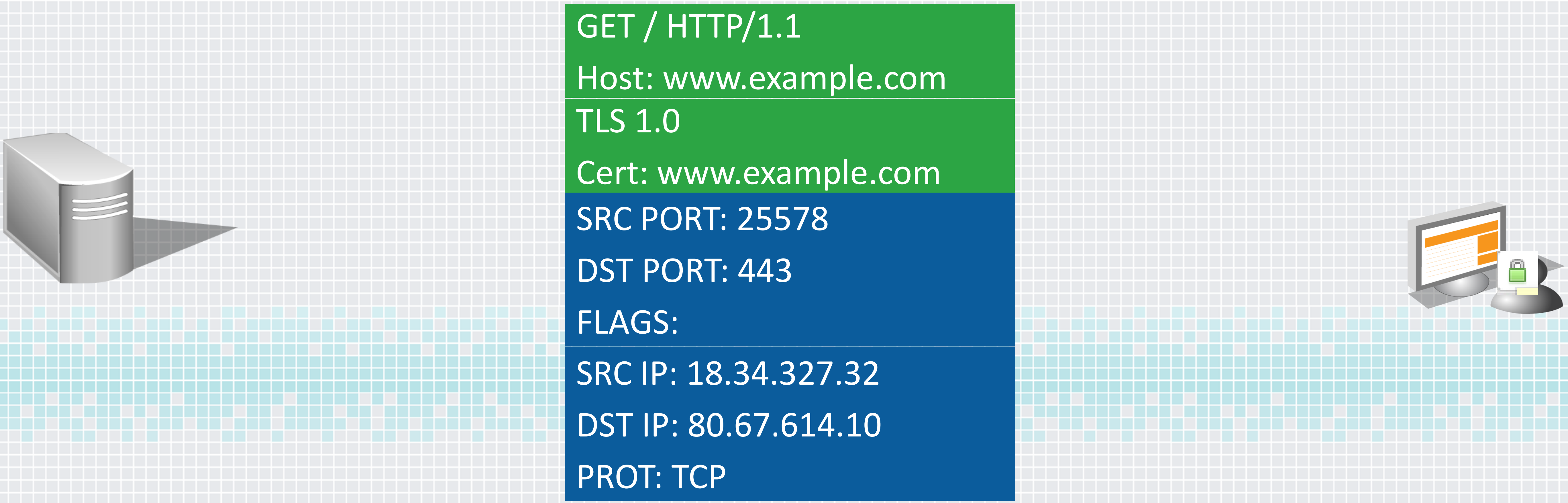
FLAGS:

SRC IP: 18.34.327.32

DST IP: 80.67.614.10

PROT: TCP

HTTPS



GET / HTTP/1.1
Host: www.example.com

TLS 1.0
Cert: www.example.com

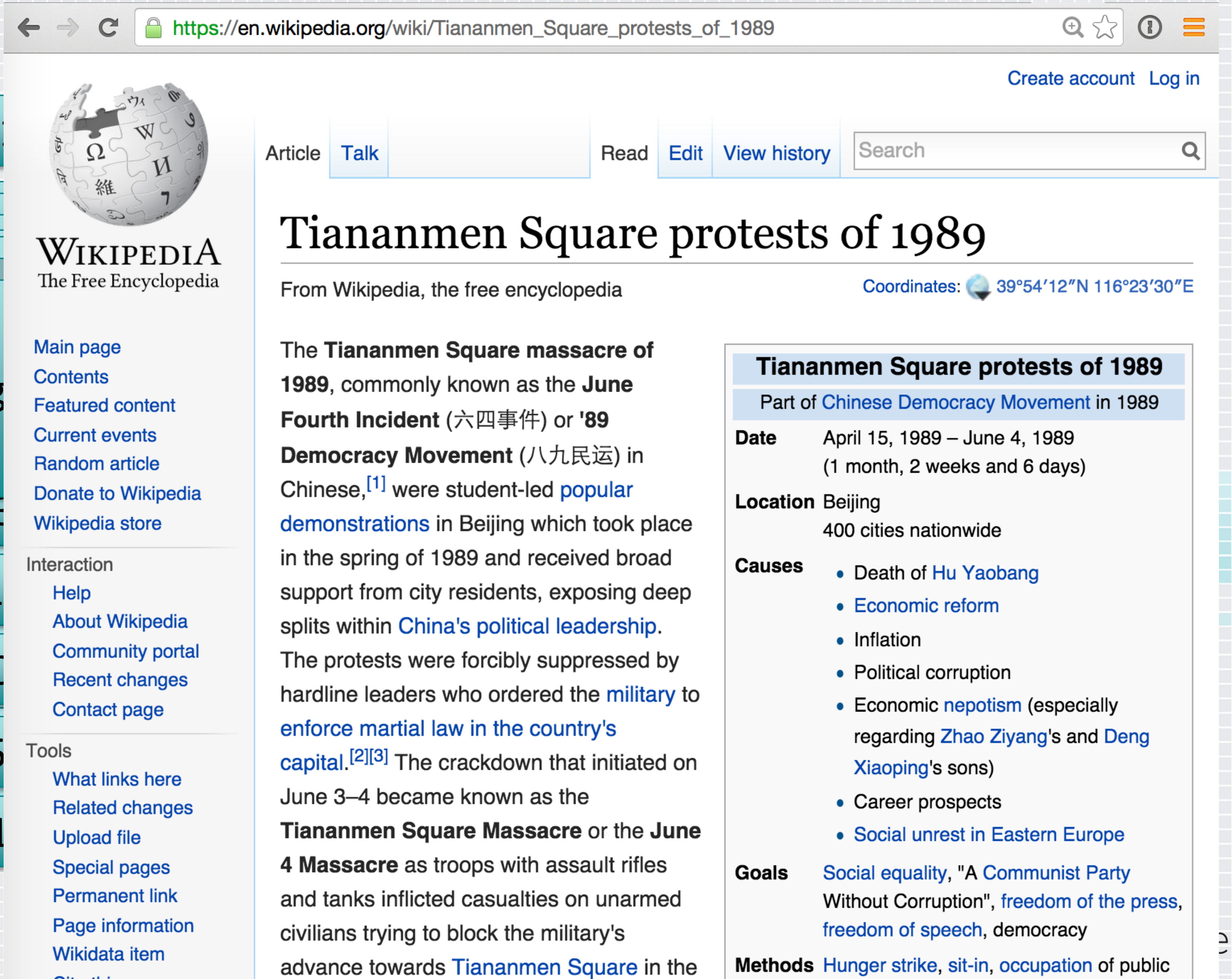
SRC PORT: 25578
DST PORT: 443
FLAGS:

SRC IP: 18.34.327.32
DST IP: 80.67.614.10
PROT: TCP

HTTPS: *secrecy* isn’t *privacy*

Privacy can be broken by too many objects…

65
1
*.wikipedia.org
7133
191
870
835
161



Tiananmen Square protests of 1989

From Wikipedia, the free encyclopedia

Coordinates: 39°54′12″N 116°23′30″E

The **Tiananmen Square massacre of 1989**, commonly known as the **June Fourth Incident** (六四事件) or **'89 Democracy Movement** (八九民运) in Chinese,[1] were student-led popular demonstrations in Beijing which took place in the spring of 1989 and received broad support from city residents, exposing deep splits within China's political leadership. The protests were forcibly suppressed by hardline leaders who ordered the military to enforce martial law in the country's capital.[2][3] The crackdown that initiated on June 3–4 became known as the **Tiananmen Square Massacre** or the **June 4 Massacre** as troops with assault rifles and tanks inflicted casualties on unarmed civilians trying to block the military's advance towards Tiananmen Square in the

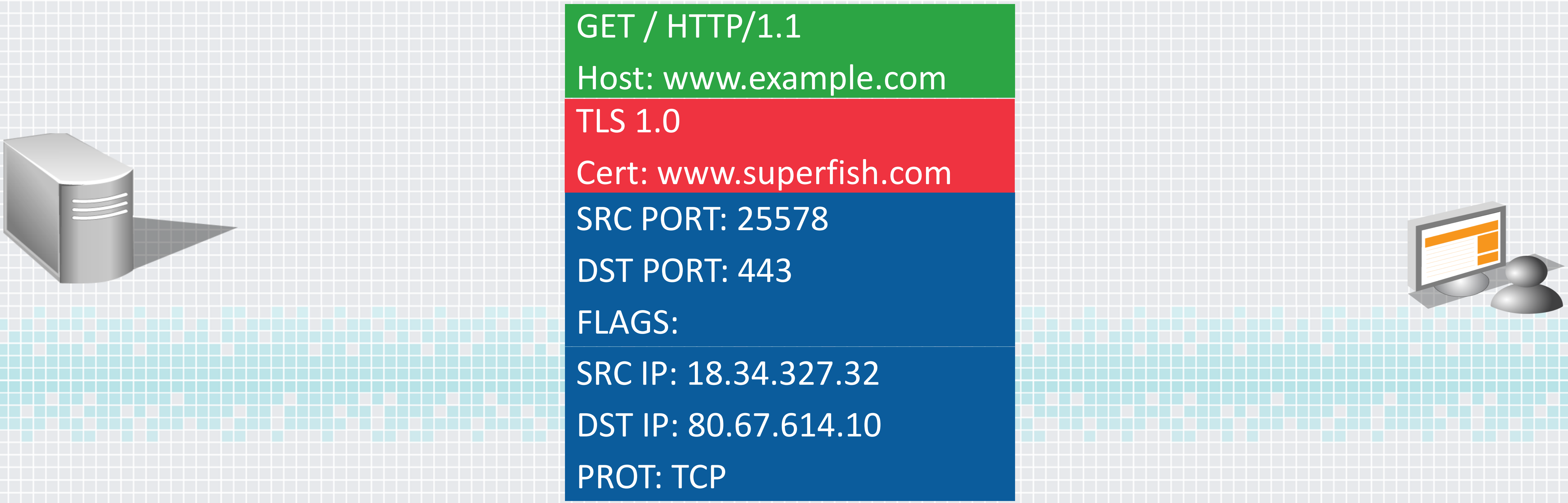
Tiananmen Square protests of 1989	
Part of Chinese Democracy Movement in 1989	
Date	April 15, 1989 – June 4, 1989 (1 month, 2 weeks and 6 days)
Location	Beijing 400 cities nationwide
Causes	• Death of Hu Yaobang • Economic reform • Inflation • Political corruption • Economic nepotism (especially regarding Zhao Ziyang's and Deng Xiaoping's sons) • Career prospects • Social unrest in Eastern Europe
Goals	Social equality, "A Communist Party Without Corruption", freedom of the press, freedom of speech, democracy
Methods	Hunger strike, sit-in, occupation of public

ence2015

More privacy breaks

- Confirmation attack: send unique object set into a stream
- Timing attack: Watch external actions
- Compression dictionary attack: BREACH
- Popularity attack: Monitor performance to detect cached requests
- Phishing: Embed hyperlinks to controlled parties

HTTP over TLS



GET / HTTP/1.1

Host: www.example.com

TLS 1.0

Cert: www.superfish.com

SRC PORT: 25578

DST PORT: 443

FLAGS:

SRC IP: 18.34.327.32

DST IP: 80.67.614.10

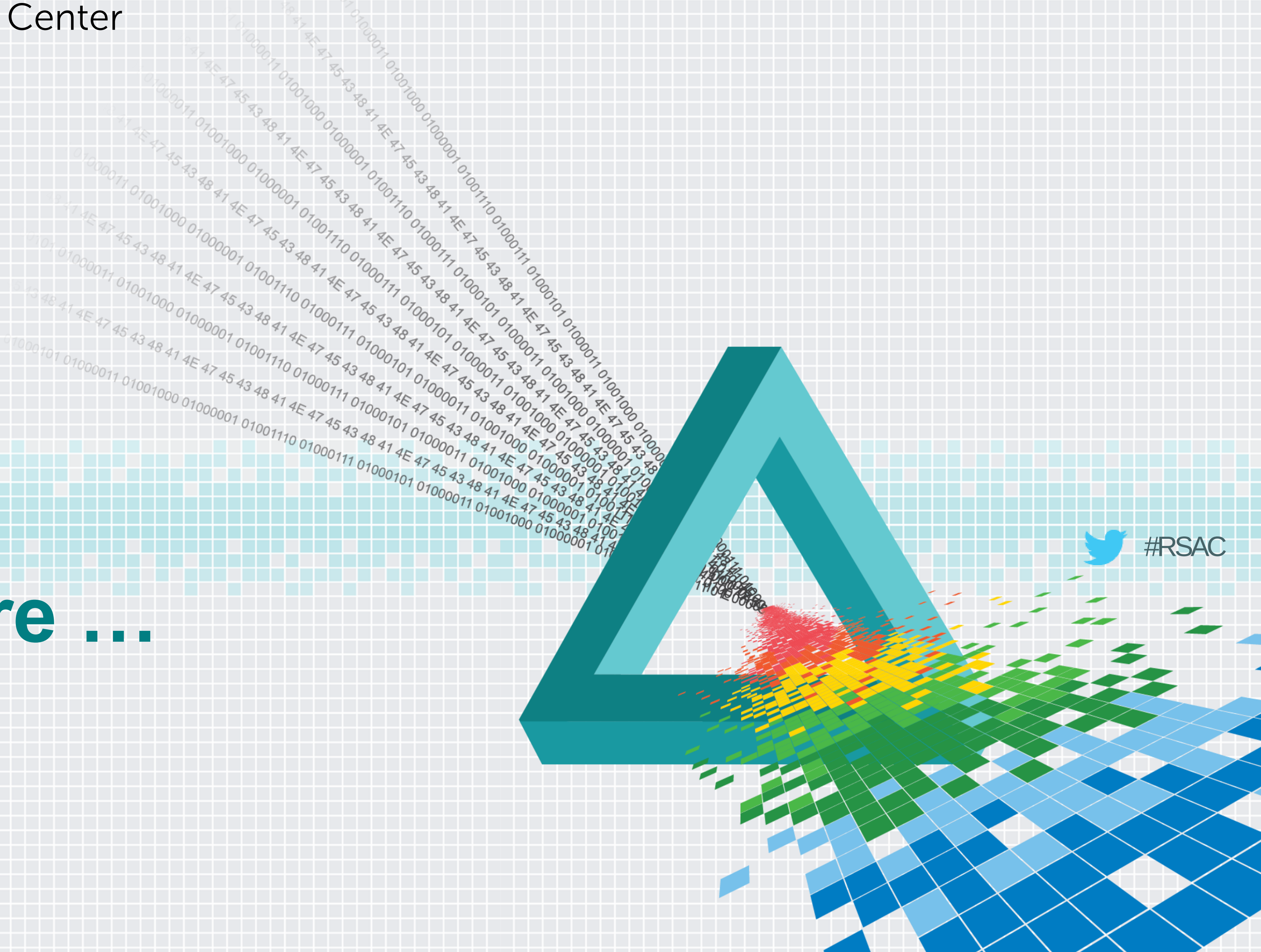
PROT: TCP

RSAConference2015

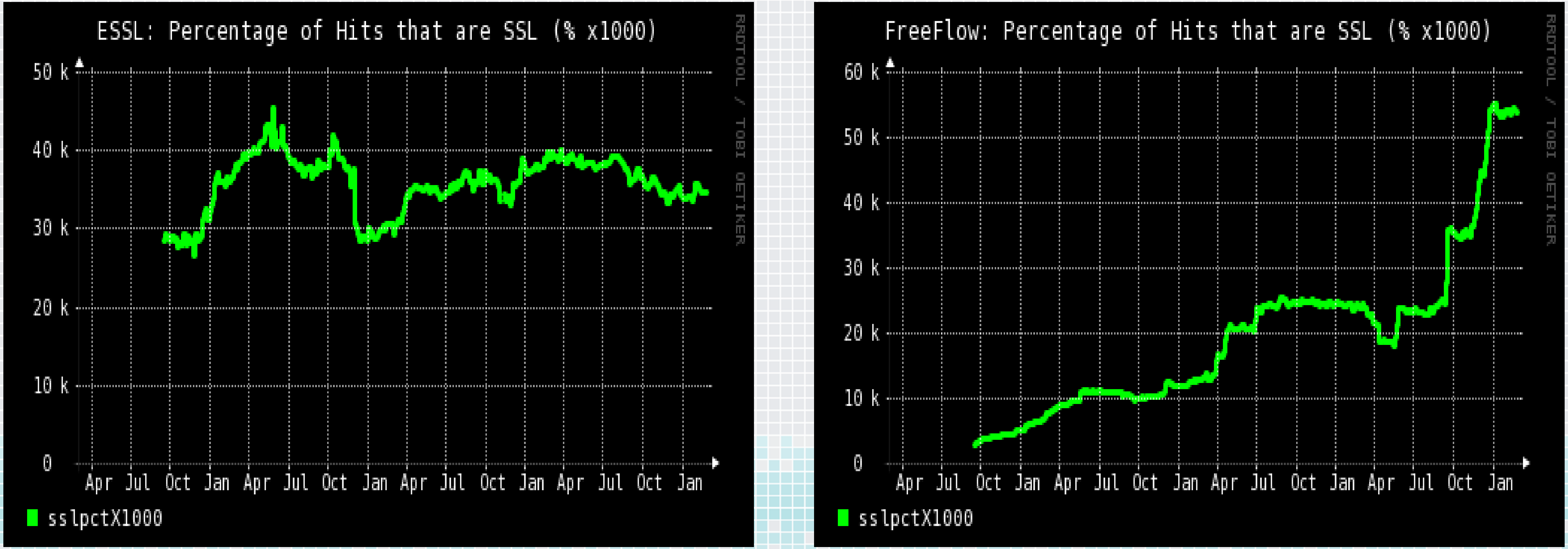
San Francisco | April 20-24 | Moscone Center

HTTPS Everywhere …

When?

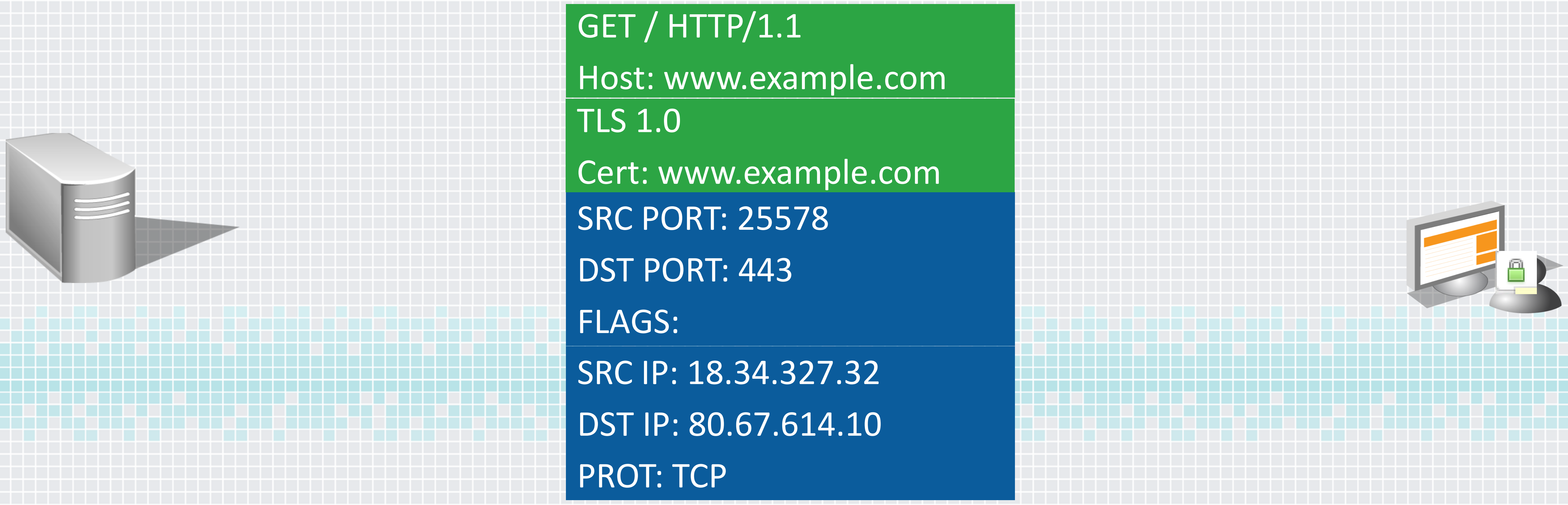


#RSAC



TLS usage is on the rise

HTTPS, SNI, and Limited IP space



GET / HTTP/1.1

Host: www.example.com

TLS 1.0

Cert: www.example.com

SRC PORT: 25578

DST PORT: 443

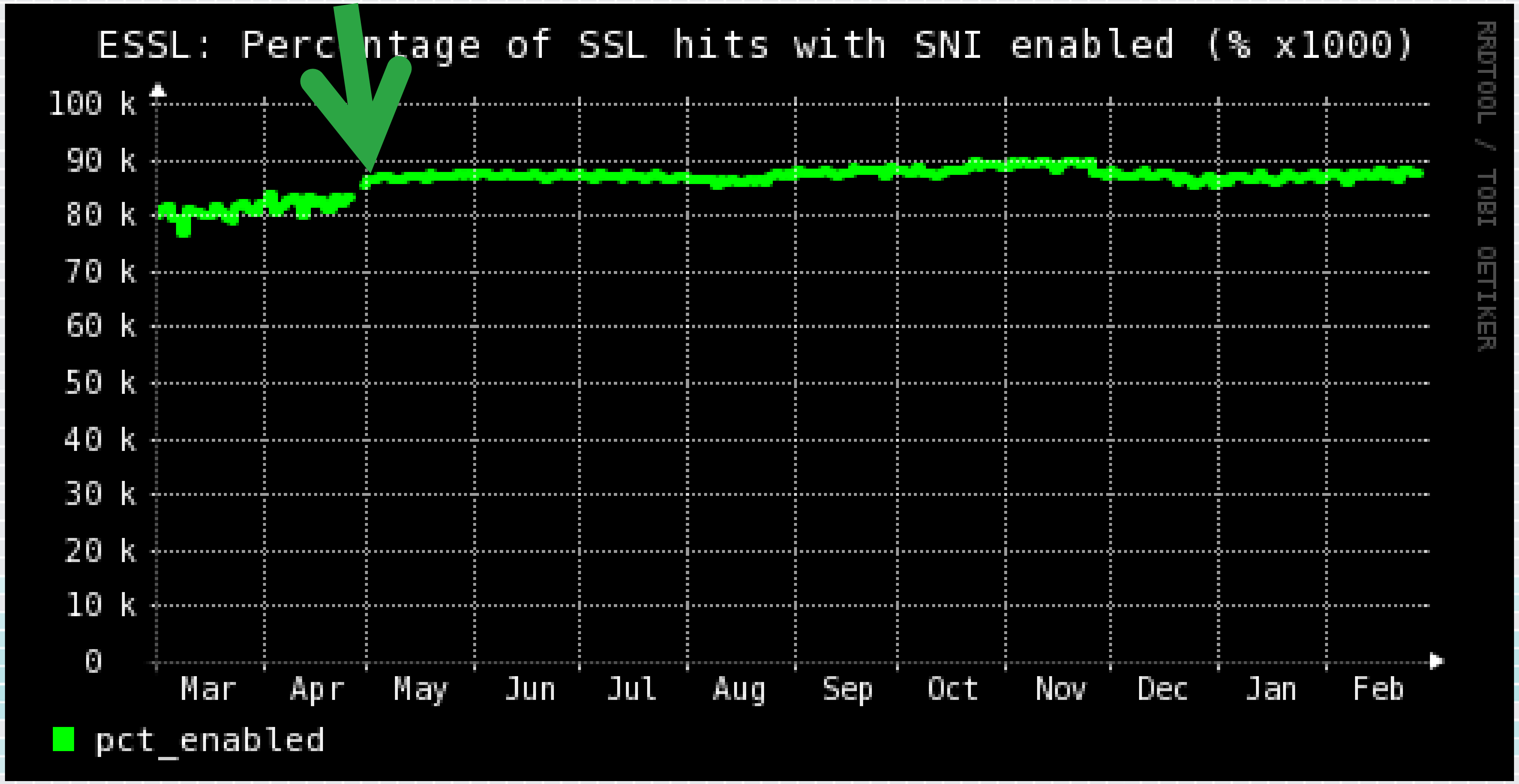
FLAGS:

SRC IP: 18.34.327.32

DST IP: 80.67.614.10

PROT: TCP

WinXP EOL



80-85%

85–90%

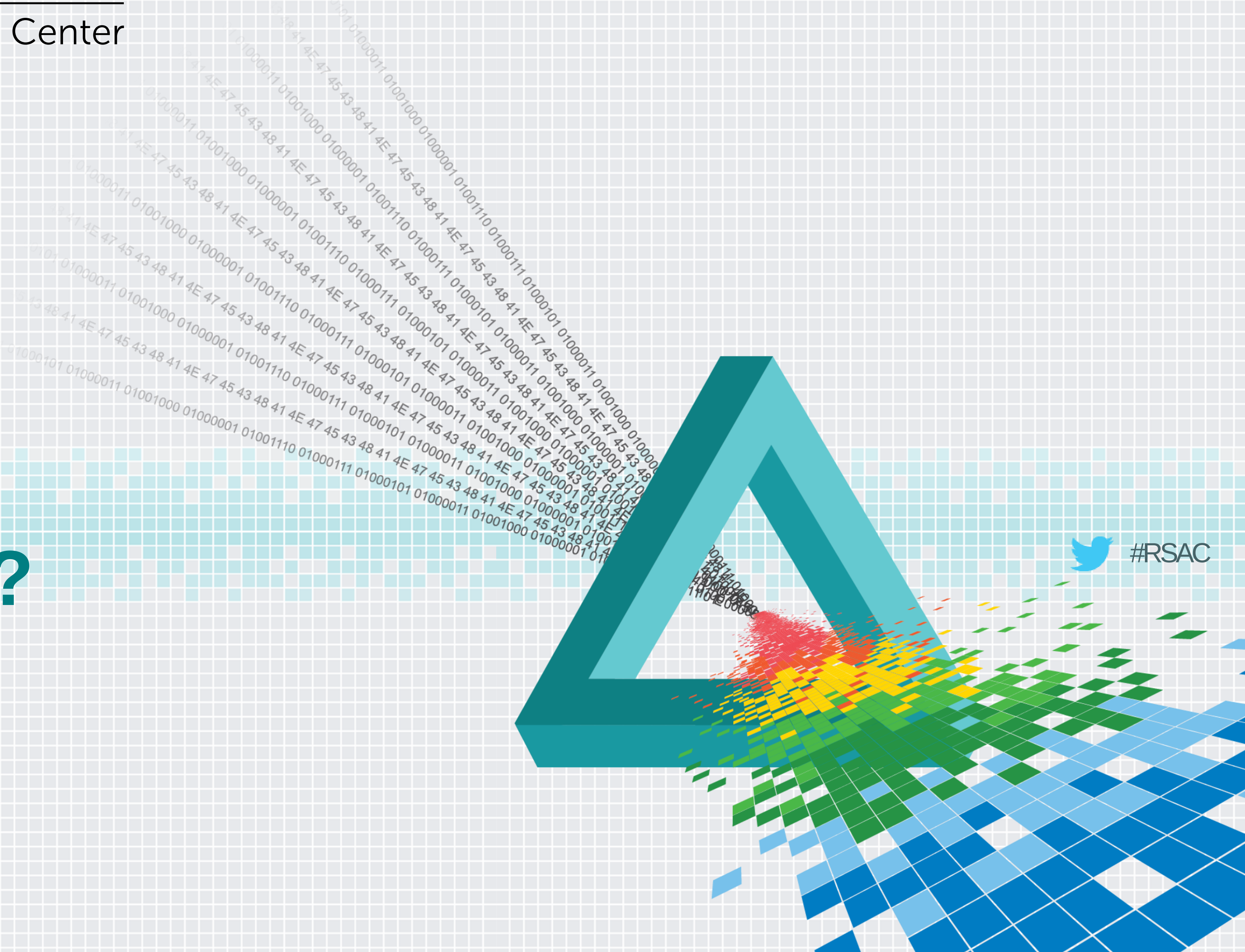
SNI support

End user requests that support the SNI extension

RSAConference2015

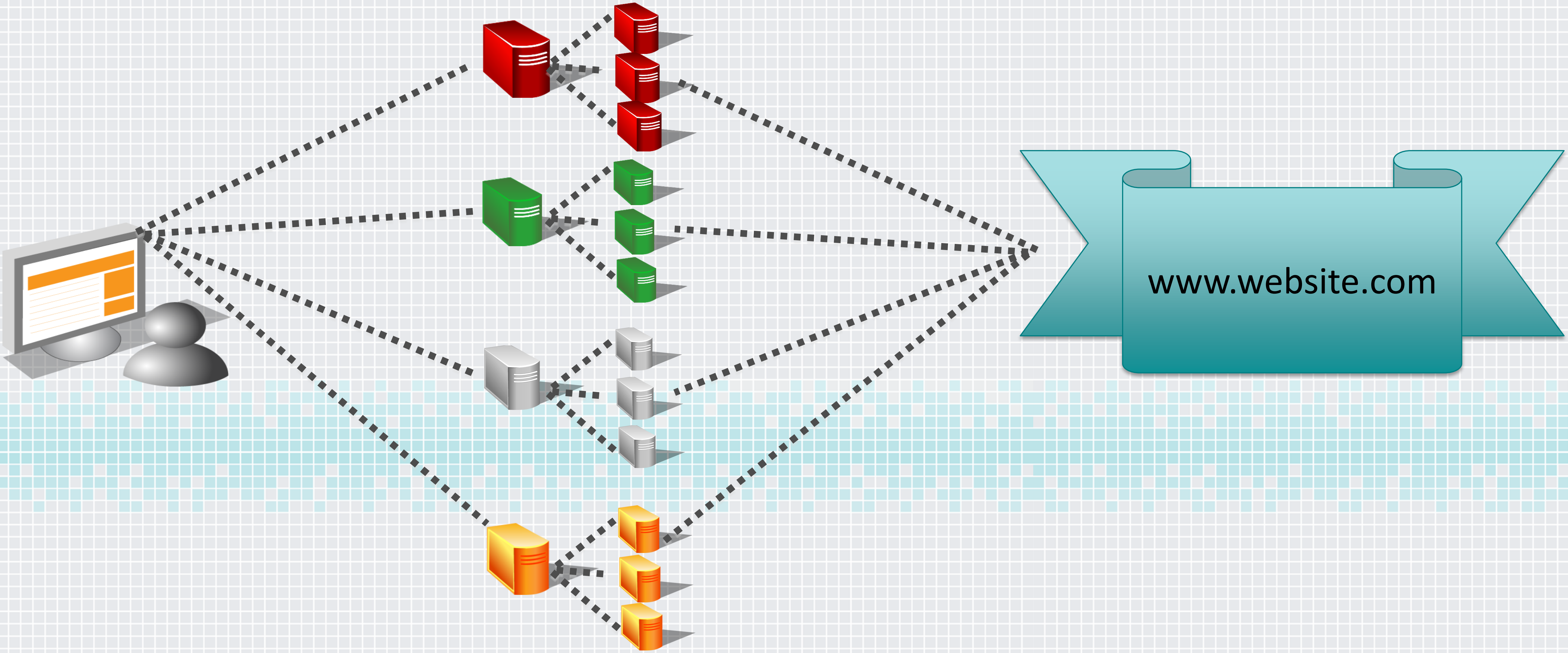
San Francisco | April 20-24 | Moscone Center

Who do you trust?
(The CAs)



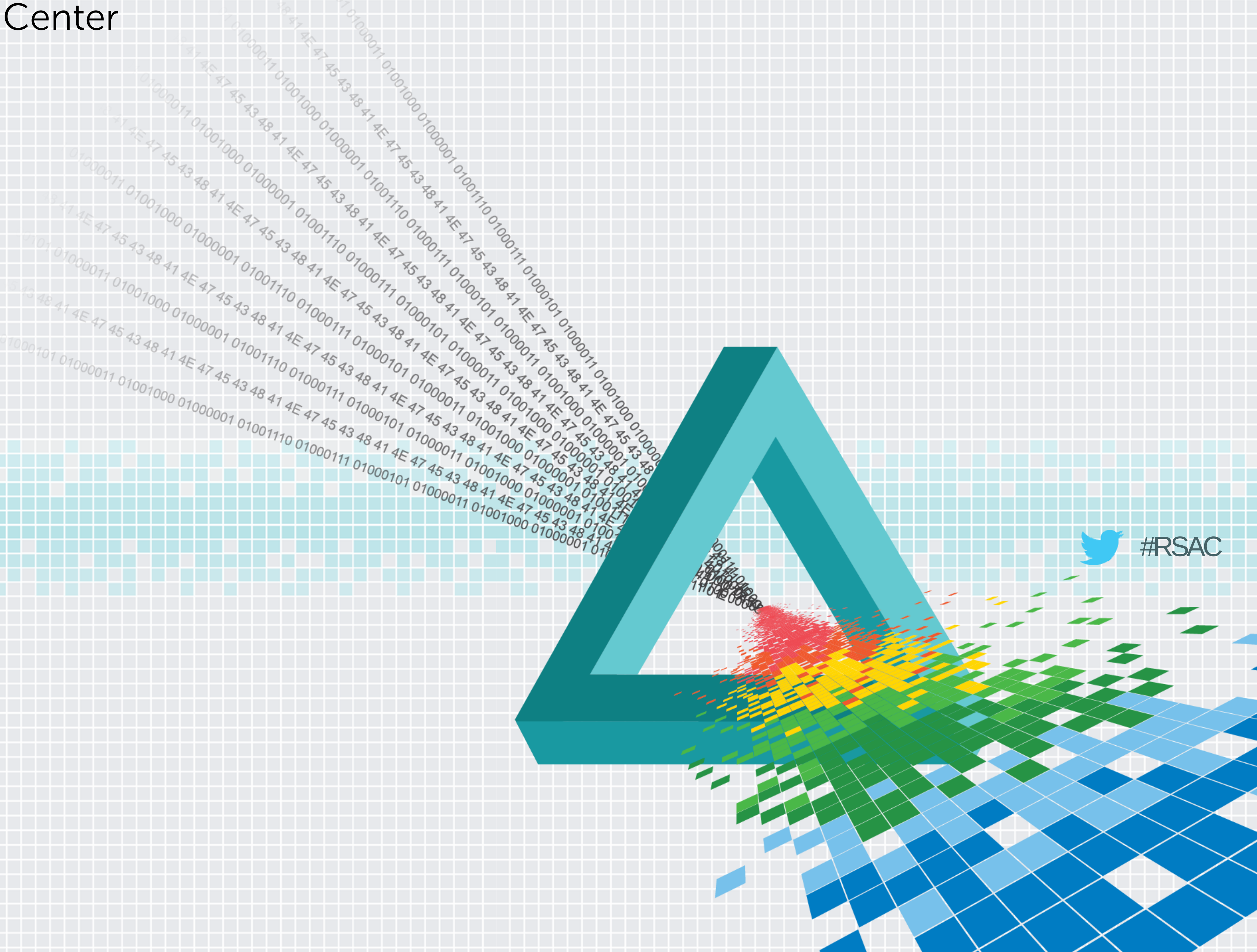
#RSAC

TLS roots of trust: Certificate Authorities



RSAConference2015

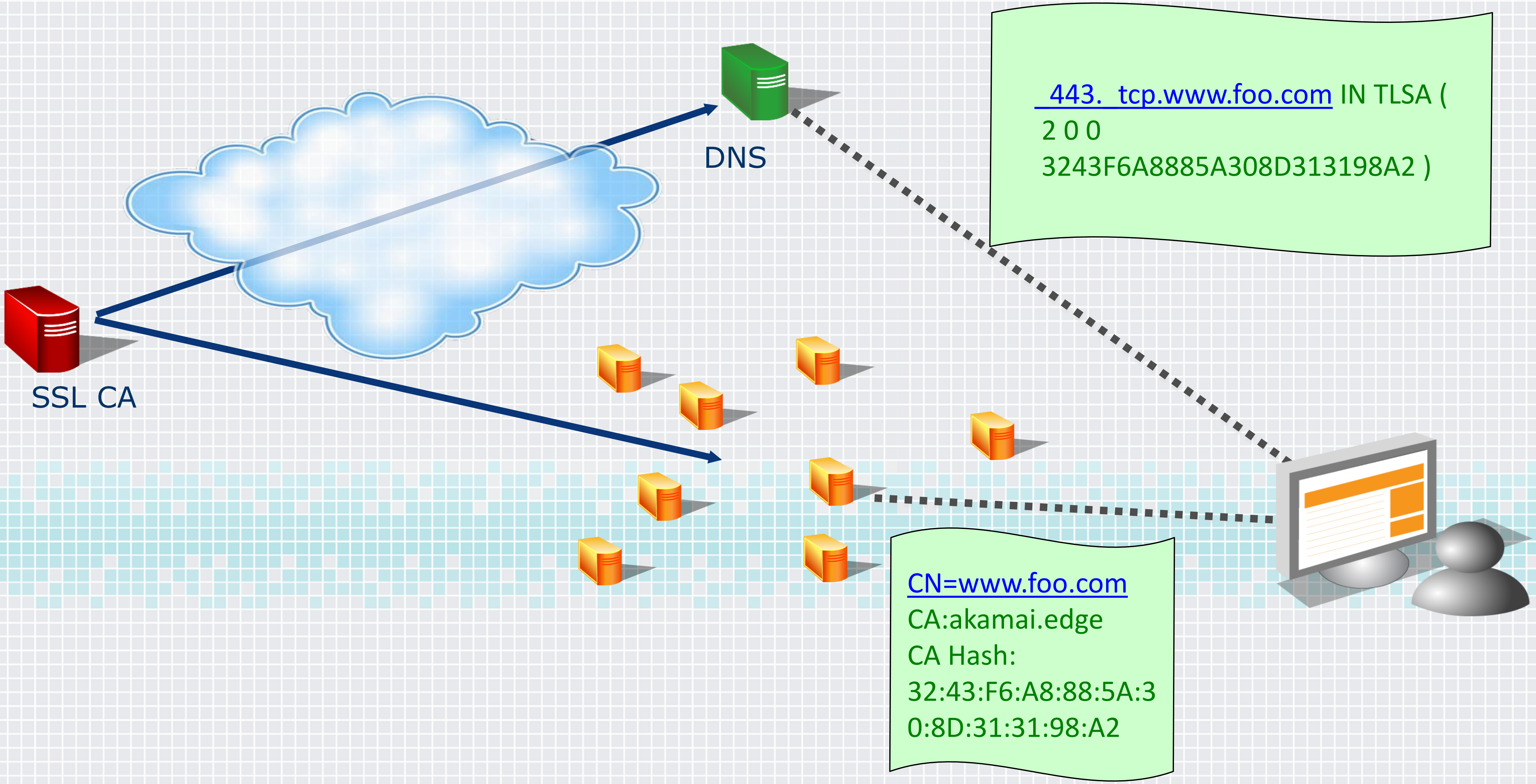
San Francisco | April 20-24 | Moscone Center



#RSAC

Evolving the CAs

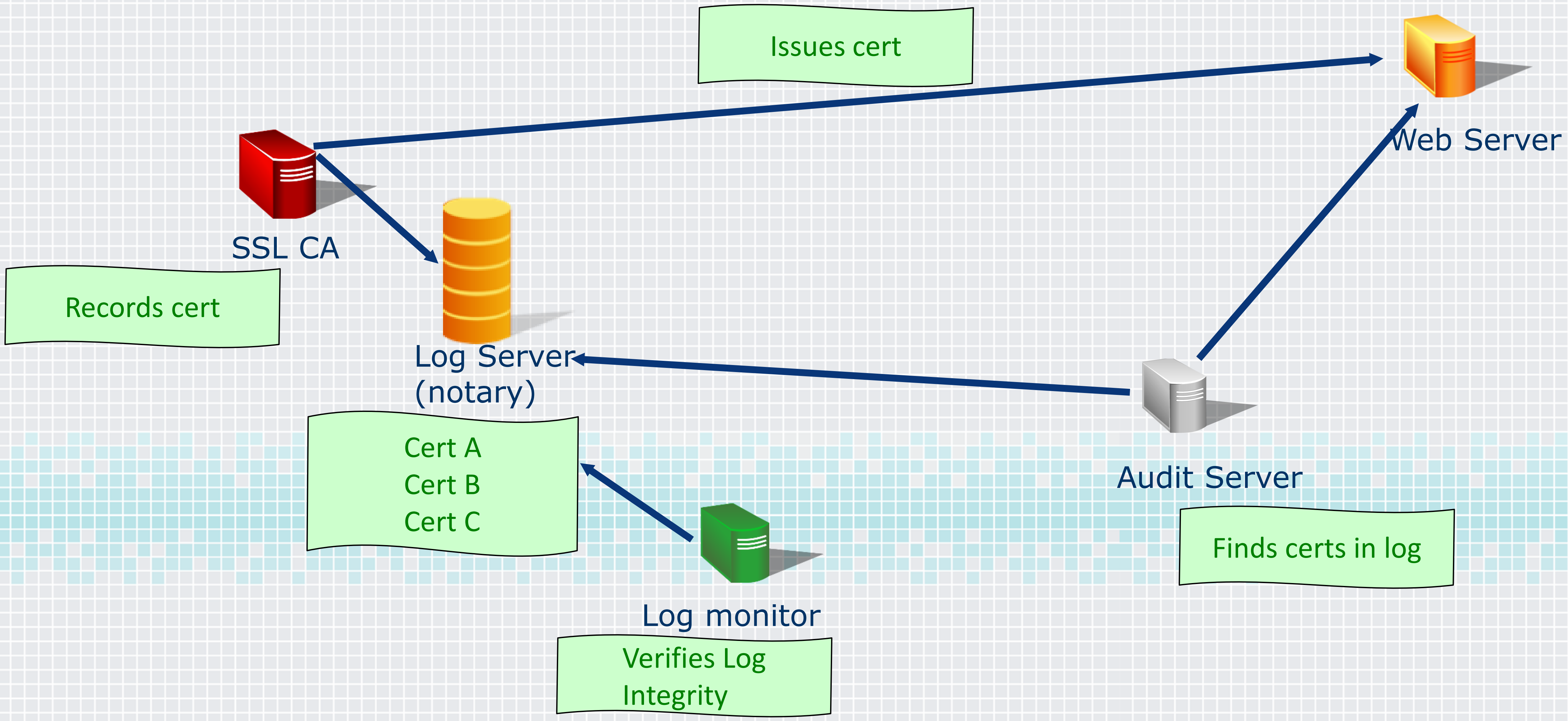
DANE



_443._tcp.www.foo.com IN TLSA (
2 0 0
3243F6A8885A308D313198A2)

CN=www.foo.com
CA:akamai.edge
CA Hash:
32:43:F6:A8:88:5A:3
0:8D:31:31:98:A2

Certificate Transparency



Issues cert

Web Server

SSL CA

Records cert

Log Server (notary)

Cert A
Cert B
Cert C

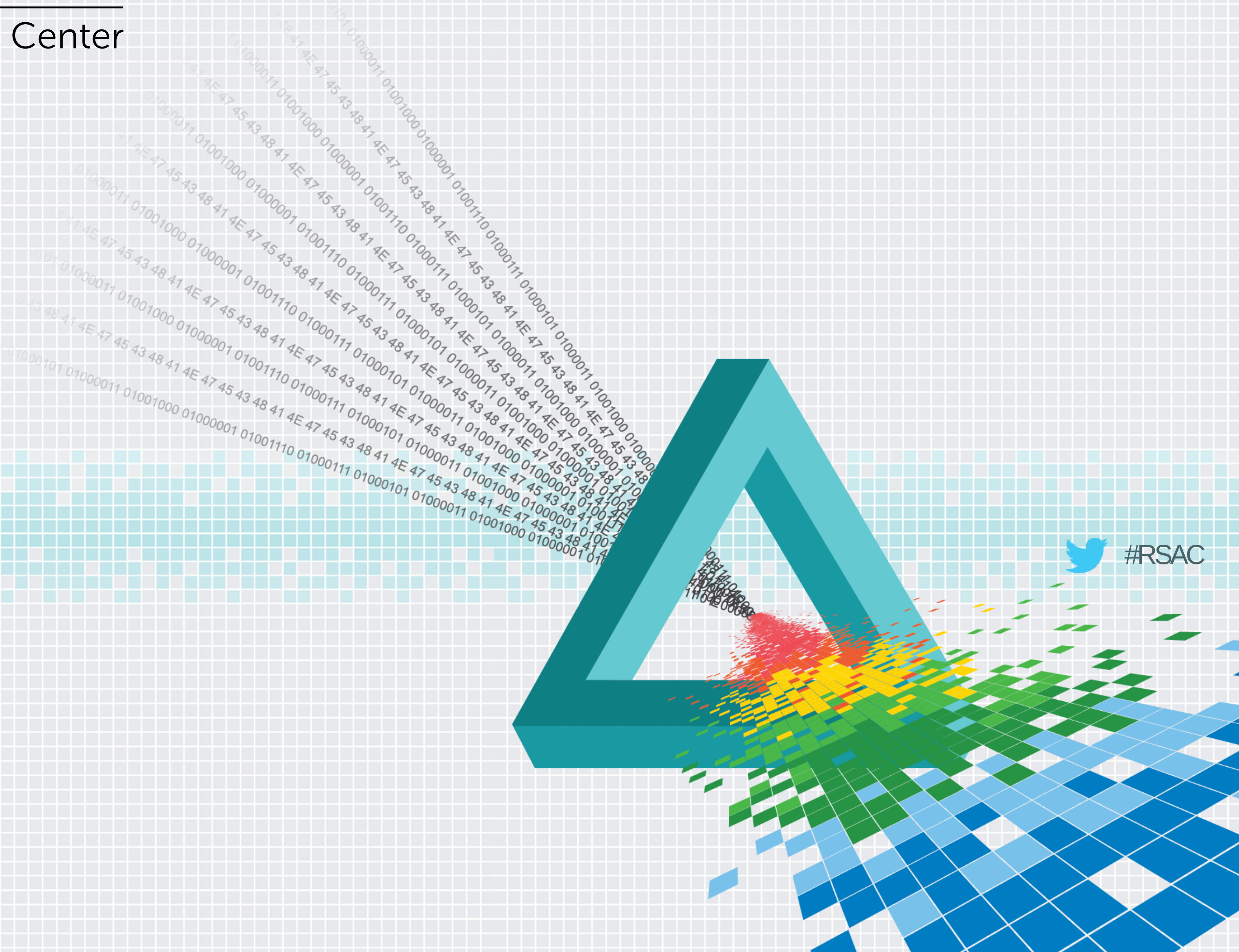
Audit Server

Finds certs in log

Log monitor

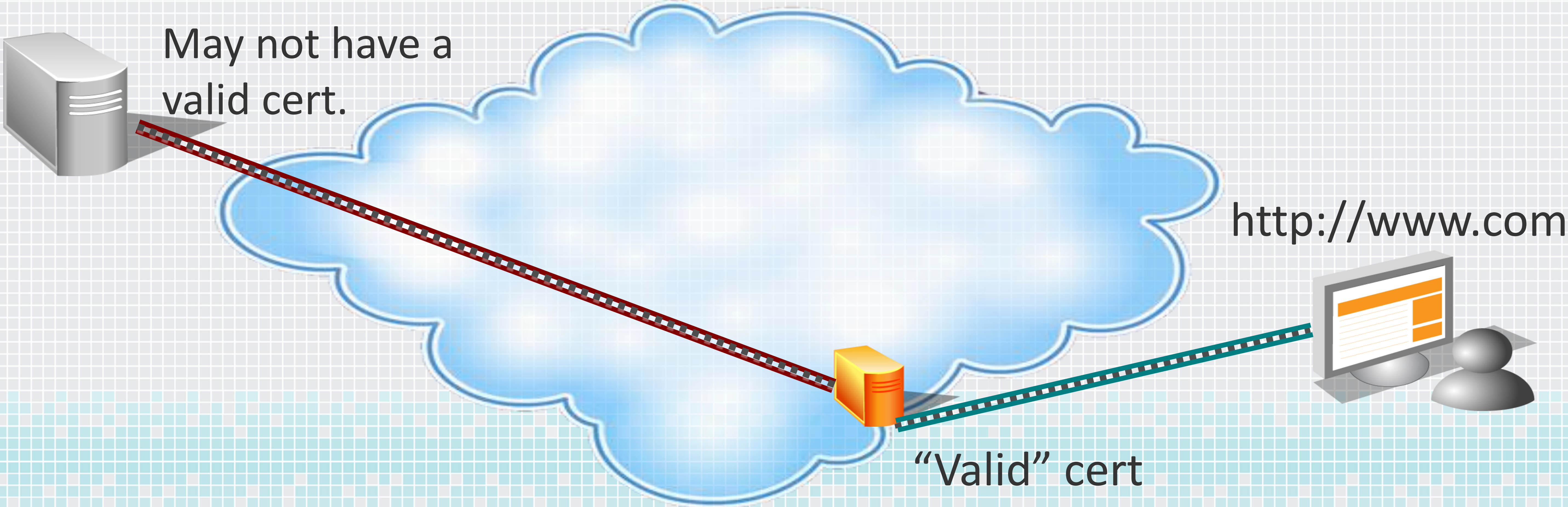
Verifies Log Integrity

The TLS proxy



#RSAC

Proxy (in)validation

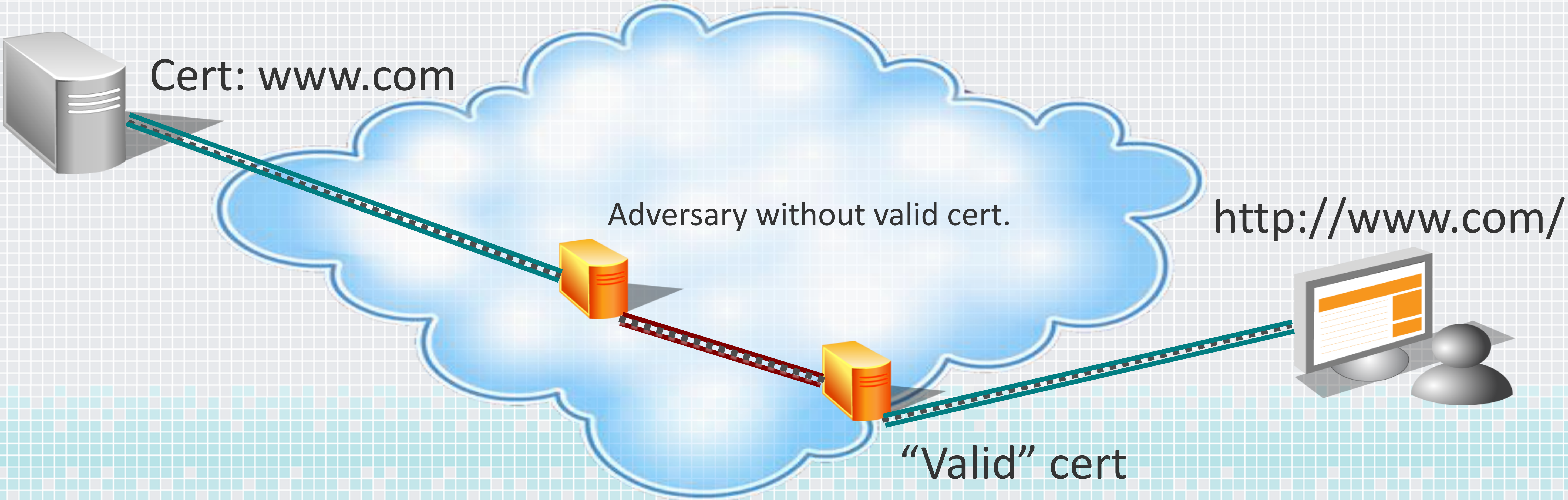


May not have a valid cert.

http://www.com/

“Valid” cert

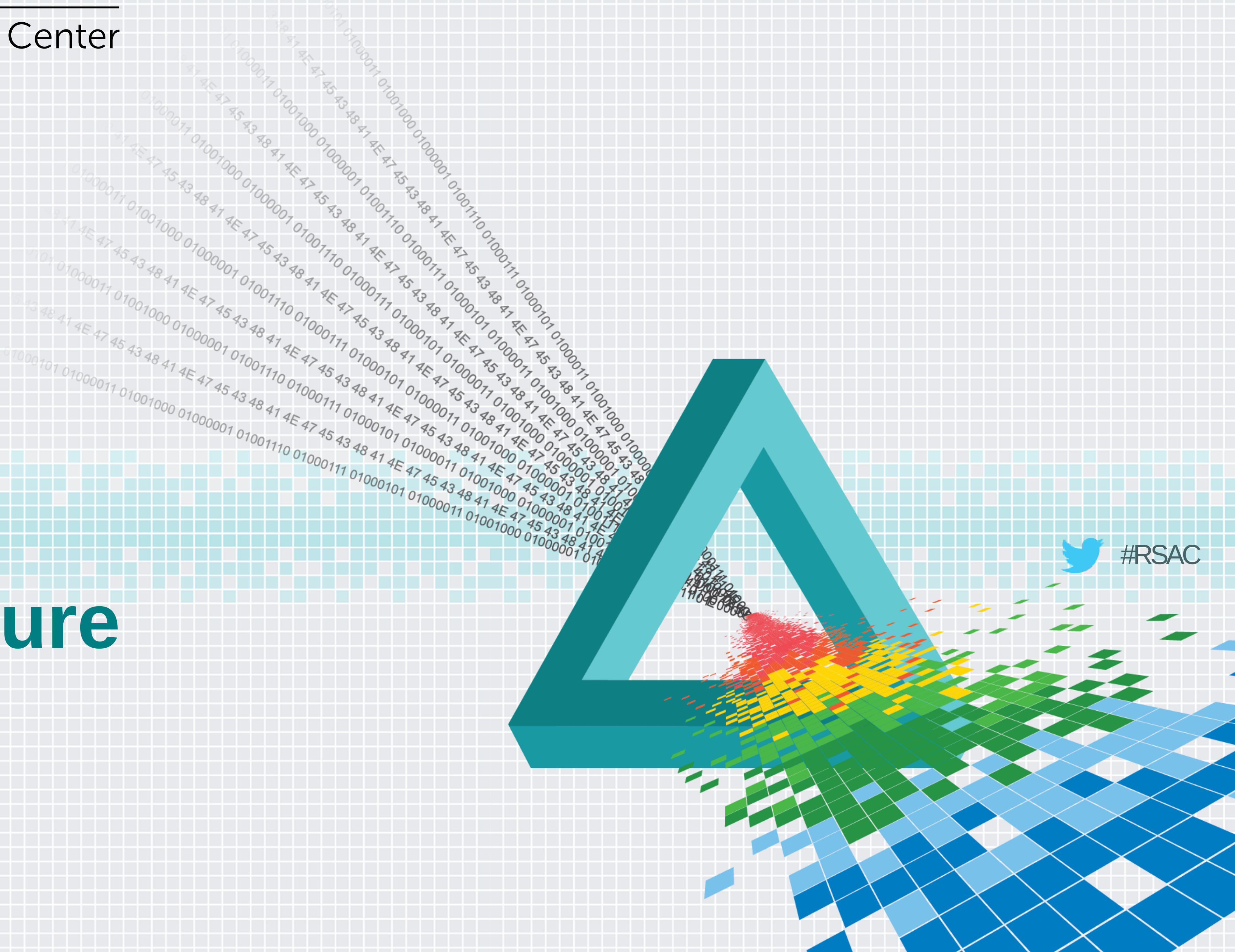
Opportunistic MitM



RSAConference2015

San Francisco | April 20-24 | Moscone Center

Looking to the future



#RSAC

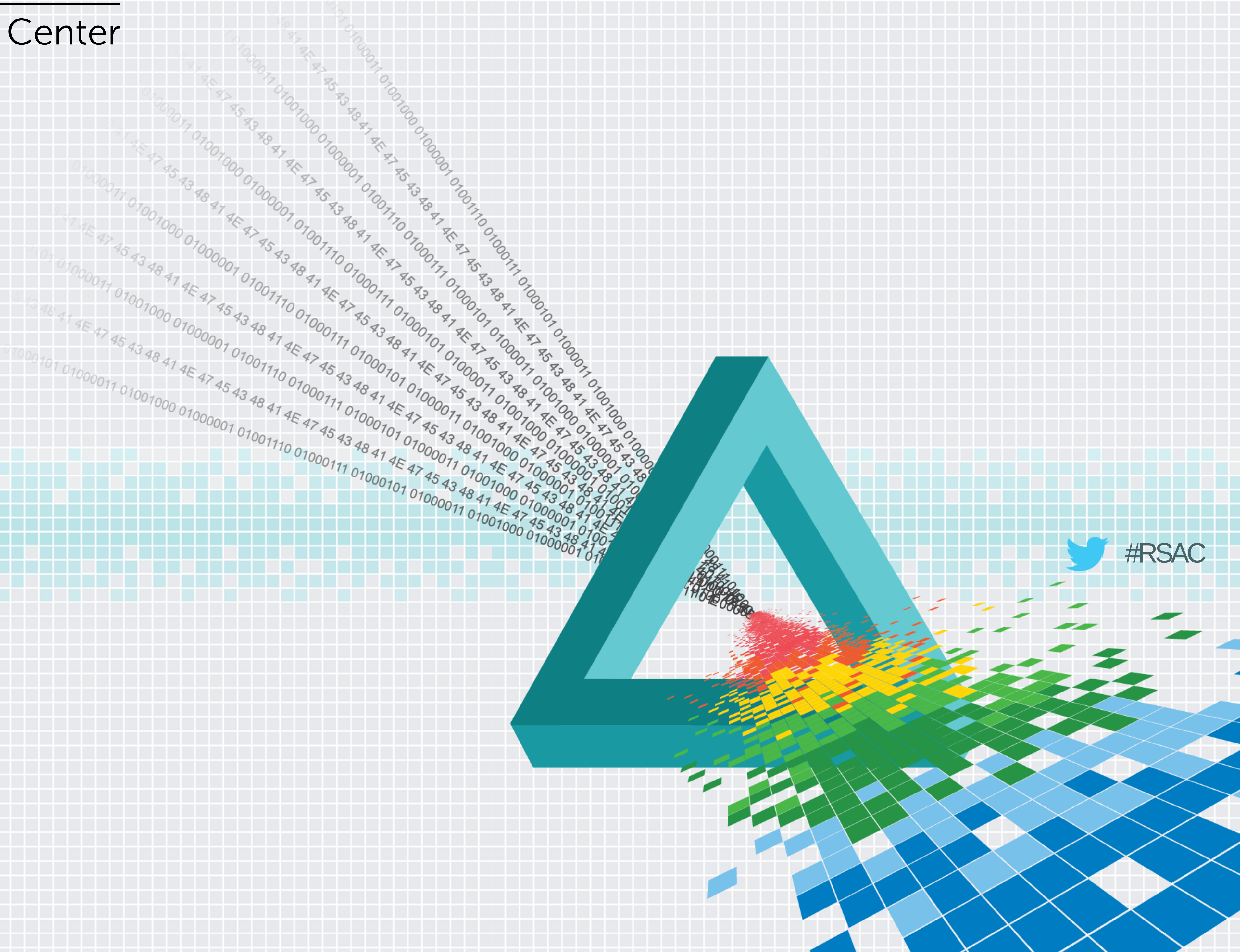
Apply

- Tactical
  - Move to TLS
  - Continue deprecating bad encryption
  - Move to SNI & IPv6
- Strategic
  - Think about privacy as a goal
  - Engage in safety analysis

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Thank You!



#RSAC