A PKI For IDR
Public Key Infrastructure and Number Resource Certification

AUSCERT 2006

Geoff Huston
Research Scientist
APNIC

If…

You wanted to be Bad on the Internet

And you wanted to:

- Hijack a site
- Inspect someone's traffic
- Alter someone's traffic
- Disrupt applications
- Cause mayhem

And not be detected

What aspect of the operation of the Internet would you attack?

Routing Security is Critical

- Inter-domain routing represents a significant area of vulnerability for the global Internet.
- Vulnerabilities include:
  - Disruption to routing protocol operation
  - Injection of false routing information
  - Traffic redirection
  - Subversion of application integrity
- Inherent information masking within BGP works against ease of detection of attacks on the routing system

Routing Security is Weak

- The inter-domain routing system is relatively easy to subvert
  - Many injection points for routing data
  - No uniform trust model for routing data
- It can be extremely difficult to detect such subversions from single or multiple observation vantage points
  - Propagation of false data can be controlled to a pre-determined locality

Routing Security is Weak

- Subversion of integrity of routing can create a platform to perform subtle directed attacks against target servers and applications, as well as general service disruption on a large scale
  - Routing attacks can support a range of attack models from targetted extortion of a single service through to general mayhem and widespread service failures

Potential Responses to Routing Vulnerabilities

- Protect the routing infrastructure
  - Secure access to the routers
  - Protect the router’s critical resources (processing, memory and switching)
- Protect the protocol sessions
  - TTL settting
  - MD5
  - IPSEC
- **Protect the payload**
  - Validate the routing protocol payload as authentic information that correctly represents the actual intentions of the parties as well as the actual state of the network’s topology

Address and Routing Security

- The basic routing payload security questions that need to be answered are:
  - Is this a valid address prefix?
  - Who injected this address prefix into the network?
  - Did they have the necessary credentials to inject this address prefix?
  - Is the forwarding path to reach this address prefix an acceptable representation of the network's forwarding state?
  - Can I trust my routing peer / customer / transit ISP to deliver me accurate information?

- Can these questions be answered **reliably**, **quickly** and **cheaply**?

A Resource Validation Framework

- To use a framework to support validation of attestations about addresses and their use

- Queries made within this validation framework should include
  - the **authenticity** of the **address object** being advertised
  - the **authenticity** of the **origin AS** of this advertisement
  - the **explicit authority** from the address holder to the AS holder that permits an **originating routing announcement** from that AS
  - the **authenticity** of the **AS path** information representing reachability to the address object. i.e. is the next hop address a valid forwarding action for this address prefix?

Choices, Choices, Choices

- As usual there is no shortage of potential technologies that could conceivably support such a validation framework
  – Attribute Certificates
  – Certificate Extensions
  – Internet Routing Registries++
  – Signed bindings
  – Signed reports
  – The DNS
  – The Phone
  – Signed Letters of Authority

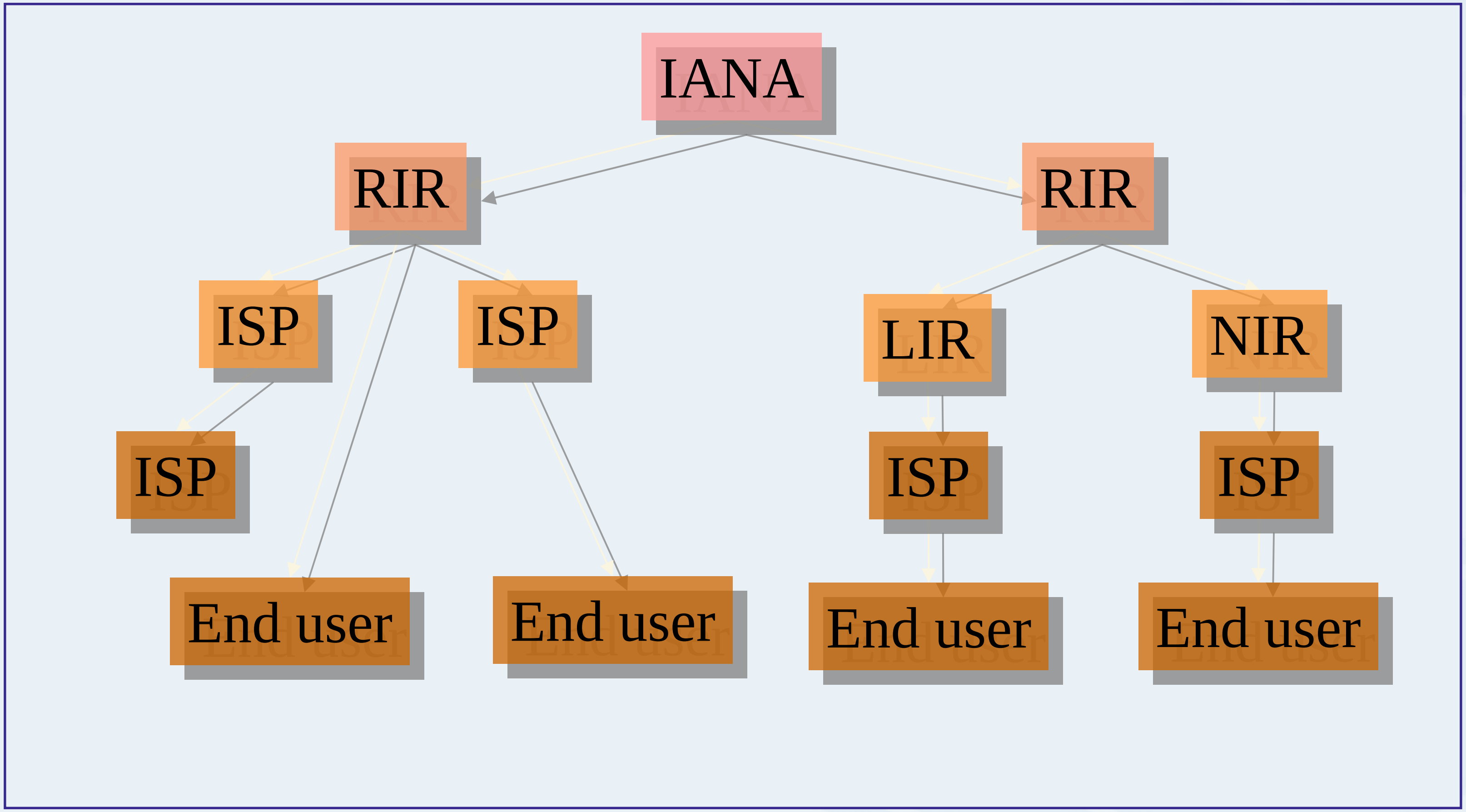
Design Principles for a Validation Framework

- **Don't force any party to claim to be authoritative beyond its actual authority and knowledge**
- Use existing standards
- No new organizations in novel trust roles
- Leverage existing roles and authorities
- Don't preclude existing processes and functions
- Offer an improvement to existing work procedures
- Allow highly reliable and trustable outcomes to be achieved efficiently

Resource Validation

- One of the most effective ways to validate "right of use" assertions is for the validation mechanism to align itself to the distribution mechanism

The Resource Distribution Function



PKI Rooted Hierarchy

- Explicitly avoid various forms of web of trust models, and use deterministic uniform validation methods based on a combination of issuer subject chains and resource extensions
- Exploit and mirror address allocation hierarchy
  - Each CA in the hierarchy can only validly make attestations and generate certificates about resources that have been delegated to them from the parent CA in the hierarchy
  - Exploit existing authoritative data regarding resource distribution

Modelling the Environment

- Use an **X.509 + PKIX certificate hierarchy** aligned to address distribution points
- The certificate “topic” is the resources allocated from the issuer to the subject at this distribution point
- Certificates allow for the generation of subordinate certificates at delegation distribution points
- Validation of a certificate entails a backwards walk towards the root of the distribution hierarchy
- Revocation can model the transfer of a resource prior to the termination of the current certificate’s validity period

RFC 3779: X.509 Extensions for IP Addresses

- RFC3779 defines extension to the X.509 certificate format for IP addresses & AS number
- The extension binds a list of IP address blocks and AS numbers to the subject of a certificate
- The extension specifies that the certification authority hierarchy should follow the IP address and AS delegation hierarchy
  - Follows IANA $\Rightarrow$ RIR $\Rightarrow$ LIR
    - And all their downstream delegations
- These extensions may be used to convey the issuer's authorization of the subject for exclusive use of the IP addresses and autonomous system identifiers contained in the certificate extension
- This is a **critical extension**

A Resource Certificate

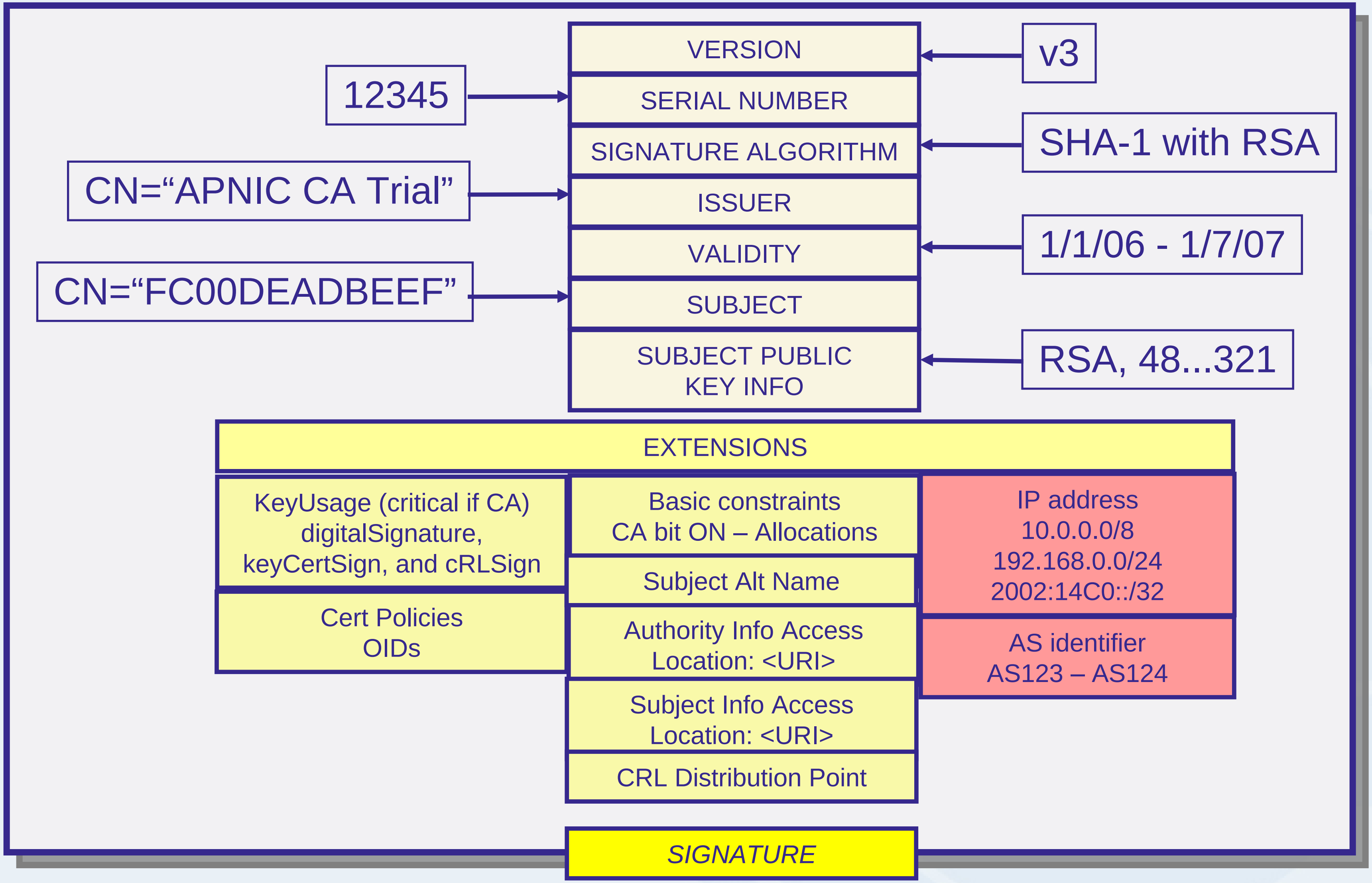
- A mechanism to provide confirmation of an association between an entity and a collection of number resources

  "this entity is the current unique holder of the following resources"

- This is **not** an identity attestation, nor is it a role permission

- This **is** similar to a traditional title certificate, where the title refers to a resource collection

Resource Certificate Format



What is being Certified

- APNIC, the “Issuer”, certifies that:

  the certificate’s “Subject”

  whose public key is contained in the certificate

  is the unique current controller of the set of IP address and AS resources

  that are listed in the certificate extension

- The certificate does NOT certify the identity of the subject, nor the quality of their intentions

Tools and Roles

- A PKI does not “do” anything at all
- It can be used as a reference source to validate various claims relating to resource control, authorities and roles.

Tools for Relying Parties

- Network Administration roles
  - "Please route my address prefix"
  - Sign and validate
- Network Security roles
  - "Why are we carrying this route?"
  - Validate and audit
- Secure inter-domain routing - the protocol
  - Why isn't this just part of BGP?
  - Online "live" validate
    - High volume, potentially very tight time constraints

Repository Model

- Distributed Certificate generators
- Local repository synchronization
  - Repository object name scheme is a critical component of repository design
  - Use a hierarchy of repository zones
  - Adopt a zone structure of “signed by public key” (as distinct from “issued by issuer”)
  - Use a repository synchronization tool with the rsync primitive as a means of identifying changed objects

What could you do with Resource Certificates?

- You could sign **routing authorities**, **routing requests**, or **Route Registry submitted objects** with your private key
  - The recipient (relying party) can validate this signature against the matching certificate's public key, and can validate the certificate in the PKI
- You could use the private key to sign routing information that could then be propagated by an **inter-domain routing protocol** that had validation extensions
- You could issue signed **subordinate resource certificates** for any sub-allocations of resources, such as may be seen in a Local Internet Registry context

APNIC Resource Certificate Trial

Trial service provides:

- Issue of RFC3779 compliant certificates to APNIC members
- Policy and technical infrastructure necessary to deploy and use the certificates in testing contexts by the routing community and general public
  - CPS (Certification practice statement)
  - Certificate repository
  - CRL (Certificate revocation list)
- Tools and examples (open source) for
  - downstream certification by NIR, LIR and ISP
  - display of certificate contents
  - encoding certificates

Expected Environment of Use

Service interface via APNIC web portal

- Generate and Sign routing requests
- Validate signed objects against repository
- Manage subordinate certificates

Local Tools – LIR Use

- Synchronize local repository
- Validate signed resource objects
- Generate and lodge certificate objects

Current Status

- Test Certificates being generated
  - Locally generated key pair
  - Cover all current APNIC membership holdings
  - CRL test
    - Reissue all certificates with explicit revocation on original certificate set
- Example tools being developed
- APNIC Trial Certificate Repository:

  rsync://rsync.apnic.net/repository

What have we learned so far?

- Maybe just overloading the DNS would've been easier!

What have we learned so far?

- Using a PKI is not a lightweight decision
- There's an entirely new terminology universe in the X.509 certificate space!
  - rites of initiation into the security world appear to be necessary
- X.509 certificate specifications appear to include a vast repertoire of extensions with elastic semantics
  - choose carefully!
- There is not a lot of diverse PKI deployment experience out there
  - each exercise is a learning experience
- Distributed authority models are very challenging to design in a robust manner
  - Think carefully about the model of synchronization across a realm of multiple issuers and multiple repositories

What have we learned so far?

- Understand the business that you are in
  - make the certificate work to the business model rather than the reverse
- This is not an exercise that is done lightly
  - considerable investment in expertise, tools, documentation, and navel-gazing over process is useful
- It's a large and diverse industry
  - Technology deployment models need to support diverse environments and extended adoption timeframes
  - Partial adoption should still be useful

What have we learned so far?

- Outcomes need to represent superior choices for players
  - Risk mitigation is an ephemeral and diverse motive for widespread adoption
  - Better, faster, and cheaper solutions tend to produce better adoption motivations
- Good Security in a diverse environment is very elusive

Thank You

Asia Pacific Network Information Centre

APNIC