RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: BAC-W10

Hacked By Crypto

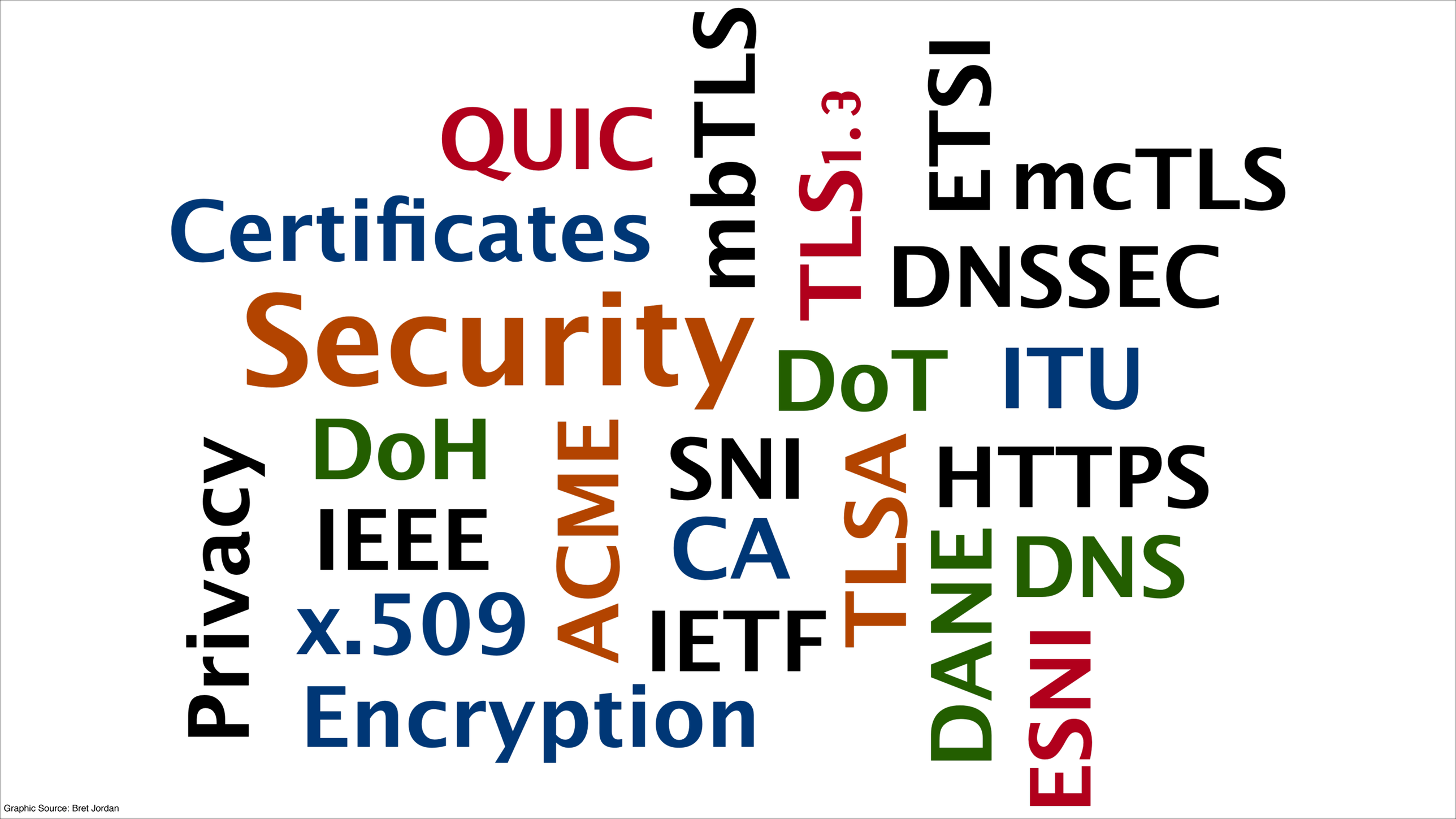
Bret Jordan, CISSP
Director, Office of the CTO
Symantec

Agenda

- Winds of Change - Protocol Evolution
- 3:00 AM - Wake Up Call
- What Now?
- Conclusion

RSA Conference 2019

Winds of Change - Protocol Evolution

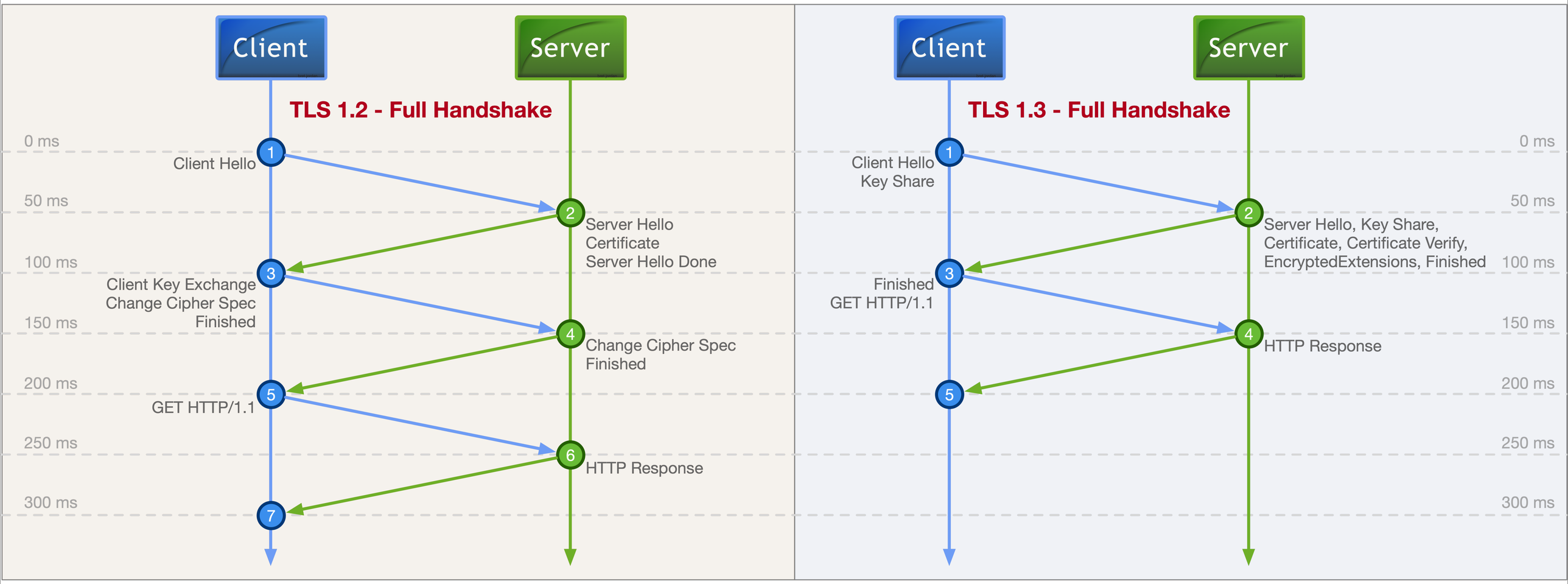


Graphic Source: Bret Jordan

TLS 1.3 - RFC 8446 / Aug 2018

- Enhanced Security
  - Removed older broken crypto
  - Removed vulnerable TLS 1.2 configuration options
  - Restricted to Perfect Forward Secrecy (PFS) based Ciphers
- Reduced latency with improved performance and speed
  - TLS handshake only requires 1 round trip now instead of 2
  - Each roundtrip can add 100-300 ms, mobile networks add more

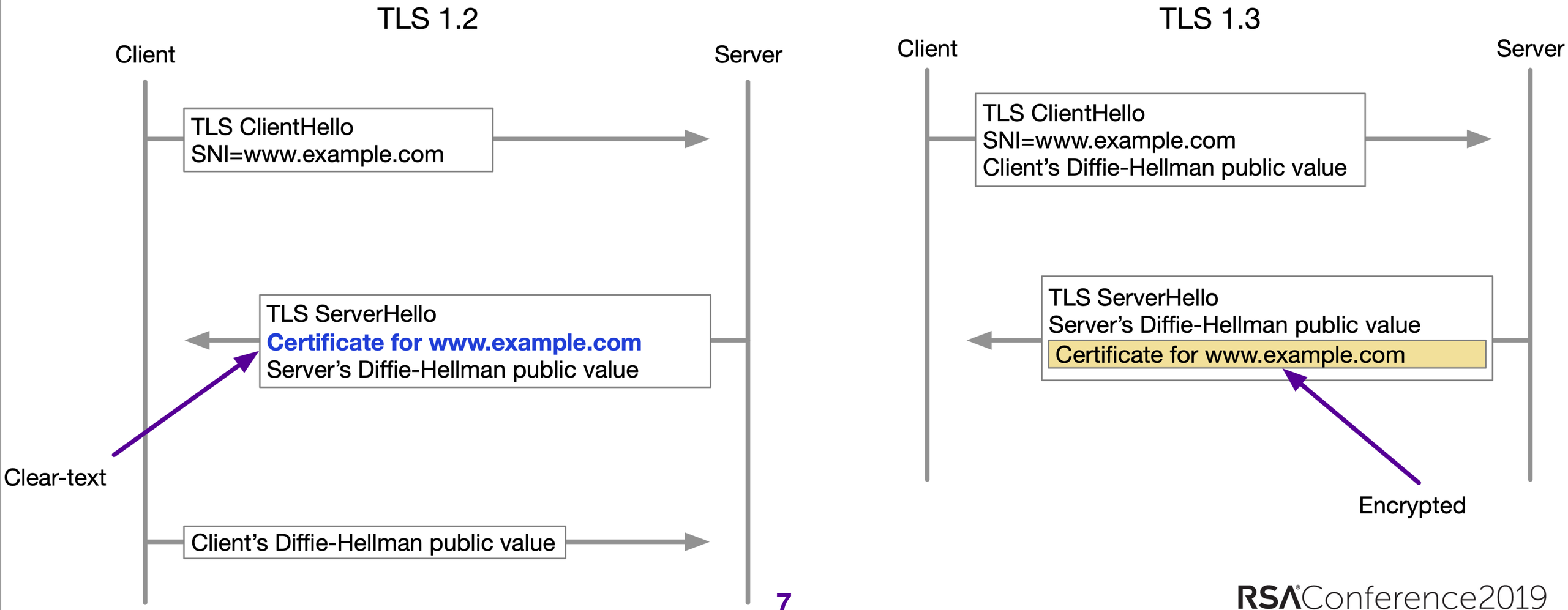
TLS 1.2 vs 1.3 Handshake Performance



Graphic Source: Bret Jordan

TLS 1.3 - Potential Complication

- Server certificate is now encrypted

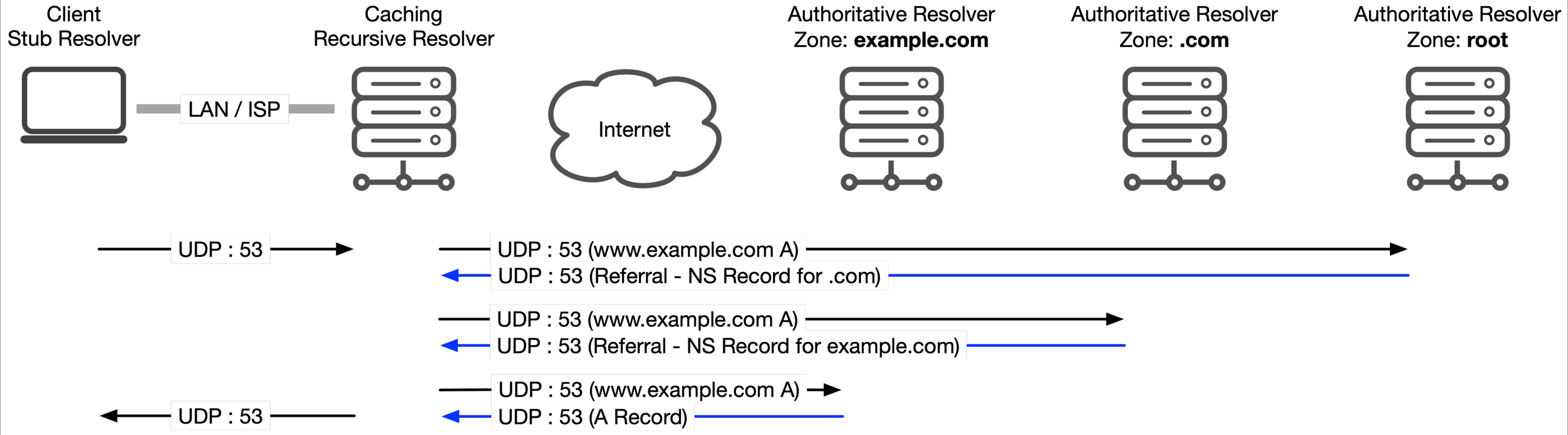


Graphic Source: Bret Jordan

TLS 1.3 - Potential Complications

- Policy-based bypass is limited and less reliable
  - SNI can no longer be validated against server certificate
  - Server certificate can only be validated with full TLS termination
  - Harder to prevent phishing, stage 1&2 malware delivery, data exfiltration, and fraudulent transactions
  - Harder to prevent data leakage & industrial espionage
- URL categorization is limited to client provided SNI and IP addresses (however, SNI can be faked)
- No static RSA support for in-the-datacenter offline decrypt

DNS - Standard Query

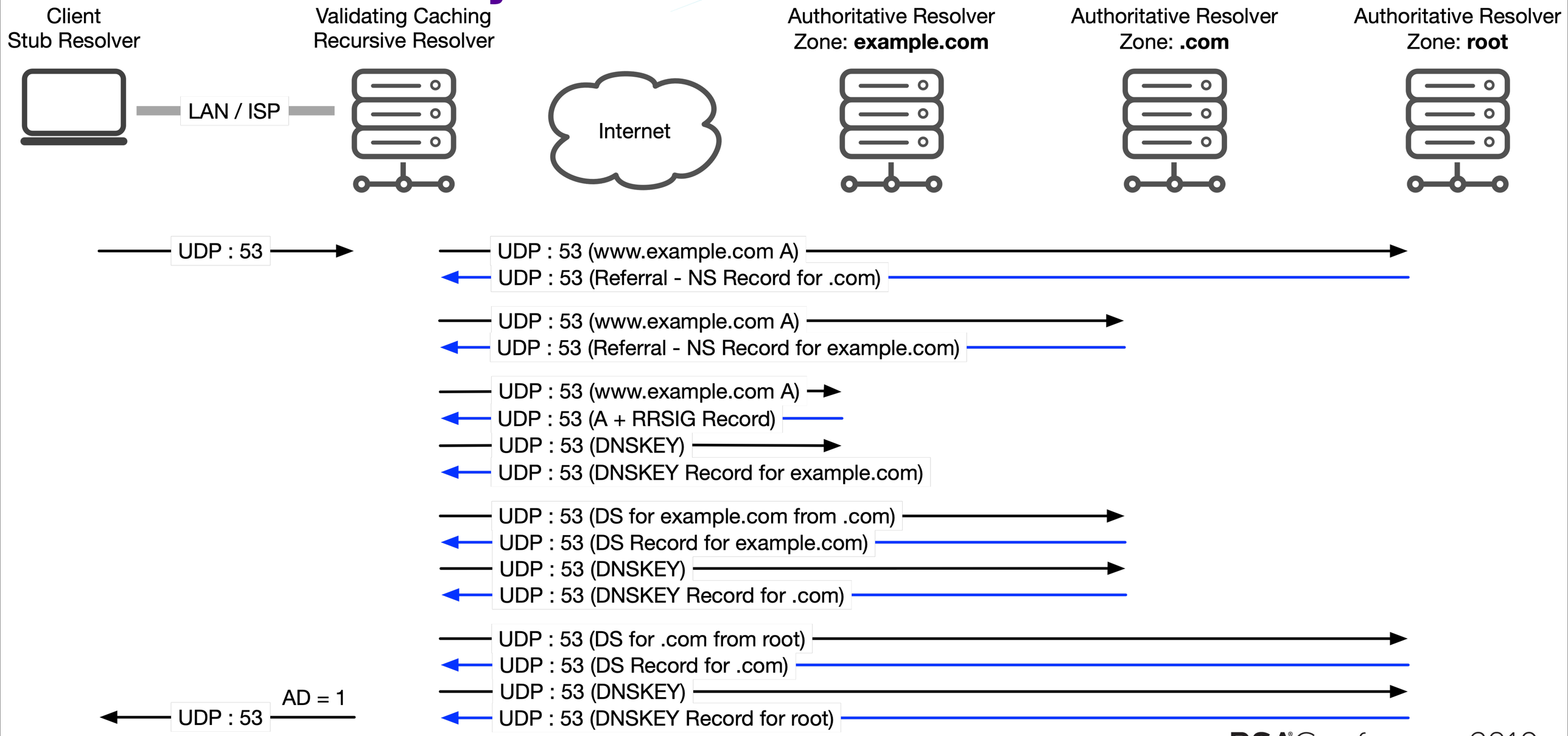


Graphic Source: Bret Jordan

DNS Security (DNSSEC) - RFC 4033, 4034, 4035

- Performed between trusted caching recursive resolver and rest of DNS world
- Provides assurance that the response is correct and current
  - It does not encrypt or hide DNS data (queries or responses)
  - “Last Mile” has to trust the AD bit in the response header
- Some endpoints are starting to add support for DNSSEC
  - Tools exist to add this to various endpoint operating systems
- Some queries/responses will need to use TCP due to size

DNSSEC Query



Graphic Source: Bret Jordan

DNSSEC - Potential Complications

- By itself, DNSSEC is a good thing
- As DNSSEC functionality moves to the endpoint, it may become harder to perform some network controls like:
  - Content filtering
  - Malicious site blocking

DNS-Based Authentication of Named Entities (DANE) - RFC 6698

- Enables mail servers to provide seamless mail encryption
- Allows verification of certificates received over HTTPS for added security
- Enables delivery of a server's certificates via DNS
  - No longer needs public Certificate Authorities
  - Requires DNSSEC
  - Self-signed certificates work just fine
  - Requires no change to the TLS server (Website)
  - Only requires a TLSA Record in the DNS Server

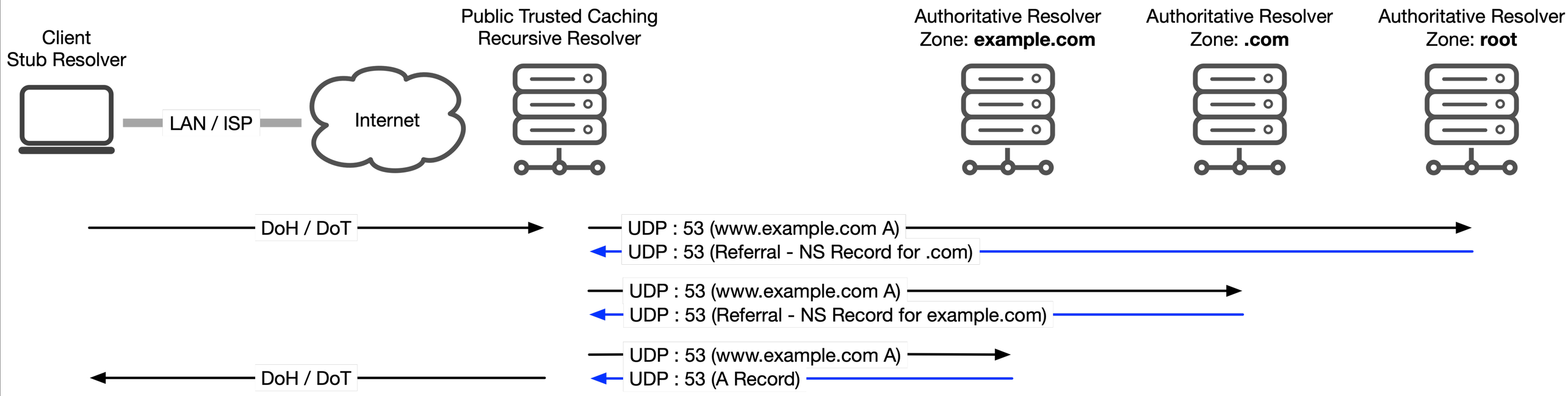
DANE - Potential Complications

- DANE combined with DNSSEC could potentially enable certificate “pinning”
- Prevent locally installed Root CAs from being effective
  - Increases the challenges to maintain regulatory compliance
- Breeds bad behavior with end users as certificate warnings become more common
- Organizations may need to build an island of trust for DNSSEC so they can rewrite TLSA records on the fly

DNS over HTTPS (DoH) - RFC 8484 / Oct 2018

- No longer over UDP/TCP 53 from client to resolver
- DNS queries and responses are encrypted in the HTTPS session
  - No more visibility from the network
- DNS resolution can be done within the browser
  - May not use OS configured DNS servers
- DNSSEC is still needed
- Another variant is DNS over TLS (DoT)

DoH / DoT



Graphic Source: Bret Jordan

DoH - Potential Complications

- Careful configuration is needed to ensure local DNS queries are not leaked to the outside world
- Increased difficulty with filtering a DNS response
- Ability to filter sites at the DNS server may not work
- Limited retrospective forensics capabilities
- The DNS server may now be outside the enterprise
  - Even if it could technically provide filtering the DNS server may be owned or managed by an entity other than the enterprise
- Organizations may need to implement their own DoH servers

Opportunistic DoH

- Currently under development in the IETF
- Websites can “server push” DNS records to a client
  - Done before the client requests them
  - Server determines what it thinks the client might need next
- Increased difficulty with the verification and removal of malicious DNS entries pushed from a compromised website
  - Could be a great attack vector for threat actors once they compromise a site

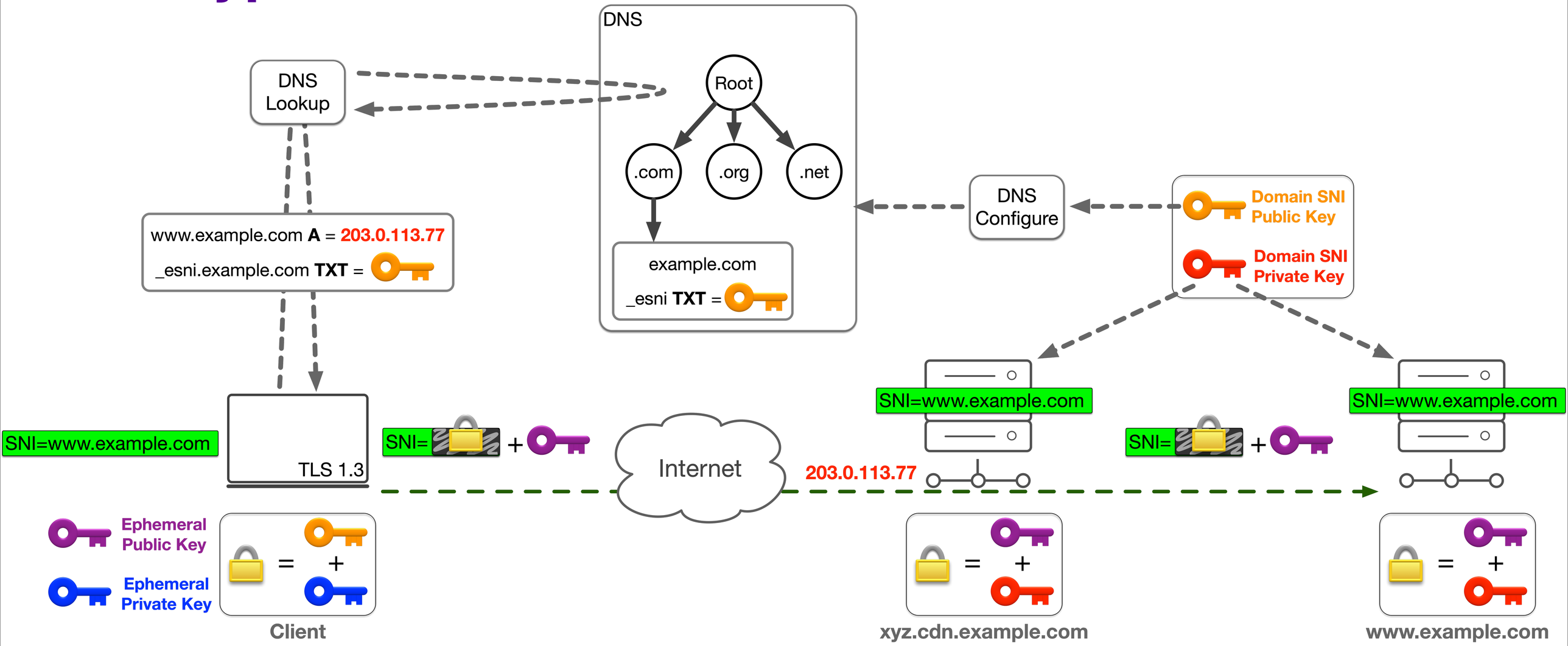
Server Name Indication (SNI) - RFC 6066

- SNI is used to help route traffic to the correct site
  - Where multiple HTTPs servers are sharing a single IP address
- SNI can expose where a client is going even with TLS 1.3

Encrypted SNI (ESNI)

- Currently under development in the IETF
- Purpose is to hide where a client is going
  - This may help protect privacy in some situations
  - Will hurt operational security everywhere
  - Repressive nation states may just prevent its use or side step it anyway
- Only for TLS 1.3 and above
  - Does not make sense for earlier versions as the server certificate is in plain text
- Really requires DoH or DoT to be useful
  - Otherwise one could just monitor the plain-text DNS traffic

Encrypted SNI

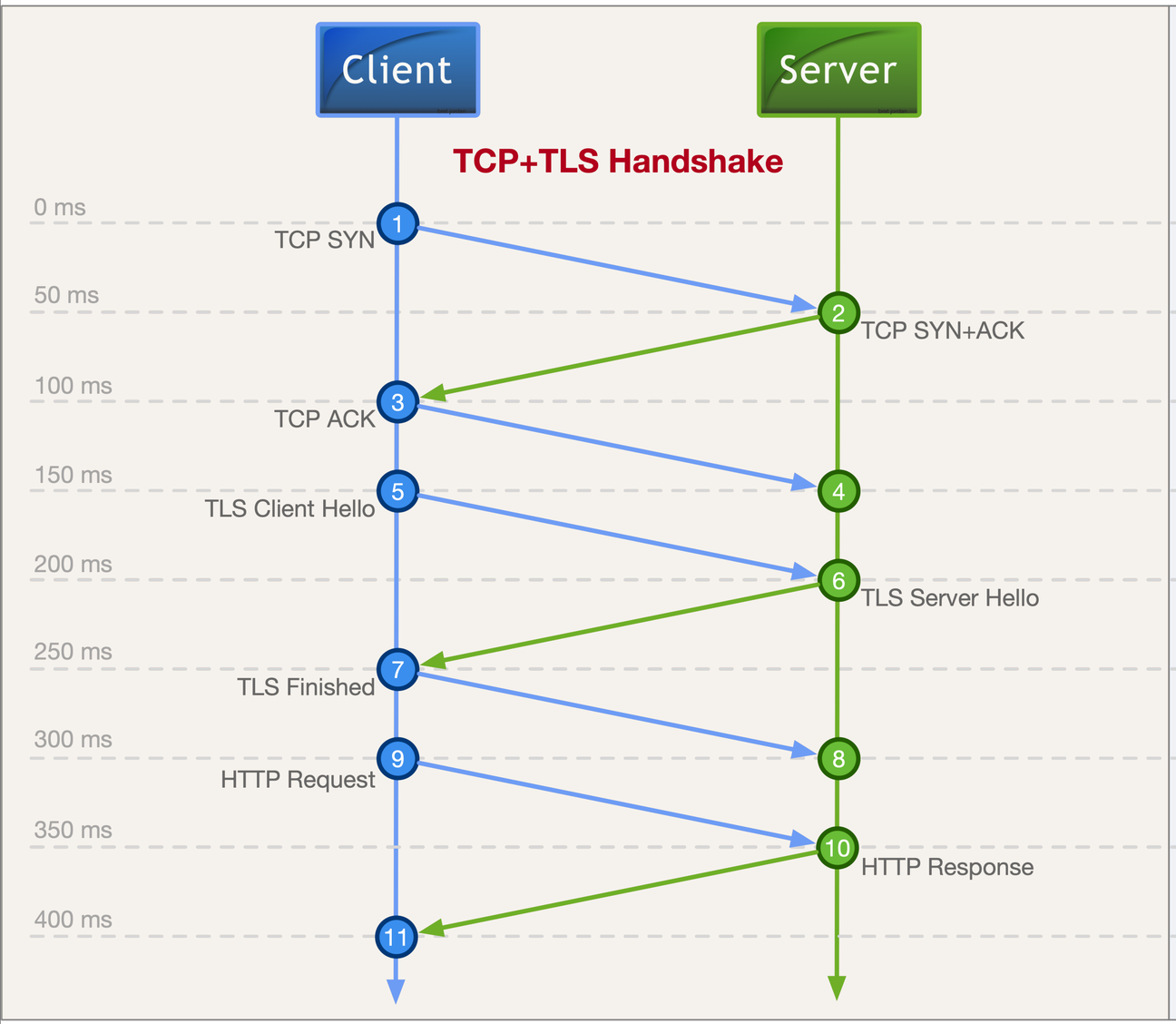


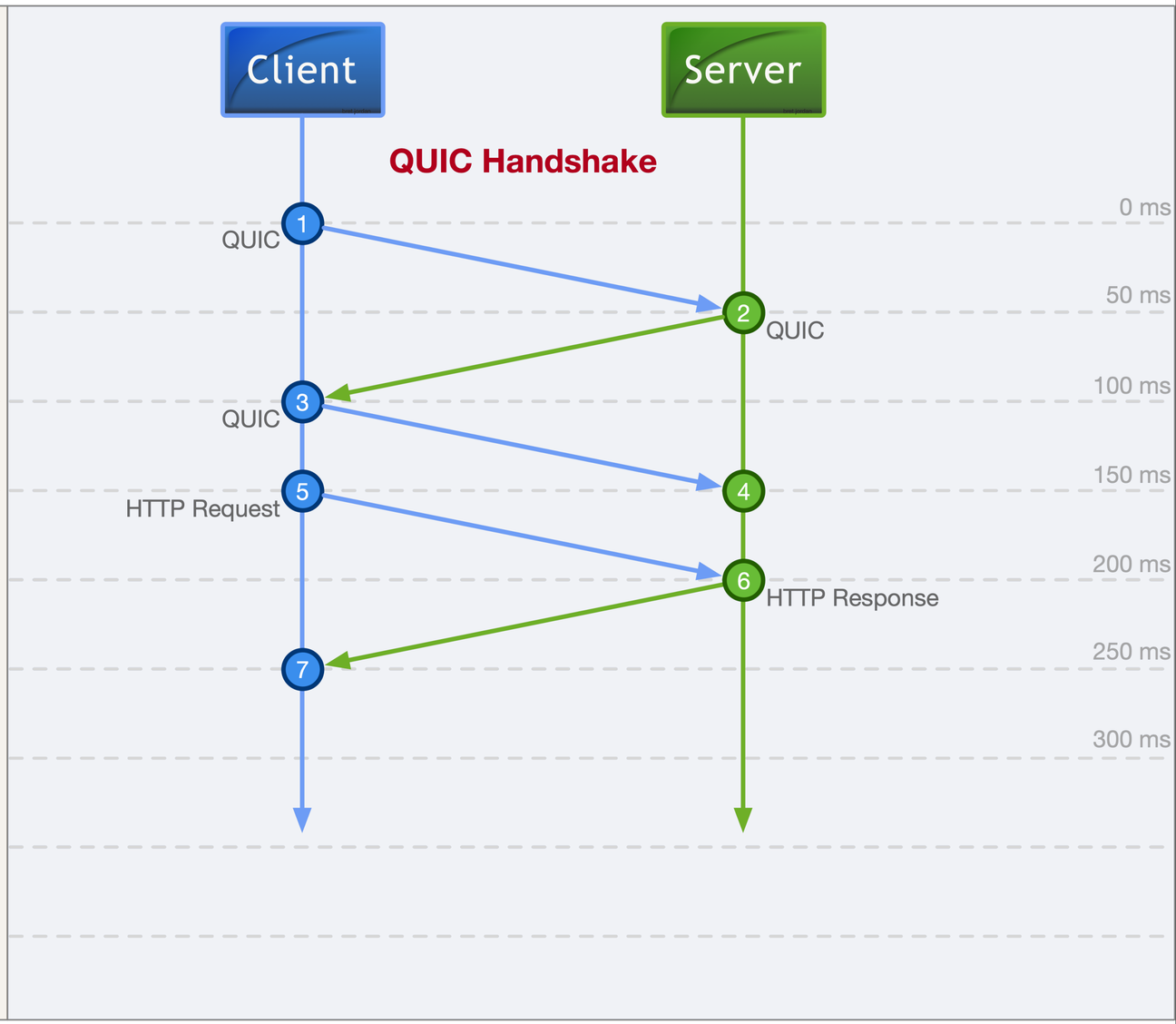
Graphic Source: Bret Jordan

QUIC (Quick UDP Internet Connections)

- Currently under development in the IETF
- Replaces TCP, all traffic over UDP 443
- TLS 1.3 used for key exchange
- Big performance advantages for web apps
- Routes HTTP streams across independent QUIC transport streams in a single QUIC connection
  - Solves head-of-line blocking problem of HTTP2
- QUIC is done in user space

QUIC





Graphic Source: Bret Jordan

QUIC - Potential Complications

- No TCP state to help network devices like firewalls
- All done in user space
  - Potential attack vector for threat actors
- All protocol controls are in the QUIC layer, no more TCP meta-data
  - Sequence number, performance monitoring, congestion analysis
  - Identify poorly performing applications at the network level
- NAT devices do not handle UDP very well
  - Load balancing will be problematic when NAT timeouts occur

QUIC - Potential Complications

- Possible fragmentation issues when different applications run their own versions of QUIC
- You may be leaking data today, if you are not blocking UDP443
  - Google proprietary QUIC has been in use for years
- Connection ID could allow a website to track users more efficiently
- Possibility of reflection and amplification attacks
- A new attack surface until implementations become hardened

What is Driving These Changes?

- There is a belief by some that privacy === security

- Also, some believe that no content should be altered or removed in transit, including malicious content or even ads and trackers.

Graphic Source: https://www.google.com/transparencyreport/https/

RSAConference2019

3:00 AM - Wake Up Call

HTTPS Usage - Chrome Browser

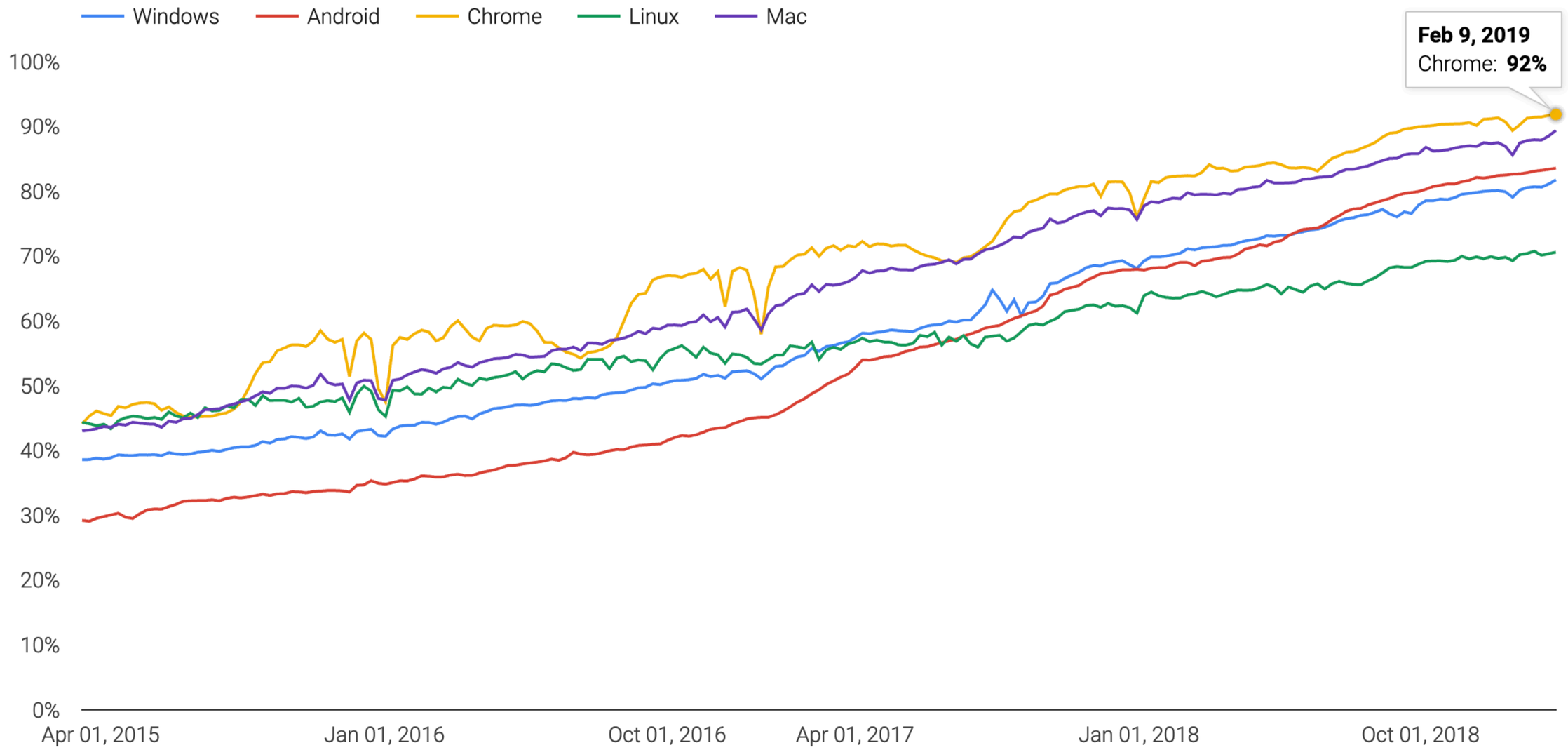


Diagram Source: https://www.google.com/transparencyreport/https/

Congratulations more than half of all web connections are now encrypted

Graphic Source: https://commons.wikimedia.org/wiki/File:Pouring_champagne.jpg

SSL/TLS Certs for Phishing

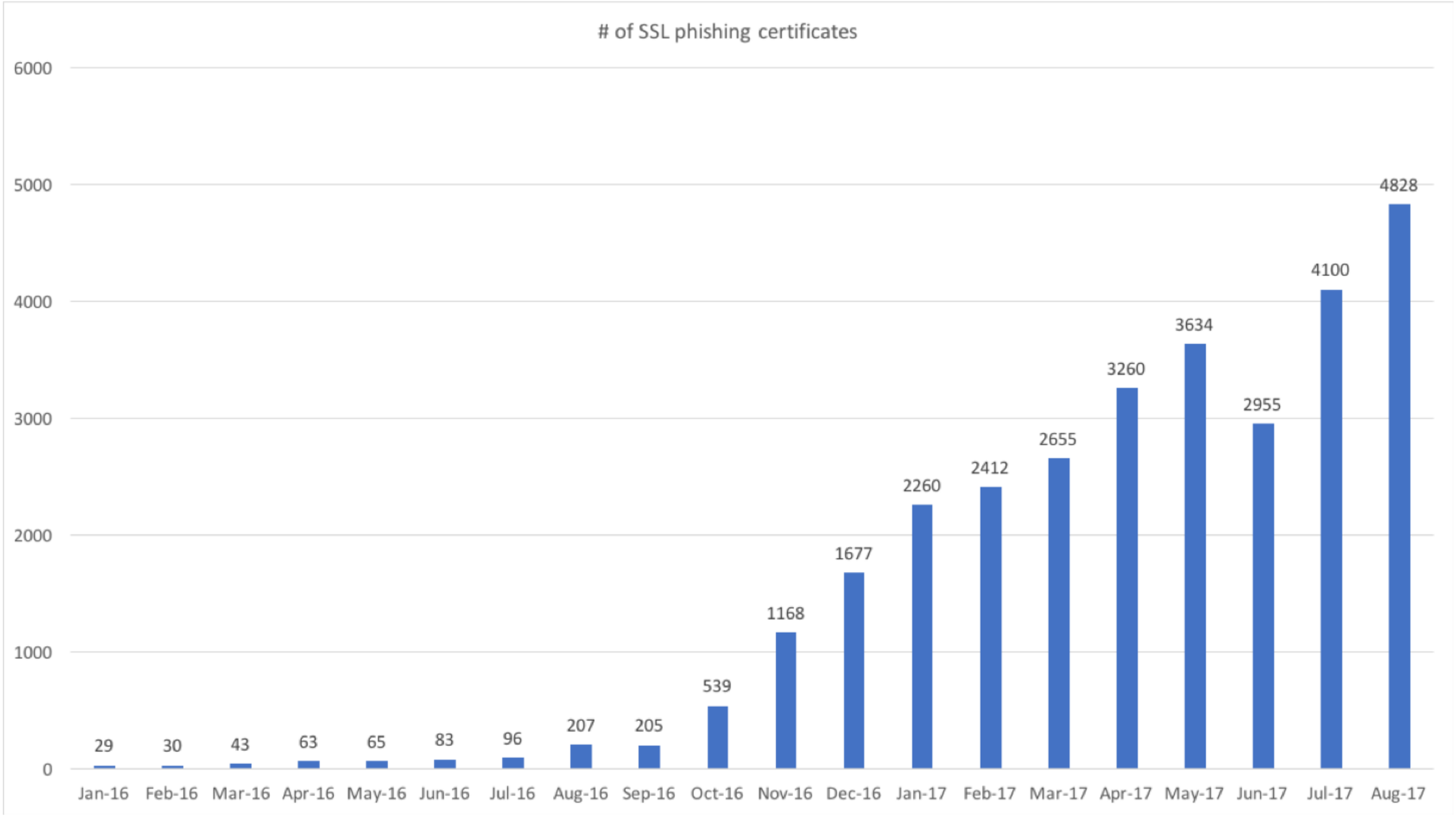


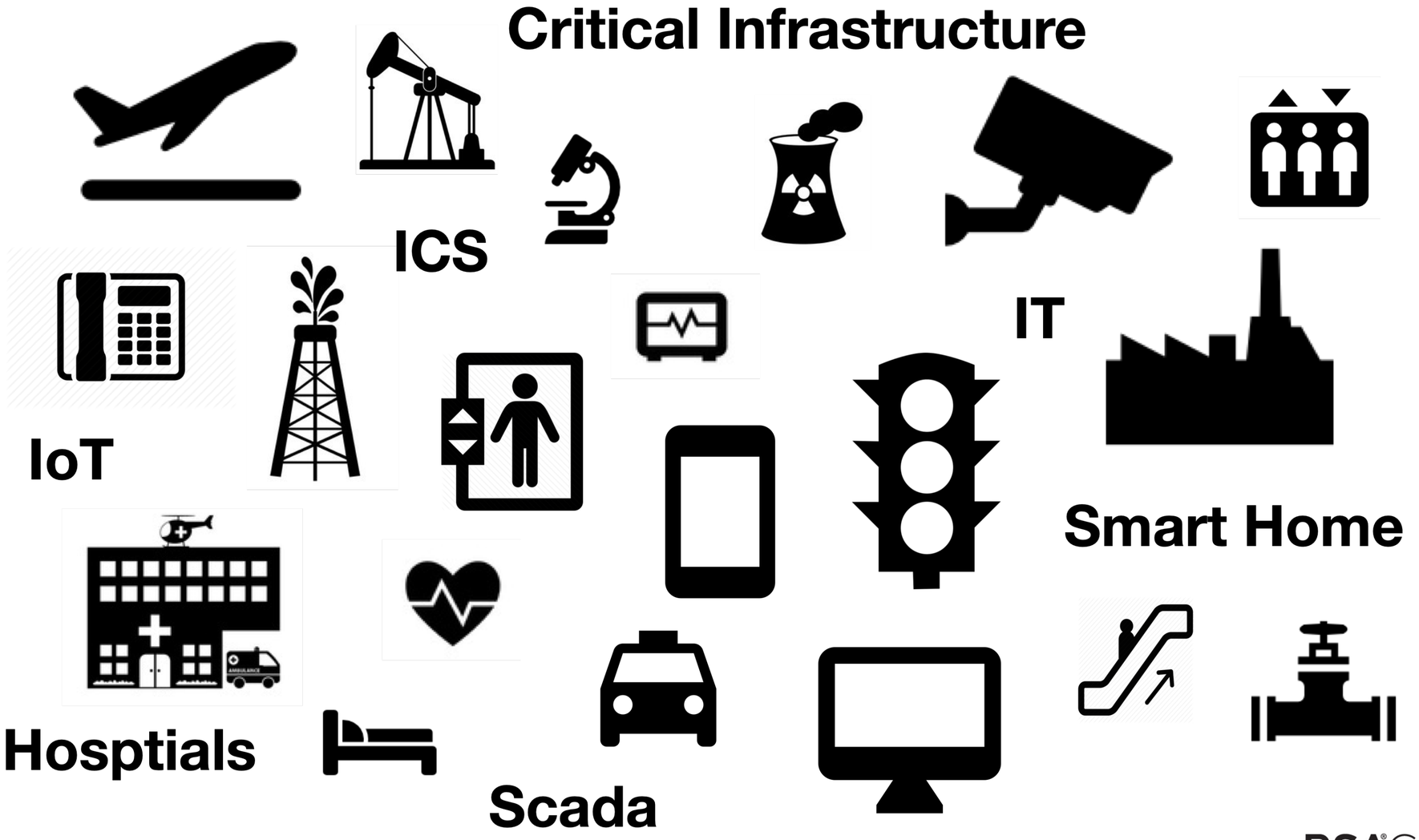
Diagram Source: Symantec

Graphic Source: https://commons.wikimedia.org/wiki/File:The_Scream.jpg

RSAConference2019

What Now?

Endpoints Everywhere!



Challenges to Endpoint Protection

- Not all endpoints can easily run security software
  - May not be available for all device types
    - Myriad of Operating Systems, RTOS
    - Embedded Platforms, ICS Systems, IoT Devices, Medical Devices, etc
  - Even if it can run it, it may not be current
- Frequent security software updates are required
- Not all endpoints see every update at the same time
  - There will always be gaps in your coverage

Challenges to Endpoint Protection

- Some equipment can not practically be updated or patched
  - 50 year old hardware that is soldered in to critical infrastructure
  - MRI Machines, IoT devices, some servers, older equipment
  - New “cost optimized” IOT devices are being deployed every year with no ability to run end point security and no ability to be updated
  - Not always safe for systems with stringent certification requirements
  - Some equipment has a very long life span
- Playing wack-a-mole is not sustainable
  - You can not patch your way into security

Challenges to Endpoint Protection

- Exploits can target or evade endpoint protection software
  - Endpoints are prone to privilege escalation vulnerabilities which may bypass any protection mechanism
- Some organizations stockpile endpoint zero-day exploits
  - Criminal organizations
  - Threat actors
  - Crime syndicates
  - Nation states

Benefits of Network Protection

- Ability to see all traffic, “the network does not lie”
- It can be the body guard to protect systems that can not do it themselves
- Allows rapid deployment of prevention, mitigation, & remediation
  - Often long before a manufacturer can patch the endpoint
  - Allows defense in depth
- Helps with regulatory compliance
  - Devices and data can not subvert network controls
- Operational Technology (OT) in Industrial Control Systems (ICS) is critical in defending SCADA systems

RSAConference2019

Conclusion

Questions to Think About

- Does more encryption increase security?
- Is every endpoint in your network always secure and able to prevent every conceivable attack?
- Can you always trust every website to never host malicious content and never attack your clients?
- Can you always trust every insider?
- Can you always trust every insider and endpoint to never exfiltrate your intellectual property?

The Future

- How are these new technologies going to impact your ability to defend your:
  - network, systems, users, and data?
- What will you do when threat actors and intrusion sets combine:
  - DNSSEC, DANE, DOH, ESNI, TLS1.3, and QUIC
- What will you do when all network traffic goes dark?
  - How will you maintain regulatory compliance?
  - What about intellectual property exfiltrated from your network?
- We need balance between privacy and security!

Apply What You Have Learned Today

- Next week you should:
  - Connect with your network security team
    - Understand how much security is lost if all of their content-aware sensors are blinded by encryption
  - Connect with your enterprise network operations team
    - See if they understand the implications of:
    - QUIC replacing TCP
    - DANE replacing Web PKI
    - Opportunistically encrypted DoH replacing DNS

Apply What You Have Learned Today

- In the first three months following this presentation you should:
  - Identify critical controls that require network based protection
  - Identify gaps and weaknesses with endpoint and network protection
  - Start engaging in IETF standards process and voicing your use cases
  - Ensure your vendors are aware of the proposed changes to standards, and see if they are engaged in the standards definition process.
- Within six months you should:
  - Have a solid plan for how your security controls will need to change

RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: BAC-W10

Hacked By Crypto

Bret Jordan, CISSP
Director, Office of the CTO
Symantec