# Fixing OCSP for Fun and Profit

David Adrian
@davidcadrian



### OCSP Is Unreliable

Certificate revocation doesn't work.

CRLs are too big and slow.

CRLSets are too small.

OCSP is slow / unreliable / fails open / leaks visited domains.

OCSP stapling is fail open.

### Solutions

OCSP Must-Staple is too scary. Web servers are bad at stapling.

Chrome Expect-Staple preload list is only useful for measurement papers.

What to do? How do we really solve revocation?

# Gamification!

## OCSP Suspect-Staple

Client and server guess if web server will correctly staple

Commit to guess in Client/ServerHello

Incentivize servers to staple

Gamification!

#### Client Hello: client random, H(random + Sc)

**Server Hello**: server random, H(random + S<sub>s</sub>)

LSB 1 = Yes

Certificate: certificate chain (public key *PK*)

LSB 0 = No

Certificate Status?: OCSP response

Client Key Exchange: Encryptpk(premaster secret),



K<sub>ms</sub>:= KDF(premaster secret, client random, server random)

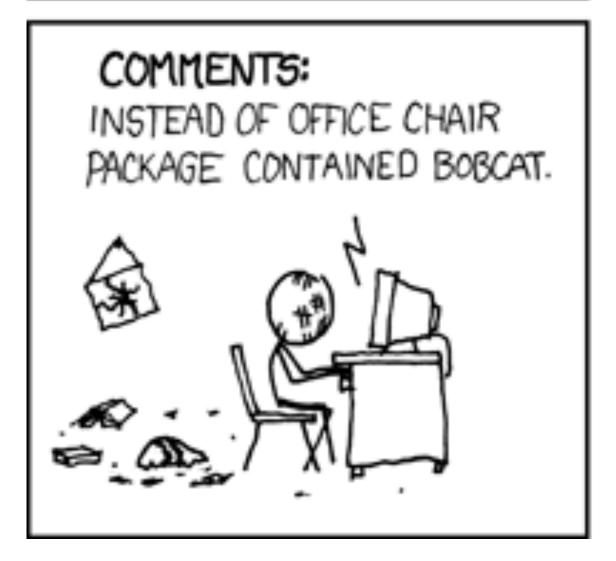
Client Finished: E<sub>Kms</sub>(Hash(m1 | m2 | ...)), S<sub>c</sub>

Server Finished: E<sub>Kms</sub>(Hash(m1 | m2 | ...)), S<sub>s</sub>











	Client: Yes Server: Yes	Client: Yes Server: No	Client: No Server: Yes	Client: No Server: No
Server Staples			Server sends client ( a bobcat	Client sends server candy
Server Does Not Staple	Client sends server a bobcat		Server sends client candy	

Coming to an IETF standard near you!

# Fixing OCSP for Fun and Profit

David Adrian
@davidcadrian

