Plan

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

Logistics

* Design project due TODAY at 11:59 pm
* No recitation Thursday 5/13
* Last recitation Tuesday 5/18
* Course evaluations open
* Office hours/AMA 9/20?
The Problem

Authentication to DNS: (mit.edu \(\Rightarrow\) 23.185.0.3)

TCP/IP provides no confidentiality, no integrity.
Recitation Qs

1. What security benefit does DNSSEC provide?
   - authentication/integrity for DNS traffic
   - confidence
   - transport layer security

#1) DNSSEC not really used.
#2) TLS
   - Doh (DNS over HTTPS)
   - DNS over TLS
Digital Signatures

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

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

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

**Correct**: Honest client accepts msgs signed with sk.

**Secure**: Infeasible for adv w/o sk. to cook valid signature.
What is DNSSEC?

Simple idea: Use digital sigs to authenticate DNS responses.

No encryption.

Recall

www.csail.mit.edu → 18.4.72.3

Chain of Trust
<table>
<thead>
<tr>
<th>Domain</th>
<th>IP Address</th>
<th>Server</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>.com</td>
<td>72.3.15.123</td>
<td>pk.com</td>
<td>root</td>
</tr>
<tr>
<td>.net</td>
<td></td>
<td>pk.net</td>
<td></td>
</tr>
<tr>
<td>.edu</td>
<td></td>
<td>pk.edu</td>
<td></td>
</tr>
<tr>
<td>.ly</td>
<td></td>
<td>pk.ly</td>
<td></td>
</tr>
</tbody>
</table>
Dh/DNS over TLS

Google
(8.8.8.8)
(1.1.1.1)

mit.edu

edu.

m.it.edu
Claim: All website operators should deploy DNSSEC.

For

+ Authentication end-to-end
+ Backwards compatible
+ Can detect/prevent in-network attacks on DNS

Against

- A lot of work.
- Not enough security.
- Violates end-to-end principle.
Plan

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

Logistics

* Design project due TODAY at 11:59 pm
* No recitation Thursday 5/13
* Last recitation Tuesday 5/18
* Course evaluation open
* Office hours/AMA 9/20
The Problem

TCP/IP provides
- no confidentiality
- no integrity

DNS resolves
- hostname (e.g., mit.edu)
- to IP address (e.g., 1.2.3.42)

TLS (HTTPS, IMAPS, ...)
1. What security benefit does DNSSEC provide?
   - Authentication of DNS records
   - NO ENCRYPTION with DNSSEC

2. How?
   - Digital signatures.
**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 client accepts msg signed w/ sk.

**Security:**
Infeasible for an attacker to cook valid sign w/ the sk.

\[ \text{Sign} \rightarrow \text{Verify} \]

\[ \text{Sign} \rightarrow \text{Reject} \]

\[ \text{Sign} \rightarrow \text{Verify} \rightarrow \text{Reject} \]

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

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

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

Simple idea:
Use digital sigs to authenticate DNS msgs.
1. "No one" uses DNSSEC. It's the Zune of internet security.

2. Use TLS.
Claim: All website owners should deploy DNSSEC.

For:
+ Not so expensive
+ Backward compatible
+ High risk settings
+ 

Against:
- Complexity
- Computational load
- No encryption
- 

e-PHESKPG-ppds.ch can't use TLS