Multiple Vantage Point Domain Validation

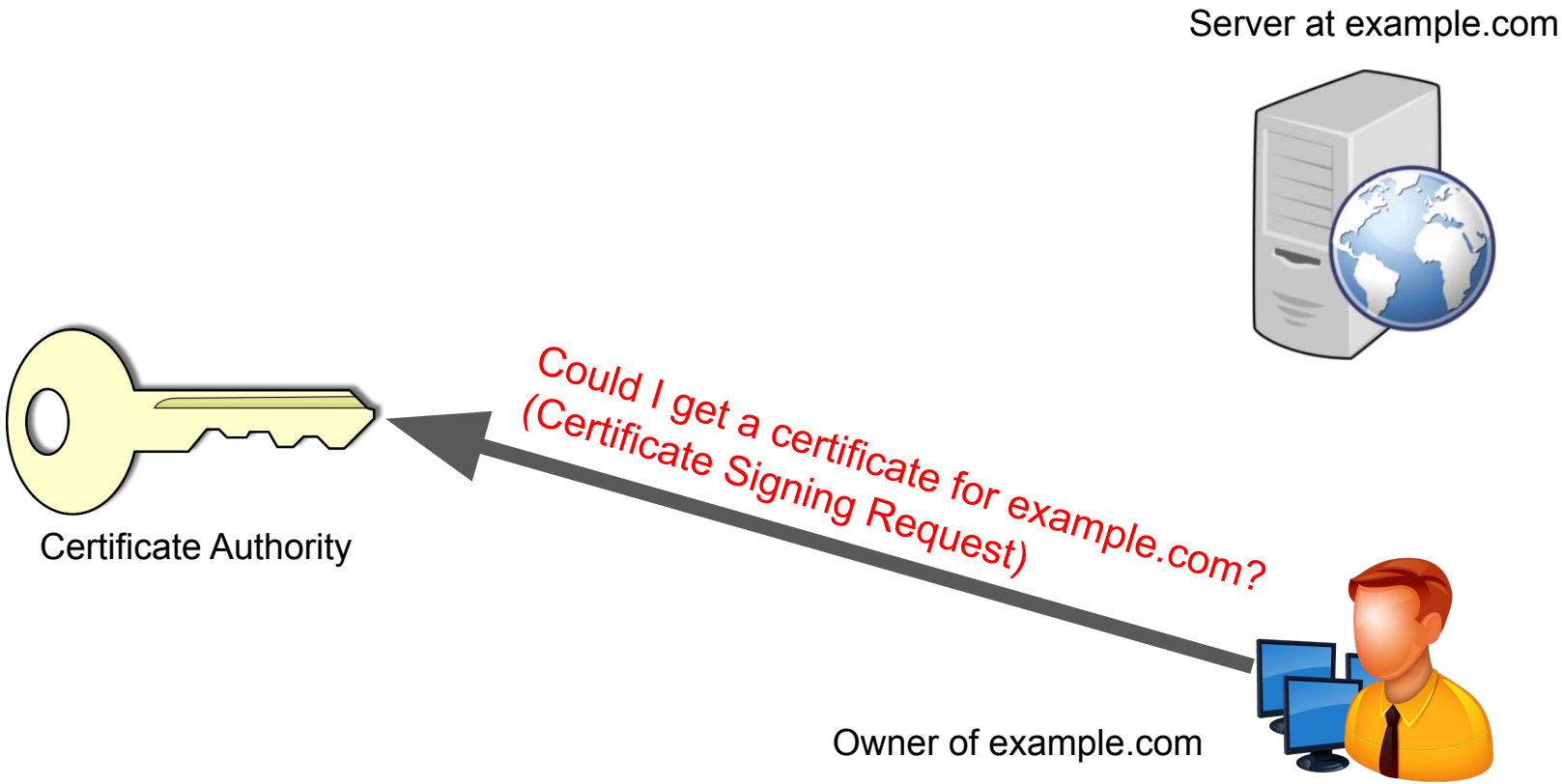
Henry Birge-Lee (Princeton University)

Remote Guest: Robert Danford (Salesforce)

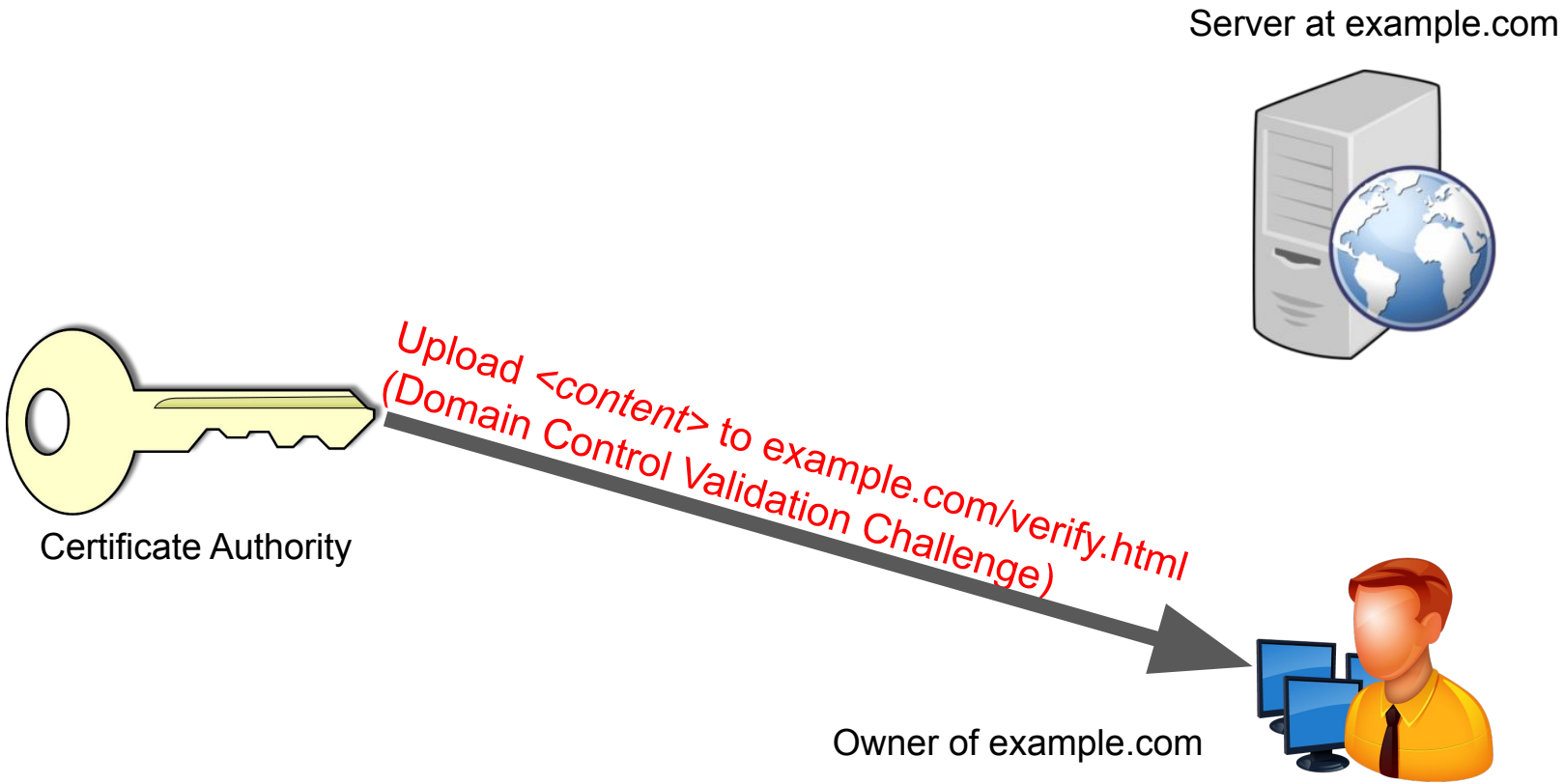
Overview

- How Domain Control Validation is Vulnerable
- Demo
- Real-world attacks
- How multiple vantage point validation works
- How effective it is
- Deployment and operational details

Domain Control Validation

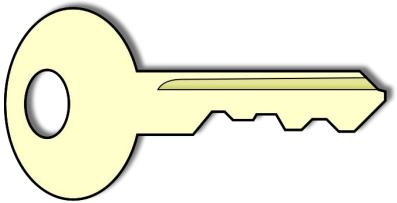


Domain Control Validation



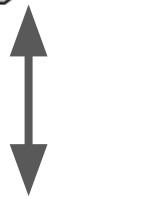
Domain Control Validation

Server at example.com



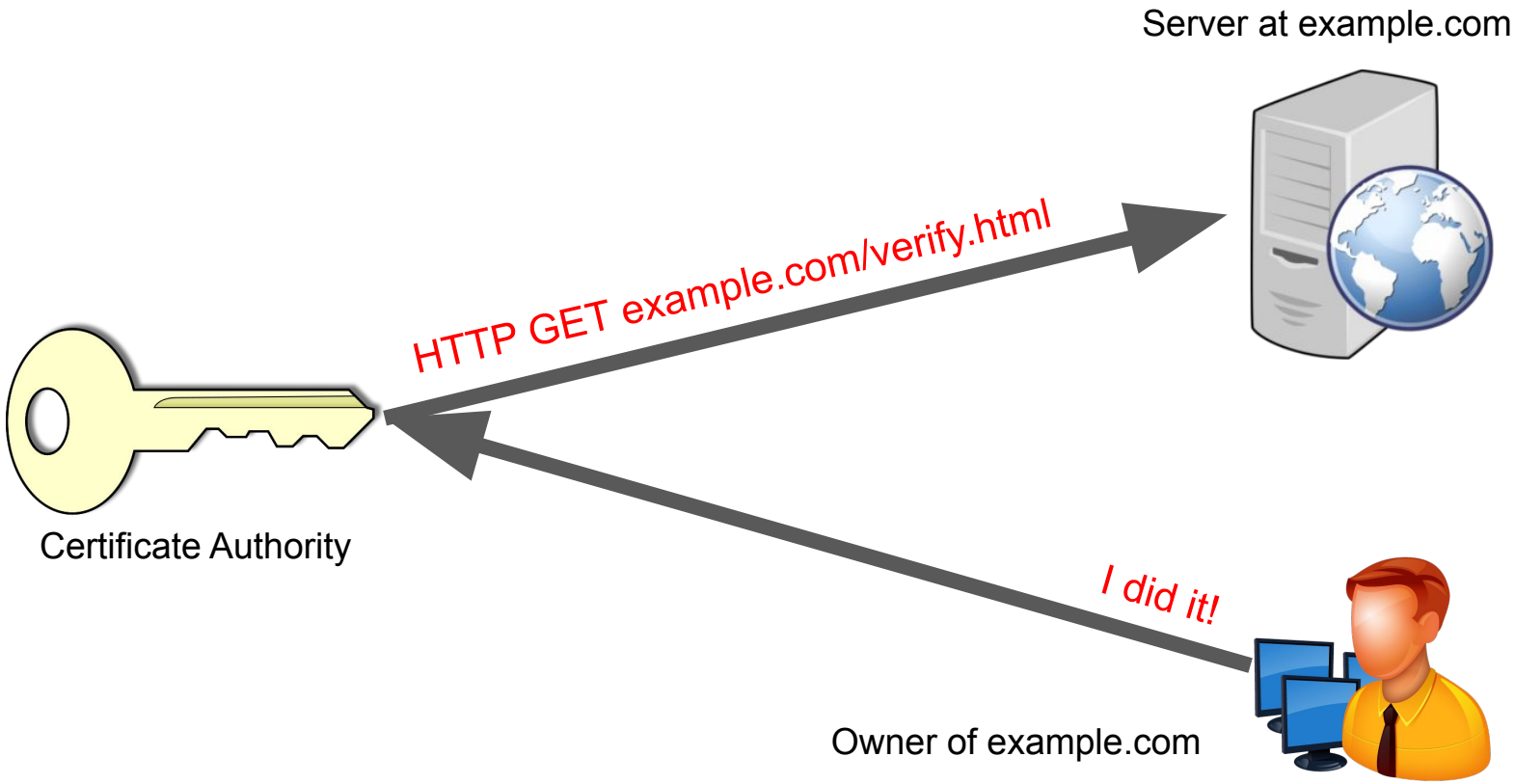
Certificate Authority

Server modifications

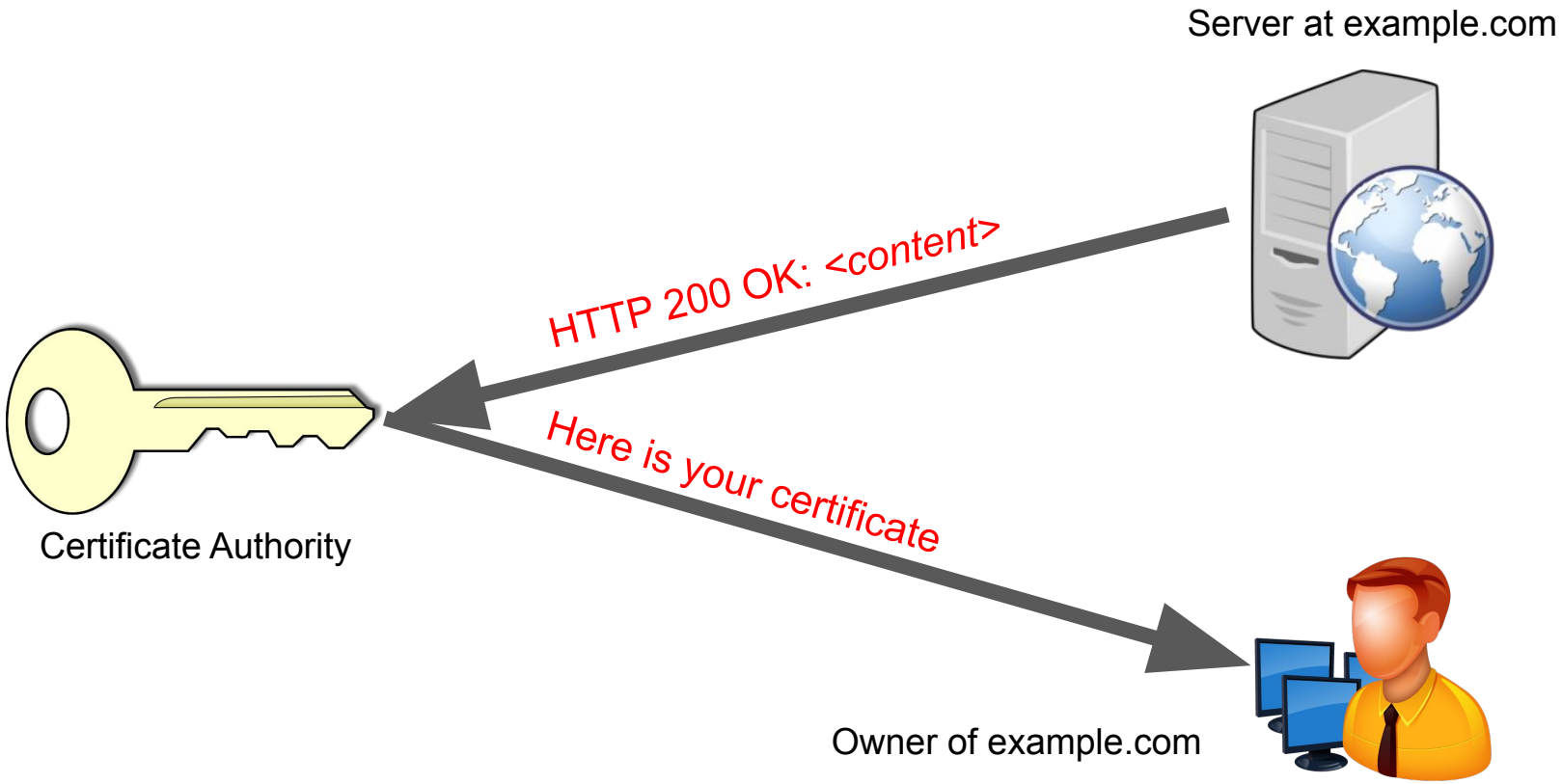


Owner of example.com

Domain Control Validation

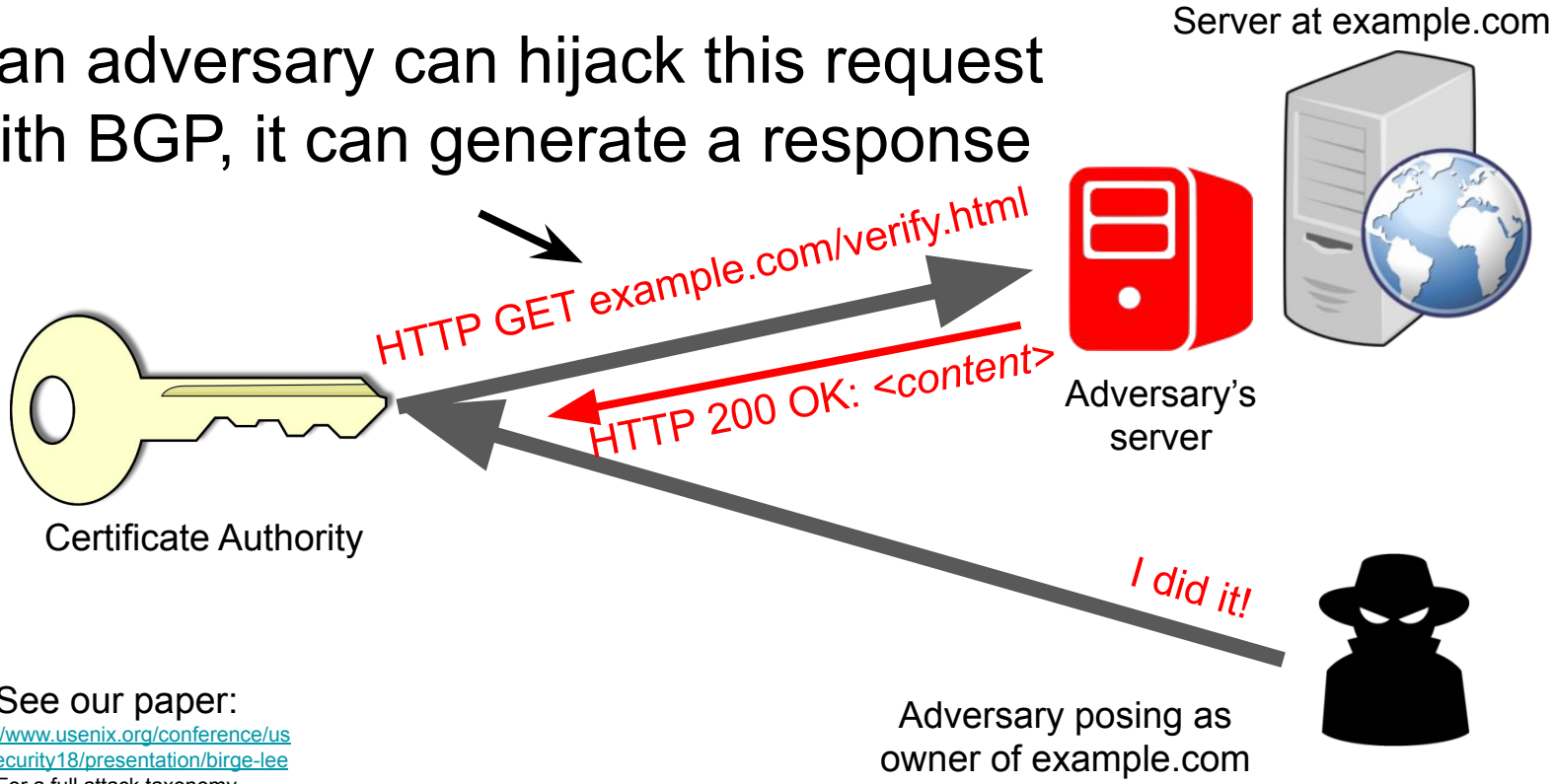


Domain Control Validation



BGP Attacks can Hijack Plaintext Validation Traffic

If an adversary can hijack this request with BGP, it can generate a response

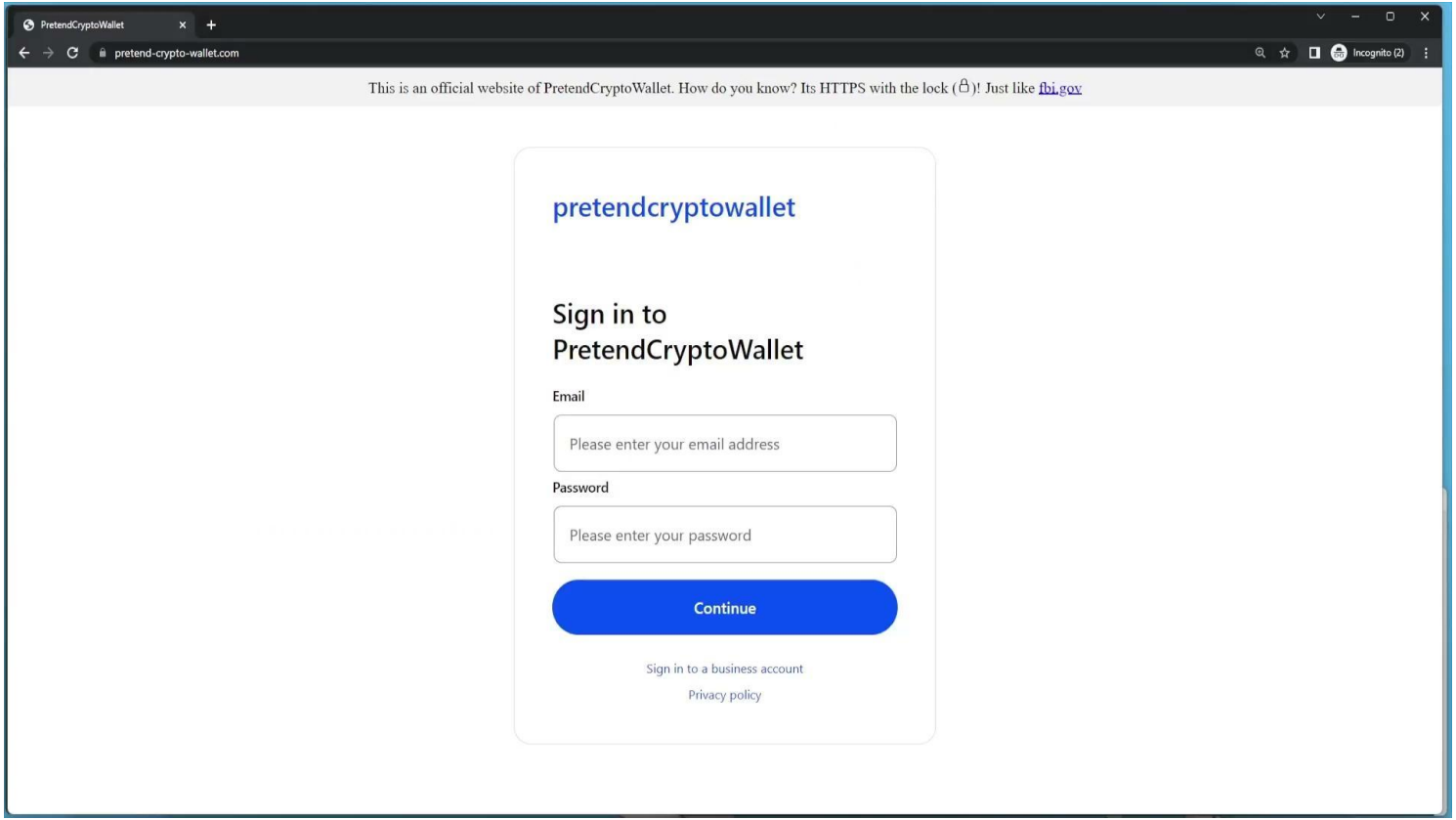


See our paper:
https://www.usenix.org/conference/usenixsecurity18/presentation/birge-lee
For a full attack taxonomy

Overview

- How Domain Control Validation is Vulnerable
- Demo
- Real-world attacks
- How multiple vantage point validation works
- How effective it is
- Deployment and operational details

Real-world demo



Overview

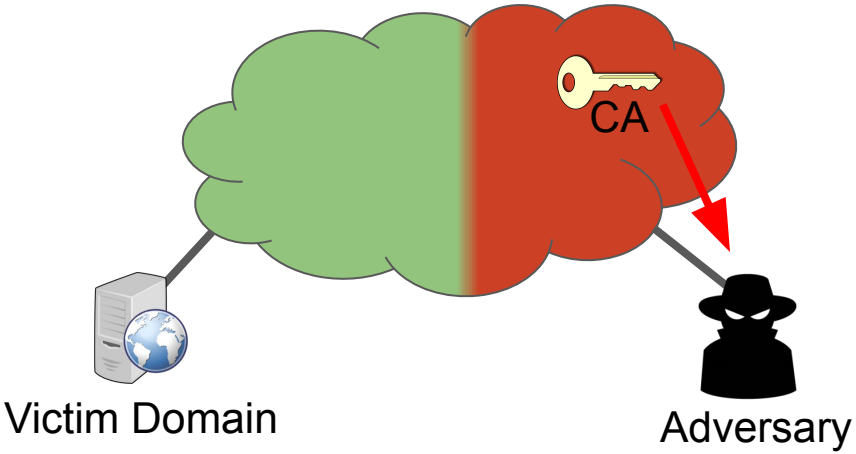
- How Domain Control Validation is Vulnerable
- Demo
- Real-world attacks
- How multiple vantage point validation works
- How effective it is
- Deployment and operational details

Real-world attacks (Robert Danford, Salesforce)

Overview

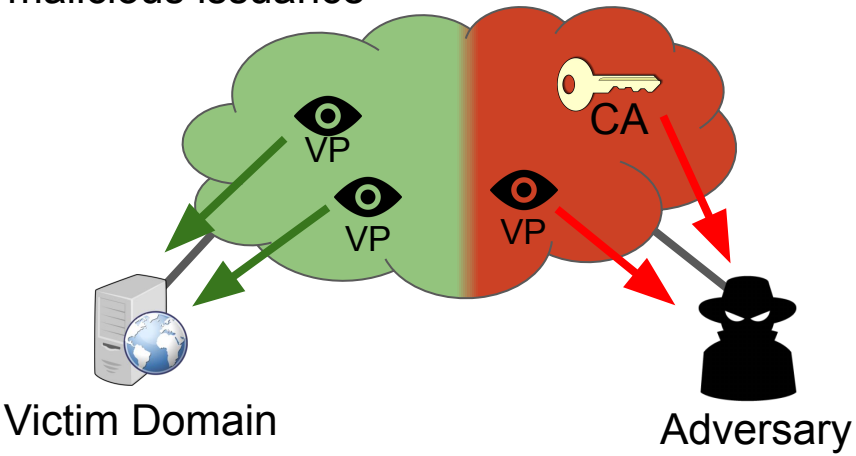
- How Domain Control Validation is Vulnerable
- Demo
- Real-world attacks
- How multiple vantage point validation works
- How effective it is
- Deployment and operational details

How Multiple Vantage Point Validation Works



Attack effective without multiple vantage point validation

Remote VPs block malicious issuance



Attack detected with multiple vantage point validation

See our paper:
https://www.usenix.org/conference/usenixsecurity21/presentation/birge-lee

Overview

- How Domain Control Validation is Vulnerable
- Demo
- Real-world attacks
- How multiple vantage point validation works
- How effective it is
- Deployment and operational details

Simulated Attacks on Real-World Domains

- **1.3M** domains sampled from Let's Encrypt logs over four months
- **31 billion** geographically-distributed DNS queries (full graph lookups)
- **400M** different simulated BGP attacks

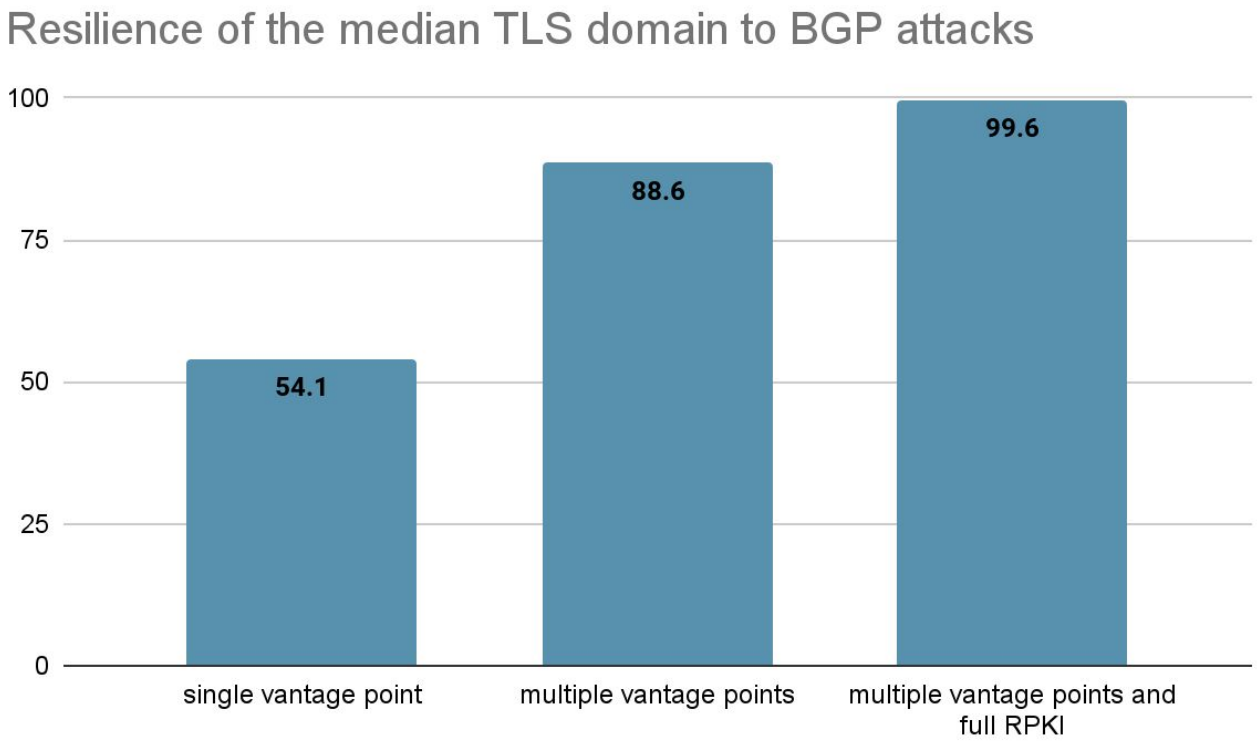
- Accounted for previous work (Let's Downgrade Let's Encrypt ACM CCS '21)
  - Counted an attack as successful if **any** name server was compromised

- Accounted for BGP routing security improvements: RPKI (which helps filter malicious BGP announcements) under both current and future conditions

- See our paper "How Effective is Multiple-Vantage-Point Domain Control Validation?" for more details: https://arxiv.org/abs/2302.08000

Simulated Attacks on Real-World Domains

Resilience: the fraction of the Internet that **cannot** obtain a certificate for a domain via a BGP hijack



Overview

- How Domain Control Validation is Vulnerable
- Demo
- Real-world attacks
- How multiple vantage point validation works
- How effective it is
- Deployment and operational details

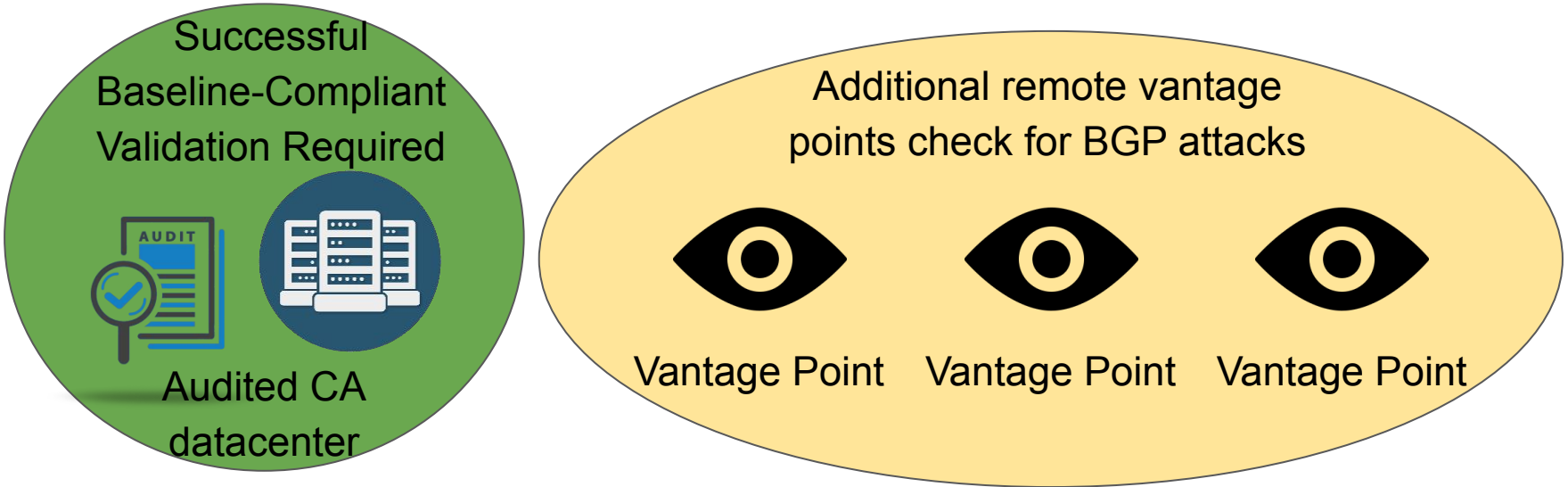
How to Deploy Multiple Vantage Point Validation

- Larger CA: Cloud Datacenters
  - Ethical real-world attacks and simulations show geographically-diverse cloud datacenters have substantial routing diversity

- Smaller CAs: Outsource via API
  - Cloudflare has developed an API and open-source protocol for remote validation
  - Contact dcv@cloudflare.com if interested

Remote Vantage Points Cannot Override Primary Validation

- Problem: Bring cloud inside the audit scope is extremely difficult
- Solution: Remote vantage points cannot override primary validation



Remote Vantage Points Cannot Override Primary Validation

- Problem: Bring cloud inside the audit scope is extremely difficult
-

All certs signed with multiple vantage points are a subset of those currently authorized by the baseline requirements

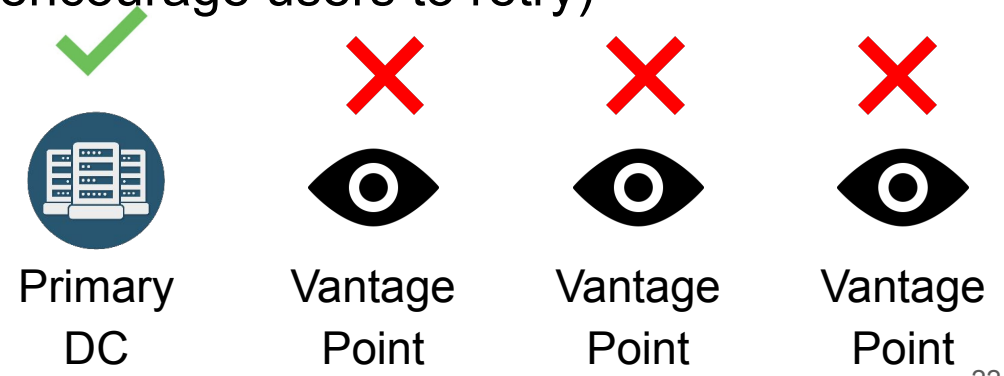
Ba
Va

Audited CA datacenter

Vantage Point Vantage Point Vantage Point

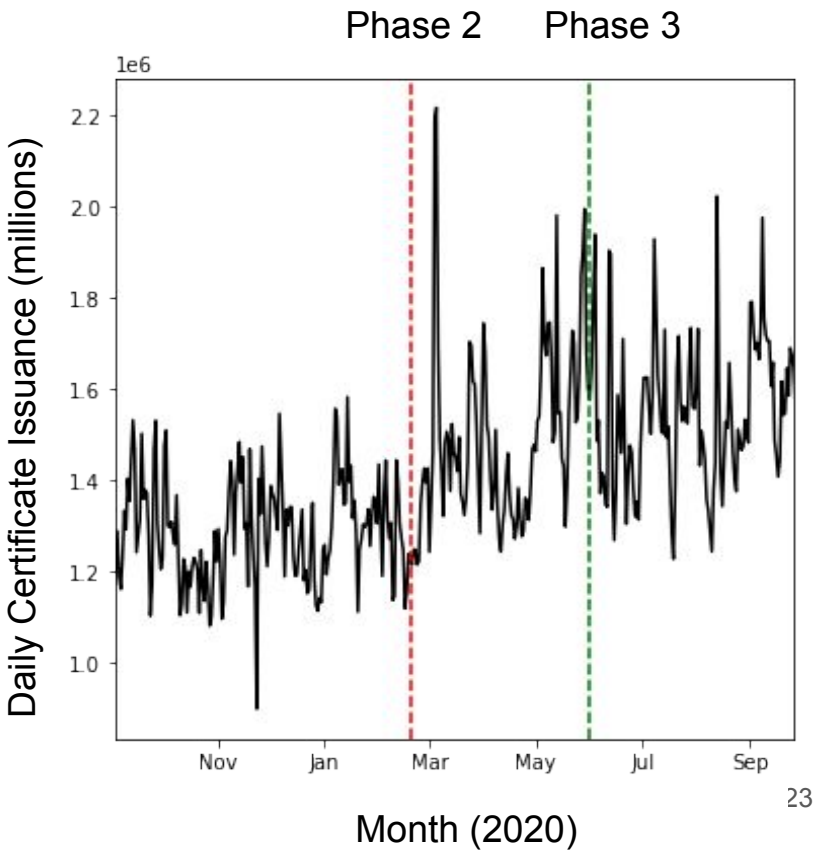
False Positives are Manageable and Easily Mitigated

- Leading cause of false positives is DNS propagation
  - Remote vantage points hit out-of-date nameservers
- False positives can be mitigated
  - Reduced with quorum policy (e.g., allow one vantage point to fail)
  - Most go away on retries (encourage users to retry)
- False positives were manageable even at Let's Encrypt's scale



Disruptions to CA Operations can be Prevented with a Phased Deployment

- Phase 1: Monitoring only: multiple vantage point results are logged but do not influence validation
  - Used to test code at scale and log any potential errors and estimate costs (~$100 per month per vantage point)
- Phase 2: Enforcing with exception list: enforced except on certain accounts
- Phase 3: Full deployment



Conclusion

- BGP attacks on domain control validation are **possible** and being **used in the real world**
- In both simulations and ethical real-world attacks, multiple vantage point validation **mitigates the risk**
- Multiple vantage point validation is **easy to deploy**
- Multiple vantage point validation **does not disrupt** a CA's operations
- Both **Let's Encrypt** and **Google Trust Services** have implemented

Questions

Henry Birge-Lee (Princeton University)
birgelee@princeton.edu

Robert Danford (Salesforce)
robert.danford@salesforce.com

BGP Attacks on the PKI: Bamboozling Certificate Authorities with BGP
https://www.usenix.org/conference/usenixsecurity18/presentation/birge-lee

Deployment Details: Experiences Deploying Multi-Vantage-Point Domain Validation at Let's Encrypt
https://www.usenix.org/conference/usenixsecurity21/presentation/birge-lee

Security Evaluation: How Effective is Multiple-Vantage-Point Domain Control Validation?
https://arxiv.org/abs/2302.08000