Homeland Security

Science and Technology

2016 | Cyber Security Division

R&D SHOWCASE AND TECHNICAL WORKSHOP

Ensuring and Accelerating Routing Security

PARSONS, Inc

Sandra Murphy

18 Feb 2016

Team Profile

PARSONS

Prime

secure infrastructure protocols

DRAGON RESEARCH LABS

Sub-contractor

network operations

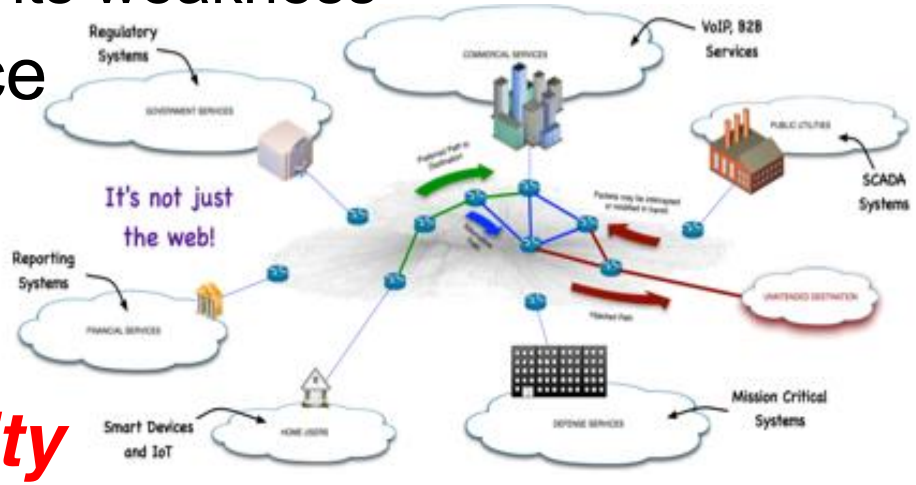
Raytheon
BBN Technologies

Sub-contractor

security; public key infrastructures

Customer Need

- Routing is a critical core-infrastructure protocol
  - *With an Achilles heel*
- Routing protocol (BGP)
  - A global, cooperative, distributed system
  - That's powerful, but also its weakness
- World-wide threat source
- World-wide impact
  - Blackholes, MITM, outages
- ***Everybody's problem***
- ***Nobody's responsibility***



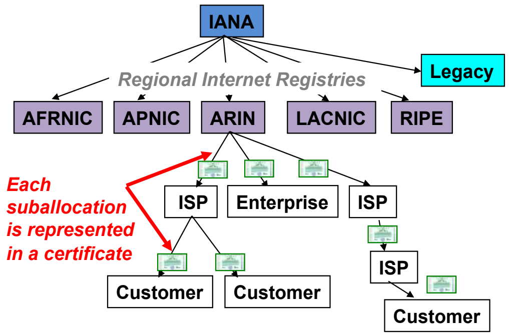
Approach (Part 1)

- **Proactive**: ***block* bogus routing information**
- Technical Solution:
  - Step 1: Certify Right to Use Addresses
  - Step 2: Origin Validation (protect creation of initial route)
  - Step 3: Path Validation (protect record of the route's path)
- Project Team and Strategy
  - Project team of experts in key areas
  - Engage with key stakeholders and gatekeepers:
    - Router vendors, operators, Internet resource registries
  - Work on all solution phases:
    standardization, implementation, and deployment
  - Parallel existing systems and operations

Approach (continued, Part 2)

STEP 1: Certify the right to use addresses

Parallel existing address allocation system



Each suballocation is represented in a certificate

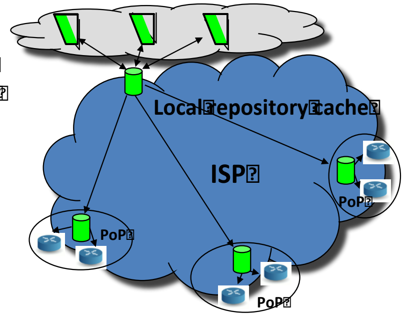
Resource Public Key Infrastructure - RPKI

STEP 2: Origin Validation
(protect creation of initial route)

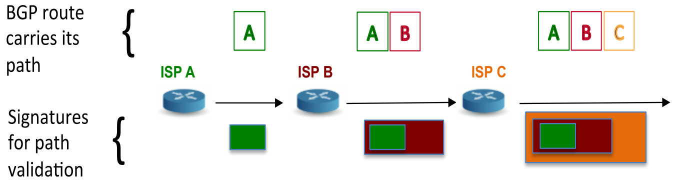
- RPKI route authorization object: prefix holder authorizes ISP to originate route
- Routers use RPKI authorization to validate the route origin

Globally Distributed CA Repositories

Cache-to-router protocol delivers list of authorized prefix origins to routers in real time.
Routers do NO crypto



STEP 3: Path Validation
(protect build up of the route's path)



ISP signs everything it receives to validate the path

- Originators, ISP A sign what they originate
- Propogators, ISP B and ISP C, sign what they propagate
- Routes collect signatures as they pass through the network

Protections parallel legitimate behavior

Proactive solution: BLOCK bogus routing

Approach (continued, Part 3)

Stages of ISP Deployment

Choose activities to facilitate deployment in each stage

	Reluctance	Doubting	Planning	Beginning to Move	Progressing Steadily
Standards	• Start solution	• Formalize Solution	• Obtain feedback • Revise as needed	• Document BCPs	• Define needed extensions
Outreach	• Recruit Core Experts • Explain need to other Experts	• Explain path • Widen Publicity • Tutorials	• Coordinate policy • Find early adopters	• Hold tutorials • Technical & Policy Conferences	• Widen outreach • Articles & Workshops
Technical	• Analyze • Measure Risk	• Predict needs • Start tools	• Interop. tests • Deploy tools	• Monitoring • Scaling • Performance tweaks	• Measure growth • Fix slow areas

Culture change: *explain the need, create the tools, find a leader, publish use cases*

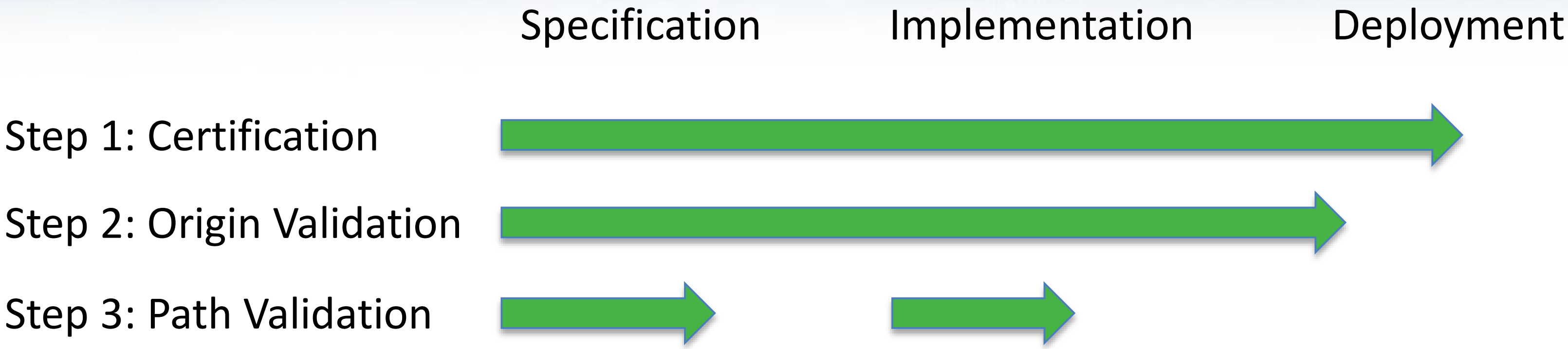
Competition

- **Reactive** systems
  - Routing-history-based anomaly detectors
    - BGP-route collectors and alert services
    - Collectors: RouteViews, RIPE RIS, PacketClearingHouse
    - Alert services: research and commercial: e.g., Cyclops, Dyn Research, BGPMON
- **Proactive** systems
  - Best current practice is BGP route filters
    - Based on customer input or Internet Routing Registry (IRR) data
  - Issues with best current practice
    - **AUTHORIZATION**: Input (customer & IRR) authorization is weak
    - **EFFECTIVENESS**: Most effective close to error
    - **COVERAGE**: Mostly for origin validation, not path validation
    - **PERFORMANCE**: Filters (475K lines) challenge memory; filters must be rebuilt and reloaded periodically; loading new filters seriously impacts operations

Benefits

- **Proactive**: Block bogus routing, rather than detect and alert
- **Authorization**: Routing information is certified with high assurance
- **Effectiveness:** Validation effective anywhere in the Internet
- **Coverage**: Path validation as well as origin validation
- **Performance:** Incremental update, no need to rebuild full set
  - Updated information can arrive in real time without disrupting operations

Current Status (Part 1)



Specification Implementation Deployment

Step 1: Certification

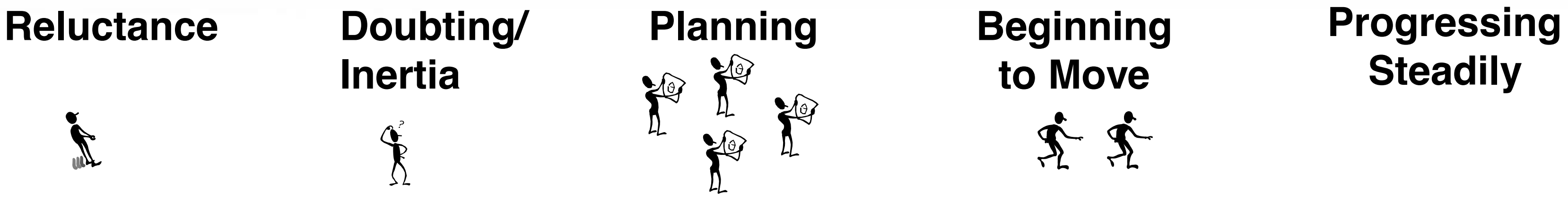
Step 2: Origin Validation

Step 3: Path Validation

- Certification:
  - All global registries certifying member resources
  - 2.3M address blocks certified, world-wide
- Origin Validation:
  - Three top router vendors support in shipping code
  - Top US companies with deployment in progress
    - using DHS funded implementations
- Path Validation:
  - specifications mature but not yet published

Current Status (continued, Part 2)

Deployment – Origin Validation - Current Stage



- Building tools to aid deployment:
  - Workshop in a Box – training and planning
  - RPKI Visualization – certification monitor
  - Router-RPKI Monitor – origin validation in operation
  - Emulation and Operation Monitor – planning and operations
  - Rpki.net and RPSTIR – standards and operation
- Participating in policy development

Next Steps

- **FROM NOW TO COMPLETION**: Ensure and accelerate deployment:
  - Tools
    - Ease barriers, monitor, diagnosis, performance
  - Community
    - Training, workshops, tutorials, outreach, community building
    - Working with major providers (ISP, data center, cloud)
    - Working with major address holders to encourage deployment
  - Policy
    - Work with principal policy bodies – registries, government, sector
    - Work with policy bodies' clients and members
  - Specification
    - Complete path validation standardization!
    - As needed, address specification issues

Potential Transition Activities

- **TECHNOLOGY TRANSITION:**
  - Transition to commercial products in place
  - Transition to critical gateholders in place
- **MAJOR CULTURE CHANGE FOR OPERATIONS:**
  - Ensure community understands need
    - (outreach; status monitors)
  - Ensure community has the means to make the change
    - (OAM tools for internal operations)
  - Find a leader
    - (working with major networks for use cases, experiments, etc.)

Contact Information

Sandra Murphy
PARSONS, Inc.
Sandra.Murphy@parsons.com
+1 443-430-8065

PARSONS

EARS information

- www.securerouting.net
- www.rpki.net
- http://sourceforge.net/projects/rpstir/

Homeland Security

Science and Technology

2016 | Cyber Security Division

R&D SHOWCASE AND TECHNICAL WORKSHOP