Routing Security: an RIR Perspective

ARIN / Los Angeles

2005.10.25

Randy Bush <randy@psg.com>

Steve Bellovin <smb@cs.columbia.edu>

<http://rip.psg.com/~randy/051025.arin-routesec.pdf>

What is Routing Security?

- Defending routers against attacks that are similar to attacks on hosts
- But the **unique threat** is attackers using routing protocols
  - To divert traffic
  - To alter traffic
- We have some ability to lessen the danger, but not enough!

History of Routing Security

- Radia Perlman dissertation: *Network Layer Protocols with Byzantine Robustness*, 1988
- Bellovin: *Security Problems in the TCP/IP Protocol Suite*, 1989
- Work accelerates 1996
- Kent et alia two papers in 2000
- Endless jawing in the IVTF

Why so Little Progress

- The problems are technically very difficult
- Simple routing is already a very complex operational issue
- It is not traditional communications security
- Installed base & transition problem
- Unmotivated vendor$

Normal Ops Security

- Go to any Routing Ops Security Tutorial
- TCP/MD5 session protection
- ACLs on everything
- ssh, not telnet. no http, …
- Route filtering (based on IRR),
- …

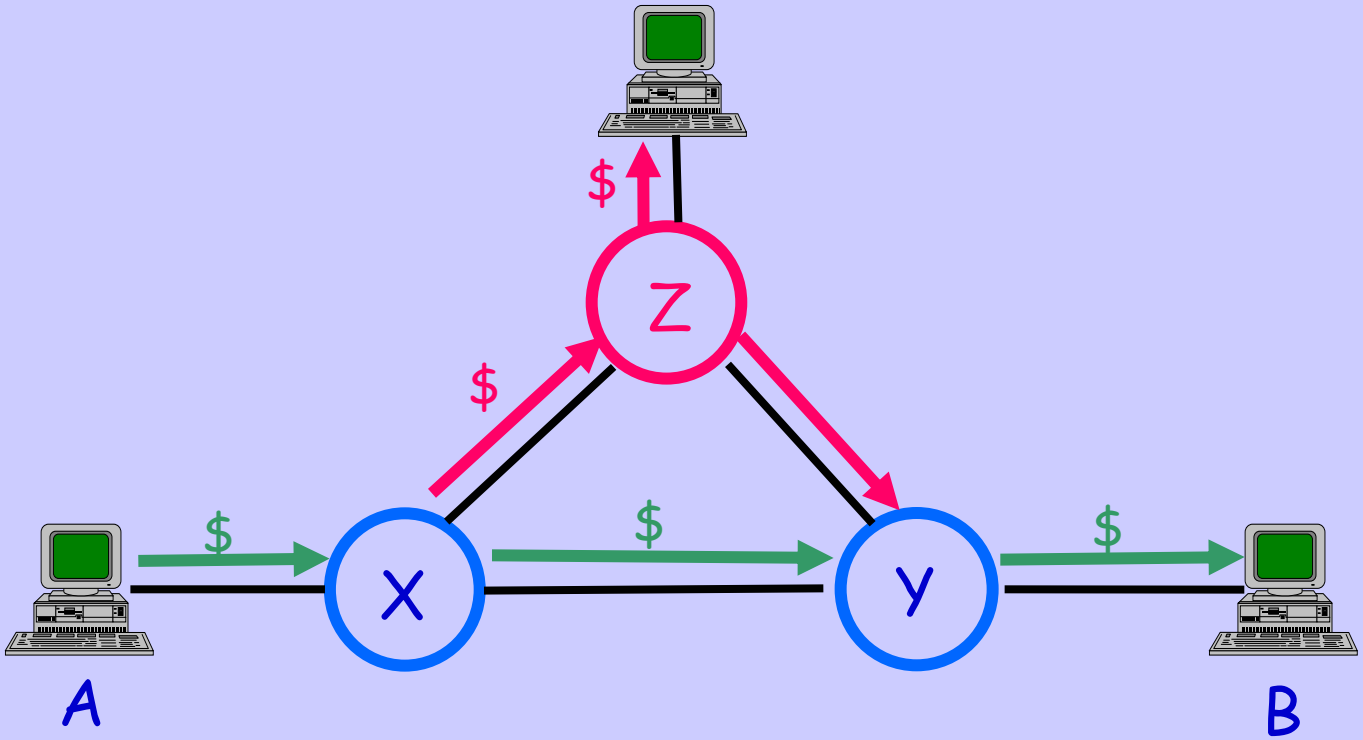
Want to Ensure

- An ISP/site owns the IP address space it is announcing
- If a router announces a path to X it can really deliver to X
- If X tells me it can get to Y, did Y authorize X to carry its packets?

What is Different Here?

- Well-studied communication and host security issues are buggy code and/or bad protocol design
- Routing is vulnerable with good code and good protocols
- **The problem is a dishonest peer**
- Hop-by-hop authentication is not sufficient

Diversion Attack



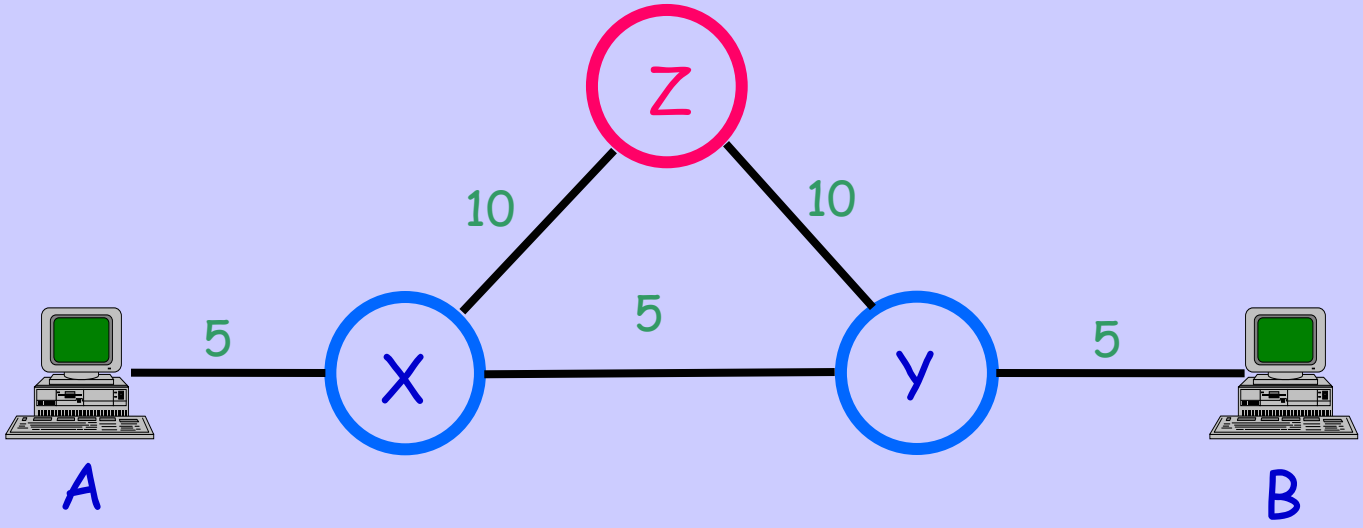
Expected Path - A->X->Y->B

Diverted Path - A->X->Z->Y->B

How does Attacker Do It?

- Routers select lowest cost path toward destination on a hop by hop basis
- Attacker 'owned' router lies about cost
- And we must assume that random routers can be owned

How Does Z Do It?

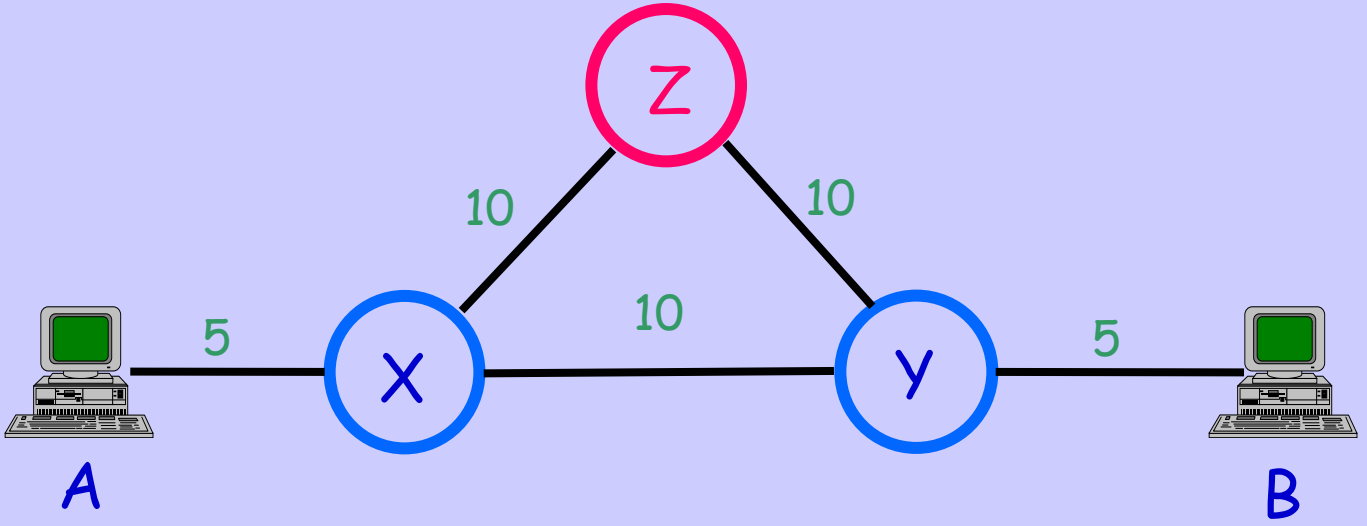


Y tells X and Z that costs are B:5
X tells A and Z that costs are Y:5 B:10
Z tells X that costs are Y:10 B:15

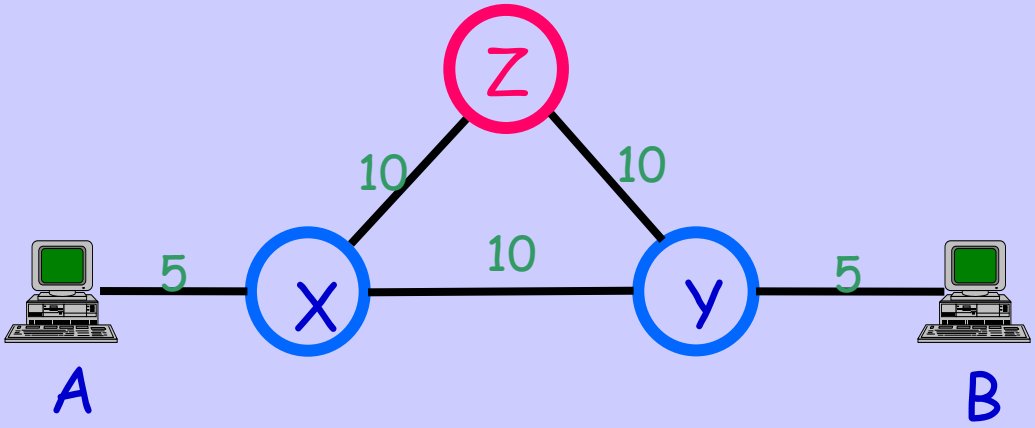
Z tells X that costs are Y:10 **B:5**

X now sends B's traffic to Z!!!

Why is this a Hard Problem?

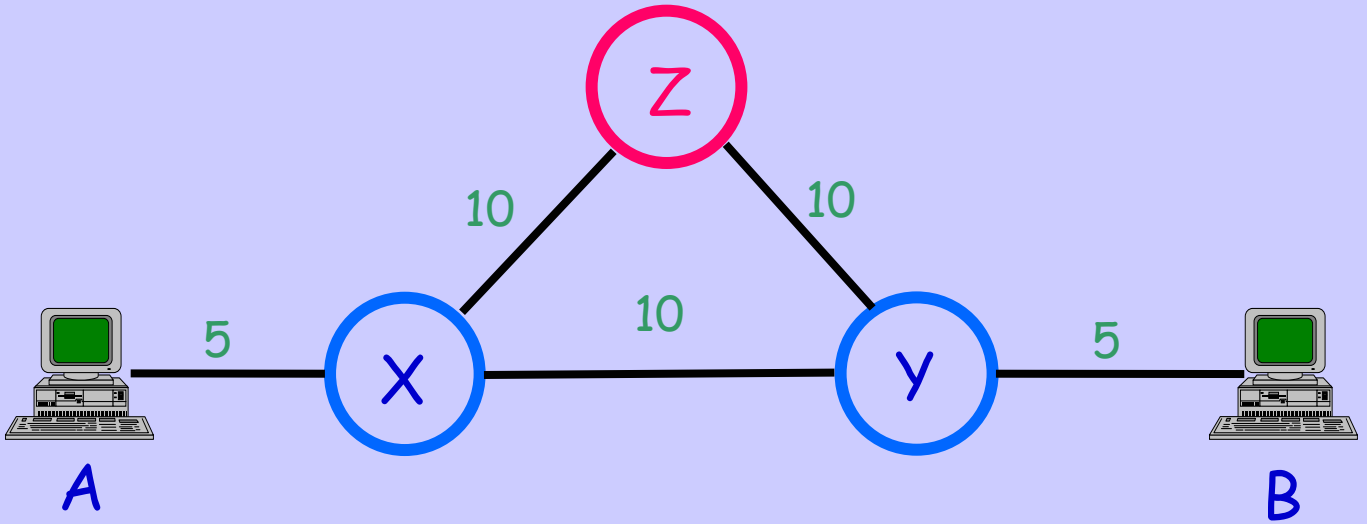


- X does not really know Z's links
- X does not really know Y's links
- They trust each other re costs!



- Validating IP prefix ownership does not help, as Z is not lying about B's owning it
- Using IRR-like peering map does not help, as Z is not lying about who connects to whom

One Approach



- B cryptographically signs the message to Y Sb(Y->B=5)
- Y signs messages to X and Z encapsulating B's message Sy(X->Y=10 Sb(Y->B=5)) and Sy(Z->Y=10 Sb(Y->B=5))
- Z can only sign Sz(X->Z=10 Sy(Z->Y=10 Sb(Y->B=5)))
- Now X can verify paths and costs
- **Forward path signing** solves the 'simple' case

Costs

- Very crypto-CPU-intensive
  - Use caching
  - Use delayed validation
  - Moore's 'Law' is your friend
- Expense is highest when routing is changing, just when we need validation the most ☹

Trust Issues

- How does X know the **identity** of ISP Y, i.e. trusted relationships?
- How does anyone know B owns the address space it is announcing?
- So there are two classes of trust,
  - IP address ownership
  - ISP identity

Address Space Ownership

- Luckily, IP space delegation is a natural hierarchy
- IANA signs address allocations to RIRs using IANA certificate
- RIR signs address allocations to ISPs/LIRs using RIR certificate
- ISP/LIR signs allocations to sites using its ISP/LIR certificate

Who Issues the Certs?

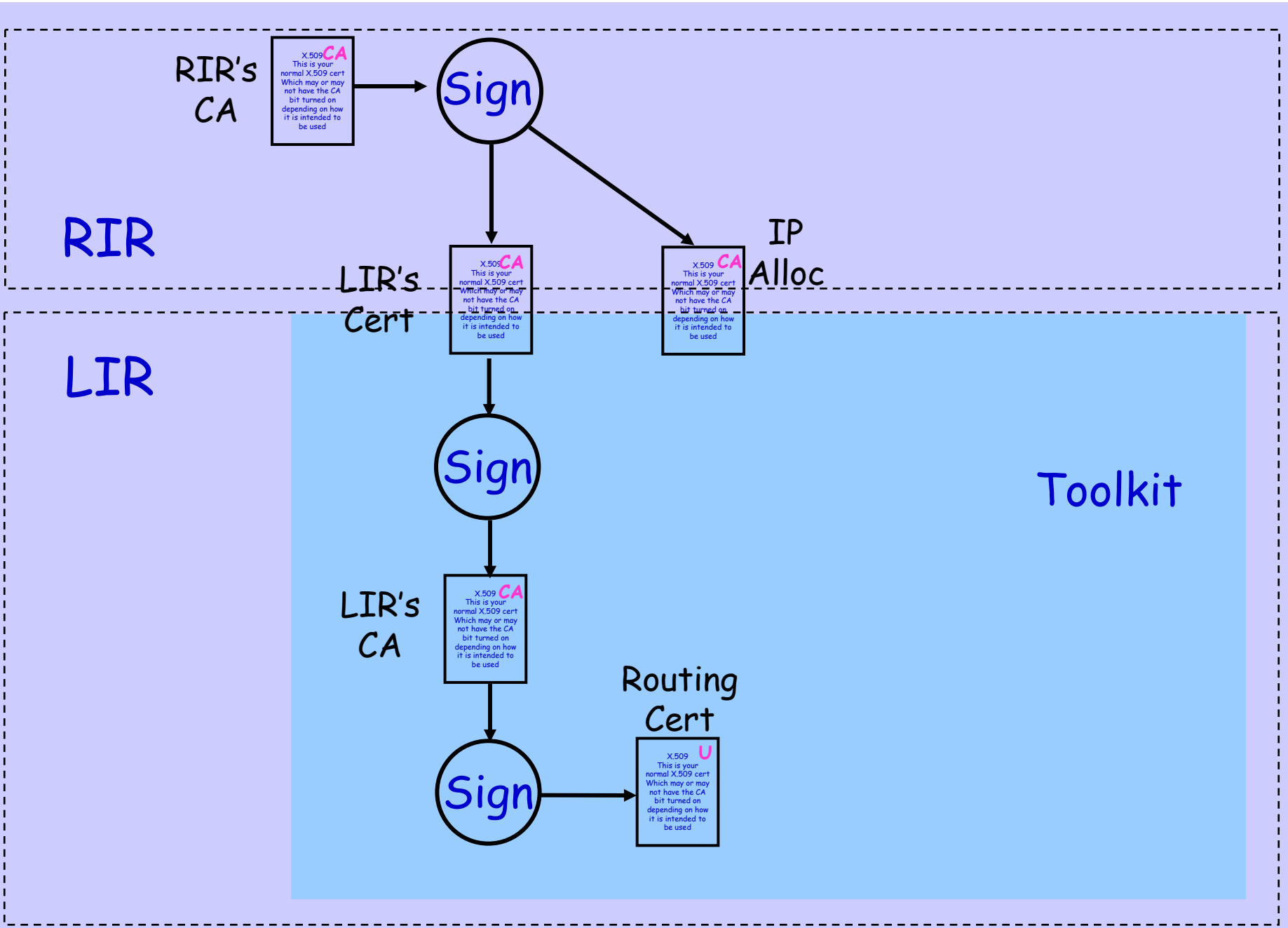
- IANA can certify itself
- Who certifies an RIR, IANA?
- Who certifies an ISP/LIR, an RIR or other ISPs in a web of trust?
- Issuing a certificate can be separated from signing that you attest that IP prefix P belongs to ISP A

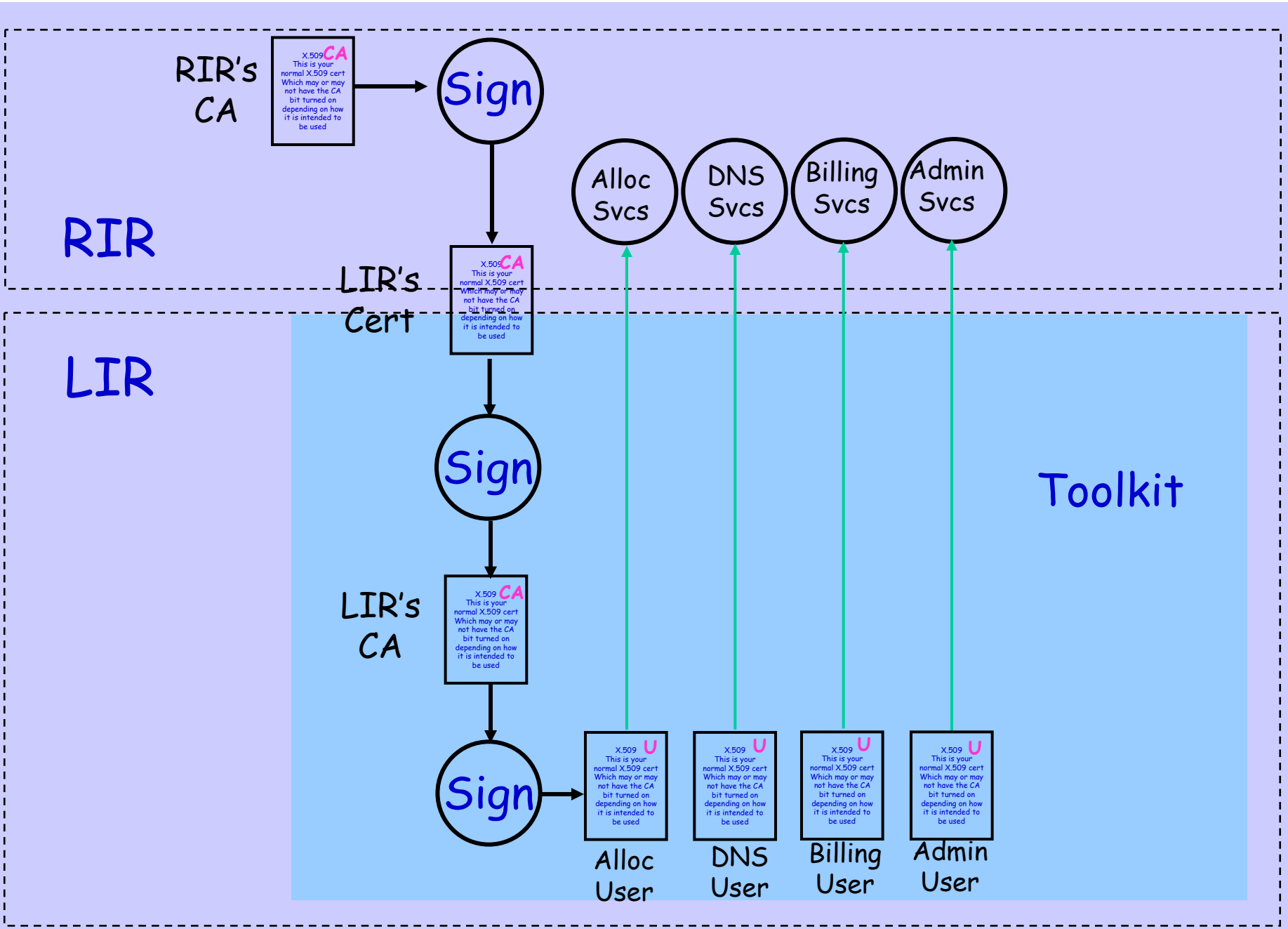
Public Key Infrastructure

- How are certs distributed?
- Administratively: ftp …?
- Out-of-band protocol: new cert distribution protocol?
- In-band protocol: yet another extension to BGP?
- Someone will think of how to do it with DNS!

What Can RIRs Do

- Work on IANA/NRO/RIR X.509 cert CA hierarchy so ISPs don't have to know 42 trusted root keys
- Prepare to sign IP address space delegations to ISPs, end sites, …
- Work with ISP community to gain their business trust to use RIRs as CA for ISP certs
- Use ISP & RIR certs for securing RIR/ISP business processes (DNS, allocation, billing)

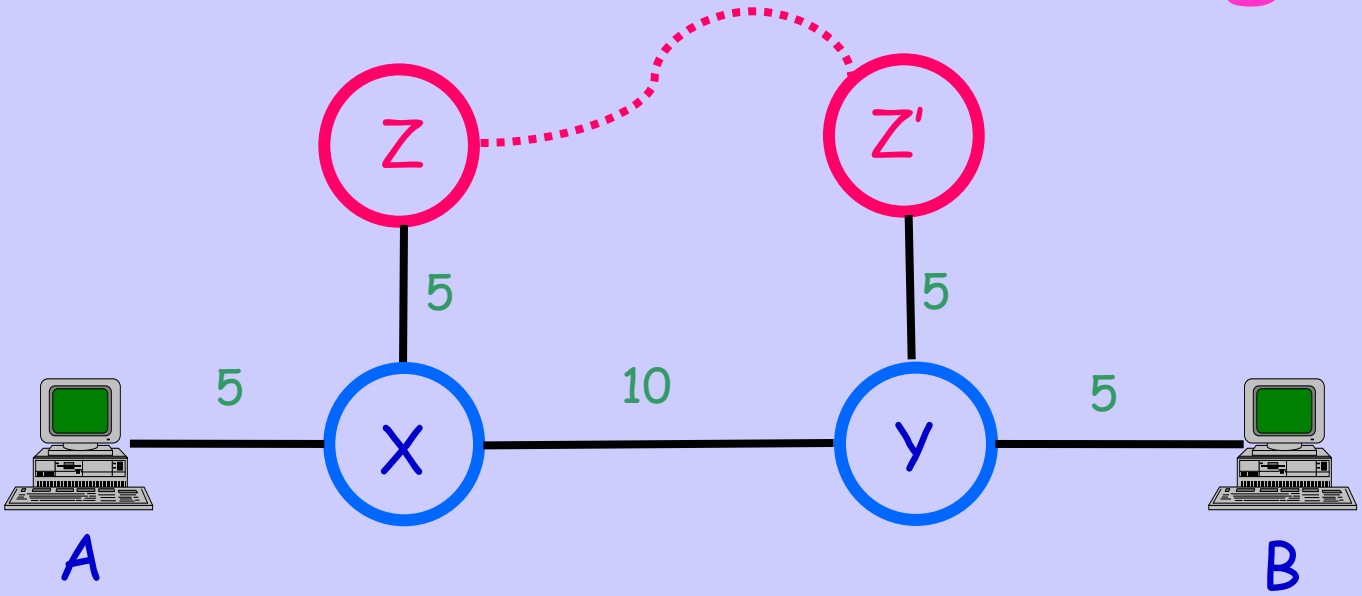




Thanks

- Steve Bellovin, whose ideas and work I liberally stole
- ARIN for time and space
- NSF via award ANI-0221435
- Internet Initiative Japan

Even that is not Enough!



- Y receives Sb(Y->B=5)
- Z' receives Sy(
- Z tells X Sz(Z->Y=5 Sx(Y->B=5))