SCION
ELEVATING SECURE COMMUNICATION

TRUST & WEBSITE CERTIFICATION

Prof. Prateek Mittal

Princeton University
USA

SCION ASSOCIATION · ETH zürich · ANAPAYA · eraneos · satw technology for society

Securing Internet Domain Validation with Multi-VA and SCION

Prateek Mittal
Princeton University

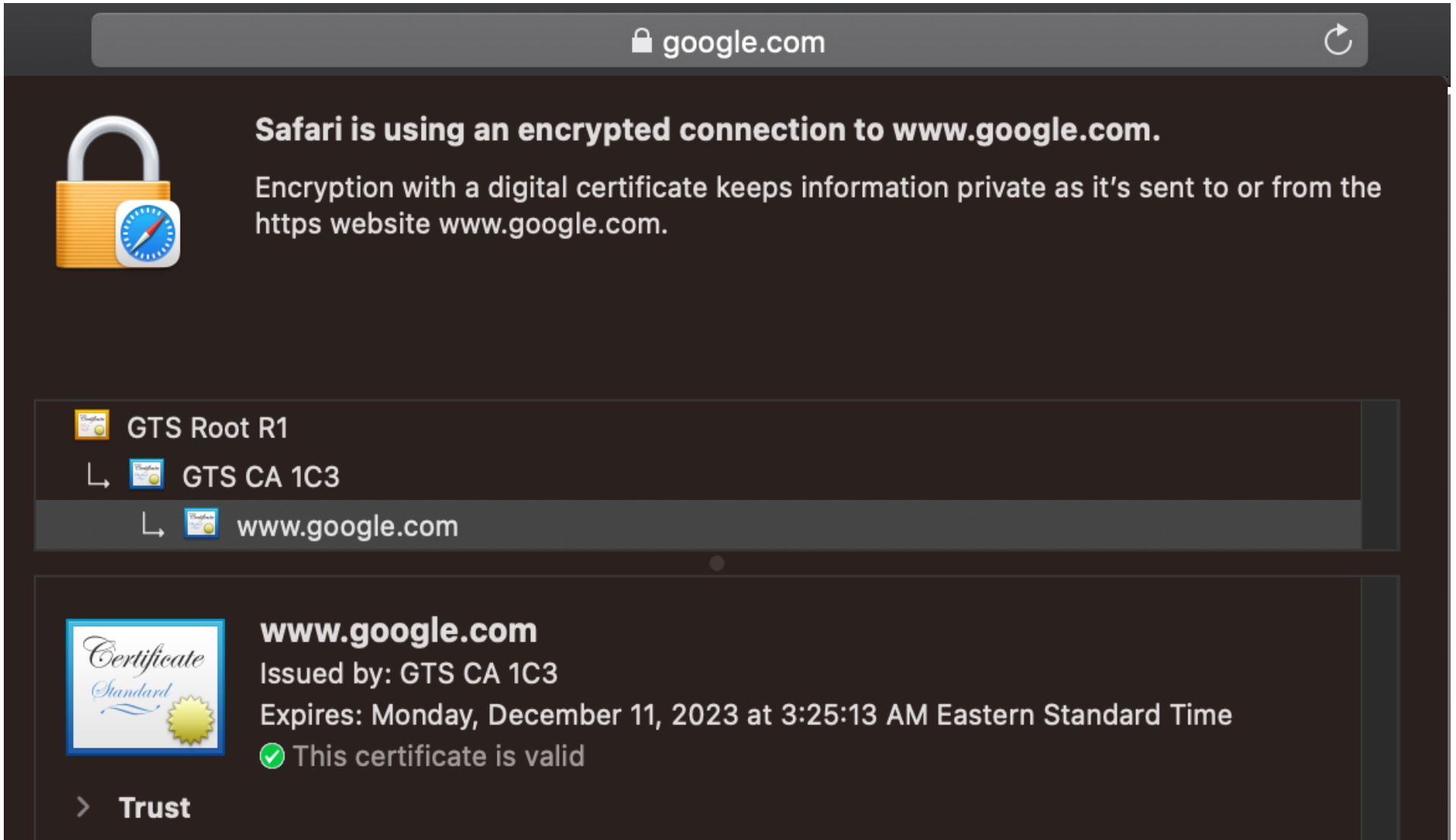
Joint work with Henry Birge-Lee, Grace Cimaszewski,
Liang Wang, Jennifer Rexford, Adrian Perrig

Status Quo: Insecurity in Internet Routing

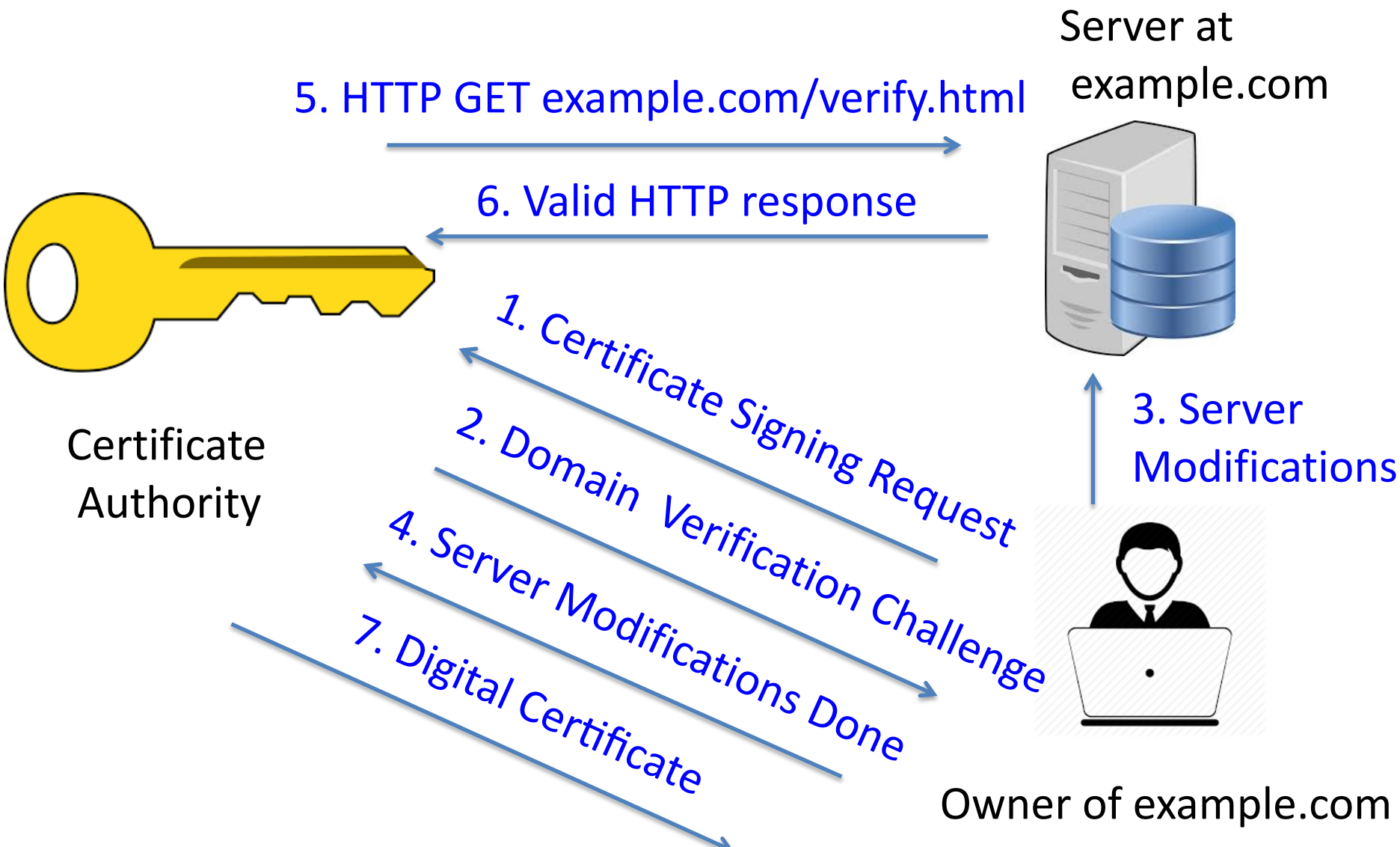
1. Border Gateway Protocol (BGP) is vulnerable to routing attacks.

2. Routing attacks can have critical consequences for Internet applications (e.g.,domain validation, crypto-currencies)

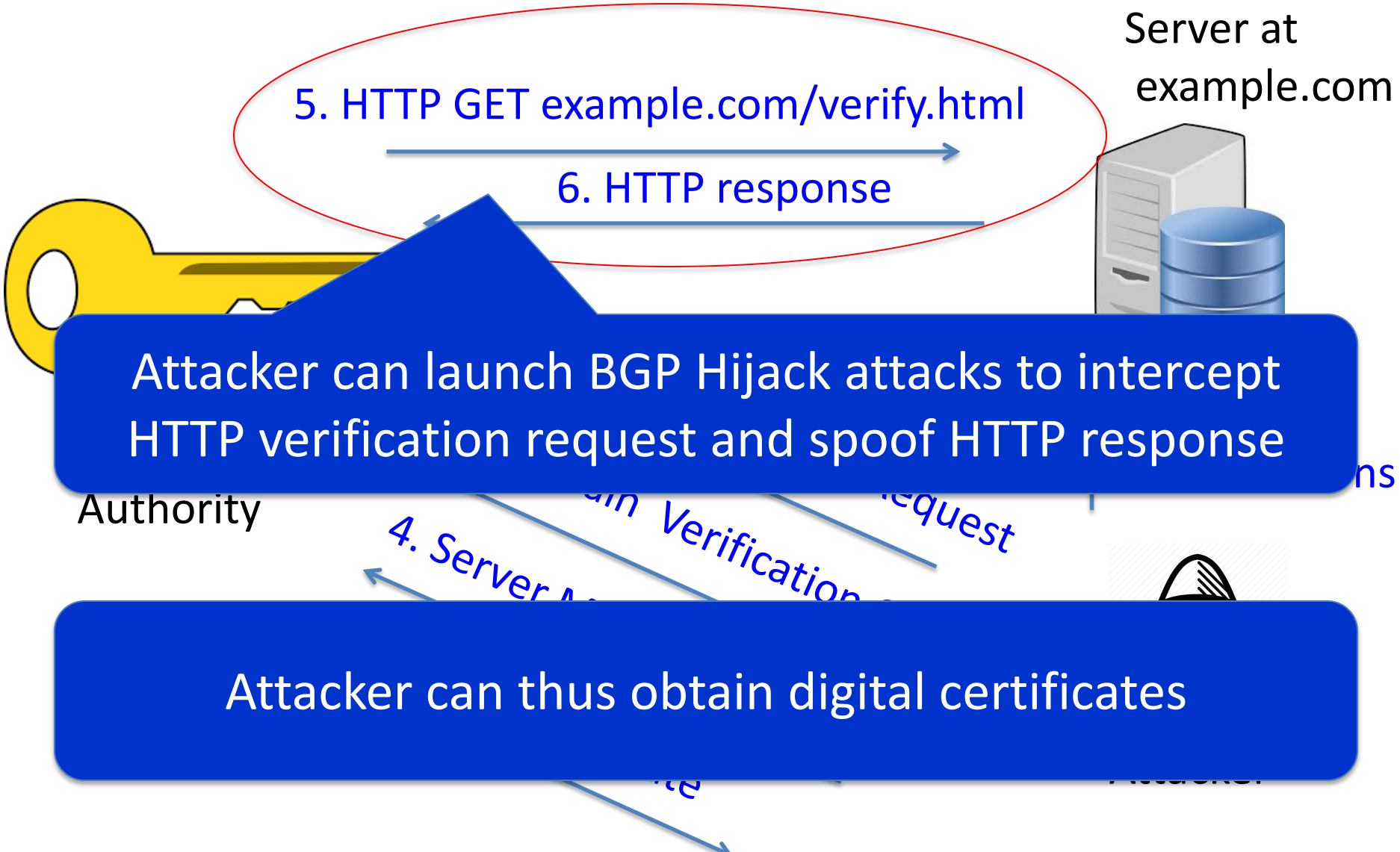
Digital Certificates are a root of trust for online communications (TLS/HTTPS)



How to get a digital certificate?
Domain Validation Protocol



Compromising Domain Validation via BGP Hijack Attacks (USENIX 2018)



Results from real (ethical) attacks

	Let's Encrypt	GoDaddy	Comodo	Symantec	GlobalSign
Time to issue	35 seconds	< 2 min	< 2 min	< 2 min	< 2 min
Vantage Points					
Validation Method Attacked	HTTP	HTTP	Email	Email	Email

All CAs are vulnerable: core foundations of Internet encryption are at risk due to BGP Dynamics

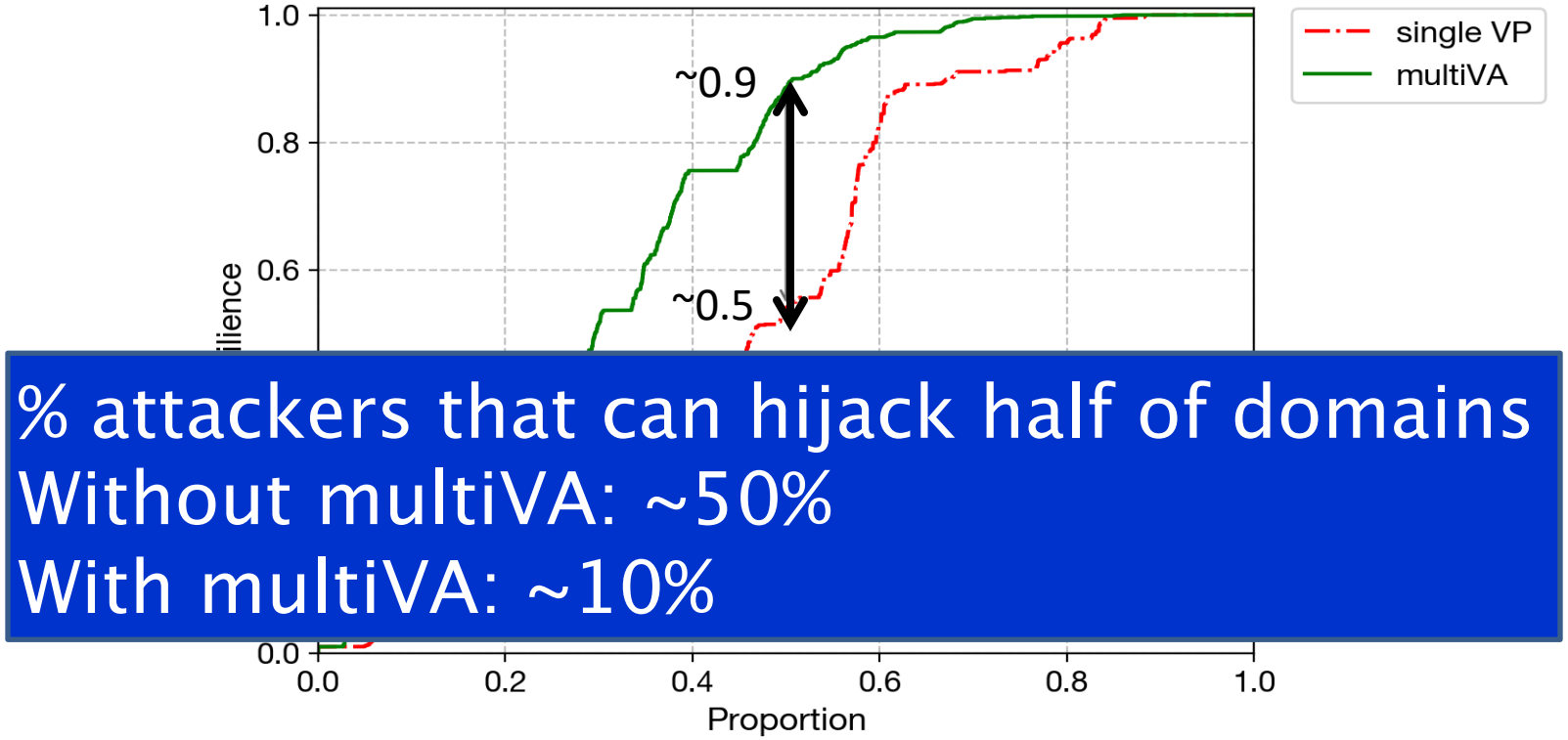
*At time of experiments Symantec was still a trusted CA

Countermeasure: Domain Validation via Multiple Vantage Points (USENIX 21)

Impact: real-world deployment of countermeasures at the Let's Encrypt CA, Google Trust Services, and CloudFlare

Impact: Our technology is supporting over 350 million websites with 2 billion+ certificates since 2020

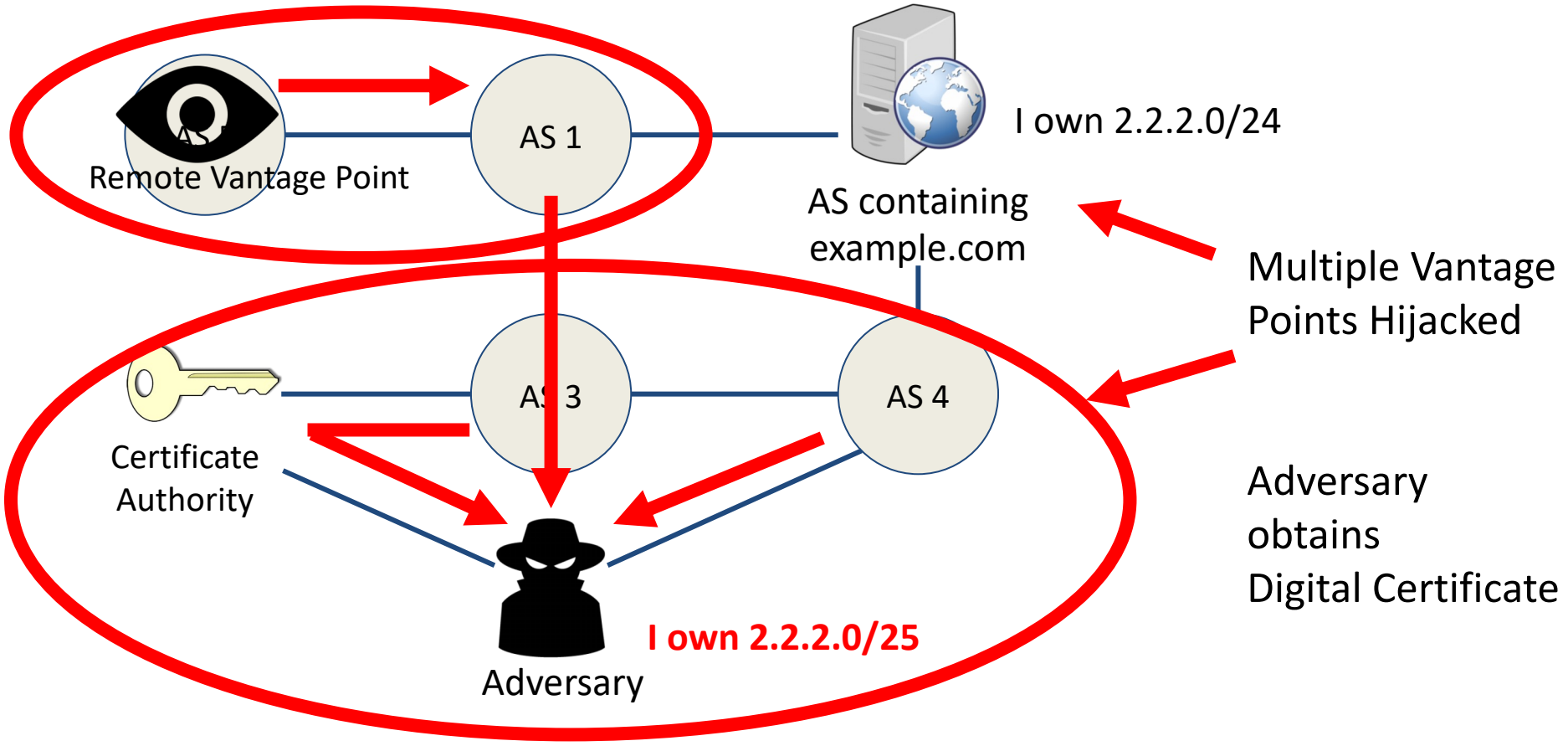
Multi-VA significantly increases resilience of Let's Encrypt against routing attacks (USENIX 23)



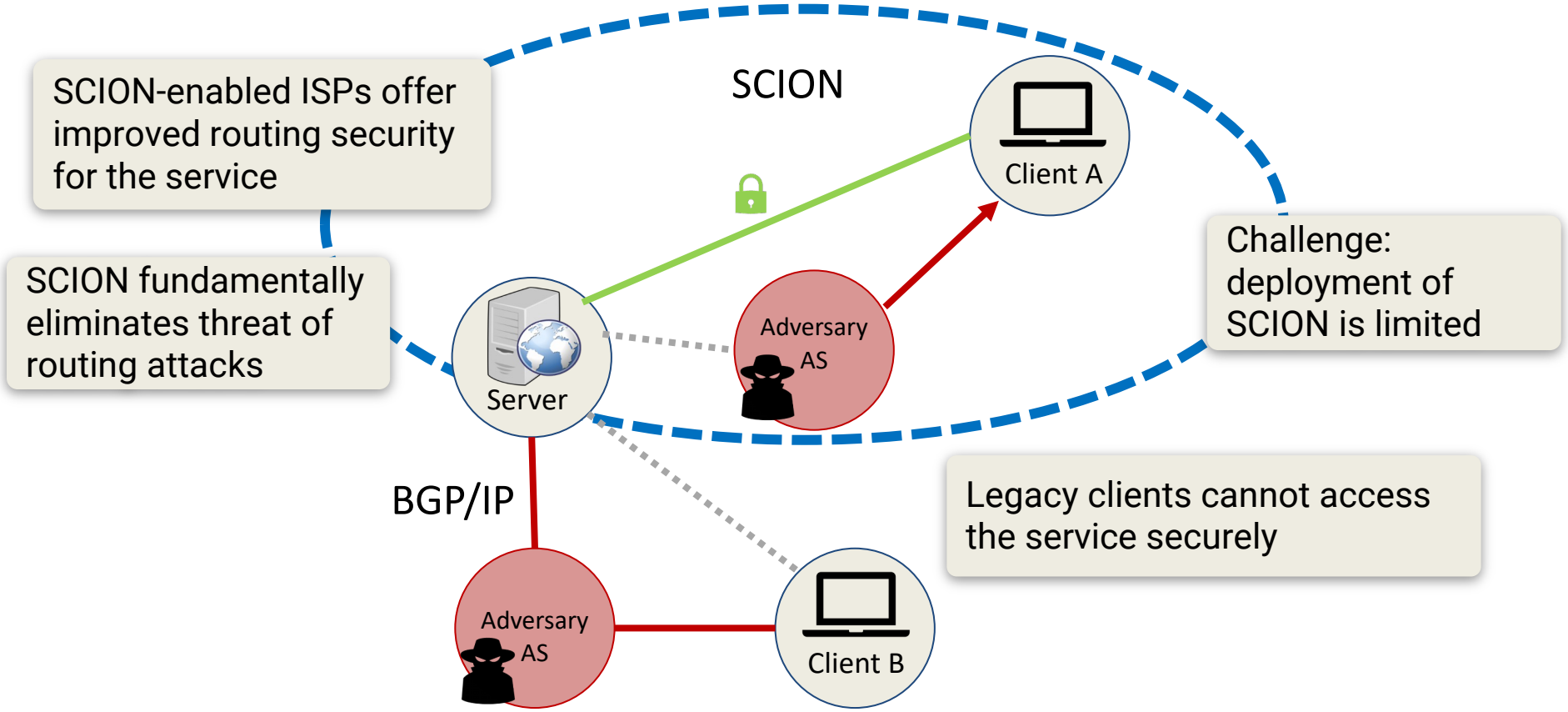
% attackers that can hijack half of domains
Without multiVA: ~50%
With multiVA: ~10%

Resilience: proportion of attackers that could NOT gain certificate for a domain using routing attacks

Challenge: How to guarantee that an attacker cannot hijack all vantage points?

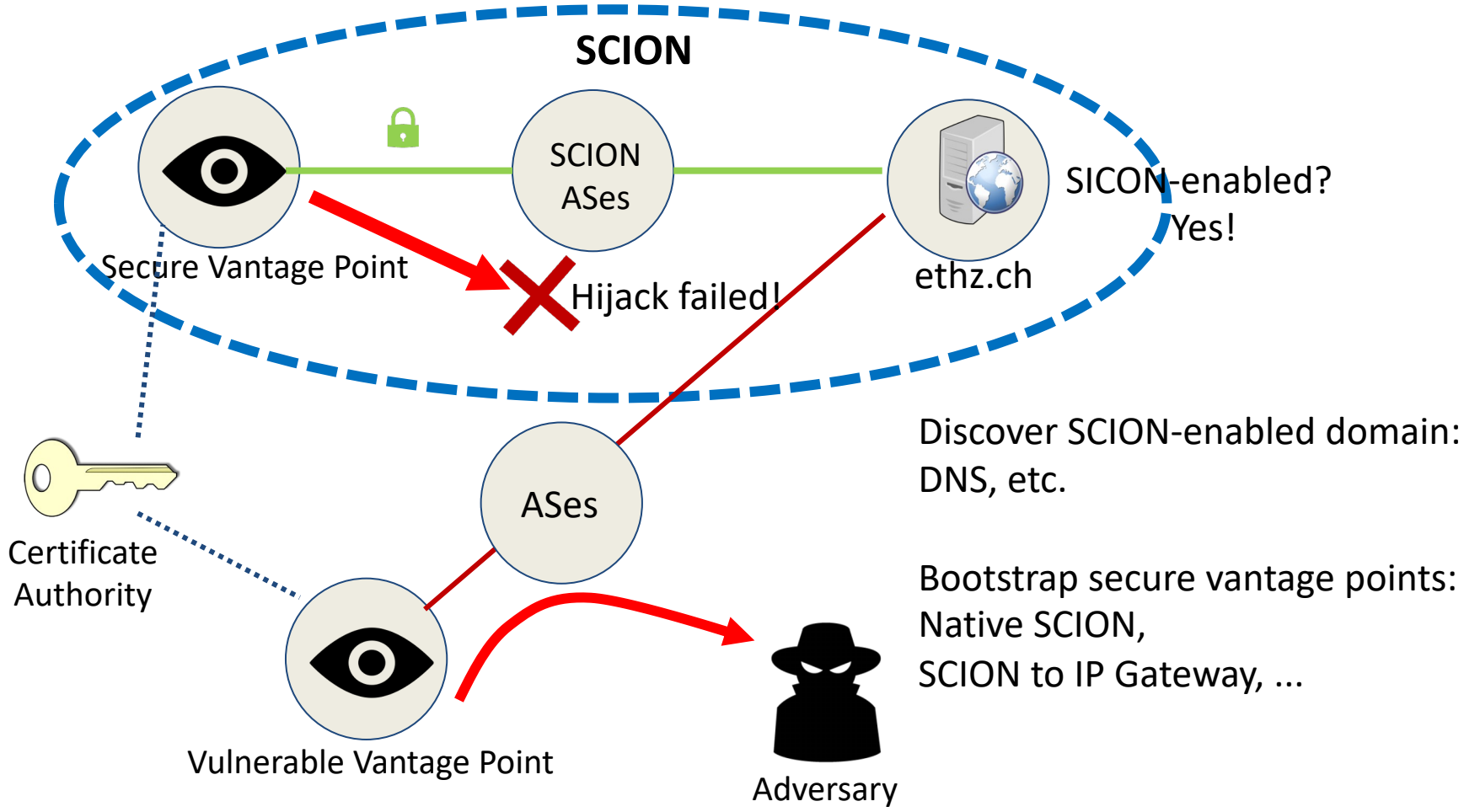


Insight: Leveraging Secure Backbones (e.g., SCION)



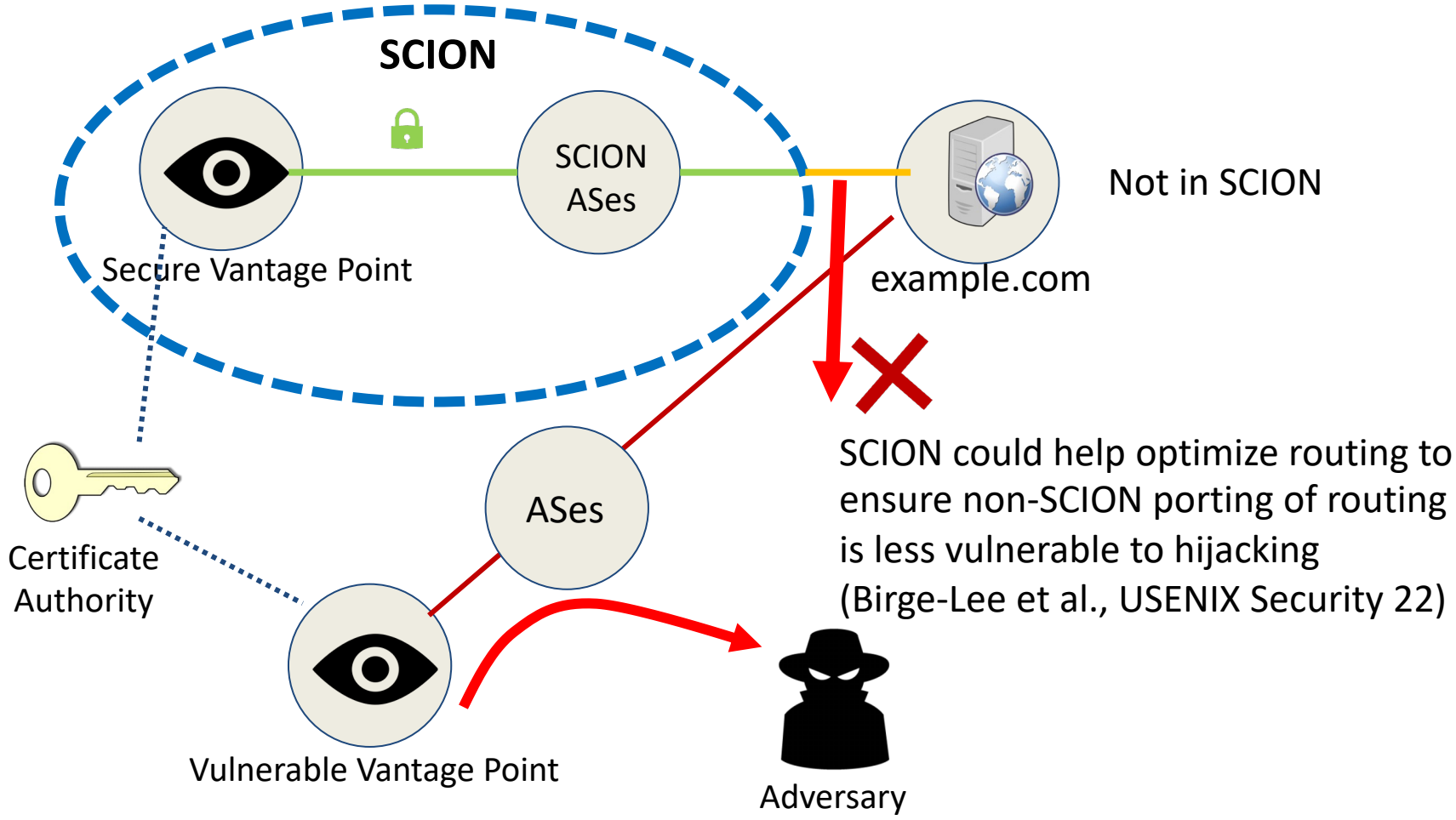
Question: Can we leverage SCION to enhance the security benefits of Multi-VA domain Validation?

Leverage SCION to secure Multi-VA



Combining Multi-VA and SCION provides cryptographic assurance for Domain Validation

Leverage SCION to secure Multi-VA



Multi-VA + SCION could also improve security for domain validation on Non-SCION hosts

Benefits of securing MultiVA with SCION

Cryptographic assurance for domain validation

Incrementally deployable

Potential performance/energy benefits offered by SCION