Enhancing and Accelerating Routing Security (EARS)

PARSONS

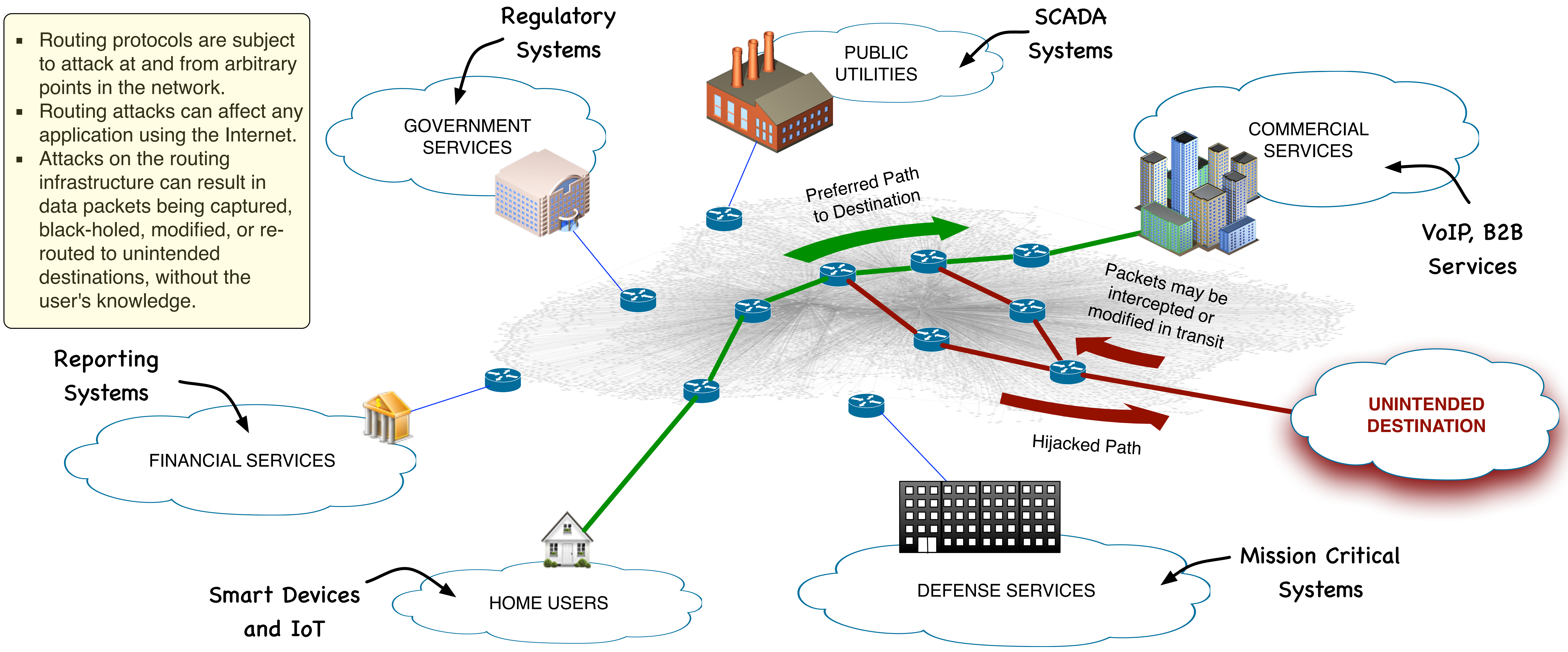
DRAGON RESEARCH LABS

Raytheon BBN Technologies

http://securerouting.net

THE PROBLEM

- Routing protocols are subject to attack at and from arbitrary points in the network.
- Routing attacks can affect any application using the Internet.
- Attacks on the routing infrastructure can result in data packets being captured, black-holed, modified, or re-routed to unintended destinations, without the user's knowledge.



THE IMPACT

- Routing is an essential part of Internet communication impacting all Critical Infrastructure Sectors.
- There have been a number of widely publicized routing incidents in the past that have resulted in real operational issues. Even unintentional attacks can cause widespread disruption of Internet communication. Some incidents may be intentional, long-term and can be difficult to correct.
- The Internet architecture and its emerging services (e.g. cloud) vastly increases the potential for routing attacks.

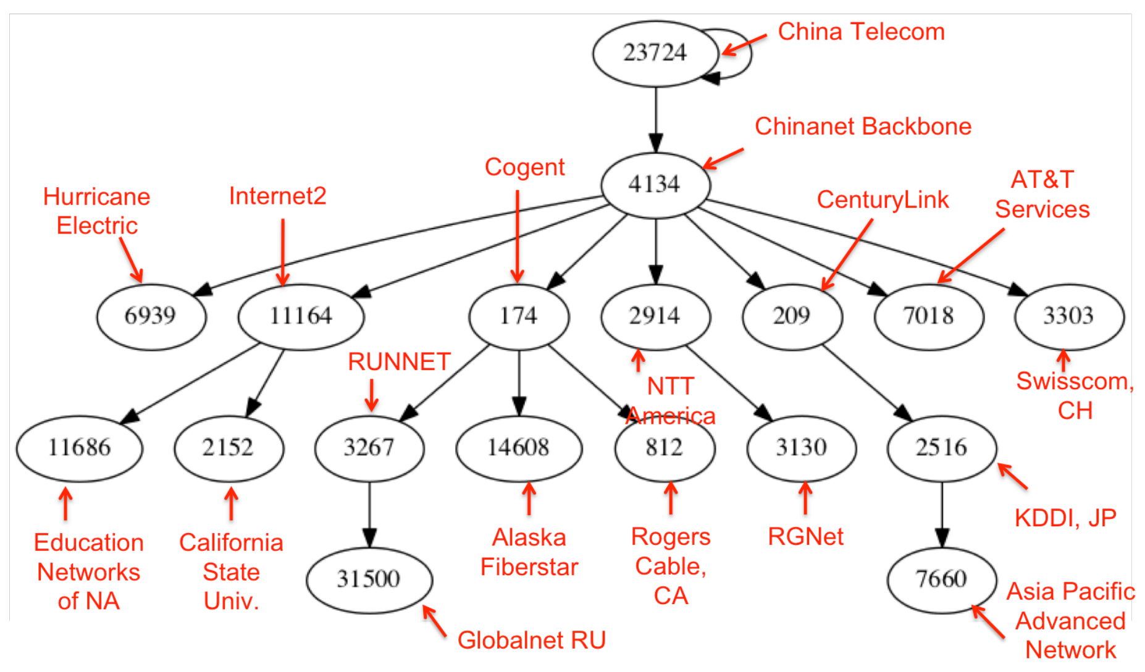
Some Recent Routing Attacks

- 2015/06/30 - A configuration error results in nearly 28,000 global prefixes being mis-originated by an ISP in Bangladesh.
- 2015/03/07 - UK traffic, including some destined for UK's Atomic Weapons establishment rerouted through Ukraine.
- 2014/09/10 - AS13110 hijacks a prefix that was assigned to the US Dept of Defense.
- 2014/03/29 - Turk Telekom deliberately hijacks the IP addresses for popular free and open DNS providers such as Google, OpenDSN and Level3.
- 2014/03/22 - Bitcoin money stolen through BGP hijack.
- 2010/04/08 - China Telecom originates 15% of the Internet's address space.

Example of Large-Scale Routing Incidents

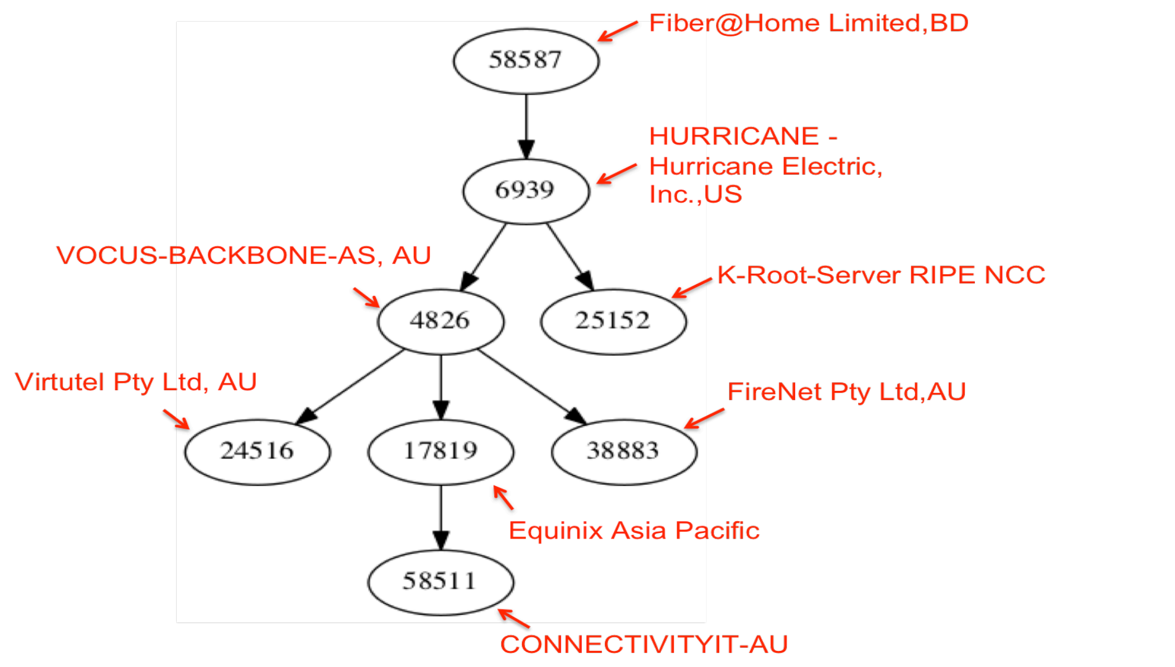
China Telecom, 2010

- On 8 April 2010 China Telecom announced itself as the originator for a large number of the Internet's address blocks.
- The incident was most likely due to an operator error, but during this incident a large proportion of the Internet's traffic was re-directed to China Telecom.
- A number of ISPs propagated the mis-originated routes, so the impact of the attack was likely to have been felt widely (albeit briefly).
- Among the mis-originated routes were address blocks that belonged to the DoD, USG, various private sector firms, and Service Providers.



Bangladesh Fibre@Home, 2015

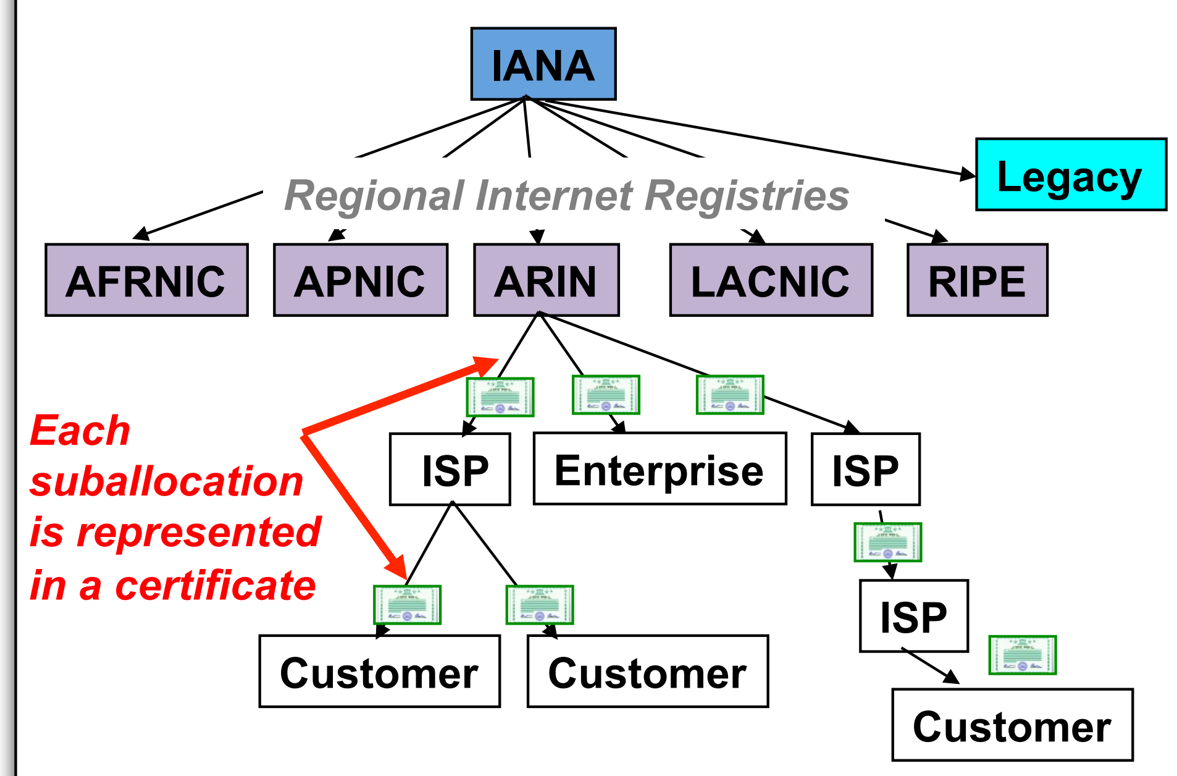
- On 30 June 2015 Bangladesh Fibre@Home announced itself as the originator for a large number of the Internet's address blocks.
- The incident was, again, quite likely due to an operator error, and again resulted in some proportion of the Internet's traffic being re-directed to an unintended destination.
- Fewer ISPs propagated the mis-originated routes but some of these were quite prominent, including Hurricane Electric and the AS used by the K-Root DNS root name server.



THE SOLUTION

STEP 1: Certify the right to use addresses

Parallel existing address allocation system


IANA
Legacy
Regional Internet Registries
AFRNIC
APNIC
ARIN
LACNIC
RIPE
Each suballocation is represented in a certificate
ISP
Enterprise
ISP
ISP
Customer
Customer
Customer

Resource Public Key Infrastructure - RPKI

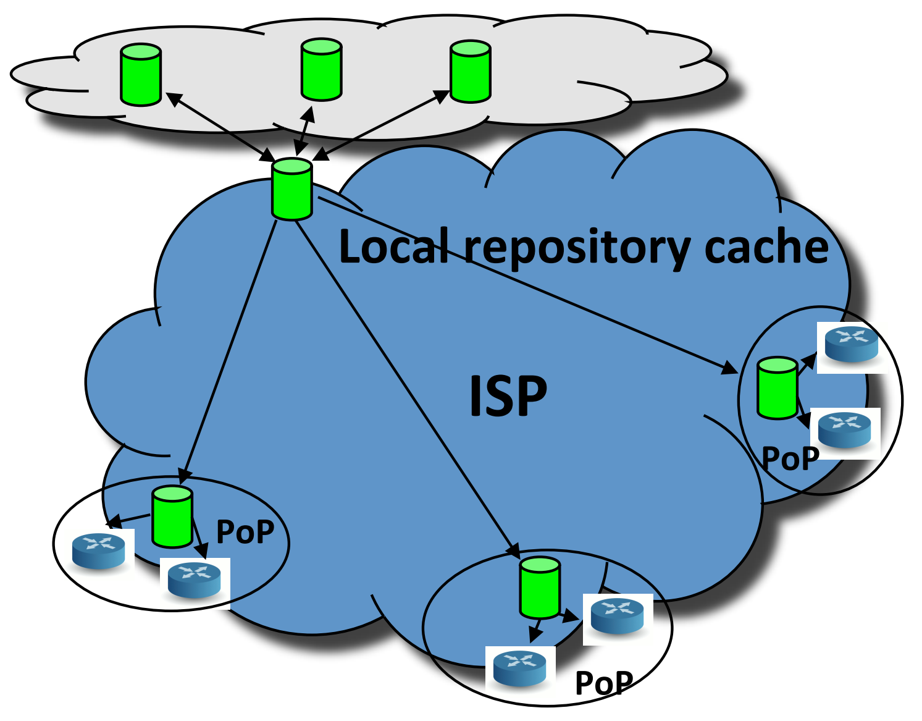
STEP 2: Origin Validation (protect the origin of the route)

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

Globally Distributed CA Repositories

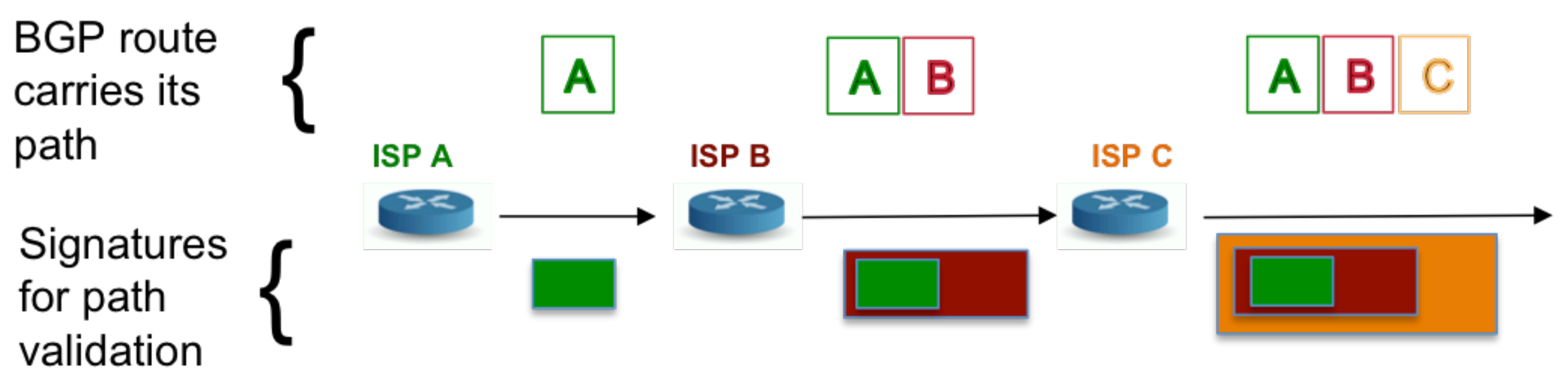
Cache-to-router protocol delivers list of authorized prefix origins to routers in real time.

Routers do NO crypto



Proactive solution: BLOCK bogus origination

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



Sign everything you receive to prove you didn't invent the path

- Originators, ISP A, sign what they originate
- Propagators, ISP B and ISP C, sign what they propagate
- Routes collect signatures as they travel through the network
- Recipients validate signatures to determine path validity

Protections parallel legitimate behavior

Proactive solution: BLOCK bogus routing

Deployment Progressing

Deployment Underway

Specification Complete, Implementation Starting