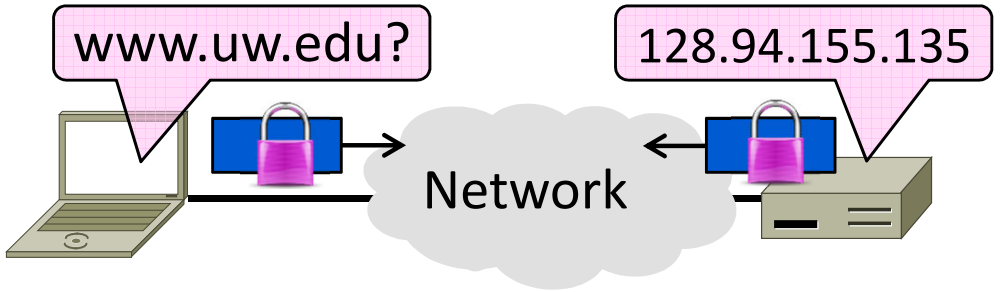
Computer Networks

DNS Security (§8.9.2)

David Wetherall (djw@uw.edu)
Professor of Computer Science & Engineering
UNIVERSITY of WASHINGTON

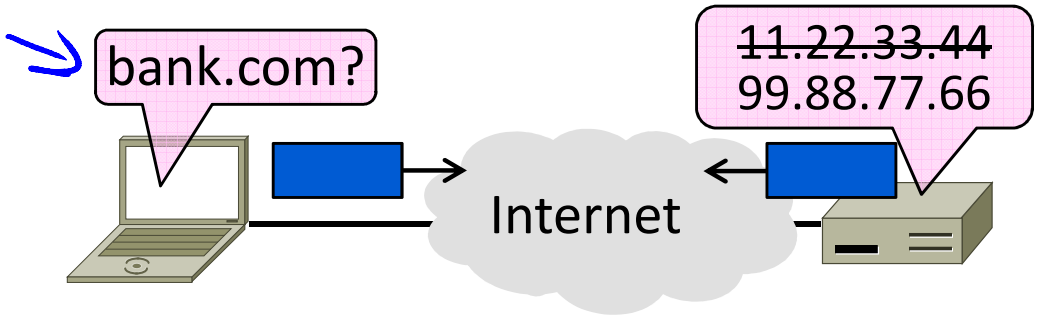
Topic

- Securing Internet naming
  - DNS security extensions (DNSSEC)



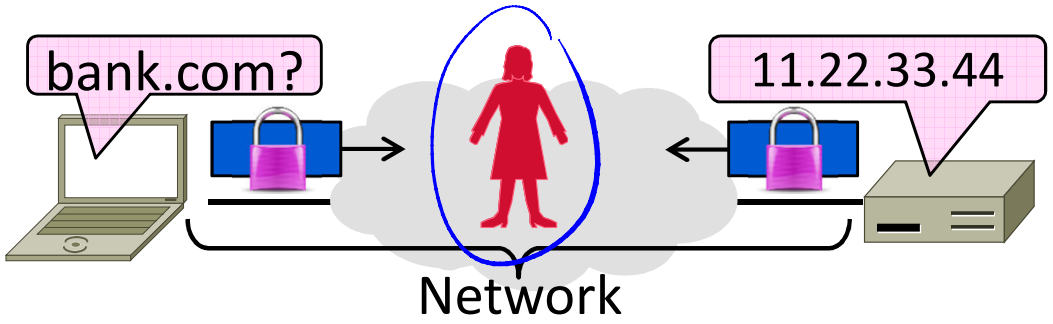
Goal and Threat Model

- Naming is a crucial Internet service
  - Binds host name to IP address
  - Wrong binding can be disastrous …



Goal and Threat Model (2)

- Goal is to secure the DNS so that the returned binding is correct
  - Integrity/authenticity vs confidentiality
- Attacker can intercept/tamper with messages on the network

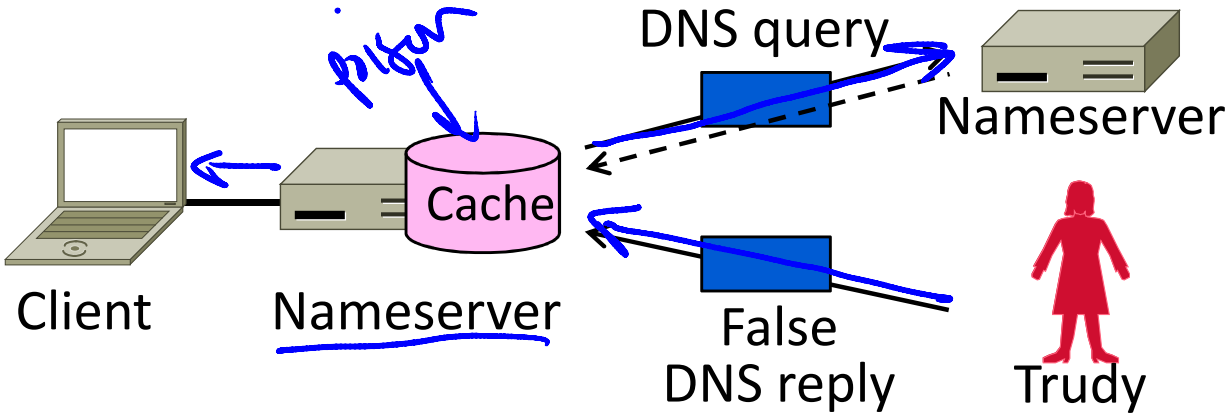


DNS Spoofing

- Hang on – how can a network attacker corrupt the DNS?
- Trudy can trick a nameserver into caching the wrong binding
  - By using the DNS protocol itself
    - This is called DNS spoofing

DNS Spoofing (2)

- To spoof, Trudy returns a fake DNS response that appears to be true
  - Fake response contains bad binding



DNS Spoofing (3)

- Lots of questions!
  1. How does Trudy know when the DNS query is sent and what it is for?
  2. How can Trudy supply a fake DNS reply that appears to be real?
  3. What happens when the real DNS reply shows up?

- There are solutions to each issue …

DNS Spoofing (4)

1. How does Trudy know when the query is sent and what it is for?

- Trudy can make the query herself!
  - Nameserver works for many clients
    - Trudy is just another client

DNS Spoofing (5)

2. How can Trudy supply a fake DNS reply that appears to be real?

- A bit more difficult. DNS checks:
  - Reply is from authoritative nameserver (e.g., .com)
  - Reply ID that matches the request
  - Reply is for outstanding query
- (Nothing about content though …)

DNS Spoofing (6)

2. How can Trudy supply a fake DNS reply that appears to be real?

- Techniques:
  - Put IP of authoritative nameserver as the source IP address
  - ID is 16 bits (64K). Send many guesses! (Or if a counter, sample to predict.)
  - Send reply right after query
- Good chance of succeeding!

DNS Spoofing (7)

3. What happens when the real DNS reply shows up?

- Likely not be a problem
  - There is no outstanding query after fake reply is accepted
  - So real reply will be discarded

DNSSEC (DNS Security Extensions)

- Extends DNS with new record types
  - RRSIG for digital signatures of records
  - DNSKEY for public keys for validation
  - DS for public keys for delegation
  - First version in ‘97, revised by ’05
- Deployment requires software upgrade at both client and server
  - Root servers upgraded in 2010
  - Followed by uptick in deployment

DNSSEC (2) – New Records

- As well as the usual A, NS records
- RRSIG
  - Digital signatures of domain records
- DNSKEY
  - Public key used for domain RRSIGs
- DS
  - Public keys for delegated domain
- NSEC/NSEC3
  - Authenticated denial of existence

DNSSEC (3) – Validating Replies

- Clients query DNS as usual, then validate replies to check that content is authentic
- Trust anchor is root public keys
  - Part of DNS client configuration
- Trust proceeds down DNS hierarchy
  - Similar concept to SSL certificates

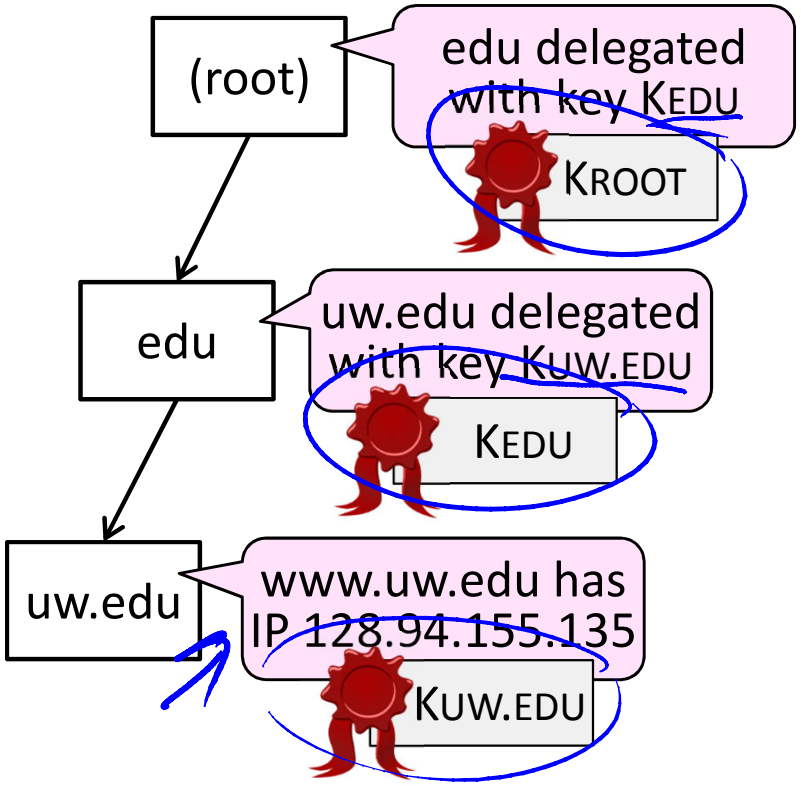
DNSSEC (4) – Validating Replies

Client queries www.uw.edu as usual

- Replies include signatures/keys

Client validates answer:

1. KROOT is a trust anchor
2. Use KROOT to check KEDU
3. Use KEDU to check KUW.EDU
4. Use KUW.EDU to check IP



DNSSEC (5)

- Other features too:
  - Authoritative answers a domain record doesn't exist (NSEC/NSEC3)
  - Optional anti-spoofing to bind query and reply
  - Flags related to deployment …

Takeaways

- DNS spoofing is possible without added security measures
  - Large problem in practice!
- DNSSEC adds authentication (only) of replies to the DNS
  - Using a hierarchy of public keys

END