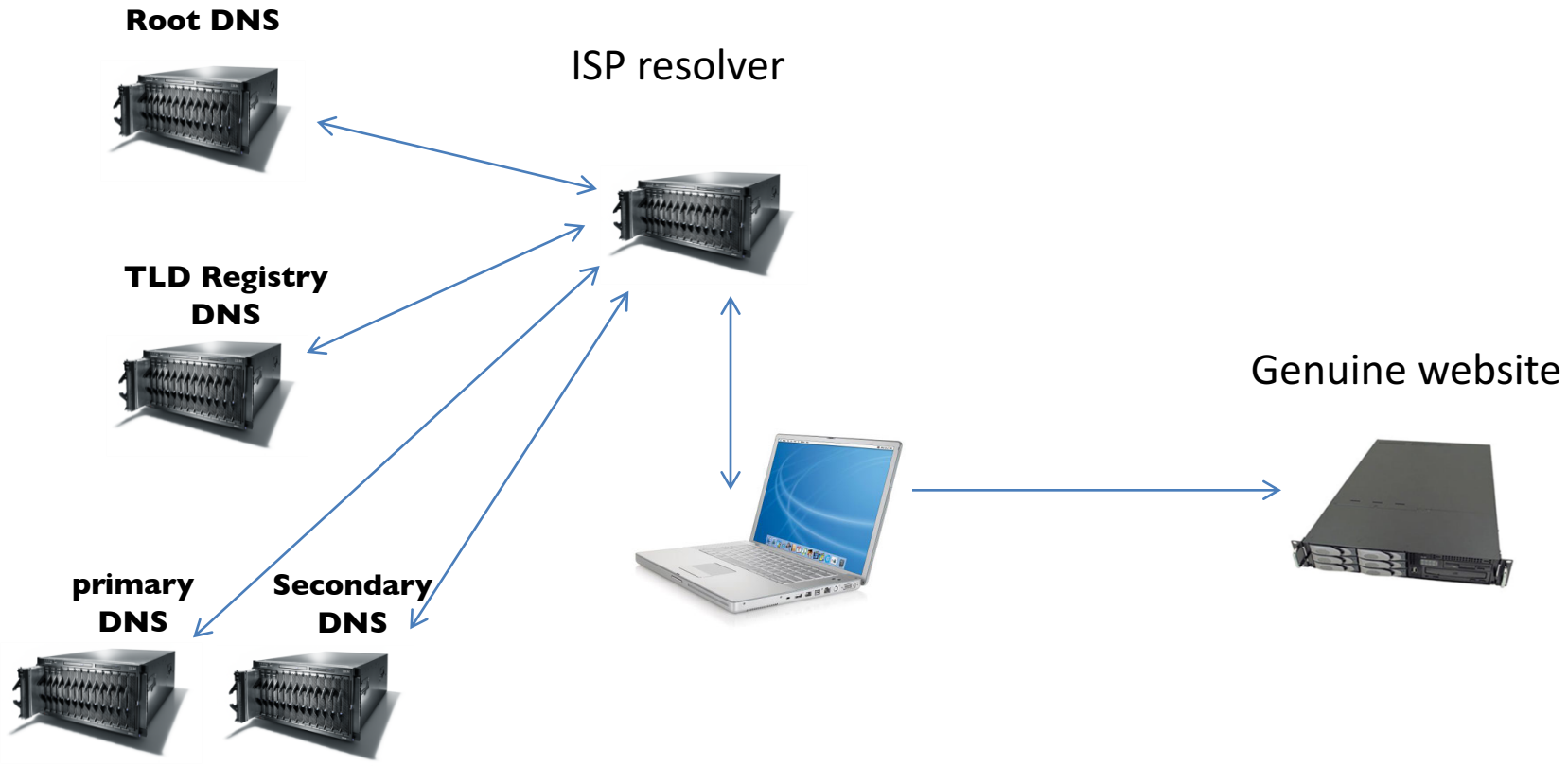
Introduction to DNSSEC

- Standard DNS
- Security concerns
- DNSSEC
- Advantage of DNSSEC
- Impact to embedded system
- Questions

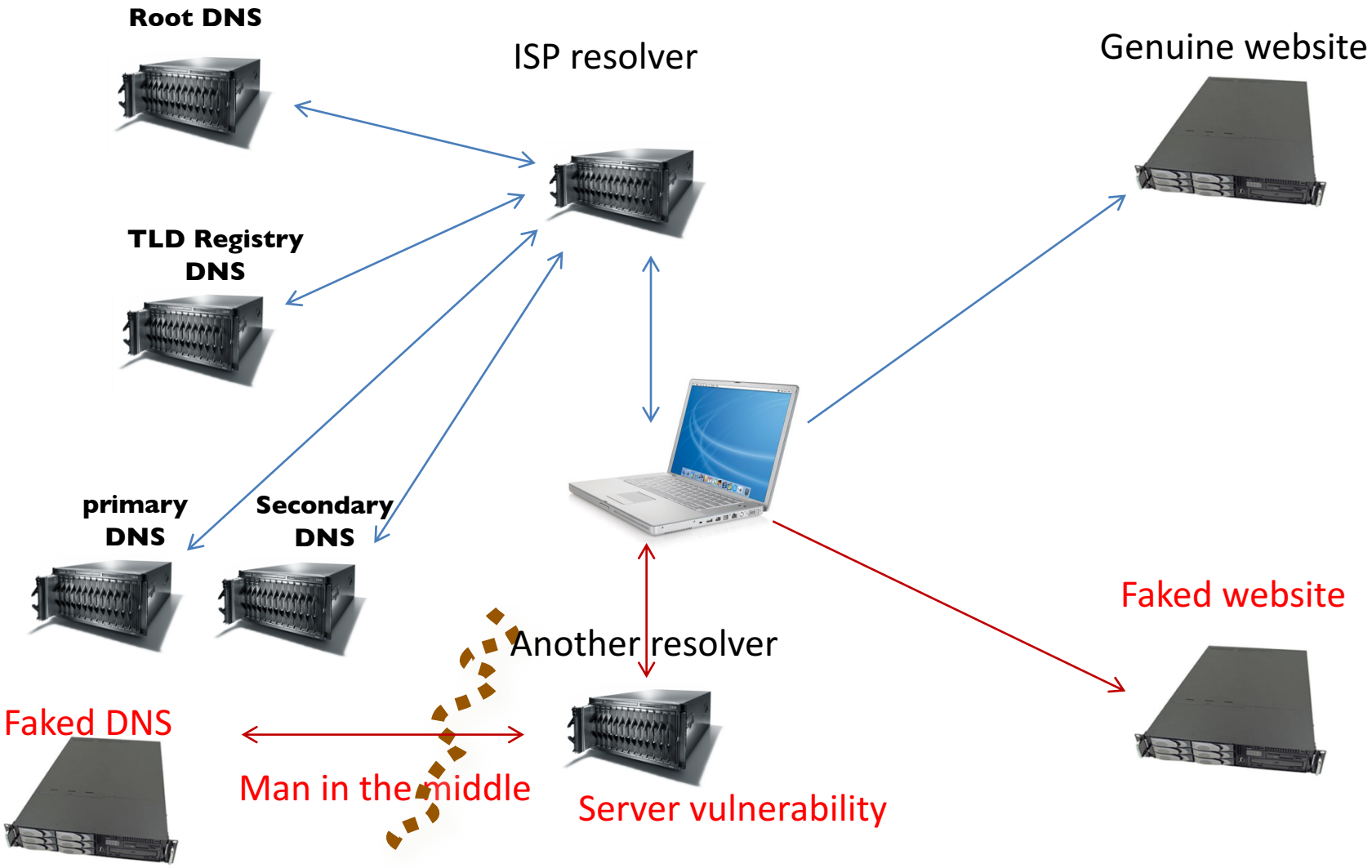
Standard DNS



DNS Security

- DNS has no security
- One UDP packet for query, one UDP packet for response
- The DNS data can be modified, causes your ISP's cache to have valid but wrong information
- Alteration of zone data - Impersonation of master/cache, which can be forged

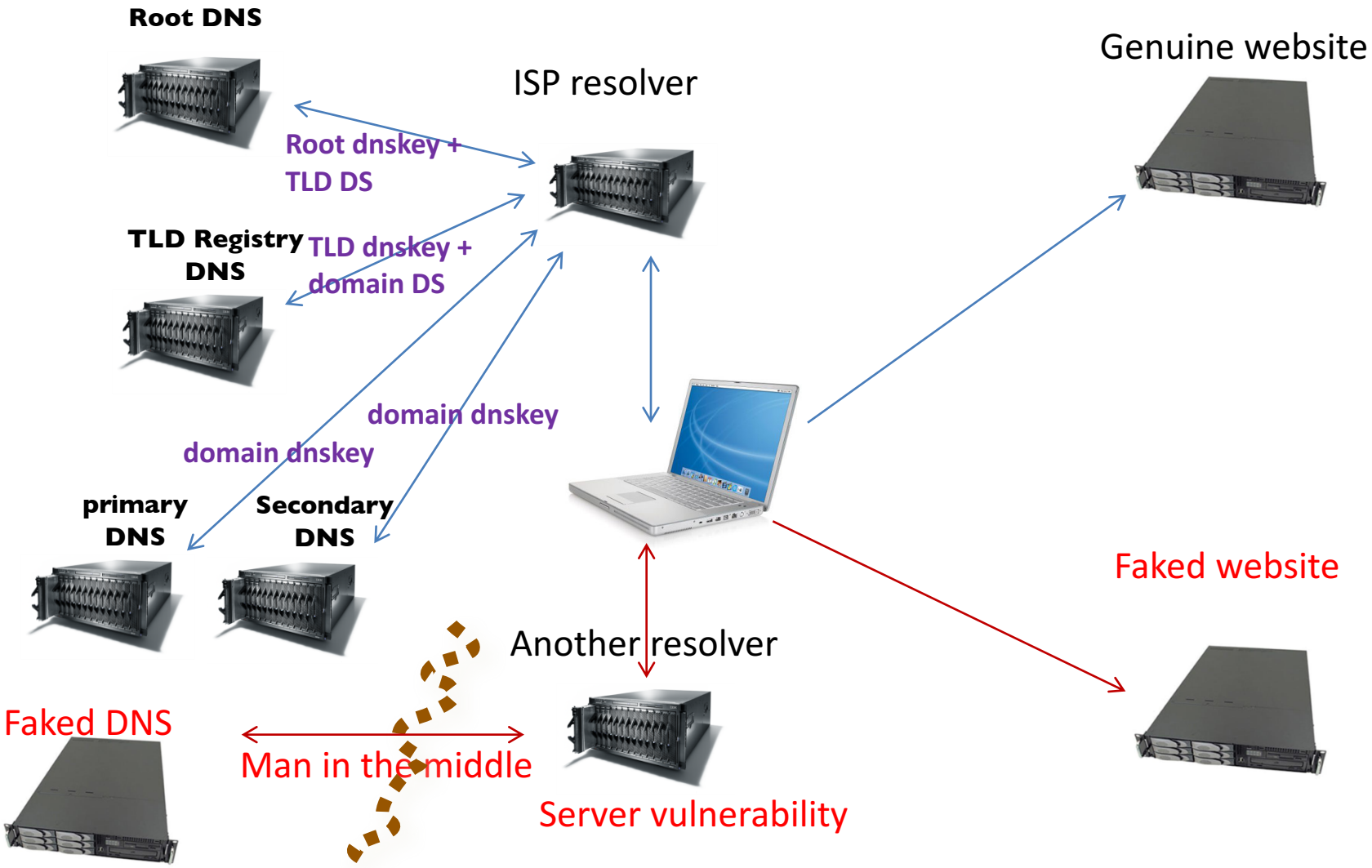
Security concerns



DNSSEC timeline

- 1993: Discussion of secure DNS begins
- 1994: First draft of possible standard published
- 1997: RFC 2065 published (DNSSEC is an IETF standard)
- 1999: RFC 2535 published (DNSSEC standard is revised)
- 2005: Total rewrite of standards published
  - RFC 4033 (Introduction and Requirements)
  - RFC 4034 (New Resource Records)
  - RFC 4035 (Protocol Changes)
- July 2010: Root zone signed
- July 2010: .edu signed
- Dec 2010: .net signed
- Mar 2011: .com signed

DNS integrity with DNSSEC



What DNSSEC does

- DNSSEC uses public key cryptography and digital signatures to provide:
- Data origin authentication

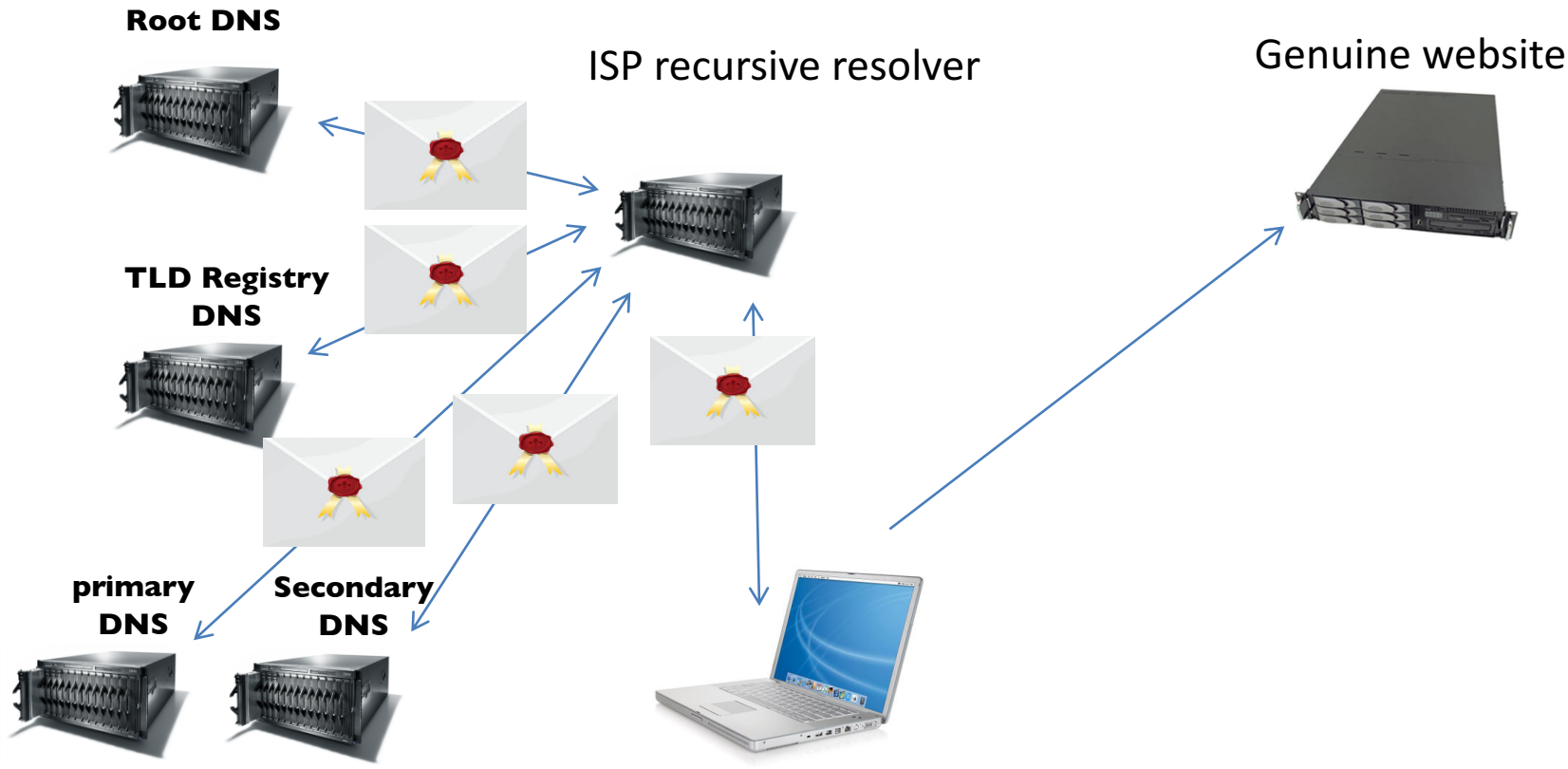
  “Did this DNS response really come from the zone?”
- Data integrity

  “Did an attacker (e.g., a man-in-the-middle) modify the data in this response since it was signed?”

What DNSSEC doesn’t do

- DNS records has no encryption, data in DNS is public
- Ordinary resolver can lookup DNS record from DNSSEC zone
- Address attacks against the name server itself
- Not solution for denial of service

DNSSEC


Root DNS
ISP recursive resolver
Genuine website
TLD Registry DNS
primary DNS
Secondary DNS

Chain of trust in DNSSEC

- There are no certificates in DNSSEC
- The trust model is rigid
- The chain of trust flows from parent zone to child zone
- Only a zone's parent can vouch for its keys' identity

Example of chain of trust

We are looking up A records for www.isc.org .

- Trust anchor for root zone KSK Ⓟ
- Statically configured in the DNSSEC validator
- root KSK Ⓟ root ZSK Ⓟ .org DS Ⓟ
- In the root zone
- .org KSK Ⓟ .org ZSK Ⓟ isc.org DS Ⓟ
- In the .org zone
- isc.org KSK Ⓟ isc.org ZSK Ⓟ

www.isc.org A

Advantage of DNSSEC

- Protecting applications against DNS spoofing attacks
- Recursive name servers will perform DNSSEC validation and throw away bad data before it reaches clients
- Eventually some stub resolvers and even applications may do their own DNSSEC validation

Impact to embedded system

- Increase of DNS traffic
  - Short question sent and long answer replied
  - System capacity planning
- Applications do their own DNSSEC validation may cause other issues.
  - e.g email delivery, it is possible to reject email inbound