Key Management in DNSSEC

Gilles Guette, gguette@irisa.fr
Advisor: Gerardo Rubino

- DNSSEC uses public key cryptography and digital signatures to protect DNS data
- Each DNS zone manages its own zone keys stored in a DNSKEY Resource Record (RR)
- Zone keys are periodically renewed for security reasons

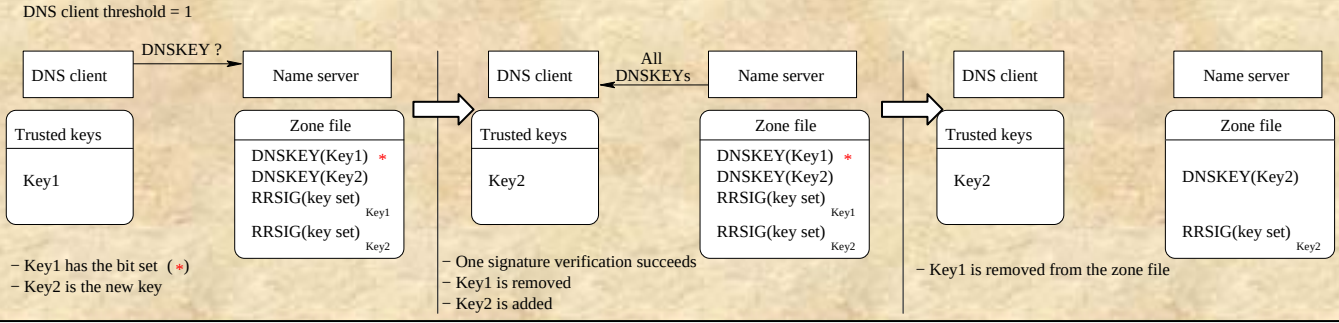
- A DNS client uses these zone keys to verify the digital signatures
- A DNS client needs to trust a zone key to perform secure name resolution
- Trusted keys are zone keys statically configured in DNS client

Problems

- **A resolver must update its trusted keys**
- **Name servers do not know all resolvers**

Proposed solution

- We use a bit in the DNSKEY RR Flags field to specify that a key will be changed
- Thus, name servers notify DNS client about key changes
- DNS client sets a threshold: minimum number of signature verifications to accept a new trusted key
- Immediate update of the client trusted keys set
- Update resists to (threshold-1) key compromissions



- Secure and unsecure zones define islands of security
- A DNS client cannot perform secure name resolution by walking through unsecure zones

Problems

- **A DNS client needs a trusted key for the root of each island of security**
- **Goal of Generalized Delegation Signer (GDS) RR: reducing the number of needed trusted keys**

Proposed solution

- The root and irisa.fr zones are islands of security
  - We have designed GDS Resource Record that authenticates Key2 and is signed by Key1
- Key1 protects GDS(Key2)
- GDS RR links two islands of security
- A DNS client authenticates the self-signed Key2 with GDS(Key2)
  - Only one trusted key is needed, the root zone key: Key1
  - One key is easy to manage on DNS client