Secure Routing with RPKI: Status, Challenges and the Smart-Validator

Amir Herzberg

Univ of Connecticut, Bar Ilan Univ, Fraunhofer SIT

Joint project with

Tomas Hlavacek, Yafim Kazak,

Rafi Peretz, Fabian Sauer and Haya Shulman

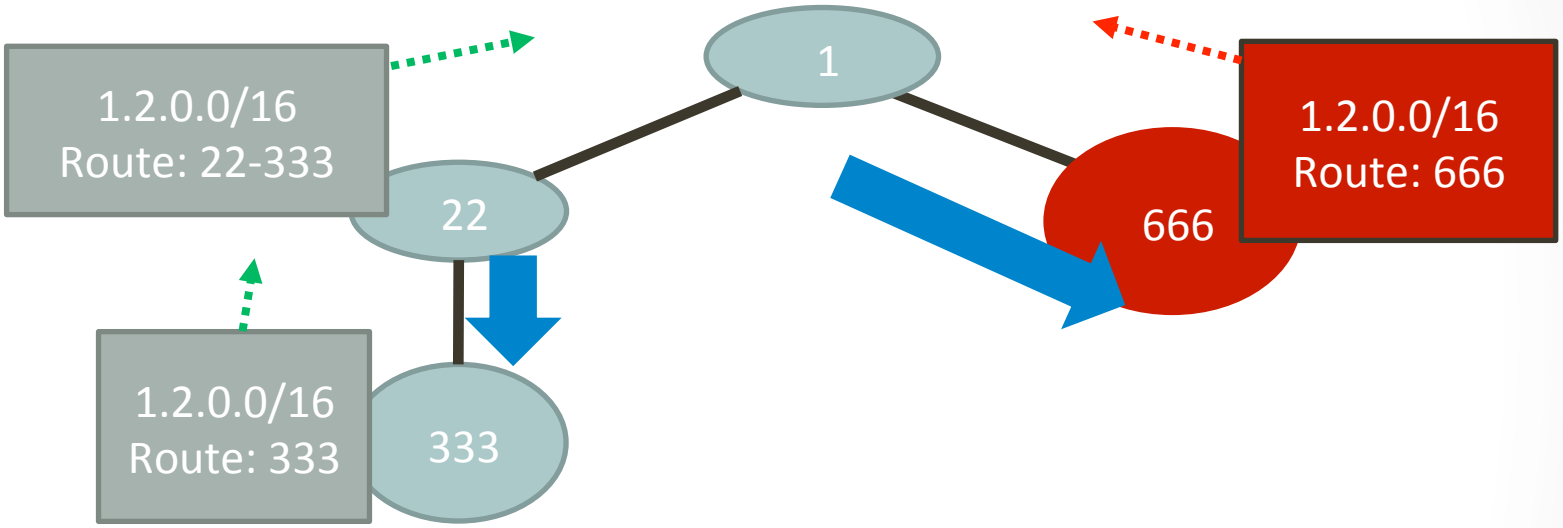
Route-Hijacking: Real-Life Example

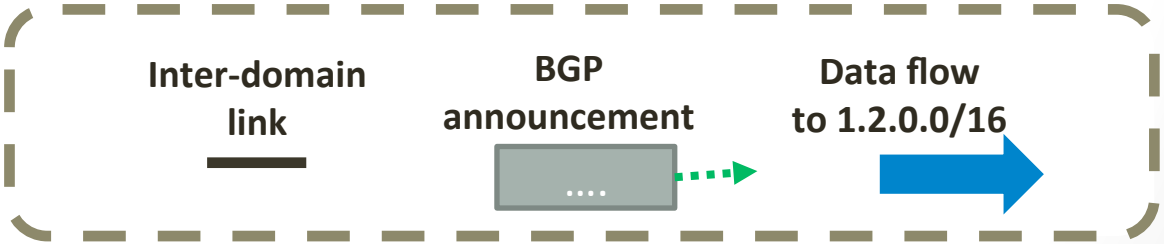
Attack Goals:

- Eavesdropping
- Spam/phishing
- Malware distribution
- Censorship
- Denial of service
- Traffic Analysis

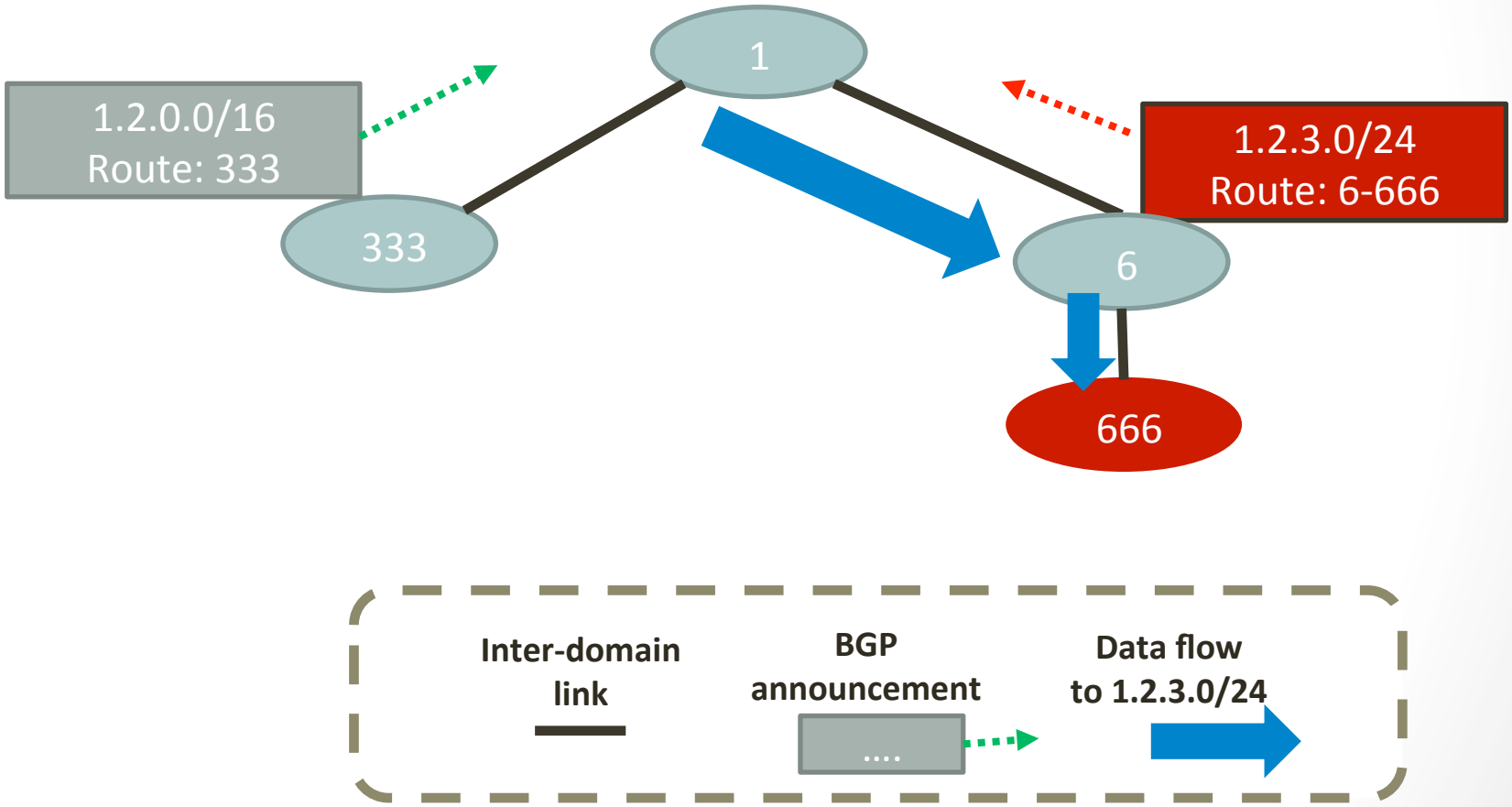
- Many proposed/deployed defenses, over many years…
- Challenge & focus : <u>deployable</u> yet <u>effective</u> defenses

Prefix Hijacking: prefer shorter route



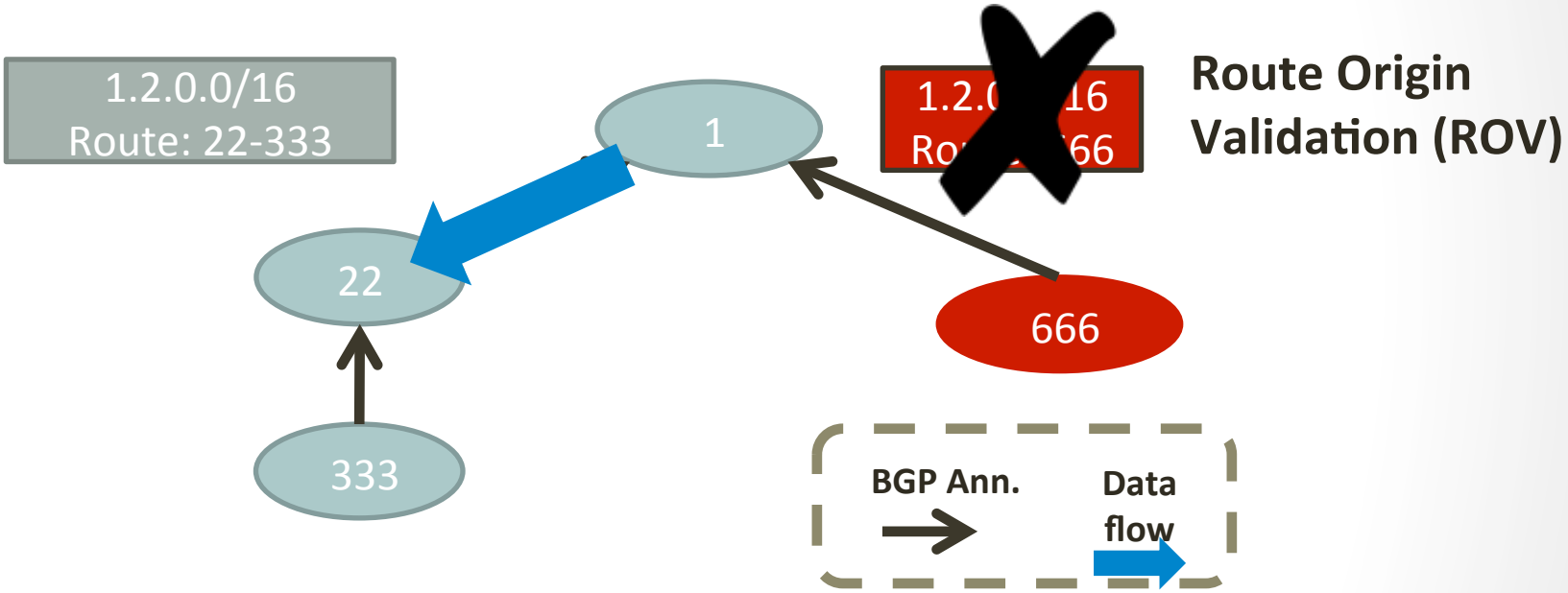


Subprefix Hijacking: **always** prefer longest matching prefix



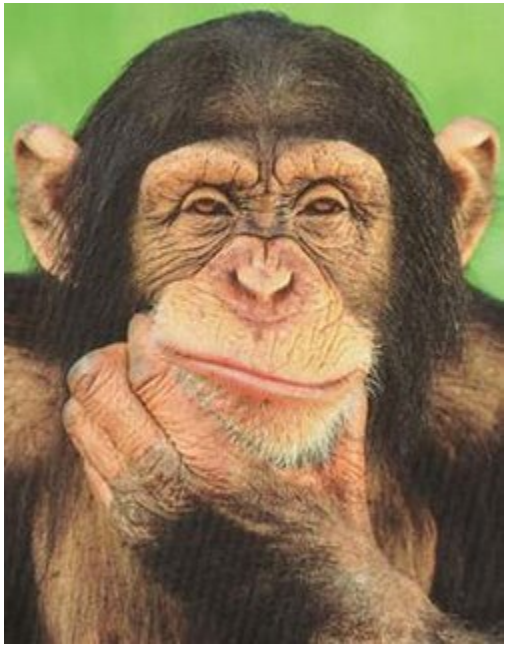
Idea: prevent hijacks using Route Origin Validation (ROV)

How??

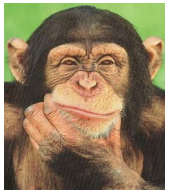


Domain 1 uses the (longer but correct) route 22-333, since only domain 333 is authorized origin for prefix 1.2.0.0/16

How to do
Route Origin Validation (ROV)
??



How to do Route Origin Validation (ROV) ??

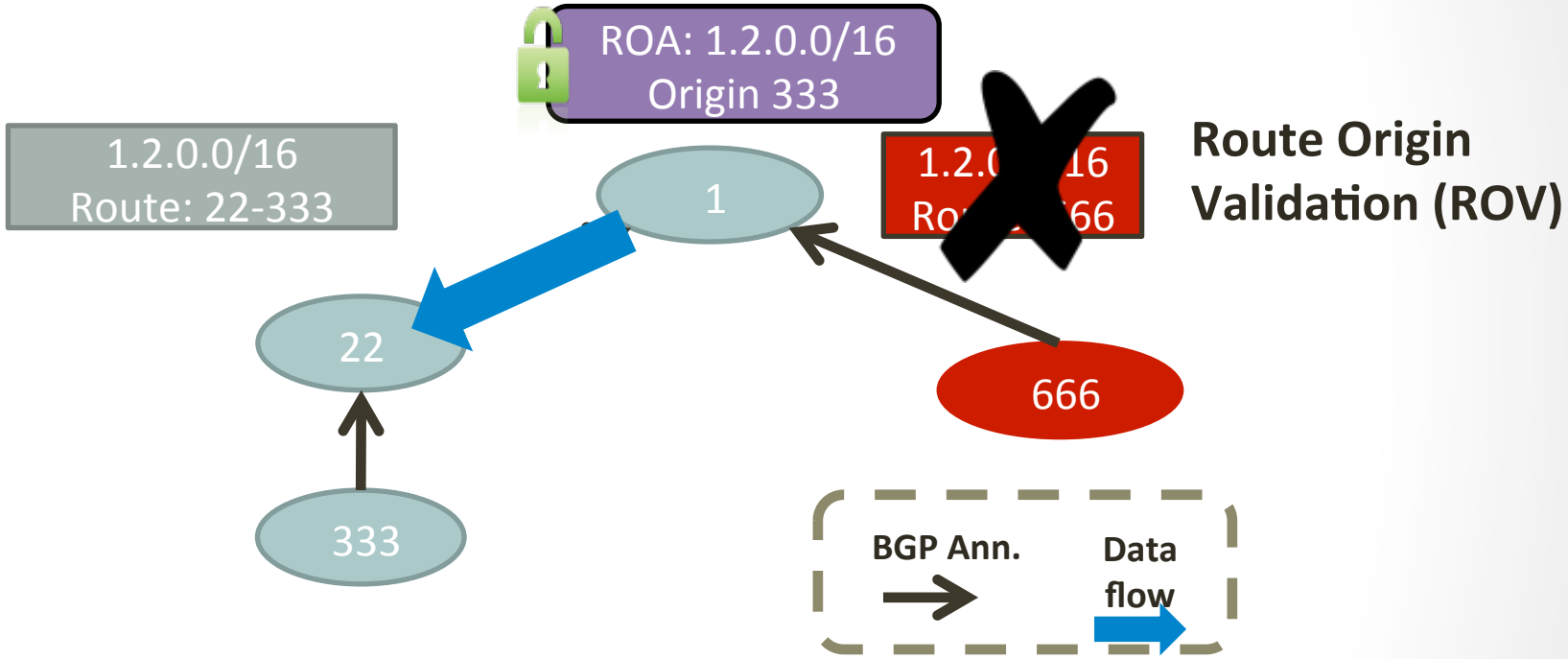


Naïvely: keep a list of valid (authorized) origin ASes for each prefix

Online check: consult DBs, e.g., Internet Routing Registries (IRRs)

Offline: digitally-signed Route Origin Authorization (ROA)

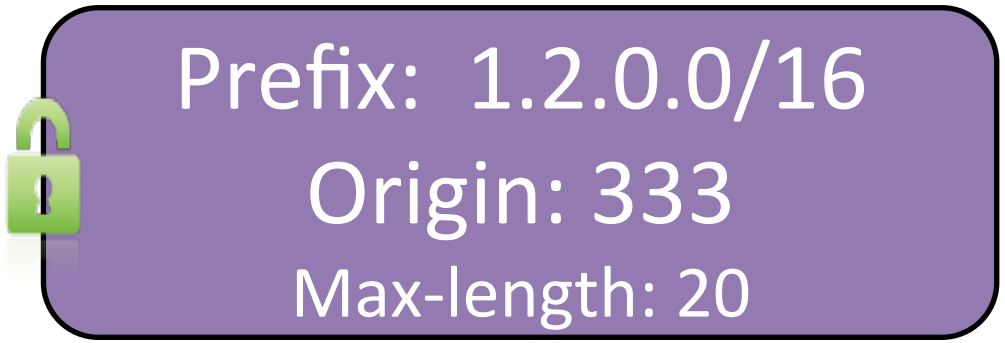
Route Origin Validation (ROV) prevents Prefix and Subprefix Hijacks



Domain 1 uses the (longer but correct) route 22-333, since only domain 333 is authorized origin for prefix 1.2.0.0/16

RPKI: Resource Public Key Infrastructure

- IETF standard [RFC 6480];
  main goal: prevent (sub)prefix hijacks (false origin domain)
- **Allows signing Route Origin Authorizations (ROAs)**:



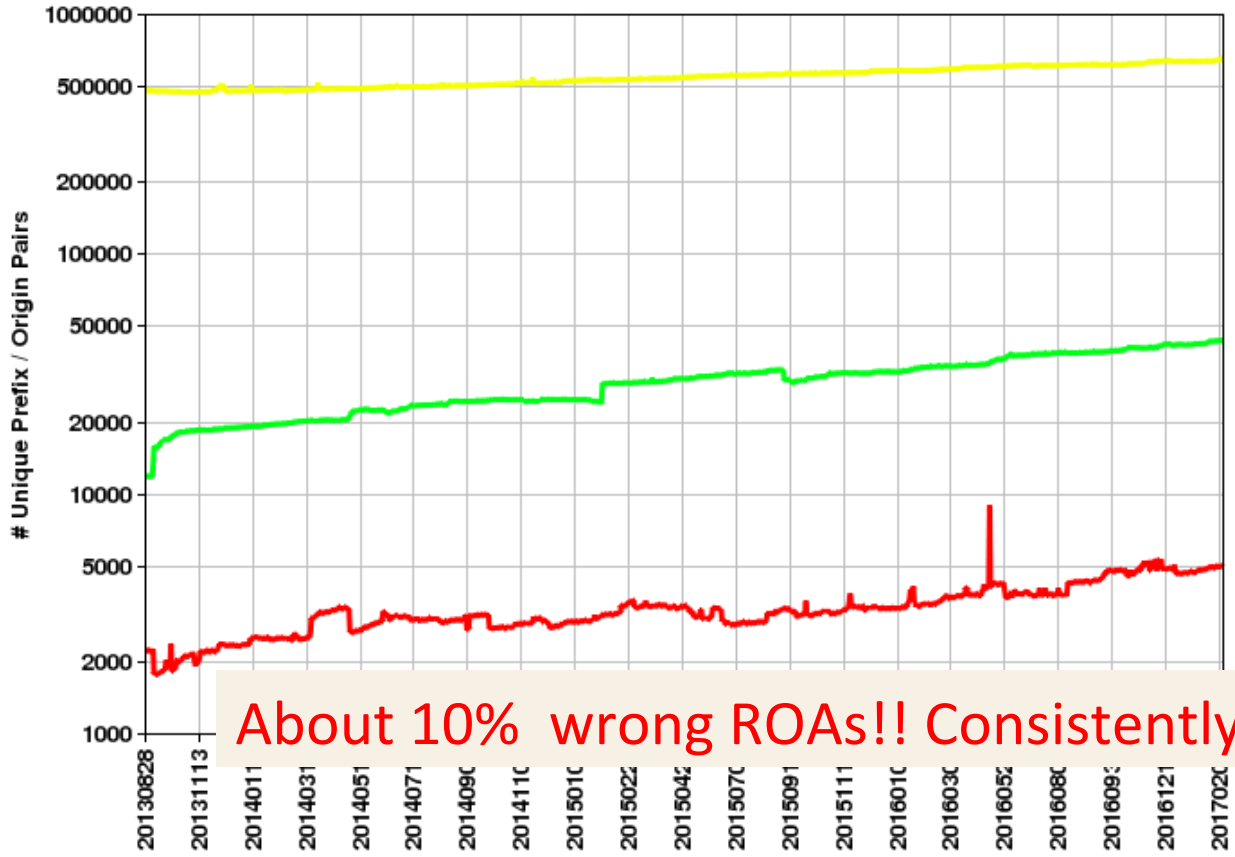
- **Facilitates Route Origin Validation (ROV):**
  - Drop BGP announcements where origin AS conflicts with ROA
  - I.e.: Origin AS is **not** 333
    Or: more specific than /20

RPKI Deployment: Agenda

- RPKI: What and Why [done]
- **State of Deployment**
  - ROA adoption: trends
  - Wrong ROA: causes and damages
  - ROV adoption status, challenges
  - Impact of partial ROV adoption
- Improving deployment: The Smart Validator
  - Phase I
  - Demo
  - Phase II
- Conclusions

ROA Adoption History

Drop BGP announcements ➔ lose (good?) traffic…
So, how many domains do Route Origin Validation?



Announced without ROA: 647,192 (93%)

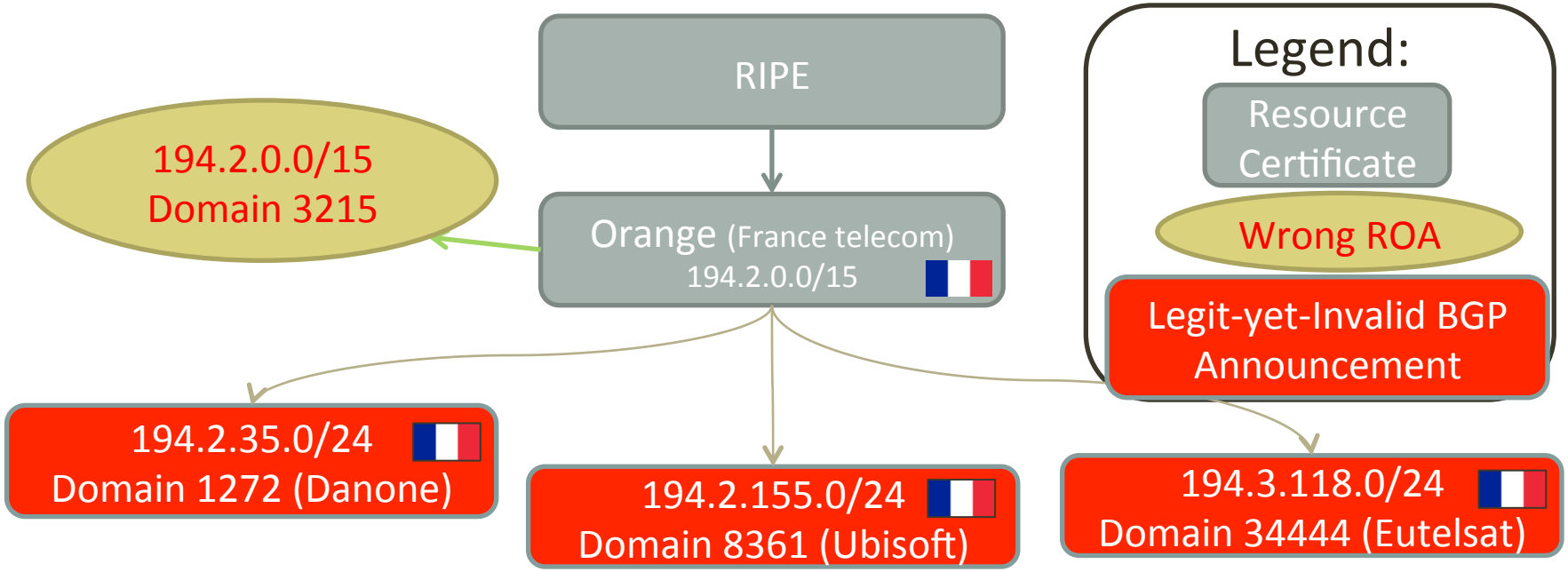
Valid ROAs: 43,796 (6.3%)

Wrong ROAs: 5,015 (0.7%)

About 10% wrong ROAs!! Consistently!!

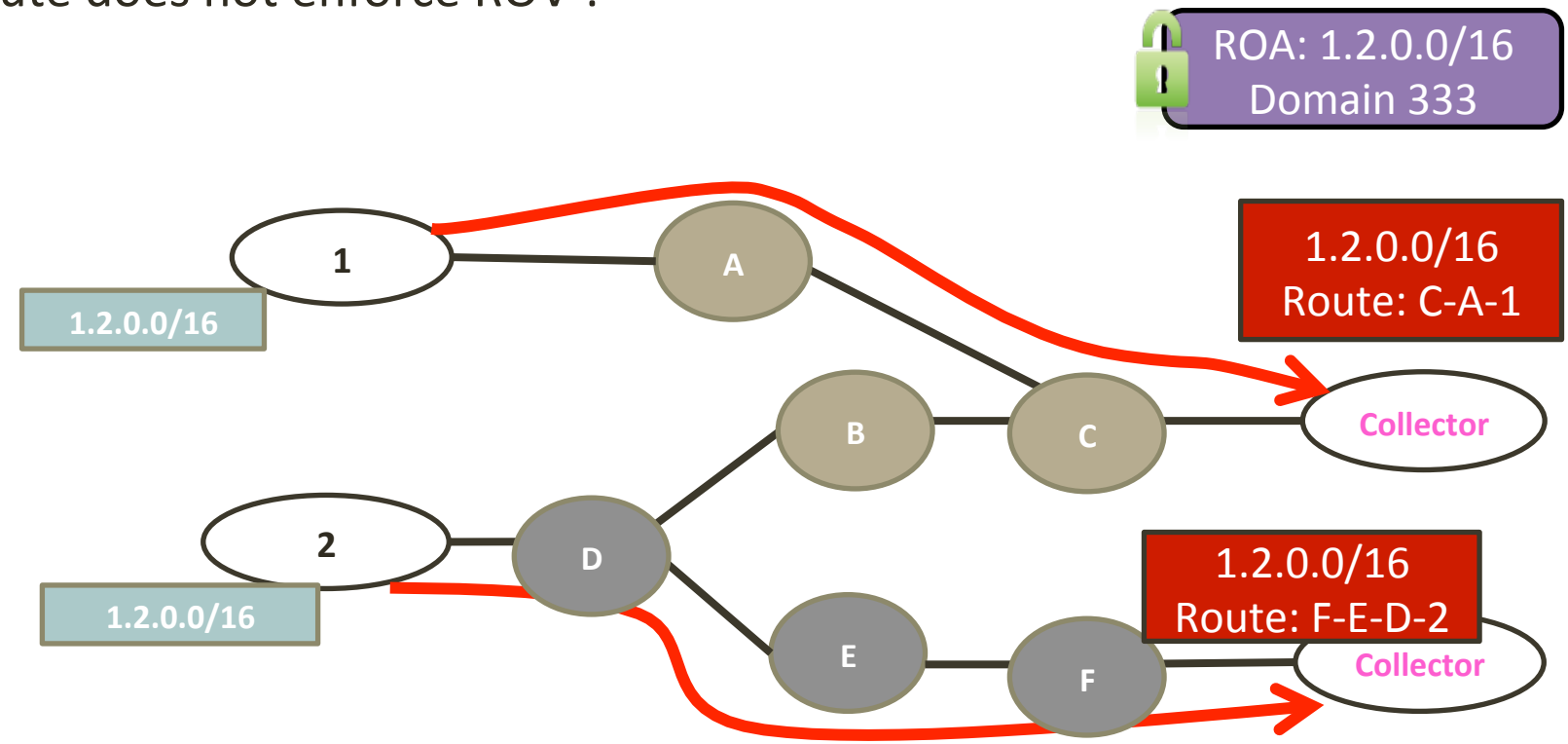
Wrong ROAs??

- Requires **both** authorizations (ROAs) and validation (ROV)
- Risk: ROV with **Wrong ROA**➔ drop legit-yet-invalid announcements
  - Does wrong-ROAs happen? – Typical, real-life example:



Measuring Adoption of Route Origin Validation

- Challenge: no direct way to measure the adoption of ROV
  ➔ no published measurements
- **Idea: use Route-View-project's BGP-collectors – and wrong ROAs!**
- Observation: if collector receives invalid announcement ➔ Entire route does not enforce ROV !

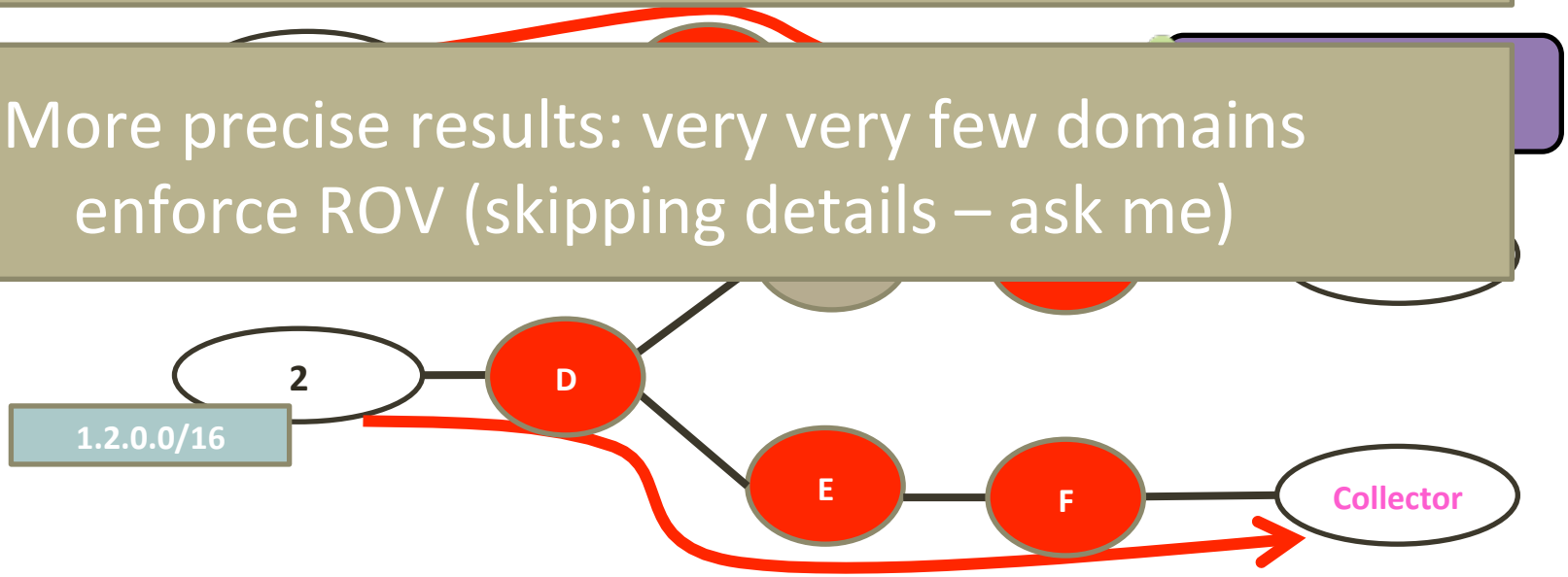


Measuring Adoption of Route Origin Validation

- Challenge: no direct way to measure the adoption of ROV
  ➔ no published measurements
- Observation : if collector receives invalid announcement
  ➔ Entire route does not enforce ROV !

At least 80 of 100 largest domains do not enforce ROV !
Can we meaure more precisely?

More precise results: very very few domains enforce ROV (skipping details – ask me)

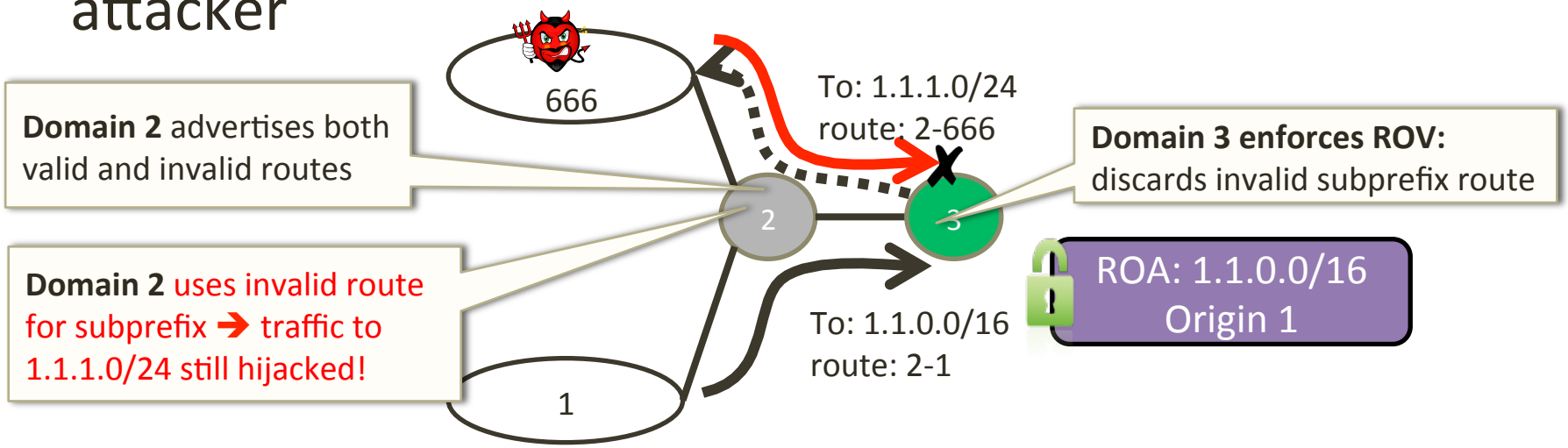


Better ROV Measurements…

- Dependency on existing wrong ROAs may be misleading
- More reliable: **publish** correct/wrong ROAs (same origin)
- Three different controlled experiments, multiple times:
  - Use RouteView Collectors (as before)
  - Use Trace-route to RIPE atlas probes
  - Use `echo' from servers (ICMP ping or TCP SYN/ACK)
- Experiments still ongoing
- Initial results: **only handful of domains enforce ROV**
  - **None** of the 100 largest domains (cf. <20)
- Similar results apparently from measurements by Randy Bush and others (didn't yet see details)
- What's the impact of partial-deployment of ROV?

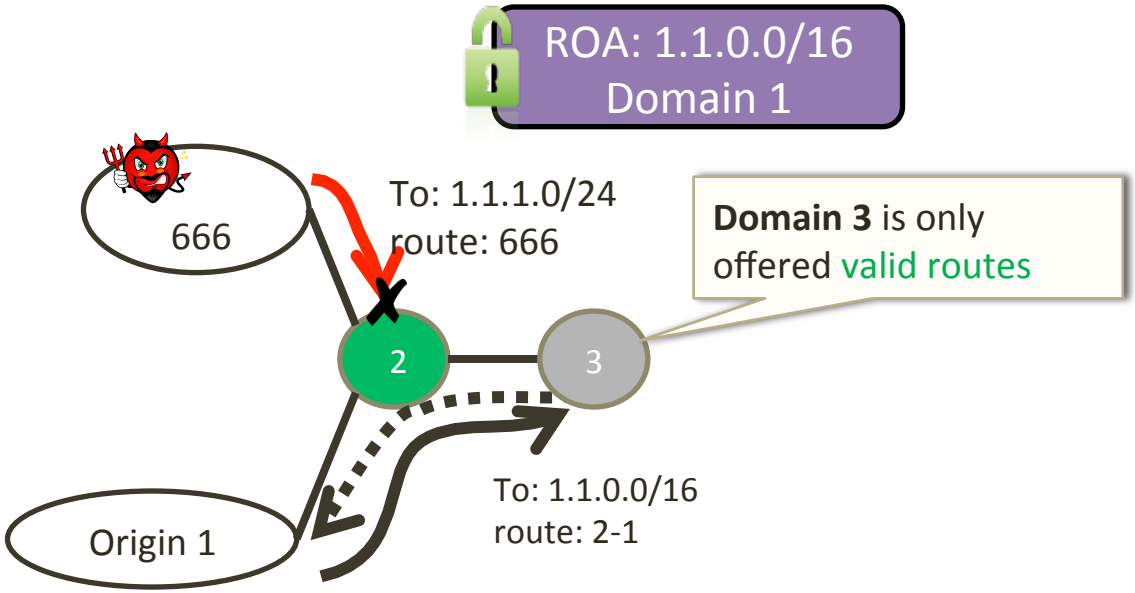
Partial Adoption of ROV:
Collateral damage

- Domains not doing ROV might cause ROV-enforcing domains to fall victim to prefix hijacking
- Control-Plane vs. Data-Plane Mismatch: domain discards invalid announcement, yet data flows to attacker



Partial Adoption of ROV:
Collateral benefit

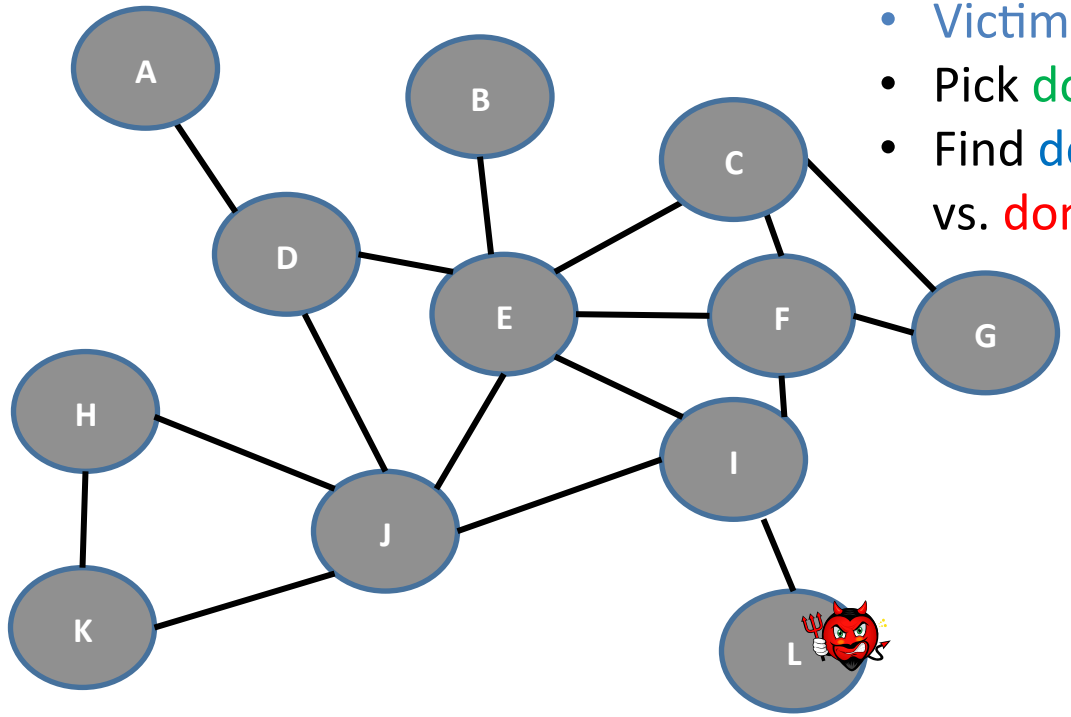
Adopters protect domains behind them by discarding invalid announcements



Drawback: less incentive to deploy (`free-riders')

Security in Partial ROV Adoption: Simulation Framework

ROA: 1.1.0.0/16
Origin: A



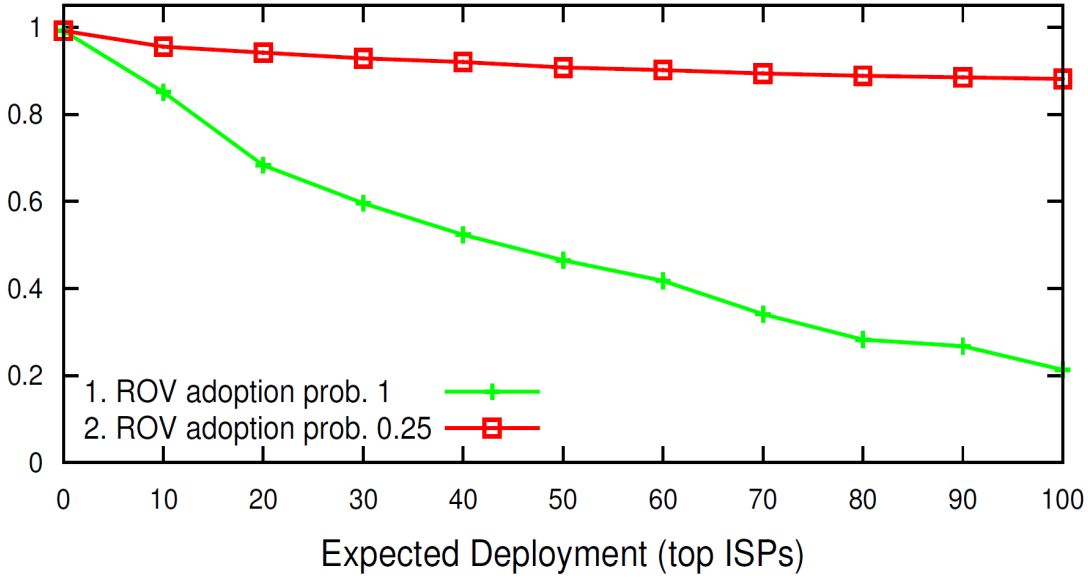
- Use Internet domain topology of CAIDA
- Pick victim & attacker
- Victim's prefix has a ROA
- Pick domains doing ROV
- Find domains sending to victim vs. domains sending to attacker

Empirically-derived topology from CAIDA. Includes inferred peering links [Giotsas et al., SIGCOMM'13]

Security with Partial ROV Adoption

- Subprefix-hijack success rate for adoption by x largest domains
- Compare: 100% vs. 25% adoption by other domains
- Significant benefit - but only if almost all large domains adopt – **and** most other domains adopt too
- We are very far from this!

Subprefix hijack success rate



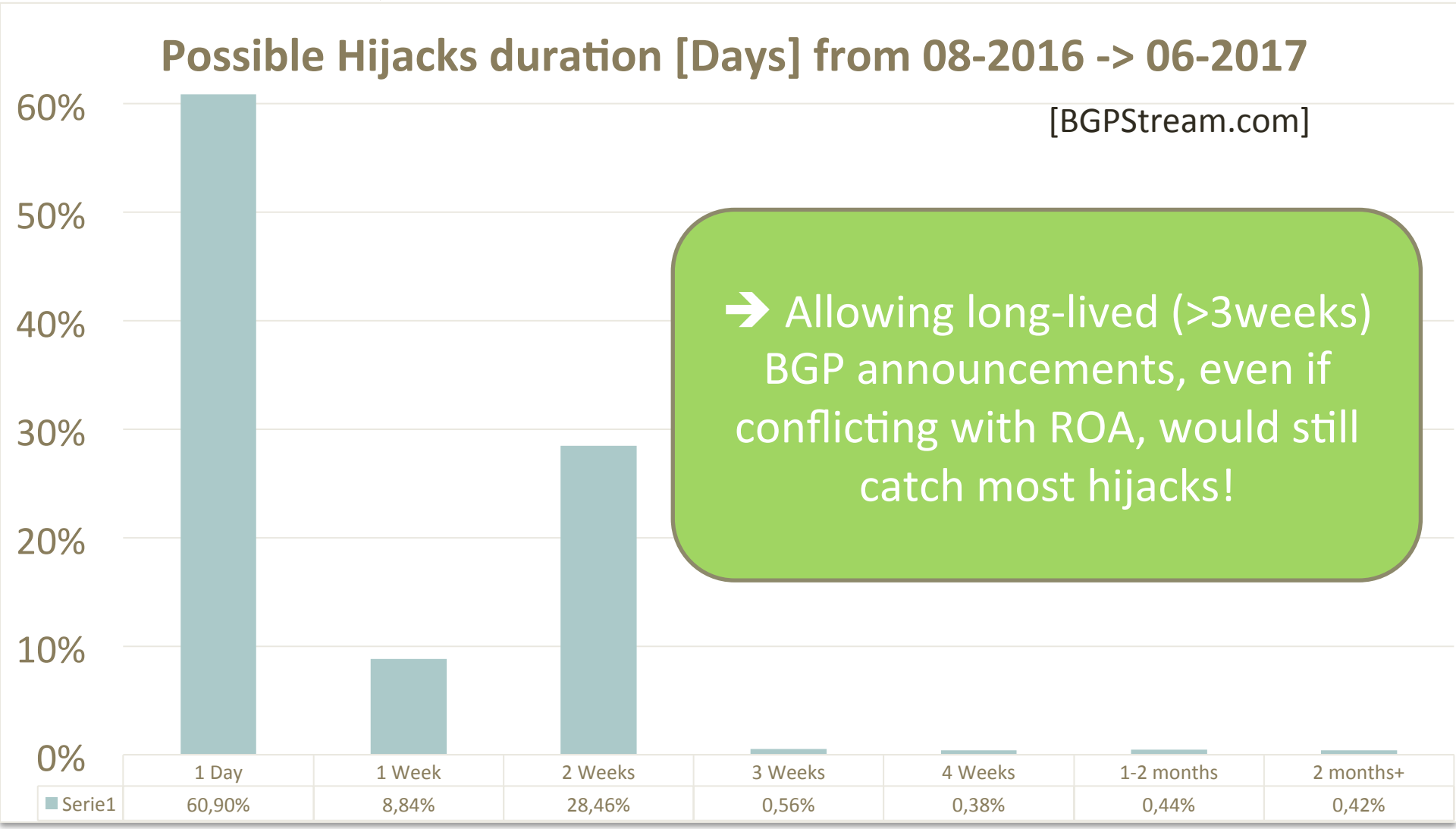
RPKI Deployment: Agenda

- RPKI: What and Why
- State of Deployment
  - ROA adoption: trends
  - Wrong ROA: causes and damages
  - ROV adoption status, challenges
  - Impact of partial ROV adoption
- **Improving deployment: The Smart Validator**
  - Phase I
  - Demo
  - Phase II
- Conclusions

Fixing ROAs and ROV deployment

- **Improve deployment of ROAs**
  - **ROAlert.org: identify wrong ROAs**
  - email alerts when sysadmin-email located: 40% fixed!
  - ➔ Should be deployed `officially'
- **Smart validator (https://github.com/SmartValidator/SmartValidator)**
  - Encourage, improve adoption of Route Origin Validation (ROV)
  - Free, open source; extends RIPE's RPKI validator
  - Phase I: `easy and safe deployment' – Do No Harm
    - Fix Conflicting-ROAs [conflicting with long-lived BGP announcments]
    - Ready, experiments beginning – join us !
  - Phase II: improved security, incentives
    - In development, will be based on new version of RIPE validator

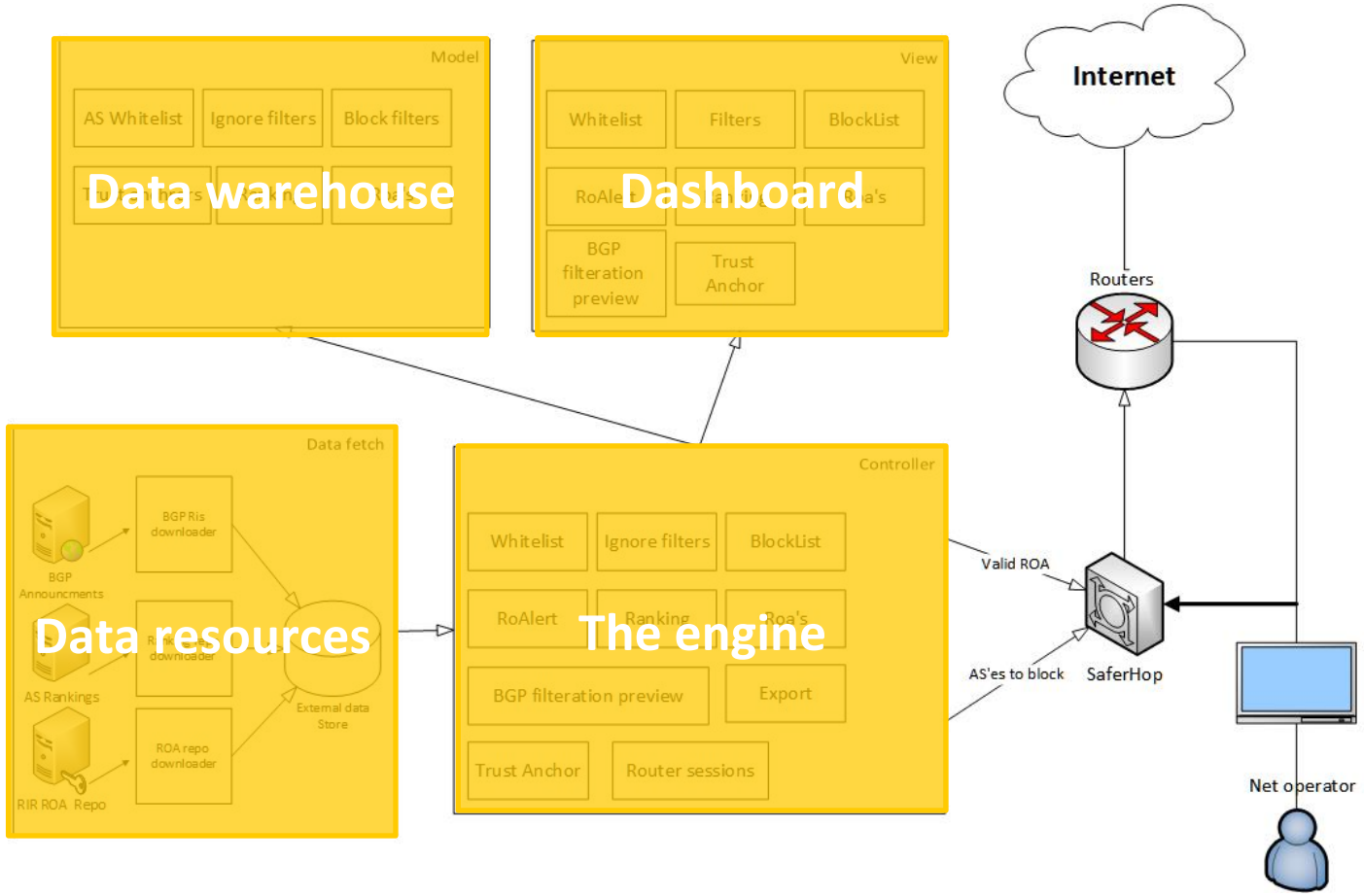
Idea: Hijacks are Short Lived



Smart-Validator: Phase I

- **Easy and safe to deploy: `plug and play'**
- **Do No Harm**
- **Recommend Mode** (default):
  - Observes ROAs and BGP announcements
  - **Recommend** BGP announcement filters
  - Operator manually applies BGP announcement filters
  - **`What-if' measurements:** impact of safe-deployment modes
- **Safe-deployment modes**
  - **Ignore mode**: ignore conflicting-ROAs
  - **Extend mode:** add auto-ROAs to cancel conflicts
- **Experiments:** Cisco, LinkedIn, … You??
- Based on RIPE's validator; free, open source

Smart-Validator: Architecture



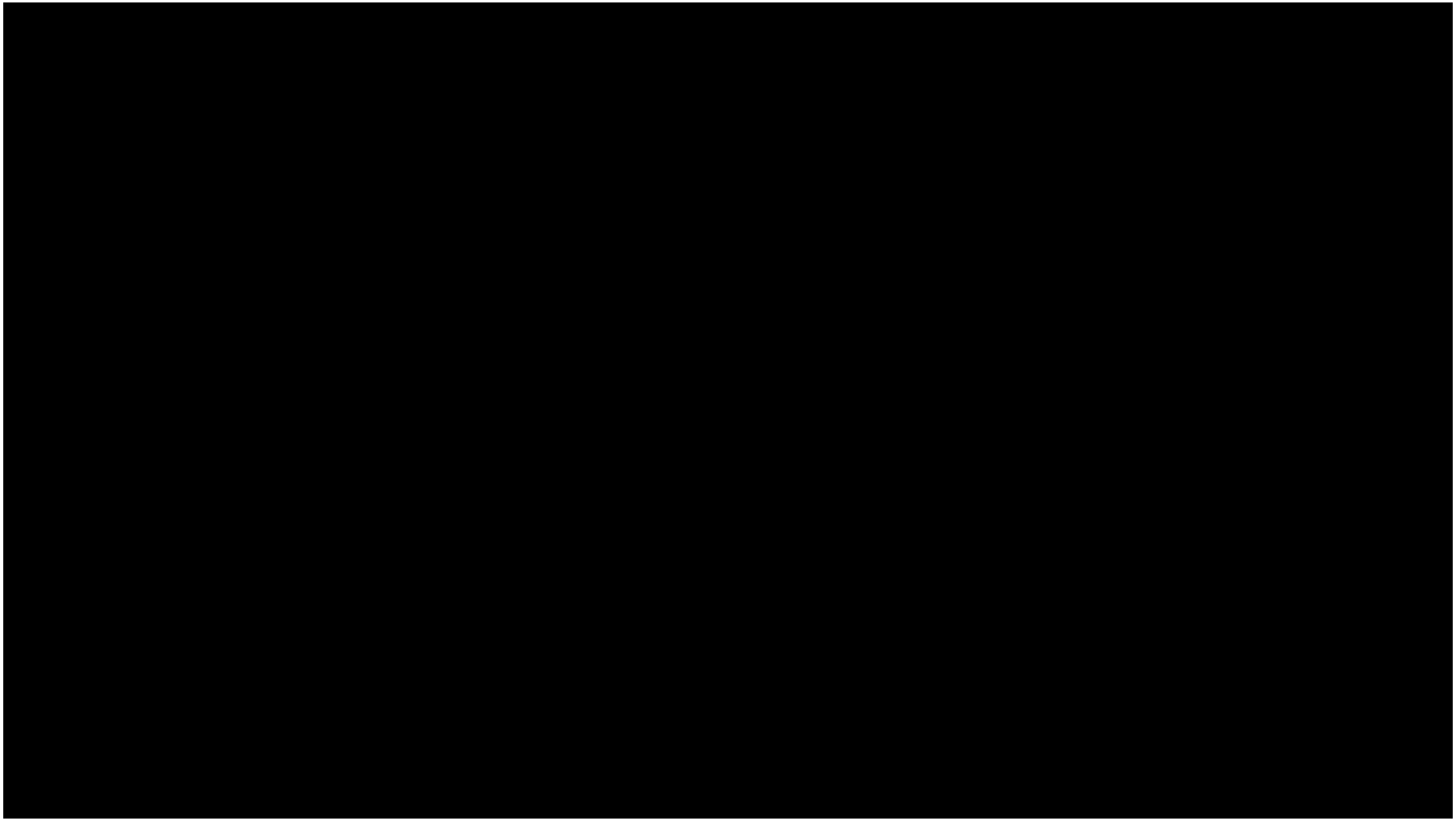
Smart Validator Dashboard Examples

Recommend mode

Extend safe-deployment mode

Demo (

github.com/SmartValidator/SmartValidator)



Smart-Validator: Phase II

- **Extend phase I with new ROV features:**
- **ROV++**:
  - Prefer ROV++ compliant providers
    - When learning of attack… or always/usually
  - Reduces risk of collateral-damage
  - An **incentive to deploy**
- **Path-end validation: easy, strong extension to RPKI**
  - Prevent `origin hijacking' by extending ROA to identify neighbor AS
  - SigComm16 paper shows: surprisingly effective!!

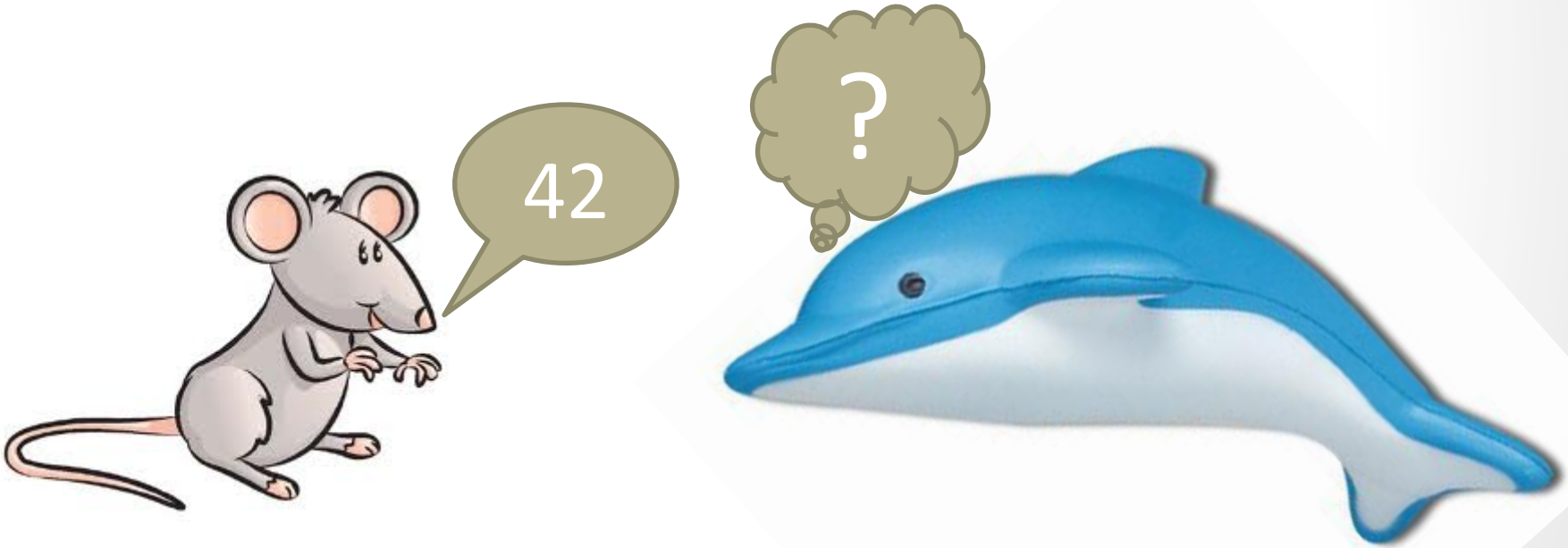
Beyond BGP: Routing Against DoS

- BGP is limited to single fixed route
  - Easier to congest – e.g., in Denial-of-Service (DoS)
- BGP isn't congestion-sensitive
  - Route does not depend on congestion, delays, loss
  - Slow response to link failure
- **IP** provides only best-effort service
  - No quality guarantees (max delay, max loss rate)
  - Quality-of-Service (QoS) extensions: only **within** domain
- → Secure Accountable Inter-domain Forwarding
  - **On going project – talk to me…**

Conclusions

- Routing security: fun & important research area
- RPKI improves BGP's security… **if** deployed widely
- Smart-validator improves ROV:
  - Phase I: make it easy and safe to deploy
  - Phase II: improve security and incentives to deployers
- Talk with us:
  - To see demo
  - To join experiments
  - To give feedback

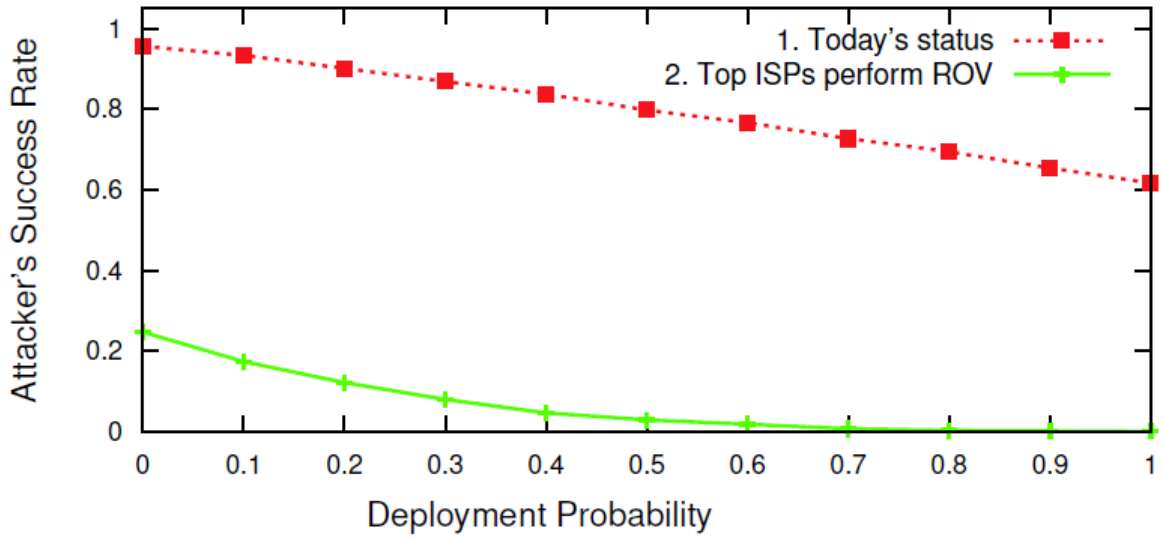
More questions?
Thanks !



Security with Partial ROV Adoption

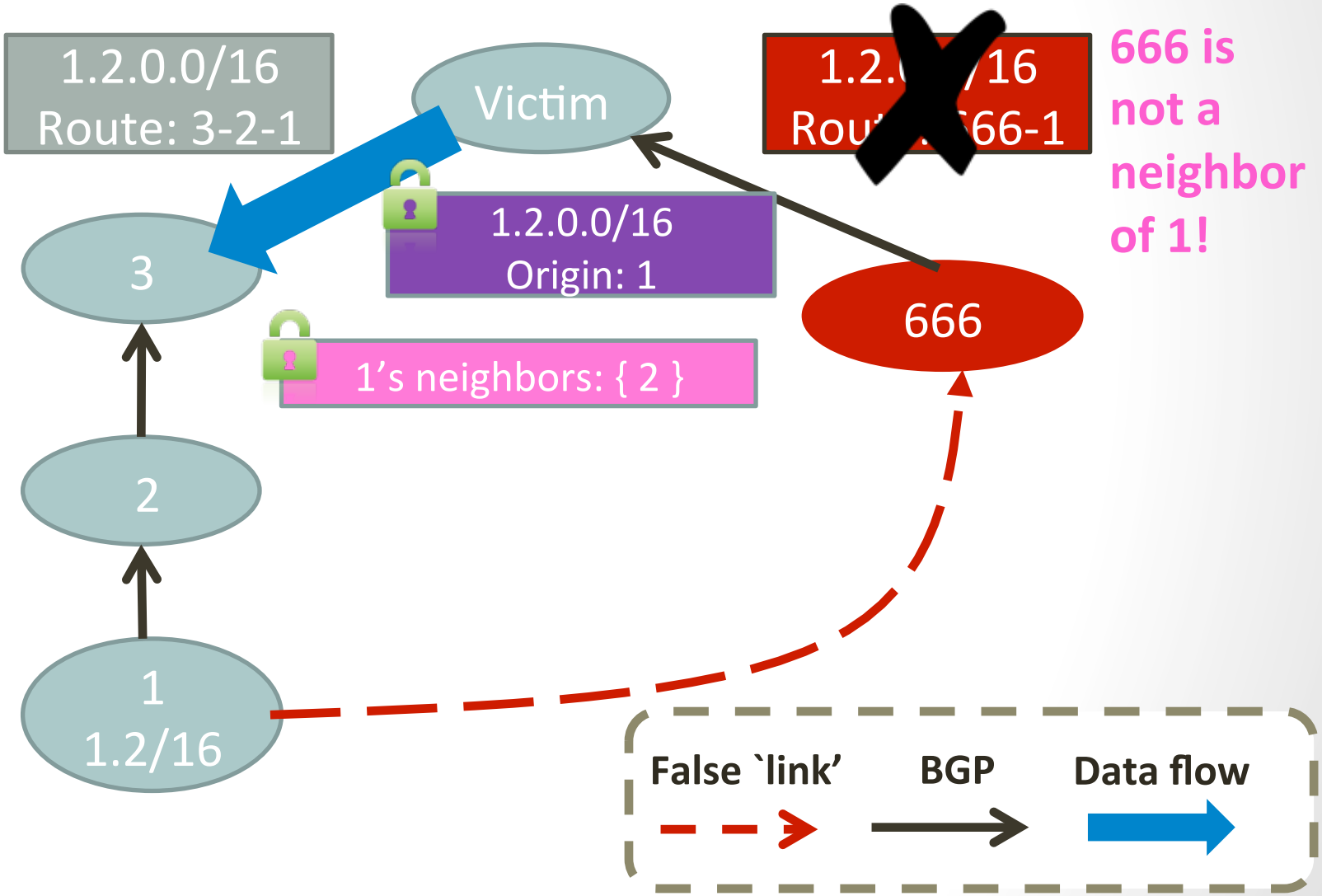
➔ Route Origin Validation (ROV) by the top domains is **necessary** and **sufficient** for substantial security benefits from RPKI

- Comparison between two scenarios:
  - ROV adopted with probability p (x axis)
  - Same, but also by the 100 top (largest) domains

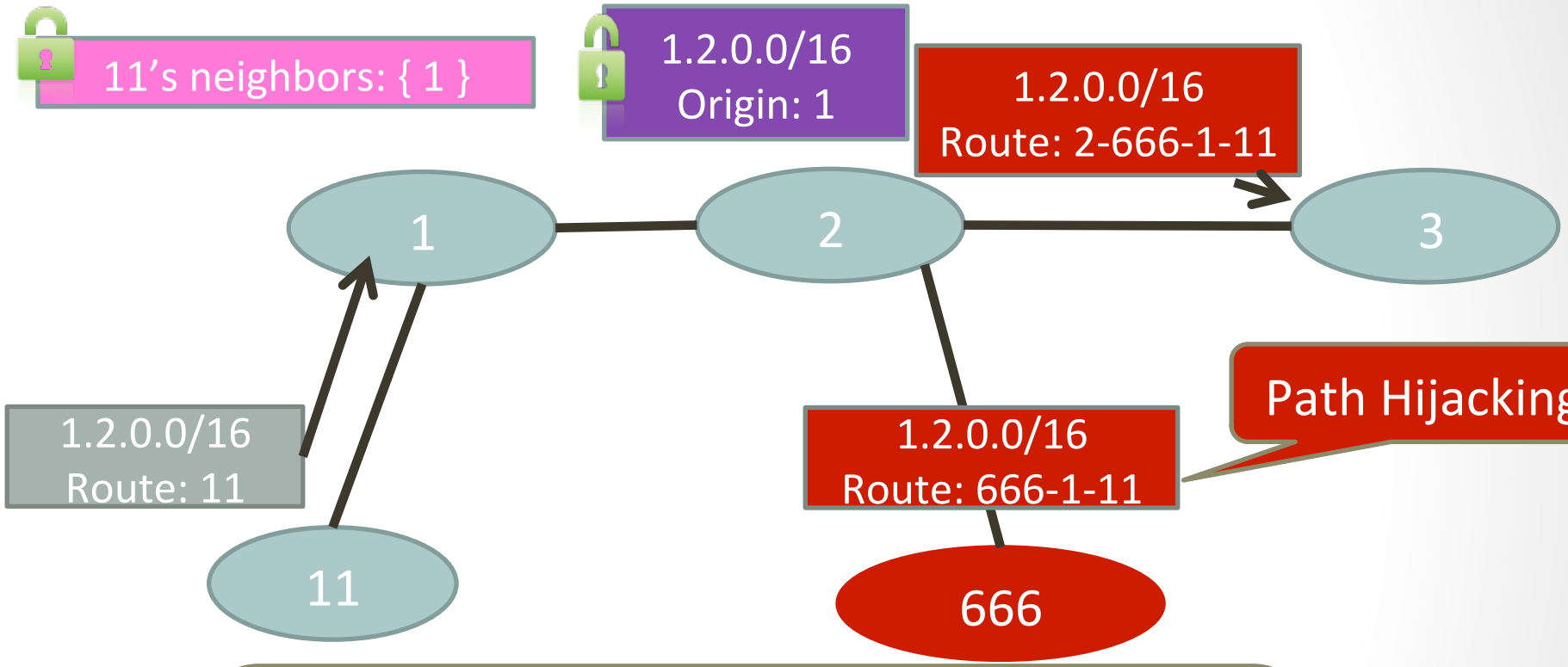


Subprefix hijack success rate

Path-End Authorization, Validation: authorized **neighbors of origin**



Path-End fails for Path Hijacking

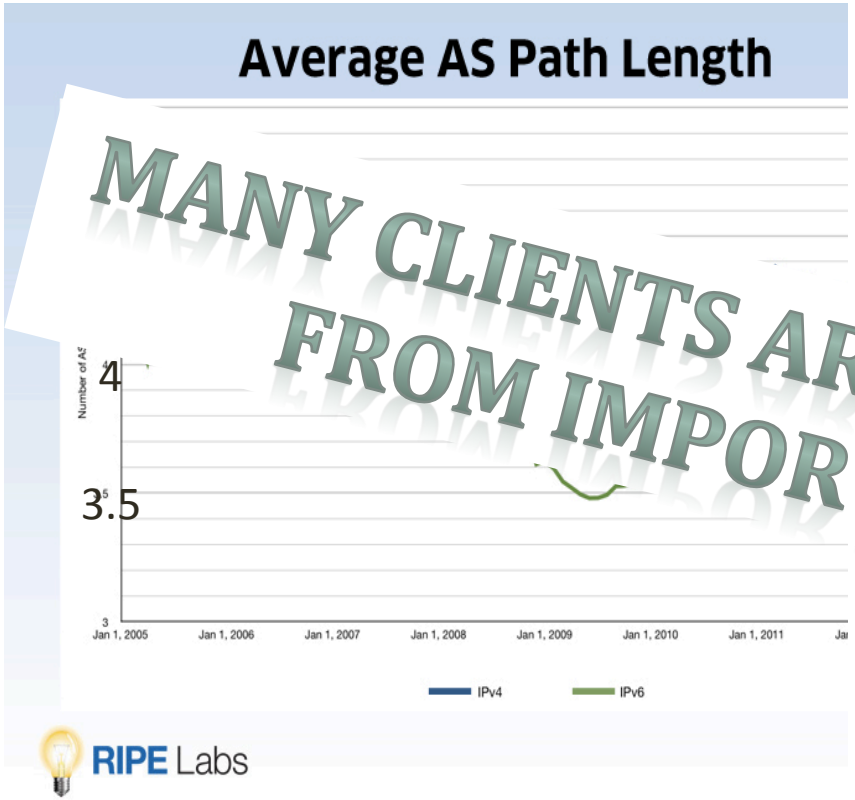


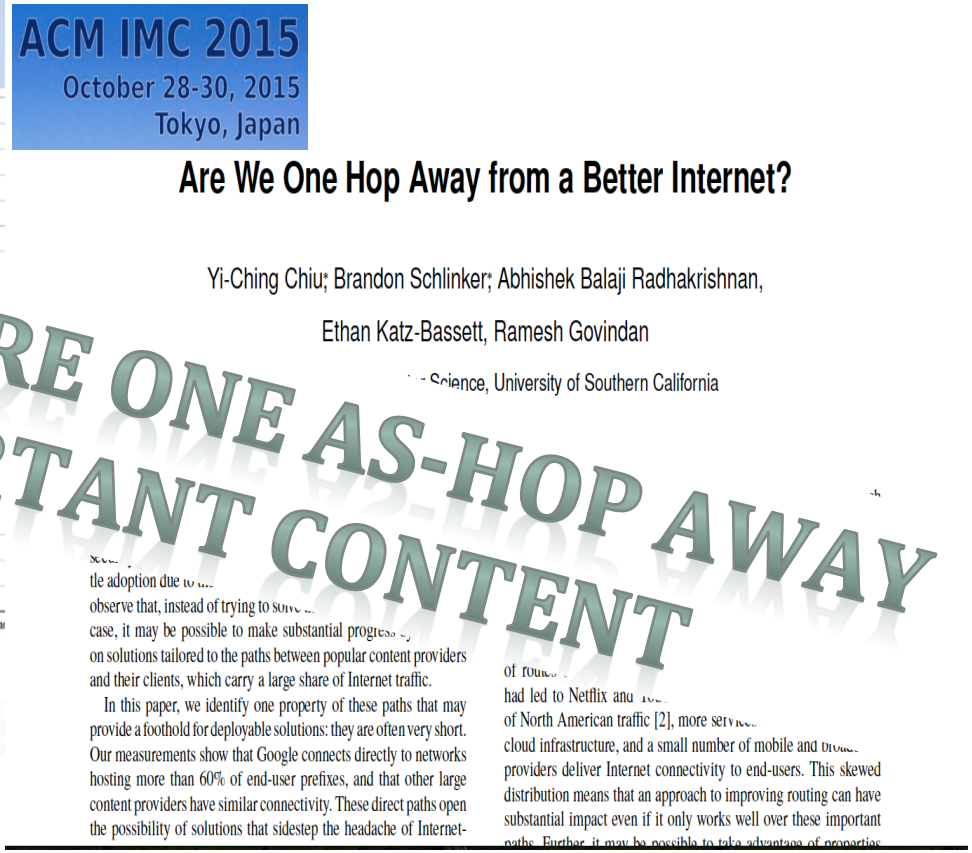
Real routes are mostly short (avg ~3.7, important content often 1!), attacker can't change relationship

➔ path hijacking rarely works!!

Path-end validation

- Extend RPKI to authenticate the “last hop”

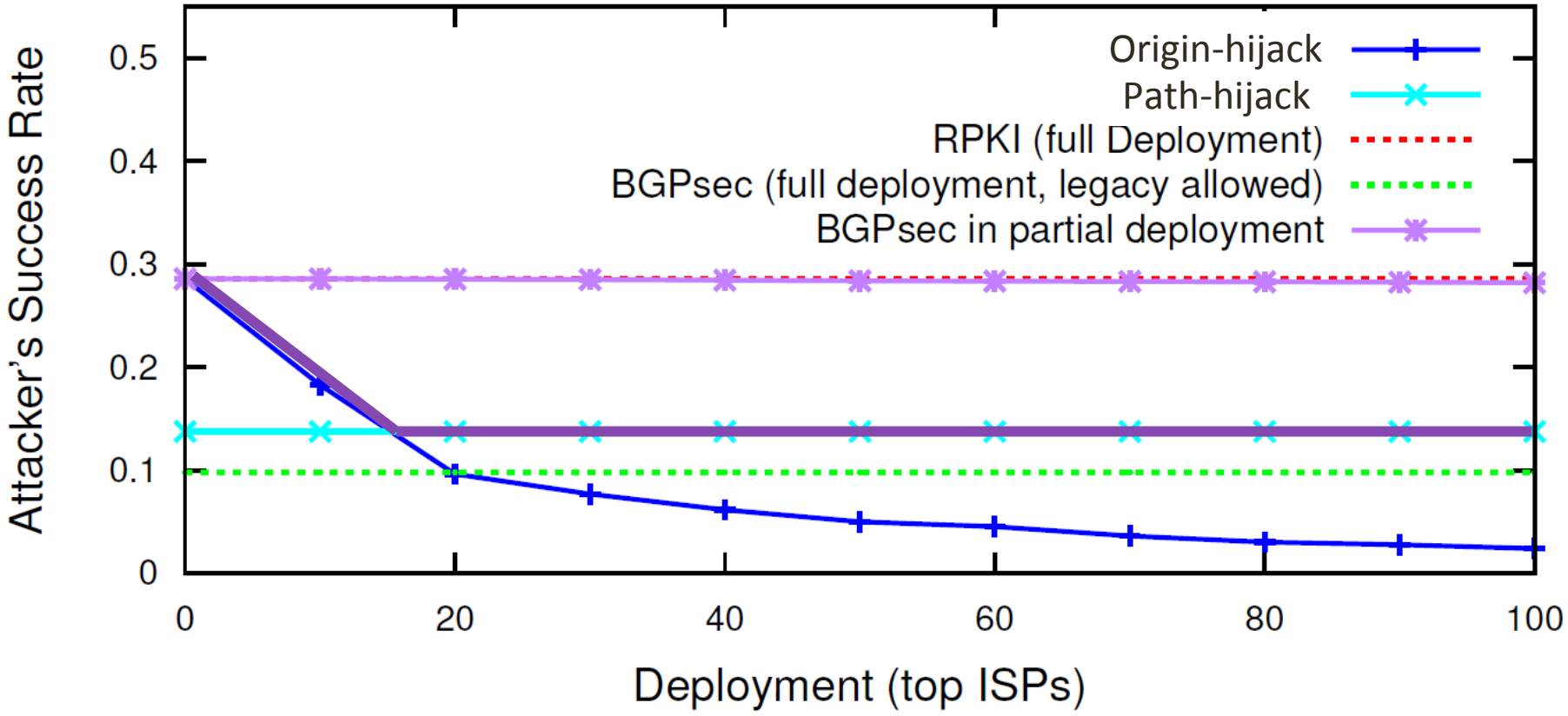




MANY CLIENTS ARE ONE AS-HOP AWAY FROM IMPORTANT CONTENT

Simulation results:

RPKI≅partial-BGPsec << Path-End



Path-End Validation: Properties

- Design ➔ Easy to deploy (≅ RPKI)
- Simulations ➔ Effective (>>BGPsec, RPKI)
- Analysis ➔
  - Do no harm property:
    preserve convergence of BGP
  - Security-monotone property:
    more adoption ➔ more security
    (BGPsec does not have this property!)

Skip theorems