

# Enhancing and Accelerating Routing Security (EARS)

Parsons Corp.

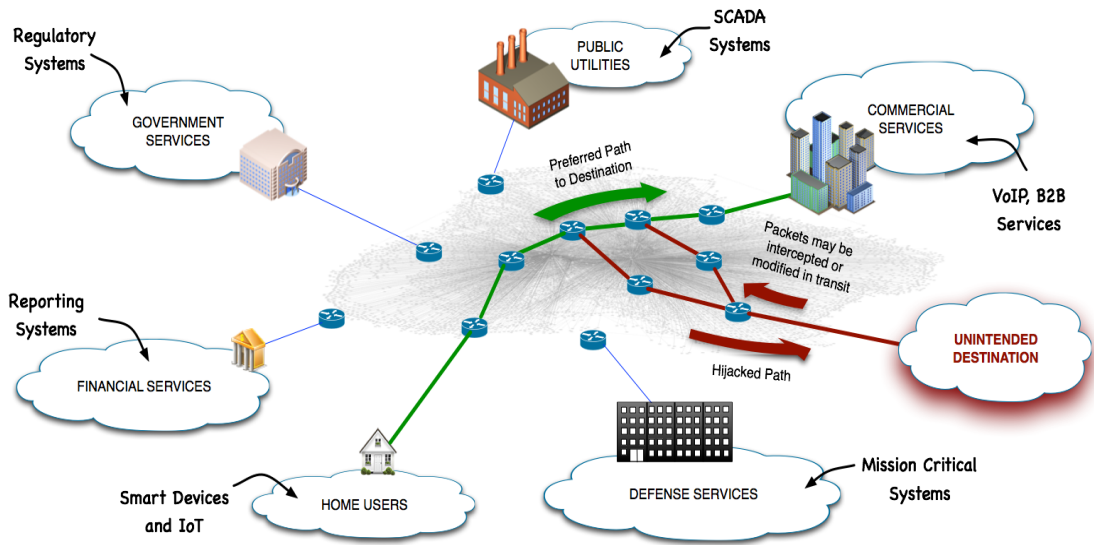
Dragon Research Labs | Raytheon BBN Technologies

<http://securerouting.net>

## For more information contact:

Sandra Murphy  
7110 Samuel Morse Dr  
Columbia MD 21046  
Tel: 443.430.8000  
sandra.murphy@parsons.com

Russ Mundy  
7110 Samuel Morse Dr  
Columbia MD 21046  
Tel: 443.430.8000  
russ.mundy@parsons.com



## Securing the Routing Infrastructure is Critical!

- Routing is an essential part of all Internet communication, impacting all Critical Infrastructure Sectors.
- Routing attacks can affect any application using the Internet.
- Attacks on Internet routing can result in data being captured, black-holed, modified, or re-routed to unintended destinations, without the user's knowledge.
- Attacks on Internet routing can happen at arbitrary points in the network. Since the attacker dictates the eventual route, the attacker is always "on path".
- The Internet architecture and its emerging services (e.g. cloud) vastly increases the potential for routing attacks.

## Existing Measures Are Insufficient

- Existing measures are either reactive, incomplete, inaccurate, or do not scale. Reactive measures also presume that it is possible to distinguish between anomalies and normal network "churn".
- User end-to-end encryption is not a substitute for Routing Security. It does not prevent collection of traffic metadata or storing of data for later decryption attempts. Some routing attacks can help in subverting encryption systems.

## Steps For Securing Routing

### 1 Certify Resources

Identify routing resources (prefixes and ASNs) that are assigned to your organization. Certify your resources through the process outlined by your RIR.

### 2 Enable Origin Validation

Confirm that routers in your enterprise are RPKI capable (recent router software provides this capability). Set up one or more RPKI validator caches and enable your routers to use validated RPKI information in their routing decisions.

### 3 Enable Path Validation

Check with your router vendor on planned support. Enable path validation once routers support this feature.

*This work was sponsored by The Department of Homeland Security, Science and Technology Directorate.*