Recitation 20: DNSSEC

MIT - 6.033

Spring 2021

Henry Corrigan-Gibbs

Plan

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

Logistics

* Design project due at 11:59pm. today
* No recitation Thursday 5/13
* Last recitation Tuesday 5/18.
* Course evaluations open
* Office hours / AMA 5/20?
  ↳ Poll, send topics by mail

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

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

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

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

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

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

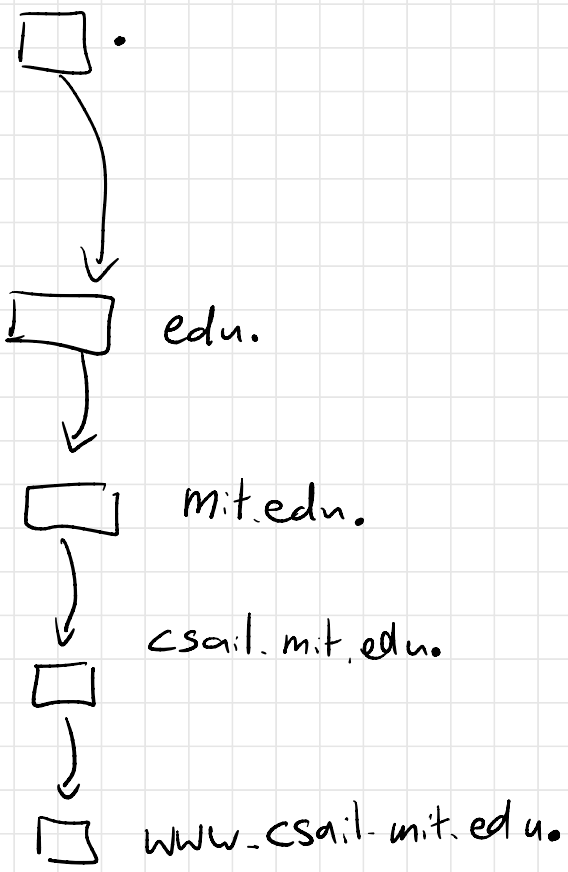
What is DNSSEC?

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 Debate

All website operators should deploy DNSSEC.

Take

Ball

A Debate

All website operators should deploy DNSSEC.

In Favor (odd rooms)

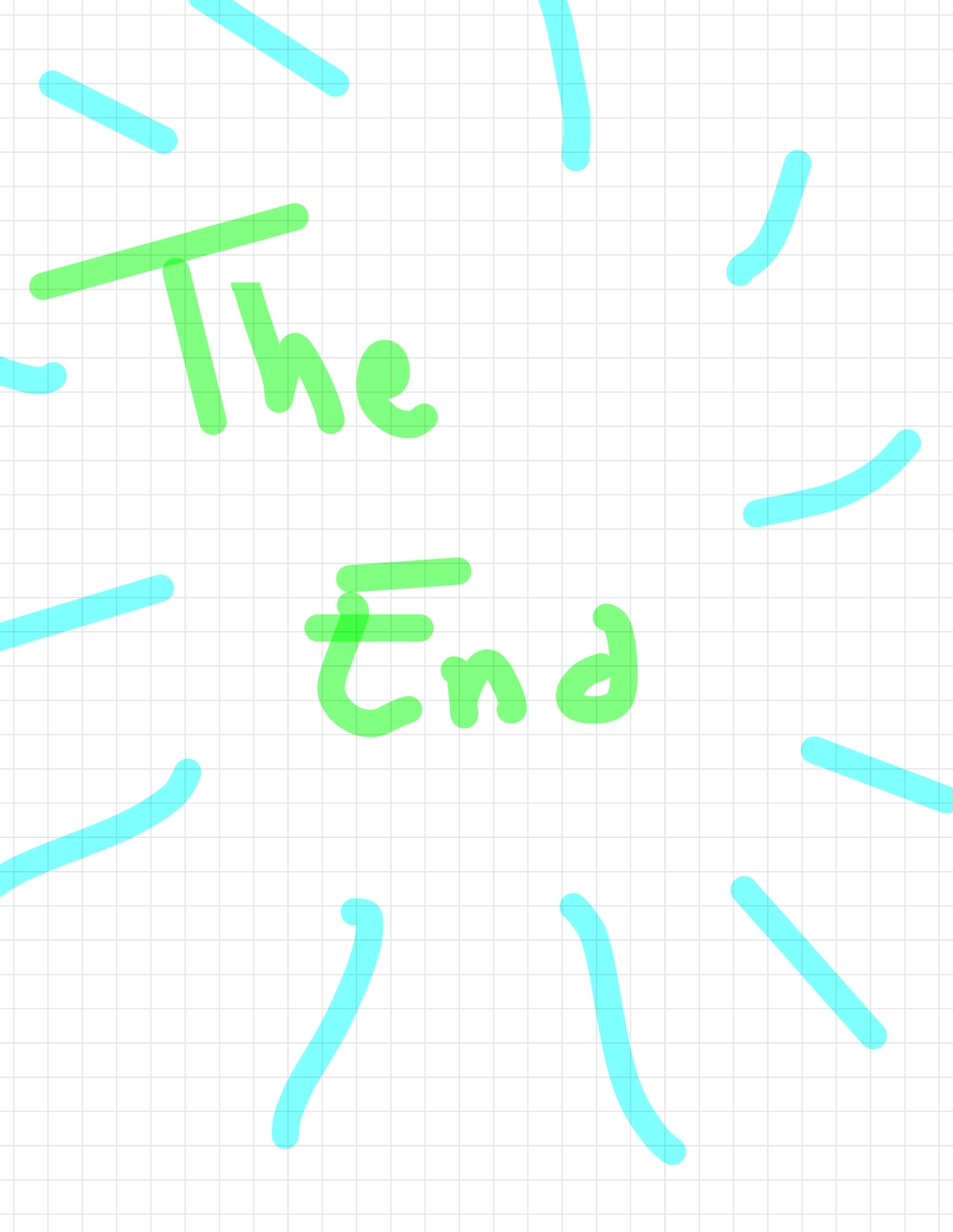
* Lots of infrastructure relies on DNS
  ↳ might as well try to secure it
* Not so expensive
* Backwards compatible

Against (even rooms)

* 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