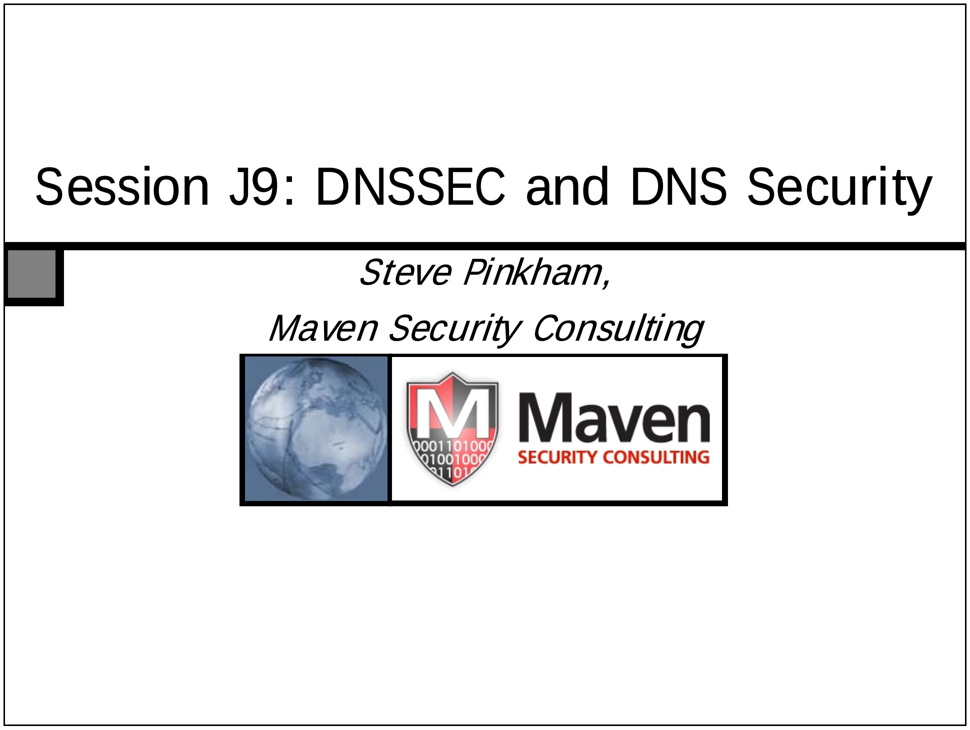
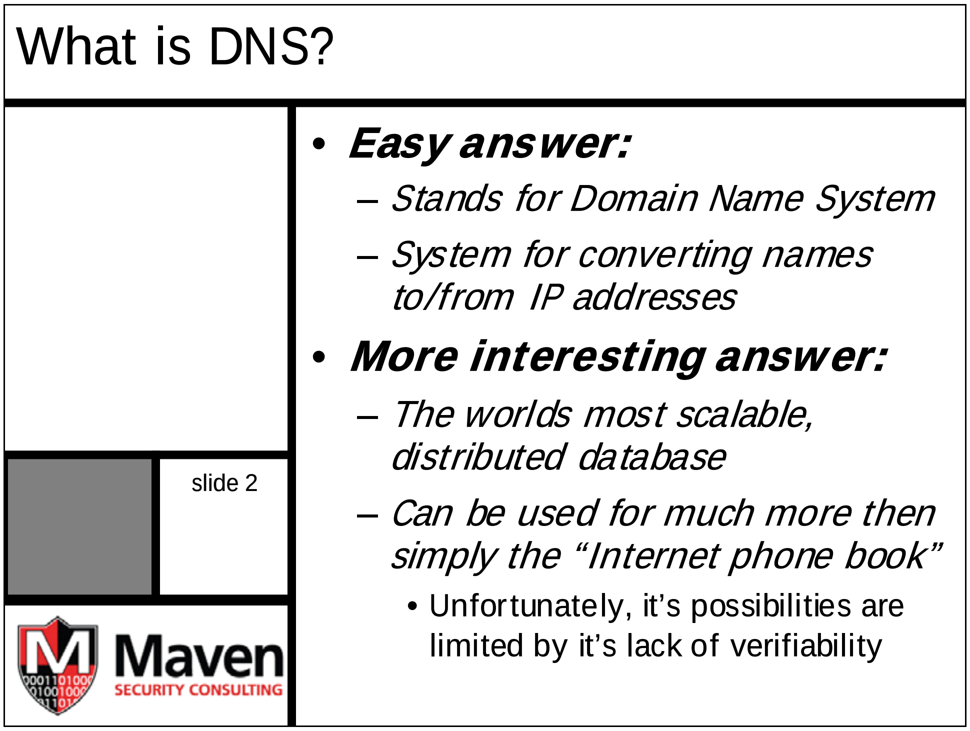


Session J9: DNSSEC and DNS Security

Steve Pinkham,

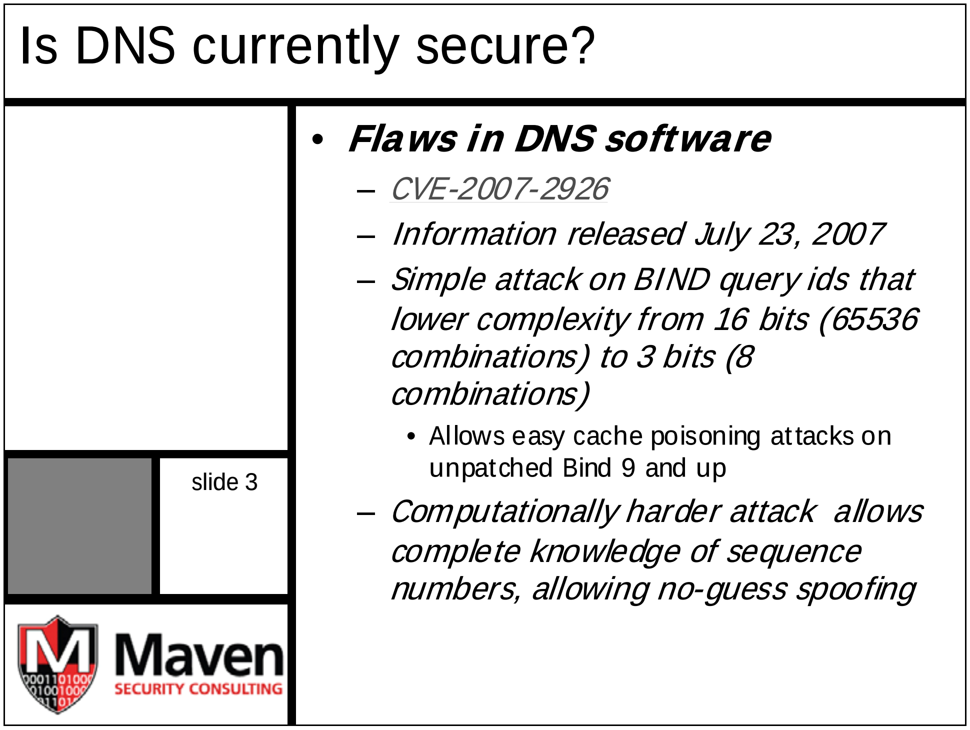
Maven Security Consulting



What is DNS?

- ***Easy answer:***
  - *Stands for Domain Name System*
  - *System for converting names to/from IP addresses*
- ***More interesting answer:***
  - *The worlds most scalable, distributed database*
  - *Can be used for much more then simply the "Internet phone book"*
    - Unfortunately, it's possibilities are limited by it's lack of verifiability

slide 2



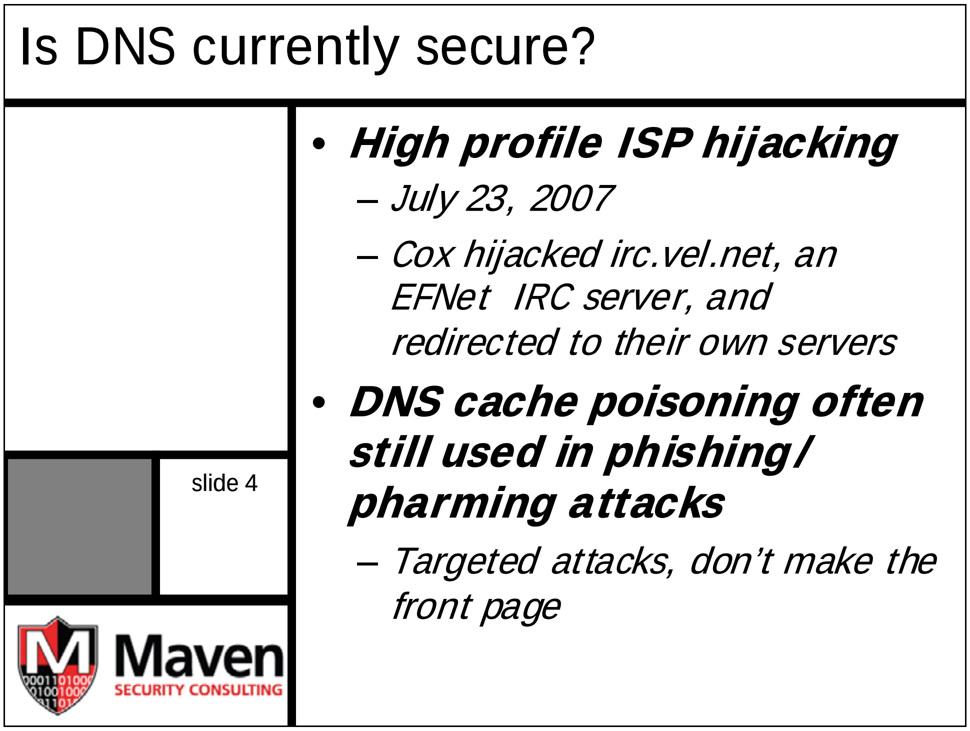
Is DNS currently secure?

- ***Flaws in DNS software***
  - *CVE-2007-2926*
  - *Information released July 23, 2007*
  - *Simple attack on BIND query ids that lower complexity from 16 bits (65536 combinations) to 3 bits (8 combinations)*
    - Allows easy cache poisoning attacks on unpatched Bind 9 and up
  - *Computationally harder attack allows complete knowledge of sequence numbers, allowing no-guess spoofing*

slide 3

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2926

http://www.trusteer.com/docs/bind9dns.html



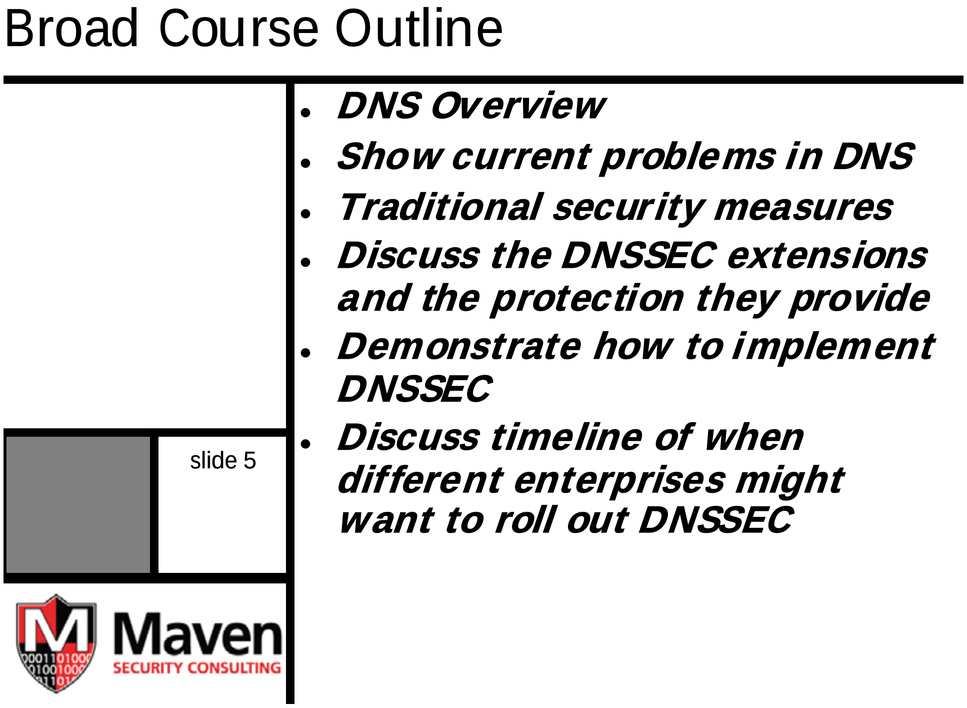
Is DNS currently secure?

- ***High profile ISP hijacking***
  - *July 23, 2007*
  - *Cox hijacked irc.vel.net, an EFNet IRC server, and redirected to their own servers*
- ***DNS cache poisoning often still used in phishing/ pharming attacks***
  - *Targeted attacks, don't make the front page*

slide 4

http://blog.wired.com/27bstroke6/2007/07/isp-seen-breaki.html

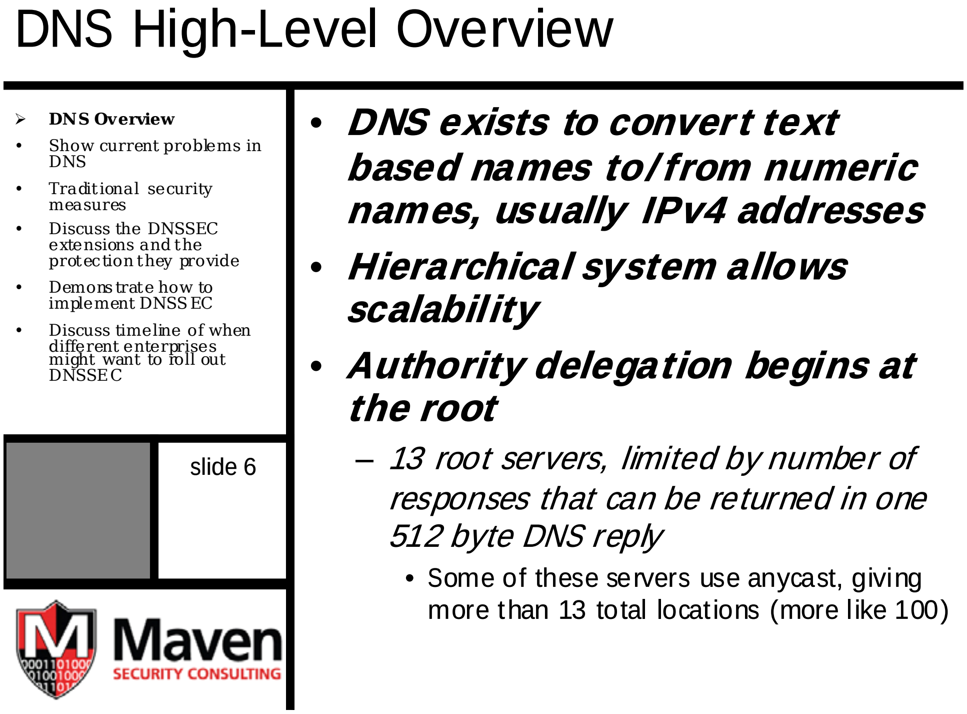
http://www.exstatica.net/hijacked/



Broad Course Outline

- ***DNS Overview***
- ***Show current problems in DNS***
- ***Traditional security measures***
- ***Discuss the DNSSEC extensions and the protection they provide***
- ***Demonstrate how to implement DNSSEC***
- ***Discuss timeline of when different enterprises might want to roll out DNSSEC***

slide 5



DNS High-Level Overview

- **DNS Overview**
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

- ***DNS exists to convert text based names to/from numeric names, usually IPv4 addresses***
- ***Hierarchical system allows scalability***
- ***Authority delegation begins at the root***
  - *13 root servers, limited by number of responses that can be returned in one 512 byte DNS reply*
    - Some of these servers use anycast, giving more than 13 total locations (more like 100)

slide 6

RFC 3258, "Distributing Authoritative Name Servers via Shared Unicast Addresses" http://www.ietf.org/rfc/rfc3258.txt

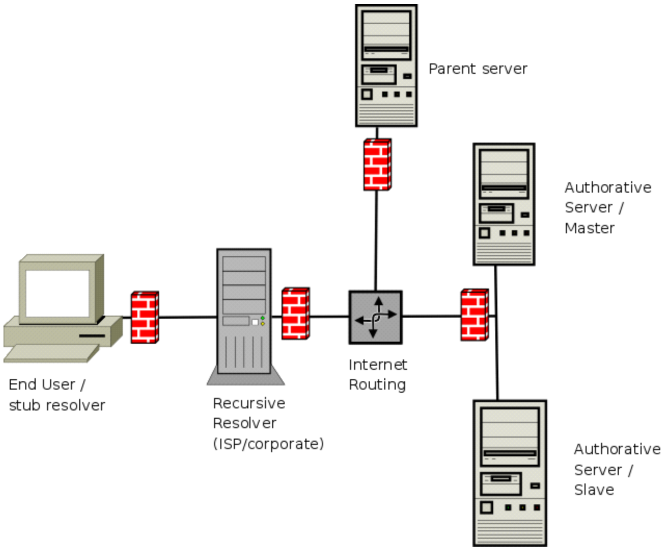
anycast is usually implemented by using BGP to simultaneously announce the same destination IP address range from many different places on the Internet.

DNS Architecture Overview

- **DNS Overview**
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 7

Maven SECURITY CONSULTING


Parent server
Authorative Server / Master
End User / stub resolver
Recursive Resolver (ISP/corporate)
Internet Routing
Authorative Server / Slave

DNS High-Level Overview

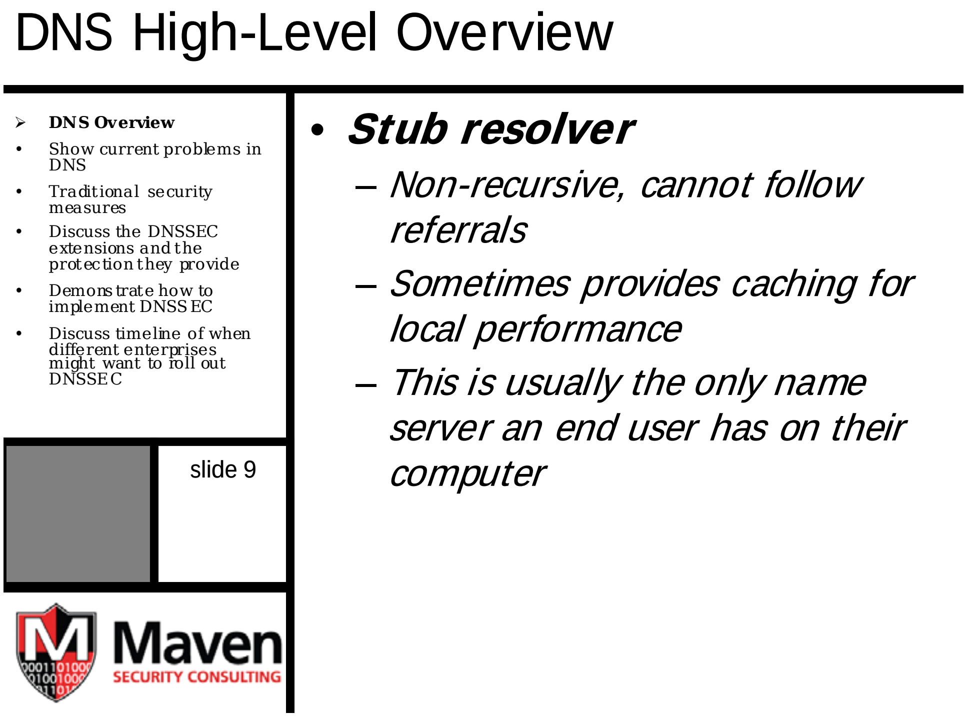
- **DNS Overview**
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 8

Maven SECURITY CONSULTING

- ***Authoritative Name Server***
  - *Name server that contains authoritative information for a domain*
- ***Resolver / Recursive Name Server***
  - *Server that can recursively look up DNS records from authoritative name servers*
  - *Complicated software, must be able to follow referrals and check for many types of possible DNS attacks*
  - *Provides caching of responses to decrease load on the DNS*
- ***Name Server***
  - *Can mean one or both of the above, depending on context*

RFC 3258, "Distributing Authoritative Name Servers via Shared Unicast Addresses" http://www.ietf.org/rfc/rfc3258.txt



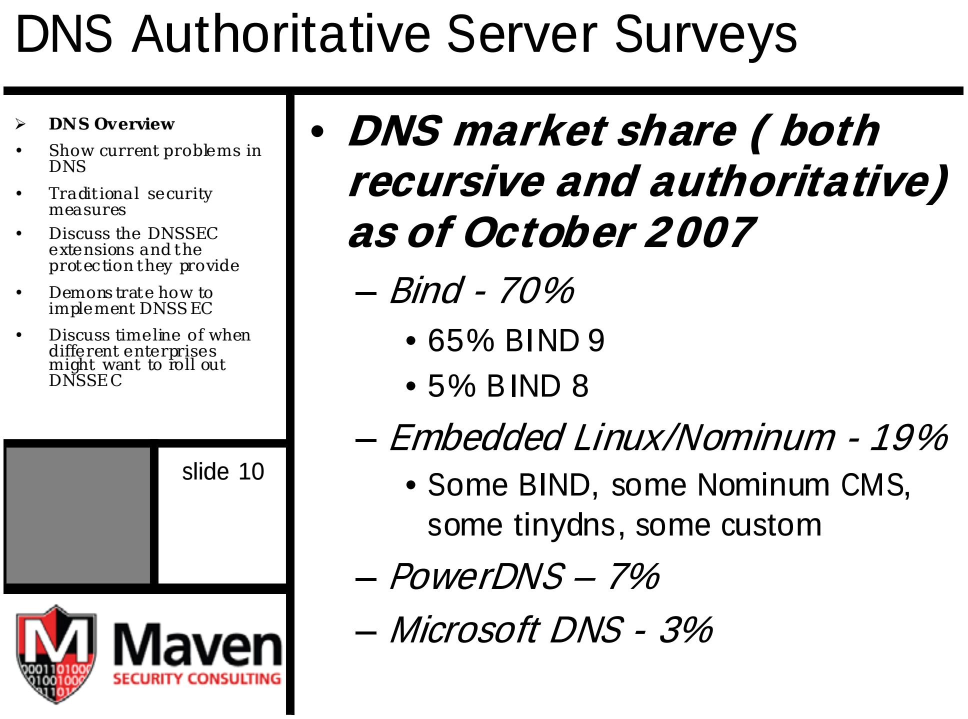
DNS High-Level Overview

- **DNS Overview**
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 9

- ***Stub resolver***
  - *Non-recursive, cannot follow referrals*
  - *Sometimes provides caching for local performance*
  - *This is usually the only name server an end user has on their computer*

RFC 3258, “Distributing Authoritative Name Servers via Shared Unicast Addresses” http://www.ietf.org/rfc/rfc3258.txt



DNS Authoritative Server Surveys

- **DNS Overview**
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 10

- ***DNS market share (both recursive and authoritative) as of October 2007***
  - *Bind - 70%*
    - 65% BIND 9
    - 5% BIND 8
  - *Embedded Linux/Nominum - 19%*
    - Some BIND, some Nominum CMS, some tinydns, some custom
  - *PowerDNS – 7%*
  - *Microsoft DNS - 3%*

Results from http://dns.measurement-factory.com/surveys/200608.html

DNS Authoritative Server Surveys

- **DNS Overview**
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 11

Maven SECURITY CONSULTING

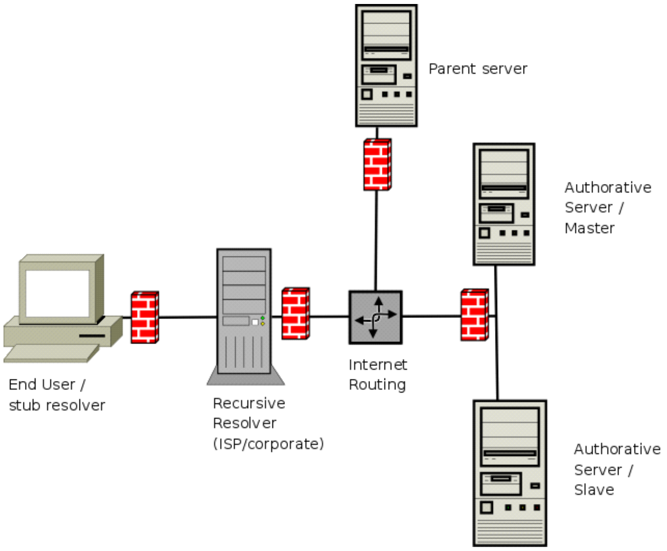
- ***BIND 8 and 9 support DNSSEC***
  - *More then 90% of authoritative domain servers, and much higher percentage of served domains*
  - *Only 9.3 and up support DNSSEC-bis*
    - BIND 9.2 and previous now EOL, most servers should now or soon be 9.3 and up
  - *Nominum, PowerDNS also support DNSSEC*

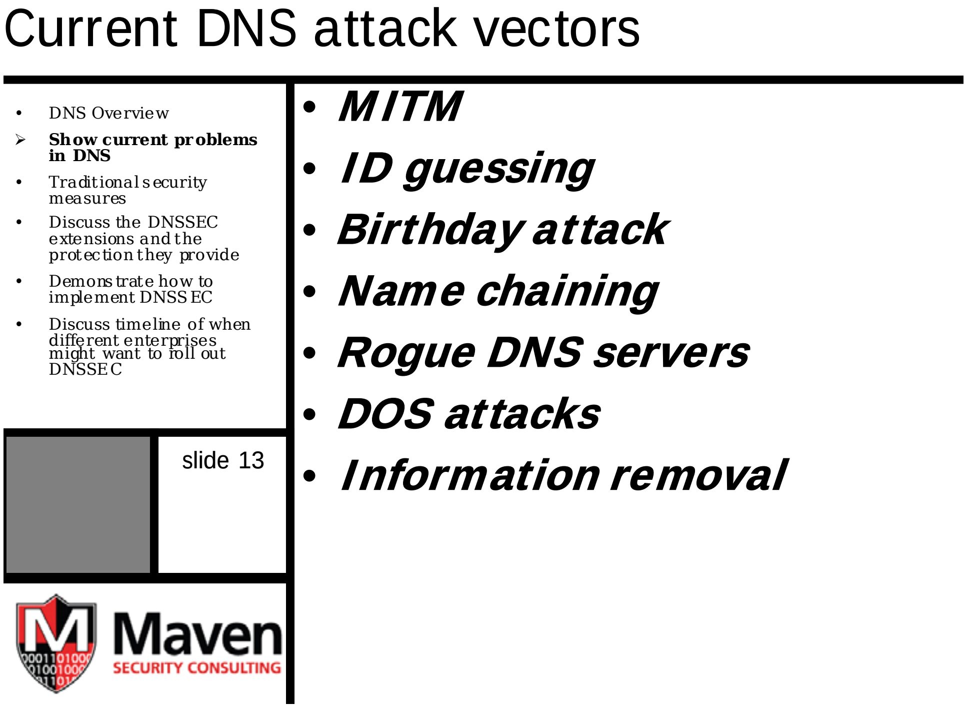
DNS Architecture Overview

- **DNS Overview**
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 12

Maven SECURITY CONSULTING


Parent server
Authorative Server / Master
End User / stub resolver
Recursive Resolver (ISP/corporate)
Internet Routing
Authorative Server / Slave



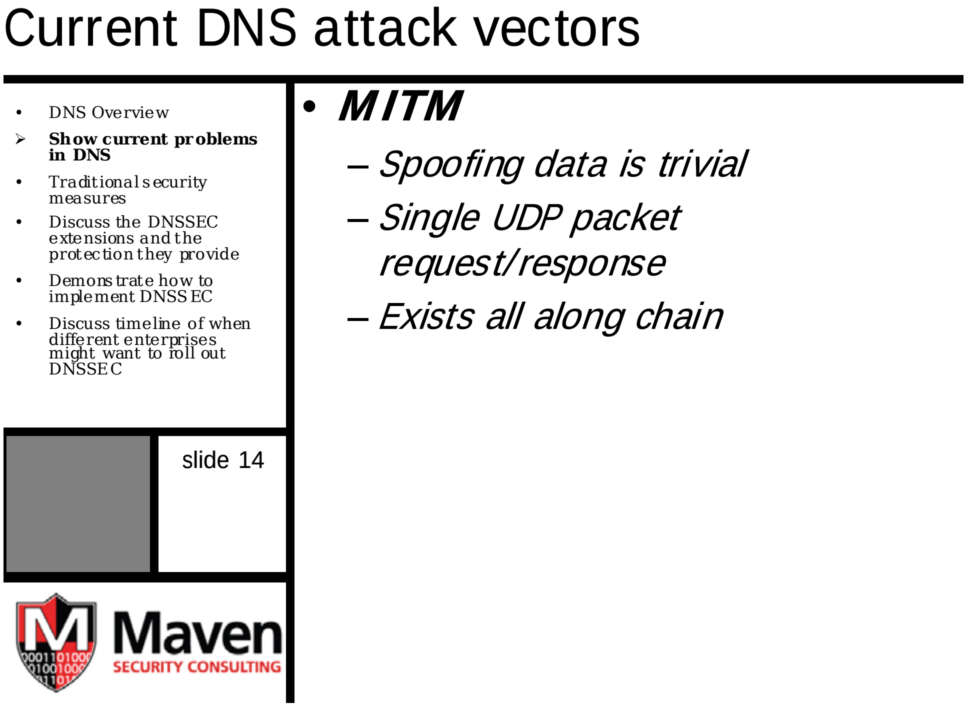
Current DNS attack vectors

- DNS Overview
- **Show current problems in DNS**
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 13

Maven SECURITY CONSULTING

- ***MITM***
- ***ID guessing***
- ***Birthday attack***
- ***Name chaining***
- ***Rogue DNS servers***
- ***DOS attacks***
- ***Information removal***



Current DNS attack vectors

- DNS Overview
- **Show current problems in DNS**
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 14

Maven SECURITY CONSULTING

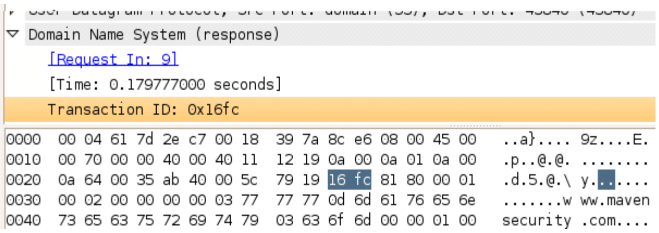
- ***MITM***
  - *Spoofing data is trivial*
  - *Single UDP packet request/response*
  - *Exists all along chain*

Current DNS attack vectors

- DNS Overview
- **Show current problems in DNS**
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 15

- ***ID guessing***
  - *Guess 16 bit nonce and possibly randomly selected port*
  - *Works on recursive resolvers and stubs*



```
▸ User Datagram Protocol, Src Port: domain (53), Dst Port: 43840 (43840)
▽ Domain Name System (response)
    [Request In: 9]
    [Time: 0.179777000 seconds]
    Transaction ID: 0x16fc

0000  00 04 61 7d 2e c7 00 18  39 7a 8c e6 08 00 45 00   ..a}.... 9z....E.
0010  00 70 00 00 40 00 40 11  12 19 0a 00 0a 01 0a 00   .p..@.@. ........
0020  0a 64 00 35 ab 40 00 5c  79 19 16 fc 81 80 00 01   .d.5.@.\ y.......
0030  00 02 00 00 00 00 03 77  77 77 0d 6d 61 76 65 6e   .......w ww.maven
0040  73 65 63 75 72 69 74 79  03 63 6f 6d 00 00 01 00   security .com....
```

  - *Need to force resolving of a known record*

Current DNS attack vectors

- DNS Overview
- **Show current problems in DNS**
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 16

- ***Birthday attack***
  - *Subset of ID guessing*
    - Send multiple requests to the targeted recursive resolver targeting the same authoritative server
    - Send your poisoning attacks, which can match any of the results from the queries
    - 50% success with 300 packets, conventional poisoning needs 32K packets for 50% success
    - Mitigated by late bind 9 by combining aggregating queries
    - Made much more difficult by query source port randomization in djbdns, soon in BIND

Current DNS attack vectors

- DNS Overview
- **Show current problems in DNS**
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 17

- ***Name Chaining***
  - *Cache poisoning attack only, doesn't affect stub resolvers*
  - *Must use one of the former methods to insert itself*
  - *Differs from conventional poisoning attacks in that only requested information is returned, but with falsified answers*
    - Conventional poisoning returns bogus records in addition to what is asked for, blocked by all modern resolvers, I.E. windows 2003, Bind 9

Current DNS attack vectors

- DNS Overview
- **Show current problems in DNS**
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 18

- ***Rogue DNS servers***
  - *DNS servers usually assigned by DHCP*
  - *Do you trust that free wifi?*
  - *Survey of DNS servers that attempt to poison old clients by returning bogus information*
    - http://dns.measurement-factory.com/surveys/poisoners.html

Current DNS attack vectors

- DNS Overview
- **Show current problems in DNS**
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 19

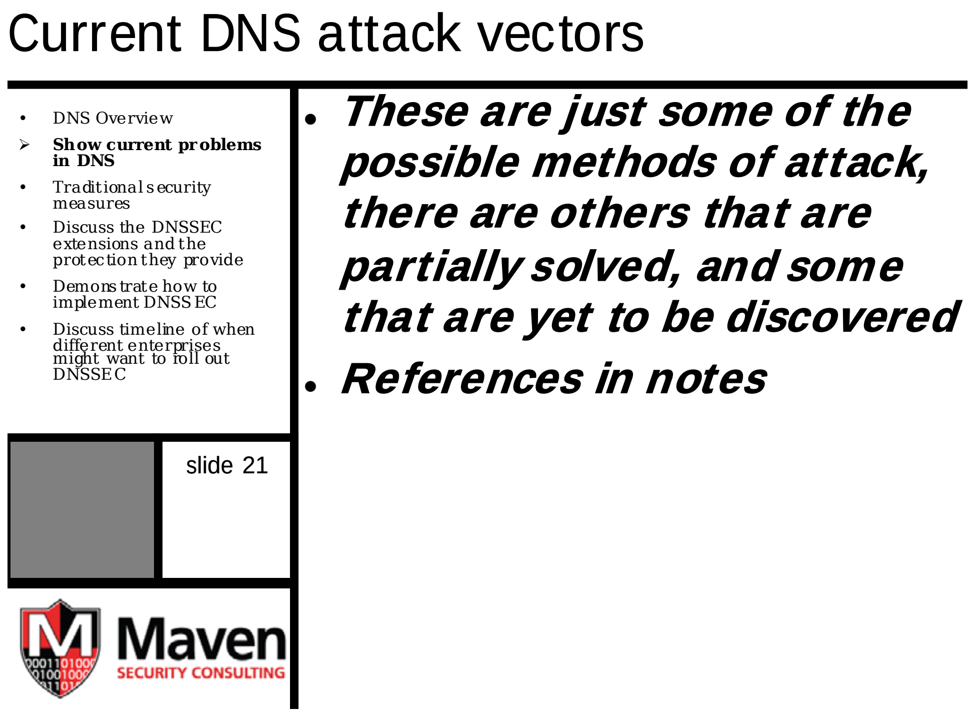
- ***DOS attacks***
  - *Attacks against the DNS servers themselves*
  - *Attacking other systems with DNS amplification*
  - *Both of these attacks are made easier by DNSSEC*

Current DNS attack vectors

- DNS Overview
- **Show current problems in DNS**
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 20

- ***Information Removal***
  - *Special case of MITM problem*
  - *For example, remove MX record for example.com, causing failover to A record*
  - *Mitigated by DNS denial of existence*



Current DNS attack vectors

- DNS Overview
- ➢ **Show current problems in DNS**
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

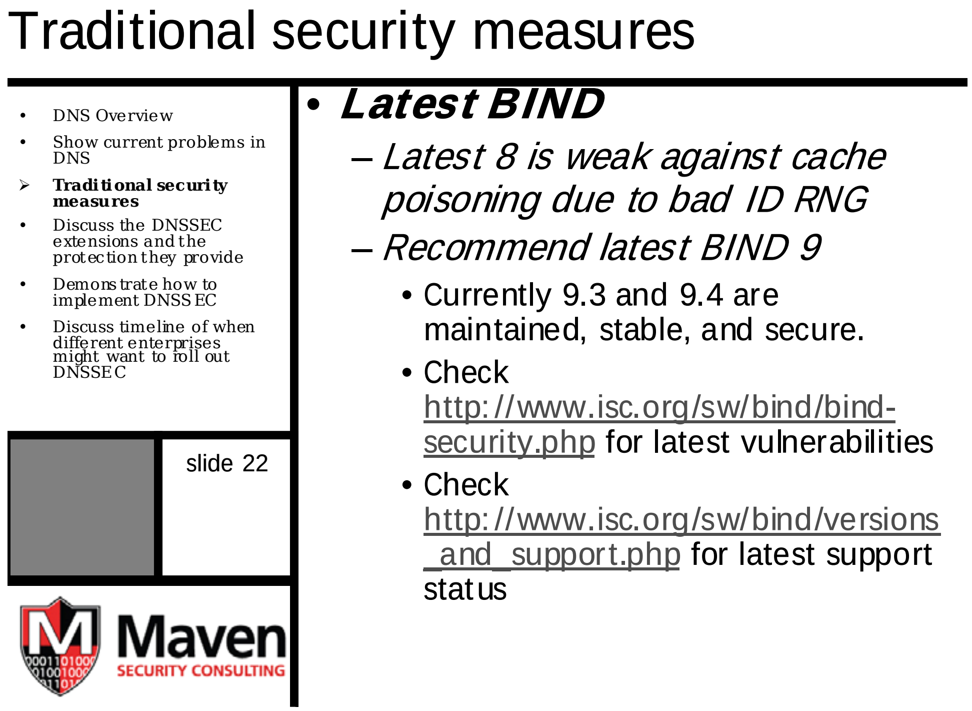
slide 21

- ***These are just some of the possible methods of attack, there are others that are partially solved, and some that are yet to be discovered***
- ***References in notes***

“Threat Analysis of the Domain Name System”, http://www.ietf.org/rfc/rfc3833.txt

Bind vulnerabilities, http://www.isc.org/sw/bind/bind-security.php

“DNS Cache Poisoning – The Next Generation”, http://www.secureworks.com/research/articles/cachepoisoning



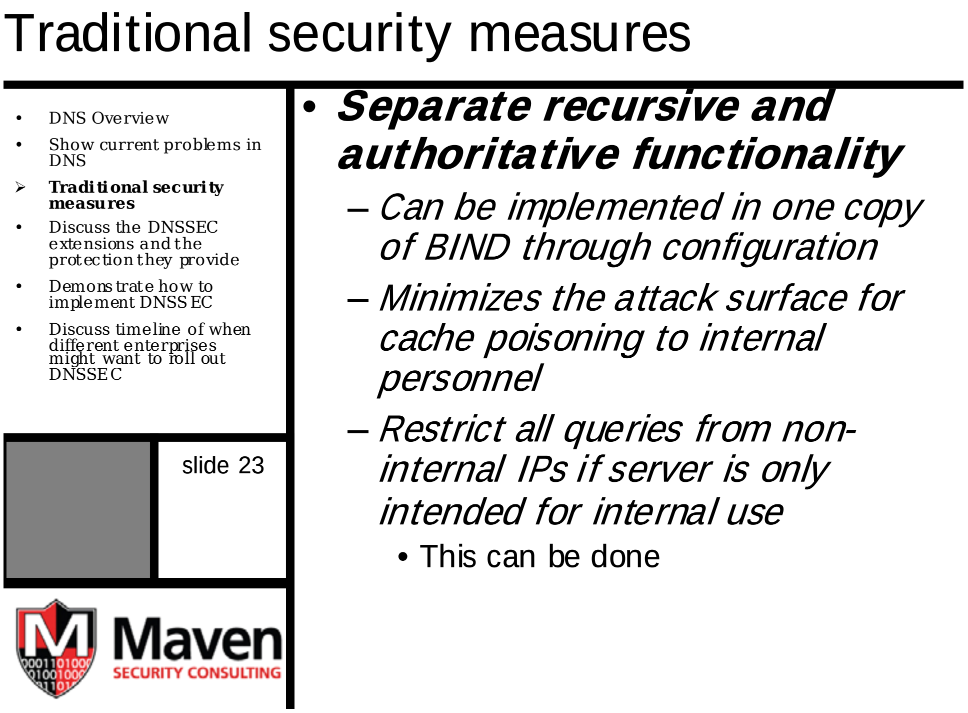
Traditional security measures

- DNS Overview
- Show current problems in DNS
- ➢ **Traditional security measures**
- Discuss the DNSSEC extensions and the protection they provide
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 22

- ***Latest BIND***
  - *Latest 8 is weak against cache poisoning due to bad ID RNG*
  - *Recommend latest BIND 9*
    - Currently 9.3 and 9.4 are maintained, stable, and secure.
    - Check http://www.isc.org/sw/bind/bind-security.php for latest vulnerabilities
    - Check http://www.isc.org/sw/bind/versions_and_support.php for latest support status

“Securing an Internet Name Server”, CERT Coordination Center, http://www.cert.org/archive/pdf/dns.pdf



Traditional security measures

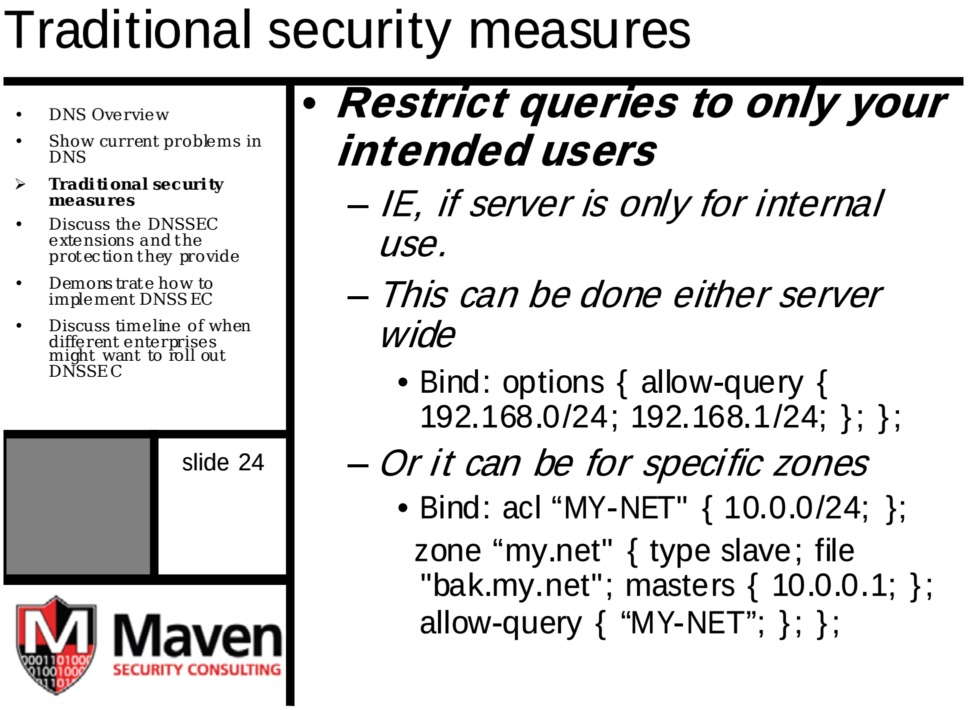
- DNS Overview
- Show current problems in DNS
- ➢ **Traditional security measures**
- Discuss the DNSSEC extensions and the protection they provide
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 23

Maven SECURITY CONSULTING

- ***Separate recursive and authoritative functionality***
  - *Can be implemented in one copy of BIND through configuration*
  - *Minimizes the attack surface for cache poisoning to internal personnel*
  - *Restrict all queries from non-internal IPs if server is only intended for internal use*
    - This can be done

“Securing an Internet Name Server”, CERT Coordination Center, http://www.cert.org/archive/pdf/dns.pdf



Traditional security measures

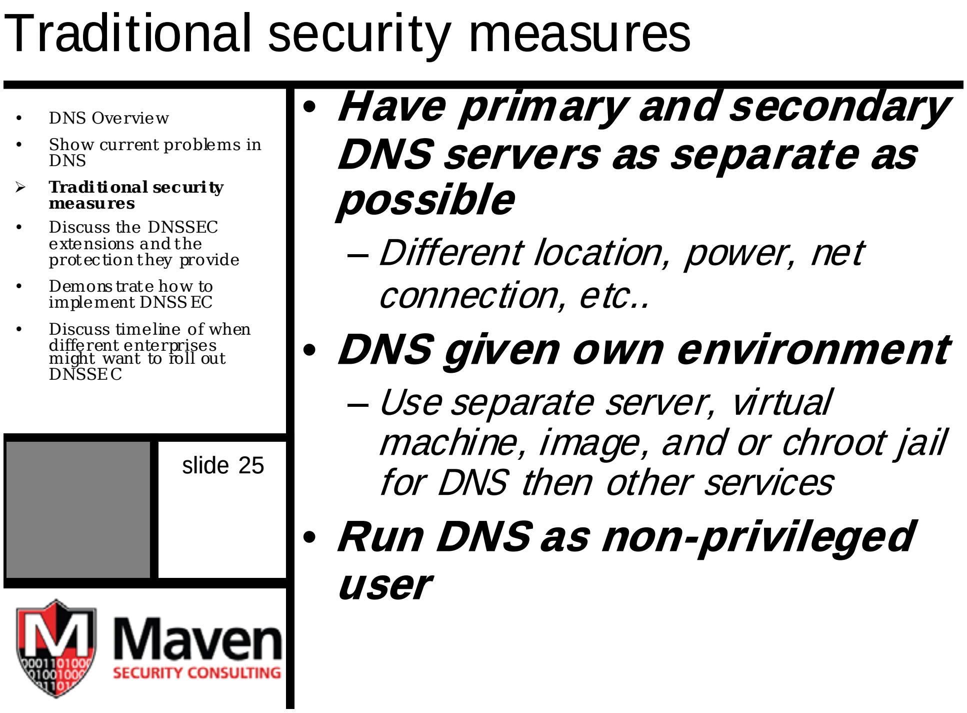
- DNS Overview
- Show current problems in DNS
- ➢ **Traditional security measures**
- Discuss the DNSSEC extensions and the protection they provide
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 24

Maven SECURITY CONSULTING

- ***Restrict queries to only your intended users***
  - *IE, if server is only for internal use.*
  - *This can be done either server wide*
    - Bind: options { allow-query { 192.168.0/24; 192.168.1/24; }; };
  - *Or it can be for specific zones*
    - Bind: acl “MY-NET" { 10.0.0/24; };
      zone “my.net" { type slave; file "bak.my.net"; masters { 10.0.0.1; }; allow-query { “MY-NET”; }; };

“Securing an Internet Name Server”, CERT Coordination Center, http://www.cert.org/archive/pdf/dns.pdf



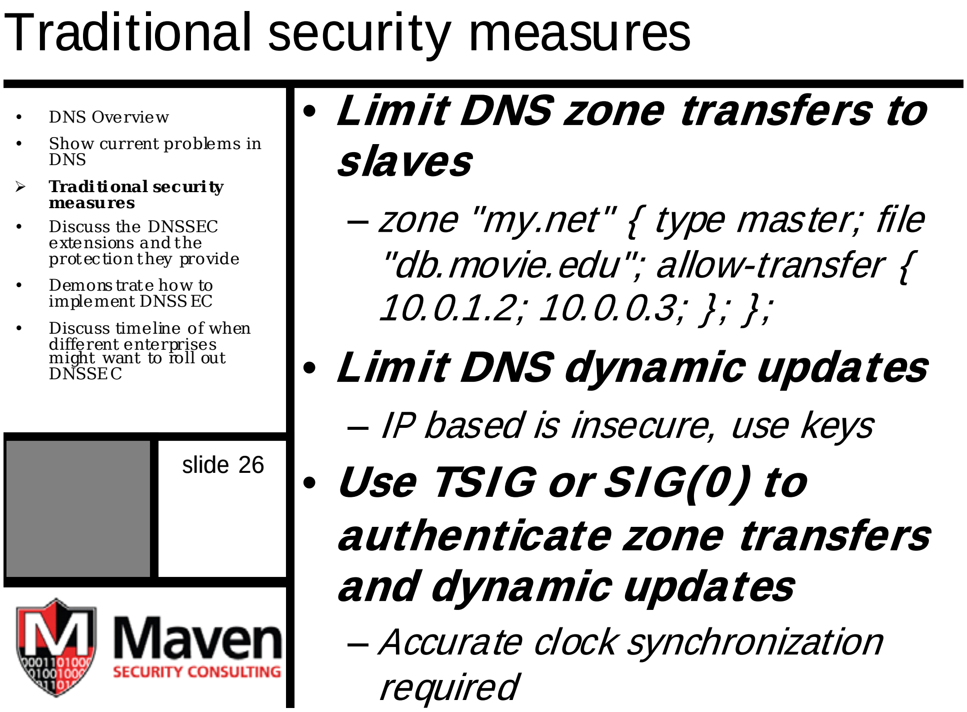
Traditional security measures

- DNS Overview
- Show current problems in DNS
- ➢ **Traditional security measures**
- Discuss the DNSSEC extensions and the protection they provide
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 25

Maven SECURITY CONSULTING

- ***Have primary and secondary DNS servers as separate as possible***
  - – *Different location, power, net connection, etc..*
- ***DNS given own environment***
  - – *Use separate server, virtual machine, image, and or chroot jail for DNS then other services*
- ***Run DNS as non-privileged user***



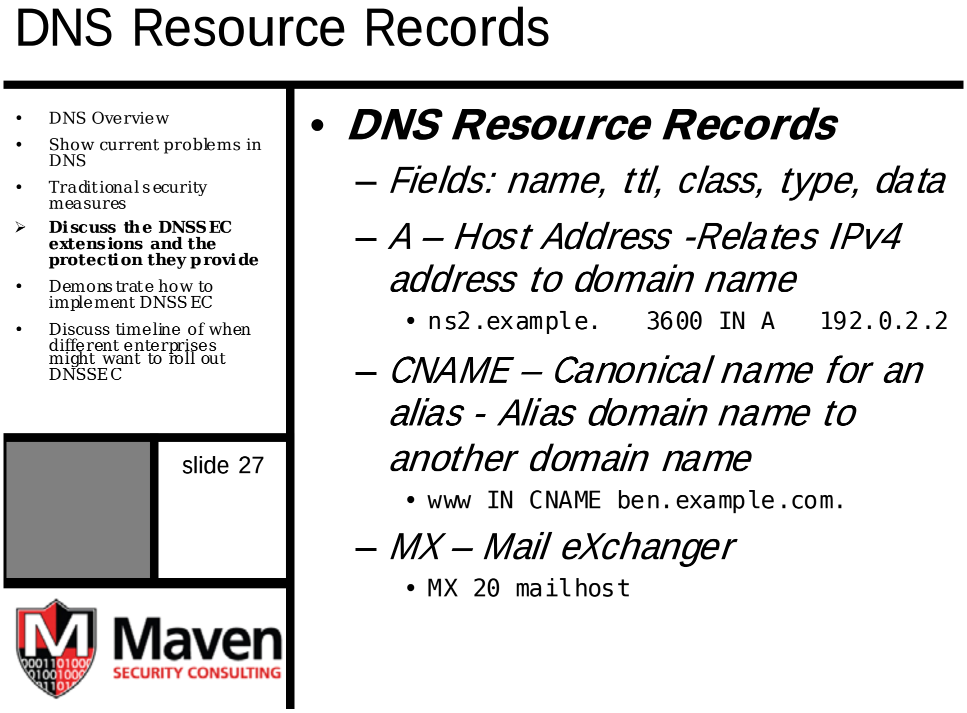
Traditional security measures

- DNS Overview
- Show current problems in DNS
- ➢ **Traditional security measures**
- Discuss the DNSSEC extensions and the protection they provide
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 26

Maven SECURITY CONSULTING

- ***Limit DNS zone transfers to slaves***
  - – *zone "my.net" { type master; file "db.movie.edu"; allow-transfer { 10.0.1.2; 10.0.0.3; }; };*
- ***Limit DNS dynamic updates***
  - – *IP based is insecure, use keys*
- ***Use TSIG or SIG(0) to authenticate zone transfers and dynamic updates***
  - – *Accurate clock synchronization required*

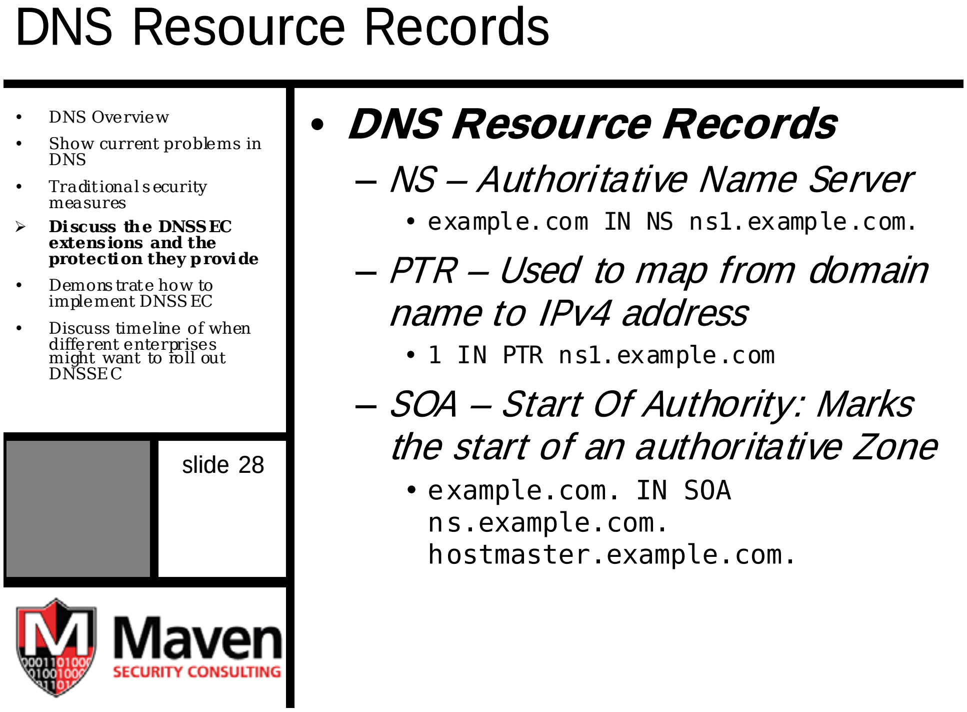


DNS Resource Records

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- **Discuss the DNSSEC extensions and the protection they provide**
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 27

- ***DNS Resource Records***
  - *Fields: name, ttl, class, type, data*
  - *A – Host Address -Relates IPv4 address to domain name*
    - `ns2.example.   3600 IN A   192.0.2.2`
  - *CNAME – Canonical name for an alias - Alias domain name to another domain name*
    - `www IN CNAME ben.example.com.`
  - *MX – Mail eXchanger*
    - `MX 20 mailhost`

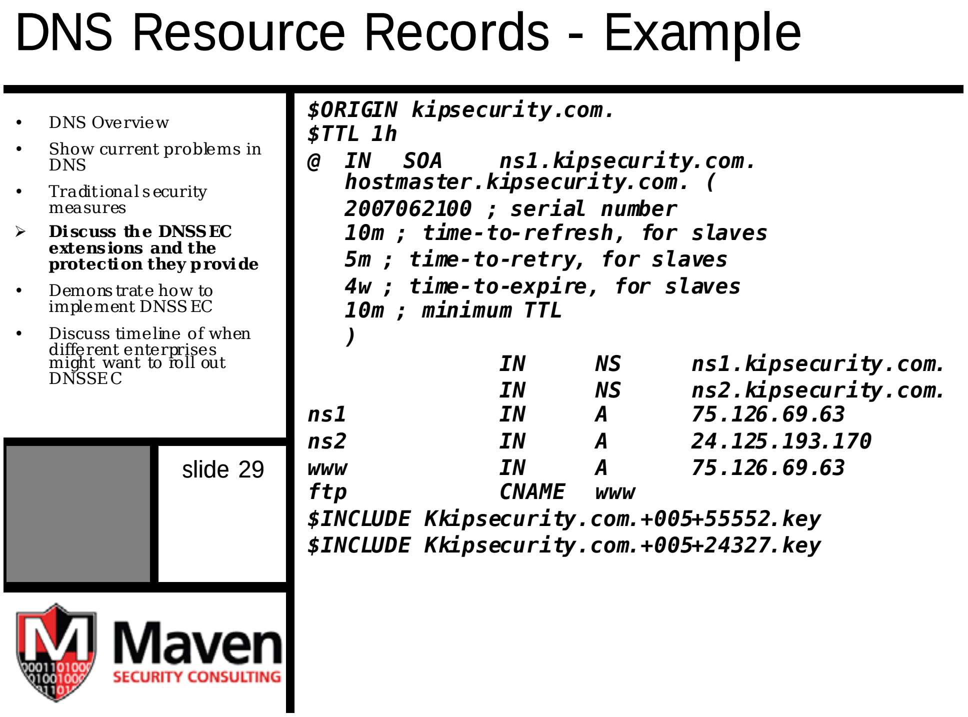


DNS Resource Records

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- **Discuss the DNSSEC extensions and the protection they provide**
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 28

- ***DNS Resource Records***
  - *NS – Authoritative Name Server*
    - `example.com IN NS ns1.example.com.`
  - *PTR – Used to map from domain name to IPv4 address*
    - `1 IN PTR ns1.example.com`
  - *SOA – Start Of Authority: Marks the start of an authoritative Zone*
    - `example.com. IN SOA ns.example.com. hostmaster.example.com.`

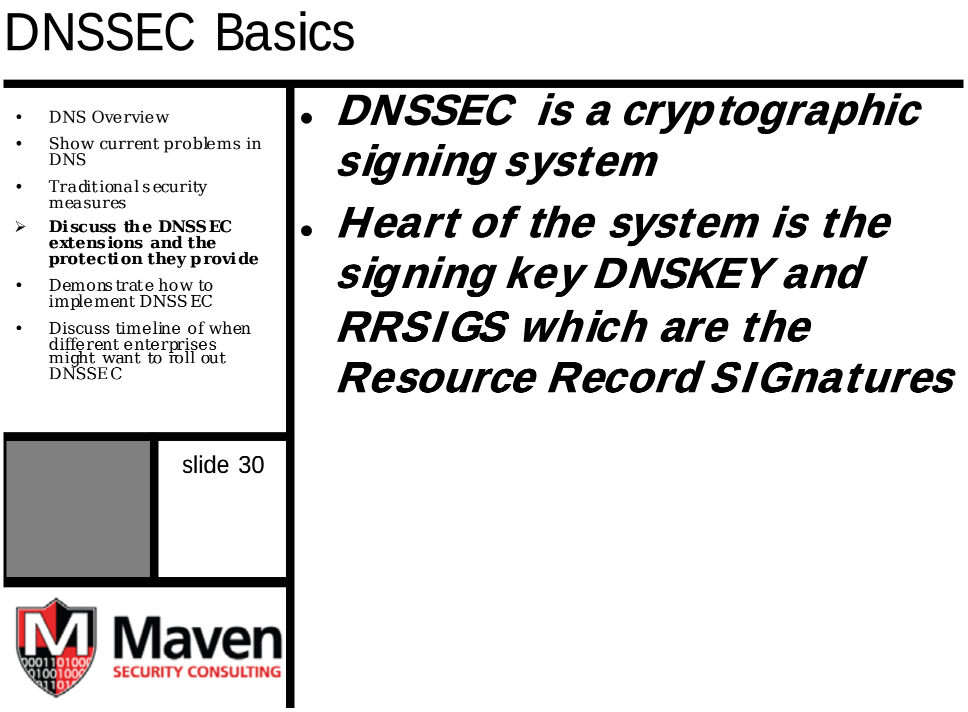


DNS Resource Records - Example

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- ➢ **Discuss the DNSSEC extensions and the protection they provide**
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 29

```
$ORIGIN kipsecurity.com.
$TTL 1h
@  IN   SOA     ns1.kipsecurity.com.
   hostmaster.kipsecurity.com. (
   2007062100 ; serial number
   10m ; time-to-refresh, for slaves
   5m ; time-to-retry, for slaves
   4w ; time-to-expire, for slaves
   10m ; minimum TTL
   )
               IN      NS      ns1.kipsecurity.com.
               IN      NS      ns2.kipsecurity.com.
ns1            IN      A       75.126.69.63
ns2            IN      A       24.125.193.170
www            IN      A       75.126.69.63
ftp            CNAME   www
$INCLUDE Kkipsecurity.com.+005+55552.key
$INCLUDE Kkipsecurity.com.+005+24327.key
```

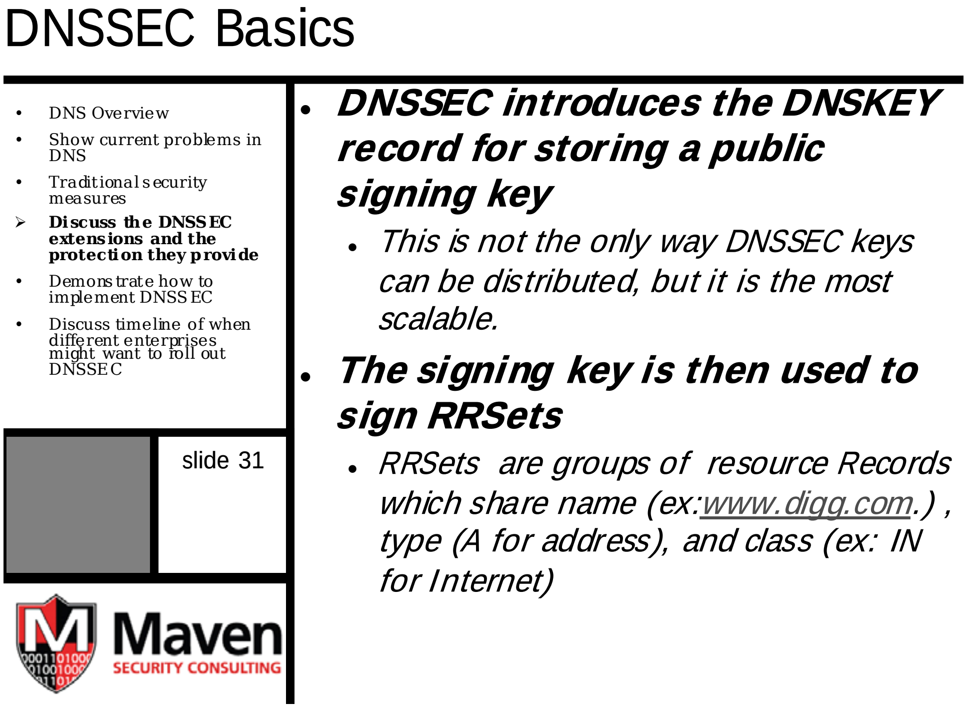


DNSSEC Basics

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- ➢ **Discuss the DNSSEC extensions and the protection they provide**
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 30

- ***DNSSEC is a cryptographic signing system***
- ***Heart of the system is the signing key DNSKEY and RRSIGS which are the Resource Record SIGnatures***



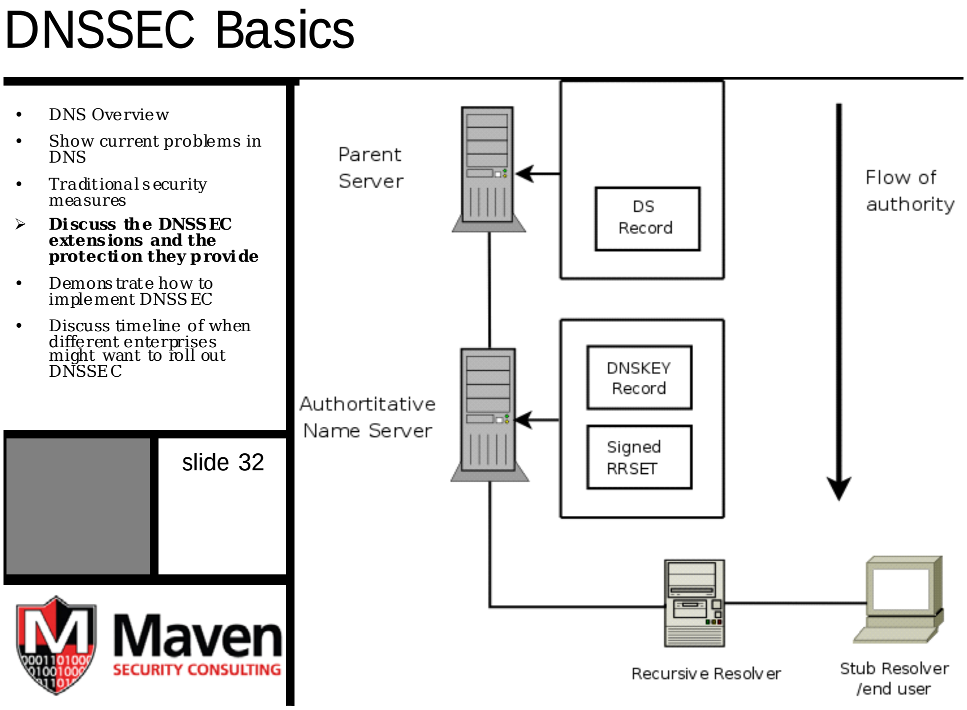
DNSSEC Basics

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- ➢ **Discuss the DNSSEC extensions and the protection they provide**
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 31

- ***DNSSEC introduces the DNSKEY record for storing a public signing key***
  - *This is not the only way DNSSEC keys can be distributed, but it is the most scalable.*
- ***The signing key is then used to sign RRSets***
  - *RRSets are groups of resource Records which share name (ex:www.digg.com.) , type (A for address), and class (ex: IN for Internet)*

RRSet vs RRset: http://mail.shinkuro.com:8100/lists/dnssec-deployment/Message/781.html?Language=

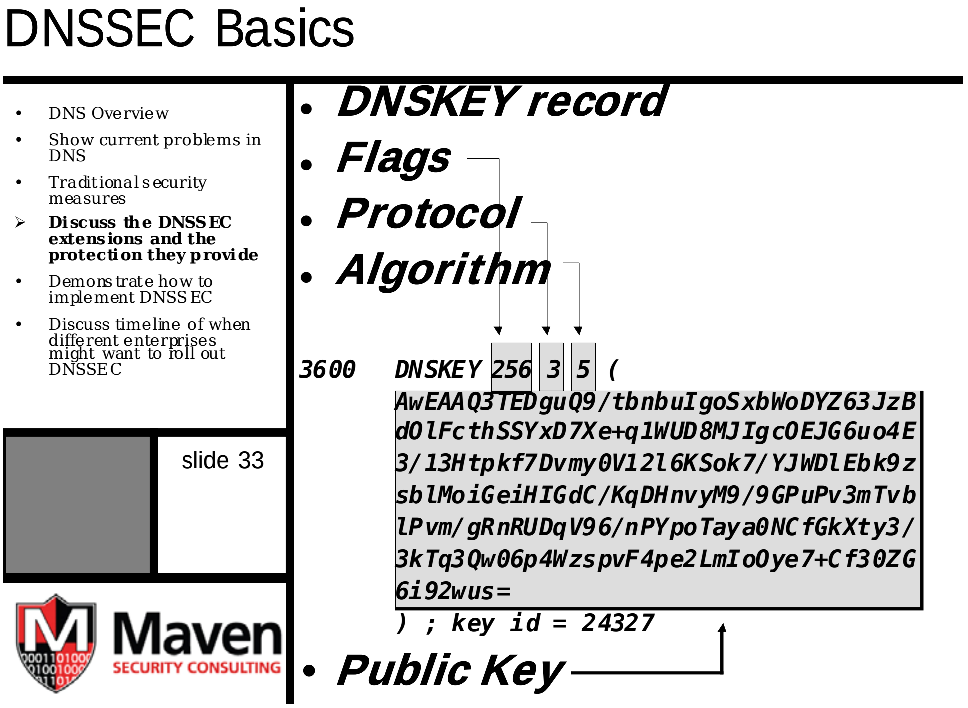


DNSSEC Basics

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- ➢ **Discuss the DNSSEC extensions and the protection they provide**
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 32

RRSet vs RRset: http://mail.shinkuro.com:8100/lists/dnssec-deployment/Message/781.html?Language=



DNSSEC Basics

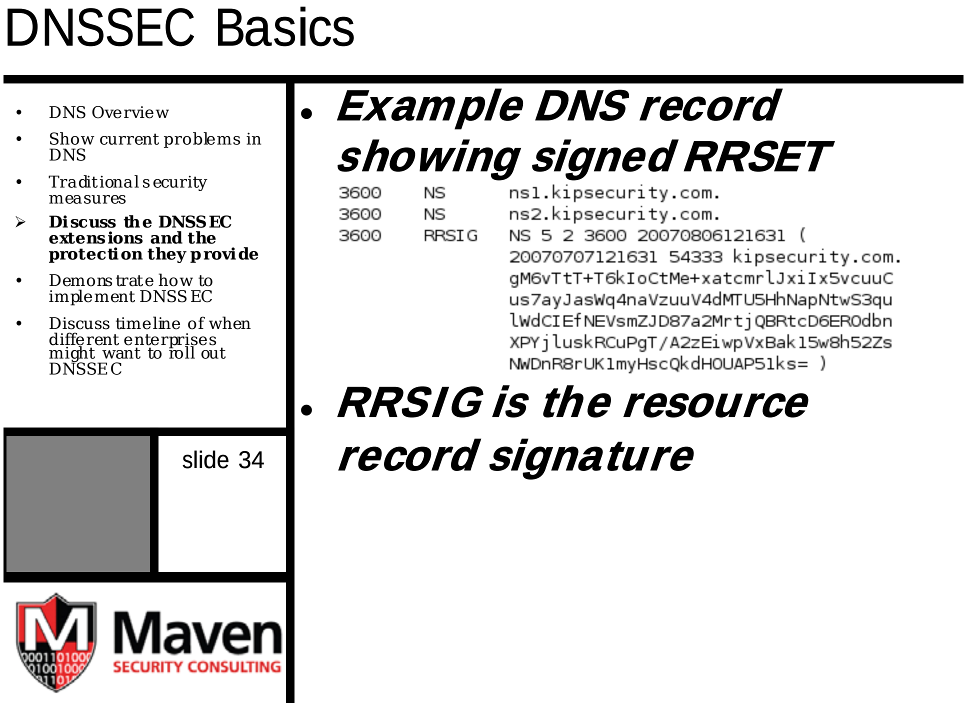
- DNS Overview
- Show current problems in DNS
- Traditional security measures
- **Discuss the DNSSEC extensions and the protection they provide**
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 33

- ***DNSKEY record***
- ***Flags***
- ***Protocol***
- ***Algorithm***

```
3600    DNSKEY 256 3 5 (
        AwEAAQ3TEDguQ9/tbnbuIgoSxbWoDYZ63JzB
        dOlFcthSSYxD7Xe+q1WUD8MJIgcOEJG6uo4E
        3/13Htpkf7Dvmy0V12l6KSok7/YJWDlEbk9z
        sblMoiGeiHIGdC/KqDHnvyM9/9GPuPv3mTvb
        lPvm/gRnRUDqV96/nPYpoTaya0NCfGkXty3/
        3kTq3Qw06p4WzspvF4pe2LmIoOye7+Cf30ZG
        6i92wus=
        ) ; key id = 24327
```

- ***Public Key***



DNSSEC Basics

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- **Discuss the DNSSEC extensions and the protection they provide**
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 34

- ***Example DNS record showing signed RRSET***

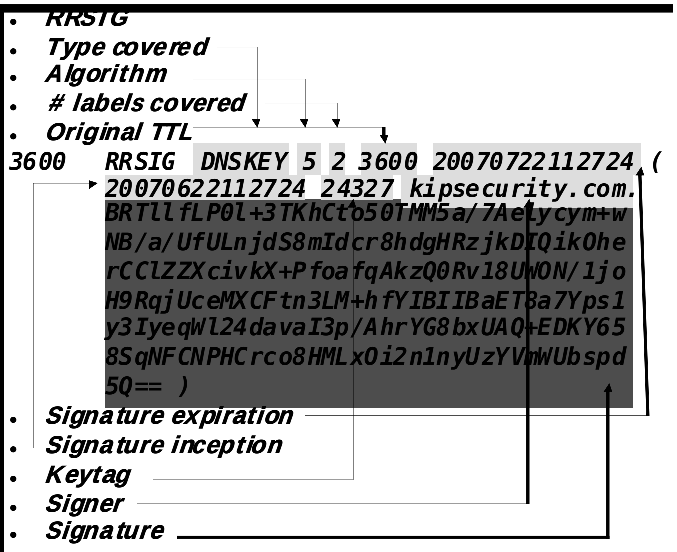
```
3600    NS      ns1.kipsecurity.com.
3600    NS      ns2.kipsecurity.com.
3600    RRSIG   NS 5 2 3600 20070806121631 (
                20070707121631 54333 kipsecurity.com.
                gM6vTtT+T6kIoCtMe+xatcmrlJxiIx5vcuuC
                us7ayJasWq4naVzuuV4dMTU5HhNapNtwS3qu
                lWdCIEfNEVsmZJD87a2MrtjQBRtcD6ER0dbn
                XPYjluskRCuPgT/A2zEiwpVxBak15w8h52Zs
                NWDnR8rUK1myHscQkdHOUAP51ks= )
```

- ***RRSIG is the resource record signature***

DNSSEC Basics - RRSIG

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- ➢ **Discuss the DNSSEC extensions and the protection they provide**
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 35



- ***RRSIG***
- ***Type covered***
- ***Algorithm***
- ***# labels covered***
- ***Original TTL***

```
3600   RRSIG  DNSKEY 5 2 3600 20070722112724 (
              20070622112724 24327 kipsecurity.com.
              BRTllfLP0l+3TKhCto50TMM5a/7Aelycym+w
              NB/a/UfULnjdS8mIdcr8hdgHRzjkDIQikOhe
              rCClZZXcivkX+PfoafqAkzQ0Rv18UWON/1jo
              H9RqjUceMXCFtn3LM+hfYIBIIBaET8a7Yps1
              y3IyeqWl24davaI3p/AhrYG8bxUAQ+EDKY65
              8SqNFCNPHCrco8HMLxOi2n1nyUzYVmWUbspd
              5Q== )
```

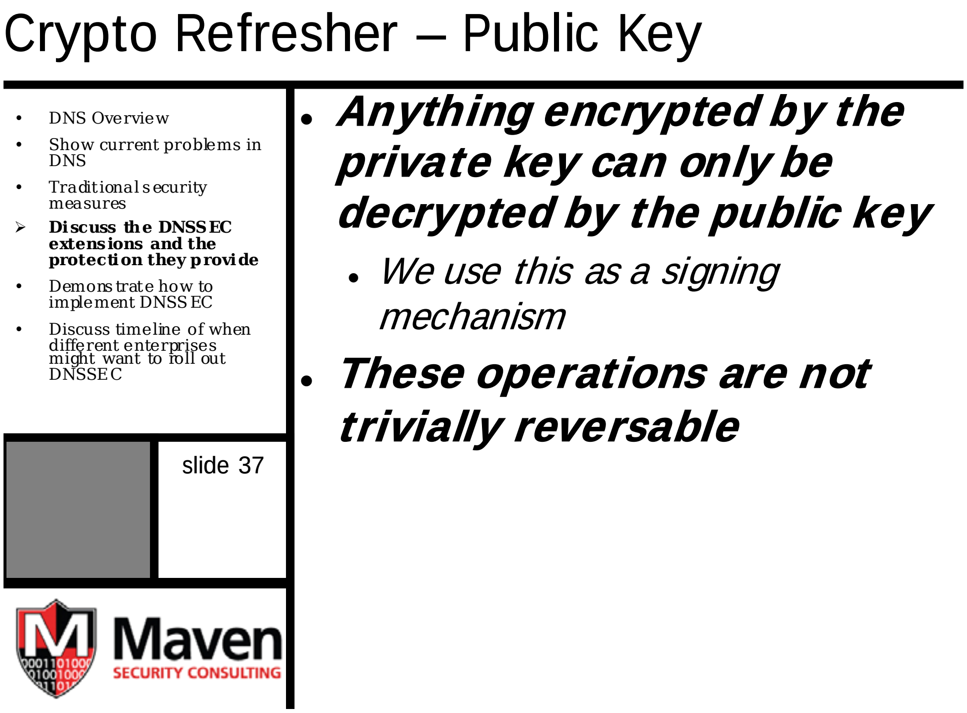
- ***Signature expiration***
- ***Signature inception***
- ***Keytag***
- ***Signer***
- ***Signature***

Cryptographic Refresher

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- ➢ **Discuss the DNSSEC extensions and the protection they provide**
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 36

- ***DNSSEC uses public key cryptography and cryptographic hashes***
- ***Public Key crypto is named for one half of its key, the public key***
- ***Anything encrypted with the public key can only be decrypted with the secret key***

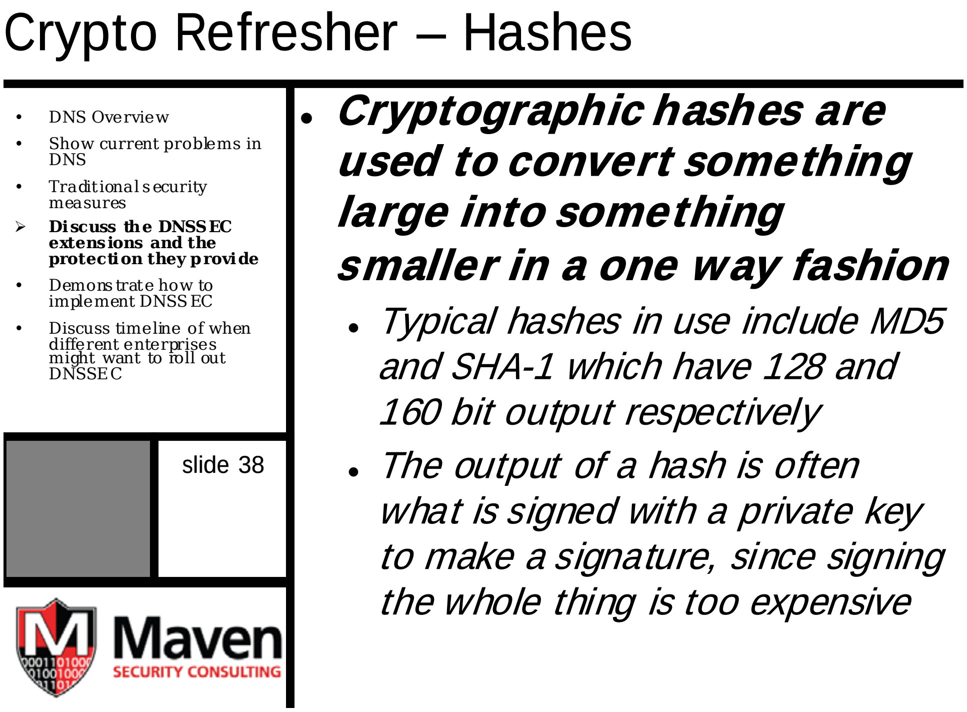


Crypto Refresher – Public Key

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- ➢ **Discuss the DNSSEC extensions and the protection they provide**
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 37

- ***Anything encrypted by the private key can only be decrypted by the public key***
  - *We use this as a signing mechanism*
- ***These operations are not trivially reversable***

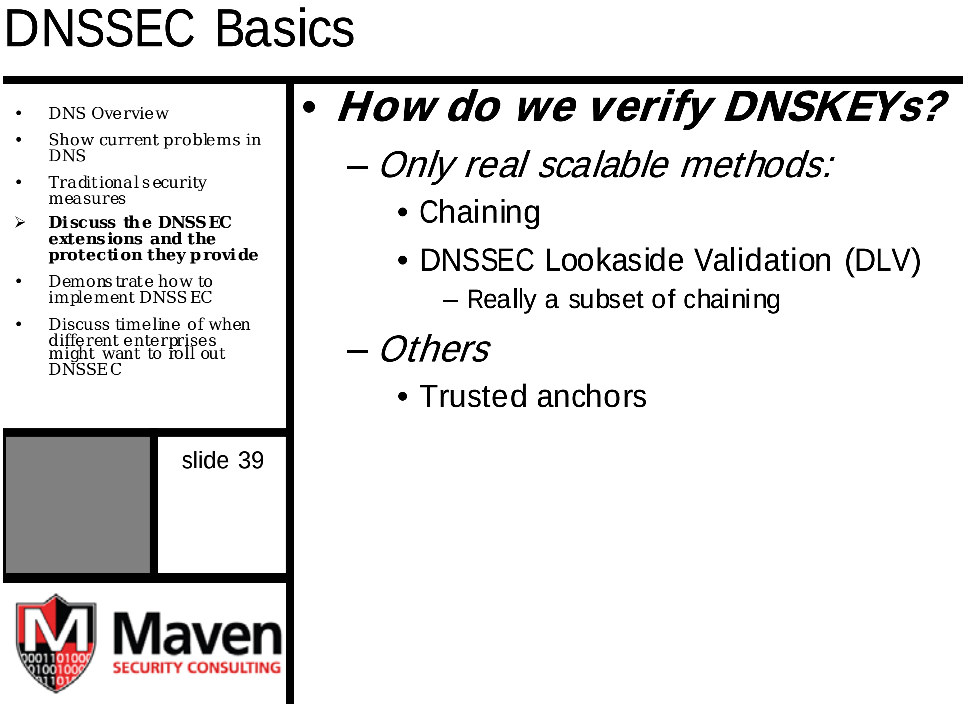


Crypto Refresher – Hashes

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- ➢ **Discuss the DNSSEC extensions and the protection they provide**
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 38

- ***Cryptographic hashes are used to convert something large into something smaller in a one way fashion***
  - *Typical hashes in use include MD5 and SHA-1 which have 128 and 160 bit output respectively*
  - *The output of a hash is often what is signed with a private key to make a signature, since signing the whole thing is too expensive*



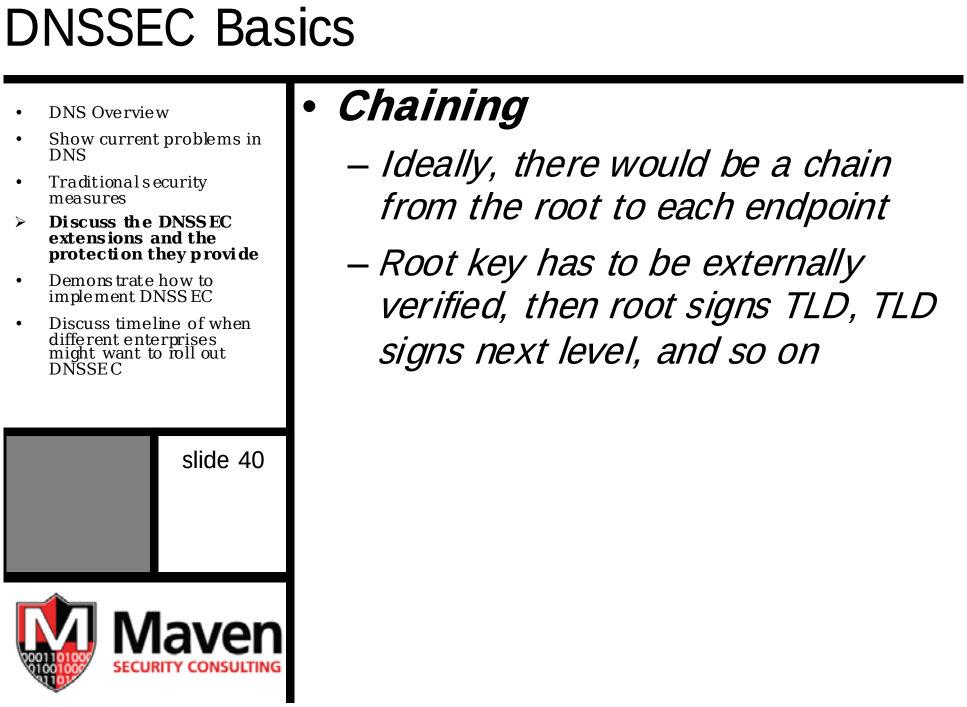
DNSSEC Basics

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- ➢ **Discuss the DNSSEC extensions and the protection they provide**
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 39

Maven SECURITY CONSULTING

- ***How do we verify DNSKEYs?***
  - *Only real scalable methods:*
    - Chaining
    - DNSSEC Lookaside Validation (DLV)
      - Really a subset of chaining
  - *Others*
    - Trusted anchors



DNSSEC Basics

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- ➢ **Discuss the DNSSEC extensions and the protection they provide**
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 40

Maven SECURITY CONSULTING

- ***Chaining***
  - *Ideally, there would be a chain from the root to each endpoint*
  - *Root key has to be externally verified, then root signs TLD, TLD signs next level, and so on*

DNSSEC Basics

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- **Discuss the DNSSEC extensions and the protection they provide**
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

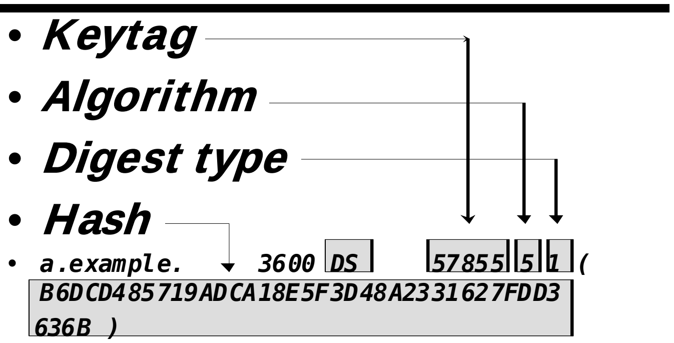
slide 41

- ***DS (Delegation Signer) resource record holds this signature***
- ***Contains a keytag, algorithm, digest type, and hash***
- `a.example.      3600 DS      57855 5 1 ( B6DCD485719ADCA18E5F3D48A2331627FDD3 636B )`

DNSSEC Basics

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- **Discuss the DNSSEC extensions and the protection they provide**
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 42



- ***Keytag***
- ***Algorithm***
- ***Digest type***
- ***Hash***
- `a.example.      3600 DS      57855 5 1 ( B6DCD485719ADCA18E5F3D48A2331627FDD3 636B )`

- ***Signed by the owners key to make signed RRSIG***

DNSSEC Basics

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- **Discuss the DNSSEC extensions and the protection they provide**
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 43

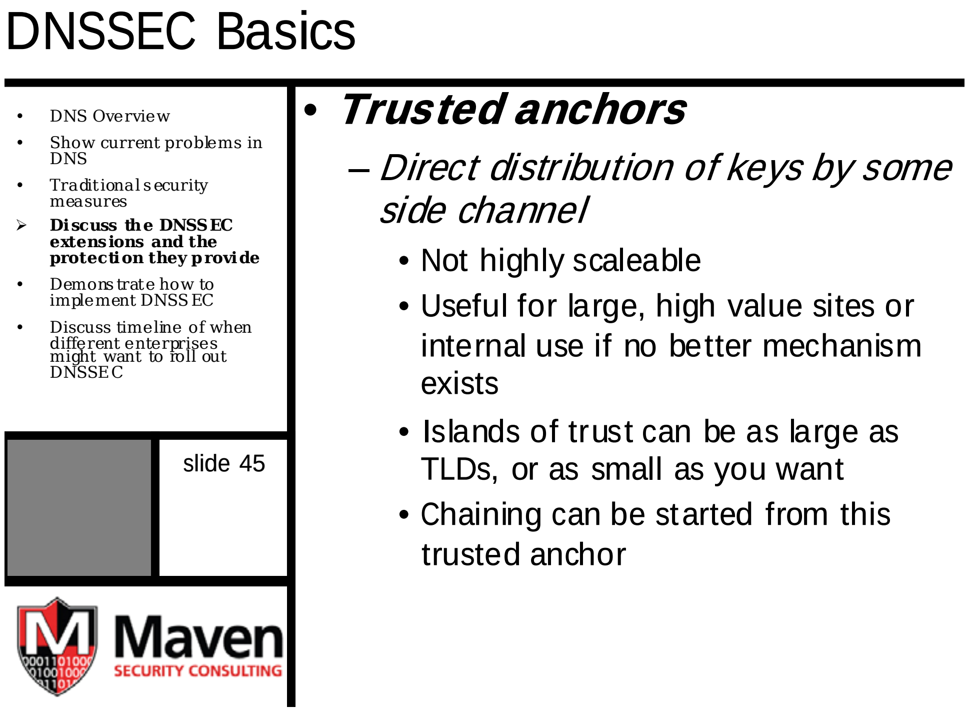
- ***This signing makes a chain from one server to it’s child whereby you can verify the DNSKEY of the child***
  - *Hashing is used for size*
- ***Can be initiated anywhere, at Root, TLD, or lower***
  - *The higher the signing starts, the more scalable it is*
    - Root and US TLD’s not signed yet

DNSSEC Basics

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- **Discuss the DNSSEC extensions and the protection they provide**
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 44

- ***DNSSEC Lookaside Validation***
  - *Allows delegation of authority to non-children*
    - Example: .com TLD not signed, but example.com provides signing service for hire
  - *Brings most of the benefits of chaining, bypassing the political problems of signing the root*



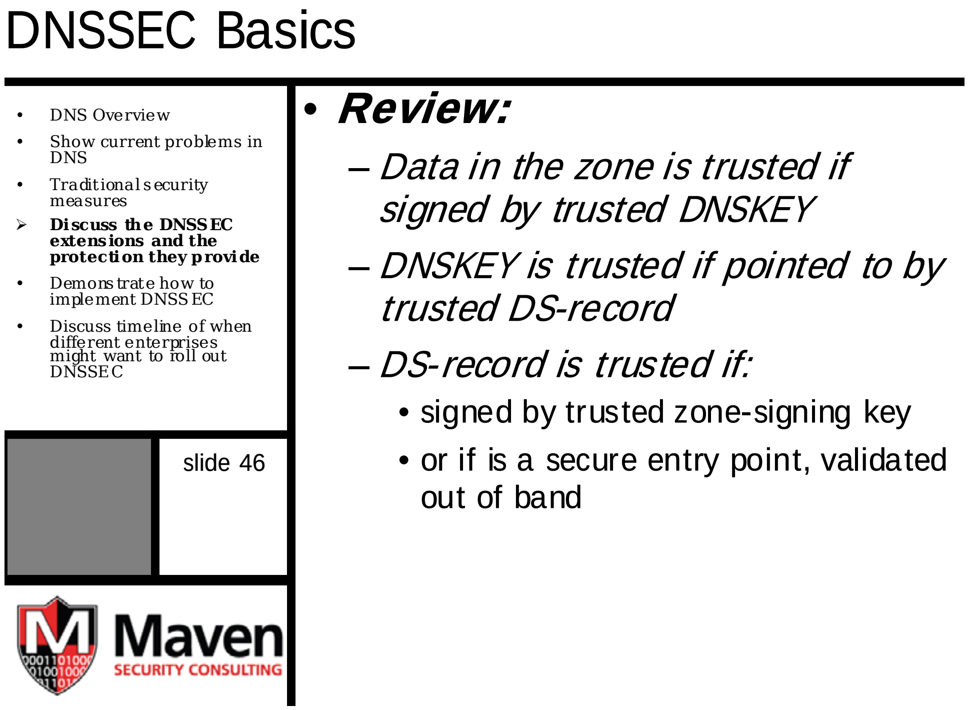
DNSSEC Basics

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- ➢ **Discuss the DNSSEC extensions and the protection they provide**
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 45

Maven SECURITY CONSULTING

- ***Trusted anchors***
  - *Direct distribution of keys by some side channel*
    - Not highly scaleable
    - Useful for large, high value sites or internal use if no better mechanism exists
    - Islands of trust can be as large as TLDs, or as small as you want
    - Chaining can be started from this trusted anchor



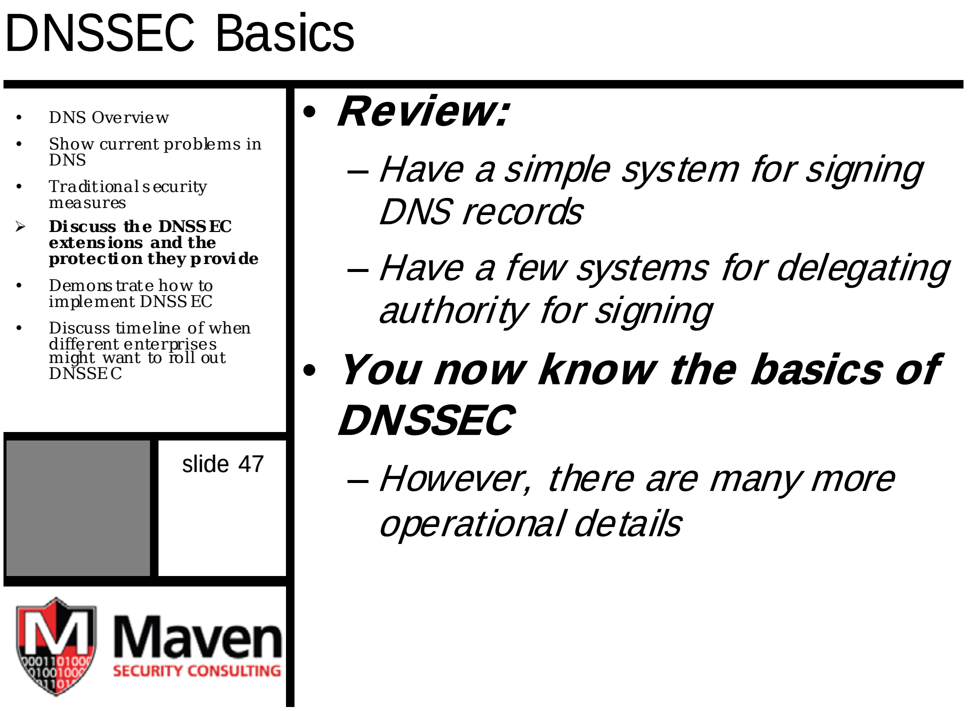
DNSSEC Basics

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- ➢ **Discuss the DNSSEC extensions and the protection they provide**
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 46

Maven SECURITY CONSULTING

- ***Review:***
  - *Data in the zone is trusted if signed by trusted DNSKEY*
  - *DNSKEY is trusted if pointed to by trusted DS-record*
  - *DS-record is trusted if:*
    - signed by trusted zone-signing key
    - or if is a secure entry point, validated out of band

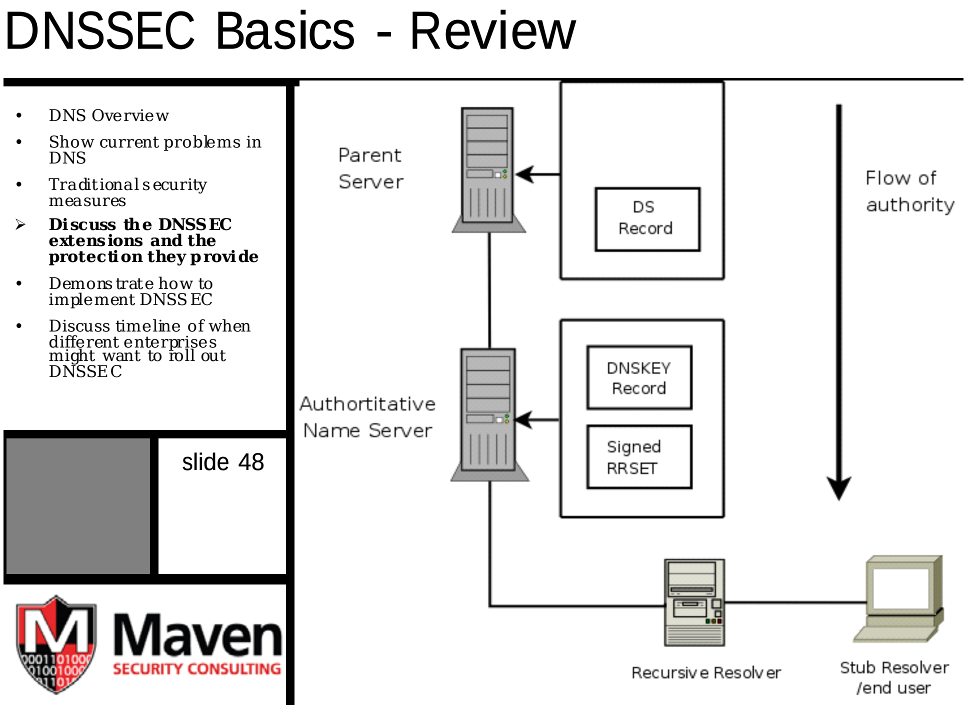


DNSSEC Basics

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- ➢ **Discuss the DNSSEC extensions and the protection they provide**
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 47

- ***Review:***
  - *Have a simple system for signing DNS records*
  - *Have a few systems for delegating authority for signing*
- ***You now know the basics of DNSSEC***
  - *However, there are many more operational details*



DNSSEC Basics - Review

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- ➢ **Discuss the DNSSEC extensions and the protection they provide**
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 48

RRSet vs RRset: http://mail.shinkuro.com:8100/lists/dnssec-deployment/Message/781.html?Language=

Signing system

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- ➢ **Demonstrate how to implement DNSSEC**
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 49

- ***DNSKEYs are optionally segmented into 2 types:***
  - – *Key Signing Keys (KSKs), used to sign subkeys*
  - – *Zone Signing Keys (ZSKs), used to sign RRsets*
- ***Differentiated by the Secure Entry Point flag***
  - – *According to the specs, this is advisory only, and can't effect the working of the software*

Signing system

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- ➢ **Demonstrate how to implement DNSSEC**
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 50

- ***Benefits of segmenting the keys:***
  - – *No upstream action required when ZSKs are changed*
  - – *KSKs can be stronger, and have a longer usage lifetime*

Signing system

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- ➢ **Demonstrate how to implement DNSSEC**
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 51

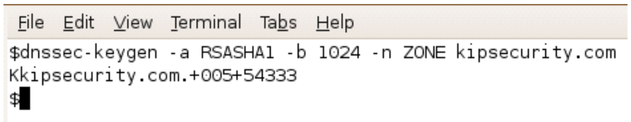
- ***Key lifetimes***
  - *Different records require different lengths*
    - Most problematic – DS records and KSKs
      - Suggest SHA-256 for DS records if possible
        - » ***Standards recommend using both SHA-1 and SHA-256 for compatibility***
      - Assuming 1 year of use, suggest at least 2048 for KSK
      - Might be limited by SHA-1 strength, to approx. 1300 – true strength of SHA-1 unknown
    - ZSK
      - Length dependant on lifetime
      - Suggest 1024 at minimum, from 1300 to 2048 for mid to high value domains
    - Keylength.com a good resource

Signing system

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- ➢ **Demonstrate how to implement DNSSEC**
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 52

- ***Generating keys***
  - *BIND*
    - dnssec-keygen -a alg -b bits -n type [-f KSK] [options] name



```
$dnssec-keygen -a RSASHA1 -b 1024 -n ZONE kipsecurity.com
Kkipsecurity.com.+005+54333
$
```

- Uses /dev/random on unix computers, can easily deplete the randomness pool with even one key

Signing system

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- ➢ **Demonstrate how to implement DNSSEC**
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 53

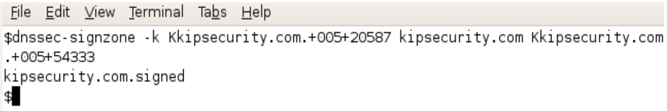
- ***Generating keys***
  - *If using Bind < 9.3, dnssec-keygen needs –e flag to generate strong RSA keys*
  - *If demos are given, I will be using –r /dev/urandom for times sake, recommend hardware randomness generator for production use*
    - Included in many recent motherboards, see linux Documentaion/hw_random.txt for linux info, supported by other unixes also

Signing system

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- ➢ **Demonstrate how to implement DNSSEC**
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 54

- ***Signing zones***
  - *BIND*
    - dnssec-signzone [–o zone] [–k KSK] [-s start-time] [-e endtime] zonefile [ZSK]
      - By default, starttime is -1 hour, endtime is 30 days
    - dnssec-signzone kipsecurity.com



```
$dnssec-signzone -k Kkipsecurity.com.+005+20587 kipsecurity.com Kkipsecurity.com
.+005+54333
kipsecurity.com.signed
$
```

Signing system

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- ➢ **Demonstrate how to implement DNSSEC**
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 55

Maven SECURITY CONSULTING

- ***Key rollover is one of the largest problems in DNSSEC***
  - *Need to avoid breaking chain of trust*
- ***2 main strategies***
  - *Pre-publish*
  - *Double sign*

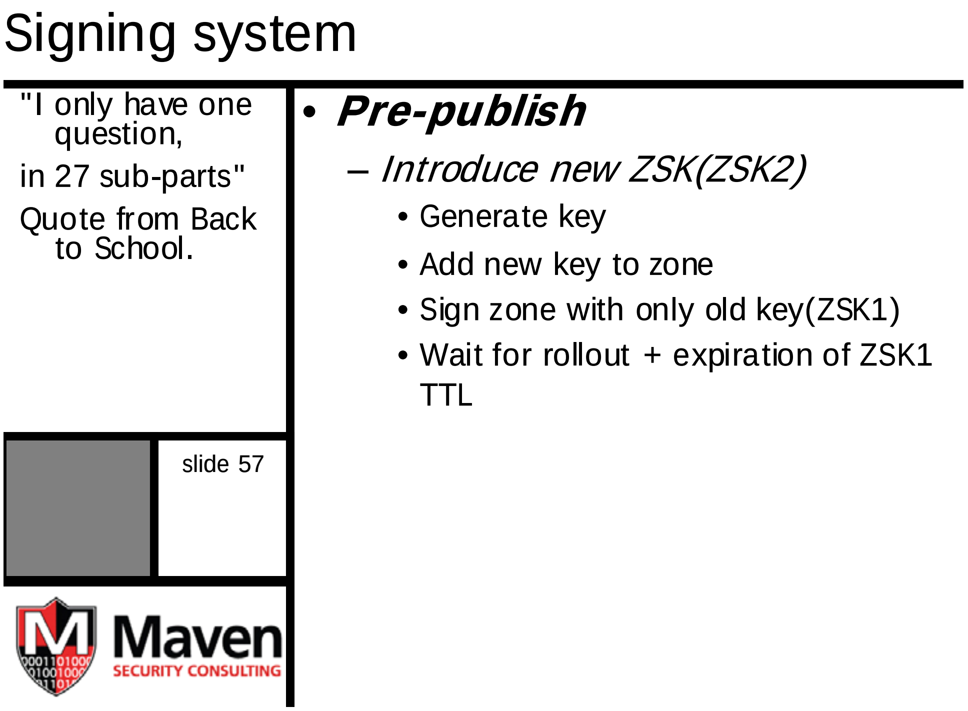
Signing system

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- ➢ **Demonstrate how to implement DNSSEC**
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 56

Maven SECURITY CONSULTING

- ***Pre-publish***
  - *3 step process (overview)*
    - Introduce new ZSK(ZSK2)
      - Wait for rollout + expiration of ZSK1 TTL
    - Sign RR with ZSK2
      - Wait for expiration of longest TTL in zone
    - Remove ZSK1
      - Optionally introduce new ZSK3 at this step to minimize future waiting



Signing system

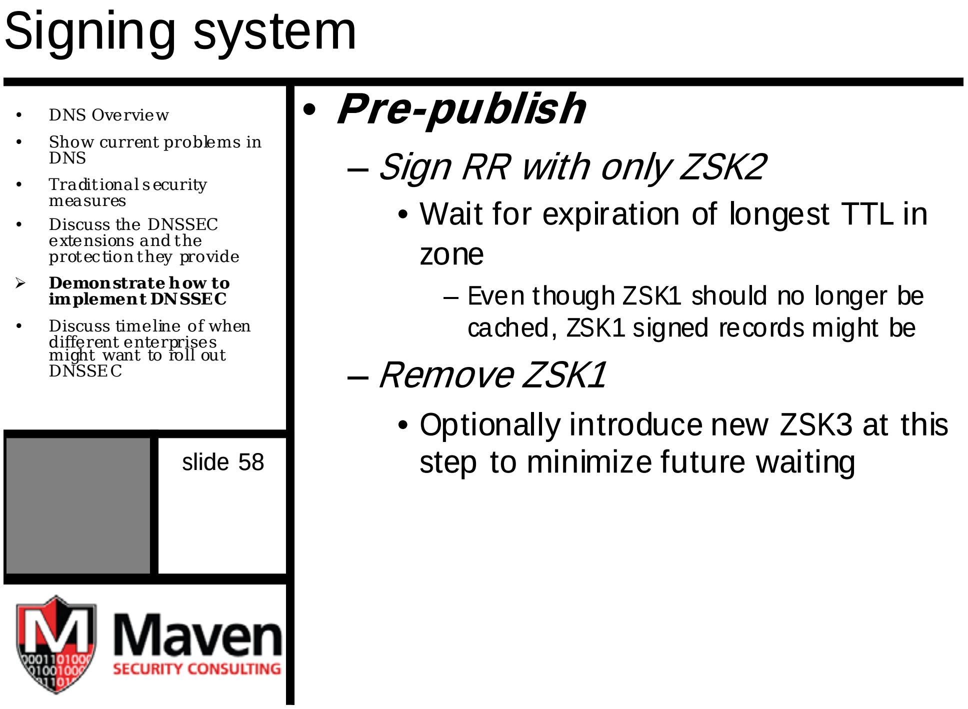
"I only have one question,

in 27 sub-parts"

Quote from Back to School.

- ***Pre-publish***
  - *Introduce new ZSK(ZSK2)*
    - Generate key
    - Add new key to zone
    - Sign zone with only old key(ZSK1)
    - Wait for rollout + expiration of ZSK1 TTL

slide 57

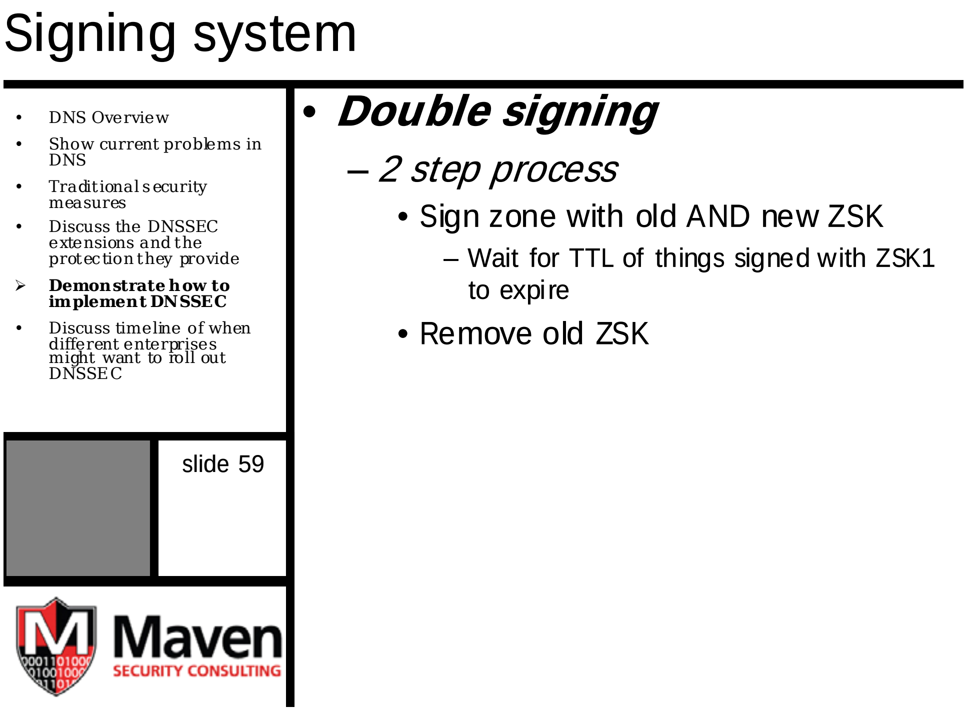


Signing system

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- ➢ **Demonstrate how to implement DNSSEC**
- Discuss timeline of when different enterprises might want to roll out DNSSEC

- ***Pre-publish***
  - *Sign RR with only ZSK2*
    - Wait for expiration of longest TTL in zone
      - Even though ZSK1 should no longer be cached, ZSK1 signed records might be
  - *Remove ZSK1*
    - Optionally introduce new ZSK3 at this step to minimize future waiting

slide 58

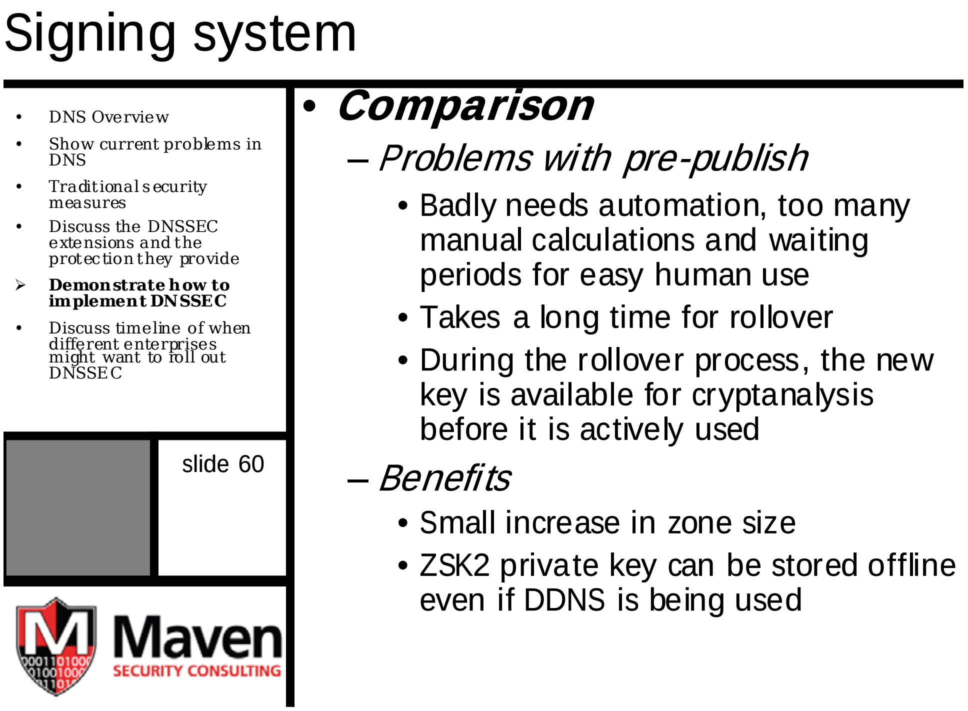


Signing system

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- **Demonstrate how to implement DNSSEC**
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 59

- ***Double signing***
  - *2 step process*
    - Sign zone with old AND new ZSK
      - Wait for TTL of things signed with ZSK1 to expire
    - Remove old ZSK

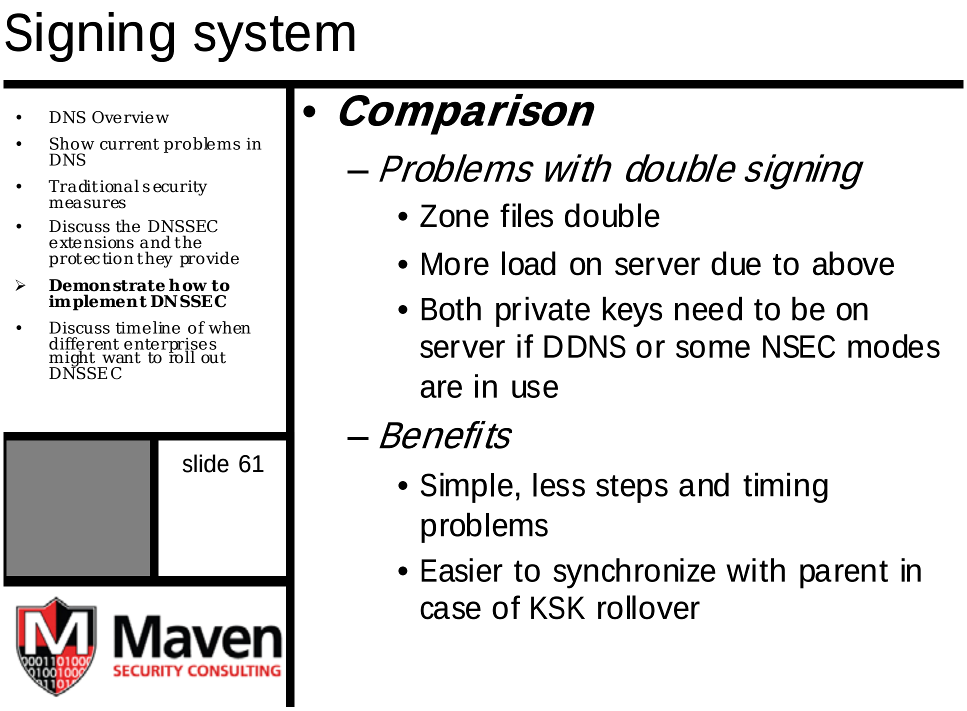


Signing system

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- **Demonstrate how to implement DNSSEC**
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 60

- ***Comparison***
  - *Problems with pre-publish*
    - Badly needs automation, too many manual calculations and waiting periods for easy human use
    - Takes a long time for rollover
    - During the rollover process, the new key is available for cryptanalysis before it is actively used
  - *Benefits*
    - Small increase in zone size
    - ZSK2 private key can be stored offline even if DDNS is being used

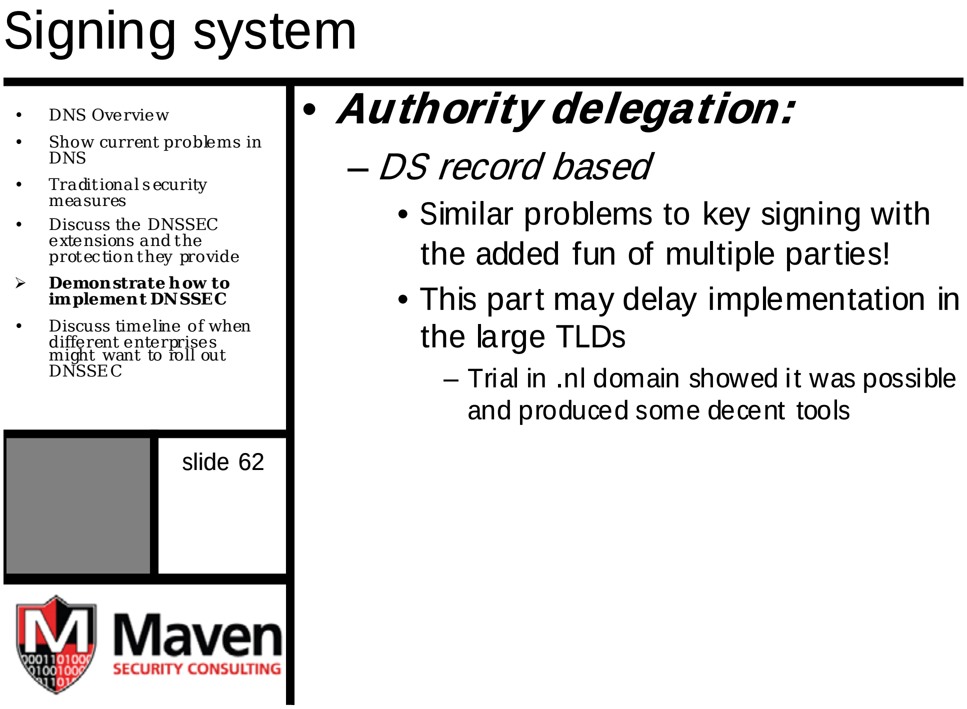


Signing system

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- ➢ **Demonstrate how to implement DNSSEC**
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 61

- ***Comparison***
  - *Problems with double signing*
    - Zone files double
    - More load on server due to above
    - Both private keys need to be on server if DDNS or some NSEC modes are in use
  - *Benefits*
    - Simple, less steps and timing problems
    - Easier to synchronize with parent in case of KSK rollover



Signing system

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- ➢ **Demonstrate how to implement DNSSEC**
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 62

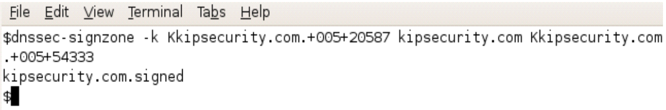
- ***Authority delegation:***
  - *DS record based*
    - Similar problems to key signing with the added fun of multiple parties!
    - This part may delay implementation in the large TLDs
      - Trial in .nl domain showed it was possible and produced some decent tools

Signing system

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- ➢ **Demonstrate how to implement DNSSEC**
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 63

- ***Authority delegation:***
  - – *Basic tools we have already used:*
    - dnssec-signzone creates DS records for us in the dsset-(zone name) file with the –g flag (on by default)



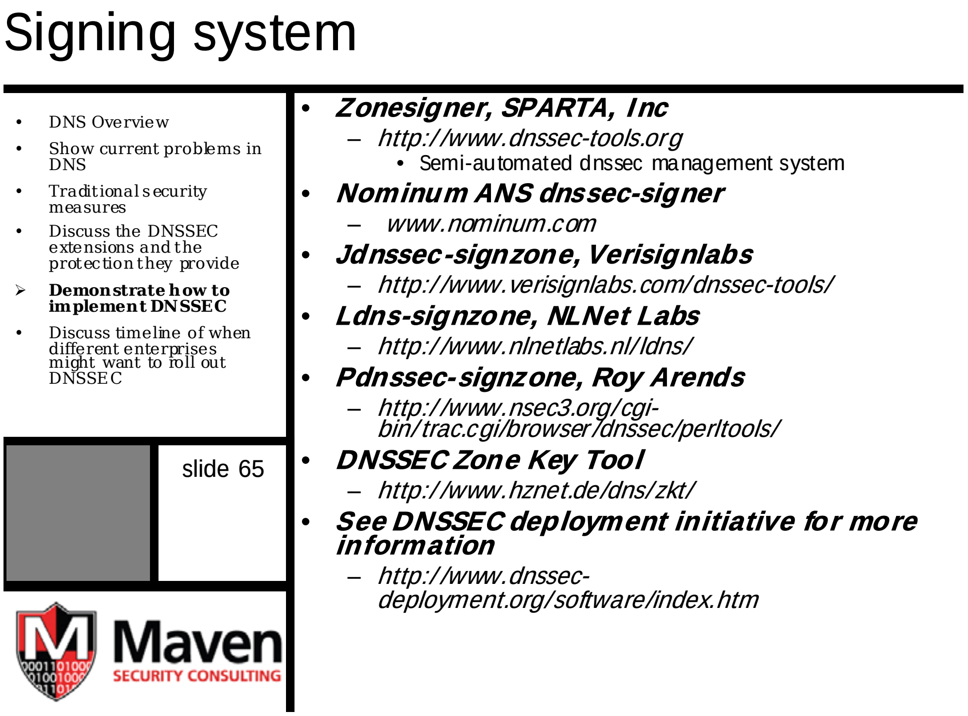
```
$dnssec-signzone -k Kkipsecurity.com.+005+20587 kipsecurity.com Kkipsecurity.com
.+005+54333
kipsecurity.com.signed
$
```

Signing system

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- ➢ **Demonstrate how to implement DNSSEC**
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 64

- ***DS/KSK rollovers***
  - – *Double signing mode recommended, only one DS record must be doubled on the parent*
  - – *2 steps*
    - Parent adds new DS key, replacing ZSK0
    - Child replaces KSK0 with KSK2, signs records with KSK1 ,KSK2
      - – Must wait for max TTL until next rollover



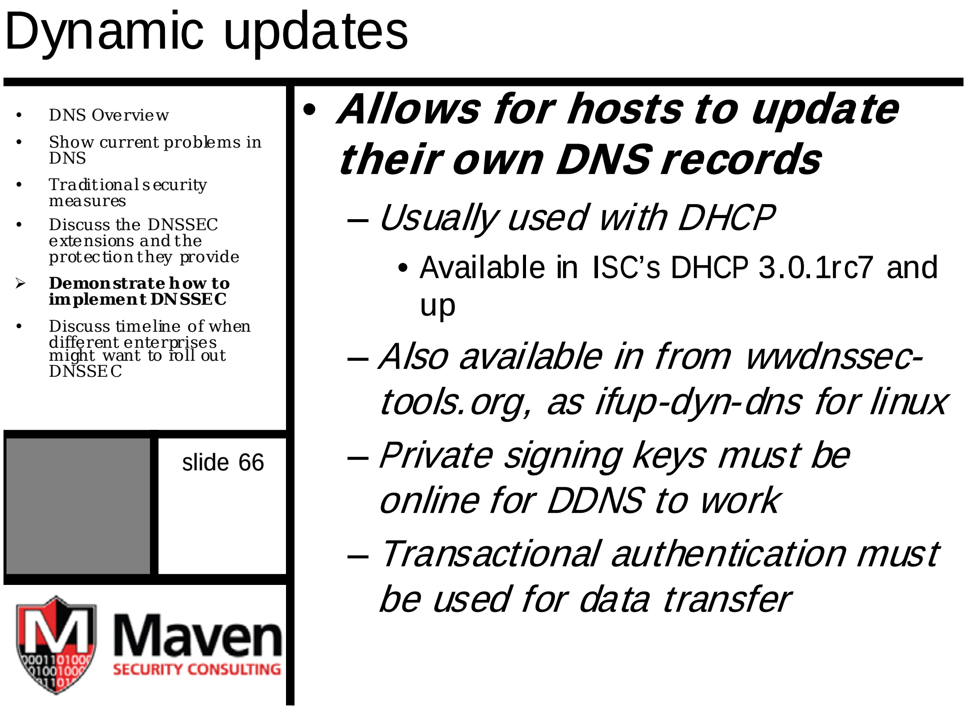
Signing system

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- **Demonstrate how to implement DNSSEC**
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 65

- ***Zonesigner, SPARTA, Inc***
  - *http://www.dnssec-tools.org*
    - Semi-automated dnssec management system
- ***Nominum ANS dnssec-signer***
  - *www.nominum.com*
- ***Jdnssec-signzone, Verisignlabs***
  - *http://www.verisignlabs.com/dnssec-tools/*
- ***Ldns-signzone, NLNet Labs***
  - *http://www.nlnetlabs.nl/ldns/*
- ***Pdnssec-signzone, Roy Arends***
  - *http://www.nsec3.org/cgi-bin/trac.cgi/browser/dnssec/perltools/*
- ***DNSSEC Zone Key Tool***
  - *http://www.hznet.de/dns/zkt/*
- ***See DNSSEC deployment initiative for more information***
  - *http://www.dnssec-deployment.org/software/index.htm*

Maven SECURITY CONSULTING



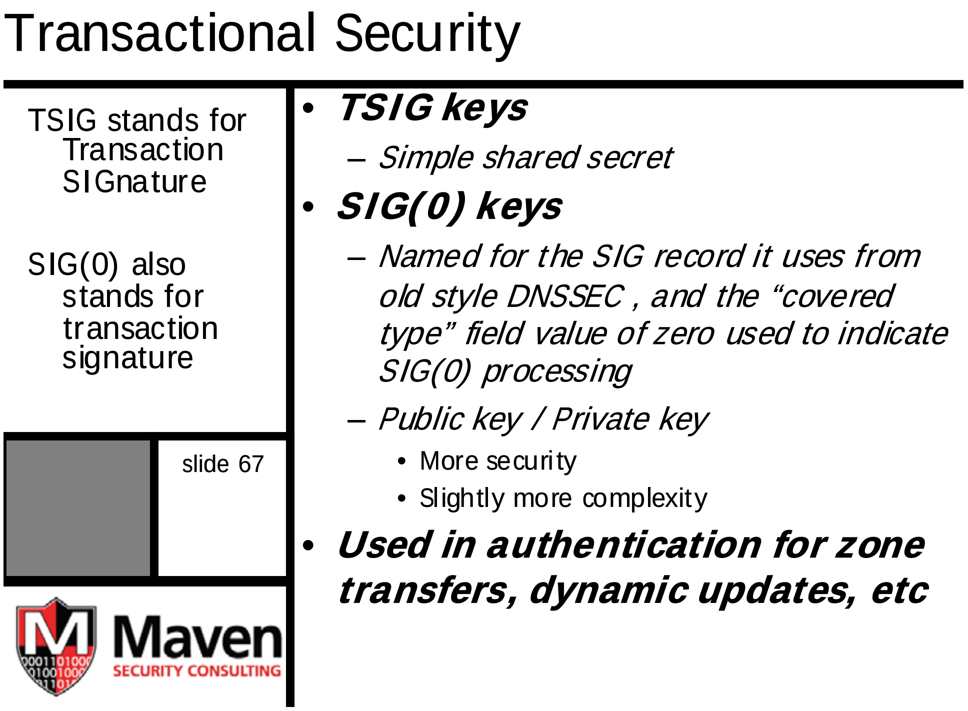
Dynamic updates

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- **Demonstrate how to implement DNSSEC**
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 66

- ***Allows for hosts to update their own DNS records***
  - *Usually used with DHCP*
    - Available in ISC's DHCP 3.0.1rc7 and up
  - *Also available in from wwdnssec-tools.org, as ifup-dyn-dns for linux*
  - *Private signing keys must be online for DDNS to work*
  - *Transactional authentication must be used for data transfer*

Maven SECURITY CONSULTING



Transactional Security

TSIG stands for Transaction SIGnature

SIG(0) also stands for transaction signature

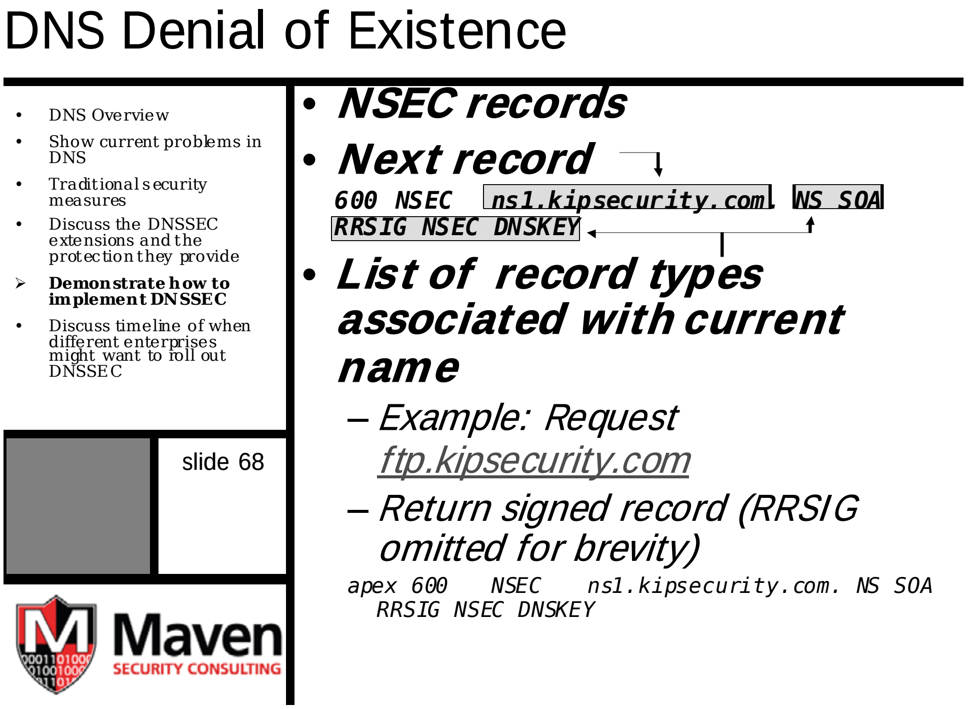
slide 67

- ***TSIG keys***
  - *Simple shared secret*
- ***SIG(0) keys***
  - *Named for the SIG record it uses from old style DNSSEC , and the "covered type" field value of zero used to indicate SIG(0) processing*
  - *Public key / Private key*
    - More security
    - Slightly more complexity
- ***Used in authentication for zone transfers, dynamic updates, etc***

"Secret Key Transaction Authentication for DNS (TSIG)", http://tools.ietf.org/html/rfc2845

Updated by http://tools.ietf.org/html/rfc3645, adding more flexability

"DNS Request and Transaction Signatures (SIG(0)s)",http://www.ietf.org/rfc/rfc2931.txt



DNS Denial of Existence

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- ➢ **Demonstrate how to implement DNSSEC**
- Discuss timeline of when different enterprises might want to roll out DNSSEC

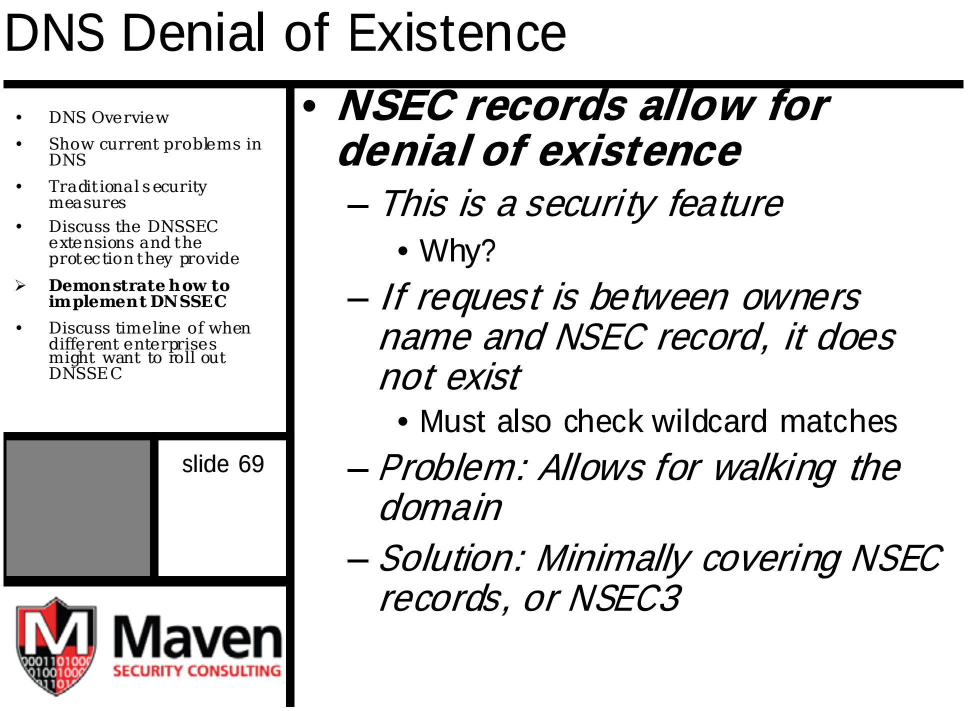
slide 68

- ***NSEC records***
- ***Next record***

```
600 NSEC  nsl.kipsecurity.com  NS SOA
RRSIG NSEC DNSKEY
```

- ***List of record types associated with current name***
  - *Example: Request ftp.kipsecurity.com*
  - *Return signed record (RRSIG omitted for brevity)*

```
apex 600   NSEC    ns1.kipsecurity.com. NS SOA
   RRSIG NSEC DNSKEY
```

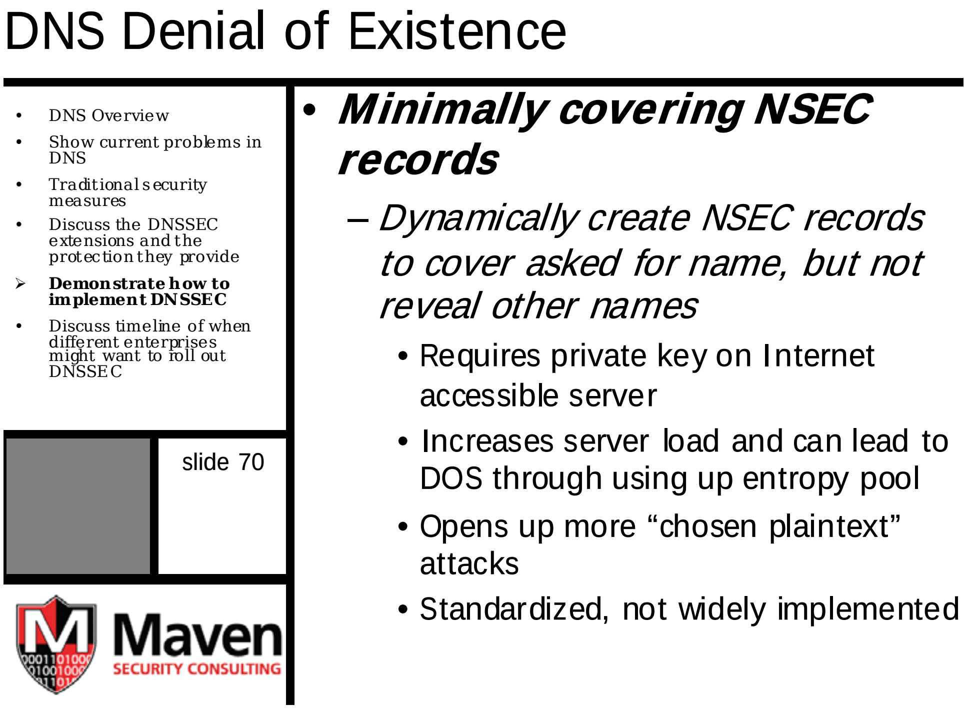


DNS Denial of Existence

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- **Demonstrate how to implement DNSSEC**
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 69

- ***NSEC records allow for denial of existence***
  - *This is a security feature*
    - Why?
  - *If request is between owners name and NSEC record, it does not exist*
    - Must also check wildcard matches
  - *Problem: Allows for walking the domain*
  - *Solution: Minimally covering NSEC records, or NSEC3*

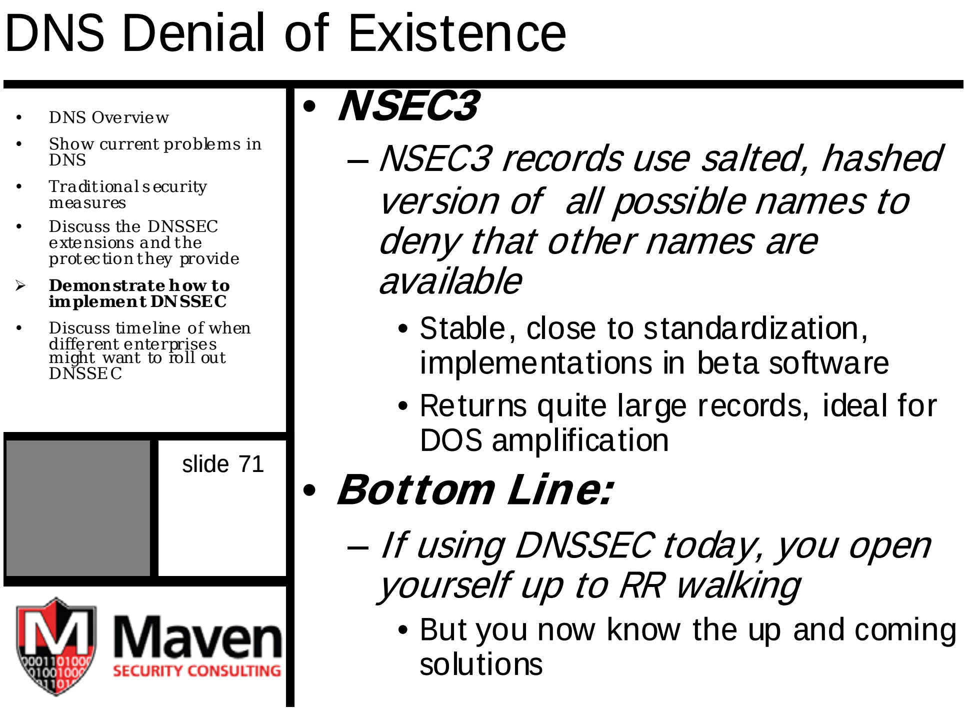


DNS Denial of Existence

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- **Demonstrate how to implement DNSSEC**
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 70

- ***Minimally covering NSEC records***
  - *Dynamically create NSEC records to cover asked for name, but not reveal other names*
    - Requires private key on Internet accessible server
    - Increases server load and can lead to DOS through using up entropy pool
    - Opens up more “chosen plaintext” attacks
    - Standardized, not widely implemented



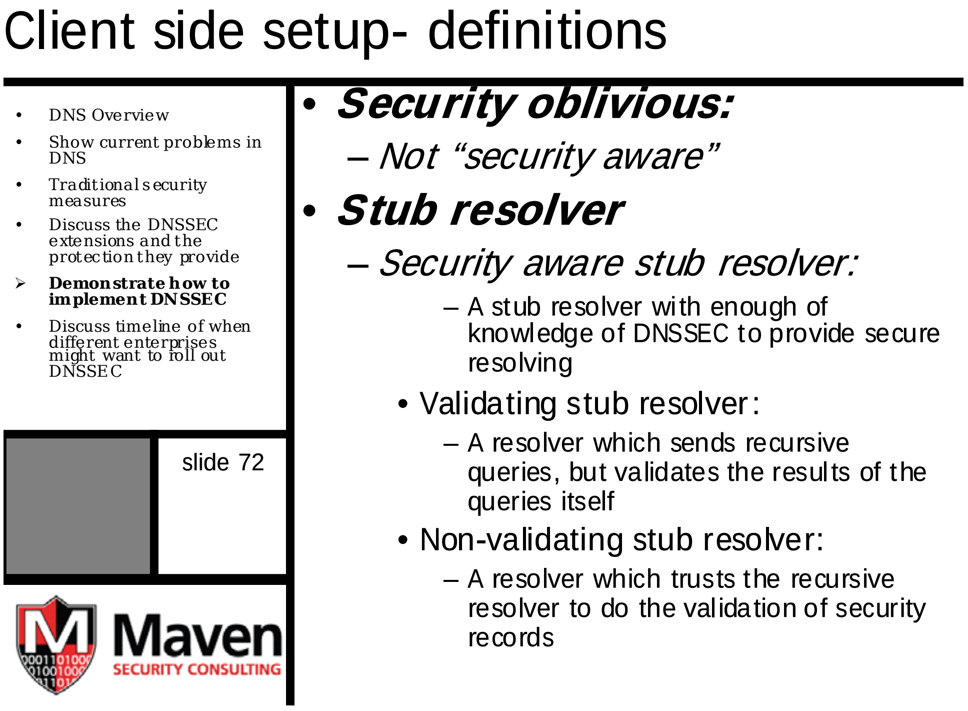
DNS Denial of Existence

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- **Demonstrate how to implement DNSSEC**
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 71

Maven SECURITY CONSULTING

- ***NSEC3***
  - *NSEC3 records use salted, hashed version of all possible names to deny that other names are available*
    - Stable, close to standardization, implementations in beta software
    - Returns quite large records, ideal for DOS amplification
- ***Bottom Line:***
  - *If using DNSSEC today, you open yourself up to RR walking*
    - But you now know the up and coming solutions



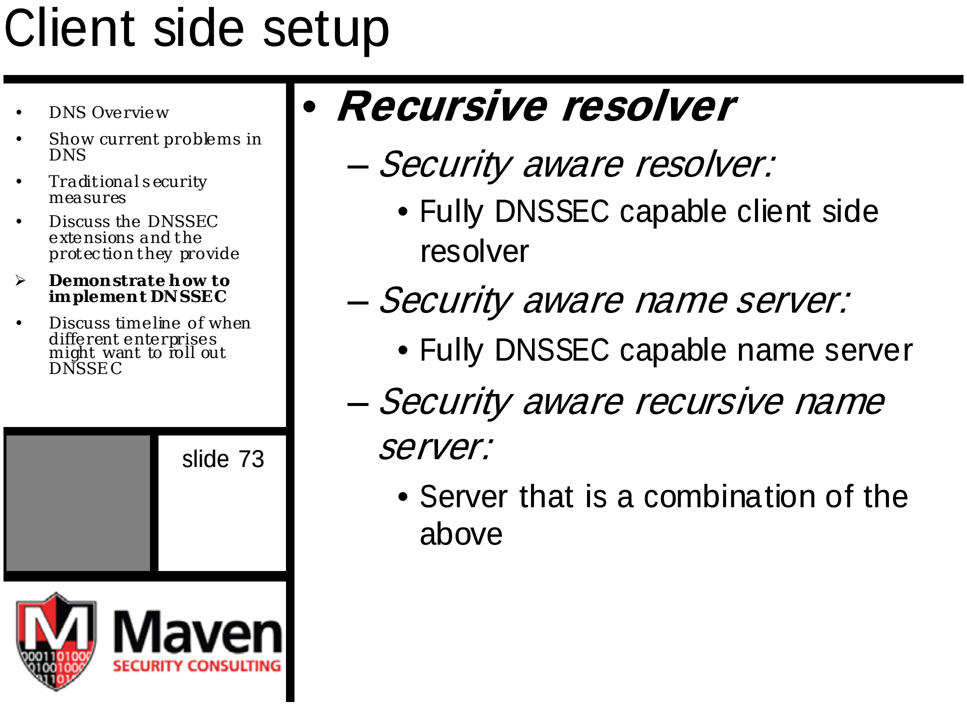
Client side setup- definitions

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- **Demonstrate how to implement DNSSEC**
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 72

Maven SECURITY CONSULTING

- ***Security oblivious:***
  - *Not "security aware"*
- ***Stub resolver***
  - *Security aware stub resolver:*
      - A stub resolver with enough of knowledge of DNSSEC to provide secure resolving
    - Validating stub resolver:
      - A resolver which sends recursive queries, but validates the results of the queries itself
    - Non-validating stub resolver:
      - A resolver which trusts the recursive resolver to do the validation of security records



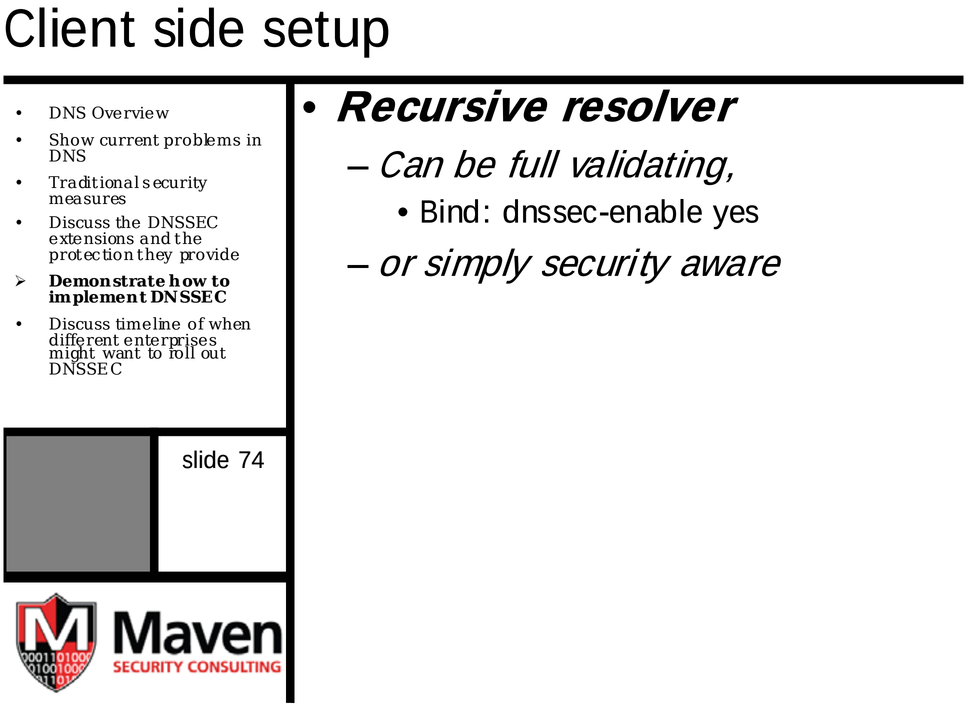
Client side setup

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- **Demonstrate how to implement DNSSEC**
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 73

Maven SECURITY CONSULTING

- ***Recursive resolver***
  - *Security aware resolver:*
    - Fully DNSSEC capable client side resolver
  - *Security aware name server:*
    - Fully DNSSEC capable name server
  - *Security aware recursive name server:*
    - Server that is a combination of the above



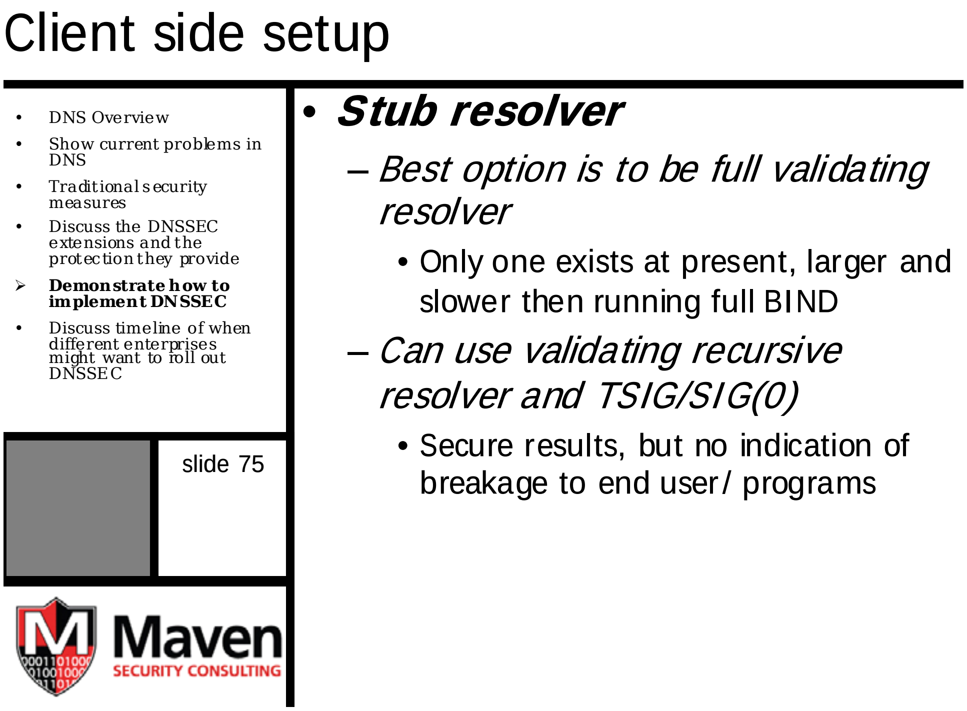
Client side setup

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- **Demonstrate how to implement DNSSEC**
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 74

Maven SECURITY CONSULTING

- ***Recursive resolver***
  - *Can be full validating,*
    - Bind: dnssec-enable yes
  - *or simply security aware*



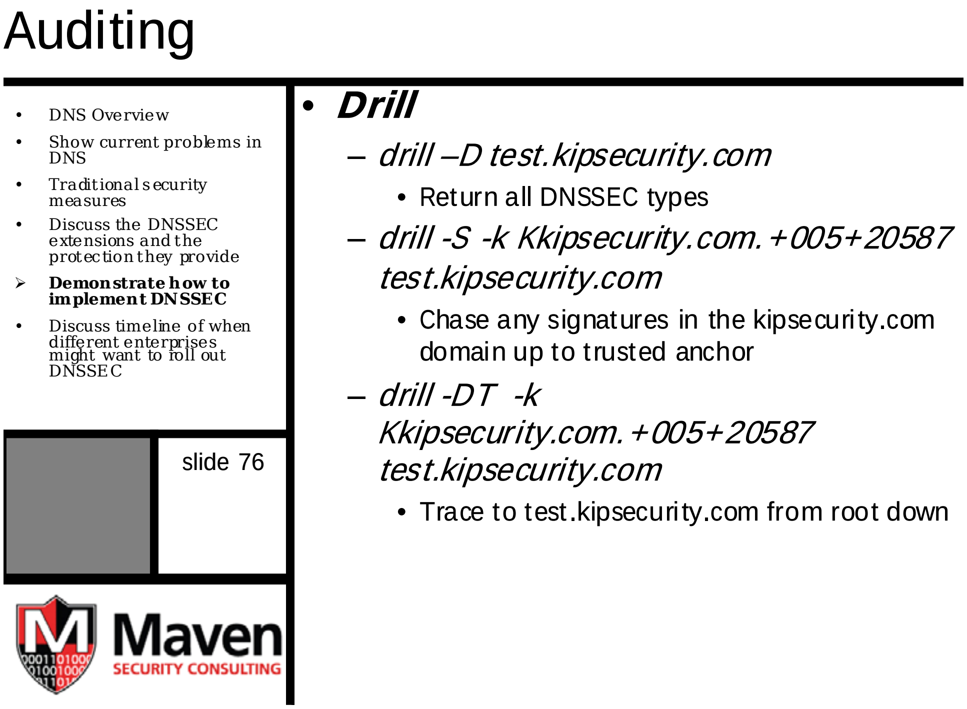
Client side setup

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- ➢ **Demonstrate how to implement DNSSEC**
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 75

Maven SECURITY CONSULTING

- ***Stub resolver***
  - *Best option is to be full validating resolver*
    - Only one exists at present, larger and slower then running full BIND
  - *Can use validating recursive resolver and TSIG/SIG(0)*
    - Secure results, but no indication of breakage to end user/ programs



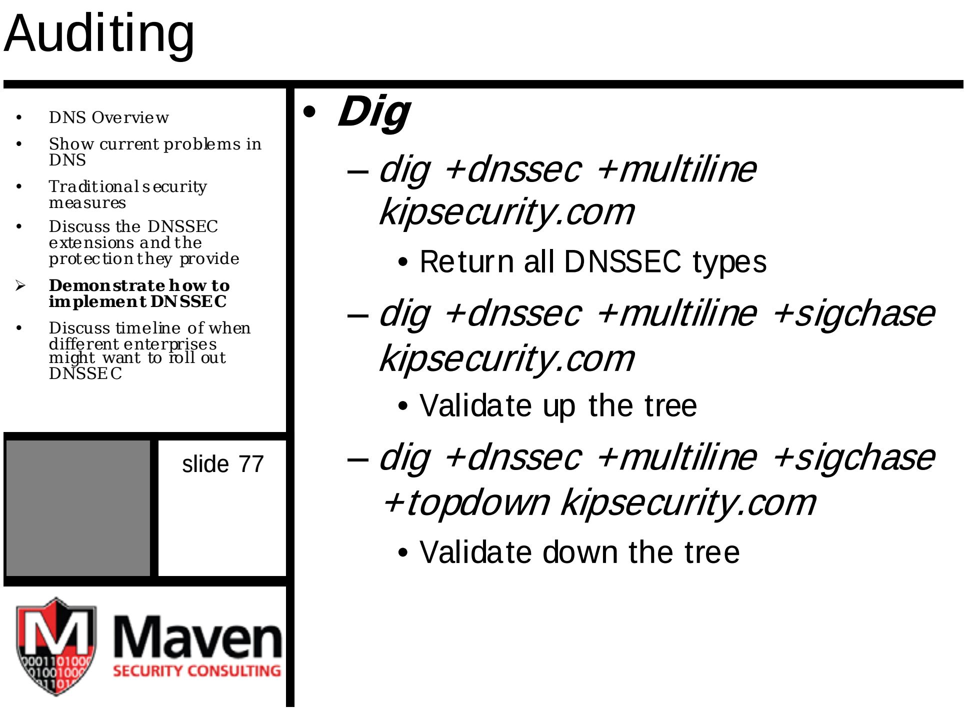
Auditing

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- ➢ **Demonstrate how to implement DNSSEC**
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 76

Maven SECURITY CONSULTING

- ***Drill***
  - *drill –D test.kipsecurity.com*
    - Return all DNSSEC types
  - *drill -S -k Kkipsecurity.com.+005+20587 test.kipsecurity.com*
    - Chase any signatures in the kipsecurity.com domain up to trusted anchor
  - *drill -DT -k Kkipsecurity.com.+005+20587 test.kipsecurity.com*
    - Trace to test.kipsecurity.com from root down

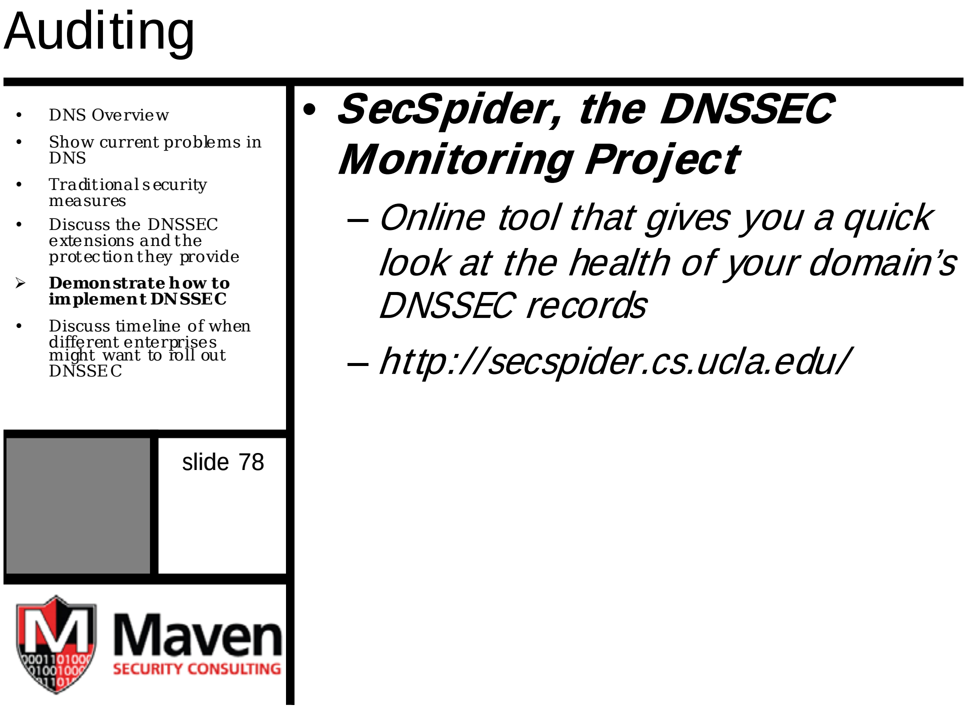


Auditing

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- ➢ **Demonstrate how to implement DNSSEC**
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 77

- ***Dig***
  - – *dig +dnssec +multiline kipsecurity.com*
    - Return all DNSSEC types
  - – *dig +dnssec +multiline +sigchase kipsecurity.com*
    - Validate up the tree
  - – *dig +dnssec +multiline +sigchase +topdown kipsecurity.com*
    - Validate down the tree



Auditing

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- ➢ **Demonstrate how to implement DNSSEC**
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 78

- ***SecSpider, the DNSSEC Monitoring Project***
  - – *Online tool that gives you a quick look at the health of your domain's DNSSEC records*
  - – *http://secspider.cs.ucla.edu/*

Technologies enabled by DNSSEC

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- ➢ **Demonstrate how to implement DNSSEC**
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 79

- ***Oh the places you'll go!***
  - *Obvious impact: DNS now secure*
  - *SPF and spam impact*
  - *Phishing relatively unaffected*
  - *IPSECKEY for secure, automatic encryption everywhere!*
  - *SSH fingerprint broadcasting*
  - *Anything small that needs to be broadcast to the world securely*

Deployment timeline

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- Demonstrate how to implement DNSSEC
- ➢ **Discuss timeline of when different enterprises might want to roll out DNSSEC**

slide 80

- ***High impact government sites***
  - *December 2007*
  - *Chosen by publication of NIST Special Publication 800-53 Rev 1*
    - http://csrc.nist.gov/publications/nistpubs/index.html#sp800-53-Rev1
  - *Deployment instructions in NIST SP 800-81*

Everyone else

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- Demonstrate how to implement DNSSEC
- **Discuss timeline of when different enterprises might want to roll out DNSSEC**

slide 81

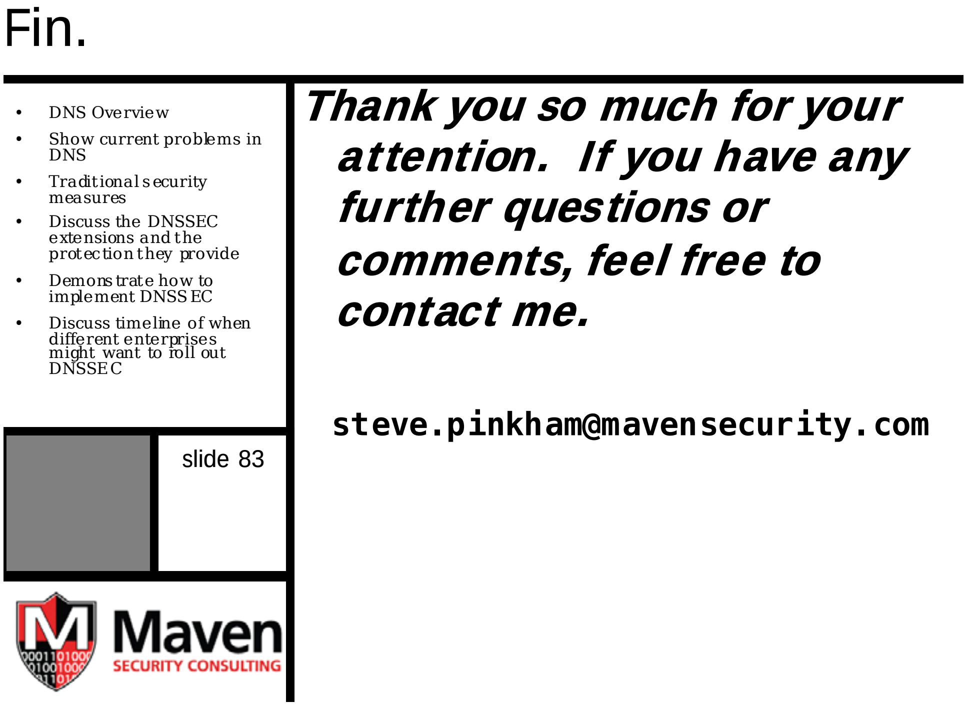
- ***Suggest small testing zones to familiarize yourself with DNSSEC***
- ***Move to corporate deployment for security of intranet***
- ***Wait for signed root or TLD, or large DLV provider for public deployment***
  - *Signed root and reverse domains in test*
  - *Wait for NSEC3 finalization? (close now, software support coming available)*
  - *Microsoft support by early 2008*

Fin.

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 82

- ***Questions?***
- ***Comments?***
- ***Snide remarks?***



Fin.

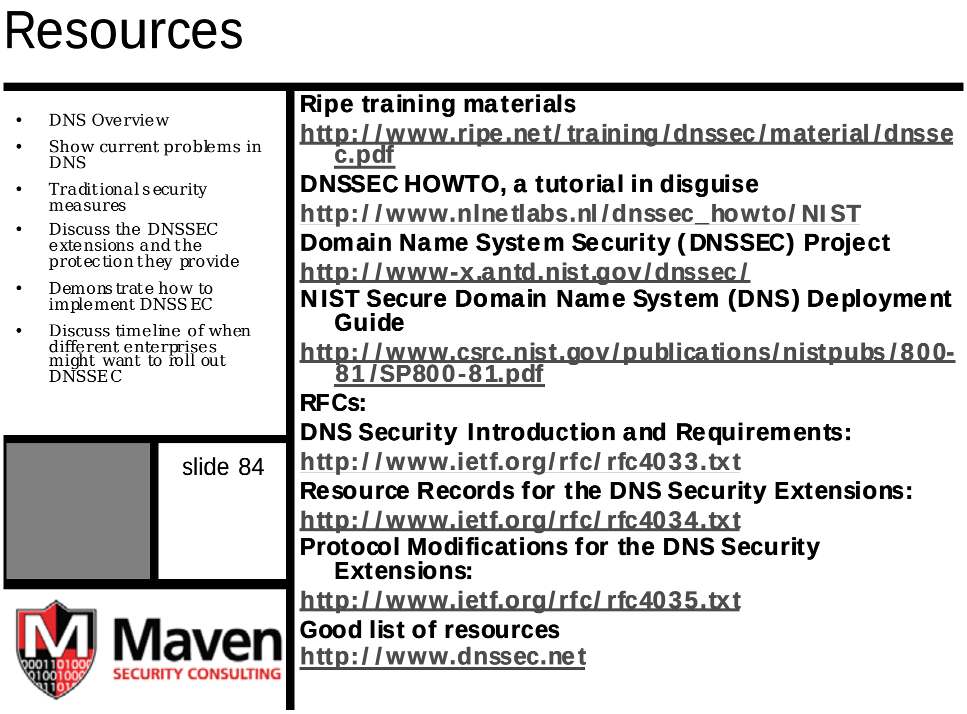
- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 83

Maven SECURITY CONSULTING

Thank you so much for your attention. If you have any further questions or comments, feel free to contact me.

steve.pinkham@mavensecurity.com



Resources

- DNS Overview
- Show current problems in DNS
- Traditional security measures
- Discuss the DNSSEC extensions and the protection they provide
- Demonstrate how to implement DNSSEC
- Discuss timeline of when different enterprises might want to roll out DNSSEC

slide 84

Maven SECURITY CONSULTING

Ripe training materials
http://www.ripe.net/training/dnssec/material/dnssec.pdf

DNSSEC HOWTO, a tutorial in disguise
http://www.nlnetlabs.nl/dnssec_howto/ NIST

Domain Name System Security (DNSSEC) Project
http://www-x.antd.nist.gov/dnssec/

NIST Secure Domain Name System (DNS) Deployment Guide
http://www.csrc.nist.gov/publications/nistpubs/800-81/SP800-81.pdf

RFCs:

DNS Security Introduction and Requirements:
http://www.ietf.org/rfc/rfc4033.txt

Resource Records for the DNS Security Extensions:
http://www.ietf.org/rfc/rfc4034.txt

Protocol Modifications for the DNS Security Extensions:
http://www.ietf.org/rfc/rfc4035.txt

Good list of resources
http://www.dnssec.net