Do Not Go Insecure (please)

Shumon Huque & Eric Osterweil
ICANN DNSSEC & Security Workshop
ICANN 79; San Juan, Puerto Rico
March 6th 2024

Background

- “Intentionally Temporarily Insecure: the cheater’s guide to algorithm rolls”
  - - Wes Hardaker; ICANN 70, March 24th 2021
- Proposes to temporarily unsign zone during DNSSEC algorithm rollovers.
- Wes and others have advocated the same strategy for migrating signed zones across providers, for the same basic reasons:
  - Operational simplicity
  - If you have a preference for stability over security
  - When you lack software automation

- This presentation argues why you should not do this.

Stability vs Security is a false choice

- We can have both, and need both!
- Any change (including going unsigned), if not done correctly, can cause stability problems. (Real world example of Slack)
- Operationally robust processes for DNSSEC are needed; not sacrificing security for stability.

Software automation deficiencies?

- Tooling is being developed (and to some extent already exists) to make DNSSEC enabled provider transitions (and DNSSEC maintenance more generally) easier.
- And this will only get better over time.
- For any existing automation (or protocol) deficiencies, please raise them to the operator and protocol engineering communities. We are eager to help identify and close them.

1. The obvious - removal of security

- Cryptographic authentication of zone data has been removed.
- Even if temporary, we've opened up a window of vulnerability where adversaries can spoof your domain names.
- Most security conscious organizations will not consider this an option.

But TLS and app layer security will protect you!?

- Not necessarily.
- Defense in depth, the need to detect attacks as early as possible, avoiding easy DoS.
- All layers of the stack should be cryptographically protected: network routing, name resolution (DNS), transport, application
- Example: in 2018, MyEtherWallet, was victimized by a routing and DNS spoofing attack, resulting in substantial monetary loss.
  - TLS did not protect the victims, since they just clicked through security warnings
- DNS spoofing can also allow attackers to more easily obtain “domain-validated” website certificates, which can be used to subvert TLS security.

2. DANE applications will break

- DANE (DNS-based Authentication of Named Entities)
  - Uses signed DNS to authenticate public keys and certificates used in application security protocols.
- Applications that use DANE can break or degrade.
- Studies show a quite high deployment rate of DANE for SMTP.
- In applications that support “opportunistic” security with DANE, there is still a significant security downgrade exposure if DANE authentication capability is removed.
  - Do you want to risk silent loss of security or dropping of email?
- If DANE is ever to be a compelling alternative Internet or Web-PKI, DANE applications must not ever go insecure.

3. Vendor Lock-in?

- Security conscious organizations will not tolerate going unsigned during provider migrations.
- If a DNS provider does not provide the mechanisms to allow non-disruptive transfer of signed zones to a new provider (e.g. supporting multi-signer transition), this may create a vendor lock-in situation. Or discourage potential new DNSSEC customers from considering them.

4. DNSSEC will not be taken seriously

- DNSSEC is a security protocol.
- If “going unsigned” is a common operational model for DNSSEC, it will not be taken seriously in the larger security community.

Questions/Comments?

Do Not Go Insecure