Domain Name System Security

T-110.4100 Tietokoneverkot

October 2009

Bengt Sahlin

<Bengt.Sahlin@tml.hut.fi>

Objectives

- Provide DNS basics, essential for understanding DNS security
- Understand threats against DNS
- Provide examples of vulnerabilities and attacks
- Understand mechanisms in DNSSEC
- Understand effects of using DNSSEC
- Understand what can be done to improve security of DNS

Humans and Addresses

- Numeric addresses are used in the Internet
  - example: 10.0.0.1 (IPv4), fe80::a0a1:46ff:fe06:61ee (IPv6)
- Humans are better at remembering names than numbers
- In the Internet, names have been used from the start on

History

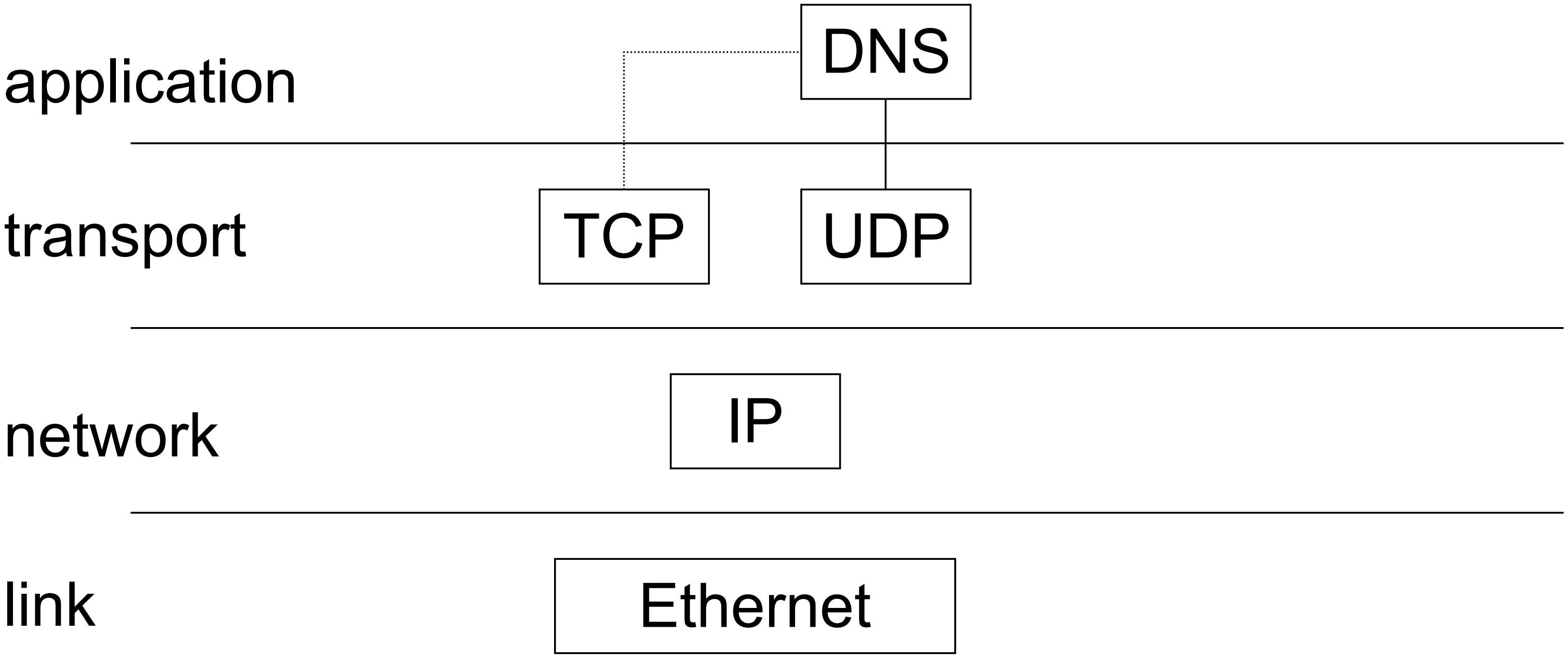
- In the beginning … there was the file **hosts**
  - mapping between "hostname" and address
- Internet grew, one file was not a scalable solution
- A more scalable and automated procedure was needed

The Solution...

- DNS (Domain Name System)
- Main tasks
  - mapping between names and IP addresses, and vice versa
  - controlling e-mail delivery
- But today DNS is used to store a lot of other data also
  - for example DNS SRV record
    - specifying the location of services

Basic Internet Infrastructure

- DNS is a fundamental component of the Internet infrastructure



Basic Characteristics (1/2)

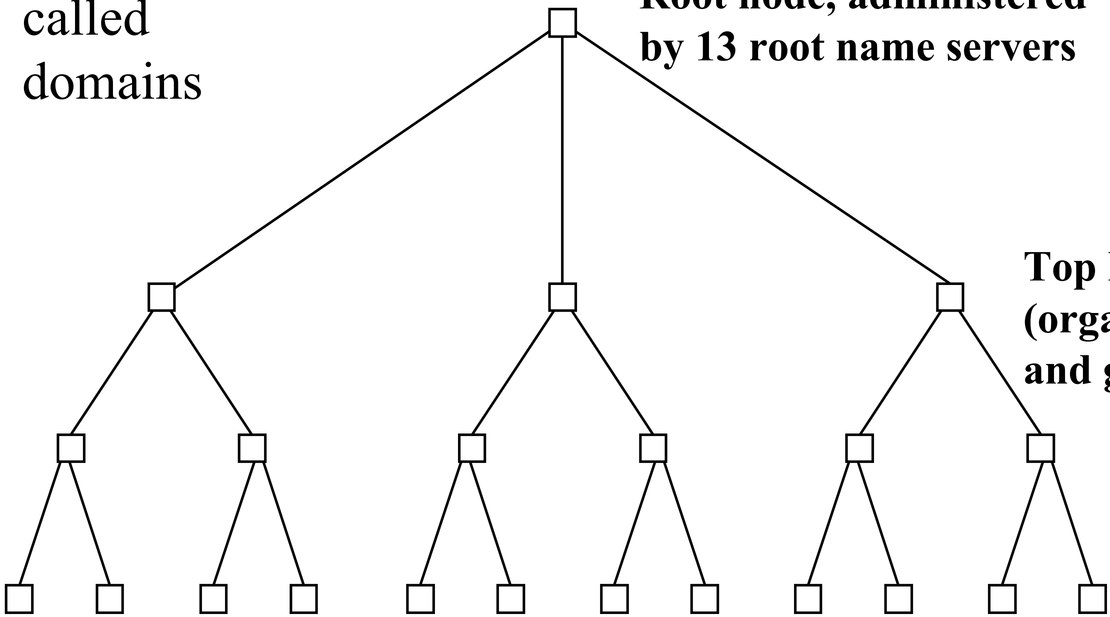
- DNS is a database
- The three basic characteristics of the database:
  - 1) global
    - All the names need to be unique
  - 2) distributed
    - no node has complete information
    - an organisation can administer its own DNS information

Basic Characteristics (2/2)

- 3) Hierarchical
  – the data is arranged in a tree structure with a single root node
  – the structure is similar to the Unix file system structure

DNS Structure

The nodes are called domains



Root node, administered by 13 root name servers

Top level domains (organisational like com, edu, and geographical like fi, se, uk)

Lower level domains (hut.fi)

Leaves (www.hut.fi -> 130.233.220.31)

DNS Concepts (1/3)

- The servers are called name servers
  - name server “roles”
    - master (primary)
      - the name server where the data is administered
      - is the ultimate authority for the data (authoritative)
    - slave (secondary)
      - is authoritative for a zone
      - gets the data from the master through a zone transfer
    - cache
      - a name server can store data DNS data (that it is not authoritative for) for a while

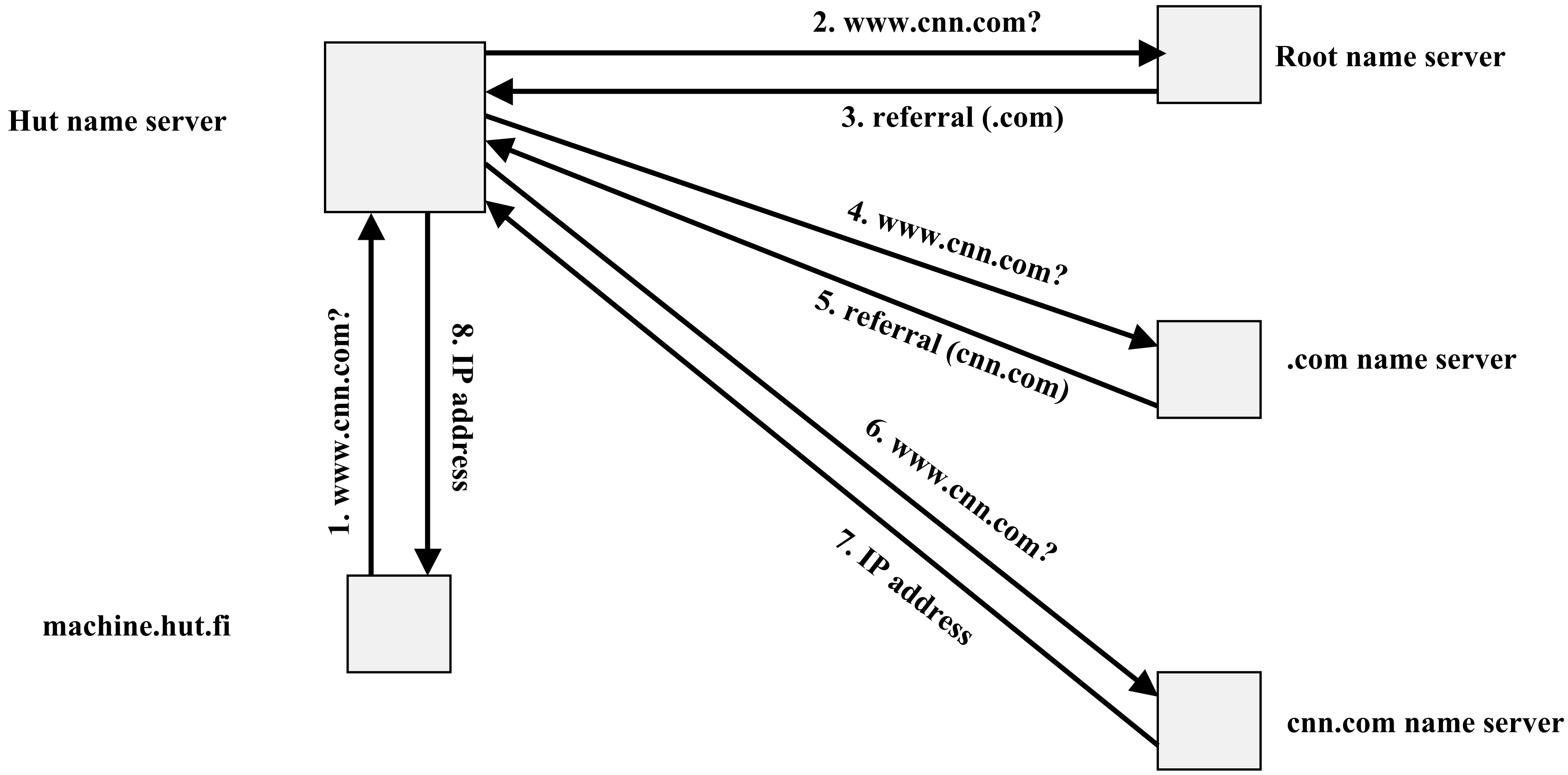
DNS Concepts (2/3)

- The client is called a resolver
  - can do name queries
  - Typically implemented with library functions that applications use
  - nslookup (looking at DNS data), dig (for serious debugging)
- Name resolution
  - the process of acquiring some data, possible by performing several name queries
- The name servers need to know (“are booted up with”) the names and addresses of the root name servers (file root.cache)

DNS Concepts (3/3)

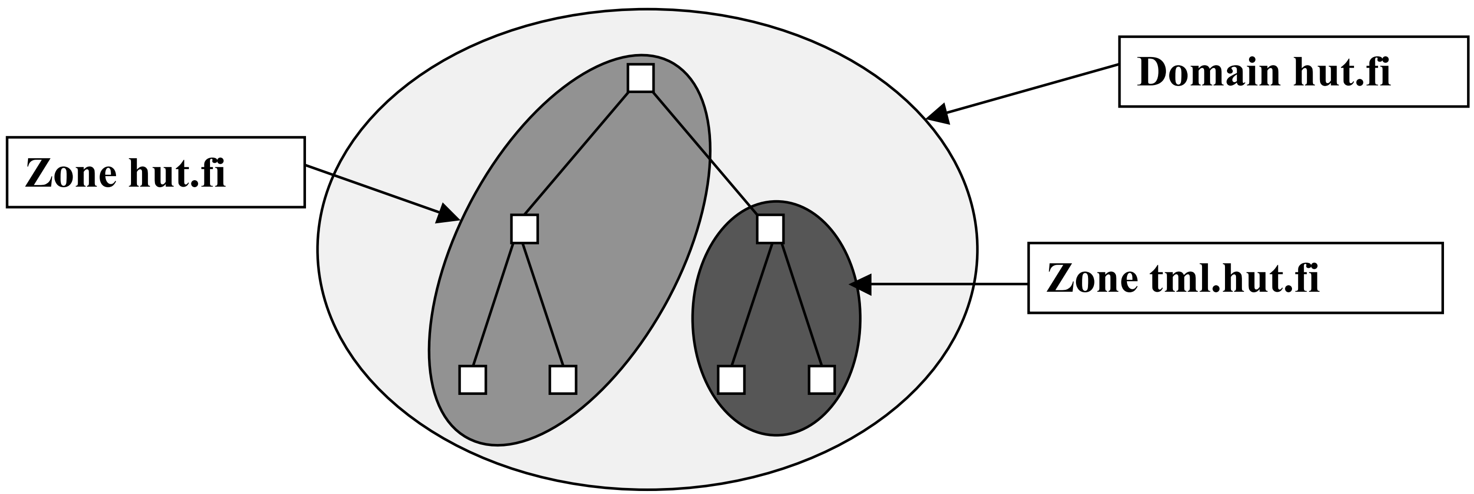
- Delegation
  - the authority for some sub-domain is given to another name server

Name resolution example



Zone vs. Domain

- Zone: a contiguous part of the DNS tree for which a name server has complete information



Resource Records

- The data in the DNS database is stored in entities called resource records
- The most common resource records:
  - A (name to address mapping)
  - PTR (address to name mapping
  - MX (Mail Exchanger record)
  - NS: name server record
  - CNAME: name alias
  - SOA: Start of authority

Master Zone File Example

```
verkot.example.   IN      SOA     ns.verkot.example.
    dnsadmin.verkot.example. (
                  6 28800 7200 604800 86400 )
                  IN      NS      ns.verkot.example.
                  IN      MX      10 mail.verkot.example.
$ORIGIN verkot.example.
localhost         IN      A       127.0.0.1
ns                IN      A       10.10.10.1
mail              IN      A       10.10.10.2
www               IN      A       10.10.10.3
                  IN      TXT     "Our web server"
ftp               IN      CNAME   mail
```

Serial, refresh, retry, expiry, minimum TTL

Error, dot missing

DNS Today

- DNS has served its purpose well
- Internet is evolving, and new requirements have been issued
  - Support for IPv6
  - DNS security extensions
    - Vulnerabilities in DNS used in many attacks (like DNS spoofing)
    - security needed
  - DNS dynamic update
  - International DNS
  - Other new requirements

DNS Threats (1/2)

- Threats to the protocol
  - Packet Interception
    - Eavesdropping, man-in-the-middle attacks, DNS spoofing
  - ID guessing and Query Prediction
    - Predict resolver behavior and send a bogus response
    - Could be a blind attack
  - Name-based attacks
    - For example cache poisoning (using packet interception attacks)

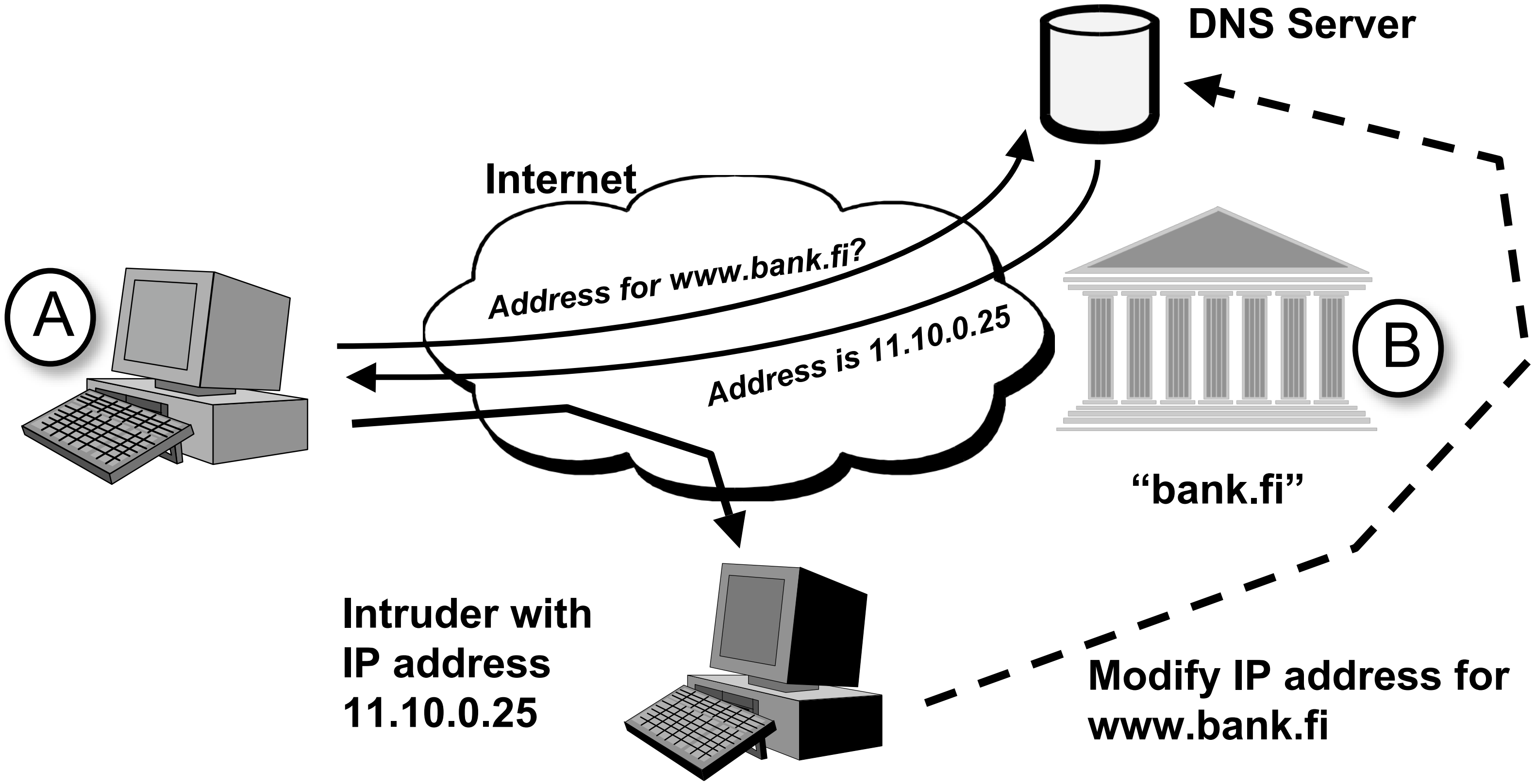
DNS Threats (2/2)

  - DOS attacks
  - Issues with authenticating non-existence of a DNS name
  - Wildcard handling issues
- DNSSEC weaknesses
- DNS Software vulnerabilities

DNS Vulnerabilities

- Crackers often start planning attacks by collecting DNS information
  - many organizations try to make this harder by prohibiting zone transfers and by using split DNS
- Crackers try to use DNS vulnerabilities
  - Both for direct attacks against DNS or for mounting further attacks

Manipulating DNS



DNS Spoofing

- Three ways to manipulate DNS
  - answer to queries with a false reply before the actual name server answers
  - cache poisoning: send false data to a recursive name server with a long TTL
    - the data is cached for a long time
  - compromise the DNS server
    - Using DNS software vulnerabilities

DOS Attacks using Name Servers

- Send a large number of DNS queries (using UDP) to a name server or several name servers (DDOS), using a spoofed IP address
  - responses will be sent to the spoofed IP address
    - the spoofed IP address is the victim
  - hard to trace because of the spoofed IP address
- the responses can be significantly larger than the queries
- DOS possibly both on victim machine and name server

BIND Vulnerabilities (1/3)

- Use the BIND vulnerabilities to compromise the DNS server machine
- often BIND is run as superuser!!!!
- Examples of vulnerabilities
  - BIND Dynamic Update DoS (July 2009)
    - BIND denial of service (server crash) caused by receipt of a specific remote dynamic update message.
    - Fix: upgrade
  - CERT VU#800113 DNS Cache Poisoning Issue (Aug 2008)
    - Fix: DNSSEC, Query Port Randomization for BIND 9 (upgrade)

BIND vulnerabilities (2/3)

- BIND 8: cryptographically weak DNS query IDs (Aug 2007)
  - Consequence: remote attacker could predict DNS query IDs and respond with arbitrary answers, thus poisoning DNS caches.
  - Fix: Upgrade or Patch
  - Note that BIND 8.x.x is End of Life as of August 2007
- BIND 9: allow-query-cache/allow-recursion default acls not set (July 2007)
  - Consequence: The default access control lists (acls) are not being correctly set. If not set anyone can make recursive queries and/or query the cache contents.
  - Fix: configure BIND correctly
- BIND 9: cryptographically weak query ids (July 2007)
  - Consequence: DNS query id generation is vulnerable to cryptographic analysis which provides a 1 in 8 chance of guessing the next query id for 50% of the query ids. This can be used to perform cache poisoning by an attacker
  - Fix: upgrade

BIND vulnerabilities (3/3)

- "BIND: Remote Execution of Code“ (Nov 2002)
  - Versions affected: BIND 4.9.5 to 4.9.10, 8.1, 8.2 to 8.2.6, 8.3.0 to 8.3.3
  - SIG RR code bug
  - Consequence: possibility to execute arbitrary code
  - Fix: upgrade
- Up-to-date information on BIND vulnerabilities
  - https://www.isc.org/advisories/bind

Attack on the DNS InfraStructure

- Distributed DOS attack against the DNS root servers 6 February 2007
  - six of the 13 root servers were affected, two badly
    - the two servers affected badly did not use anycast
  - Anycast
    - spread the load on several servers in different locations
  - Also measures to block the packets part of the DDOS
    - the packets had a larger size than 512 bytes
  - If the root servers do not function, eventually name resolution will not work
    - in this case, fast reaction and a new technology (anycast) lead to limited impact on the actual Internet users

DNS Security (1/3)

- Main documents
  - DNS security extensions
    - New RFCs approved 2005
      - DNS Security Introduction and Requirements, RFC 4033
      - Resource Records for DNS Security Extensions, RFC 4034
      - Protocol Modifications for the DNS Security Extensions, RFC 4035
    - new RFC in 2006
      - Minimally Covering NSEC Records and DNSSEC On-line Signing, RFC 4470
  - Protection of queries and responses
    - Secret Key Transaction Authentication for DNS (TSIG), RFC 2845
    - DNS Request and Transaction Signatures (SIG(0)s), RFC 2931
  - Secure Dynamic Update
    - Secure Domain Name System (DNS) Dynamic Update, RFC 3007
  - Storing Certificates in the Domain Name System (CERT RR), RFC 4398

DNS Security (2/3)

- Security services:
  - Data origin authentication and integrity
    - including ability to prove non-existence of DNS data
  - Transaction and request authentication and integrity
  - Means for public key distribution

DNS Security (3/3)

- DNS security does not offer:
  - confidentiality
  - access control
    - but often the DNS server implementations do
  - protection against attacks on the name server node itself
  - protection against denial of service attacks
  - protection against misconfiguration

DNSSEC Security Extensions (1/9)

- Signature record (RRSIG)
  - a record containing a signature for a DNS RR
  - contains the following information
    - type of record signed
    - algorithm number
    - Labels Field
    - Original TTL
    - signature expiration and inception
    - Key tag
    - signer name
    - Signature
  - replaces SIG record

DNSSEC Security Extensions (2/9)

- Example

```
host.example.com. 86400 IN RRSIG A 5 3 86400 20030322173103 (
                  20030220173103 2642 example.com.
                  oJB1W6WNGv+ldvQ3WDG0MQkg5IEhjRip8WTr
                  PYGv07h108dUKGMeDPKijVCHX3DDKdfb+v6o
                  B9wfuh3DTJXUAfI/M0zmO/zz8bW0Rznl8O3t
                  GNazPwQKkRN20XPXV6nwwfoXmJQbsLNrLfkG
                  J5D6fwFm8nN+6pBzeDQfsS3Ap3o= )
```

DNSSEC Security Extensions (3/9)

- DNSKEY record
  - Stores public keys that are intended for use in DNSSEC
  - contains the following fields
    - flags (indicating a zone key, public key used for TKEY)
    - the protocol (DNS, value 3)
    - the algorithm (RSA, DSA, private)
    - the public key
  - replaces KEY record

DNSSEC Security Extensions (4/9)

- Example

```
example.com. 86400 IN DNSKEY 256 3 5 ( AQPSKmynfzW4kyBv015MUG2DeIQ3
                                       Cbl+BBZH4b/0PY1kxkmvHjcZc8no
                                       kfzj31GajIQKY+5CptLr3buXA10h
                                       WqTkF7H6RfoRqXQeogmMHfpftf6z
                                       Mv1LyBUgia7za6ZEzOJBOztyvhjL
                                       742iU/TpPSEDhm2SNKLijfUppn1U
                                       aNvv4w== )
```

DNSSEC Security Extensions (5/9)

- Delegation Signer record (DS)
  - Indicates which key(s) the child zone uses to sign its records.
  - Contains the following fields
    - Key tag
    - Algorithm
    - Digest type
    - Digest

DNSSEC Security Extensions (6/9)

- Example

dskey.example.com. 86400 IN DNSKEY 256 3 5 (
AQOeiiR0GOMYkDshWoSKz9Xz fwJr1AYtsmx3TGkJaNXVbfi/
2pHm822aJ5iI9BMzNXxeYCmZDRD99WYwYqUSdjMmmAphXdvxegXd/
M5+X7OrzKBaMbCVdFLUUh6DhweJBjEVv5f2wwjM9Xzc
nOf+EPbtG9DMBmADjFDc2w/rljwvFw==) ; key id = 60485

dskey.example.com. 86400 IN DS 60485 5 1 (
2BB183AF5F22588179A53B0A 98631FAD1A292118)

DNSSEC Security Extensions (7/9)

- NSEC record
  - data origin authentication of a non-existent name or record type
  - implies a canonical ordering of records
  - NSEC records are created automatically when doing the signing process
  - replaces NXT records

DNSSEC Security Extensions (8/9)

- Example:

```
ns      86400 IN   A      10.10.10.1
ns      86400 IN   NSEC   www.example.com. (A NSEC)
www     86400 IN   A      10.10.10.3
```

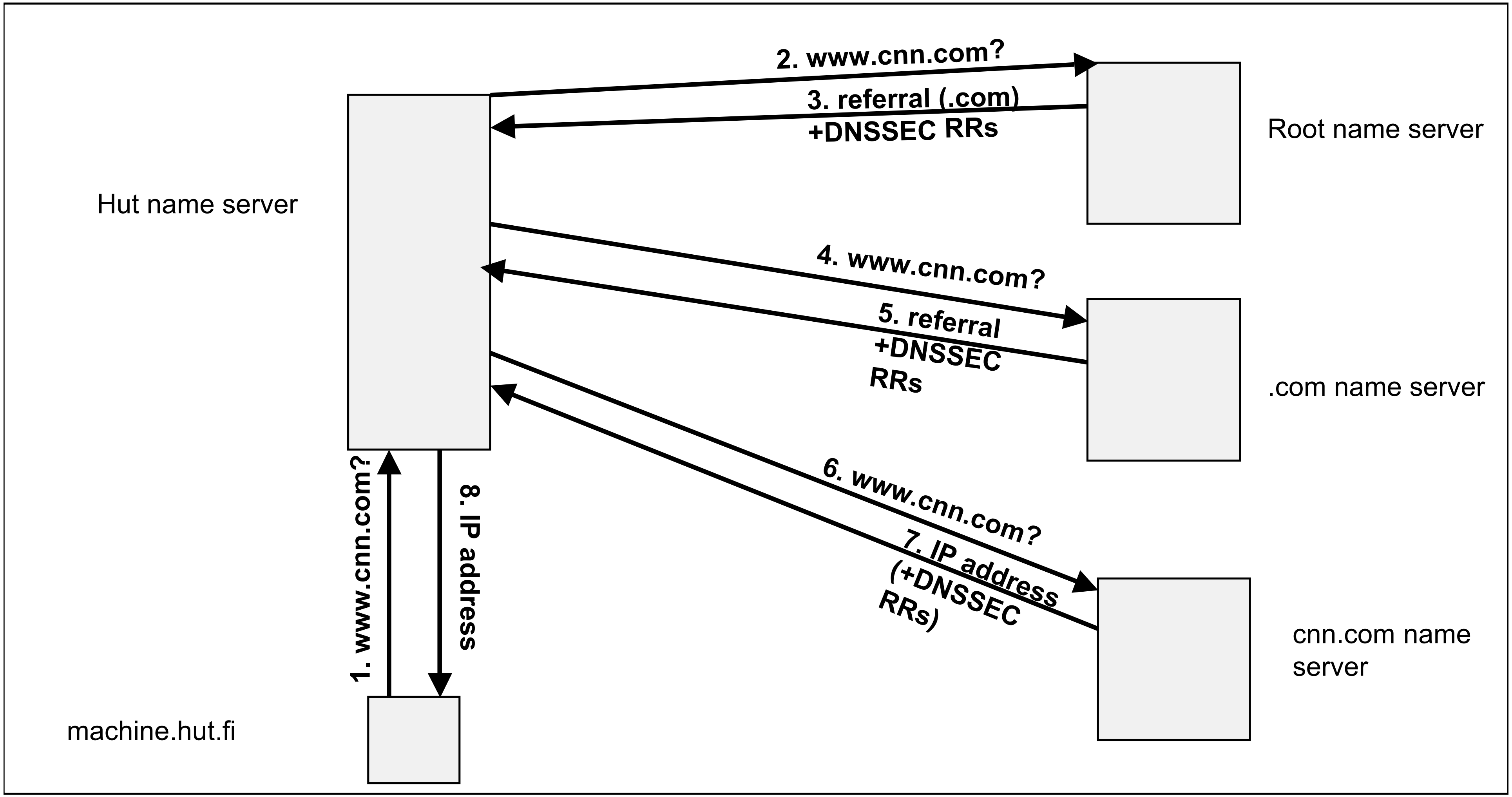
DNSSEC Security Extensions (9/9)

- CERT record
  - can contain different kinds of certificates (SPKI, PKIX X.509, PGP)
  - recommended to be stored under a domain named related to the subject of the certificate

Secure Name Resolution

- The resolver is statically configured with some keys (*key signing key*) it trusts
- the process involves verifying a chain of keys and signatures
  - a record retrieved will include a signature
  - the resolver needs to retrieve the corresponding *zone signing key* to be able to verify the signature
  - Verifications starts from the highest level RR and continues through a chain of verifications, until the zone signing key for the DNS data is verified
  - After that, the DNS data can be verified

Secure Name Resolution (Scenario)



Original Master Zone File

```
verkot.example.          IN          SOA        ns.verkot.example.
dnsadmin.verkot.example. (
                                     6 28800 7200 604800 86400 )
                                     IN         NS          ns.verkot.example.
                                     IN         MX          10 mail.verkot.example.
$ORIGIN verkot.example.
localhost                IN          A          127.0.0.1
ns                                   IN         A           10.10.10.1
mail                                 IN         A           10.10.10.2
www                                  IN         A           10.10.10.3
                                     IN         TXT         "Our web server"
ftp                                  IN         CNAME       mail
verkot.example. IN DNSKEY 256 3 5
AQOoIPWnXoZXUI26cJmIWDNps+hes9uKt71+QzFiTc3FB3xIUPd+nyjB
hArIe1HqcKW4+hE8DtDl//zeVa90LEid2PvdP8Zy++tFZ7Zyhg1IKgIc
TD8qA7DaqHa9Rwhtl9U=
```

Zone File after Signing (1/4)

```
; File written on Wed Sep 28 16:17:16 2005
; dnssec_signzone version 9.3.1
verkot.example.          86400      IN SOA     ns.verkot.example. dnsadmin.verkot.example.
                         (6       ; serial 28800     ; refresh (8 hours) 7200      ; retry (2 hours)
                         604800     ; expire (1 week) 86400      ; minimum (1 day))

86400        RRSIG       SOA 5 2 86400 20051028121716 (
20050928121716 23576 verkot.example.
VZ92OWwT7rK5Nj9yksqdsWJ3GaNGp8tNAL7Bs2Vb8uB1+XN+EPHP4uwlDK43JyzlV0Vj0FHt7hmj9bgws
u6A3Mp332D7k+DRFmhfgHMRdXeMxSGrP+IB89f2BknCyoXQ )
86400        NS          ns.verkot.example.
86400        RRSIG       NS 5 2 86400 20051028121716 (20050928121716 23576 verkot.example.

hXX6fGWcTI+q1NFWJznffkCYPg86wQyW7nwHcdKg0YF2FX57w12A1P9zUlxT8SJ5kJyAEAjBvaxbzKy3q
q3NiNq24vaaU0gjJFt7z+4ZgvVBjcGPq3owrlVX+IjlTCue )
86400        MX          10 mail.verkot.example.
86400        RRSIG       MX 5 2 86400 20051028121716 (20050928121716 23576 verkot.example.

RqOyunvHTO1Rbuc/HNMe35kXNddlHGrtMubjra7CdO5mDrOJlQicdy7YSuyFfeUdZrF0+px8gv0x0daZabP
73zMNW2nKIRtuwDhoNlZLK+op3ycurZ38BR2s79JqfHyD )
86400        NSEC        ftp.verkot.example. NS SOA MX RRSIG NSEC DNSKEY
86400        RRSIG       NSEC 5 2 86400 20051028121716 (20050928121716 23576 verkot.example.

Yi2YRyNpRCUujfWUt0TaG4zyHb1CTVr3BRXDU0JWvG9ECD6AYvpYpMrPUj4pN+qKa4v4MaXNaSKC4
XWsv8Hk/OJIf/BrgCK9OlrPMnPokSd/NSJYEGeTJoI38TZOQYBf )
86400        DNSKEY      256 3 5
(AQOoIPWnXoZXUI26cJmIWDNps+hes9uKt71+QzFiTc3FB3xIUPd+nyjBhArIe1HqcKW4+hE8DtDI//zeVa9
0LEid2PvdP8Zy++tFZ7Zyhg1lKgIcTD8qA7DaqHa9Rwhtl9U=) ; key id = 23576
```

Zone File after Signing (2/4)

86400 RRSIG DNSKEY 5 2 86400 20051028121716 (20050928121716 23576 verkot.example.

EYhRu2WPmgjo8O1JeIgTGgVJvLpExihk8ZDMENyBp5PI+/ioyFFnDeBbi7JtflMGtzHL5oi7yhTVebH5SXZxsxu/Xg6wVD9G6nQIx/19XNgP5RqMOjA9+z5I8mIye386)

ftp.verkot.example. 86400 IN CNAME mail.verkot.example.

86400 RRSIG CNAME 5 3 86400 20051028121716 (20050928121716 23576 verkot.example.

JIVlLtqKls8Km78rAIInGb7uwLF6SQxl7WjXHem6LJ/R2nemrPfpYml0YNXdeVGOTv3n+mRZK4Z/yTySfIxckTqk666X8WYIsRMhwsvdljWHjlj2u4eArbYcdCLeO33s)

86400 NSEC localhost.verkot.example. CNAME RRSIG NSEC

86400 RRSIG NSEC 5 3 86400 20051028121716 (20050928121716 23576 verkot.example.

J3DgodgZgvbnnvZBWzgdJ2qrWjHg19d88Mwj6LiRP+Z8n7xFa9km8Dh/YT+MUWv10nd5b9qOzVYMqmPzxJ7EVd0LgTp09V3lgz7Ki7pZcfIzNhnLHc+03racm5ImHf12)

localhost.verkot.example. 86400 IN A 127.0.0.1

86400 RRSIG A 5 3 86400 20051028121716 (20050928121716 23576 verkot.example.

Uq0P6qTaT2sxSbXqZwqyKNEBUXNS49zUPAJxdcdwukcO3FyQYb6ld269Q7XAhVPVgxXCYOupcU47vWrPhb9C+/ymRhEYFKi/zXt+pNVQyedVKtLtTSqoLzcjsC7kbVXw)

86400 NSEC mail.verkot.example. A RRSIG NSEC

86400 RRSIG NSEC 5 3 86400 20051028121716 (20050928121716 23576 verkot.example.

M1YNaBE08lbE3k97kOBhItlp4dnVCZUrTQSZFr/h?izgth5z4CnX3NLAZdr3d55bNqGa75xPm+1Dg4igfQ/TZRK+p/IOplgCZzggVIWbcTQkndifyHa8tF3mskekSii/)

Zone File after Signing (3/4)

```
mail.verkot.example.    86400   IN A    10.10.10.2
                        86400   RRSIG   A 5 3 86400 20051028121716 (20050928121716 23576
verkot.example.

Nhk09EIqZAT/KOkfLtkf9S4IwI8dlxZHsDQFPuqRUP/riA8HAI1CzcBVZrZ19S8MNiJ6o22yFQp/0rzMfBnJD/0f0hL
o2kaz7Zcsapk+mXd7vsf9Fpi2HrRrdMFWP6nt )
                        86400   NSEC    ns.verkot.example. A RRSIG NSEC
                        86400   RRSIG   NSEC 5 3 86400 20051028121716 (20050928121716
23576 verkot.example.

SxxQMF2soXT3gHrVV9TNEsA6zPXEifGynZ7eFi4/vGm12tkKzA3BTpkImRrLHTrxWuFHpvpUQHxvCxaO8ad3
oP6NCHesI1ICENkuUsFW3MMo7uXNZa3t3VxwOIjtVsw+ )
ns.verkot.example.      86400   IN A    10.10.10.1
                        86400   RRSIG   A 5 3 86400 20051028121716 (
                        20050928121716 23576 verkot.example.

dQIY/CTSUMbPKKxv1DcN1osbAuEpjt5SWmgZgLYx3kpVAk4aSuCGdOWCylRoQdRs/MRx62K6dHhyDy7qtA
yMM//NHwGUbnkrDoSurXsmDS2ud6JCfNyTCWJI+qK5MUKH )
                        86400   NSEC    www.verkot.example. A RRSIG NSEC
                        86400   RRSIG   NSEC 5 3 86400 20051028121716 ( 20050928121716
23576 verkot.example.

Ik+ovY4k2CFyX3vEo66N0HUHNgLmv7h2a7T08E/4FocQgKXhAv8LU4tG+437IEYxwfKo9/j2w5E9cjb+oikTqWq
i3jPTD/Zi74wvVa1SHQR4Is6AMwE7DBdM1od3tSrY )
```

Zone File after Signing (4/4)

www.verkot.example. 86400 IN A 10.10.10.3

86400 RRSIG A 5 3 86400 20051028121716 (20050928121716 23576 verkot.example.

bsxBpAxE7xw9uzV30kTjif7E6IMHHOsn17EZyDp+01dFR3zNv2Zcu6bvy+crnihJNzgzASeXYvnUq4JaJk0U0q
GTDJSlEiDfti/XzflYH3sqDFjw1Yw+ykp4x+gwXOk6)

86400 TXT "Our web server"

86400 RRSIG TXT 5 3 86400 20051028121716 (20050928121716 23576 verkot.example.

Spxg5JIy7vMK8co6hgFng1rISRZENhxkD27jGPxOtH7wjd7wuuktvI2sNgkBo2dtNuAPVdh256jRe9Eo8xd3cP2
MG//NzLjhL05coelgKEpThHQ6orT2WE0FbN/FNxLW)

86400 NSEC verkot.example. A TXT RRSIG NSEC

86400 RRSIG NSEC 5 3 86400 20051028121716 (20050928121716 23576 verkot.example.

mgO9FIagQqRCmsGbKnBizkxHxUizPv79gclAl1eaoSAAFwciTWQpJ4hqrcE9MgS67K0qK/aouoLiNct966GlvK
uk41HEIXaDDoCBQ2YJ+zA9 n9CGqRiO4NRY++eKN5AA)

Implications of the Security Extensions (1/2)

- the record number in the database grows roughly by a factor of three (NSEC, RRSIG records needed)
  - New records have a large size, so the actual database grows even more.
- NSEC records make it possible to list the complete contents of the zone (effectively do a zone transfer)
  - Some ideas
    - Minimally Covering NSEC Records and DNSSEC On-line Signing, RFC 4470
    - DNSSEC Hashed Authenticated Denial of Existence, RFC 5155

Implications of the Security Extensions (2/2)

- DNS UDP packets are limited to the size of 512 (RFC 1035)
  - answer packets including required signature records might exceed the limit
  - IPv6 support also increases DNS message sizes
  - Extension mechanism for DNS (EDNS) provides a solution
  - EDNS must be supported in DNSSEC

Transaction and Request Authentication and Integrity

- Secret Key Transaction Authentication for DNS (TSIG)
  - symmetric encryption
  - covers a complete DNS message with a Message Authentication Code (MAC)
  - signature calculation and verification relatively simple and inexpensive
- DNS Request and transaction signatures (SIG (0))
  - public key encryption, sign the message
  - offers scalability

DNS Dynamic Updates (1/2)

- Authorized clients or servers can dynamically update the zone data
  - zones can not be created or deleted
- example

```
prereq nxrrset www.example.com A
prereq nxrrset www.example.com CNAME
update add www.example.com 3600 CNAME test.example.com
```

DNS Dynamic Updates (2/2)

- Example of use
  - mechanism to automate network configuration even further
    - a DHCP server can update the DNS after it has granted a client a lease for an IP address
  - Can be protected with transaction protection methods
    - Secret Key Transaction Authentication for DNS (TSIG), RFC 2845
    - DNS Request and Transaction Signatures (SIG(0)s), RFC 2931

TKEY RR

- TKEY record
  - can be used for establishing a shared secret between the server and the resolver
    - negotiate a shared secret using Diffie-Hellman
      - Authentication using public keys (SIG (0)) or a previously established shared secret
    - The resolver or server generates the key and encrypts it with the server or resolver public key
  - meta-RR, not present in any master zone files or caches

DNSSEC Issues (1/2)

- DNSSEC is complex
- Significant increase of response packets
- Signature validation increases work load and thus increases response time
- Hierarchical trust model
- Key rollover at the root and TLD name servers
  - for example .com contains millions of RRs
- Strict time synchronization needed

DNSSEC Issues (2/2)

- TSIG
  - Keys need to be online
  - Fine grained authorization not possible
- Many workshops have been held to progress DNSSEC
  - Number of open issues decreasing
- Not much real deployment yet
  - Some secure islands exist
  - TSIG more common

Internationalized DNS (IDN)

- DNS originally designed to work with ASCII as the character set
- Internationalized DNS aims to provide support for other character sets.
  - An encoding from other character sets to ASCII is needed

Security Problems in Internationalized DNS (IDN)

- Phishing concerns known related to IDN
  - Idea: use a different characters set where a name looks the same, but translates to an entirely different domain name
    - Example: http://www.pàypal.com instead of www.paypal.com
- No technical solution has been found to the problems

DNS as a PKI? (1/3)

- Public keys of an entity can be stored under its domain name
  - not intended for personal keys
- DNS can be used to store certificates (CERT record)
  - can include personal keys

DNS as a PKI? (2/3)

- the public key or certificate will be bound to a domain name
  - search for a public key or a certificate must be performed on basis of the domain name
  - a convenient naming convention needs to be used
  - an efficient search algorithm is required

DNS as a PKI? (3/3)

- research on DNS as a certificate repository can be found from the Tessa project at Helsinki University of Technology
  - http://www.tml.tkk.fi/Research/TeSSA/

Conclusions: how to handle DNS Security (1/4)

- Basic security first!
  - Run latest version of the name server
  - Firewall protection
  - Don’t run any other services on the machine
  - Run as non-root
  - Run in a sandbox: chroot environment (“jail”)
  - Eliminate single points of failure
    - Redundancy, run at least two name servers
    - Put name servers in separate sub-networks and behind separate routers

Conclusions: how to handle DNS Security (2/4)

- Basic security (cont.)
  - Consider non-recursive behavior and restricting queries
    - To mitigate against cache poisoning
  - Use random message Ids
  - Hide version number
  - Prevent unauthorized zone transfer
    - TSIG can be used to authenticate zone transfers
  - Restrict DNS dynamic updates
    - TSIG can be used to authenticate dynamic updates

Conclusions: how to handle DNS Security (3/4)

- Split DNS (internal/external)
  - Useful when using private addresses in the internal network
    - Enhances overall security of the network, as only some nodes can connect to the external network directly
    - Firewalls between external and internal network
    - External DNS servers in the DMZ
    - Internal DNS servers in the internal network

Conclusions: how to handle DNS Security (4/4)

- Additional security measures
  - Secret Key Transaction Authentication for DNS (TSIG)
    - Can be used to ensure authentication and integrity for queries, responses, zone transfers, dynamic updates
    - The communication parties need a shared secret
    - Good performance
  - DNS Security Extensions (DNSSEC)
    - Public-key methods
    - Provides scalability but bad performance
- Security is a process
  - Monitor CERT and similar organizations, monitor relevant mailing lists

Some interesting books and links

- Cricket Liu, Paul Albitz, DNS & BIND
  - **the** DNS book
- http://www.ietf.org/html.charters/dnsext-charter.html
- www.dns.net/dnsrd
- www.menandmice.com