What DNSSEC is.
And what it isn't.

Paul Ebersman - Neustar
paul.ebersman@team.neustar
NANOG 76 – DC 10-12 Jun 2019

DNS Basics

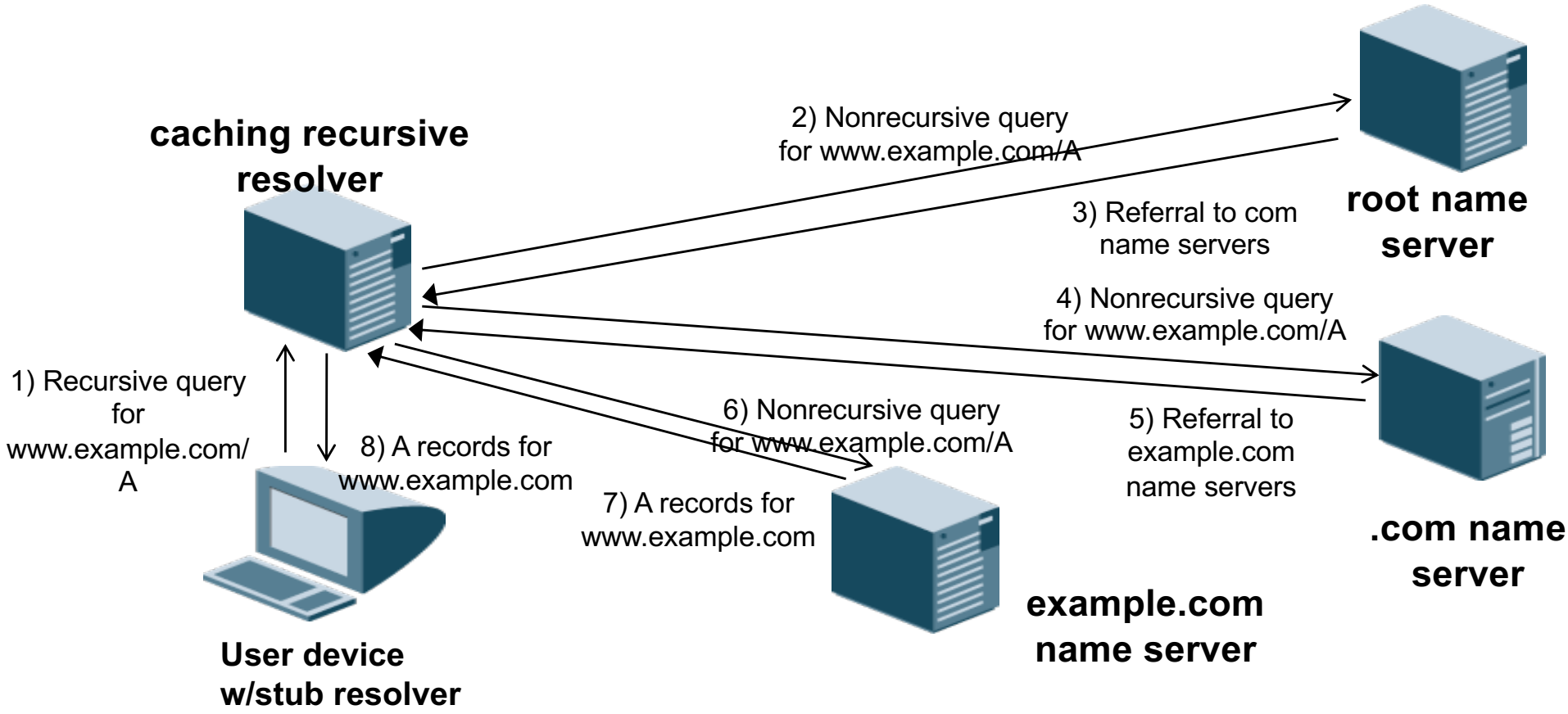
ROLES

- DNS Zone Owner: actual company/organization owning domain name
- DNS Operator: runs the public authoritative servers for a domain name
- Registrar: reseller of domain names withinTLDs (Top Level Domains), sometimes also DNS operator
- Registry: usually TLD operator for TLDs, like .BIZ or .COM

TYPES OF DNS SERVERS/SOFTWARE

- Stub resolver: usually the operating system of the user device, just asks upstream recursive resolver for answers
- Recursive resolver: does all the work of asking all authoritative resolvers needed to get answer to question from stub resolver. Usually also caches answers to improve performance
- Authoritative server: has the full zone data for whatever domains for which it's authoritative

RECURSION QUERY FLOW



DNS Security Problems

TYPICAL DNS ATTACKS

- DoS (Denial of Service)
- Cache poisoning
- False authoritative servers
- Modifying zone data

RESULTS OF ATTACKS

- No answer at all
- Fake sites:
  - Disclosure of login credentials
  - False data given
  - Eavesdropping on sensitive communications

DNSSEC Basics

DNSSEC BASICS

- Public-key/asymmetric encryption
- Private keys kept secret/secure
- Zone data and delegations digitally signed w/private key
- Public keys published in the DNS
- DNS query results validated using public key
- Validation failure results in no answer

What does DNSSEC solve?

BASIC SECURITY CONCEPTS

- Confidentiality
- Integrity
- Availability

WHAT DNSSEC DOES SOLVE

- Integrity
  - Cache poisoning
  - False authoritative servers

What doesn't DNSSEC solve?

WHAT DNSSEC DOESN'T SOLVE

- Confidentiality
- Availability
- Correct DNS data
- Parent zone security

Case Studies

DNS HIJACKING INCIDENTS

- Brazilian bank Oct 2016
- WikiLeaks Aug 2017
- MyEtherWallet Apr 2018
- DNSpionage 2018

BRAZILIAN BANK

- How was attack done:
  - changed recursive resolver consumer routers used
  - fake DNS recursive resolver gave A record for false website
  - fake website stole user credentials for bank accts
- What did this mean:
  - user/consumer acct money stolen
- Remediations:
  - current patches for routers
  - DNSSEC (if user devices had validating stub resolvers)
  - regular searches for bad/malicious SSL certs

WIKILEAKS

- How was attack done:
  - appears DNS administrator account hacked and A record for website changed
  - fake website at that new address
- What did this mean:
  - appeared to be a website defacement
- Remediations:
  - secure DNS admin account credentials better
  - DNSSEC if NS/DS in parent checked regularly and changes alerted

MYETHERWALLET

- How was attack done:
  - BGP hijack of AWS address space
  - set up fake DNS servers giving fake web site A record
  - web site certificate failed but users clicked through
- What did this mean:
  - crypto currency credentials stolen, crypto currency then stolen
- Remediations:
  - RPKI to secure BGP announcements of DNS servers
  - DNSSEC (false web site A records wouldn't validate)
  - regular searches for bad/malicious SSL certs

DNSPIONAGE

- How was attack done:
  - EPP credentials found in previous attack
  - NS (but not DS) records changed four one-hour periods
  - False web cert from Comodo
  - DNS changes to web/mx hosts to phish for domain acct credentials using false web site/cert
  - fake IMAP site to steal registry/registrar credentials
  - email/vcard/vcal info stolen
  - customers of registry/registrar login credentials stolen
- What did this mean:
  - able to do surveillance of multiple govt agencies with email/domain login credentials

- Remediations:
  - more frequent monitoring of DNS changes
  - Walking full DNS chain for NS/DS changes
  - registry/registrar locks
  - multifactor auth for logins
  - disable direct IMAP access from internet
  - MDM on phones to disable resolver changes
  - DNSSEC (one registry only vulnerable via 2 employees travelling and forced to use hotel non-DNSSEC-validating resolvers)
  - regular searches for bad/malicious SSL certs
  - DANE for certs

What can you do?

All the things you should everywhere else in InfoSec…

Such as…

CREDENTIALS SECURITY

- Use strong passwords
- Don’t re-use passwords
- Use a password manager
- Use multifactor authentication
- Phishing training for staff
- Use role or company only emails for recovery emails
- Regularly audit access and accounts

AUDITING AND LOGGING

- Monitor your DNS servers and parent zone servers for NS/DS changes multiple times per hour
- Monitor key records/services, such as MX, A/AAAA for critical services
- Alert on critical or unexpected changes

- Regularly check your SSL certs for unexpected certs
- Check Certificate Transparency Logs
- Use stronger than “the credit card worked” validation of identity cert providers for your critical sites
- Use ACLs or VPN to your critical internal servers

DNS SPECIFIC

- Enable DNSSEC validation on all your recursive servers
- DNSSEC sign all your zones
- Use registry locking for critical zones

Q & A

Thanks!

Further Reading

FURTHER READING

- ICANN DNS security tips: https://www.icann.org/news/announcement-2019-02-15-en
- ICANN SSAC docs 40, 44, 74:https://www.icann.org/groups/ssac/documents
- DNSpionage article:https://krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-dns-hijacking-attacks/

FURTHER READING

- Talos DNSpionage blog: https://blog.talosintelligence.com/2019/04/dnspionage-brings-out-karkoff.html
- Talos SeaTurtle blog: https://blog.talosintelligence.com/2019/04/seaturtle.html
- Oilrig APT/DNSpionage article: https://securityaffairs.co/wordpress/84418/malware/oilrig-apt-karkoff-dnspionage.html