NIST
National Institute of
Standards and Technology

INFORMATION
TECHNOLOGY
LABORATORY

Cyber and Network Security Program

DNSSEC Basics and Key Management Issues

Internet Infrastructure Protection

- Importance of Internet / Internet Technologies
  - Vital to commerce, defense, quality of life.
- Threats to Internet Infrastructure increasing
  - Innovation in the threat space far out paces innovation in the protection space.
  - "Good guys" constantly in a reactionary / catch up mode that can't scale.
    - Innovation driven by the "bad guys" … global infrastructures do not respond well to day-zero attacks.
  - Many Internet critical infrastructure systems lack viable basic security mechanisms
    - Routing, Naming, Email, telephony, etc.
- Security and Stability of the Internet
  - Can not be maintained by status quo in the infrastructure.
  - Lack of innovation in this space is a threat in and of itself.

Domain Name System

- Importance of the DNS
  - We all understand the 1st order importance of the DNS.
    - 1st step in every instance of Internet communication.
    - Attacks can hijack/DoS services, machines, zones.
  - Not everyone understands the 2nd order implications of the implicit trust model that is based upon this insecure basic service.
    - Exploiting the DNS is a tool in undermining what we think of as “trusted” services.
      - CA validations, SSL connections, on-line authentication factors.
    - Sophistication of attacks increasing as are their risks.

Kaminsky Attack.

- What was known / unknown
  - Technically nothing new
    - vulnerability identified in ‘95 at least.
  - What opened eyes …
    - …was the scope of vulnerability – millions of recursive resolvers.
    - … was the ease of executing the attack.
    - … was the novel ways in which cache poisoning could be used as a tool to undermine other critical network services and trust models.
  - What people are learning …
    - Is that there is not simple quick fix.
    - “The patch” – while important – only moved the vulnerability from trivial to exploit to easy to exploit
    - The real vulnerability is the inherent lack of security in the DNS.
    - The Kaminsky attacks will continue – software available, patched systems proven still vulnerable.
    - The Kaminsky attack is just the latest instance to exploit a systemic problem. There will be more.

DNS Security

- DNS Security Extensions
  - Widely recognized as the correct long term fix to the systemic problem that underlies the Kaminsky attack.
  - Base standards are mature, implementations are available, operational experience available.
  - Global DNSSEC deployment activities / interests are accelerating
    - .se, .br, .uk, .org, .arpa, .gov – have deployments or plans underway.
- Lack of a signed root
  - Clear technical and business case barrier to wider deployment.
  - Community desire for a signed root will continue to increase.
  - DoC increasingly viewed as an impediment to progress on this issue.
  - Need a clear DoC decision about plans for DNSSEC deployment.

NIST and DNSSEC

A brief summary of some of our efforts/activities follows:

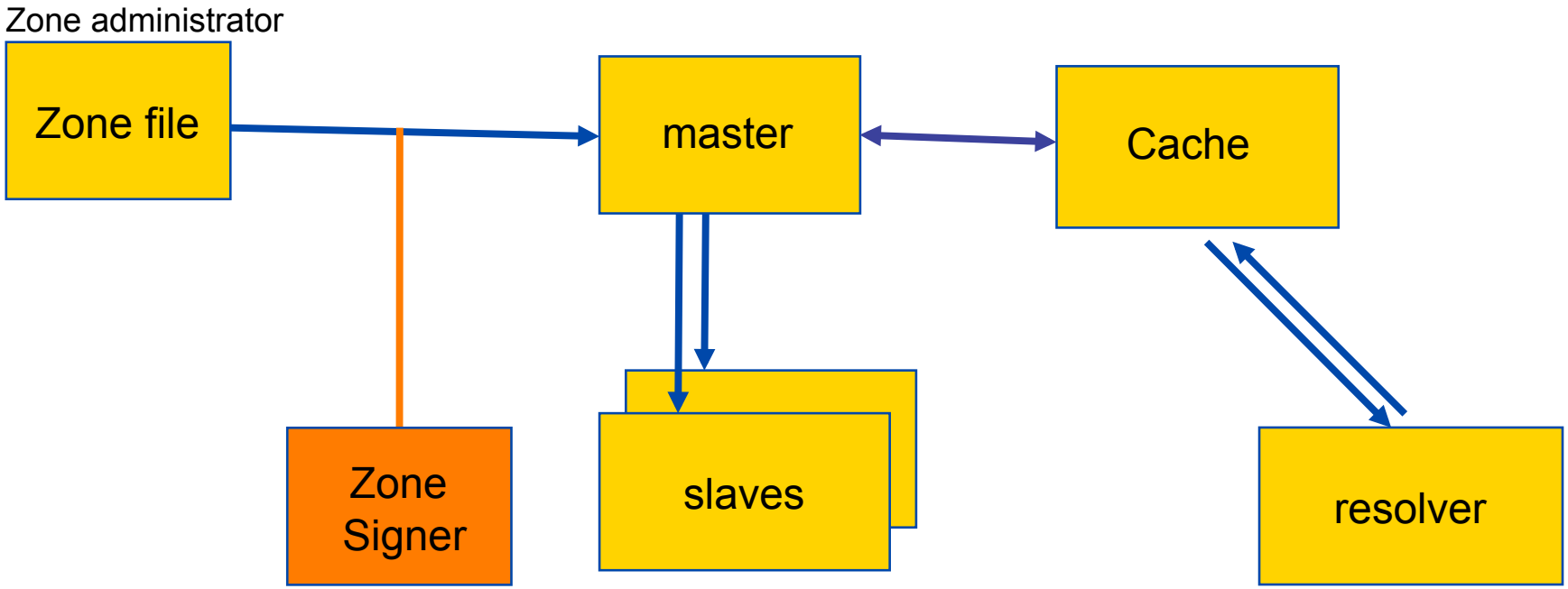
- **NIST staff edited the base DNSSEC standard specifications in the IETF:**
  - RFC4033 - "DNS Security Introduction and Requirements" March 2005.
  - RFC4034 - "Resource Records for the DNS Security Extensions", March 2005.
  - RFC4035 - "Protocol Modifications for the DNS Security Extensions", March 2005.
  - NIST staff continue to lead development of other DNSSEC related specifications in the IETF.
- **NIST staff have developed a Secure DNS Deployment Guide NIST SP800-81 that is widely cited in the industry/DoD.**
  - http://csrc.nist.gov/publications/nistpubs/800-81/SP800-81.pdf
- **NIST is implementing a staged USG DNSSEC deployment strategy**
  - through the development and promulgation of appropriate FISMA technical security controls. Initial DNSSEC security controls were published in the 2006 version (NIST Special Publication 800-53r1, Recommended Security Controls for Federal Information Systems) of these controls and are also referenced in NIST Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems. Additional controls will be added in the next version of Special Publication 800-53, due to be published in the fall of 2008.

NIST and DNSSEC

A brief summary of some of our efforts/activities follows:

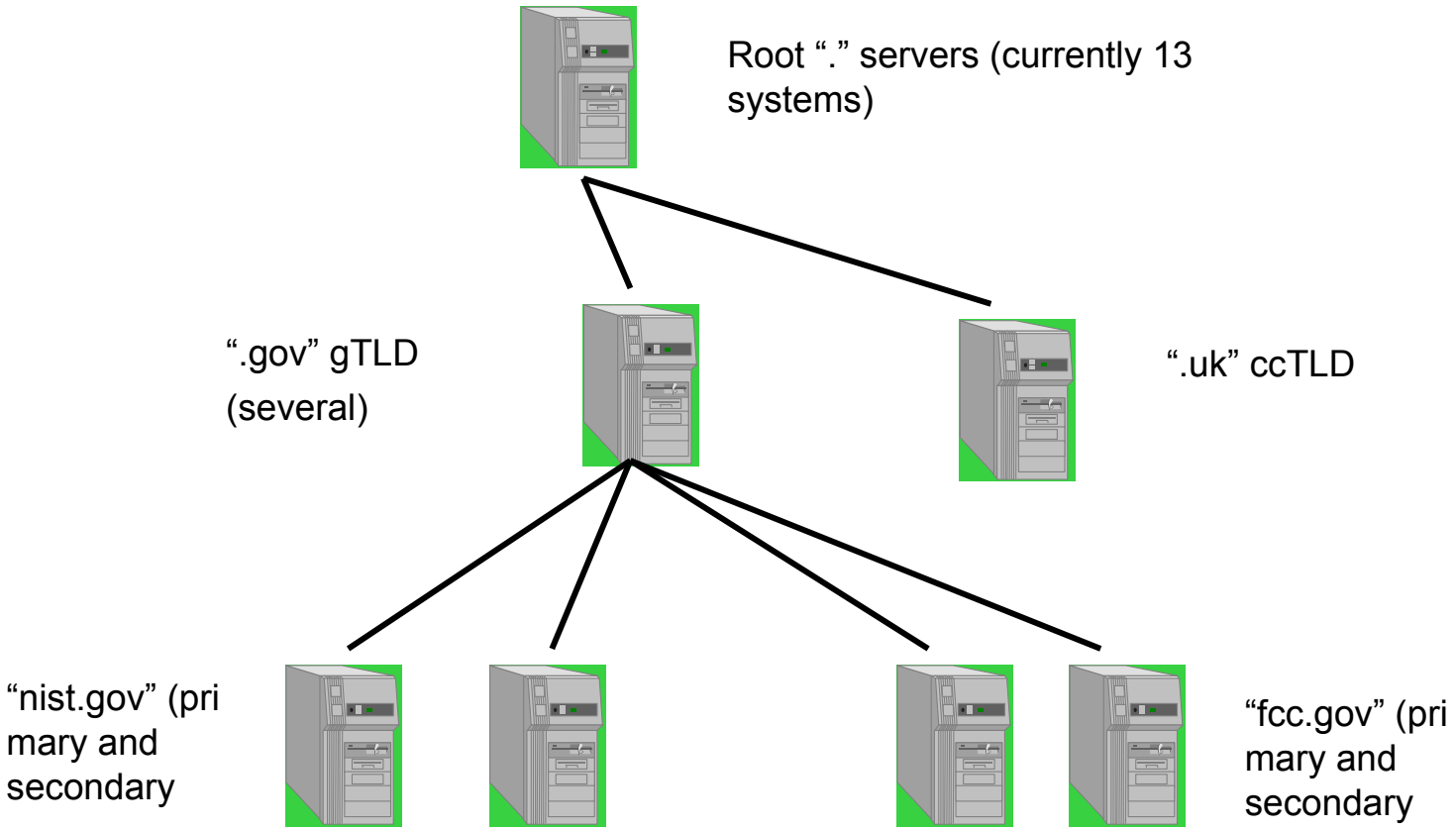
- **NIST contributing to technical analysis of global deployment issues.**
  - Technical plans for signing the root.
  - Technical plans for Trust Anchor Repositories.
  - Technical plans for .gov deployment.
  - Performance and stability of large scale deployment.
  - Leading standardization of DNSSEC future proofing: algorithm rollover mechanisms, etc.
- **NIST leading SNIP – Secure Naming Infrastructure Pilot**
  - Distributed testbed for operational experiments / training in DNSSEC operations.
  - Conducting hands on training for DNS operators / managers.

DNS: Data Flow

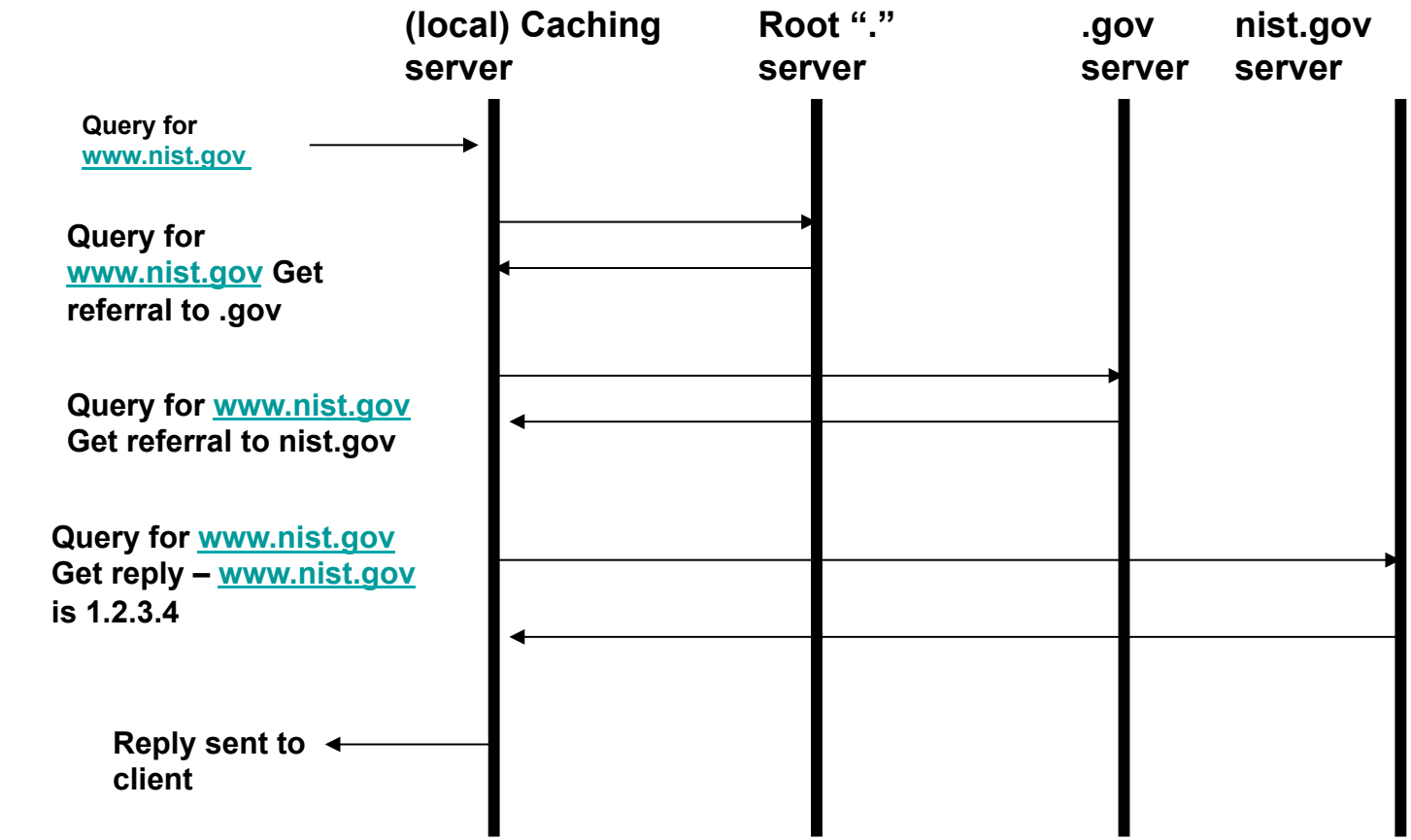


All DNS data is transmitted as plaintext

Topological view of DNS



Example of DNS Query



What DNSSEC Was Designed For:

- Source Authentication
  - Owner of zone database entered in DNS data
  - Signature indicates who generated the data
- Integrity
  - DNS data was not tampered with by other parties.
- Authenticated Denial of Existence
  - Name does not exist in the DNS – and the owner of that zone can prove it.
- All aimed to protect the end user system

DNSSEC Was Not Designed For:

- Confidentiality
  - DNS data is not encrypted
- DoS prevention at the server
- User/Service authentication
  - Just DNS data
- A poor man's PKI

DNS + DNSSEC

DNS

Query:
www.nist.gov

Response:
www.nist.gov A
129.6.13.23

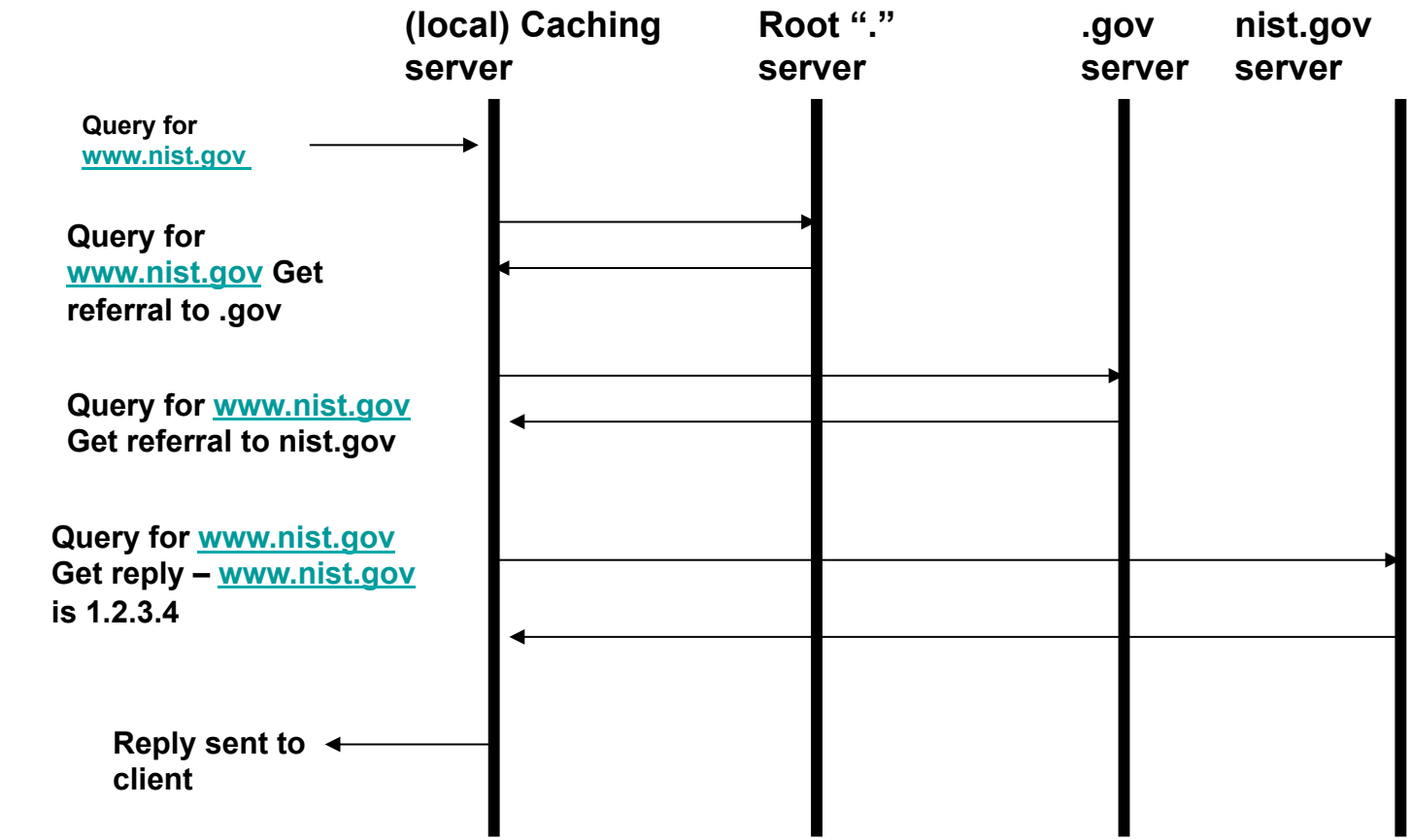
DNSSEC

Query:
www.nist.gov
+*DNSSEC*

Response:
www.nist.gov A
129.6.13.23

Signature
www.nist.gov
<encoded sig>

Example of DNS Query



Now with DNSSEC…

- Host A queries for www.nist.gov
  - Server does not have info in cache, queries Root (pre-configured with root key).
  - Gets referral to ".gov" (containing NS, A and DS records for .gov's key)
  - Client queries .gov. Gets referral to "nist.gov" (containing NS, A and DS records for "nist.gov"s key)
  - Client queries nist.gov and gets reply: Address for www.nist.gov and RRSIG record covering that Address record
    - nist.gov zone key included in reply.
  - Client must construct Chain of Trust:

From nist.gov			From .gov			From root	
www A	RRSIG	nist.gov DNSKEY	nist.gov DS	RRSIG	.gov DNSKEY	.gov DS	RRSIG

DNSSEC and Key Roles

- 2 types of keys (does not matter to the protocol – just administration and policy)
  - Zone Signing Key (ZSK) – key that signs DNS data
  - Key Signing Key (KSK) – key that signs the DNSKEY data ONLY
- The owners of these two keys can be unique
- KSK can be thought of as the "Master Key" that authenticates the data signing key (ZSK)

In the Zone					**Parent Zone**		
Data	Sig (Data)	ZSK	Sig (ZSK)	KSK	DS (KSK)	Sig (DS)	ZSK

Features of DNSSEC

- Zones are signed, not servers
  - Keys are associated with zones
- Backward Compatible
  - Client must signal it wants signatures in response
  - Also allows for other DNS extensions to co-exist
- Crypto agnostic
  - Cryptographic algorithms can be swapped out
- Based on open standards
  - Several independent implementations
  - DNSSEC totally contained within DNS protocol

Trust Anchor Repositories

Types of TARs

- Community of Interest
  - Closed membership
  - Grouped around an industry, country, TLD, etc.
    - Example: .aero or US banks
- Global
  - Open to everyone
  - Who runs the global TAR?
  - How to establish trust in a TAR?
    - Back to the same problem for DNSSEC without a signed root

The Positives of TARs

- Some domains may not be able to be in signed tree, must rely on getting their keys out another way
- Step to have as much of the DNS covered until root zone is signed
- Ability to have private communities
  - Example: USG consisting of .gov, .mil, .us, etc.
- Root zone key distribution
  - A TAR of one key, the root key

The Negatives of TARs

- Only push the problem up one level
  - How does one establish trust in a newly discovered TAR?
- How many TARs are too many?
  - Clients must individually manage each TAR they are interested in – potentially hundreds to thousands.
- Note: There is only one root zone
  - One root key for all of the DNS

Resources

- General DNSSEC
  - http://www.dnssec.net/
- NIST DNSSEC project
  - http://www-x.antd.nist.gov/dnssec/
  - http://www.dnsops.gov/