Plan

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

Logistics

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

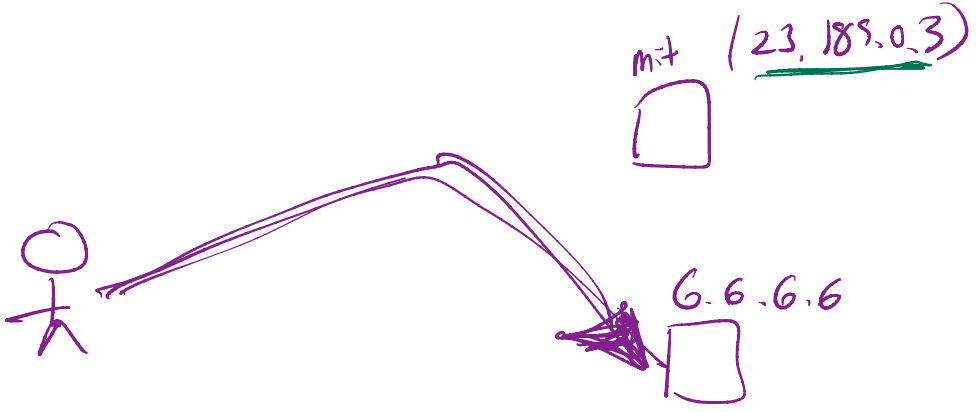
The Problem

Authentication to DNS. (mit.edu ⟹ 23.185.0.3)

6.6.6.6

TCP/IP provides no confidentiality.

no integrity.



Recitation Qs

1. What security benefit DNSSEC provide?
   - ↳ authentication/integrity for DNS traffic
   - ↳ ~~confidentiality~~

#1) DNSSEC not really used.

#2) TLS ← transport layer security
   - DoH (DNS over HTTPS)
   - DNS over TLS

Digital Signatures

$Gen() \rightarrow (sk, pk)$

sk → DNS server, pk → client

$Sign(sk, m) \rightarrow \sigma$

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

Correct: Honest client accepts msgs signed with sk.

Secure: Infeasible for adv w/o sk. to cook valid signature.

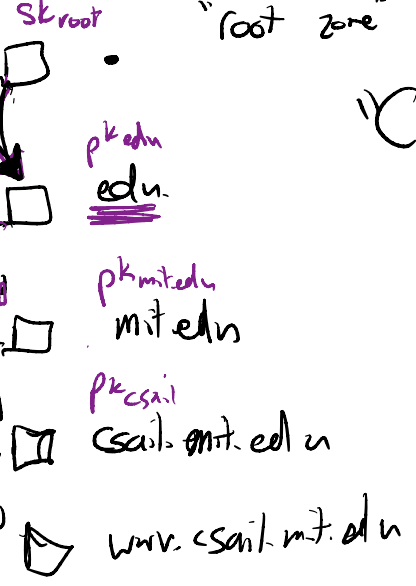
What is DNSSEC?

Simple idea: Use digital sigs to authenticate DNS responses.

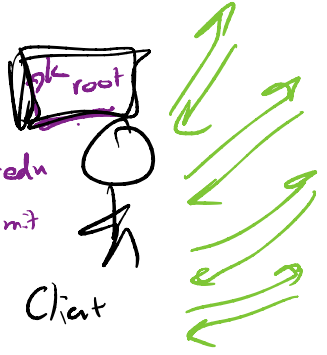
↳ NO ENCRYPTION

Recall

www.csail.mit.edu. → 18.4.72.3

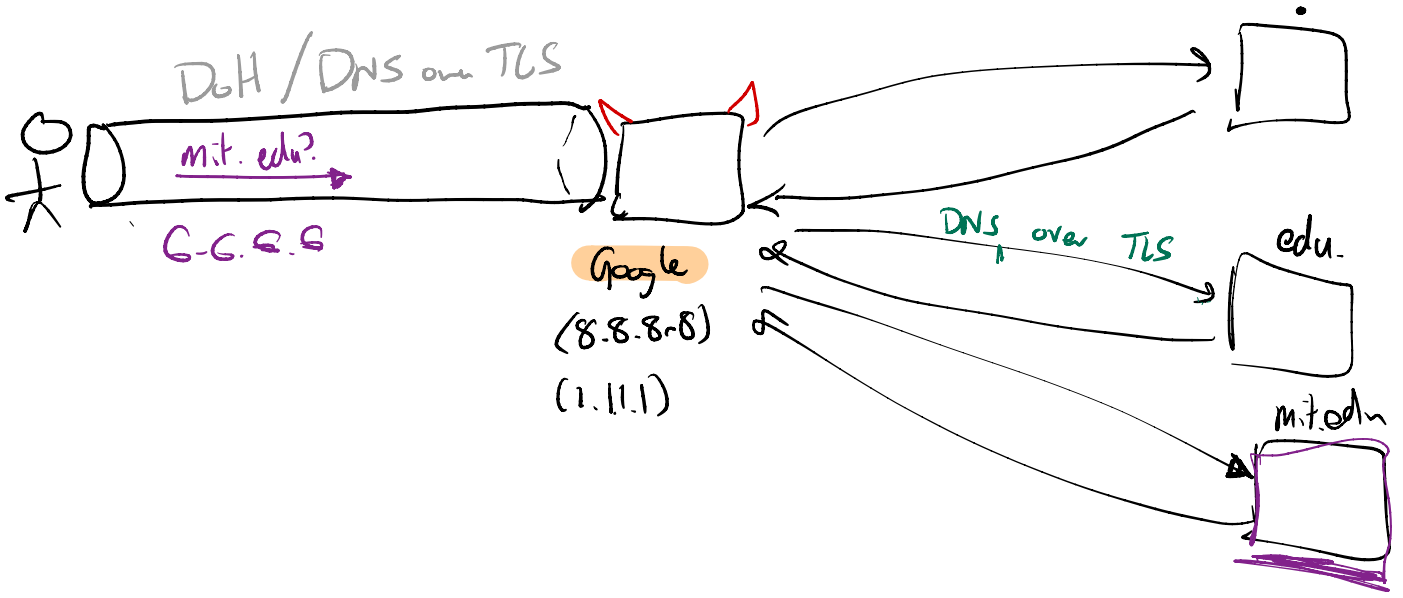


"Chain of Trust"



Root server

.com	72.3.15.123	pk_{com}
.net	~	pk_{net}
.edu	~	pk_{edu}
.ly	~	pk_{ly}
⋮	⋮	⋮


DoH / DNS over TLS
m.i.t. edu?
G.G.G.G
Google
(8.8.8.8)
(1.1.1.1)
DNS over TLS
edu.
m.i.t.edu

Claim: All website operator 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

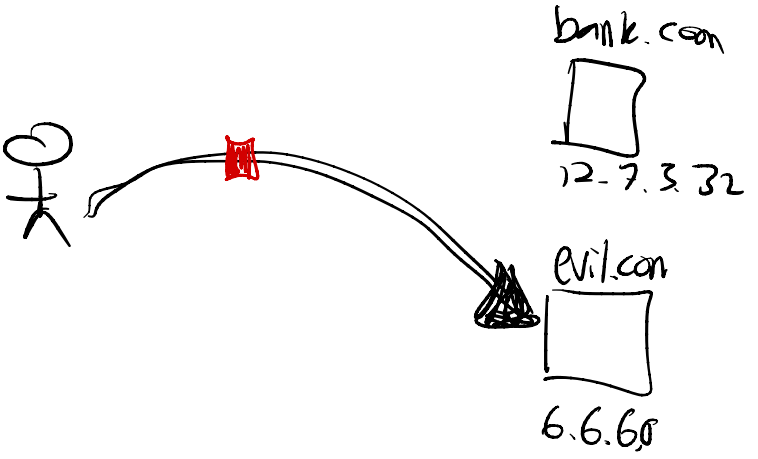
* Design project due TODAY at 11:59pm
* No recitation Thursday 5/13
* Last recitation Tuesday 5/18
* Course evaluations open
* Office hours/AMA 5/20?

The Problem

TCP/IP provides [TCP, UDP]

- ✗ no confidentiality
- ✗ no integrity

↳ TLS (HTTPS, IMAPS, ...)



DNS: hostname (mit.edu) ⟹ IP addr (1.2.3.42)

1. What security benefit does DNSSEC provide?

↳ Authentication of DNS records

NO ENCRYPTION with DNSSEC

2. How?

↳ Digital signatures.

Digital Signature

$Gen() \rightarrow (sk, pk)$

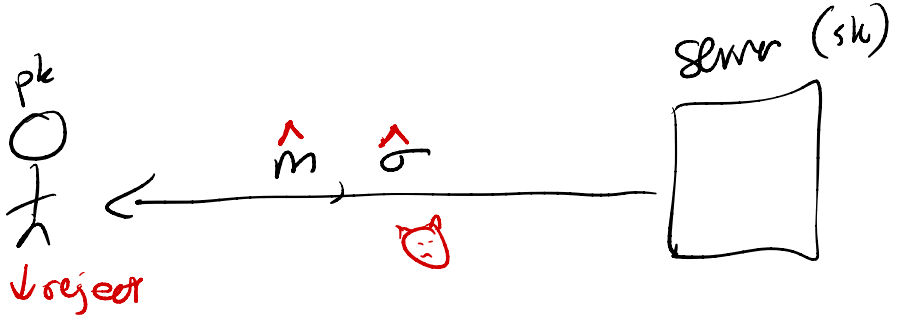
DNS server ↑ pk ↑ client

$Sign(sk, m) \rightarrow \sigma$

Correct: Honest client (holds pk) accepts msg signed w/ sk.

Security: Infeasible for an attacker to cook valid sigs w/o the sk.

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



Ralph Merkle CS276 | 6.5060

Diffie-Hellman key exchange, digital sig (2015)

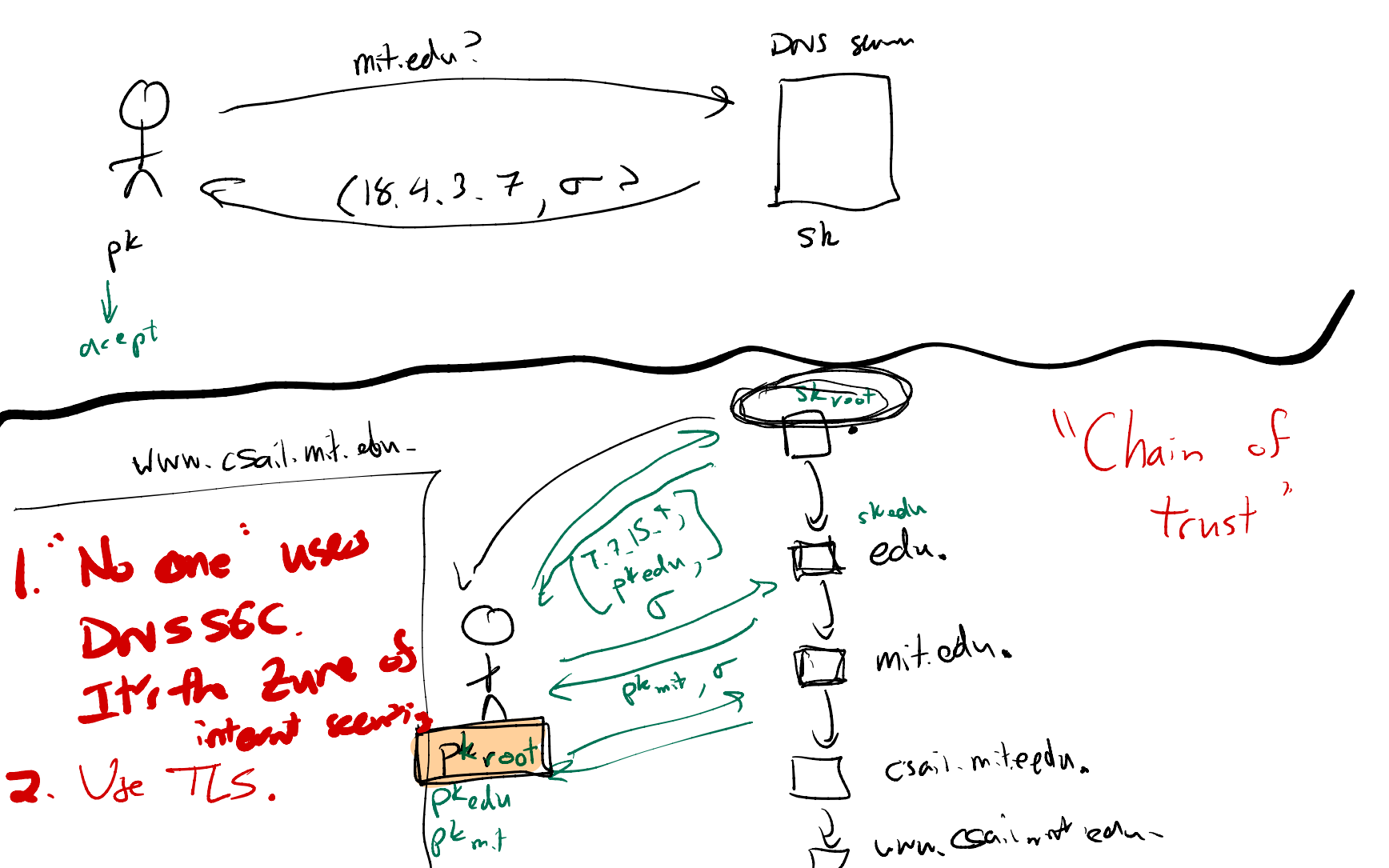
↳ shared secret w/ public discussion

Ron Rivest, Shamir, Adleman (1994)

Simple idea:

Use digital sigs

to authenticate DNS msgs.


mit.edu?
DNS server
(18.4.3.7, σ)
pk
sk
accept
www.csail.mit.edu
1. "No one" uses DNSSEC. It's the 2nd of internet security
2. Use TLS.
sk_root
sk_edu
edu.
mit.edu.
csail.mit.edu.
www.csail.mit.edu
T, 7_IS_T
pk_edu
σ
pk_mit, σ
pk_root
pk_edu
pk_mit
"Chain of trust"

Claim: All website owners should deploy DNSSEC.

FOR

+ Not so expensive
+ Backwards compatible
+ high-risk settings
+ [redacted]
+ [redacted] protocol that can't use TLS

AGAINST

- Complexity
- Computational load
- no encryption →
-