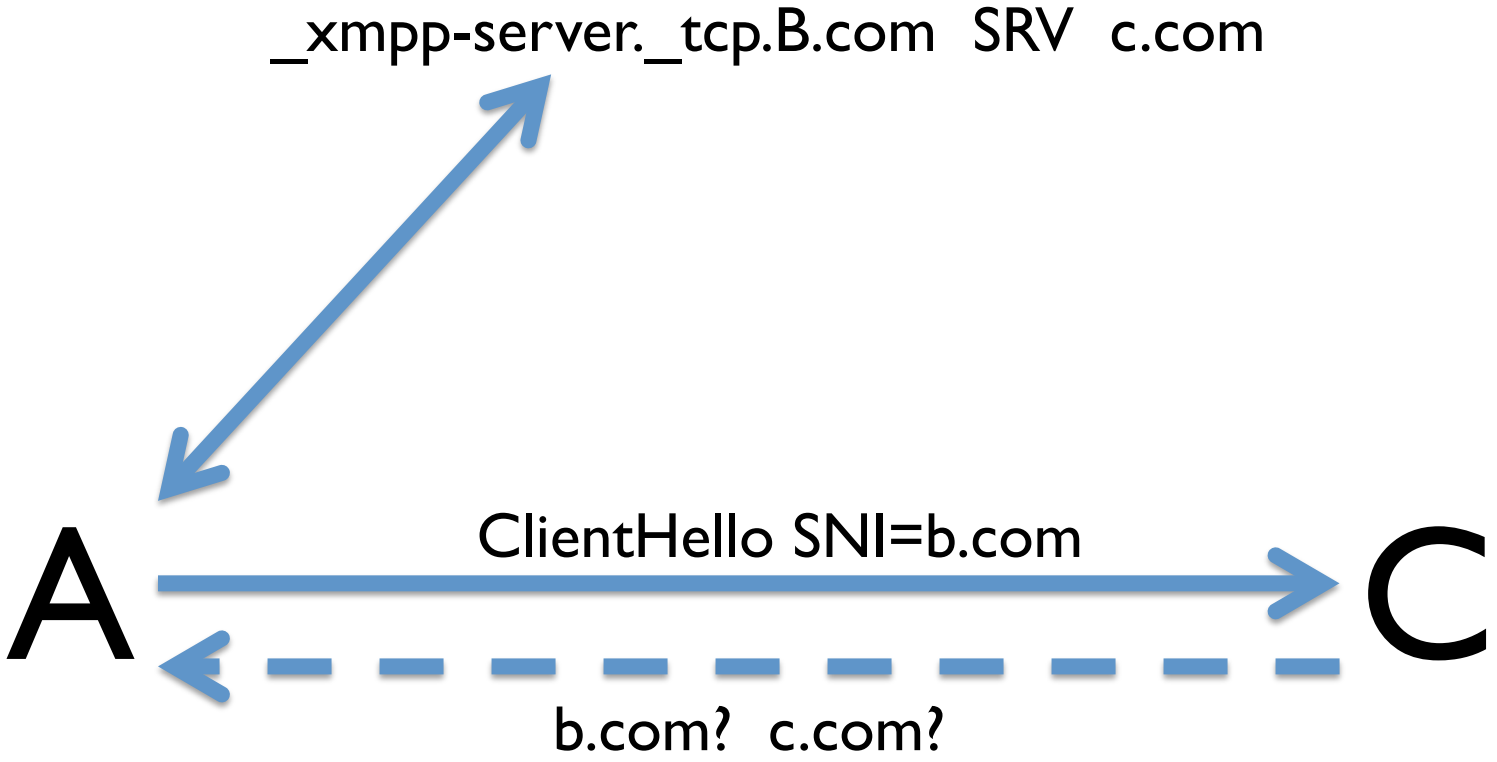
XMPP DNA

Outline

- What's the problem here?
- DNSSEC is the solution … ?
- If not DNSSEC, then … ?
- Where do we go from here?

XMPP Server Authentication



Current Requirements

- "The server certificate MUST be checked against the hostname as provided by the entity (client or server), not the hostname as resolved via the Domain Name System"
- Hosting providers can't hold customer certs
  - Too much responsibility; not allowed
- Two different channels for each src-dst pair
  - 10k domains on each side => 200M sockets

Basic problem

- Requirement to authenticate "human-entered" domain because redirect isn't authenticated
  - Don't know that B.com actually sent you the SRV, as opposed to some attacker
- Need a way for B.com to sign a statement of the redirection

DNSSEC!

- SRV is a DNS resource record
- DNSSEC is the way to sign DNS RRs
- If a client sees a signed SRV RR, then it is safe to authenticate the target domain

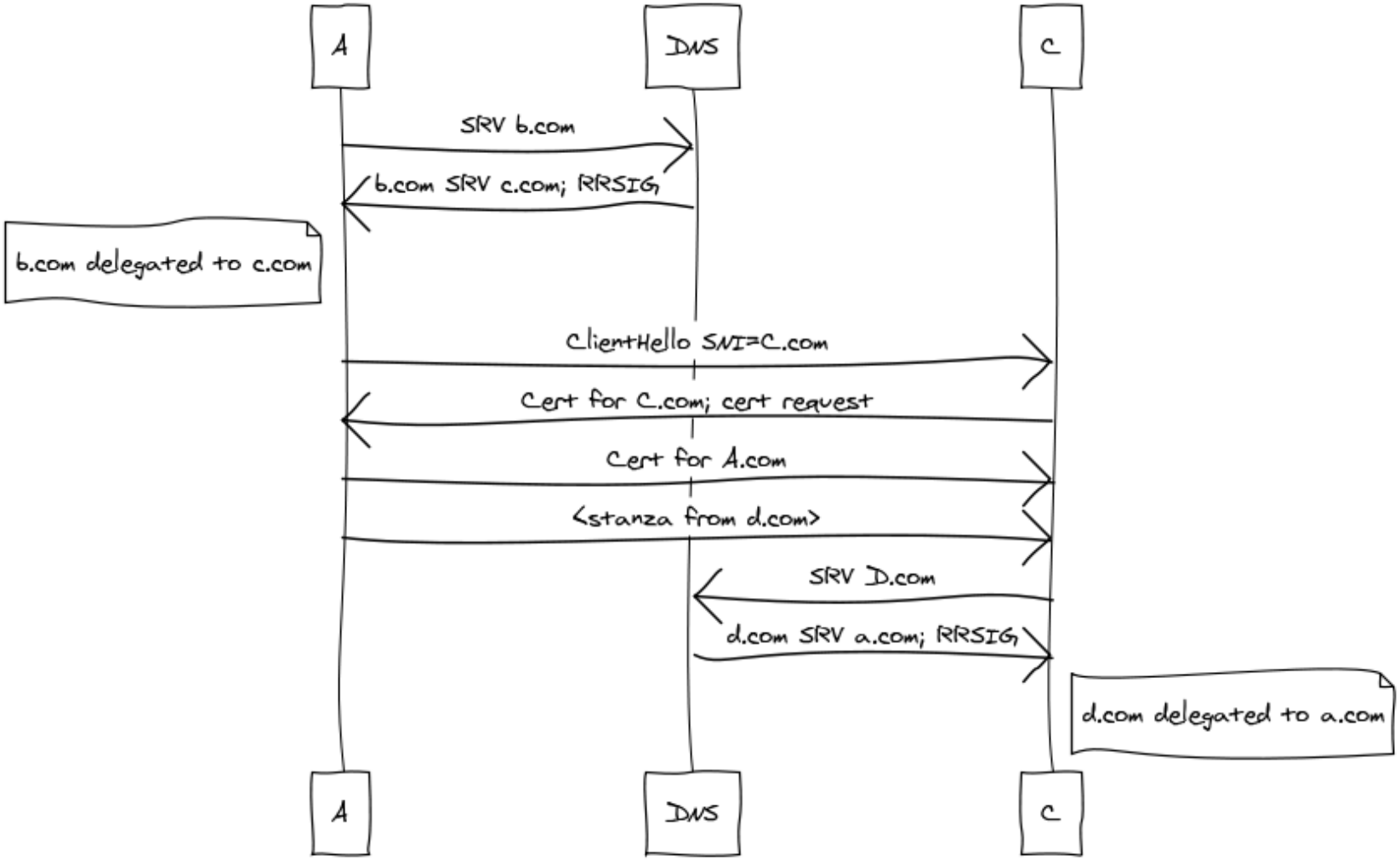
DNSSEC solution

- On establishing a connection:

```
if ((dNSName == srcName)
    ||(dnssec && (dNSName == dstName))) {
    /* SUCCESS */
} else { /* FAIL */ }
// Establish TLS, looking for authName
```

- Connection reuse: If we get a second redirect to the same name, re-use the connection

Mutual Authentication



DNSSEC challenges

- Need DNSSEC chains to trust anchors
  - Root now signed, com coming in March 2011
  - 45% of gTLDs, 18.5% of ccTLDs
  - Also have alternative trust anchors
- Customers have to provision DNSSEC

If not DNSSEC, then what?

- draft-barnes-xmpp-dna
- How do you encode the delegation?
  - DNS record, X.509 attribute cert, text, JSON, …
- How do you find the delegation?
  - DNS, HTTP, XMPP, …
- How do you trust the signing key?
  - DNSSEC, X.509, …

Non-DNSSEC Challenges

- Encoding: Either you have to use the signed thing for redirection or you have to compare across encodings
  - Use DNS record or re-invent SRV
- Discovery: When in the connection process do you find the signed delegation?
- Keys: Use domain certs?

What now?

- Does DNSSEC solve the problem?
  - Probably need to update RFC 3920 either way
- Is DNSSEC a practical solution?
  - Not deployed across all TLDs
  - Provisioning constraints
- If not DNSSEC, then what?