Burt Kaliski
Senior Vice President and CTO, Verisign

NSF Technology Transfer to Practice in Cyber Security Workshop
November 4, 2015

Domain Name System (DNS) Overview

- Hierarchical, global name space for Internet names, e.g., www.example.com
- DNS records associate IP addresses, other data with domain names
- Authoritative name servers publish records, delegate to other name servers
- Clients typically query via a recursive name server

DNS Resolution

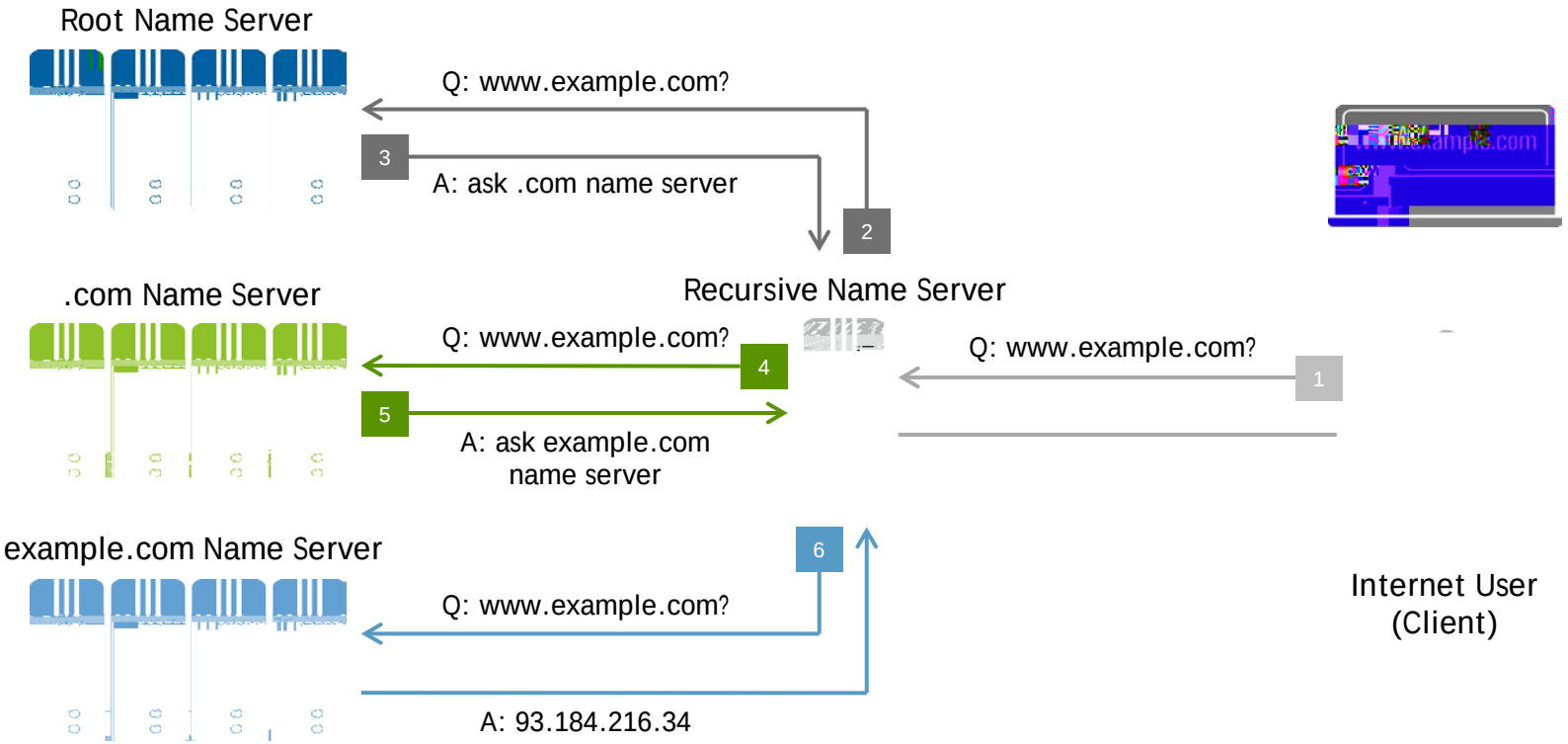
- Resolution is the process of answering a query by following the hierarchy of name servers
- To resolve www.example.com, query root server, then .com, then example.com
  - Each refers to next in hierarchy
- Recursive name server optimizes process by caching recent results

Privacy Risks

Risk 1: Between Client and Recursive

- Client effectively reveals browsing history via DNS traffic to recursive name server
- Adversary must be “on path” to see it, but it’s all in one place
- Risk increases when recursive name server deployed outside organization
- How to protect against eavesdropping?

Risk 2: At Recursive Name Server



Risk 3: Between Recursive and Authoritative

- Recursive name server reveals samples of community's browsing history via DNS traffic to authoritative name servers
- Adversary again must be "on path" to see traffic, but all in one place
- Authoritative name servers by definition deployed outside organization
- How to protect against eavesdropping?

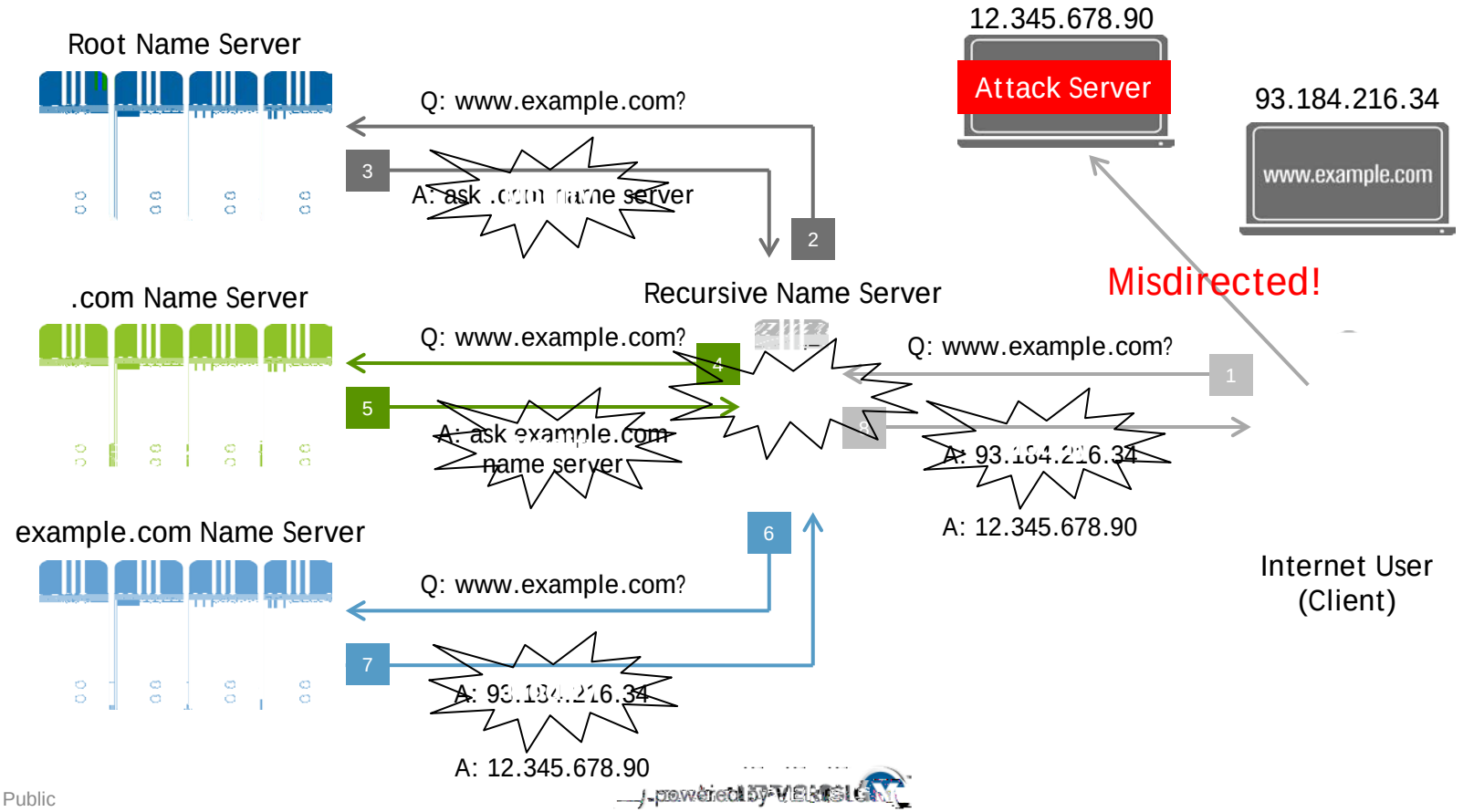
Risk 4: At Authoritative Name Server

•

Risk 5: Modification

- In addition to risks related to disclosure of DNS traffic, clients' privacy may also be at risk if DNS responses are modified
- By modifying a DNS response, an adversary can misdirect a client to an incorrect server, facilitating an attack

Risk 5: Modification



Verisign Public

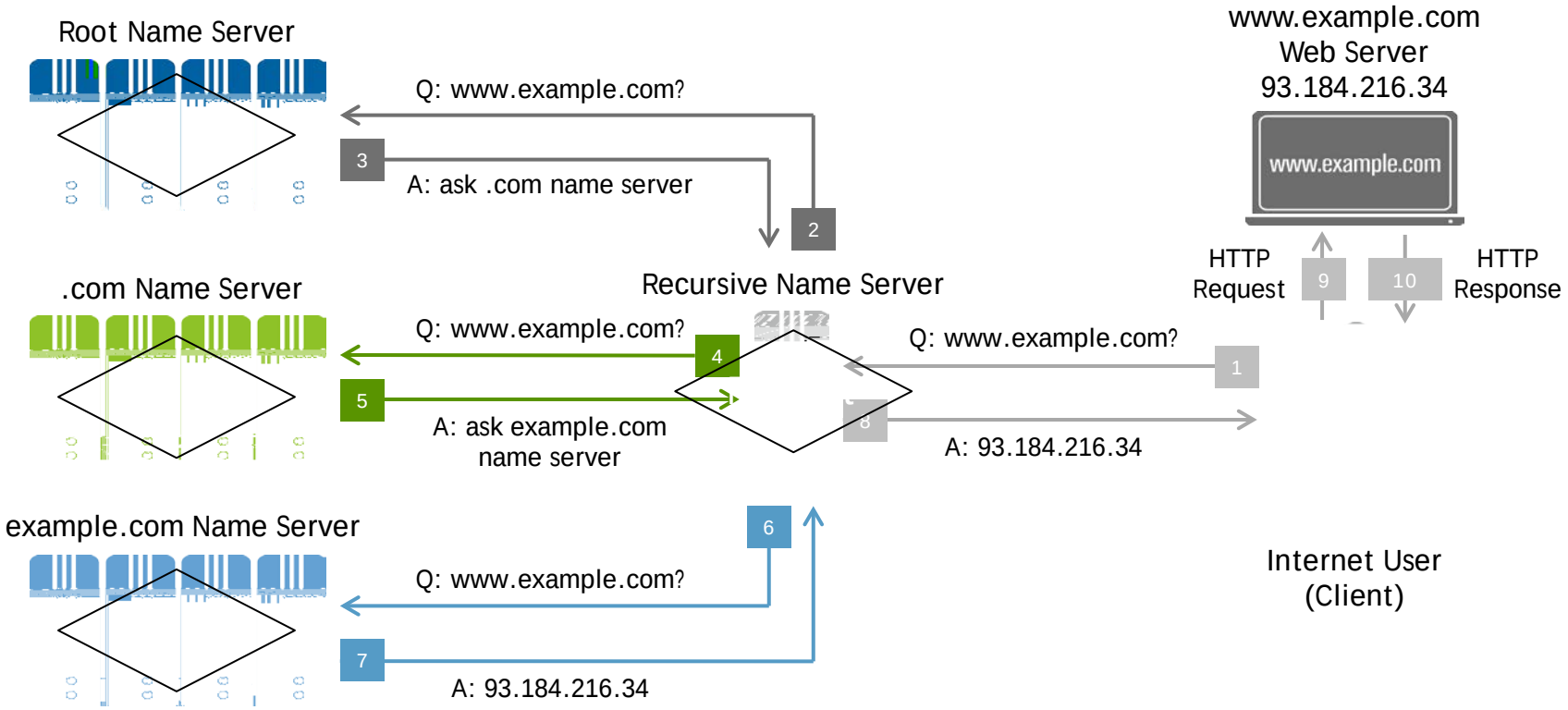
Mitigating DNS Privacy Risks

- Data handling policies can help mitigate the risks
- Technical enhancements to DNS have also been introduced in recent years to mitigate these risks:
  - DNS-over-TLS
  - qname-Minimization
  - DANE and DNSSEC

Mitigation 1: Data Handling

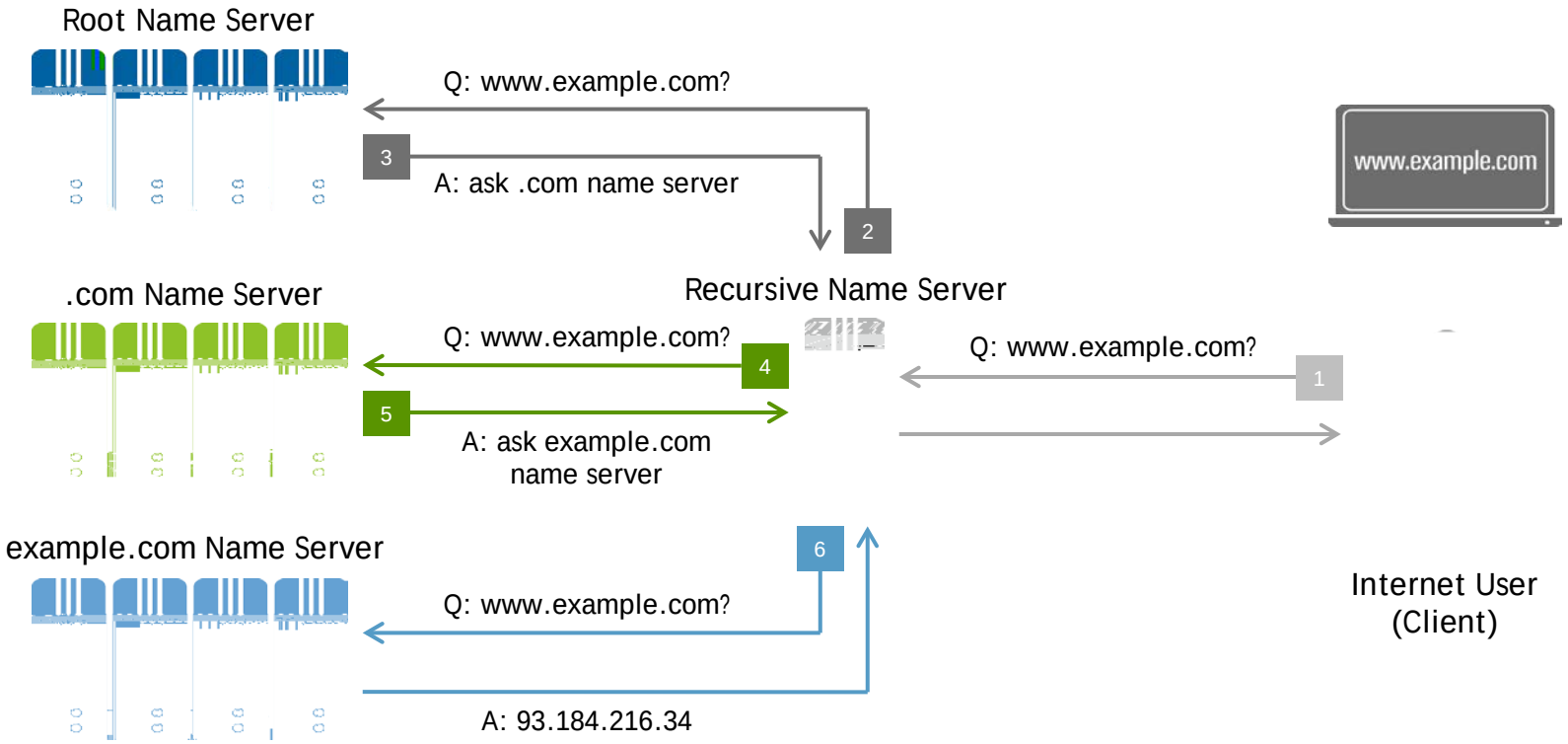
- Data handling policies, technologies and audits can mitigate risk of compromise, misuse of data at recursive, authoritative servers
- Root, top-level domain servers generally operate under established agreements
- Other authoritative name servers, recursive name servers may not

Mitigation 1: Data Handling



Risks 1 & 3: Eavesdropping

Mitigation 2: DNS-over-TLS

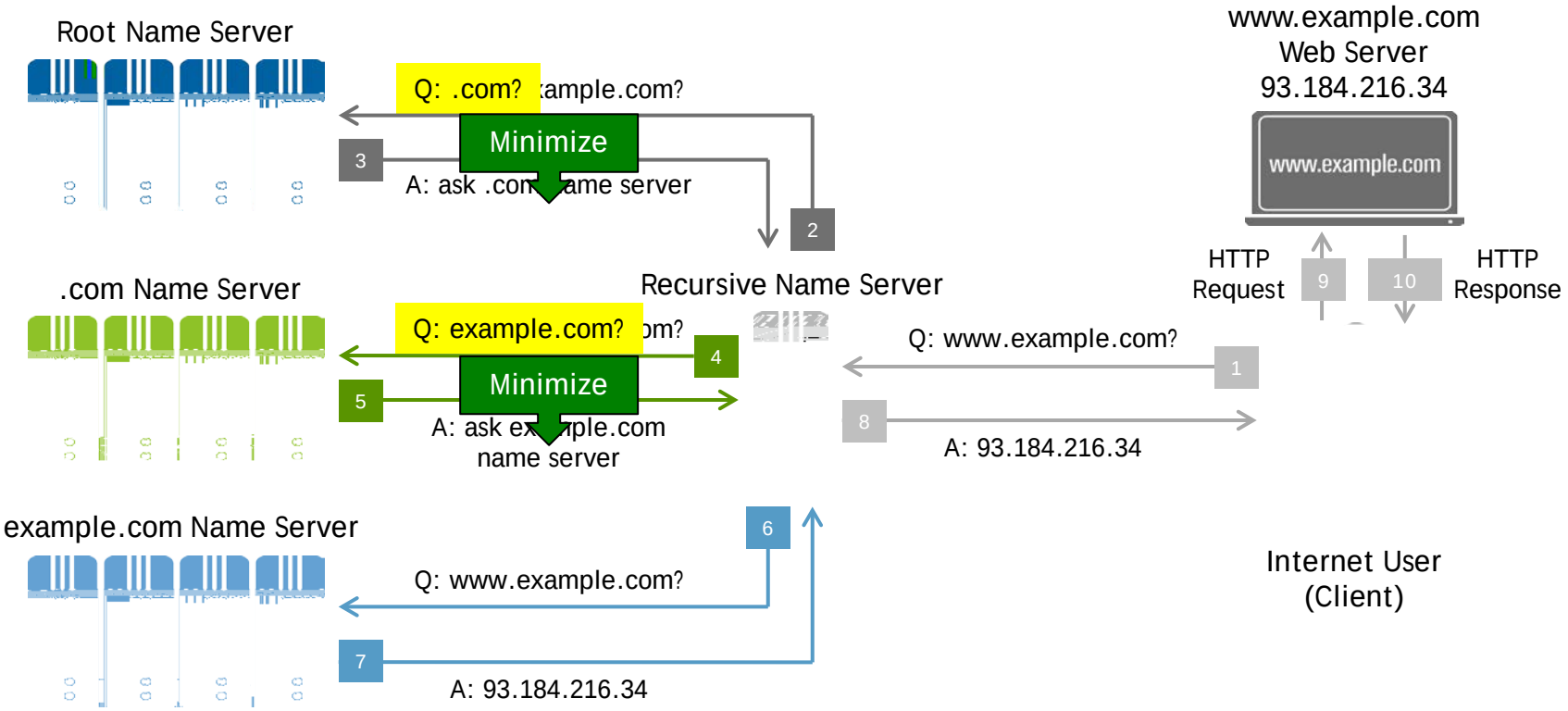


Mitigation 3: qname-Minimization

- DNS information disclosure can be reduced by asking authoritative only enough for referral to next server – not full query name (“qname”) each time
- IETF DNSOP working group currently developing qname-minimization spec
- Partially mitigates eavesdropping (risk 3) w/o encryption or changing authoritative

Risks 1 & 3: Eavesdropping

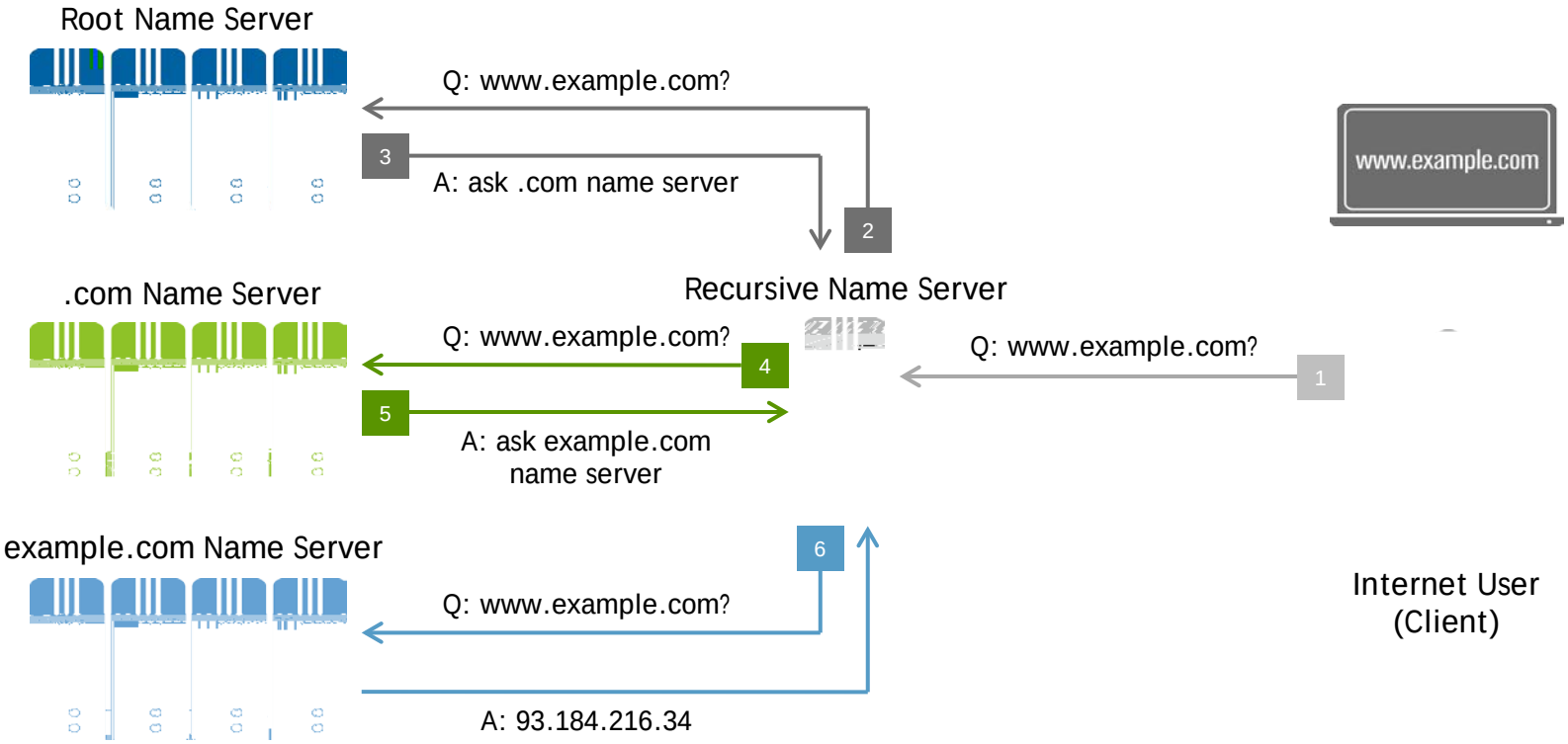
Mitigation 3: qname-Minimization



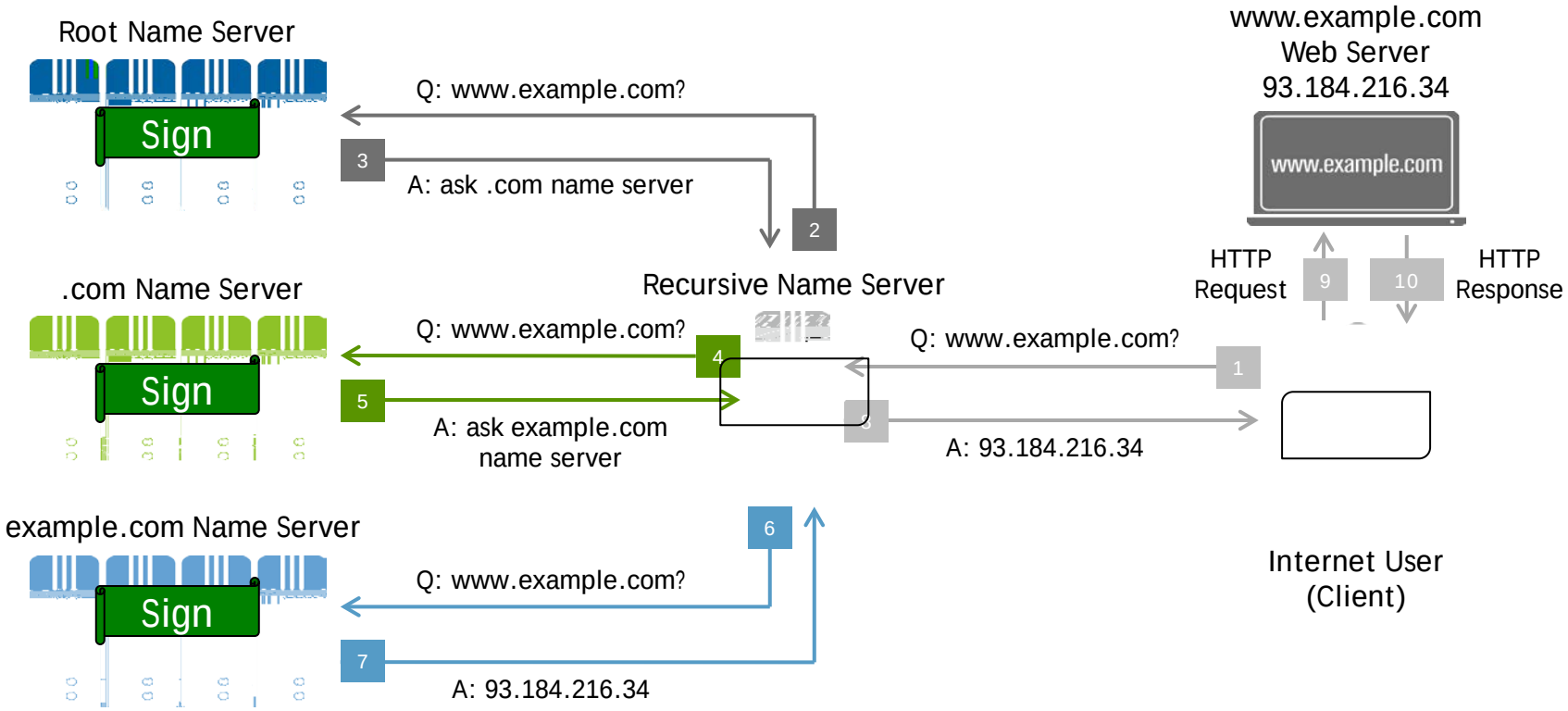
Mitigation 4: DNSSEC and DANE

- DNS Security Extensions (DNSSEC) mitigates modification risk by adding digital signatures to DNS records
- Recursive, client can validate that records are unmodified
- DNS-Based Authentication of Named Entities (DANE) extends validation to include web server keys and certificates

Risk 5: Modification



Mitigation 4: DNSSEC and DANE



Summary: Risk Mitigation Matrix

		Risk				
		Disclosure or Misuse				Modification
		Client to Recursive	At Recursive	Recursive to Authoritative	At Authoritative	
Mitigation	Data Handling		**Protect**		**Protect**	**+**
	DNS-over-TLS	**Encrypt**		**Encrypt**		**+**
	qname-minimization			**Minimize**	**Minimize**	
	DNSSEC and DANE					**Sign Validate**

Recommendations

Recommendations for Privacy Professionals

- If DNS is part of the system you're protecting ...
-

For More Information

Burt Kaliski

bkaliski@verisign.com

www.verisign.com

Q & A