Towards Secure Name Resolution on the Internet

C. Grothoff M. Wachs M. Ermert J. Appelbaum

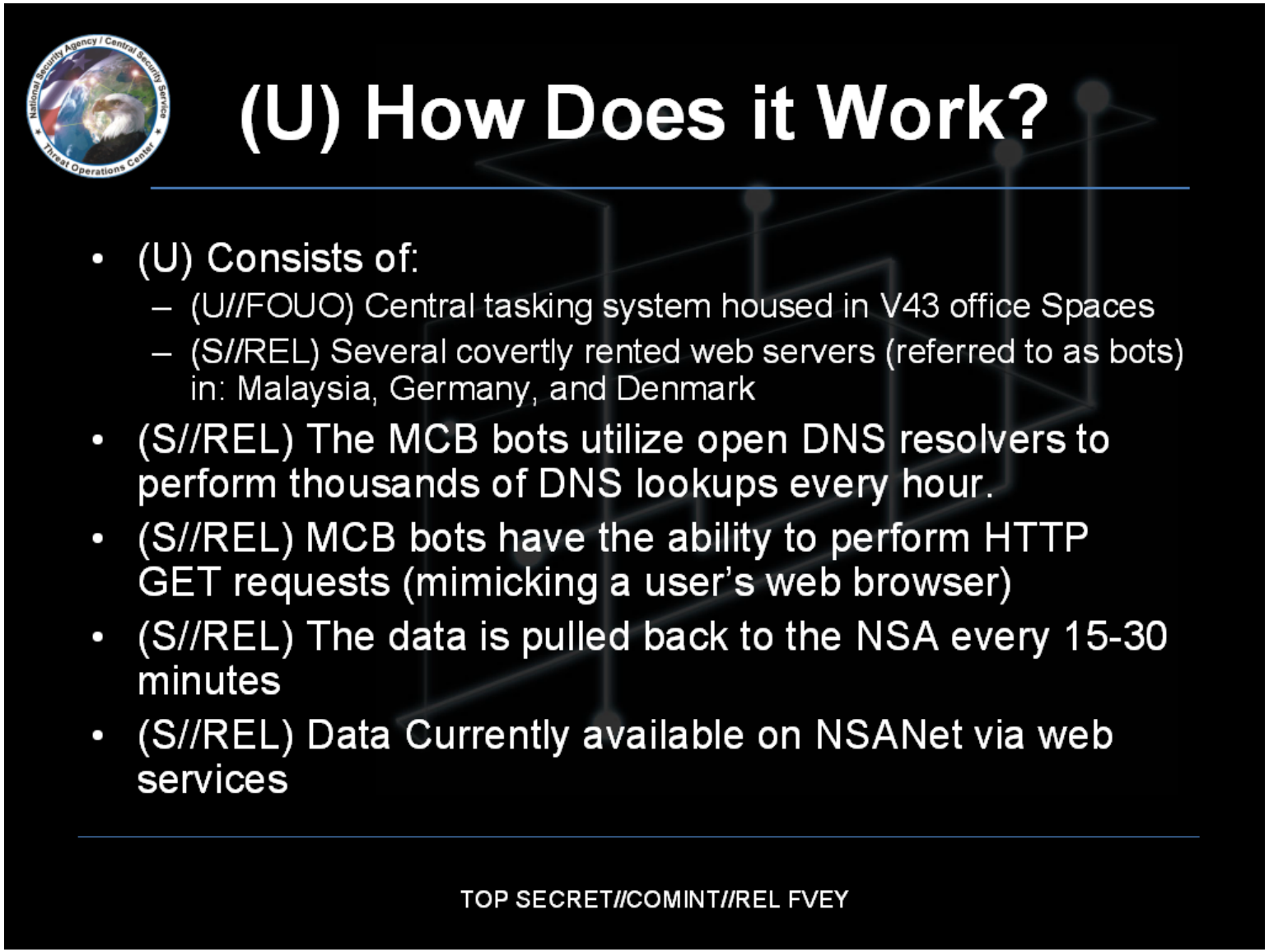
26.2.2017

"The Domain Name System is the Achilles heel of the Web." –Tim Berners-Lee

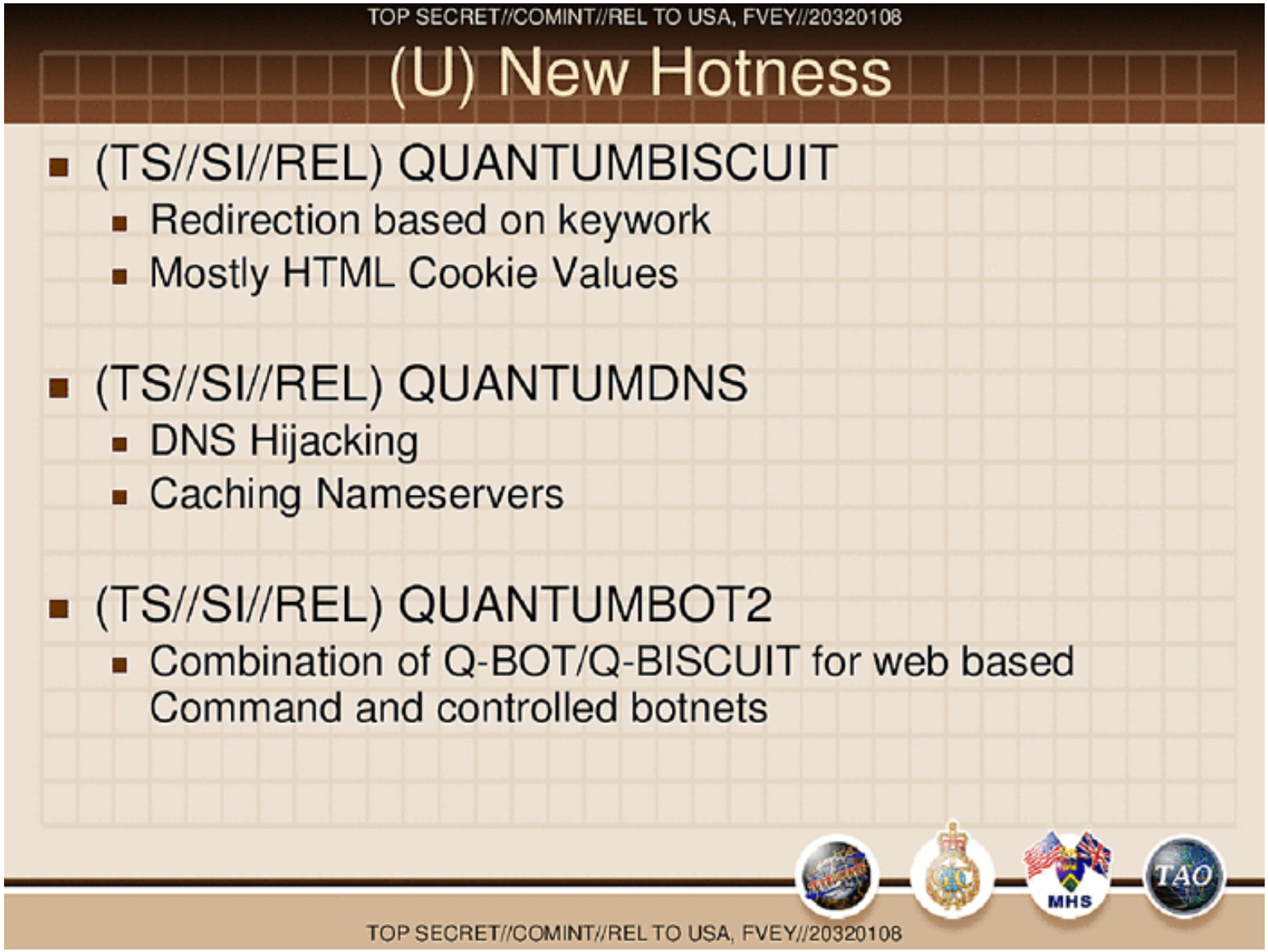
Security Goals for Name Systems

- Query origin anonymity
- Data origin authentication and integrity protection
- Zone confidentiality
- Query and response privacy
- Censorship resistance
- *Availability*, *DDoS-resistance*

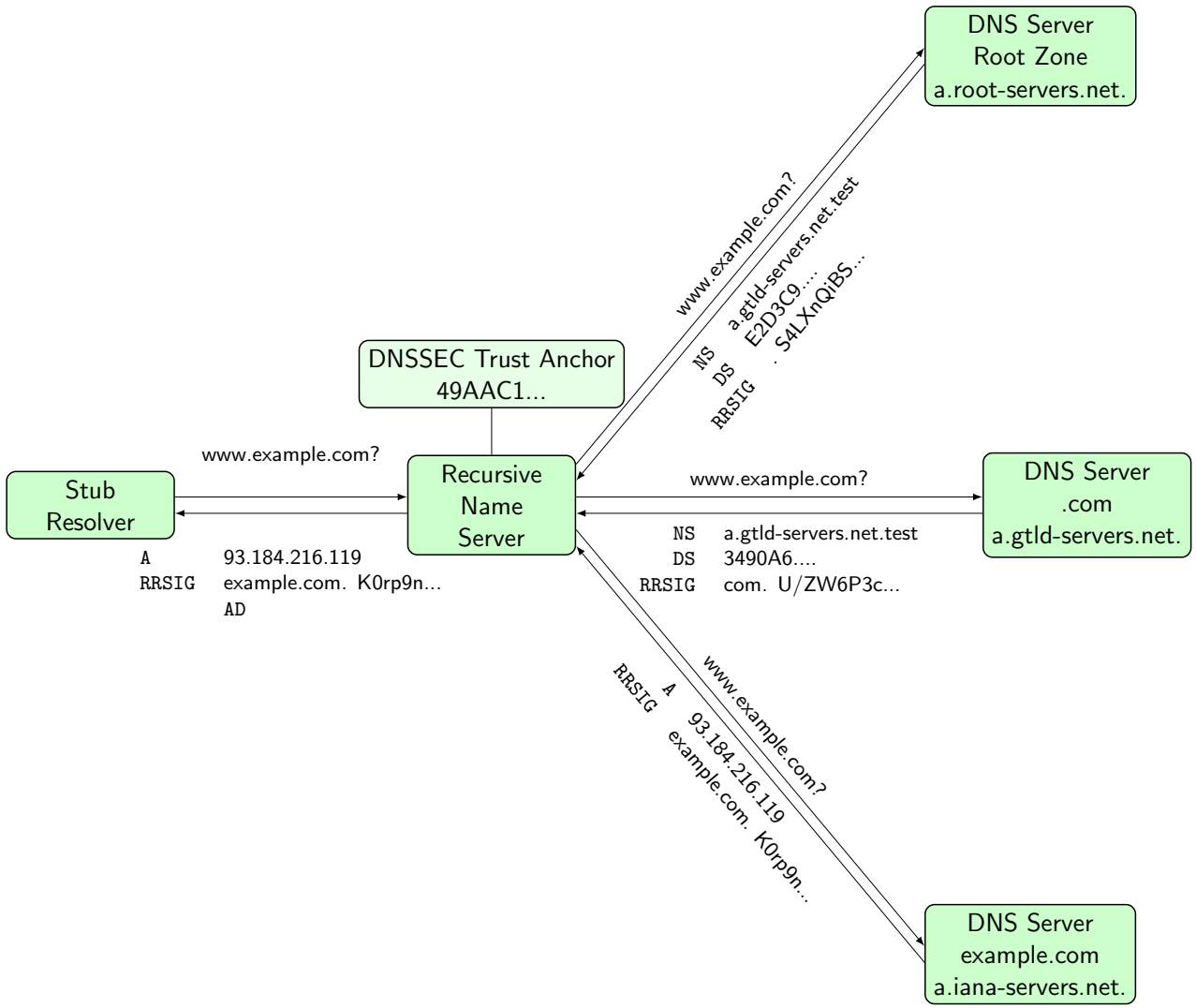
Exemplary Attacks: MORECOWBELL



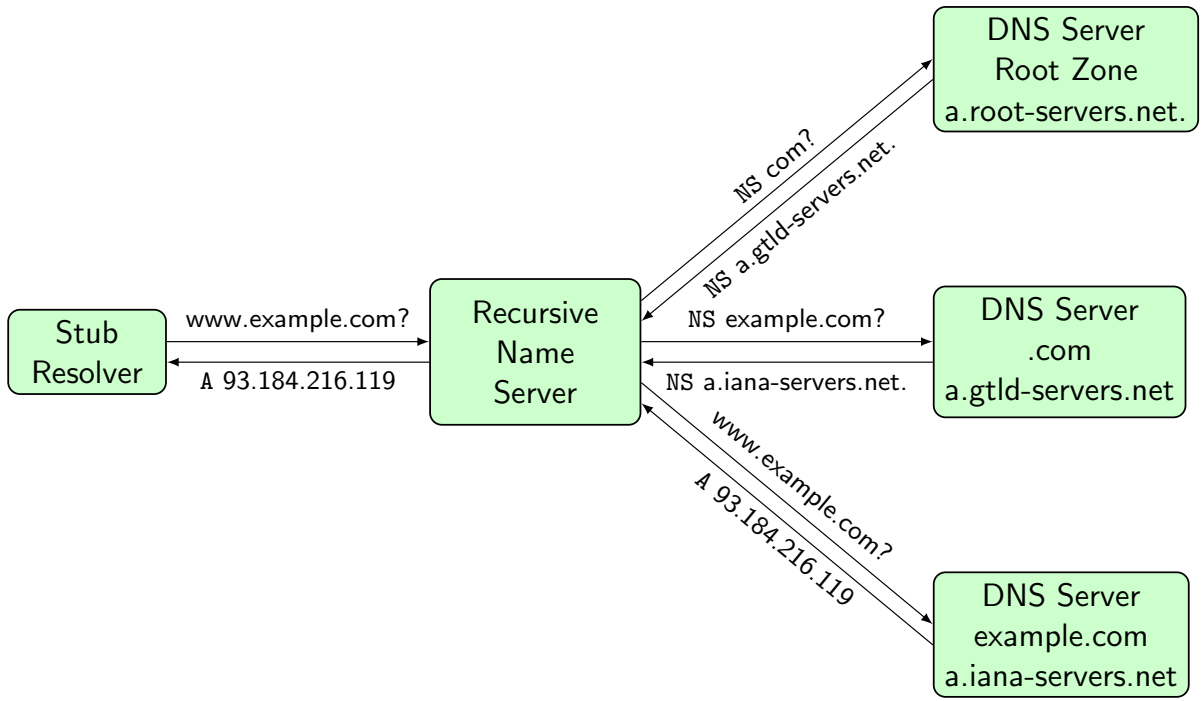
Exemplary Attacks: QUANTUMDNS



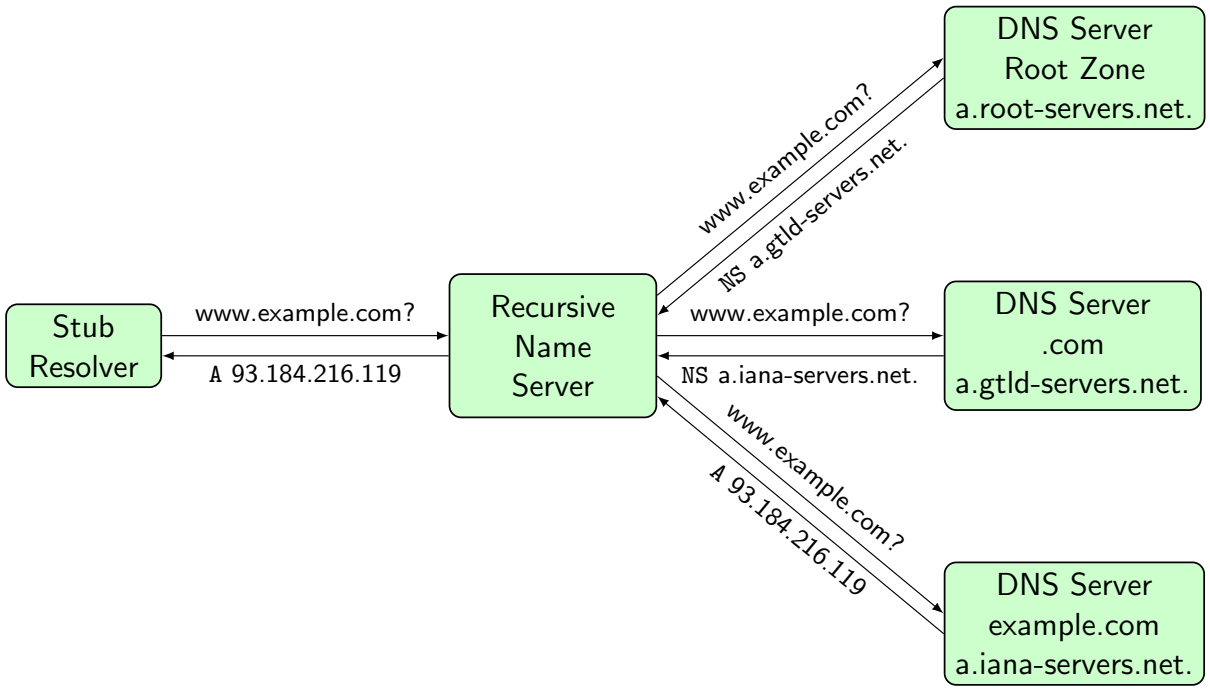
DNSSEC


DNS Server
Root Zone
a.root-servers.net.
www.example.com?
NS a.gtld-servers.net.test
DS E2D3C9....
RRSIG . S4LXnQiBS...
DNSSEC Trust Anchor
49AAC1...
www.example.com?
Stub
Resolver
Recursive
Name
Server
www.example.com?
DNS Server
.com
a.gtld-servers.net.
NS a.gtld-servers.net.test
DS 3490A6....
RRSIG com. U/ZW6P3c...
A 93.184.216.119
RRSIG example.com. K0rp9n...
AD
www.example.com?
A 93.184.216.119
RRSIG example.com. K0rp9n...
DNS Server
example.com
a.iana-servers.net.

Query Name Minimization



DNS over TLS


Stub Resolver
www.example.com?
A 93.184.216.119
Recursive Name Server
www.example.com?
NS a.gtld-servers.net.
DNS Server Root Zone a.root-servers.net.
www.example.com?
NS a.iana-servers.net.
DNS Server .com a.gtld-servers.net.
www.example.com?
A 93.184.216.119
DNS Server example.com a.iana-servers.net.

The Textbook Version of the Internet

Layering, $\approx$ 1990

	HTTPS
DNS	TLS
UDP	TCP
IPv4	
Ethernet	
Phys. Layer	

The Textbook Version of the Internet

Layering, ≈ 1990

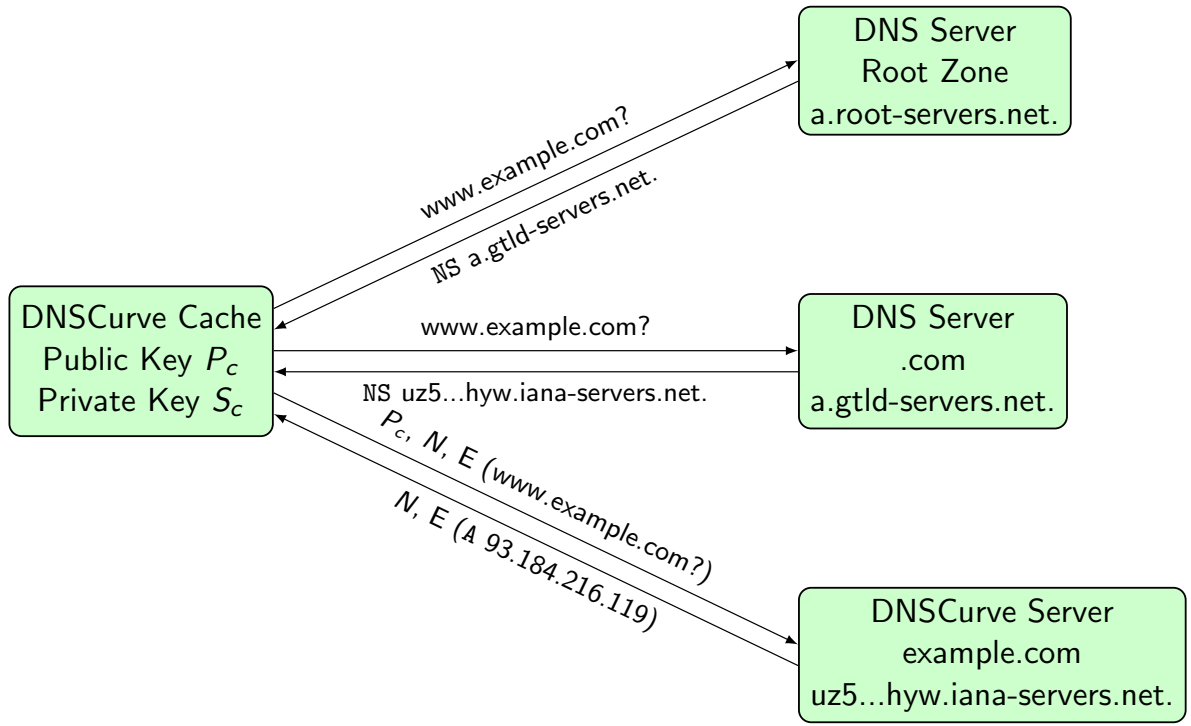
	HTTPS
DNS	TLS
UDP	TCP
IPv4	
Ethernet	
Phys. Layer	

"Layering", ≈ 2020

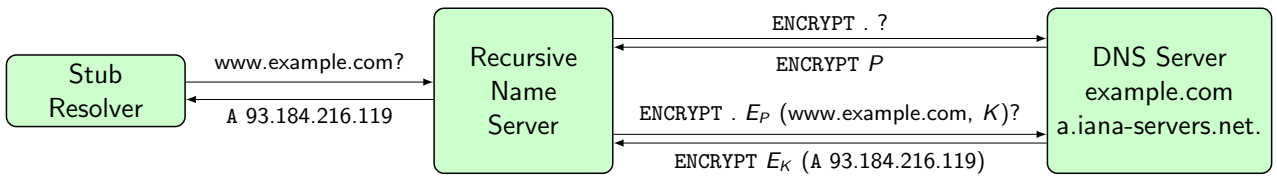
HTTPS	libmicrohttpd
TLS-with-DANE	libgnutls
DNS-over-TLS	libunbound
TLS*	libnss
TCP	Linux
IPv6	Linux
Ethernet	
Phys. Layer	

* = castrated version without RFC 6125 or RFC 6394, possibly NULL cipher, see TLS profiles draft.

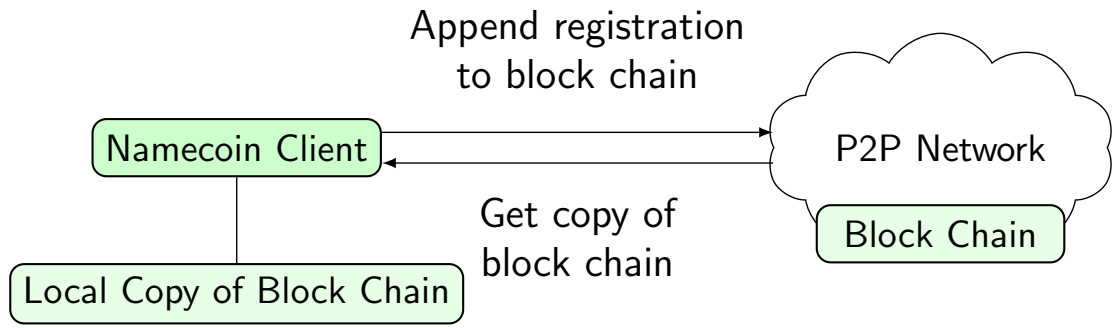
DNSCurve


DNS Server
Root Zone
a.root-servers.net.
www.example.com?
NS a.gtld-servers.net.
DNSCurve Cache
Public Key P_c
Private Key S_c
www.example.com?
NS uz5...hyw.iana-servers.net.
DNS Server
.com
a.gtld-servers.net.
P_c, N, E (www.example.com?)
N, E (A 93.184.216.119)
DNSCurve Server
example.com
uz5...hyw.iana-servers.net.

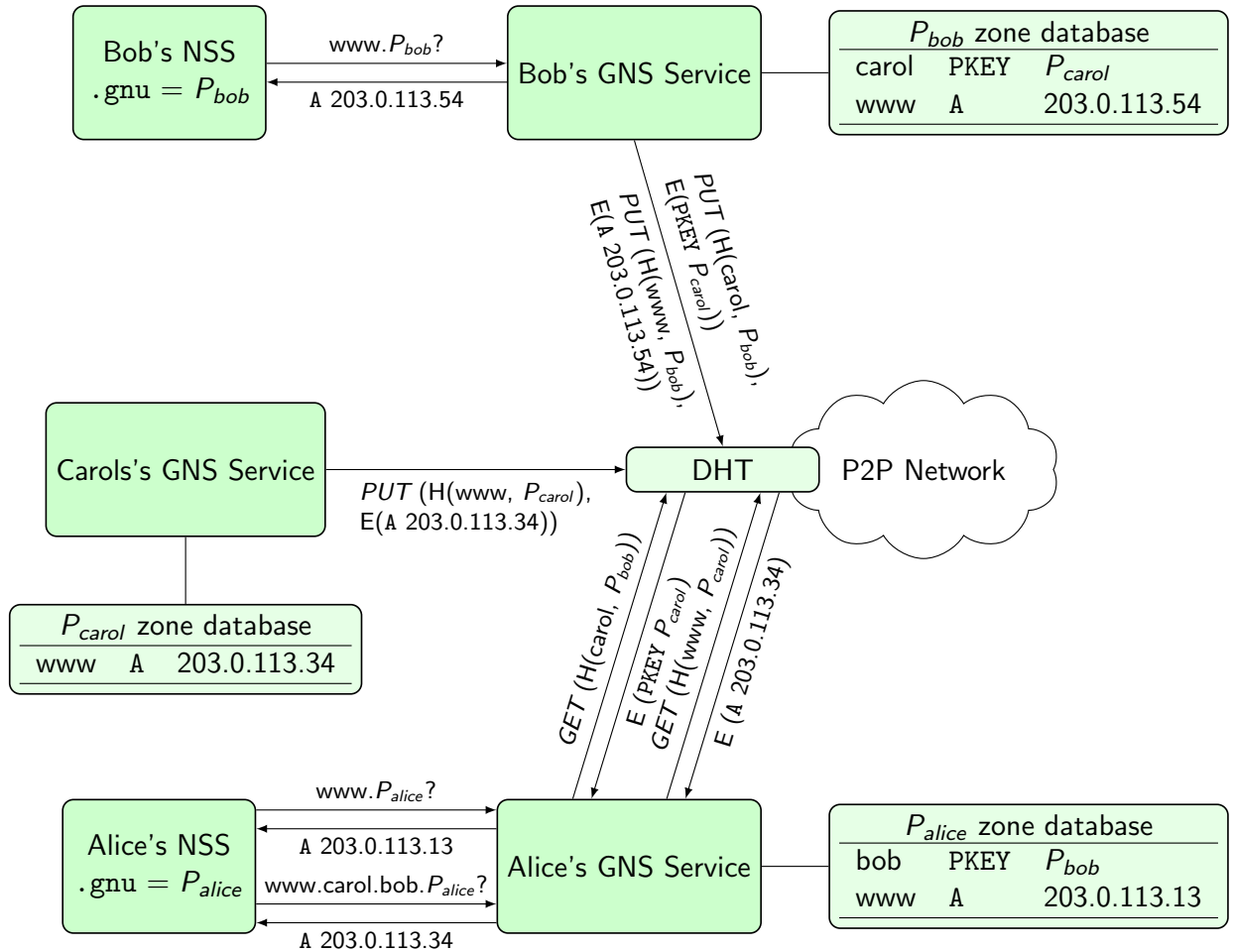
Confidential DNS



Namecoin


Append registration
to block chain
Namecoin Client
P2P Network
Block Chain
Get copy of
block chain
Local Copy of Block Chain

The GNU Name System (GNS)



GNS and Query Privacy: Terminology

G	generator in ECC curve, a point
n	size of ECC group, $n := \|G\|$, n prime
x	private ECC key of zone ($x \in \mathbb{Z}_n$)
P	public key of zone, a point $P := xG$
l	label for record in a zone ($l \in \mathbb{Z}_n$)
$R_{P,l}$	set of records for label l in zone P
$q_{P,l}$	query hash (hash code for DHT lookup)
$B_{P,l}$	block with encrypted information for label l in zone P published in the DHT under $q_{P,l}$

GNS and Query Privacy: Cryptography

Publishing records $R_{P,I}$ as $B_{P,I}$ under key $q_{P,I}$

$$h := H(I, P) \tag{1}$$

$$d := h \cdot x \mod n \tag{2}$$

$$B_{P,I} := S_d(E_{HKDF(I,P)}(R_{P,I})), dG \tag{3}$$

$$q_{P,I} := H(dG) \tag{4}$$

GNS and Query Privacy: Cryptography

Publishing records $R_{P,l}$ as $B_{P,l}$ under key $q_{P,l}$

$$h := H(l, P) \tag{1}$$
$$d := h \cdot x \mod n \tag{2}$$
$$B_{P,l} := S_d(E_{HKDF(l,P)}(R_{P,l})), dG \tag{3}$$
$$q_{P,l} := H(dG) \tag{4}$$

Searching for records under label l in zone P

$$h := H(l, P) \tag{5}$$
$$q_{P,l} := H(hP) = H(hxG) = H(dG) \Rightarrow \texttt{obtain } B_{P,l} \tag{6}$$
$$R_{P,l} = D_{HKDF(l,P)}(B_{P,l}) \tag{7}$$

Summary

	Protection against						Ease of
	Manipulation by MiTM	Zone walk	Client observation network	Client observation operator	Traffic Amplifi.	Censorship / Legal attacks	Migration / Compatibility
DNS	✗	✓	✗	✗	✗	✗	+++
DNSSEC	✓	failed	✗	✗	+/-	✗	+*
DNSCurve	✓	✓	✓	✗	✓	✗	+*
DNS-over-TLS	✓	n/a	✓	✗	✓	✗	+
Conf. DNS	✗	n/a	✓	✗	✗	✗	++
Namecoin	✓	✗	✓	✓	✓	✓	-
GNS	✓	✓	✓	✓	✓	✓	- -

*EDNS0

Conclusion

- Query name minimization is low-cost, low-benefit approach, but should clearly be done
- Simple encryption schemes offer medium-cost, medium-benefit approach
- NameCoin does not help with privacy at all
- GNU Name System performance depends on the DHT
  $\Rightarrow$ need to invest more in DHT design & implementation

Do you have any questions?

- Yves Eudes, Christian Grothoff, Jacob Appelbaum, Monika Ermert, Laura Poitras, Matthias Wachs: *MoreCowBell, nouvelles révélations sur les pratiques de la NSA*. **Le Monde**, 24.1.2015.
- Nathan Evans and Christian Grothoff. *R^5N. Randomized Recursive Routing for Restricted-Route Networks*. **5th International Conference on Network and System Security**, 2011.
- Matthias Wachs, Martin Schanzenbach and Christian Grothoff. *A Censorship-Resistant, Privacy-Enhancing and Fully Decentralized Name System*. **13th International Conference on Cryptology and Network Security**, 2014.