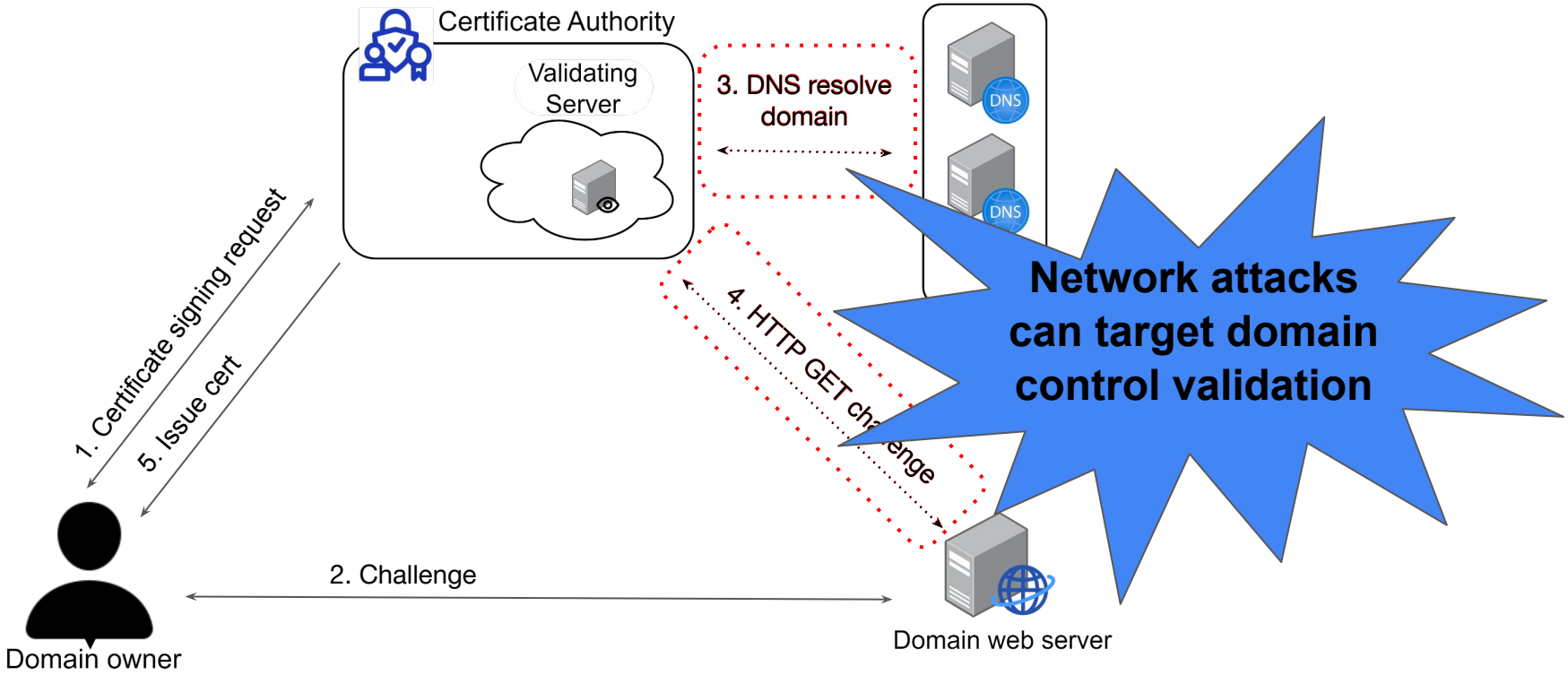
How Effective is Multiple-Vantage Point Domain Control Validation?

Grace Cimaszewski

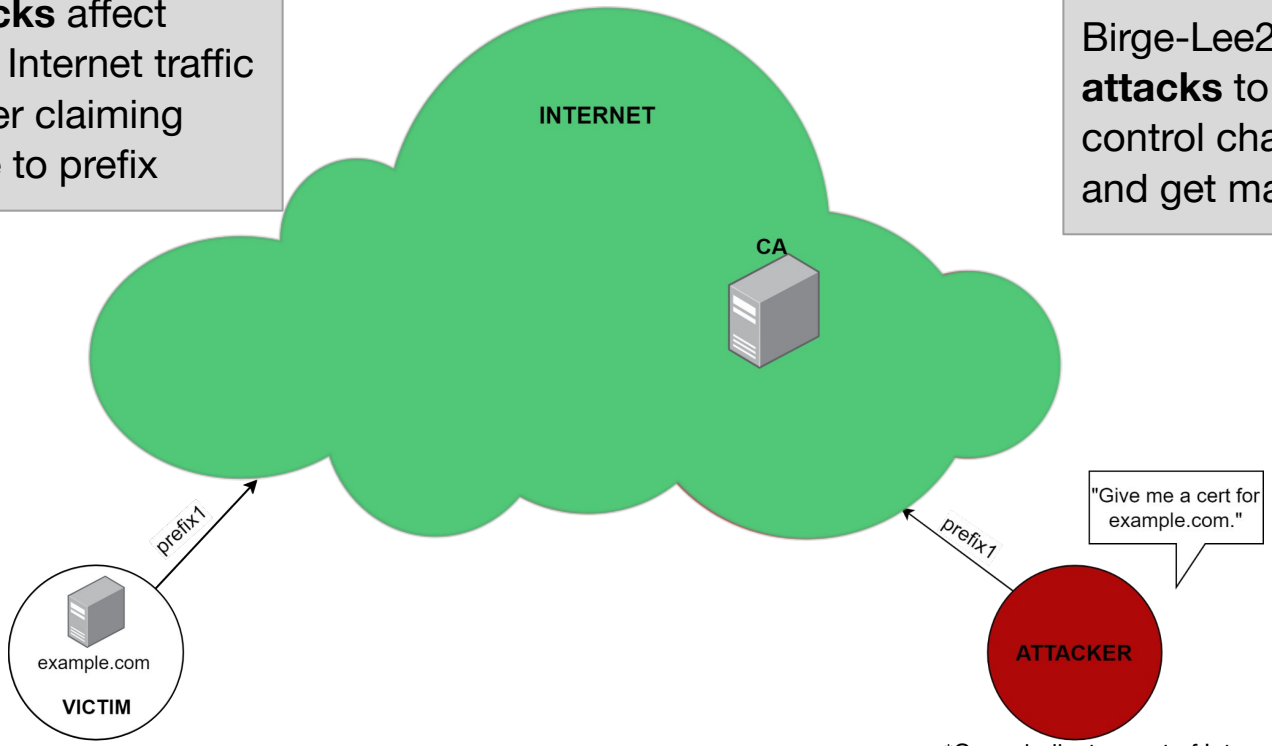
Henry Birge-Lee, Liang Wang, Jennifer Rexford, Prateek Mittal

Certificate Issuance Vulnerable to Network Attacks



Routing Attacks to Break Domain Control Validation

BGP hijacks affect portion of Internet traffic by attacker claiming fake route to prefix

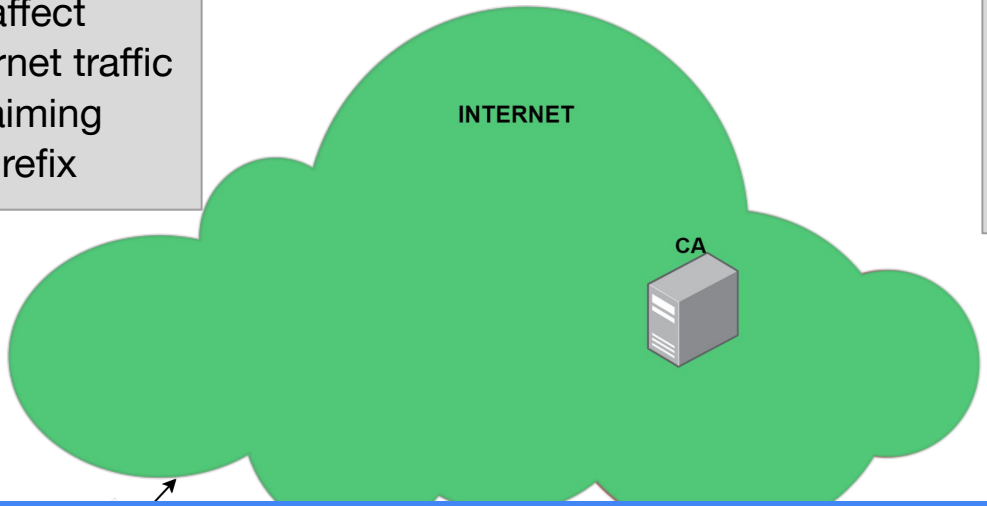


Birge-Lee2018 used **routing attacks** to redirect domain control challenge to attacker and get malicious certificate

*Green indicates part of Internet that routes correctly to victim; red indicates part that routes to attacker.

Routing Attacks to Break Domain Control Validation

BGP hijacks affect portion of Internet traffic by attacker claiming fake route to prefix



Birge-Lee2018 used **routing attacks** to redirect domain control challenge to attacker and get malicious certificate

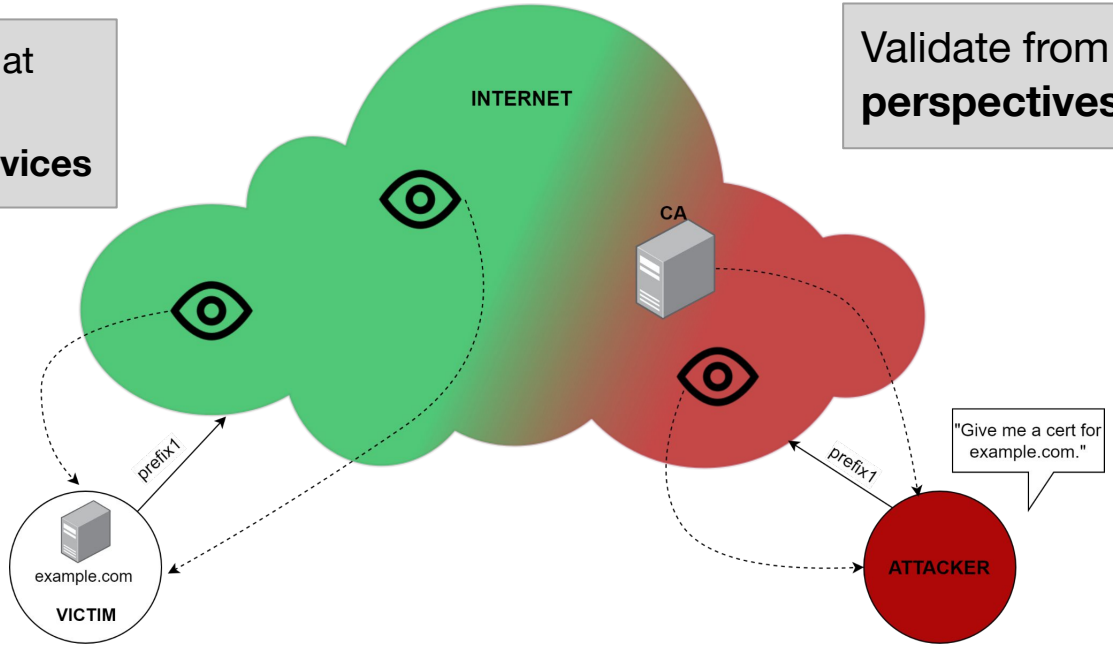
Real attacks observed in the wild confirm urgency to deploy countermeasures

*Green indicates part of Internet that routes correctly to victim; red indicates part that routes to attacker.

multiVA: a Defense Against Localized Routing Attacks

Already deployed at **Let's Encrypt**, **Google Trust Services**

Validate from multiple **distinct perspectives** throughout Internet

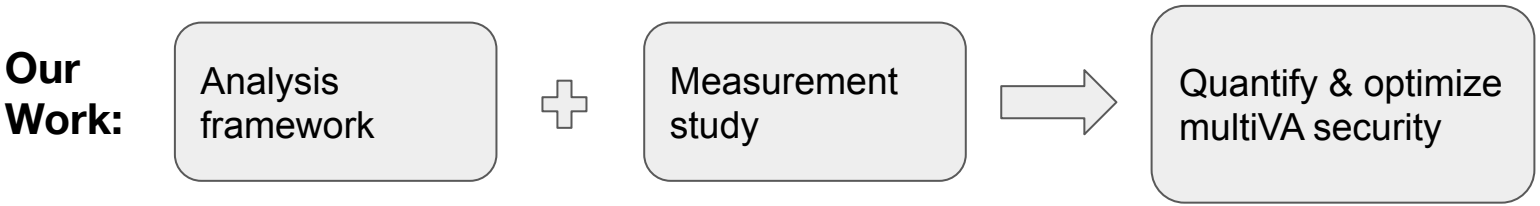


Routing at vantage points not affected by attack → **attack detected**

*multiple-vantage point domain control validation ≡ multiVA

Our paper: a rigorous analysis of multiVA

- multiVA gaining momentum (and sparking debate) in Web PKI
- Key bottleneck for deployment at CAs: lack of clear understanding of multiVA security benefits
  - Effectiveness depends on deployment details
  - ***How effective is multiVA deployment in practice?***



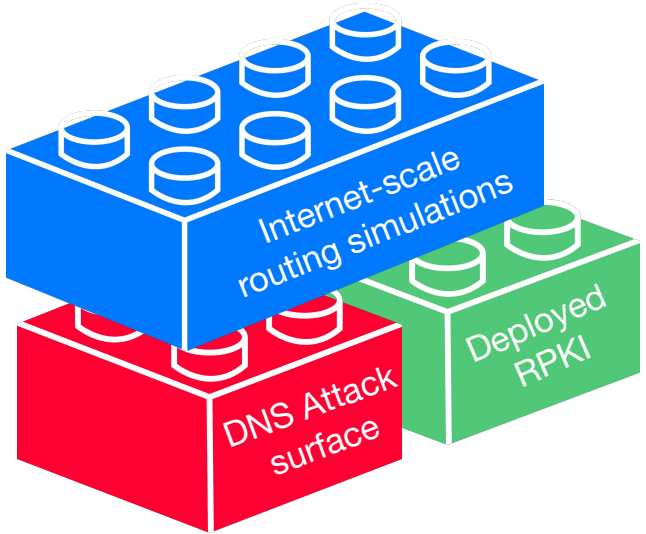
What we did: our contributions

1. ***Analysis framework:*** incorporate real-world routing factors into estimation of multiVA's resilience to localized network attacks (e.g., DNS and RPKI)

2. ***Measurement study:*** data collection at scale for accurate snapshot of web landscape, focusing on Let's Encrypt domains - capturing both existing deployment and what-if scenarios for vantage point locations

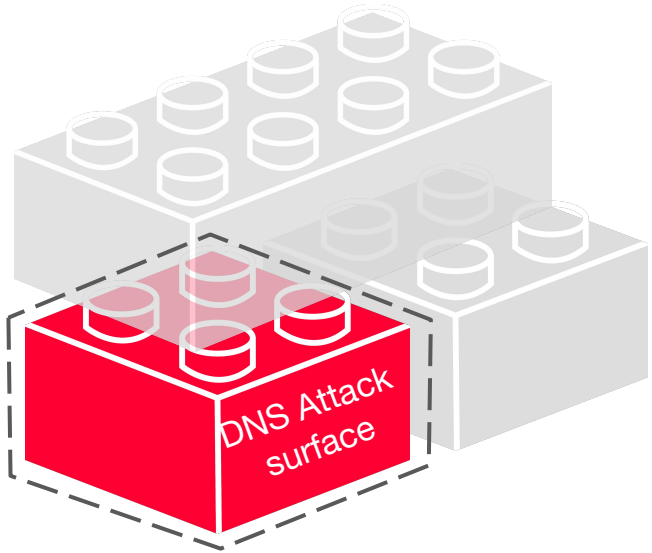
What we did: our contributions

1. ***Analysis framework:*** incorporate real-world routing factors into estimation of multiVA's resilience to localized network attacks (e.g., DNS and RPKI)



Analysis framework: multiVA model built on real-world routing intricacies

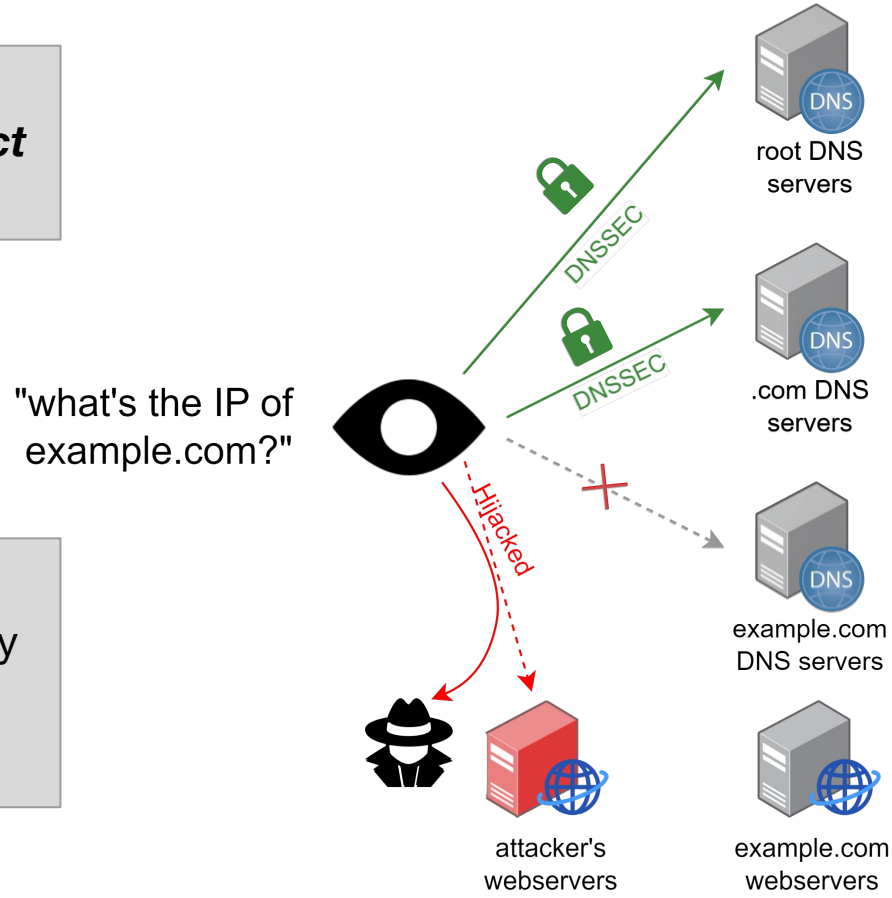
Consider **full DNS graph** of domain name



Point #1: Consider routing **hijacks on DNS resolution of domain**

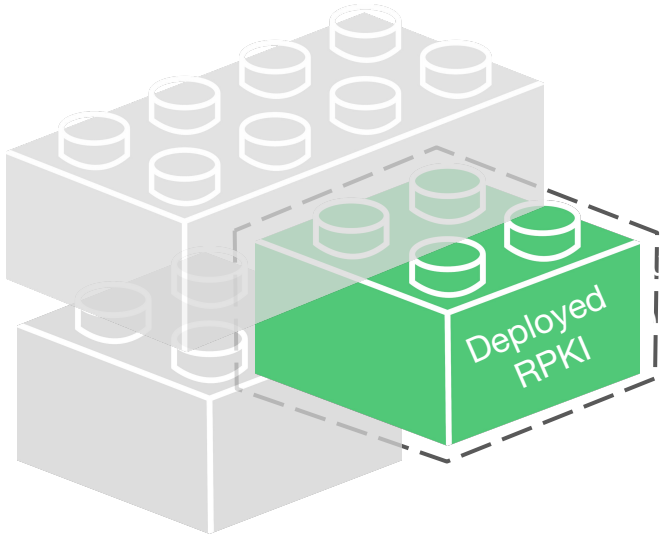
DNSSEC signatures can be a tool to ***detect hijacks***

BGP hijacks on DNS are highly viable: only 5.6% of domains are fully DNSSEC-signed



Attacker can hijack prefix of domain's webserver(s) or its **DNS nameservers**

Analysis framework: multiVA model built on real-world routing intricacies

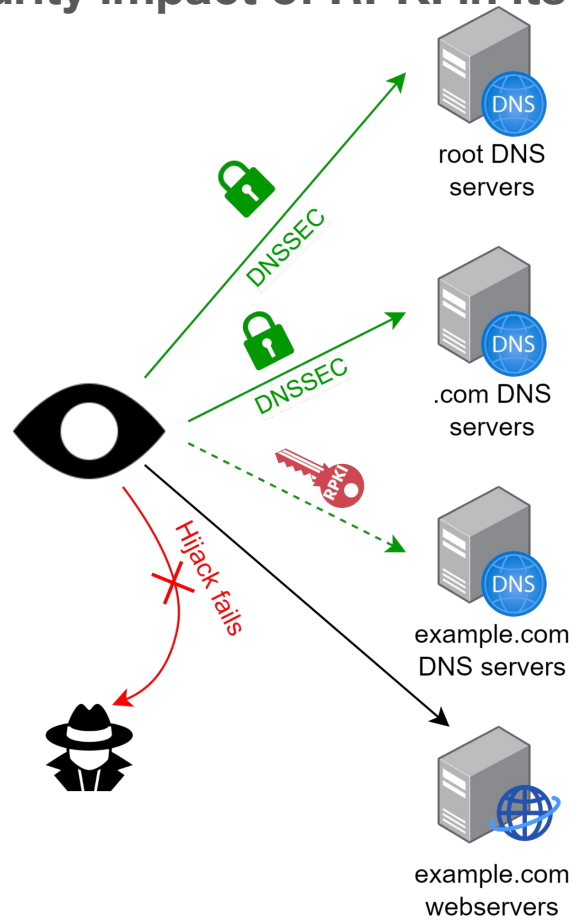


RPKI: a PKI for **Internet routes** and **prefixes**

Consider **prefixes with RPKI records** and **vantage points that perform RPKI filtering**

Point #2: Model the **security impact of RPKI in its current deployment**

RPKI does not make BGP hijacks impossible, but **reduces the power of a potential attack.**



RPKI counterbalances DNS attack surface: popular DNS providers adopt RPKI at higher rate than rest of Internet

60% of target IPs sampled had covering RPKI ROA records.

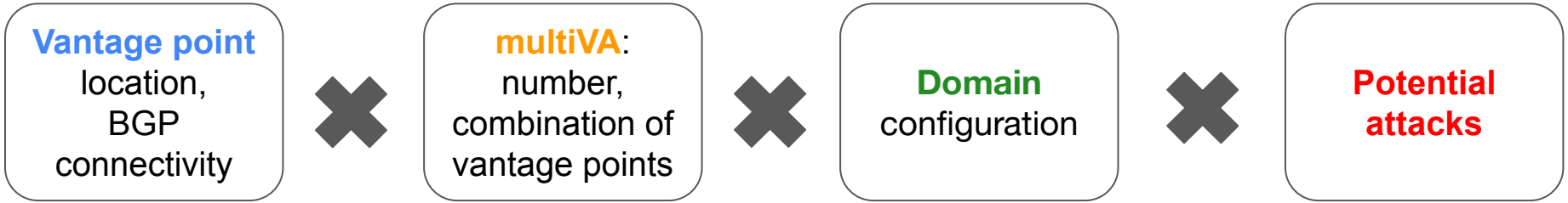
What we did: our contributions

1. ***Analysis framework:*** leverage CA design, domain configuration, and routing configuration to calculate resilience to localized BGP attacks

2. ***Measurement study:*** data collection at scale for accurate snapshot of web landscape, focusing on **Let's Encrypt** - capturing both existing deployment and what-if scenarios for vantage point locations

Measurement study at Let's Encrypt

Challenges: **huge search space** of multiVA variables;
need to instantiate analysis framework with **concrete data**



Measurement study at Let's Encrypt

Challenge: huge search space of multiVA variables

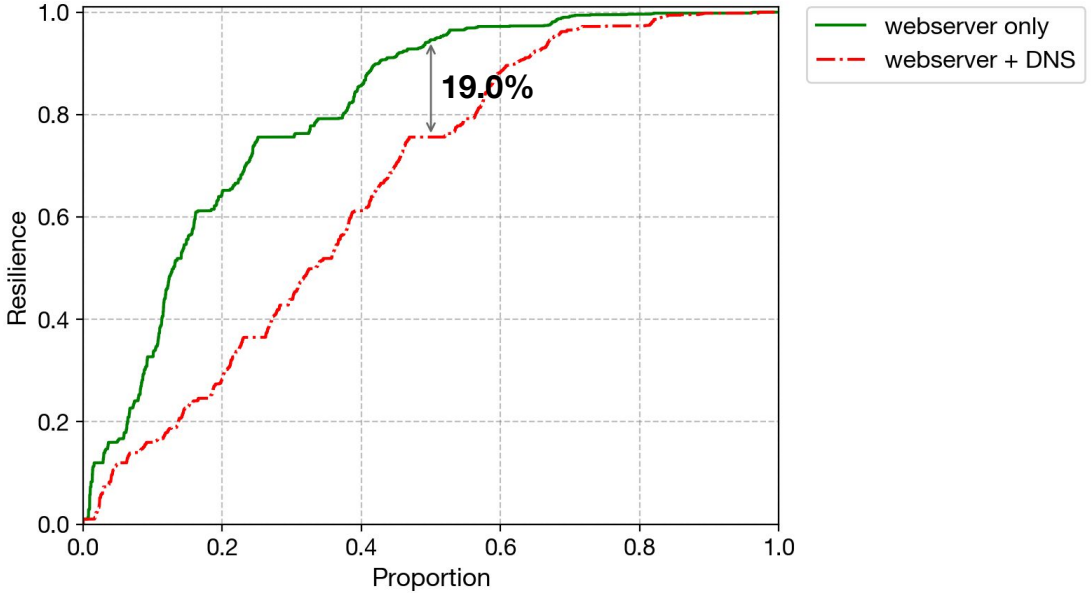
Some numbers of our measurement:

- ➔ Analyzed security of **~1.4 million domain names** from 19 VP locations
- ➔ Sent over **31 billion DNS queries**
- ➔ Simulated more than **400M network attacks** on **11K potential multiVA deployments**

Experimental Results at Let’s Encrypt

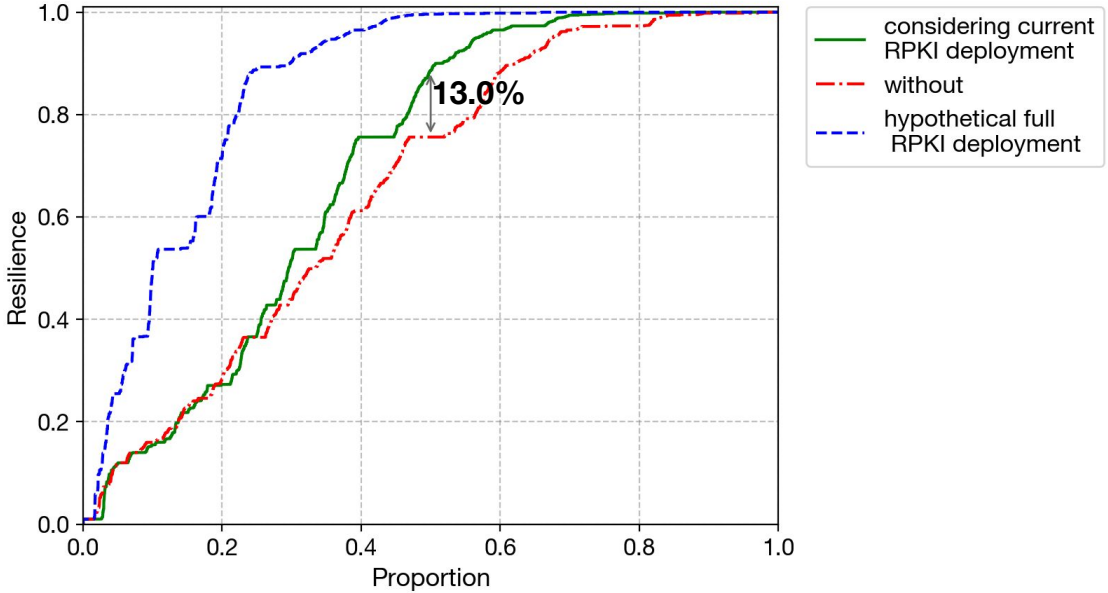
Point #1: DNS as a potent attack vector for BGP hijacks

resilience: proportion of attackers that could not gain certificate for a domain using network attacks



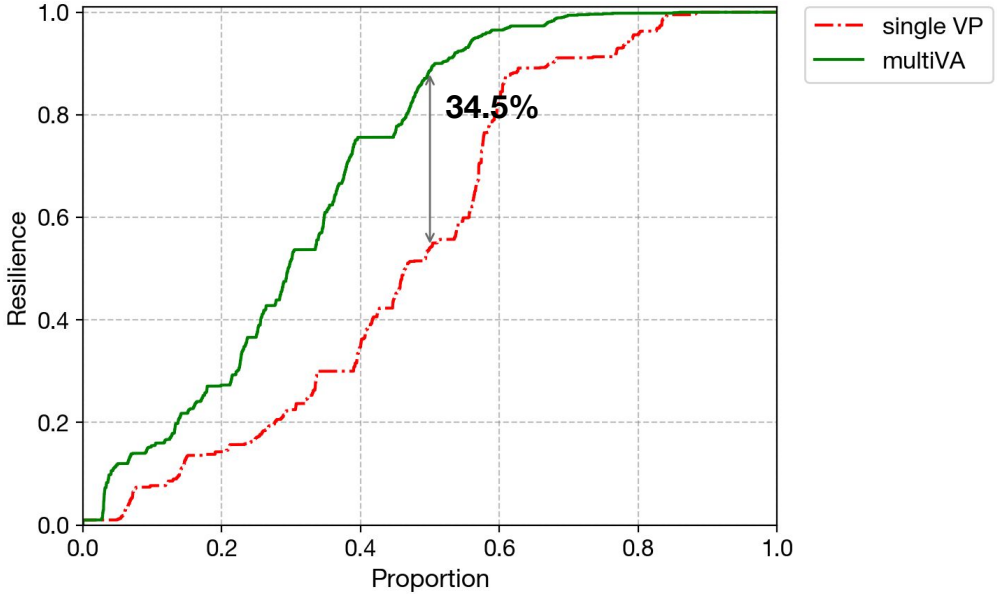
Enhanced attack surface uncovers ***almost 20% more attackers could succeed in gaining a cert for the median domain*** than previously estimated; underlines need for more usage of DNSSEC

Point #2: RPKI yields significant security gains even in partial deployment



Encouraging results for growing RPKI: **improvement of 13%** for the median domain when considering security benefit of current deployment of RPKI

Point #3: Security benefit of multiVA in the face of multiple network attacks



Let's Encrypt's current multiVA strongly beats single VA: ***without multiVA, over 45% of attackers can hijack a cert for half of the sampled domains***

Live Impact in the Web PKI ecosystem

- Draft of ballot proposal for requiring **multiVA as CA baseline requirement** underway

- Per our recommendations, Let's Encrypt deployed an ***additional VP in North Europe***

Conclusion

- We present concrete evidence that **multiVA provides significance resilience gains against localized routing attacks**, even in the face of live Internet routing conditions
- We develop an extensible **framework for CAs** to measure and evaluate the security of their multiVA deployments

Questions?
Grace Cimaszewski
gcimaszewski@princeton.edu

Open-source code