Enabling Secure On-line DNS Dynamic Update

Xunhua Wand,
Yih Huang,
David Rine
Department of Computer Science
George Meson University

Yvo Desmdt
Department of Computer Science
Florida State University

by Isaac Arega
Computer Science
CS595SEC
CSUN , 5-2-2002

Domain Name System

Domain Name System (DNS) is a distributed database system used in Internet Protocol (IP) to map host names to IP addresses.

Major components of DNS

- Domain Name Space - will be covered by video presentation
- Zone - will be covered by video presentation
- DNS Transaction – will be covered by video presentation
- DNS Database
- Name Server (DNS Server) - will be covered by video presentation

DNS Database

DNS database or a zone file contain Recourse Records (RR) belonging to a zone.

Example of DNS database

		Type	IP / PTR	Decryption
	IN	NS	csun.edu	Domain
	IN	MX	email-csun.edu	Email server
csun	IN	A	136.166.1.1	Main domain
email-csun	IN	A	136.166.1.2	Email server
www	IN	A	136.166.1.3	www server
FTP	IN	A	136.166.1.4	FTP server
Computer 1	IN	A	136.166.1.5	Host 1 at csun
Computer 2	IN	A	136.166.1.6	Host 2 at csun

Name Server (DNS Server)

Name Server is a computer with DNS server application that is responsible for providing address translation service to clients.

Two types of DNS servers:

Primary (Master) DNS Server

- Responsible for address translation.
- Stores a master read/write DNS database.
- Responsible DNS database maintenance & replication

Secondary (Slave) DNS Sever

- Responsible for address translation.
- Stores a master read only DNS database.

The purpose of secondary DNS server is to ease the workload of primary DNS server. (i.e. large network with multiple subnets, a secondary DNS server is placed at each major subnets)

DNS Transactions

The three common DNS transactions are zone transfer, query request & response, and dynamic update.

Zone Transfer

A zone transfer is a process of replicating DNS database between DNS servers. Usually zone transfer occurs between primary and secondary DNS servers.

Query request / response- occurs between host and DNS server

1) Host name – to - IP mapping
2) IP – to - host name mapping

DNS Transactions (continued)

Dynamic update:

Dynamic update enable real-time update to zone file (DNS database). The update consists of record insertion and modification.

Dynamic update transaction occurs between:

- host and DNS server
- two internal DNS servers

Dynamic update is a preferred method over manual update.

Example usage for Dynamic DNS update include:

- Campuses (CSUN)
- ISP providers,
- multi-network corporations.

Security of Domain Name System

The original DNS was designed without a security measure in place. The design did not provide data origin authentication and data integrity. The system was design with concept that the information contained in DNS database is considered “public”. Therefore, it didn’t require security.

Example

Original DNS operation is similar to 411 telephone operation where information is given to anyone and without validation and consideration for privacy.

Threats to Domain Name System

Types of Threats include:

- Modification: unauthorized alteration of records in DNS database.
- Interruption: interruption of communication between source & destination.
- Interception: interception of message between source & destination.

Example of attacks

DNS Spoofing

An attacker can send false information to DNS server to be stored into DNS database. This type of attack can result in DoS attack.Clients are redirected to false location that does not contain the service the clients desire.

Man- In-the- Middle

An attacker can intercept, read, or intentionally corrupt communication between source and destination. Email, password, and personal info can be intercepted and analyzed by this type of attack

DNSSEC (Domain Name System Security Extension)

DNSSEC was developed to combat the security problems of the original DNS. The primary goal of DNSSEC is to provide data origin authentication and data integrity by using Digital Signature and Public-Key Cryptography. The DNSSEC design introduced number of new resource records. They include SIG, KK, NXT, and CERT records.

SIG and KK are the only relevant records to DNS dynamic update

SIG RR record

SIG (SIGnature) record stores digital signature signed by DNS server. The digital signature is created using private key of DNS server. Each RR record in DNS database will appended with a SIG record. The digital signature enables a host to check the integrity of data upon receiving it from DNS server.

KK RR record

KK record stores public key and digital signature of parent DNS server. The public key belongs to a zone or the entire domain. The public key combined with digital signature of parent DNS, enables a host to check for data origin. A host can determine if the information it received come from authorized DNS server.

Dynamic Update Schemes in DNSSEC

Two modes are developed in DNSSEC to support dynamic update.

Mode A

- Two keys named zone private key and dynamic update key are used. The zone private belongs to DNS server and it is key is kept off-line for maximum security. The dynamic update key is kept on-line and shared with other DNS servers in the zone.

- Two DNS database used, static database kept offline for maximum security, a separate temporary database kept online for purpose of dynamic update.

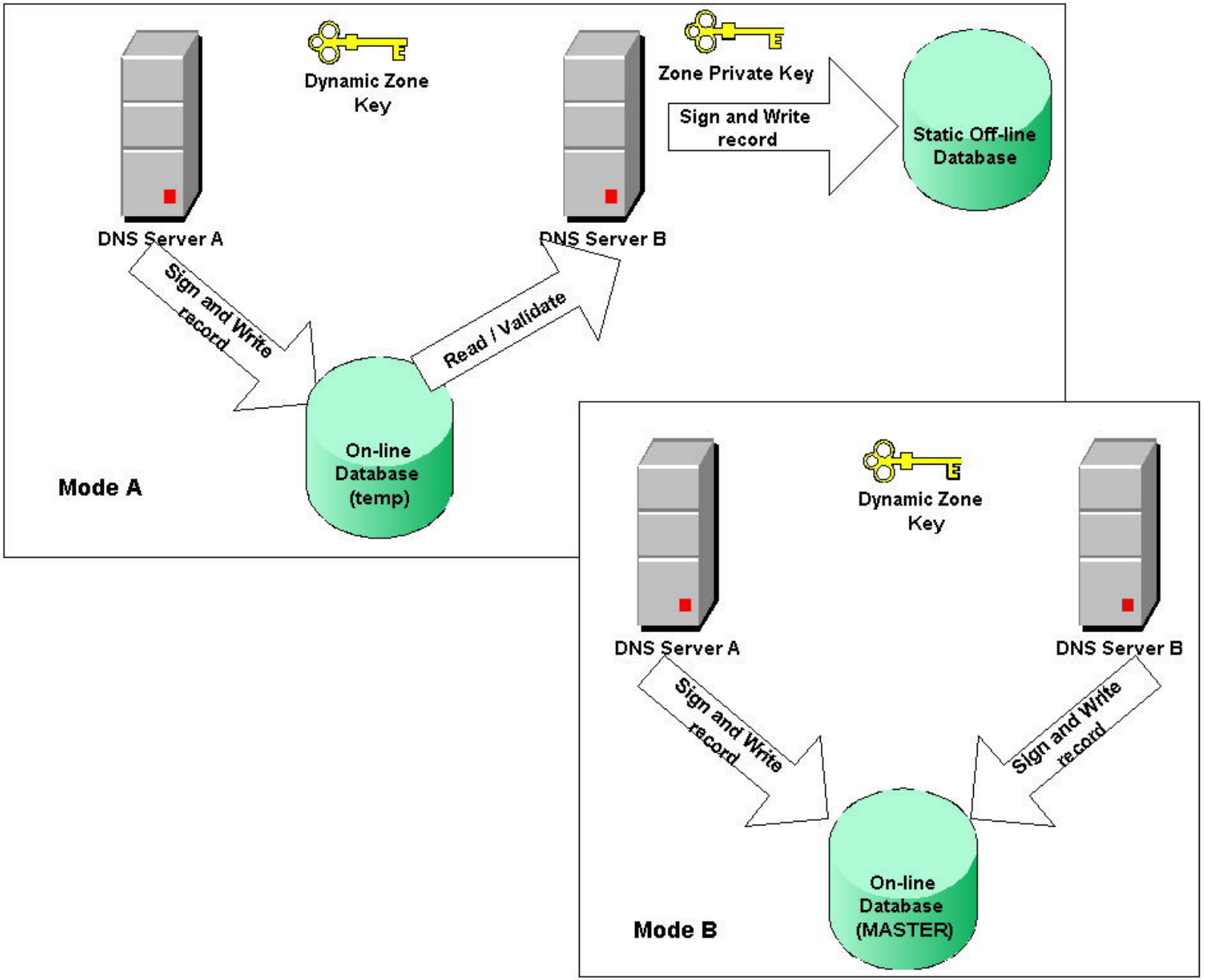
- Update to the static database is not automatic (not a real-time update process).

Dynamic Update Schemes in DNSSEC (continued)

Mode B

Only dynamic update key is used. The key is kept on-line and shard with other DNS servers in the zone.

One dynamic DNS database used. The Database is kept on-line to provide real-time update.



Mode A & B Dynamic Update Schemes in DNSSEC

Weakness of Dynamic Update in DNSSEC

(Motivation points for RFC authors)

Since the zone key and DNS database are kept off-line, direct remote access to the DNS database is not possible. Therefore, it is not considered as a genuine DNS dynamic update process.

Both dynamic update modes do not provide protection against single point attack. Should the primary DNS be compromised, the zone key and static master database will be exposed.

Both dynamic update modes do not provide protection against inside intruders such as “BAD” administrator. DNS system can be abused by administrator who already has access to the zone keys and database. This violates the role of separation principle making is possible for a single person to abuse the system

Alternative Approach to Secure DNS Dynamic Update

The alternative approach to securing dynamic update is designed to use threshold cryptography. The new approach provides:

- support for role of separation principle
- support for genuine secure dynamic update with tolerance against inside / outside intrusion attack

How Threshold Cryptography works

In threshold cryptography, there is a single public key shared among users. The corresponding private key is partitioned and shared among multiple users. Encrypting or decrypting process requires the corporation of all users holding the shared private key. This means, it is not possible for single user to encrypt or decrypt protected message.

(Example: bank safe box deposit / withdraw transaction require two people to lock and unlock safe box)

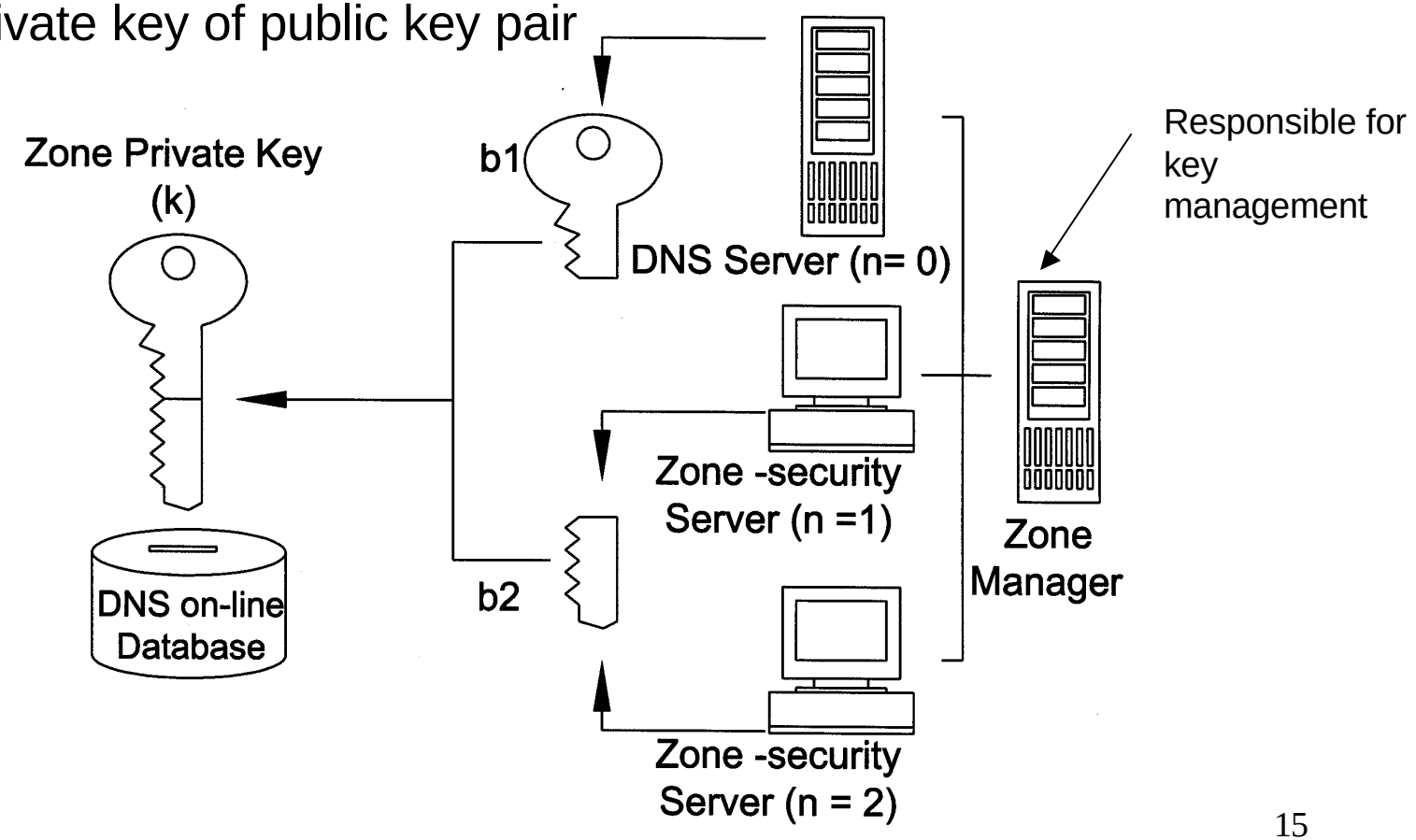
Example of DNS Dynamic Update using Threshold Cryptography

n = 3 , DNS server, 2 zone security servers

t = 1 , threshold (for role of separation principle, intrusion tolerance)

b =2 = t + 1 , members servers actually involve in computation
(servers with partial zone keys)

K = whole private key of public key pair



Configuration and Performance

Table 1. Example configurations in terms of t-n.

Security Level	RSA/MD5 SIG		DSA SIG	
	1-2	2-4	1-3	2-5
Intrusion tolerant against outsider attacks (Y/N)	Y	Y	Y	Y
Intrusion tolerant against insider attacks (Y/N)	N	Y	N	Y

Table 3. Experimental Results

	Zone Key Size (bits)	t-n	Time Cost, in seconds, to compute a SIG	
			Proposed Archtecture	On one machine
RSA/MD5 SIG	1024	1-2	2.172	2.0935
		2-4	2.110	
	2048	1-2	15.9295	15.9408
		2-4	15.8311	
DSA SIG	512	1-3	0.7906	0.1942
		2-5	1.371	
	1024	1-3	1.4217	0.4646
		2-5	2.6999	

Advantages / Disadvantages of Using Threshold Cryptography for DNS Dynamic Update

Advantages

- Protects against inside and outside intruders because the whole private key cannot be recovered or reconstructed from single location.
- Supports the role of separation principle by involving multiple users in cryptographic computation process.
- Highly configurable. The threshold (t) value can be configured to achieve a high level of intrusion tolerance.
- Provides Real-time secure DNS dynamic update is possible provided multiple member's signature.

Disadvantages

- Threshold cryptology does not work if 'n' value is 1
- Provides no protection for DNS dynamic update between host and DNS server