DNSSEC
Raising the Barriers against DNS exploits

Olaf M. Kolkman
(Olaf@NLnetLabs.nl)
Cyber Crime and the role of DNS Registries

- **Good Netizens**
  - Being Involved, recognizing the problem
  - Community education and awareness raising

- **Registration Services**
  - Under appropriate circumstances providing registration data to appropriate authorities

- **DNS infrastructure**
  - Providing DNSSEC to raise the barrier for DNS based attacks
DNSSEC evangelist of the day

- **NLnet Labs**
  - Not for profit Open Source Software lab
    - Developed NSD
  - DNS and DNSSEC research
    - Protocol and software development
    - Deployment engineering

- Co-Chair of the IETF DNSEXT working group
The Problem

- DNS data published by the registry is being replaced on its path between the “server” and the “client”.
- This can happen in multiple places in the DNS architecture
  - Some places are more vulnerable to attacks than others
  - Vulnerabilities in DNS software make attacks easier (and there will always be software vulnerabilities)
Provisioning

DNS Protocol

http://www.nlnetlabs.nl/
DNS Architecture

- Server compromise
- Inter-server communication
- Cache Poisoning

Provisioning

DNS Protocol

Registry DB

Registrars

http://www.nlnetlabs.nl/
Example:
Unauthorized mail scanning

Big Corp Mail Server

Important Corp Mail Server

DNS

Where?
There!
Example:
Unauthorized mail scanning

Where?
Elsewhere
Targets…
Where do DNS and economics meet?

• SPF, DomainKey and family
  – Technologies that use the DNS to mitigate spam and phishing: $$$ value for the black hats

• Stock tickers, RSS feeds
  – Usually no source authentication but supplying false stock information via a stock ticker and via a news feed can have $$$ value

• ENUM
  – Mapping telephone numbers to services in the DNS
DNSSEC properties

• DNSSEC provides message authentication and integrity verification through cryptographic signatures
  – Authentic DNS source
  – No modifications between signing and validation

• It does not provide authorization
• It does not provide confidentiality
Metaphor

- Compare DNSSEC to a sealed transparent envelope.
- The seal is applied by whoever closes the envelope.
- Anybody can read the message.
- The seal is applied to the envelope, not to the message.

http://www.nlnetlabs.nl/
Instruct your lawyers

- A DNSSEC signature is not a certification for the correctness of the provisioned data
- It only serves to proof that the data is not changed after it made its transition from the provisioning system into the DNS
- DNSSEC validation failures indicate possible malicious activity
- Do not put legal weight on DNSSEC signatures

http://www.nlnetlabs.nl/
Deployment and Development Status

• DNSSEC is seeing very early deployment
  – .SE and RIPE NCC reverse tree

• Further protocol refinements in the make
  – To address privacy issues for some TLD registries
  – Automatic key rollover protocol
Role of Registries

• Registries one of the parties in the deployment chain
• Due Diligence
  – Possible regulator or community pressure in the future
• There are real costs and no obvious immediate benefits
  – Good PR… maybe
  – More support calls… probably
QUESTIONS?

Acknowledgements: A number of these slides are based on earlier work at RIPE NCC.

http://www.nlnetlabs.nl/
http://www.nlnetlabs.nl/