Recitation 23: DNSSEC

MIT - 6.033

Spring 2022

Henry Corrigan-Gibbs

Plan

- The problem
- Recitation Qs
- Digital sigs & DNSSEC
- Demo & visualization
- Discussion

Logistics

* Design project due **May 2** at 11:59pm.
  → 6000 words <u>only</u>
* No recitation next Tues 5/3
* AMA Session 10am - 12pm on Th 5/12 in 32-G970 A
* Poll: Last recitation.

The Problem

TCP/IP provides

- * no confidentiality
- * no integrity

Most Internet protocols don't either

HTTP, SMTP, POP, IMAP, DNS, ...

DNS is the system mapping

hostnames www.csail.mit.edu.

⇓

IP addresses 23.185.0.3

⇒ Attacker in network can hijack traffic, cause all sorts of chaos

Recitation Questions

1. What security benefit does DNSSEC provide?
   - Authentication of DNS records
     ↳ Prevents attacker in the middle from tampering w/ DNS replies

2. How does it provide that?
   - "Chain of trust"
     ↳ Digital signatures

3. Why is DNSSEC necessary? Why hasn't it been deployed?

   → To discuss...

Digital Signature

$\mathrm{Gen}() \longrightarrow (sk, pk)$

$\mathrm{Sign}(sk, m) \longrightarrow \sigma$

$\mathrm{Verify}(pk, m, \sigma) \longrightarrow \{\text{valid}, \text{invalid}\}$

Correct: Honest verifier accepts with pk accepts msg signed with sk.

Secure: Infeasible for an adversary to cook up valid signatures without sk.

- Proposed by Diffie & Hellman in 1976 paper
- RSA '79 gave first widely used instantiation.

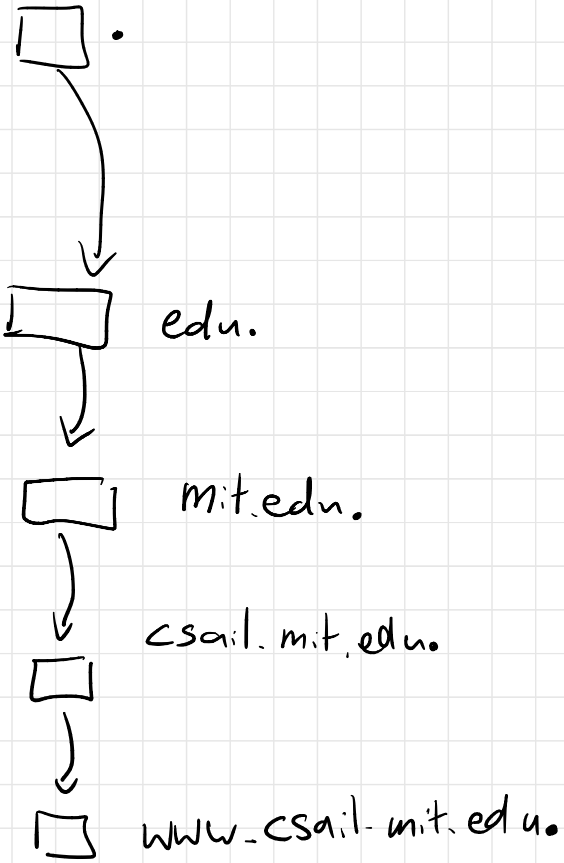
What is DNSSEC?

Simple idea:

Use digital signatures to authenticate all DNS answers

→ No encryption / confidentiality

Recall DNS



Demo: Dnsviz

Look at a few sites

- * cloudflare.com
- * google.com
- * nsa.gov
- * www.mit.edu

Things to notice

- * Key-signing key (recover from theft)
- * Complexity, many choices
- * Lack of support! Misconfiguration!

Question: How to sign "does not exist" record?

A Discussion (not a debate)

All website operators should deploy DNSSEC.

Take

Ball

Discuss in groups

All website operators should deploy DNSSEC.

In Favor (odd groups)

- * Lots of infrastructure relies on DNS
  ↪ might as well try to secure it
- * Not so expensive
- * Backwards compatible

Against (even groups)

- * violates end-to-end principle
- * complexity w/o security
  ↪ no encryption anyhow
- * duplicates work at other layers of stack
- * Internet works pretty well without it
- * False sense of security.

Take

Ball

The

End