Recitation 23: DNSSEC
Plan

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

Logistics

* Design project due **May 2**
  * at 11:59 pm.
  * 6000 words only

* No recitation next Tues 5/3

* AMA Session 10am - 12pm
  * on Th 5/12 in 32-9970A

* 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


⇒ 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 with 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

\[ \text{Gen}(\cdot) \rightarrow (sk, pk) \]

\[ \text{Sign}(sk, m) \rightarrow \sigma \]

\[ \text{Verify}(pk, m, \sigma) \rightarrow \{ \text{valid}, \text{invalid} \} \]

- **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

```
.  →  edu.
   ↓  →  mit.edu.
   ↓  →  csail.mit.edu.
```
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 \text{P.10}
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 P.11
The End