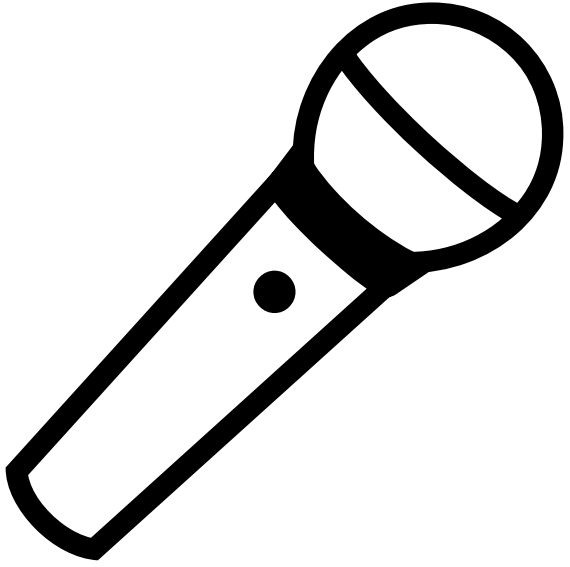
Protocol Vulnerabilities panel

- Richard Meeus, Akamai
- Xiang Li, Nankai University / Yunyi Zhang, Tsingua University
- Huayi Duan, ETH Zurich
- Elias Heftrig, ATHENE, Goethe-Universität Frankfurt
- Yehuda Afek, Tel-Aviv University

Discussion time



Attack	**Resource**	**Vector**
KeyTrap	CPU	DNSSEC data
NRDelegation	CPU, Memory	Delegation count
CacheFlush	Memory	RR size
CAMP*	Network	Indirection
DNSBomb	Network	*Timing, queueing*
NXNSAttack	Network	NS indirection
Reflection	Network	*Source address*

Common theme

limits

Limits?

- RR set size – CacheFlush
- Referral size – NRDelegation
- Recursion / packet count – CAMP, NXNSAttack
- Indirection – CAMP
- Query name minimization – CAMP
- Crypto operations – KeyTrap
- Queueing limits – DNSBomb
- Per-client/server/zone query rate limiting – Reflection

Why?

Why has the **industry not** focused on resource exhaustion attacks?

Where from Here?

- Future proof limits
  - What if RFC 883, November 1983, had limits …
  - Related talk: CNAMEs in the wild – this afternoon
- Limits set by
  - Operators?
  - Software developers?
  - Standardized minimum thresholds?
- Automatic verification methods? Formal?
- Volumetric protections? DNS cookies? DNS-over-QUIC? Something else?

Where from Here?

- Future proof limits
- What if RFC 883, November 1983, had limits …

Where from Here?

- Limits set by …
  - Operators?
  - Software developers?
  - Standardized minimum thresholds?

Where from Here?

- Automatic verification methods?
  - Formal?

Where from Here?

- Volumetric protections?
- DNS cookies?
- DNS-over-QUIC?
- Something else?