DNSSEC Apps

Remind me again why we are doing this DNSSEC stuff

Ron Aitchison

ICANN - Singapore - March 2014

DNSSEC's Purpose

- Classic RFC Stuff
  - Authenticated - Authoritative source
  - Integrity - Data is unmodified
  - PNE - Negative responses correct
- So what....

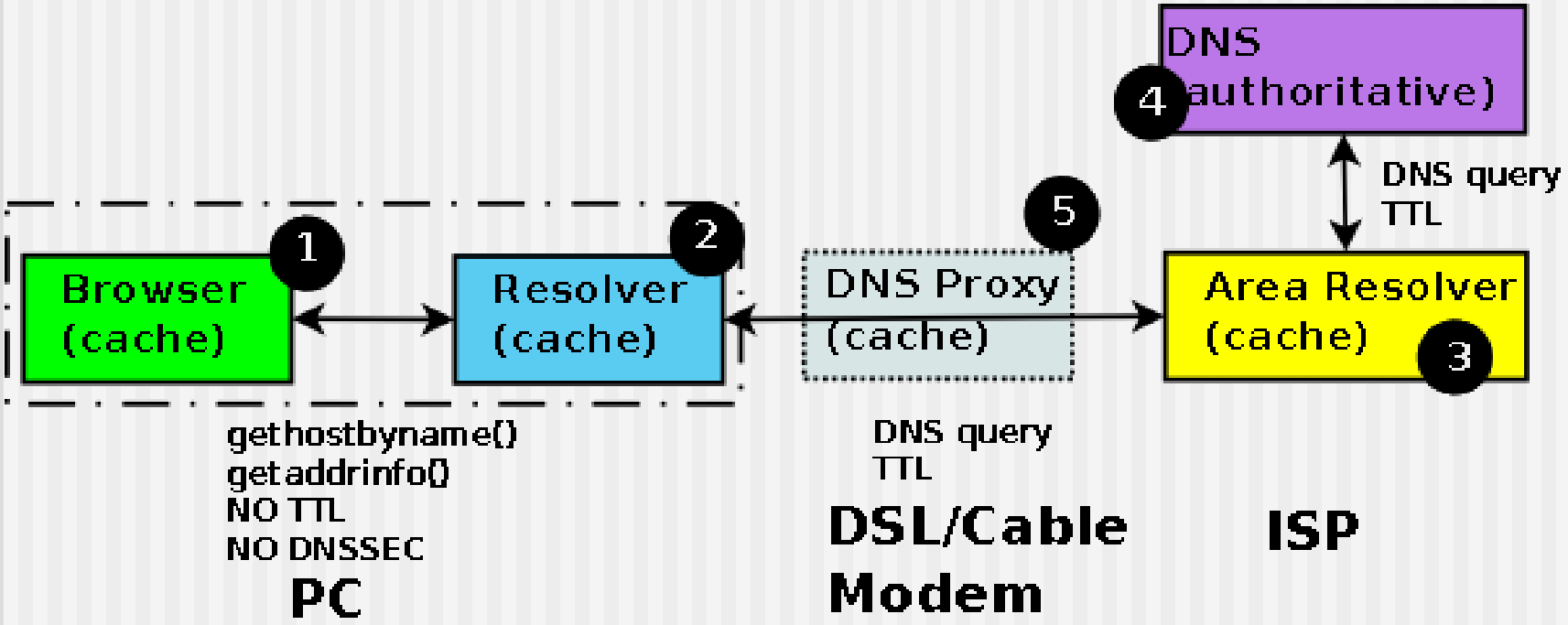
DNSSEC's Purpose

- Classic RFC Stuff Response
  - Authenticated - Data from authoritative source
  - Integrity - Data is unmodified
  - PNE - Negative responses correct
- So what....
  - 'cos applications can use the results
    - Browsers, Mail, LDAP clients etc.
- Which means...

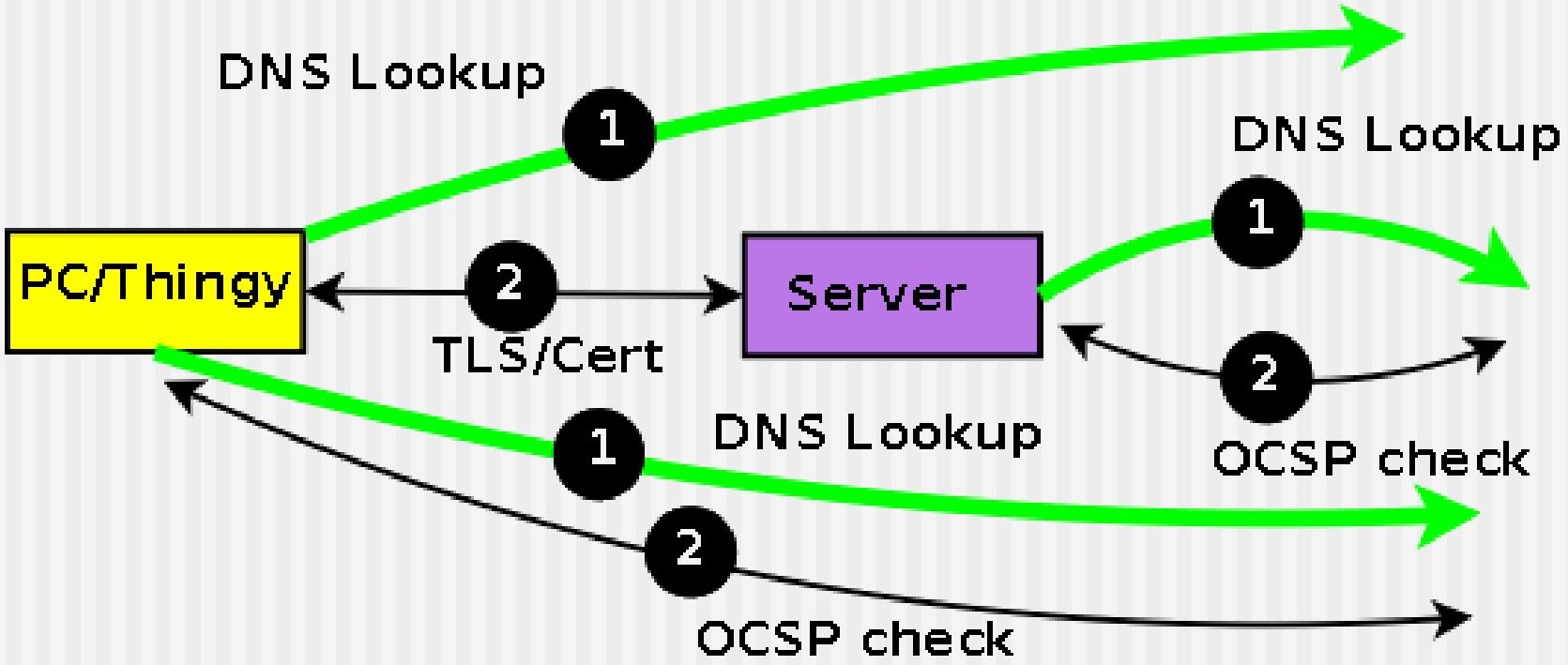
If we have....

- DNSSEC-aware API
  - POSIX, MS
  - Capable of signalling secure/insecure status
- What can we do?
  - If secure - We know it came from the right place
  - If secure - We can trust all DNS data
- So.....

DNS Journey


DNS
authoritative)
4
DNS query
TTL
5
1
2
Browser
(cache)
Resolver
(cache)
DNS Proxy
(cache)
Area Resolver
(cache)
3
gethostbyname()
getaddrinfo()
NO TTL
NO DNSSEC
PC
DNS query
TTL
DSL/Cable
Modem
ISP

The First Step - Always



DNSSEC - It's a new world

- Get Public Keys from secure DNS
  - TLS - X.509 replacement
  - OE made easier/possible?
  - Personal Digital Signatures
- Other Data in DNS
  - RR Proliferation
  - Easier RR registration

TLS - X.509 Replacement

- X.509 is just a method to get public key
  - DH, DANE etc.
- EV comparable
  - Not another color on browser bar?
  - OCSP not needed
- Wrinkles:
  - TLS cipher suite negotiation (client requests)

Opportunistic Encryption

- Mail/Web/chat etc.
- TLS Encryption currently driven by server (easy to snoop/subvert)
- TLS Encryption driven by user
- Where do we place the public keys
  - DNS?
  - Wrinkles:
    - Structure (ENUM/ccTLD)
    - Private Key - Where/What

Personal Digital Signatures

- ENUM/ccTLD structure
- Ownership/Governance Issues
- Private Key - Where/What

DNSSEC Apps

- Apps are the reason for DNSSEC
- Missing key element - DNSSEC API
  - Surprise - No DNSSEC Apps
- No shortage of imagination
  - But lots of vested interests

Thanks for your patience