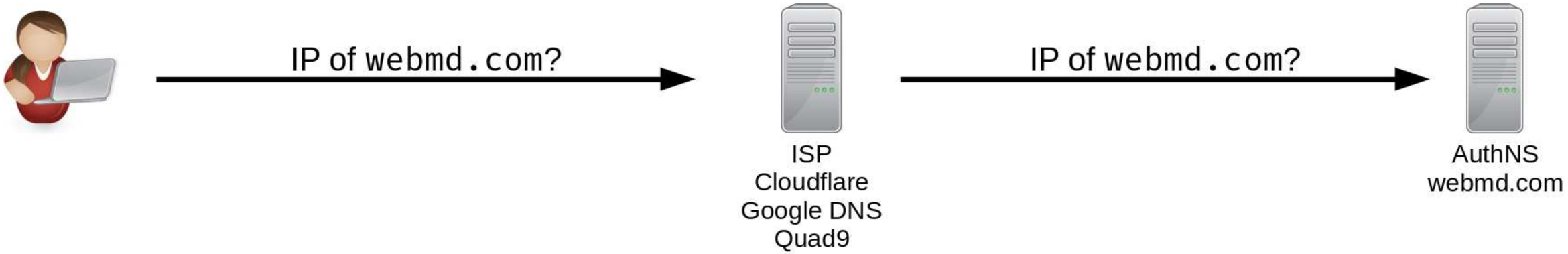
CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

Padding Ain't Enough: Assessing the Privacy Guarantees in Encrypted DNS

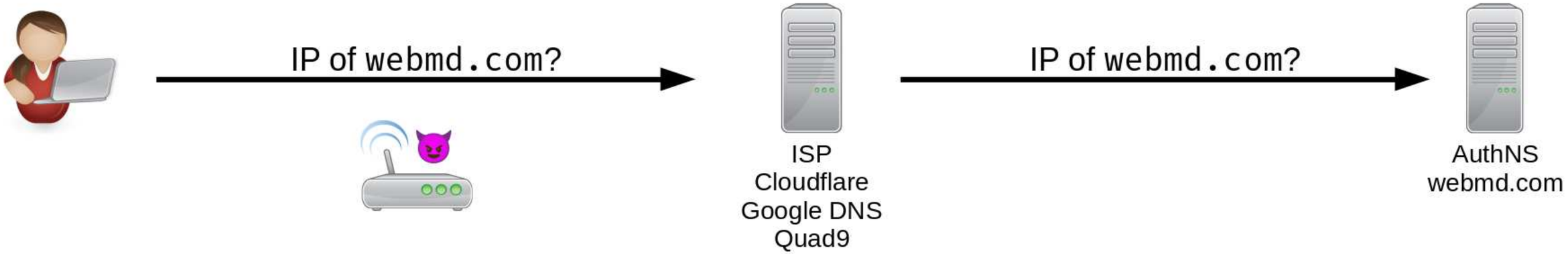
Jonas Bushart, Christian Rossow

Privacy of DNS



RFC 7858: Specification for DNS over Transport Layer Security (TLS)
RFC 8484: DNS Queries over HTTPS (DoH)

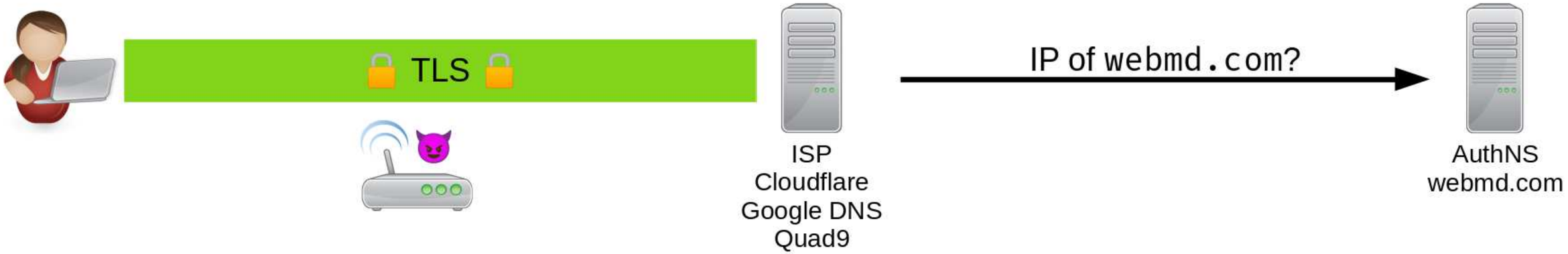
Privacy of DNS



- Passive Adversary
  - Wi-Fi point, ISP, etc.

RFC 7858: Specification for DNS over Transport Layer Security (TLS)
RFC 8484: DNS Queries over HTTPS (DoH)

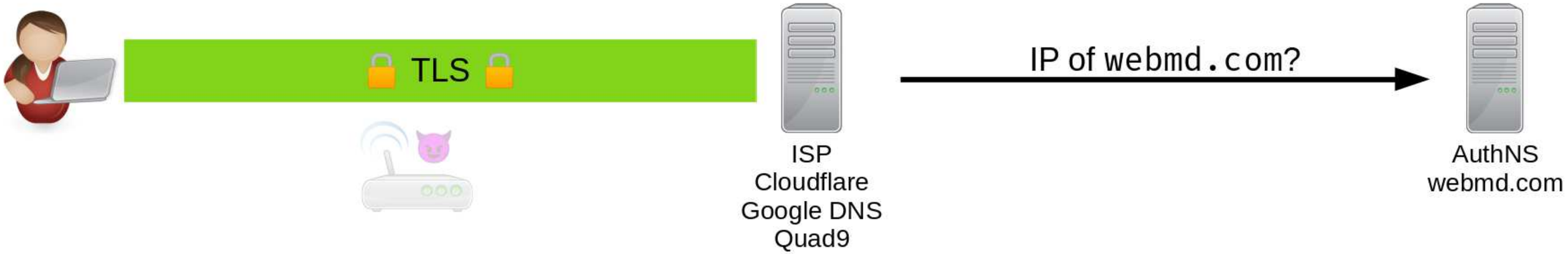
Privacy of DNS



- Passive Adversary
  - Wi-Fi point, ISP, etc.

RFC 7858: Specification for DNS over Transport Layer Security (TLS)
RFC 8484: DNS Queries over HTTPS (DoH)

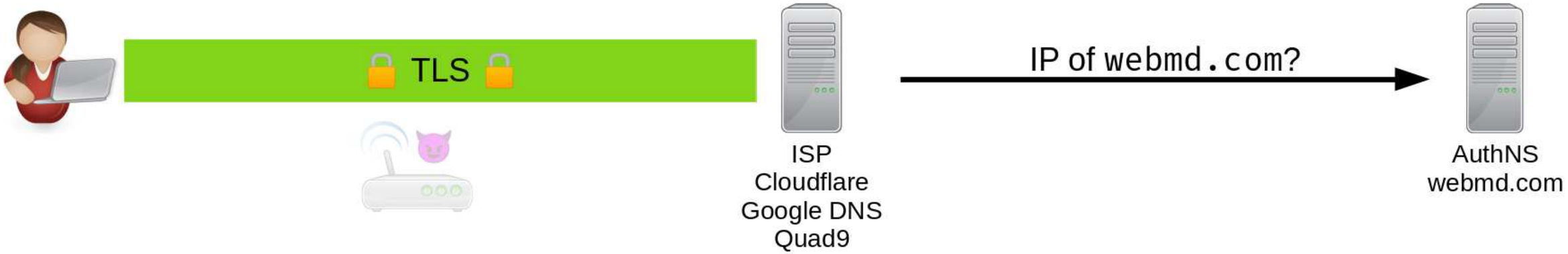
Privacy of DNS



- Passive Adversary
  - Wi-Fi point, ISP, etc.

RFC 7858: Specification for DNS over Transport Layer Security (TLS)
RFC 8484: DNS Queries over HTTPS (DoH)

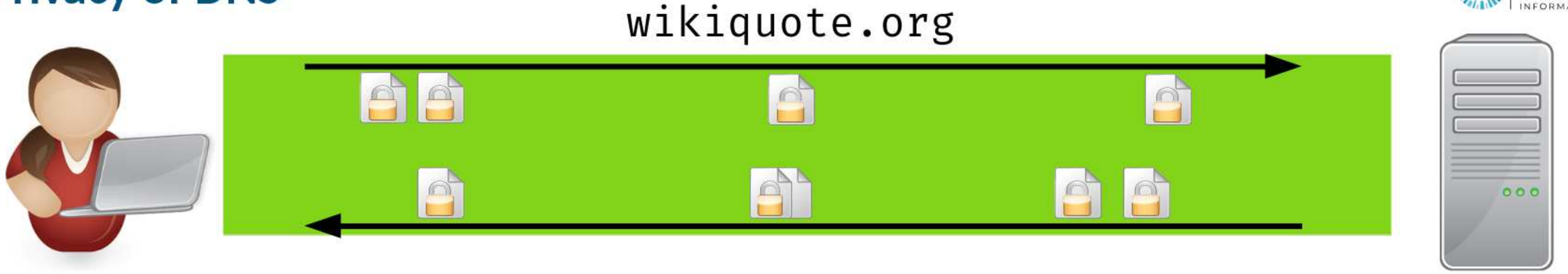
Privacy of DNS



- Passive Adversary
  - Wi-Fi point, ISP, etc.
- Side-Channels

RFC 7858: Specification for DNS over Transport Layer Security (TLS)
RFC 8484: DNS Queries over HTTPS (DoH)

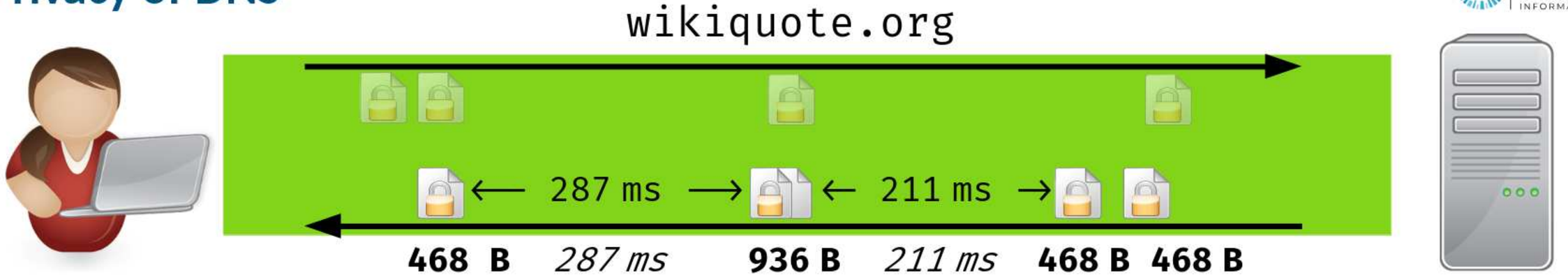
Privacy of DNS



- Threat model like DoT/DoH

RFC 7830: The EDNS(0) Padding Option
RFC 8467: Padding Policies for Extension Mechanisms for DNS (EDNS(0))

Privacy of DNS



- RFC 8467: Block padding 128B / 468B
- Threat model like DoT/DoH

RFC 7830: The EDNS(0) Padding Option
RFC 8467: Padding Policies for Extension Mechanisms for DNS (EDNS(0))

Privacy of DNS

- RFC 8467: Block padding 128B / 468B
- Threat model like DoT/DoH

RFC 7830: The EDNS(0) Padding Option
RFC 8467: Padding Policies for Extension Mechanisms for DNS (EDNS(0))

Privacy of DNS

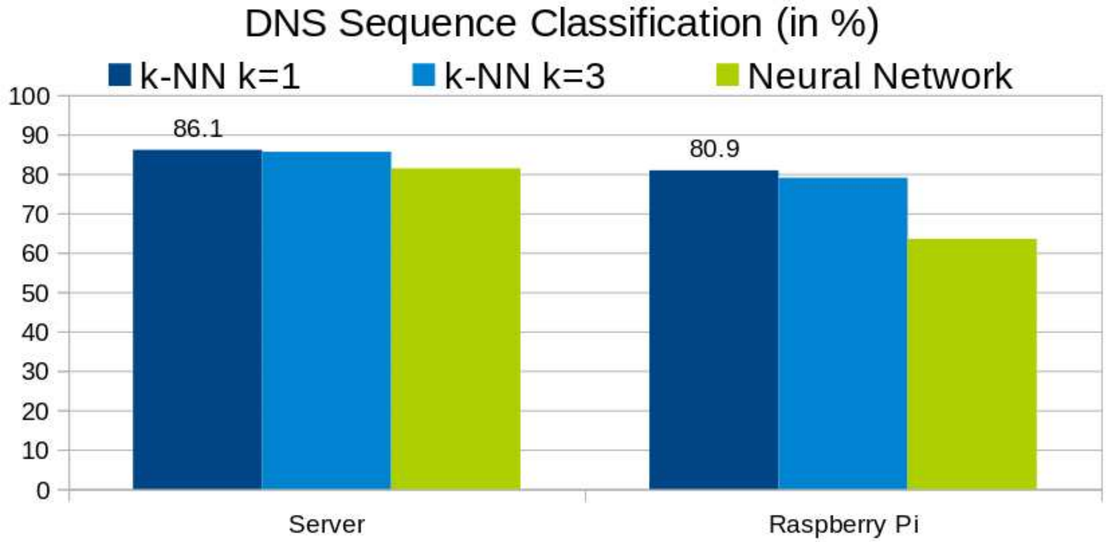
- RFC 8467: Block padding 128B / 468B
- k-NN with Edit-Distance
  - Customized weights
- Simple Neural Network
- Threat model like DoT/DoH

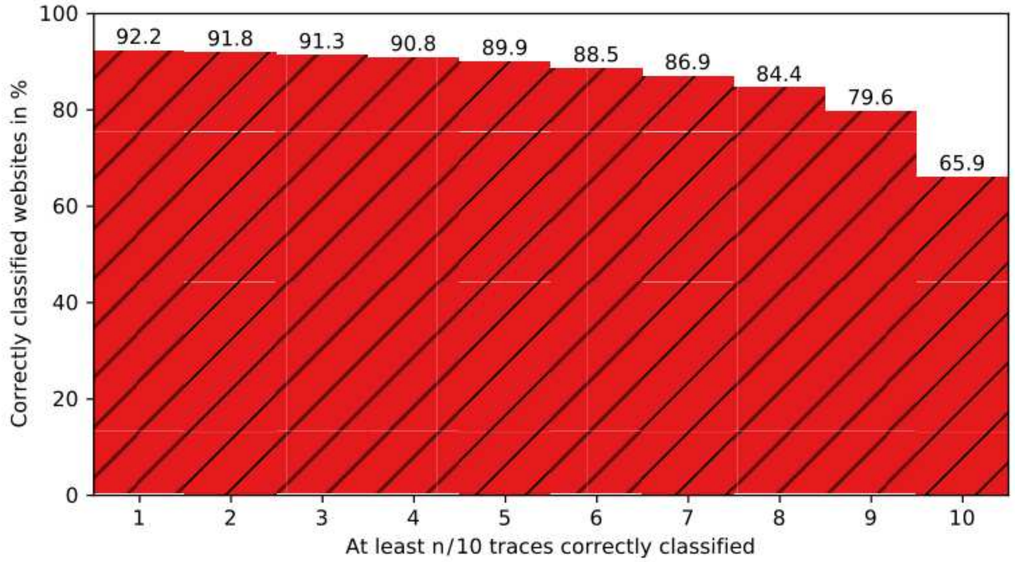
RFC 7830: The EDNS(0) Padding Option
RFC 8467: Padding Policies for Extension Mechanisms for DNS (EDNS(0))

Evaluation: Closed World

- Adversary knows all websites

- Dataset
  - Tranco List
  - 9235 websites / 10 sequences
  - Pi: 7699 websites / 4 sequences
- unbound 1.1.1.1

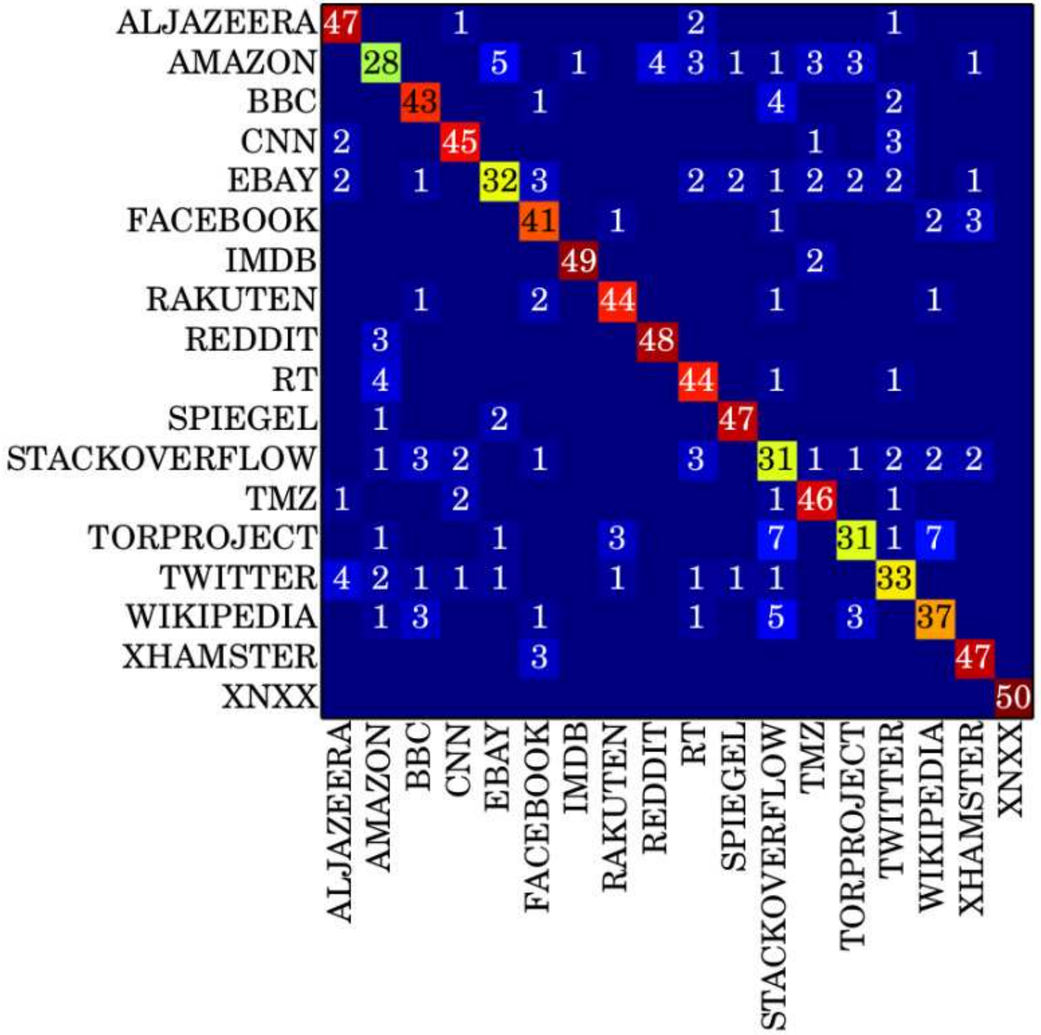


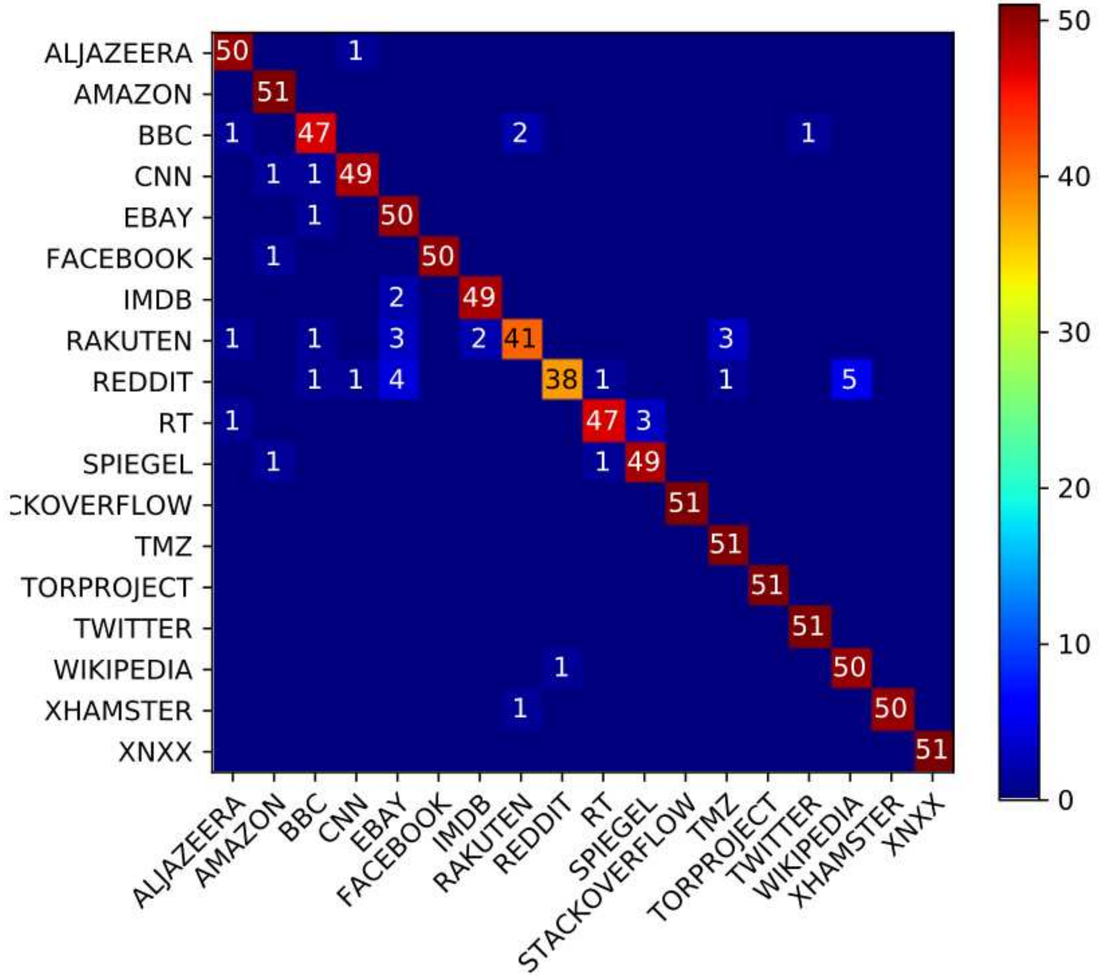


Website Classification

Evaluation: Subpage-Agnostic Domain Classification

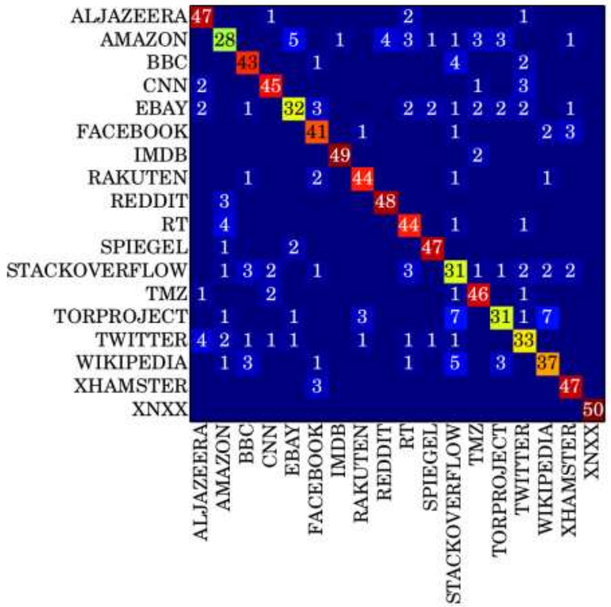
Panchenko et al. (2016)



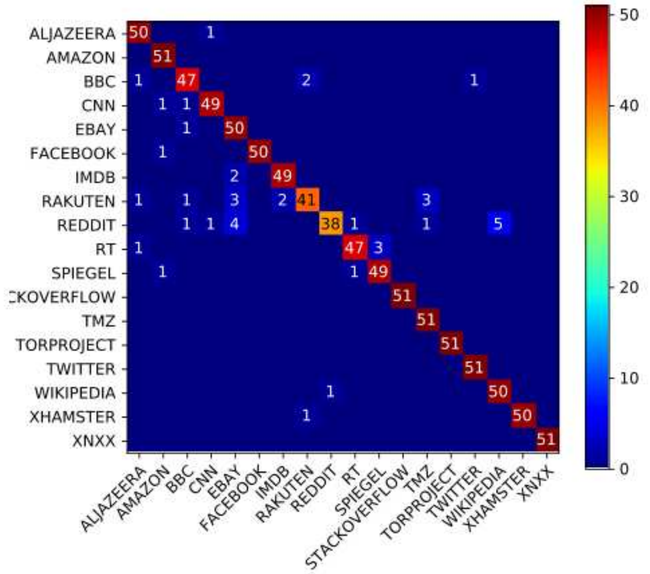


Panchenko et al. “Website Fingerprinting at Internet Scale” NDSS 2016

Evaluation: Subpage-Agnostic Domain Classification

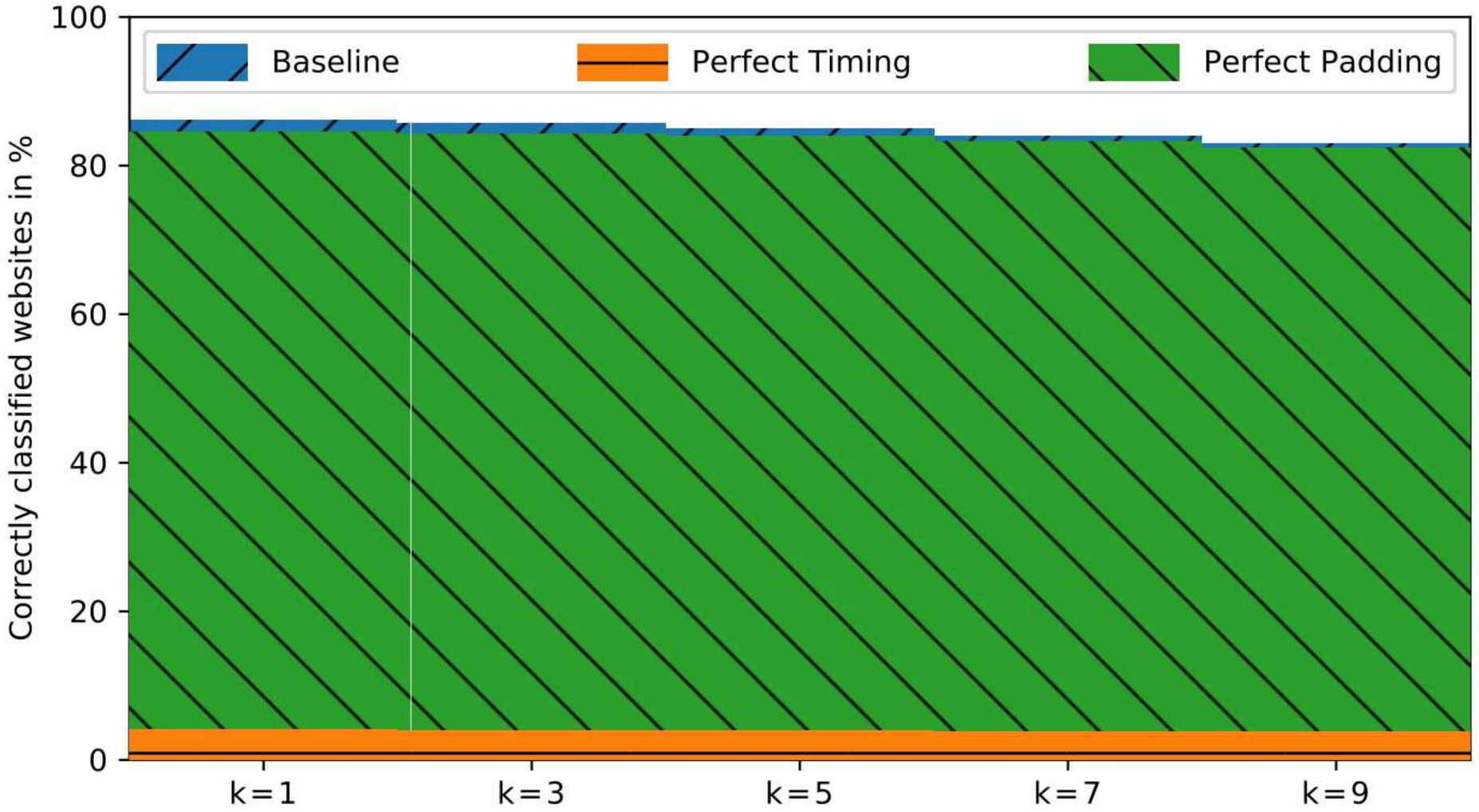


- Index page + 50 random
- 19.1 % vs. 4.7 % error
- Better on 15 / 18 domains
- HTTP
  - variable
  - Sizes + #Resources change
- DNS
  - “stable”
  - Resource domains are stable



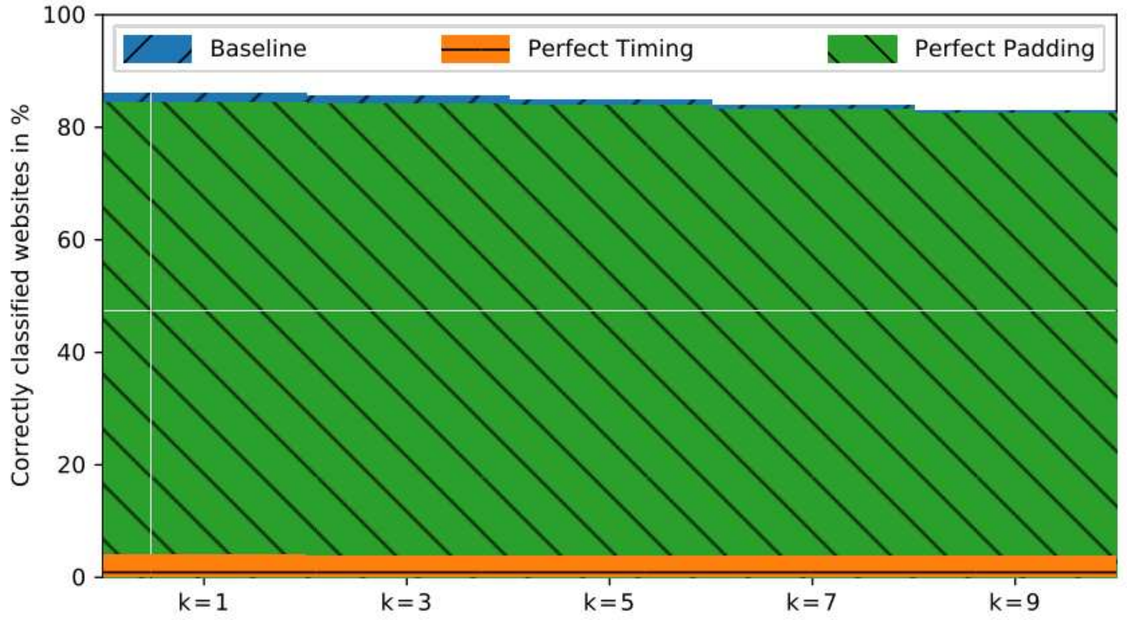
Panchenko et al. “Website Fingerprinting at Internet Scale” NDSS 2016

Countermeasures



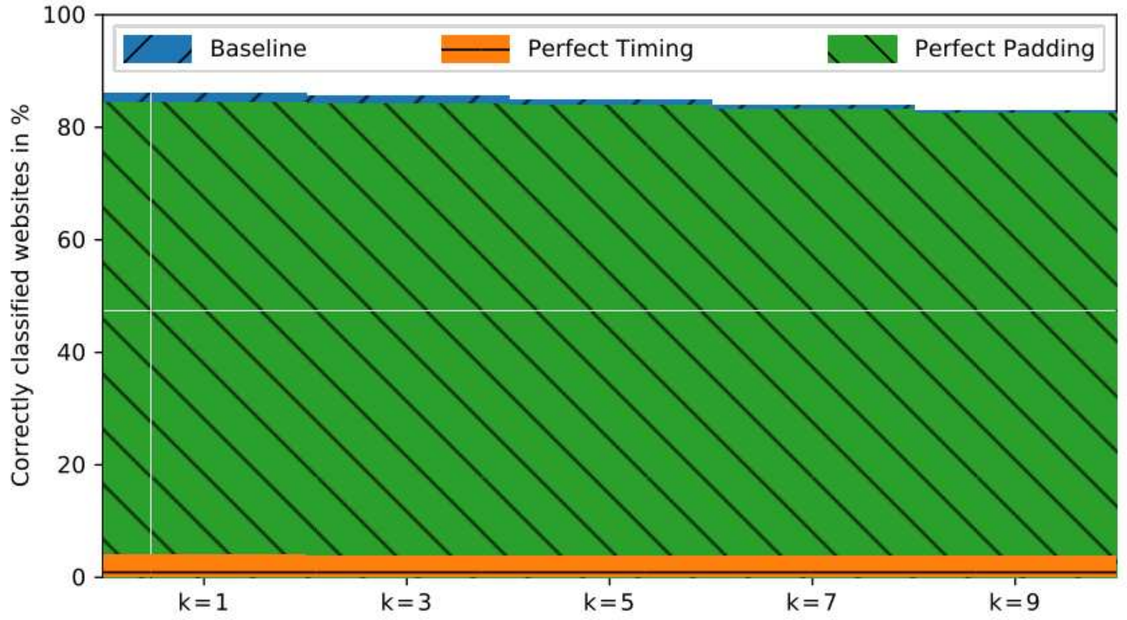
Countermeasures

- More entropy: Timing
- Existing padding scheme is great
  - 99.76 % are 468 bytes



Countermeasures

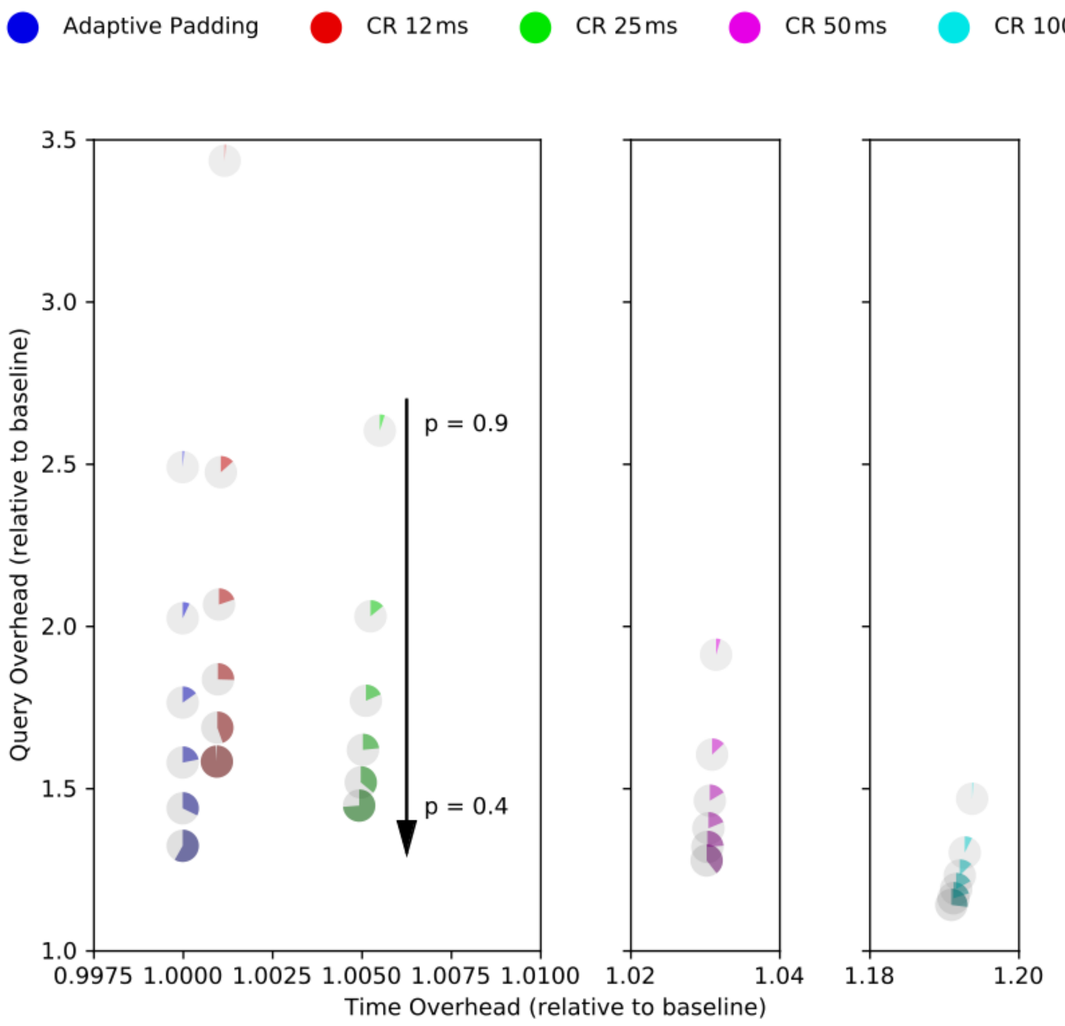
- More entropy: Timing
- Existing padding scheme is great
  - 99.76 % are 468 bytes
- Timing Defenses
  - Constant-Rate
  - Adaptive Padding[1]



[1] Shmatikov and Wang, “Timing analysis in low-latency mix networks: Attacks and defenses.” 2006

Countermeasures: Overheads

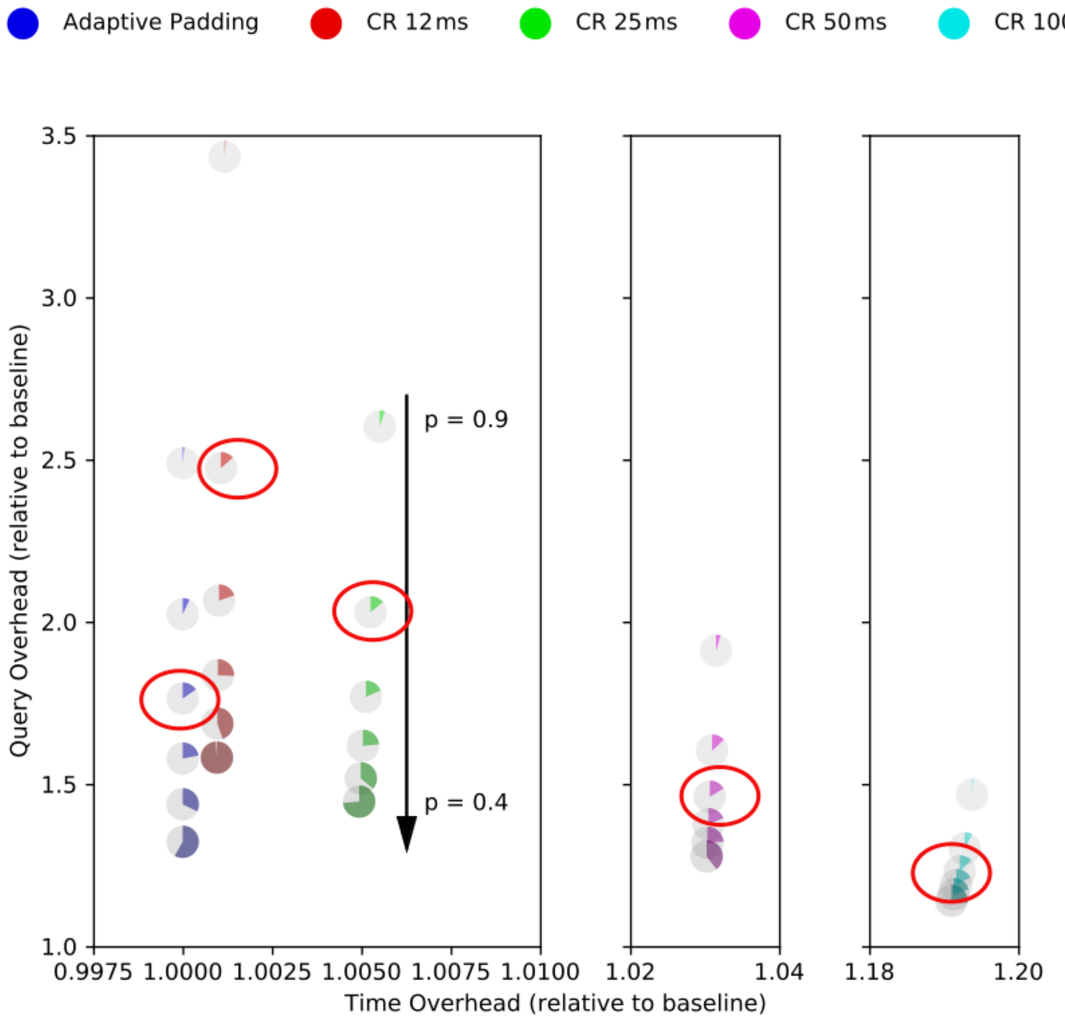
- Constant-Rate (CR)
  - Latency + Bandwidth Overhead
- Adaptive Padding (AP)
  - Bandwidth Overhead



5/10 DNS Sequences correct

Countermeasures: Overheads

- Constant-Rate (CR)
  - Latency + Bandwidth Overhead
- Adaptive Padding (AP)
  - Bandwidth Overhead

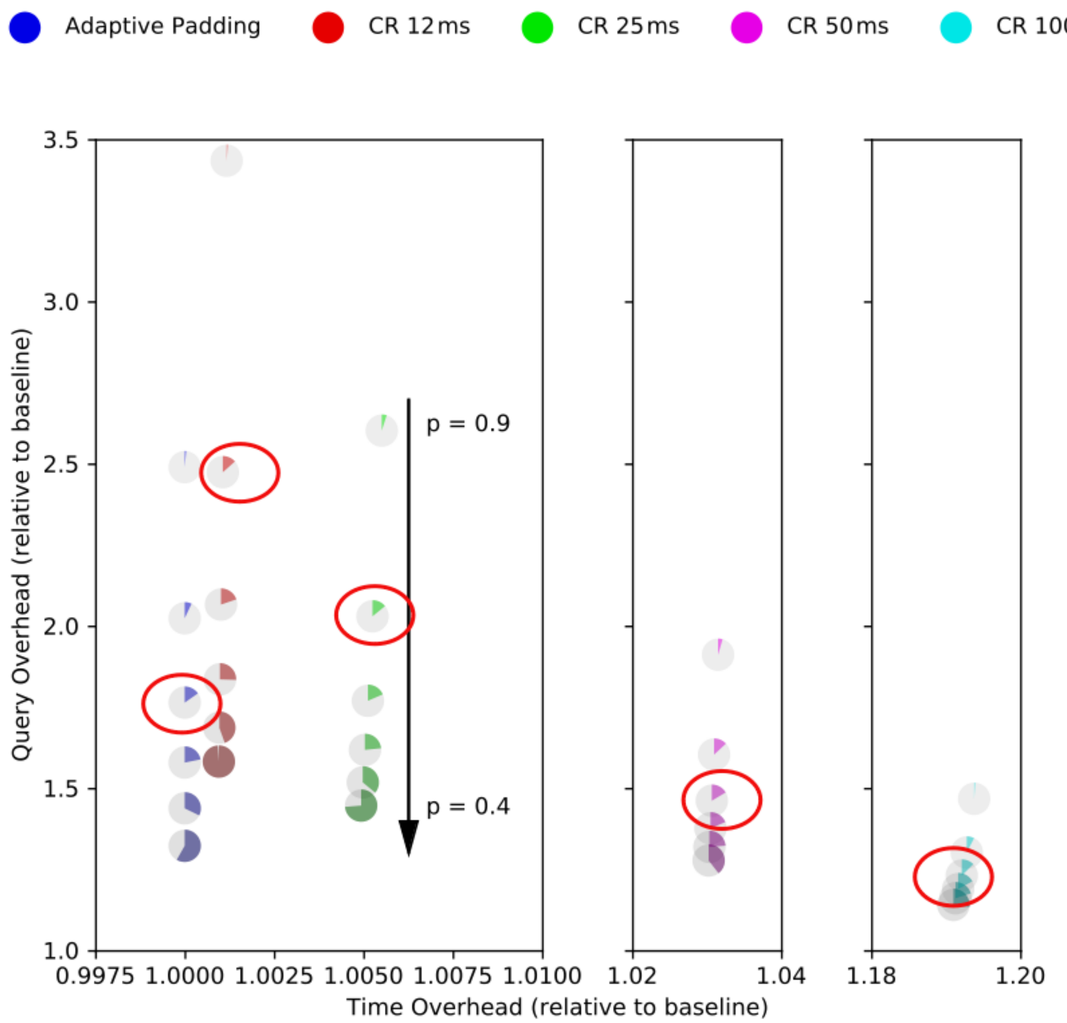


5/10 DNS Sequences correct

Countermeasures: Overheads

- Constant-Rate (CR)
  - Latency + Bandwidth Overhead
- Adaptive Padding (AP)
  - Bandwidth Overhead

- Good Defenses
  - Interactive use → AP
  - Constrained use → CR



5/10 DNS Sequences correct

Conclusion

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

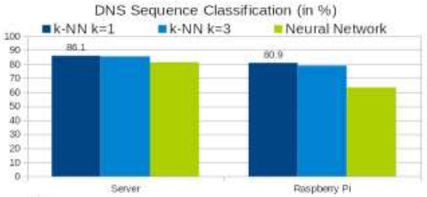
Privacy of DNS

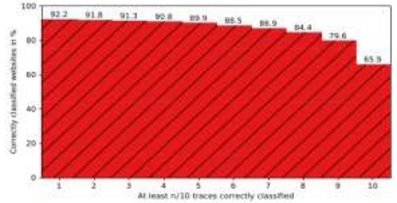
- RFC 8467: Block padding 128B / 468B
- k-NN with Edit-Distance
  - Customized weights
- Simple Neural Network
- Threat model like DoT/DoH

RFC 7830: The EDNS(0) Padding Option
RFC 8467: Padding Policies for Extension Mechanisms for DNS (EDNS(0))

Evaluation: Closed World

- Adversary knows all websites
- Dataset
  - Tranco List
  - 9235 websites / 10 sequences
  - Pi: 7699 websites / 4 sequences
- unbound 1.1.1.1

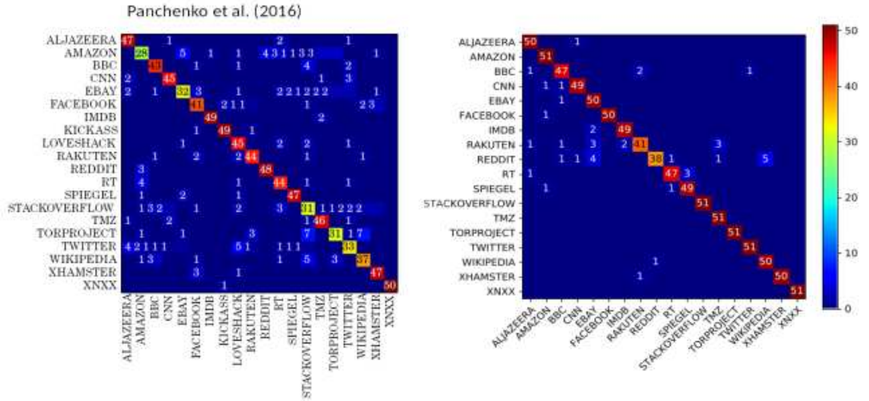




Website Classification

Evaluation: Subpage-Agnostic Domain Classification

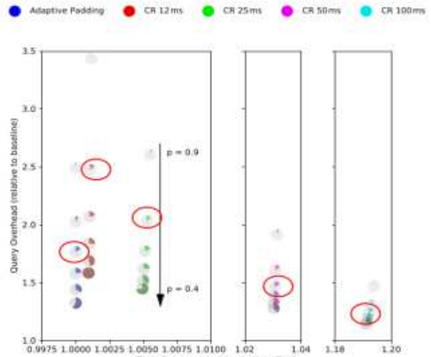
Panchenko et al. (2016)



Panchenko et al. "Website Fingerprinting at Internet Scale" NDSS 2016

Countermeasures: Overheads

- Constant-Rate (CR)
  - Latency + Bandwidth Overhead
- Adaptive Padding (AP)
  - Bandwidth Overhead
- Good Defenses
  - Interactive use → AP
  - Constrained use → CR



5/10 DNS Sequences correct

Conclusion

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

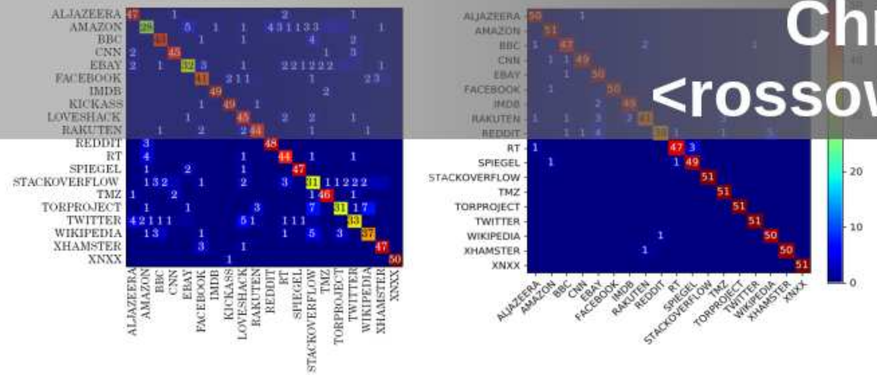
Privacy of DNS

- RFC 8467: Block padding 128B / 468B
- k-NN with Edit-Distance
  - Customized weights
- Simple Neural Network
- Threat model like DoT/DoH

RFC 7830: The EDNS(0) Padding Option
RFC 8467: Padding Policies for Extension Mechanisms for DNS (EDNS(0))

Evaluation: Subpage-Agnostic Domain Classification

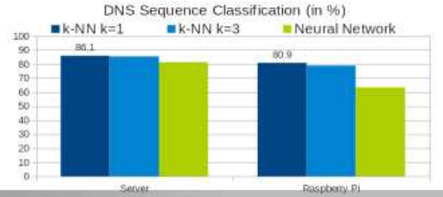
Panchenko et al. (2016)

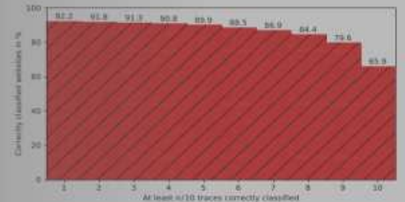


Panchenko et al. "Website Fingerprinting at Internet Scale" NDSS 2016

Evaluation: Closed World

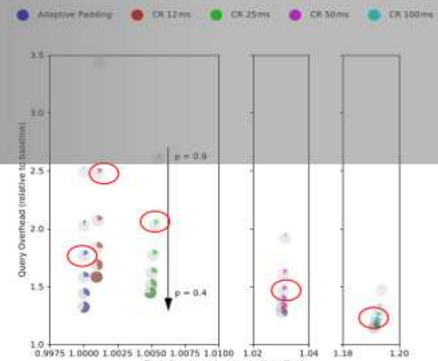
- Adversary knows all websites
- Dataset
  - Tranco List
  - 9235 websites / 10 sequences
  - Pi: 749 websites / 4 sequences
  - Lowbound 1.1.1.1





Website Classification

- Constant-Rate (CR)
- Accuracy + Bandwidth Overhead
- Bandwidth Overhead
- Good Defenses
  - Interactive use → AP
  - Constrained use → CR



5/10 DNS Sequences correct

Thank You!

Jonas Bushart
<jonas.bushart@cispa.saarland>
Christian Rossow
<rossow@cispa.saarland>