

### DNSSEC Basics, Risks and Benefits

#### Olaf M. Kolkman olaf@ripe.net

Olaf M. Kolkman Domain Pulse, February 2005, Vienna http://www.ripe.net/disi



#### This presentation

- About DNS and its vulnerabilities
- DNSSEC status
- DNSSEC near term future



#### **DNS: Data Flow**







## DNS exploit example

 Mail gets delivered to the MTA listed in the MX RR.





## Mail man in the middle

- Ouch that mail contained stock sensitive information'
  - Who per default encrypts all their mails?
- We'll notice when that happens, we have log files
  - You have to match address to MTA for each logline.



- SPF, DomainKey and family
  - Technologies that use the DNS to mitigate spam and phishing: \$\$\$ value for the black hats
- StockTickers, RSS feeds
  - Usually no source authentication but supplying false stock information via a stockticker and via a news feed can have \$\$\$ value
- ENUM
  - Mapping telephone numbers to services in the DNS
    - As soon as there is some incentive



## Mitigate by deploying SSL?

- Claim: SSL is not the magic bullet
   (Neither is DNSSEC)
- Problem: Users are offered a choice
  - happens to often
  - users are not surprised but annoyed
- Not the technology but the implementation and use makes SSL vulnerable
- Examples follow

## **Example 1: mismatched CN**

3 Mozilla Firefox	
<u>File Edit View Go Bookmarks Tools H</u> elp	Certificate Viewer:"www.robecodirect.nl"
📀 📀 🧿 💭 🏠 🦂 💿 http://www.robecoadvies.nl/finsebrok	General Details
🎐 Plug-in FAQ 🎐 IETF ID Tracker v1.0 🎐 Mail Thread Index 🎐 AEGON Nederland m	This certificate has been verified for the following uses:
<section-header><section-header><image/><text><text><text><text></text></text></text></text></section-header></section-header>	SSL Server Certificate      Issued To      Common Name (CN)    www.robecodirect.nl      Organizational Unit (OU)    Robico      Serial Number    68:108:F6:D8:74:C9:1E:1C:86:52:98:4E:82:43:EC:86      Issued By    Common Name (CN)      Common Name (CN) <nit certificate="" of="" part="">      Organizational Unit (OU)    Ver Sign Trust Network      Organizational Unit (OU)    Ver Sign Trust Network      Organizational Unit (OU)    Ver Sign, Inc.      Validity    Issued On      Issued On    6/18/2004      Expires On    6/19/2005      Fingerprints    S9:A7:A8:1C:C3:64:FE:93:75:03:A3:4D:C5:DD:75:81:FE:12:98:46      MD5 Fingerprint    E:21:4D:E3:B8:4A:EE:21:26:D0:4D:8C:CB:26:A7:87</nit>
	www.robecodirect.nl (Help) Close
Done	
Olaf M Kolkman Domain Pulso E	abruary 2005. Vienna bttp://www.ripe.net/disi



## Example 2: Course And And CA

Could not verify this certificate because the issuer is unknown.

×

#### Web Site Certified by an Unknown Authority



#### Unknown Certificate Authority



#### Confused? Security Aler

#### Information you exchange with this site cannot be viewed or Web Site Certified by an Unknown Authority changed by others. However, there is a problem with the site's security certificate. Unable to verify the identity of bert secret-wollow as a trusted site. Possible reasons for this error Warning - Security company you have o determine whether - Your browser does not recor 00 Do you want to accept the certificate from web site "www.p3.postbank.nl" for the - The site's certificate is incom purpose of exchanging encrypted information? - You are connected to a site confidential information. Publisher authenticity verified by: "VeriSign, Inc." Please notify the site's webma matching the name. The security certificate was issued by a company that is not trusted. Before accepting this certifica willing to to accept this certific bert.secret-wg.org? The security certificate has not expired and is still valid. Certificate Examine Certificate... Certificate signer not found Security Alert Caution: "www.p3.postbank Information you exchange with thi accept this content if you tru The server's certificate chain is incomplete, and the signer(s) are not changed by others. However, the registered. Accept? security certificate. The security certificate was bert.secret-wg.org View Yes not chosen to trust. View the you want to trust the certifyin The security certificate date is valid. - The certificate for "bert.secret-wg.org" is signed by the unknown 📥 The security certificate has a valid name matching the name Certificate Authority "Secret WG Certificate Authority". It is not of the page you are trying to view. possible to verify that this is a valid certificate • Do you want to proceed? Accept Cancel Help View Certificate No Yes

Olat M. Kolkman

Domain Pulse, February 2005, Vienna

http://www.ripe.net/disi

×

# Ripe How does DNSSEC come into this picture

- DNSSEC secures the name to address mapping
  - before the certificates are needed
- DNSSEC provides an "independent" trust path.
  - The person administering "https" is most probably a different from person from the one that does "DNSSEC"
  - The chains of trust are most probably different
  - See acmqueue.org article: "Is Hierarchical Public-Key Certification the Next Target for Hackers?"



### Any Questions so far?

• We covered some of the possible motivations for DNSSEC deployment

Next: What is the status of DNSSEC, can it be deployed today?



#### **DEPLOYMENT NOW** DNS server infrastructure related signing



#### Protocol spec is clear on:

- Signing
- Serving
- Validating

#### Implemented in

- Signer
- Authoritative servers
- Security aware recursive nameservers



# Main improvement Areas

- "the last mile"
- Key management and key distribution
- NSEC walk



#### The last mile



- How to get validation results back to the user
  - The user may want to make different decisions based on the validation result
    - Not secured
    - Time out
    - Crypto failure
    - Query failure
- From the recursive resolver to the stub resolver to the Application



#### **Problem Area**



#### Key Management

- Keys need to propagate from the signer to the validating entity
- The validating entity will need to "trust" the key to "trust" the signature.
- Possibly many islands of security





### Secure Islands

- Server Side
  - Different key management policies for all these islands
  - Different rollover mechanisms and frequencies
- Client Side

(Clients with a few to 10, 100 or more trust-anchors)

- How to keep the configured trust anchors in sync with the rollover
- Bootstrapping the trust relation





- The record for proving the non-existence of data allows for zone enumeration
- Providing privacy was not a requirement for DNSSEC
- Zone enumeration does provide a deployment barrier
- Work starting to study possible solutions
  - Requirements are gathered
  - If and when a solution is developed it will be coexisting with DNSSEC-BIS !!!
  - Until then on-line keys will do the trick.



# Current work in the IETF

(a selection based on what fits on one slide)

- Last Mile
- draft-gieben-resolver-application-interface
  Key Rollover
- draft-ietf-dnsext-dnssec-trustupdate-timers
- draft-ietf-dnsext-dnssec-trustupdate-treshold
  Operations
- draft-ietf-dnsop-dnssec-operations
  NSEC++
- draft-arends-dnsnr
- draft-ietf-dnsext-nsec3
- draft-ietf-dnsext-trans



#### or send questions and feedback to olaf@ripe.net

Olaf M. Kolkman Domain Pulse, February 2005, Vienna http://www.ripe.net/disi



## References and Acknowledgements

- Some links
  - www.dnssec.net
  - www.dnssec-deployment.org
  - www.ripe.net/disi/dnssec\_howto
- "Is Hierarchical Public-Key Certification the Next Target for Hackers" can be found at: http://www.acmgueue.org/modules.php?name=Content&pa=

http://www.acmqueue.org/modules.php?name=Content&pa=sho wpage&pid=181

• The participants in the dnssec-deployment working group provided useful feedback used in this presentation.