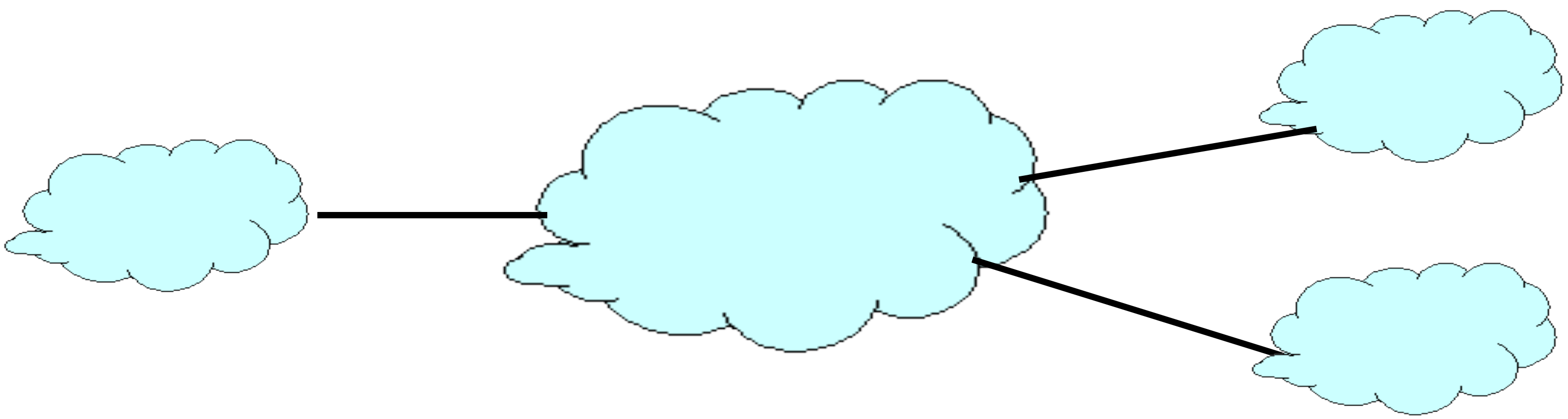
Securing Internet Applications from Routing Attacks

Jennifer Rexford

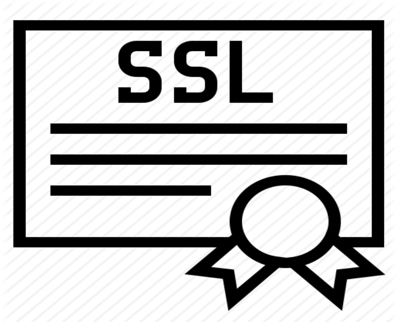
PRINCETON UNIVERSITY

Interdomain Routing Security

- Border Gateway Protocol (BGP)
  - Vulnerable to attack and misconfiguration
  - Attacks affecting availability and confidentiality
  - Yet, deploying BGP security solutions is hard

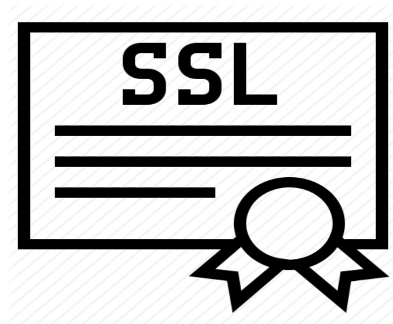


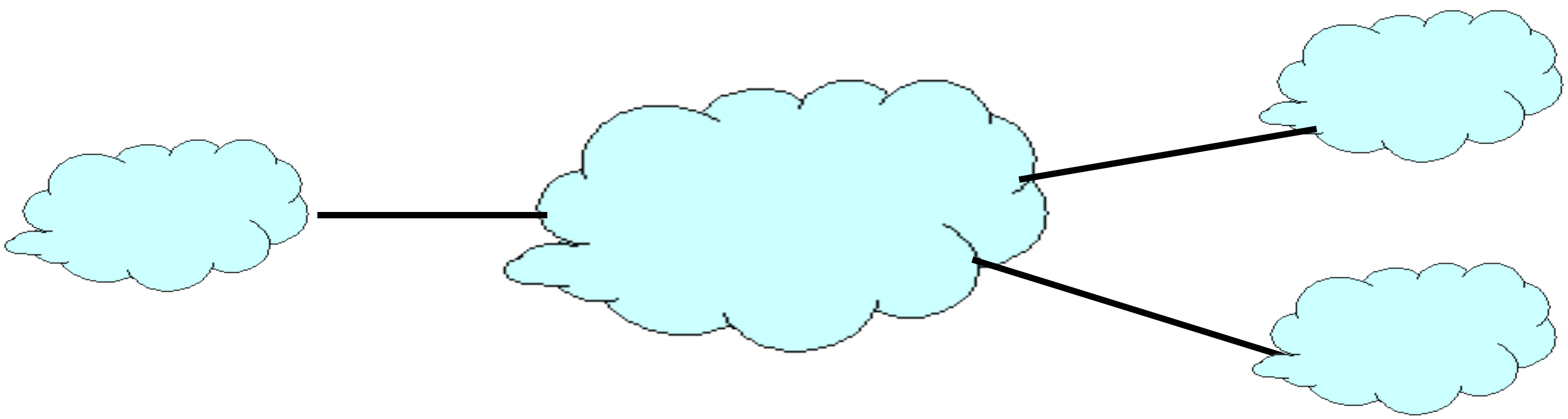
Application Security



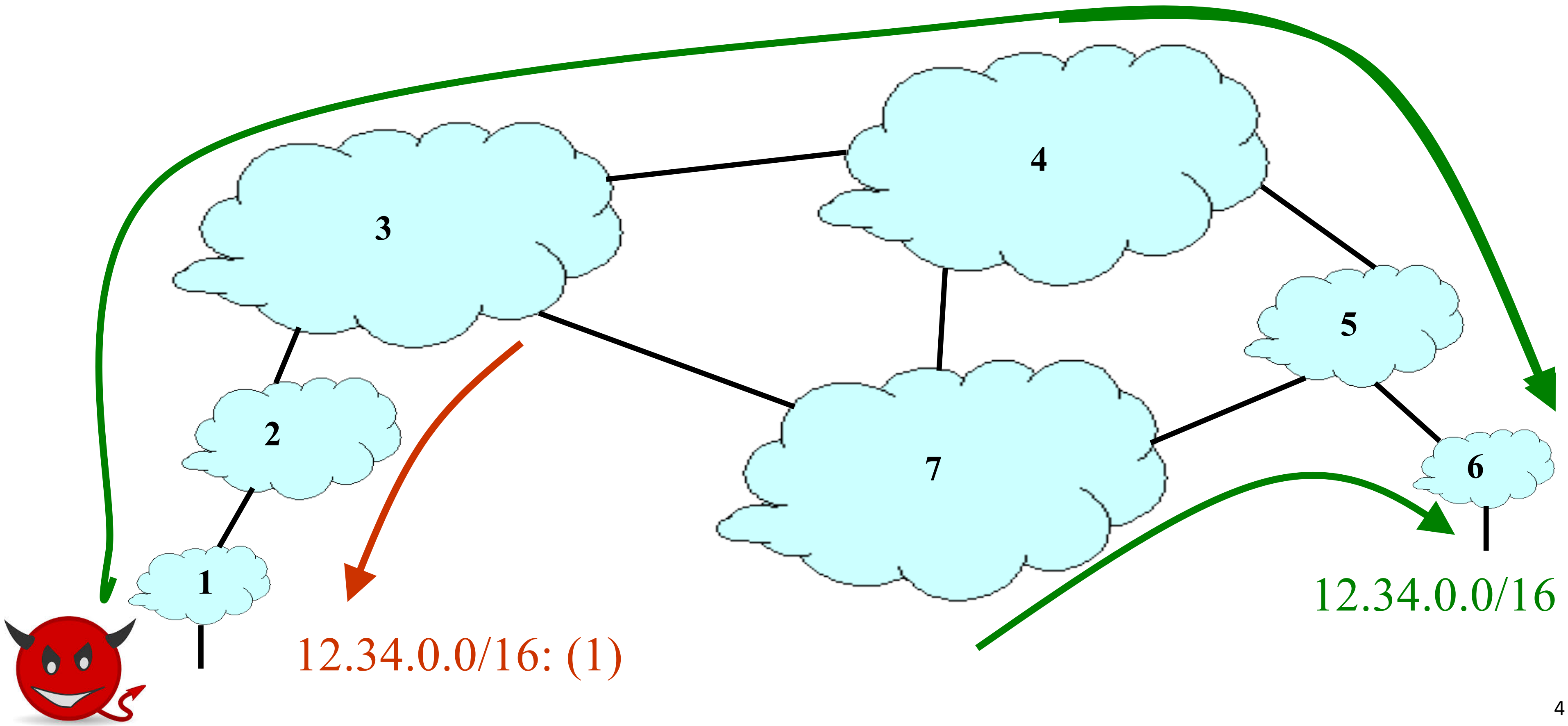
- Security-sensitive applications
  - Use cryptography to protect end users
  - Rely on the underlying network to deliver data
  - Treat the network as a “dumb pipe”… but should they?

Cross-Layer Routing Attacks

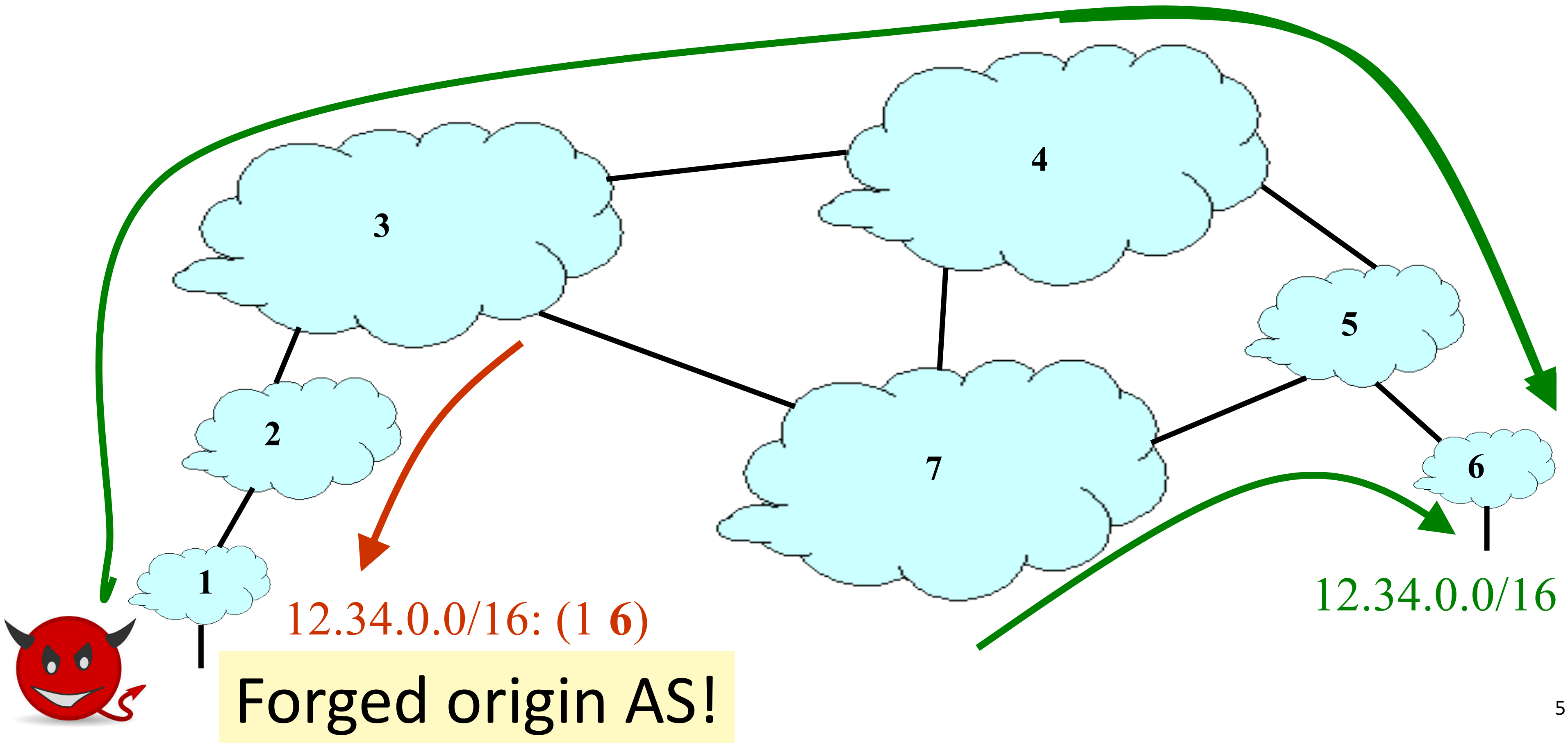




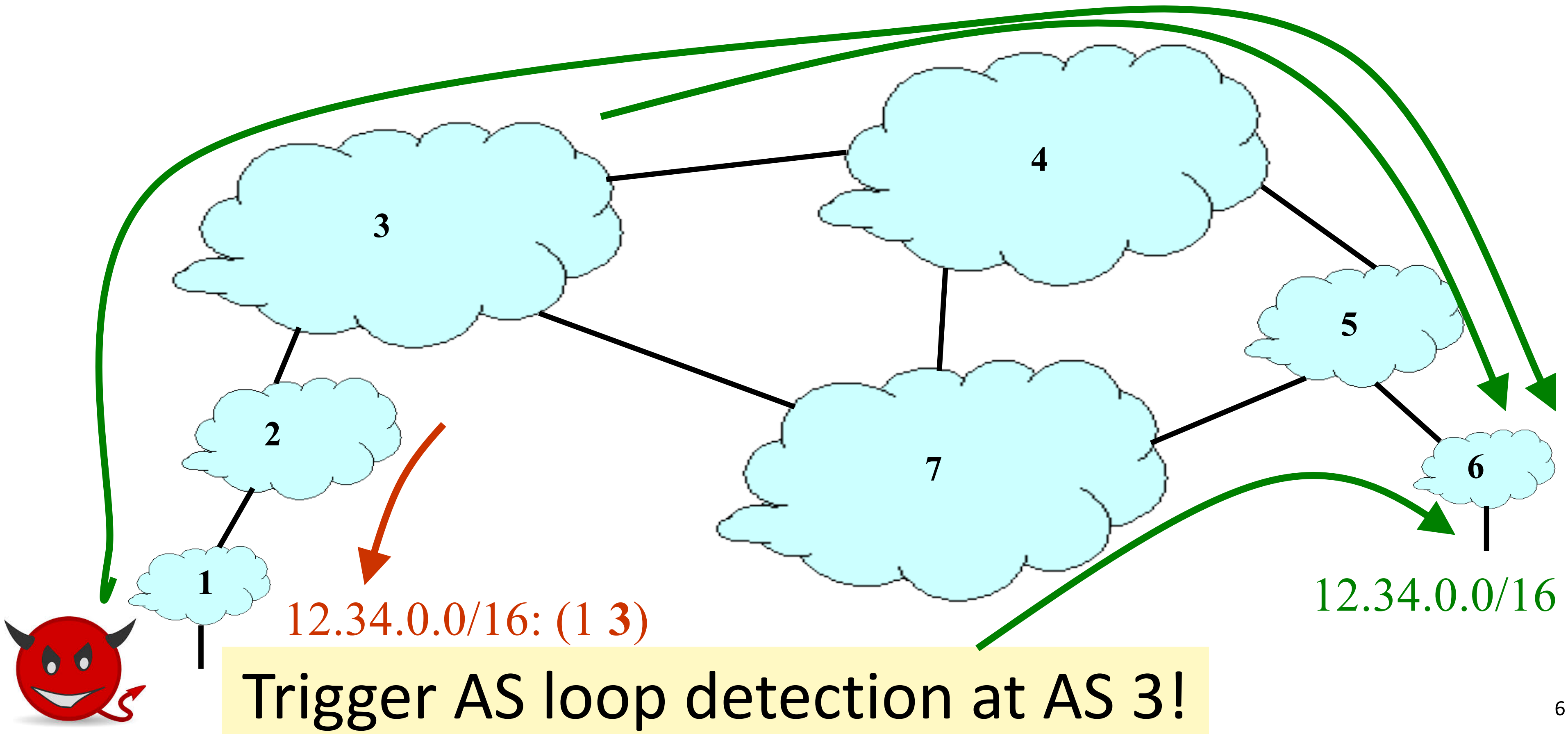
Simple BGP Prefix Hijack



Forged Origin AS



Path Poisoning

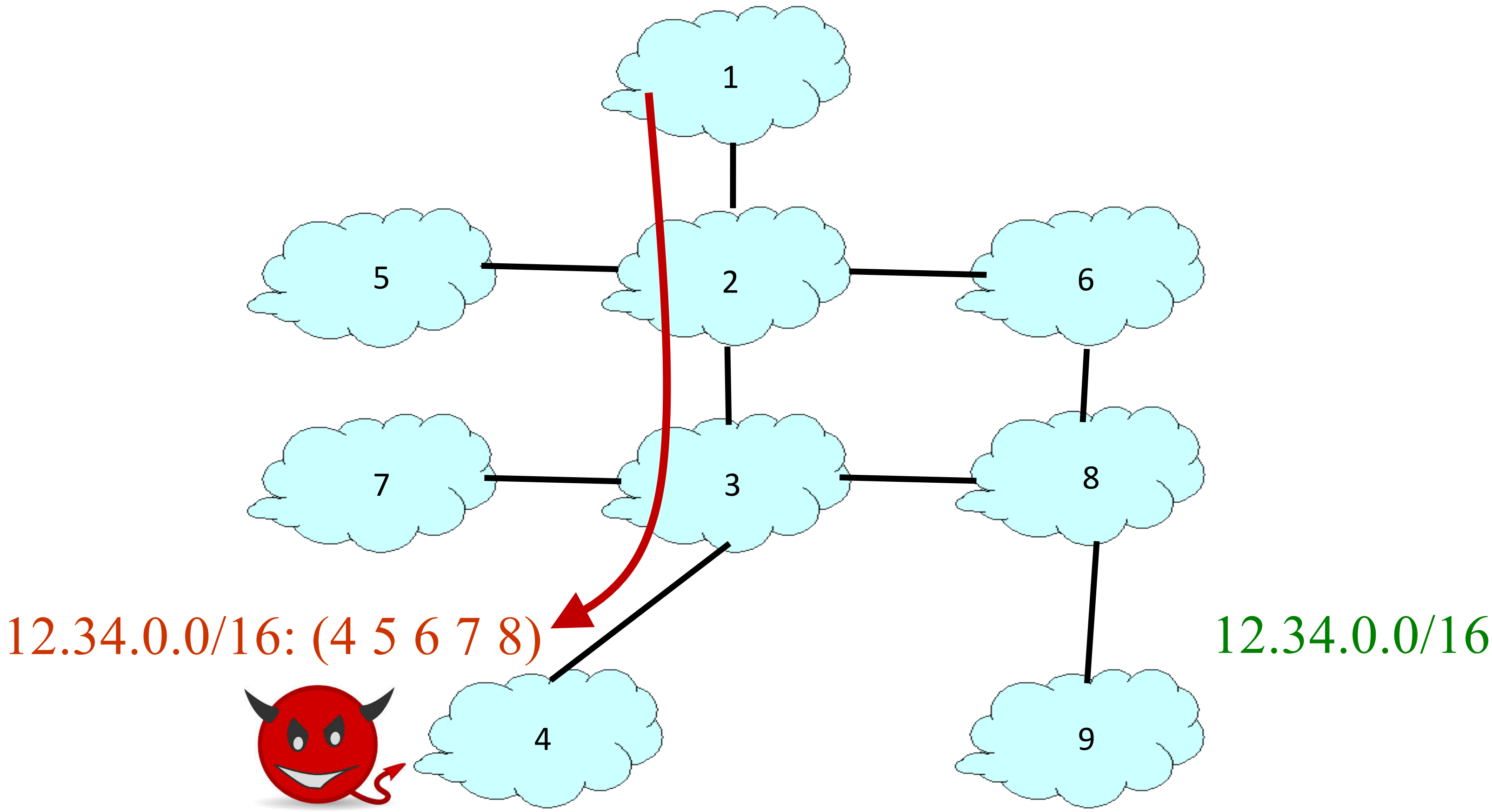


Trigger AS loop detection at AS 3!

Stealthy, Targeted Attacks

- Targeted senders
  - Specific sender
  - Easiest sender to attack of a group
- Limited scope
  - Limit the other ASes that see the hijack
  - Limit the data traffic that follows the hijack path
- Limited time
  - Short interval of time
  - During a sensitive event

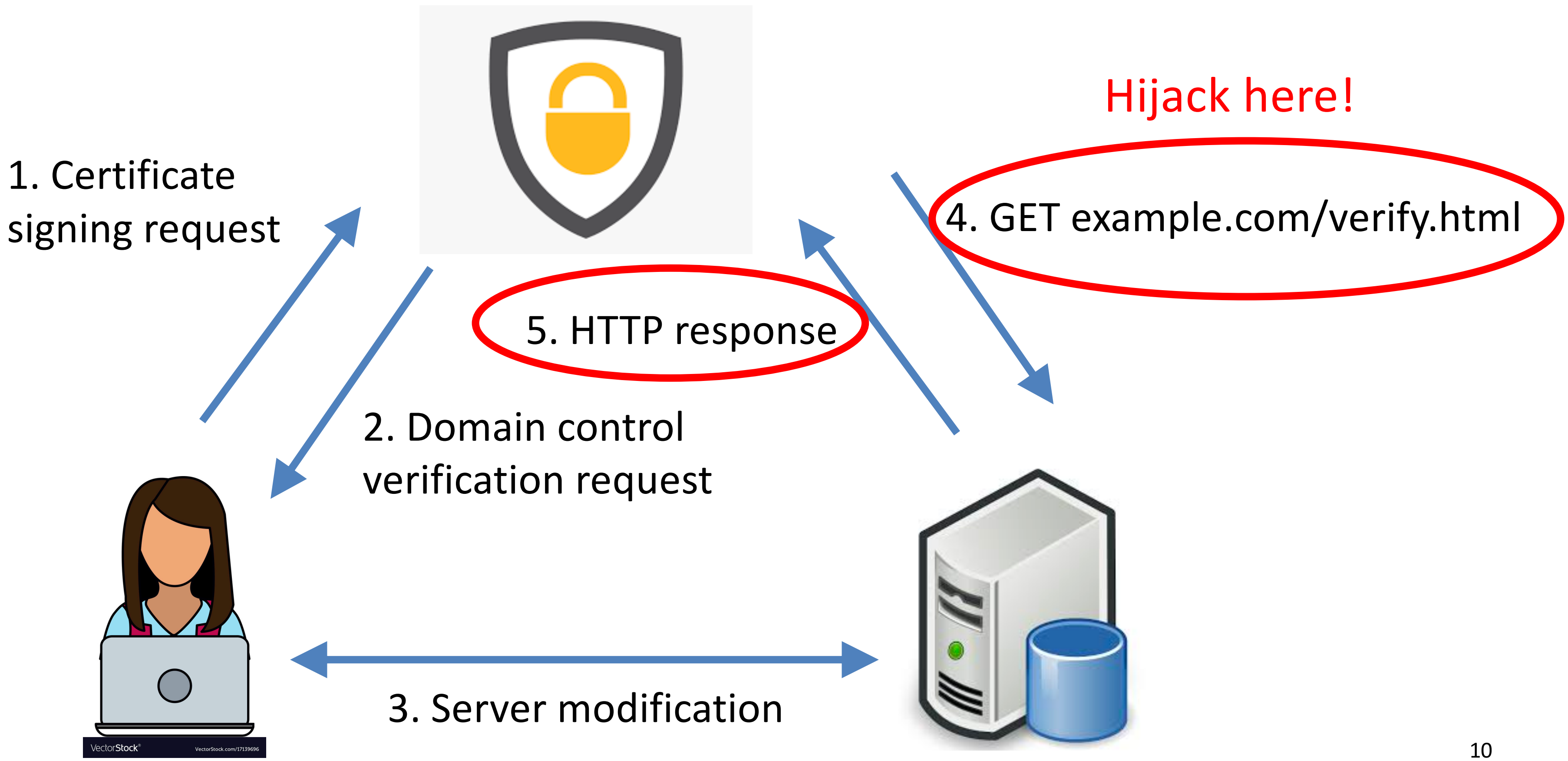
Surgical Hijack



Stealthy, Targeted Attacks

- Targeted sender
  - Specific sender (e.g., a specific certificate authority)
  - Easiest sender to attack of a group (e.g., any certificate authority)
- Limited scope
  - Limit the other ASes that see the hijack
  - Limit the data traffic that follows the hijack path
- Limited time
  - Short interval of time
  - During a sensitive event (e.g., acquiring a certificate)

CA Domain Control Verification

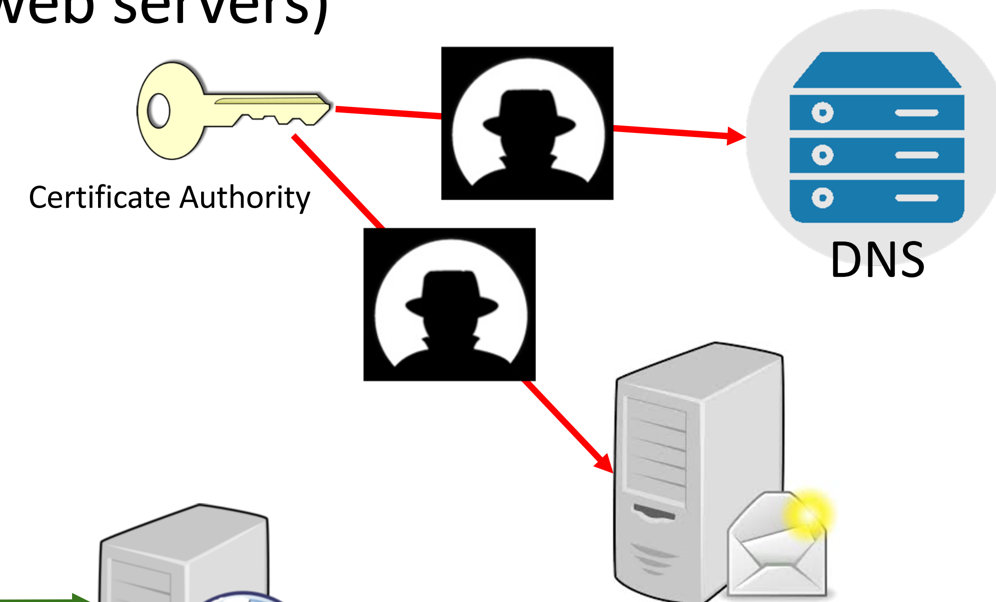


Launching Ethical Attacks

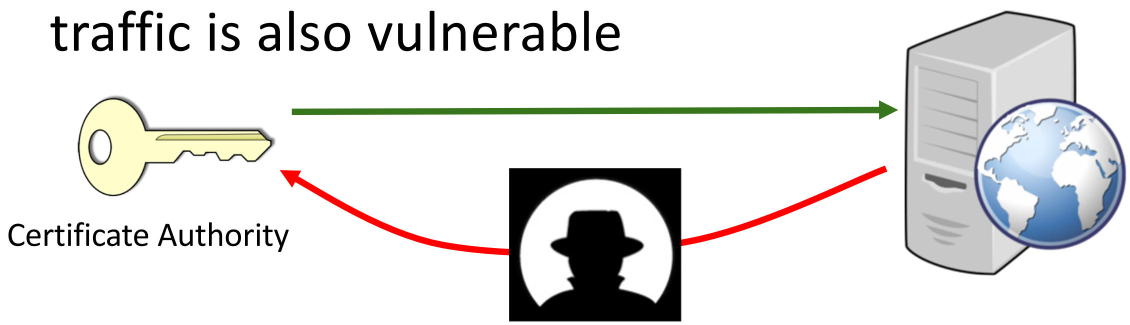
- Attacking ourselves
  - IP prefix we control (PEERING testbed at Columbia University)
  - Domain names created for the experiment
  - No real clients accessing the server
- Bamboozling the certificate authorities
  - Let’s Encrypt, GoDaddy, Comodo, Symantec, GlobalSign
  - Domain validation using either HTTP request or email
  - All five CAs signed our certificate requests in < 2 minutes

Additional Attacks

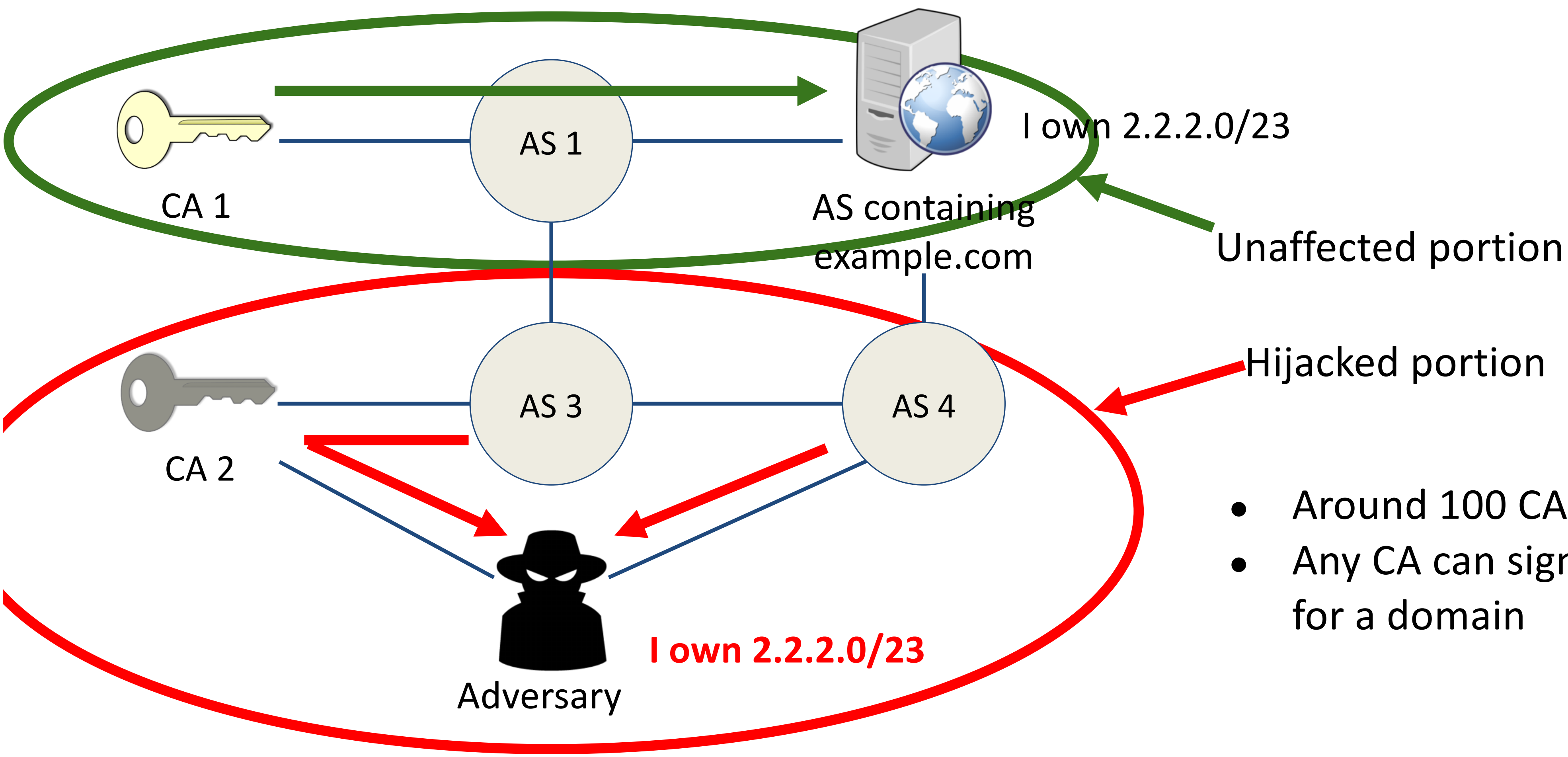
- More targets (beyond victim web servers)
  - Authoritative DNS servers
  - E-mail servers



- Attacking CA prefixes
  - Reverse (victim domain → CA) traffic is also vulnerable



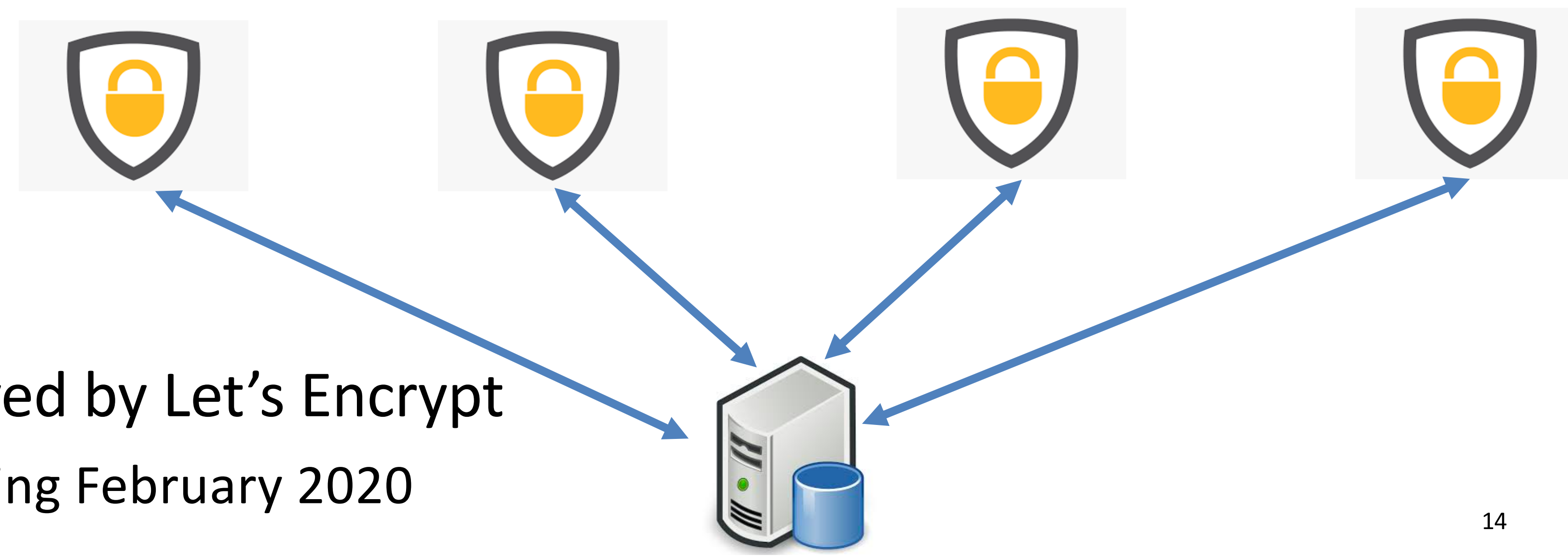
Adversary Can Pick the Easiest CA to Fool



- Around 100 CAs
- Any CA can sign for a domain

Application-Level Defense

- You can fool some of the people some of the time
  - But not all of the people all of the time
- Multiple vantage point domain verification by the CA

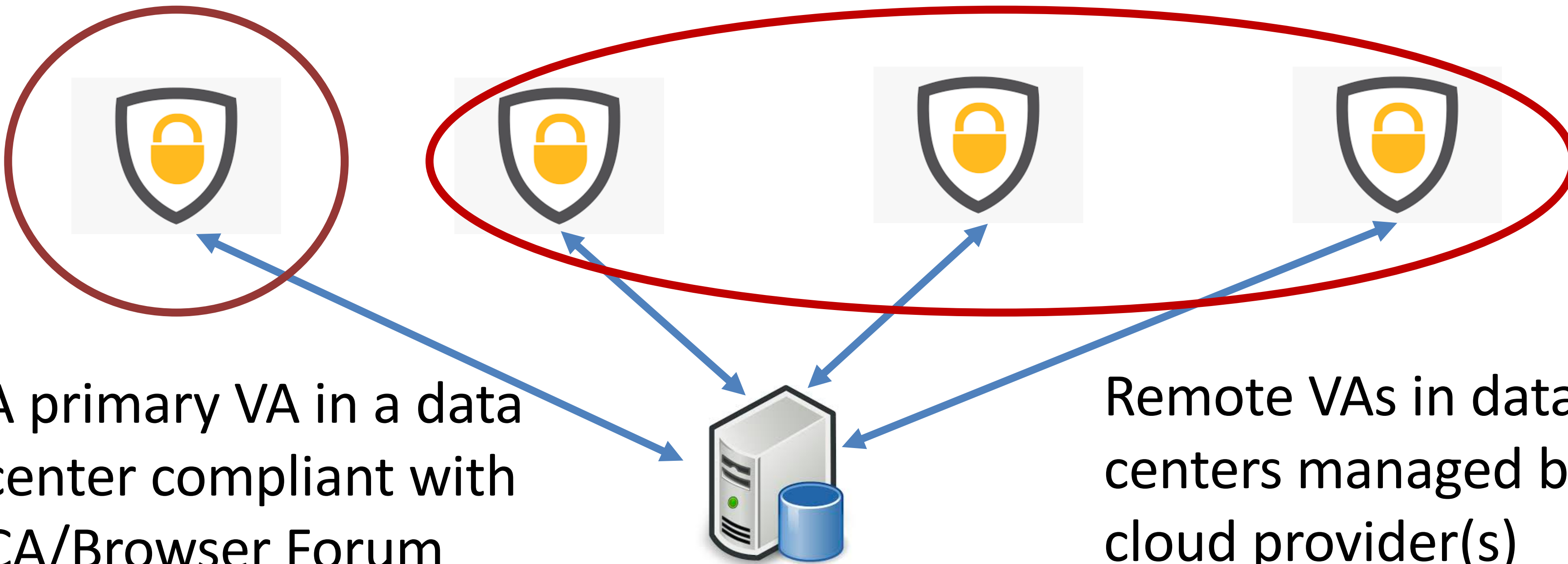


- Deployed by Let's Encrypt
  - Starting February 2020

Practical Design Challenges

- Security
  - Vantage points with diverse perspectives
  - Strong enough quorum policy to thwart attacks
- Manageability
  - Compliance with the CA/Browser Forum requirements
  - Avoid complexity of vantage points in multiple clouds
- Performance
  - Minimizing latency and communication overhead
- Benign failures
  - Avoid rejecting valid requests for certificates

Compliance with CA/Browser Forum

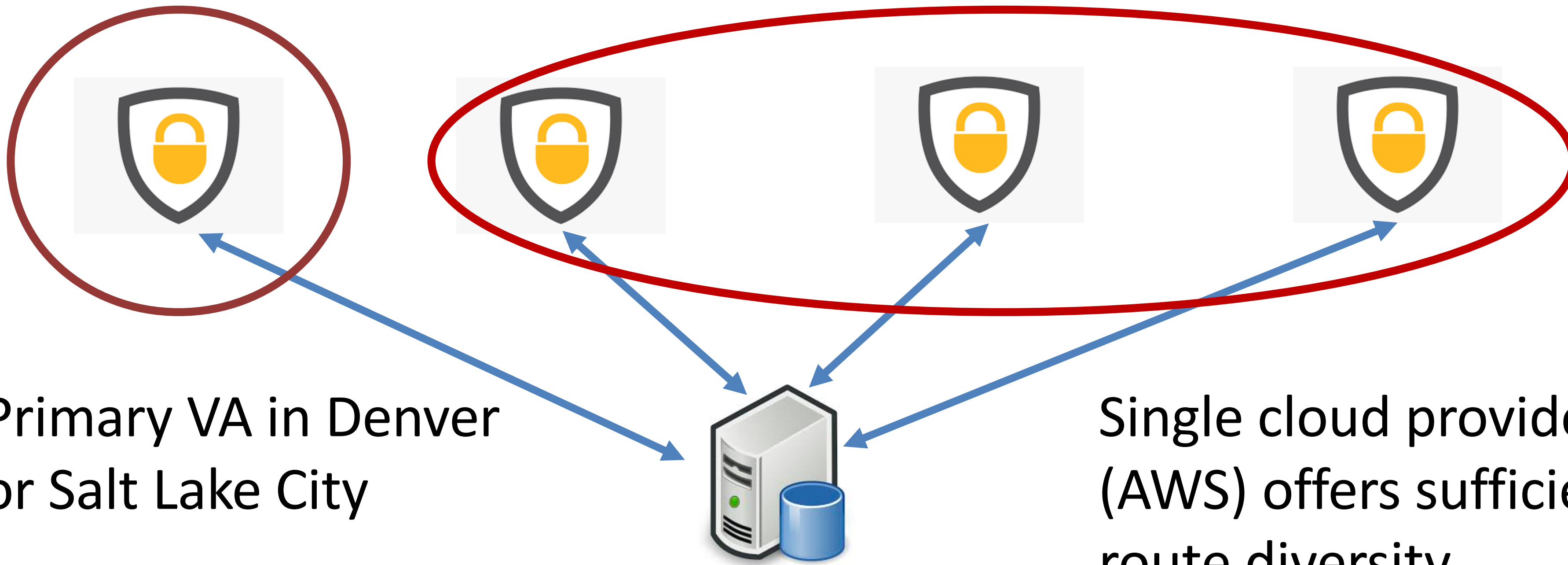


A primary VA in a data center compliant with CA/Browser Forum

Remote VAs in data centers managed by cloud provider(s)

Primary VA's validation *must* succeed.

Balancing Security and Cloud Complexity

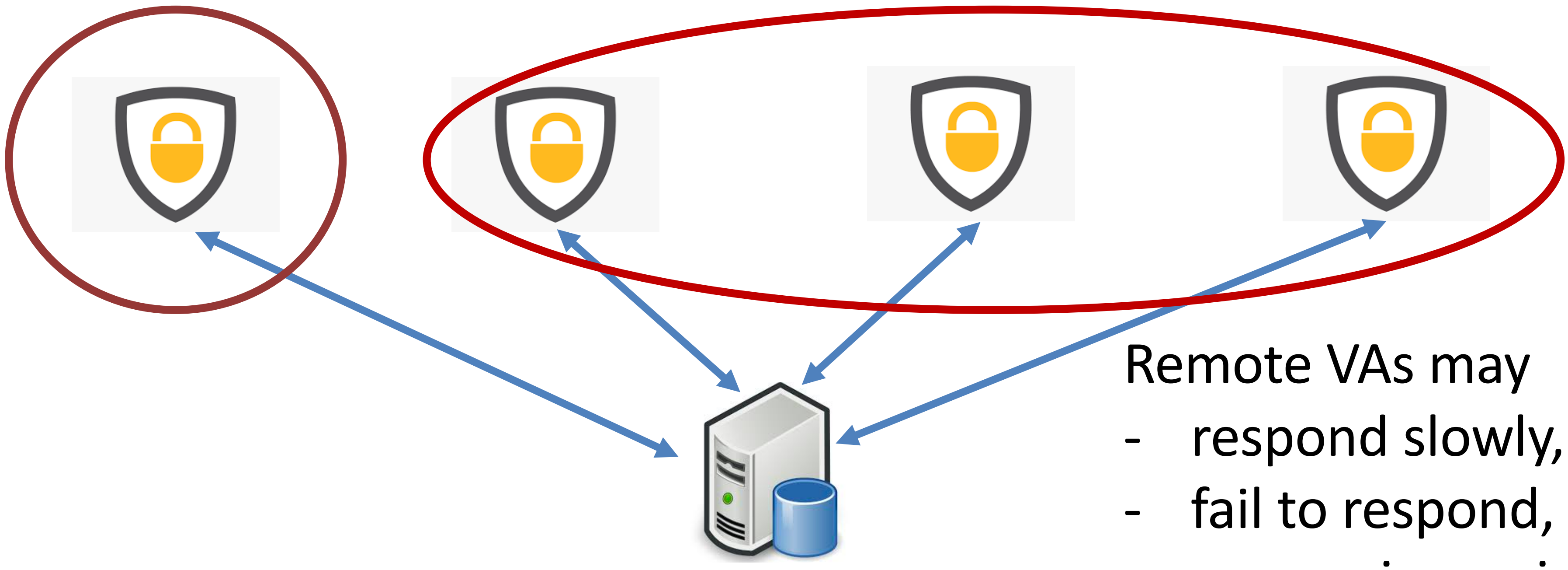


Primary VA in Denver
or Salt Lake City

Single cloud provider
(AWS) offers sufficient
route diversity

Remote VAs in Oregon, Ohio, and Frankfurt.

Balancing Security and Benign Failures



Remote VAs may
- respond slowly,
- fail to respond, or
- answer inconsistently

Primary VA and at least *two* remote VAs must succeed.

Let’s Encrypt Phased Deployment

- Staging deployment
  - Internal testing of new features
- Testing in production environment
  - Remote VAs performed domain validation
  - But, the primary VA drove all validation decisions
- Production deployment with domain exceptions
  - Temporarily excluding certain domains renewing their certificates
- Full production deployment
  - All certificate requests (~1.5M per day) validated by multiple VAs

Deployment Anecdotes

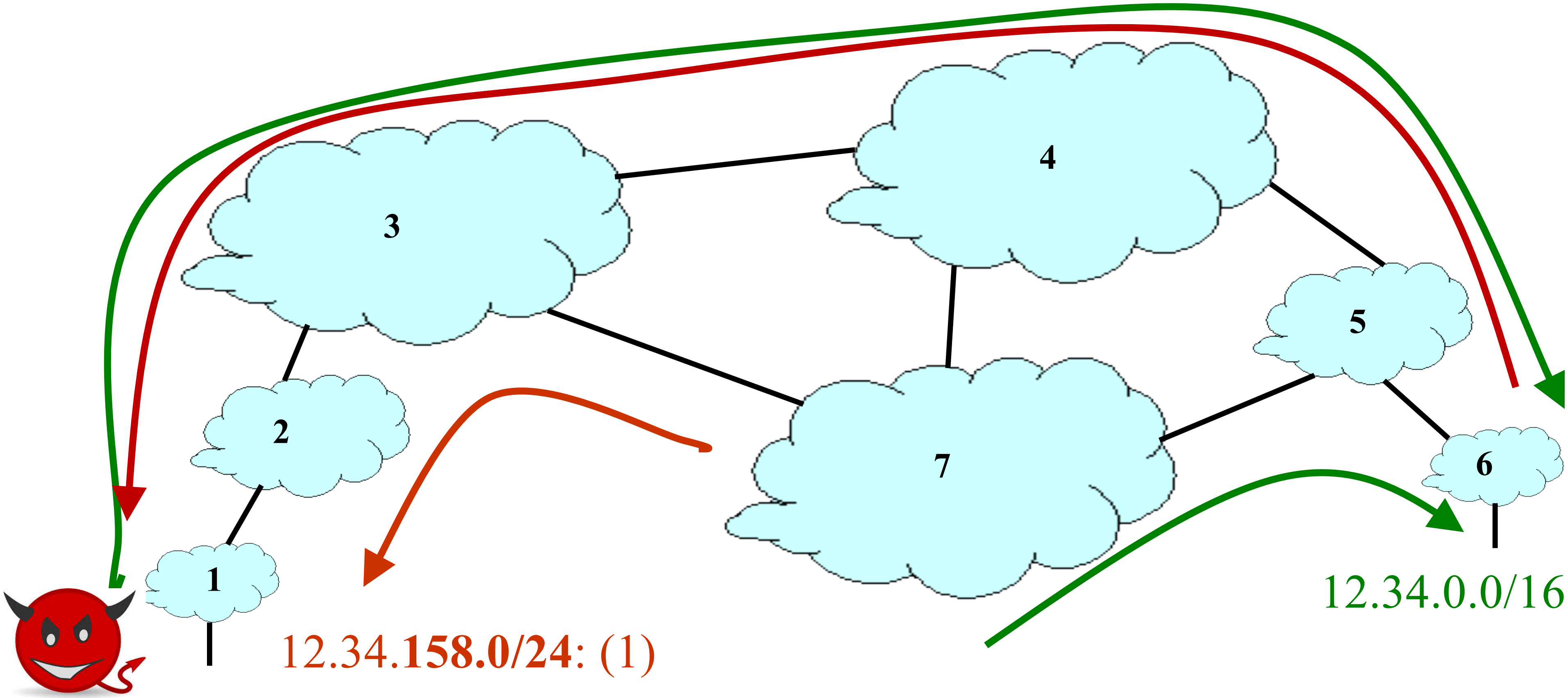
- Low validation latency
  - Remote VAs usually perform *better* than the primary VA
- Low validation bandwidth
  - Only 0.5 Mbps per remote VA for ~20 certificates/second
- Low benign failures
  - Primary succeeds but *any* remote VA fails: just 1.2% of validations
  - Most due to a remote VA failing DNS resolution of domain's name
  - Some due to multiple validation requests triggering DDoS detection
  - Almost all were successful after retrying the request

Quantifying the Security Improvement

- Ethical attacks on Let's Encrypt
  - Using Columbia University's PEERING testbed
  - Quorum policy caught most of the attacks
  - ... though some well-connected adversaries still successful
- BGP simulation experiments
  - Extensions to model AS connectivity of each AWS data center
  - Evaluation of a much wider range of BGP attacks
  - Median domain is resilient to attacks from > 90% of ASes

Good to add 1-2 more AWS locations (Paris, Singapore) and/or require a full quorum

Other BGP Attacks: Sub-Prefix Hijack



Not always possible (e.g., domain on /24) and visible in BGP monitoring

Protecting More Applications

- Domain validation (beyond CAs)
  - Changing an account password
  - Verifying ownership of a restaurant, hotel, etc.
- Anonymous communication
  - Tor, I2P, and VPNs
  - BGP interception attacks to enable traffic-analysis attacks
- Bitcoin network
  - Disrupting the consensus protocol in the overlay network

Conclusion

- Cross-layer attacks
  - Layering simplifies protocol design
  - But, adversaries can work across layer boundaries
- Cross-layer defenses
  - Application-layer defenses are easier to deploy
  - But, network-layer defenses are still important
- A way forward
  - Protect popular applications and important prefixes
  - Continue the important work of securing BGP
  - Incentivize BGP security by favoring secure prefixes and ASes

Thank You!

- Henry Birge-Lee, Yixin Sun, Annie Edmundson, Jennifer Rexford, and Prateek Mittal, "Bamboozling certificate authorities with BGP," in *USENIX Security*, August 2018. https://www.cs.princeton.edu/~jrex/papers/bamboozle18.pdf

- Yixin Sun, Maria Apostolaki, Henry Birge-Lee, Laurent Vanbever, Jennifer Rexford, Mung Chiang, and Prateek Mittal, "Securing Internet applications from routing attacks," to appear in *Communications of the ACM*. https://arxiv.org/pdf/2004.09063.pdf

- Henry Birge-Lee, Liang Wang, Daniel McCarney, Roland Shoemaker, Jennifer Rexford, and Prateek Mittal, "Experiences deploying multi-vantage-point domain validation at Let's Encrypt," October 2020. https://www.cs.princeton.edu/~jrex/papers/multiva20.pdf