How to Implement DNSSEC without Losing Your Mind

OWASP Atlanta -- Feb 15, 2010

Joseph Gersch
Secure64 Software Corporation

Agenda

Why is DNSSEC vitally important?

How does DNSSEC work?

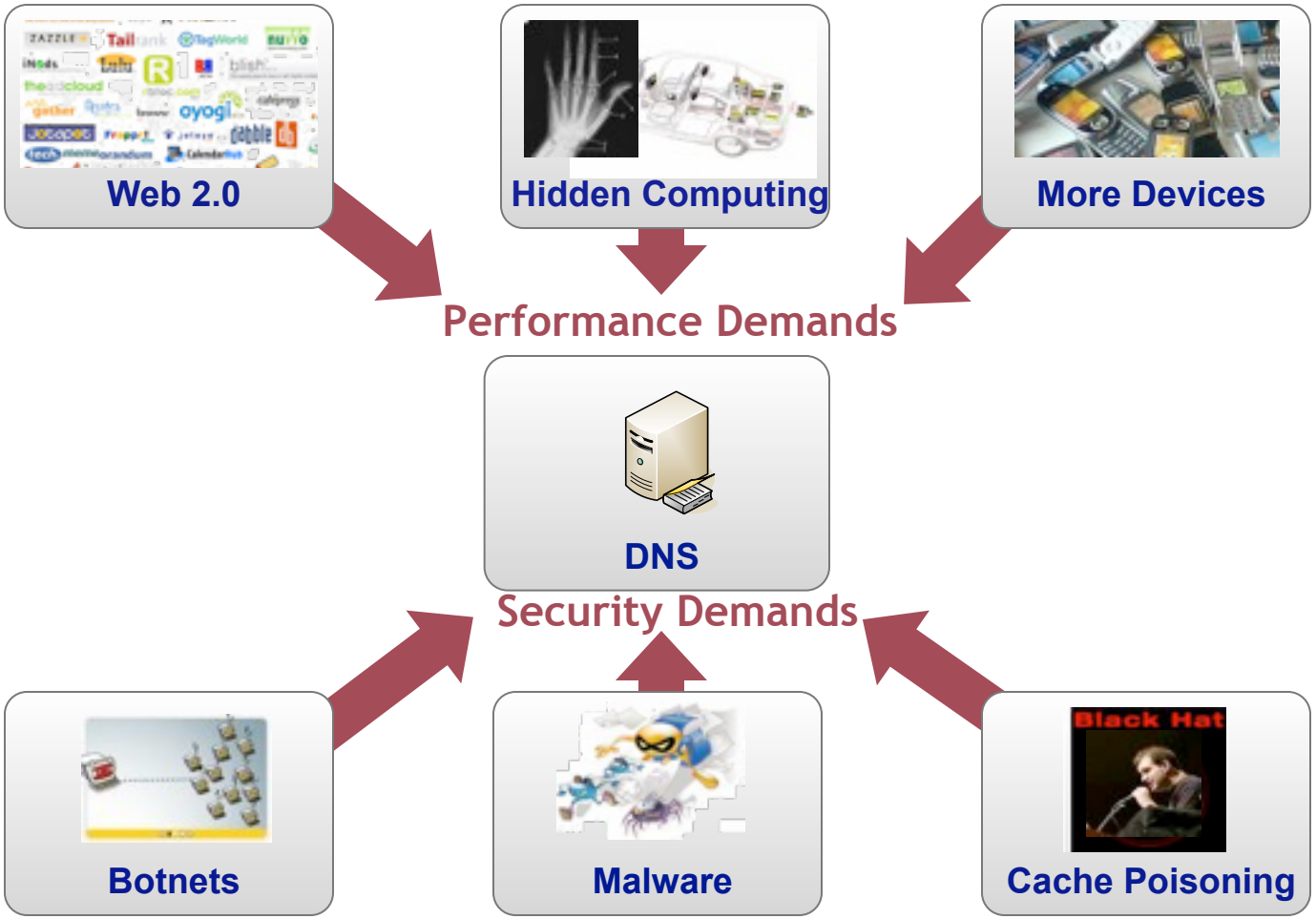
What are my options for implementing it?

Now what do I do?

SECURE64

Why is DNSSEC vitally important?

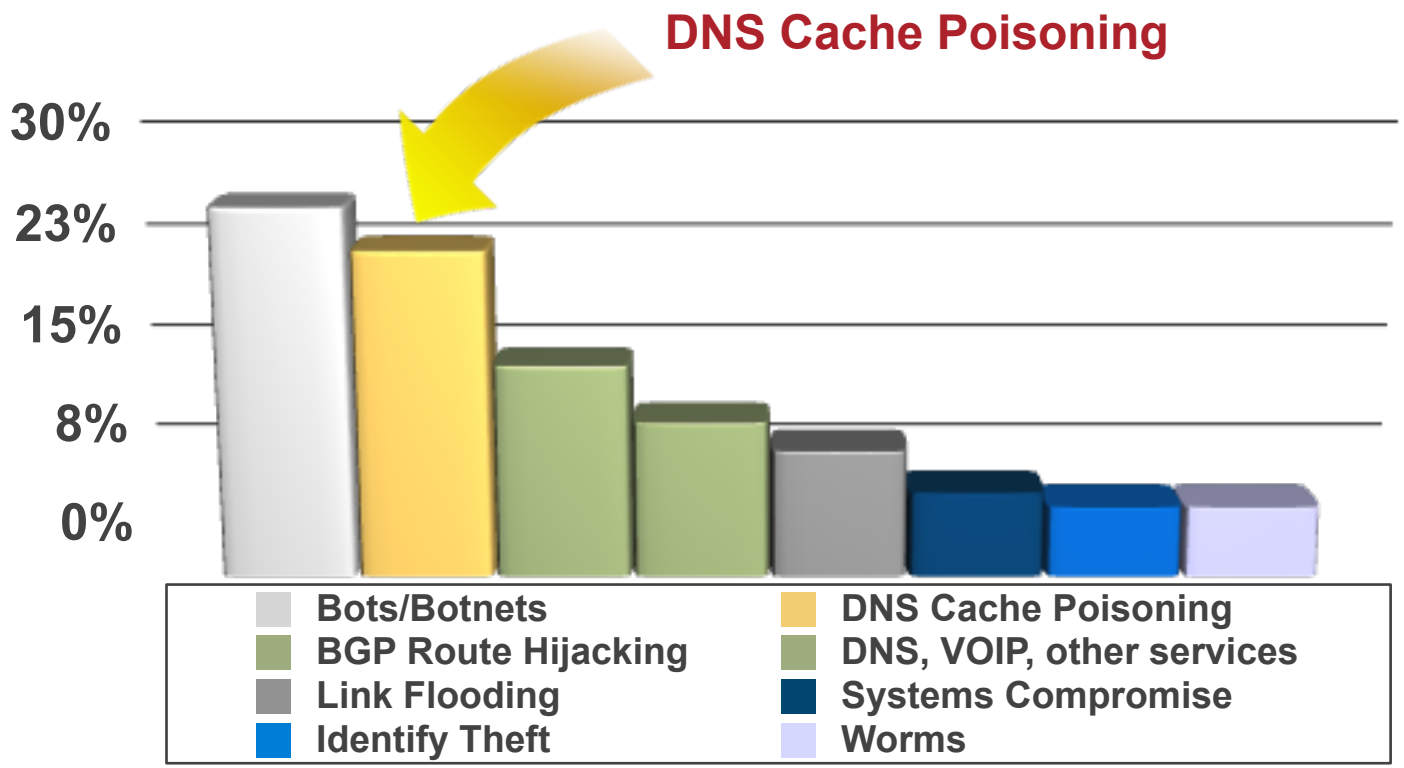
DNS Infrastructure Challenges



SECURE64

Conventional DNS solutions can't keep up with performance and security demands

Most Concerning Threats



SECURE64

Botnets, DNS and cache poisoning among the top concerns

You think your IT is protected, but....

- Firewalls, IPS, IDS....

SECURE64

But users might not even get to you!

DNS Query:
"where is *mybank.com*"?

real site:
"my firewalls are up, but where did everyone go?

poisoned DNS Server:
"It's at 1.2.3.4", *honest!!!*"

fake site

SECURE64

Lots of queries, lots of wrong answers

Truth... or Consequences

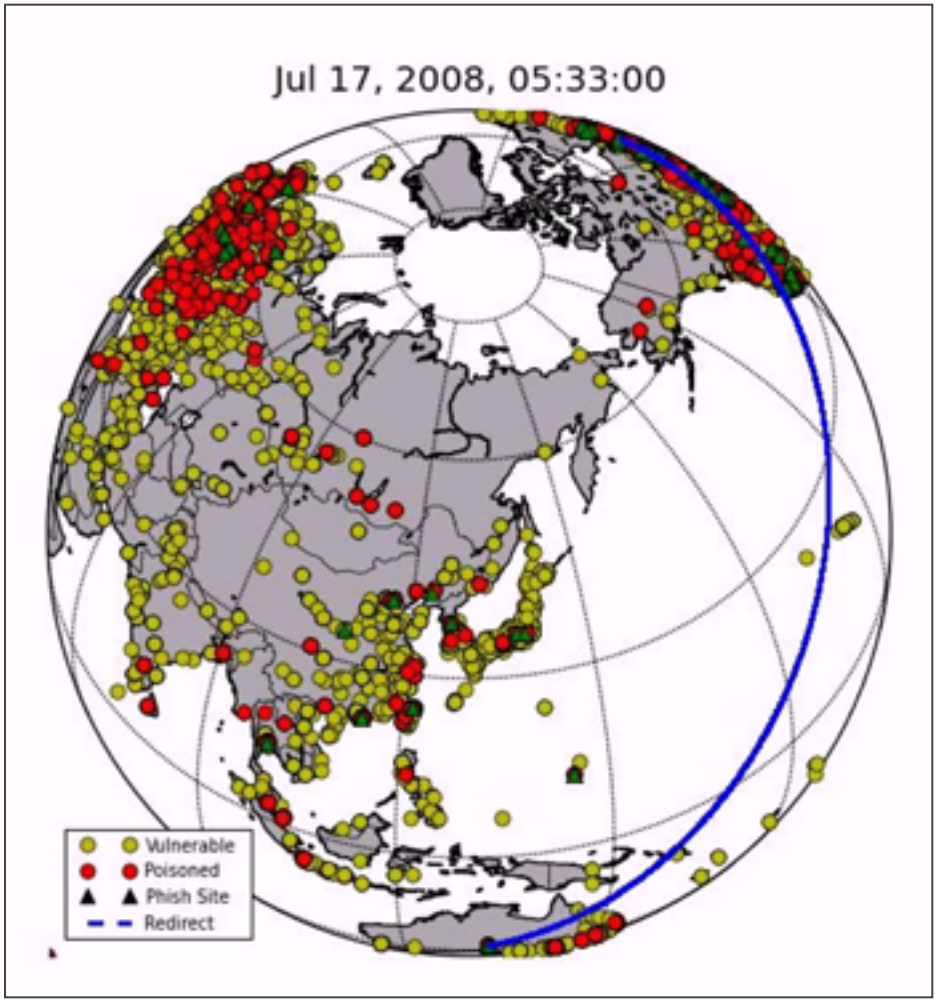
SECURE64

It’s been a year since Blackhat...

- Is the Kaminsky attack still relevant?

SECURE64

Yes, DNS Poisoning Really Happens



Source: IO Active, Dagon et. al.

Attacks are real

- 1-3% of monitored unpatched nameservers have had a poisoning event detected
- Confirmed phishing attacks have been found
- Brazilian Bank poisoned April 23, 2009

Patches are short term fix

- Patched systems have been compromised in <10 hours
- Use of botnets can greatly reduce time to compromise

DNSSEC is permanent solution

SECURE64

What's the solution?

- The DNS patch raises the bar, but DNS can still be breached

- How do you stop the storm?
- DNSSEC is the long-term permanent solution

SECURE64

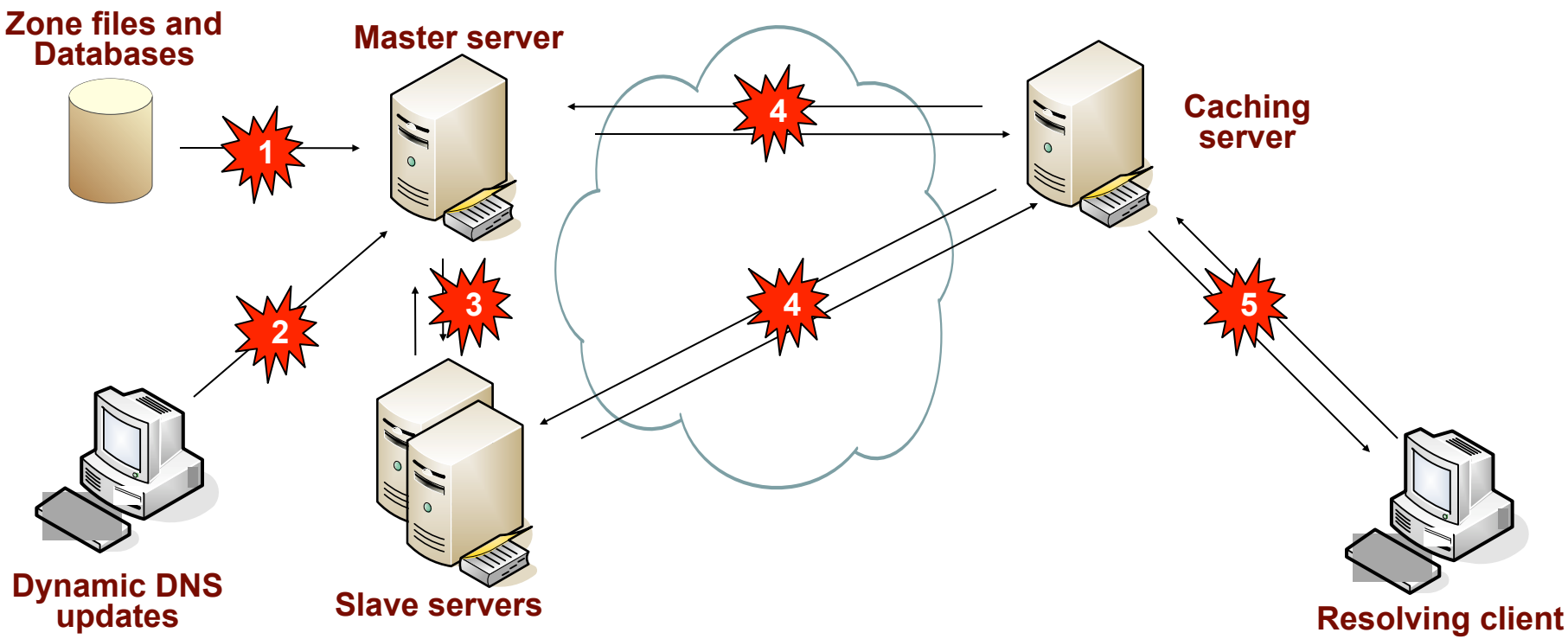
DNSSEC does more than defend

- Sure It reduces risk
  - buts it's not just about the Kaminsky attack
- It adds value and enables new killer apps
  - AUTHENTICATION on the net!!!
  - email, SSL, VOIP can all be made better.
  - Authentication for doctors, privacy issues, etc.
  - everything that RSA likes to talk about
- What can you do with an authenticated internet?

SECURE64

How does DNSSEC work?

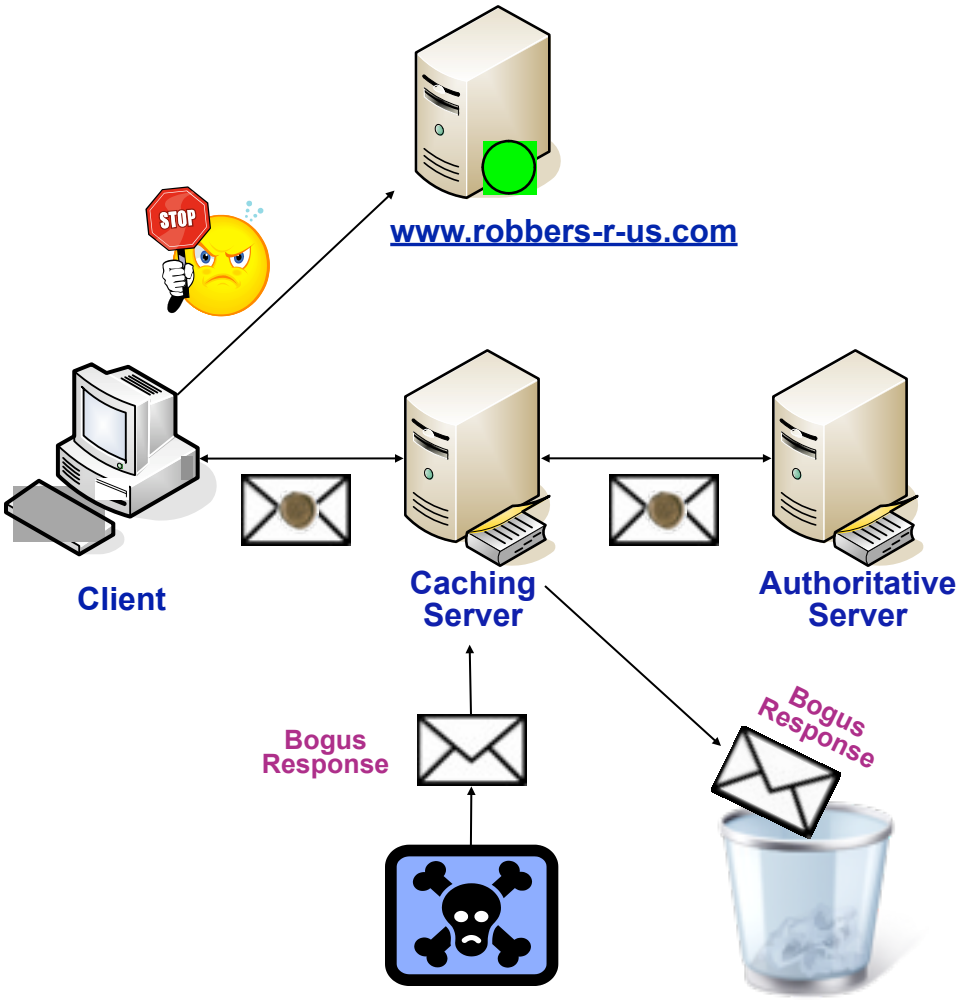
DNS attack vectors



1. Tampering with zone data / Domain hijacking
2. Forged DNS updates
3. Master impersonating / Unauthorized zone transfers
4. Cache poisoning / DoS
5. Man in the middle / Corrupted DNS resolution path

SECURE64

What Is DNSSEC?



What does it do?

- Validates the source of the DNS response
- Ensures the response has not been altered in transit
- Authenticates replies of non-existence

How does it work?

- Adds digital signatures to DNS responses
- Uses chains of trust to validate responses
- Identifies bogus responses

SECURE64

With DNSSEC, we are certain that a response is correct

Well, if DNSSEC fixes the problem...

- Why hasn’t it been more widely deployed?
- Who has already deployed it?
- Should I deploy it?

SECURE64

DNSSEC Deployment Challenges

Complexity

Security

Operational Mechanics

Disaster Recovery

Scalability

Auditability

SECURE64

Early adopters invest 4-6+ man-months to deploy, ½ full time person to maintain

The Process Is Complex

Sign all zones
- Generate public/private key pairs (one pair per zone, ideally)
- Insert keys into zone files
- Sign the zones

Once

Re-sign the zones
- Retrieve keys from secure storage
- Re-sign the zones

Weekly or whenever data changes

Roll the ZSKs for each zone
- Generate new key pairs per zone
- Add the new keys to the zone
- Re-sign the zone using the old key
- Wait for one TTL period
- Re-sign the zone using the new key
- Wait for one TTL period
- Remove the old ZSK from the zone file
- Re-sign the zone

Monthly

Roll the KSKs for each zone
- Generate new key pairs (ideally one per zone)
- Sign the DNSKEY RRset with both KSKs
- Wait one TTL period
- Update the DS record at the parent and verify
- Remove the old KSK from the zone and re-sign

Annually

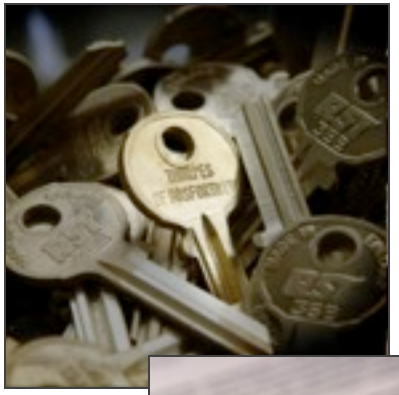
SECURE64

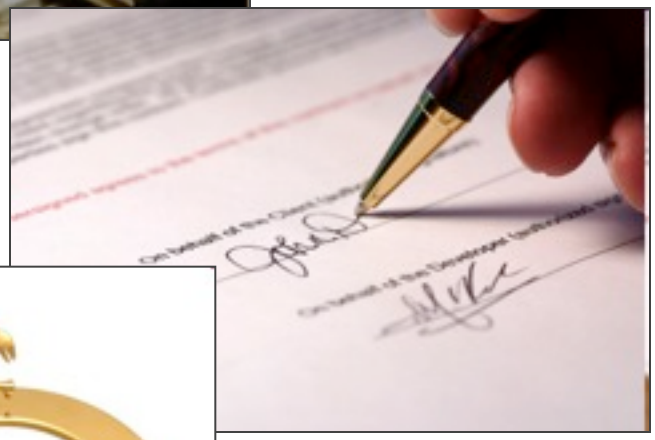
Good process discipline requires tools, procedures and training

Manual DNSSEC Deployment Steps

- **Generate keys and Insert them into zone files**
- **Sign and publish the zones**
  - **generate NSECs**
  - **generate RRSIGs**
- **Do process over and over again when data changes or when keys need to be replaced**

- *Labor and training intensive*
- *OK for small deployments, but begs for automation*



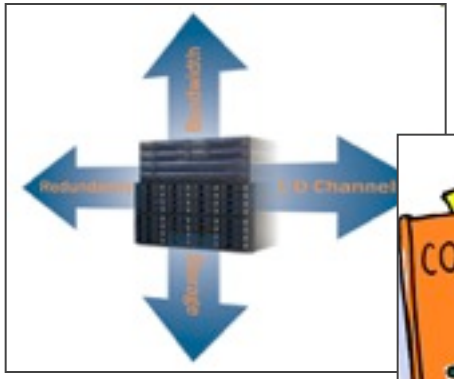


SECURE64

The Human Element:
What could ***possibly*** go wrong…

- Wrong keys
- Expired Keys
- Stolen Keys
- Training/Turnover
- Solution doesn't scale

Good Until 21/10/09



SECURE64

Keys Must Be Kept Secure

Why?

- Digital signatures guarantee authenticity, but...
- Signatures can be forged if attacker gains access to private key
- Someone can hijack your domain and guarantee it!

How to protect keys?

- Keep them offline
  - Must ensure only authorized personnel can access
  - Labor intensive
  - Doesn't work well for ZSKs in dynamic environments
- Keep them online
  - Must protect them from unauthorized access
  - OS hardening insufficient to guarantee security
  - FIPS 140-2 level 2-4 certified crypto modules work best, but can require custom hardware integration

SECURE64

Nevertheless, DNSSEC is deployed

- In Europe
  - .se --- Sweden is the poster child
  - .cz
  - .uk and other ccTLD's in the works
  - .nl has signed its ENUM zone
  - many individual organizations

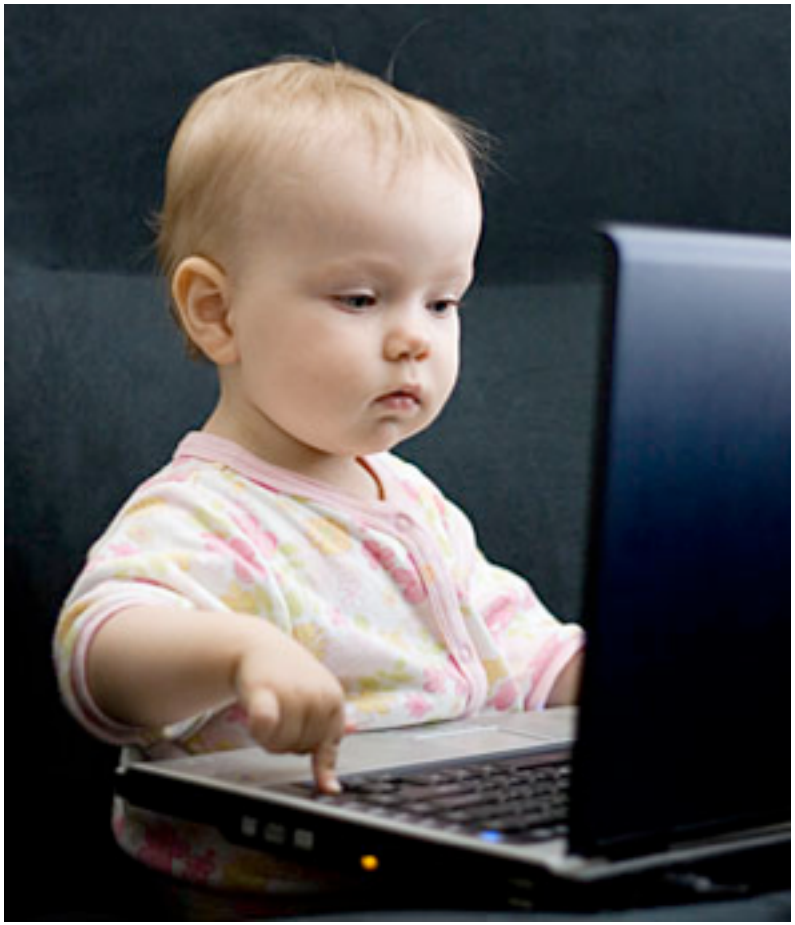
and growing!

- Around the globe:
  - .org is signed; .com and .net will be signed; root to be signed
  - .gov (USA) is signed
  - check out secspider.cs.ucla.edu
    - 3929 production zones signed
    - >16.000 zones with DNSSEC data

SECURE64

And DNSSEC technology is on the rise

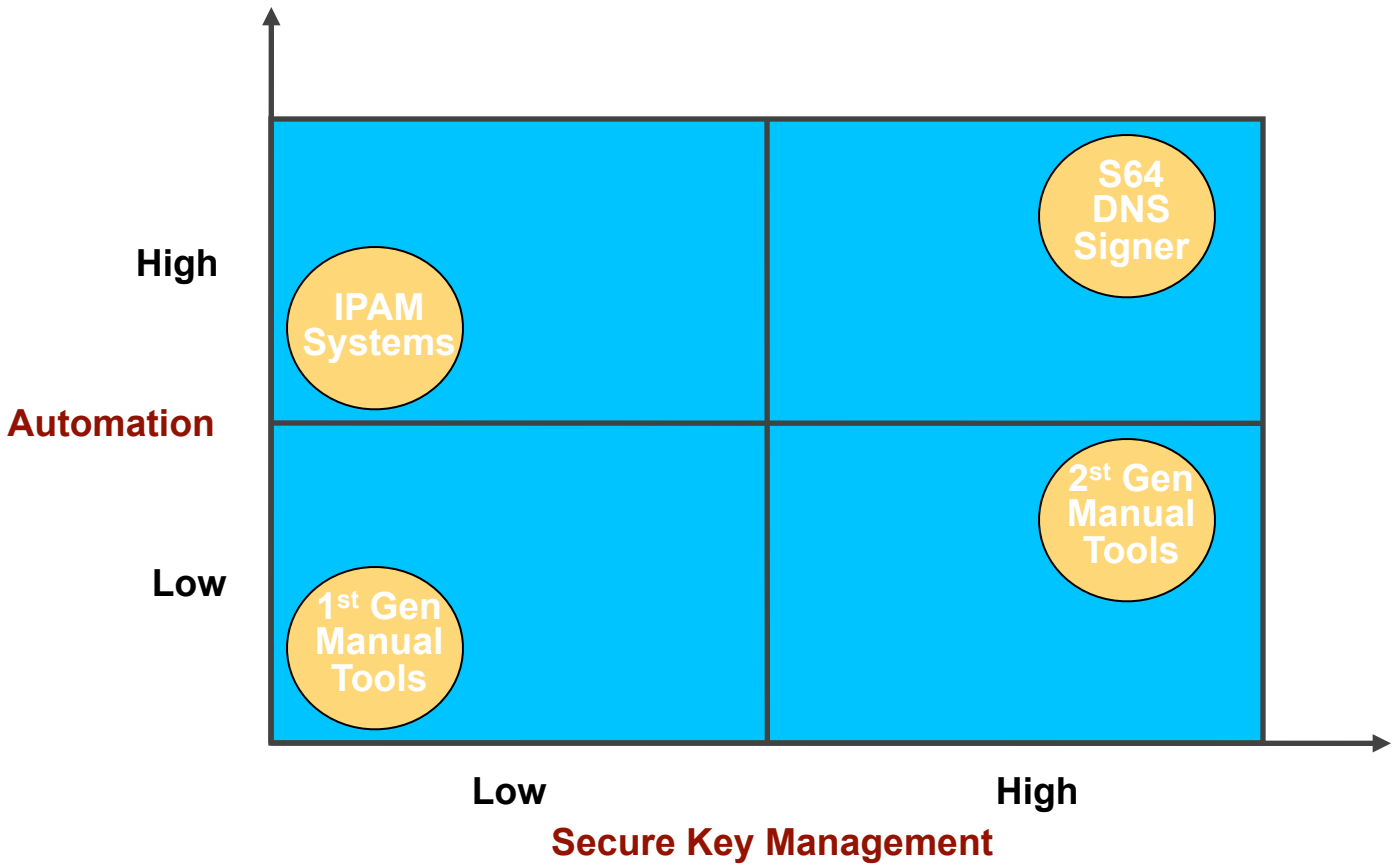
- make it easy



SECURE64

What are my options for implementing DNSSEC?

Solution Matrix



For info on this matrix, download "Choosing a DNSSEC Solution: Beware Dark Zones Ahead"

http://www.zytrax.com/books/dns/info/choosing-dnssec-solution.pdf

SECURE64

Do-It-Yourself Methods

- BIND “do-it-yourself” programs
  - DNSSEC-Keygen & DNSSEC-Signzone

- 1st & 2nd generation tools/scripts
  - www.nlnetlabs.nl : LDNS library has signer tool, etc.
  - www.dnssec-tools.org : dozens of scripts, signer, key roller
  - www.opendnssec.org :
    - not yet formally released, technology preview
    - 2nd generation tool has automation and a XML format for specifying DNSSEC policies

SECURE64

Full Automation Handles all the details

1. Key Generation for huge numbers of keys
   - pre-generate “spare keys”
2. Bulk Signing and Re-signing can take lots of time
   - fast crypto
3. Dynamic Updates
   - incremental signing
4. Disaster Planning
   - Automatic & Secure Backup of Metadata
5. Chain-of-Trust Coordination
   - automated key rollover

But be careful: some appliances are only “DNSSEC-compliant”, not automated

SECURE64

Automation: Secure64 DNS Signer

- **Simple Deployment**
  - Automated key management, rollover, signing, re-signing
- **Secure Key Repository**
  - Malware-immune OS
  - FIPS 140-2 compliant (in-review)
- **Scalable**
  - High performance signing
  - Incremental zone signing

Secure64 DNS Signer makes it easy to deploy DNSSEC correctly and securely

SECURE64

Simple to Configure

```
SERVER:

# Default signing policy

    Dnssec-automate: ON
    Dnssec-ksk: 1024 RSASHA1
    Dnssec-ksk-rollover:   0  2  1  2,8   *
    Dnssec-ksk-siglife:  7D
    Dnssec-zsk: 2048 RSASHA1
    Dnssec:zsk-rollover:   0  1  1  *  *
    Dnssec-zsk-siglife: 7D
    Dnssec-nsec-type: nsec3
    Dnssec-nsec-settings: OPT-OUT 12 aabbccdd

ZONE:
    Name: myzone.
    File:    myzonefile
    Dnssec-nsec-type: nsec

...
```

Configuration file

1-line automation

Optional parameters
to override defaults

Can be applied system-wide
or zone by zone

DNSSEC can be deployed in days, not months

SECURE64

Compatible With Current Infrastructure

Just plug it into your existing DNS provisioning system

SECURE64

Now what do I do?

Develop a plan to deploy DNSSEC

- Consider your situation:
  - Do I do this myself, or have my ISP do it for me?
- Consider your Objectives & Alternatives:
  - do I have the skills, enough training, the process discipline?
  - are my zones small and relatively static?
  - can I keep my keys off-line?

    » consider tools & scripts

  - does my DNS data change often? are my keys safe?
  - do I have staff turn-over?

    » consider automation appliance

SECURE64

Full Planning: Design For Scalability

- Can you keep up with dynamic update loads?
  - Peak DHCP load may require lots of signing horsepower
- Do you have lots of zones to sign?
  - Some zones may be changing all the time
  - Different zones roll keys on different schedules
- Do you have a Service Level Agreement to meet?
  - DNS update intervals may be guaranteed

SECURE64

Full Planning: Plan for Disaster

- Back up the data whenever anything changes
  - Keys can change, but also…
  - Zone signing state can change (zones may be in the process of a key rollover)
  - Must back up *all* information required to recover

- Protect the keys!
  - Private keys should not be in the clear in the backup

- Have a failover signing system
  - Backup signer or active/active configuration
  - Monitor active signer to detect outage

- Document backup/restore processes
  - Personnel can change
  - Don't "lose the recipe"

SECURE64

If DNSSEC signatures expire, your entire domain goes dark

Consider your staff

- Your administrators already have more than enough to do

SECURE64

But above all:

- Do it -- <u>deploy DNSSEC</u> and protect your users
- but don't drive your administrators crazy, consider automation appliances and tools

SECURE64

Thank You!

For More Information

- Secure64 web site: www.secure64.com
- Search YouTube for “Secure64” to view some useful DNSSEC tutorials
- Sign up for access to an online signing engine to try it out with your own data

SECURE64