ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

XDRI Attacks - and - How to Enhance Resilience of Residential Routers

Philipp Jeitner, Haya Shulman, Lucas Teichmann and Michael Waidner

German National Research Center for Applied Cybersecurity ATHENE
Technical University of Darmstadt
Fraunhofer Institute for Secure Information Technology SIT

Outline

1. DNS in residential routers
2. Attacker Models
3. Attacks
4. Black & White-Box evaluation
5. Do we need DNS in routers?
6. Disclosure and Conclusion

DNS in residential routers

What is DNS?

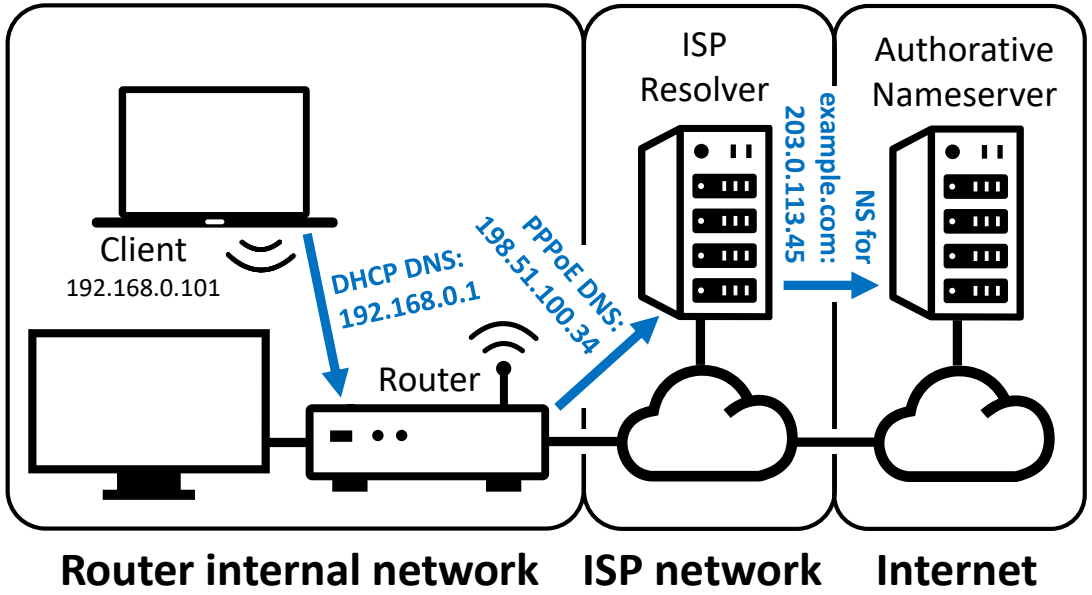
- Resolve domain names (example.com) to addresses (1.2.3.4)

How?

- Clients send DNS requests to router
- Router forwards to ISP/public resolver
- Resolver queries authoritative nameservers
- Router and Client are auto-configured

Attacks against DNS in routers

- Cache poisoning -> associate victim domain with attacker address -> allows traffic hijacking



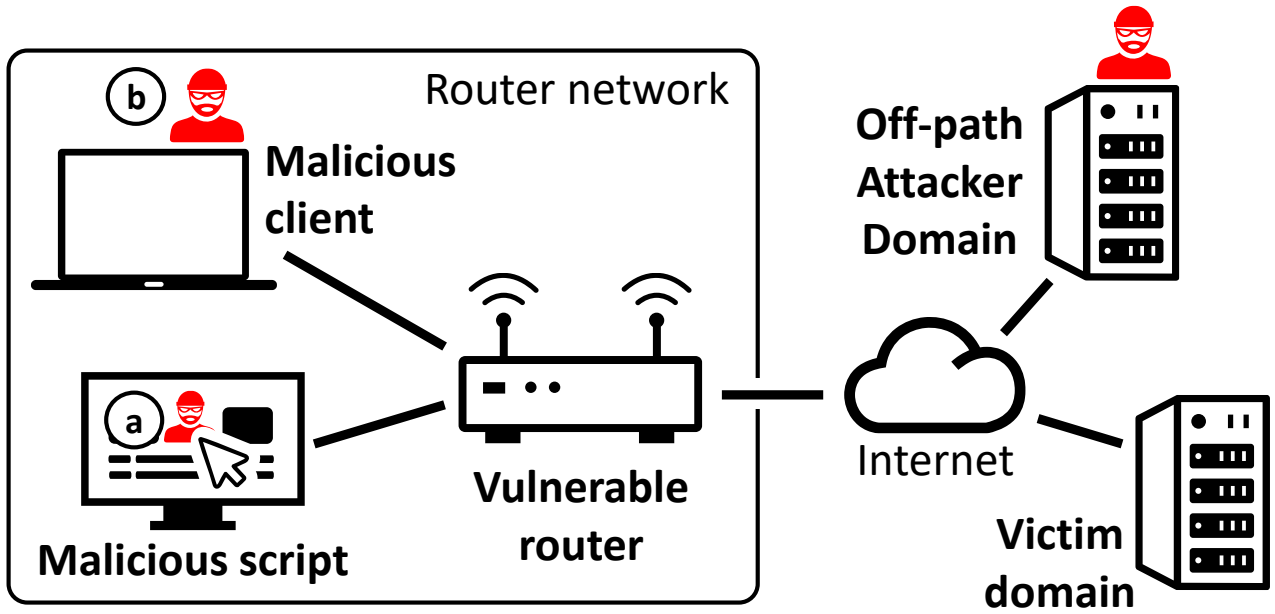
Attacker Models

(a) Malicious script

- Eg. Website controlled by the attacker
- Can only trigger standard A/AAAA queries via browser

(b) Malicious Client

- Eg. Laptop in public wifi
- Can Send arbitrary DNS messages
- Including unusual queries and/malformatted queries

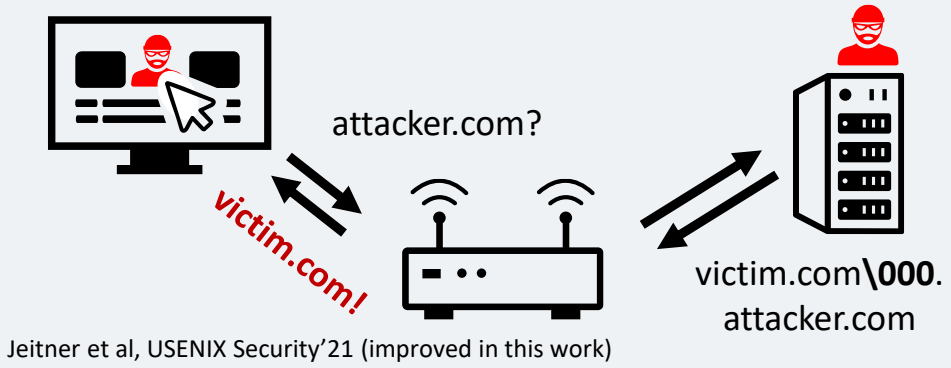


(b) Is a superset of (a)

Attacks and Vulnerabilities

Character misinterpretation

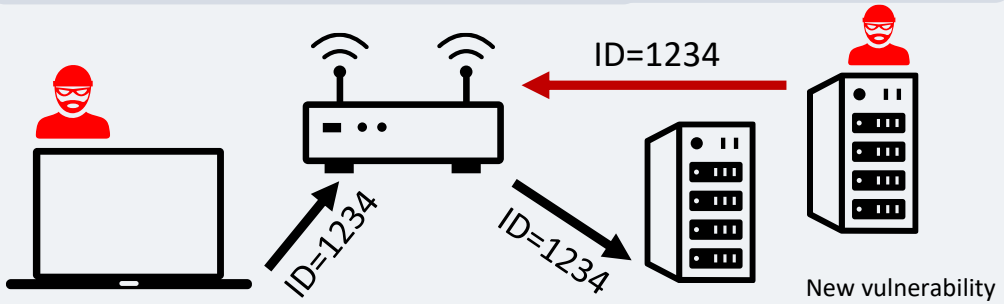
Attacker domain misinterpreted for victim domain



Jeitner et al, USENIX Security'21 (improved in this work)

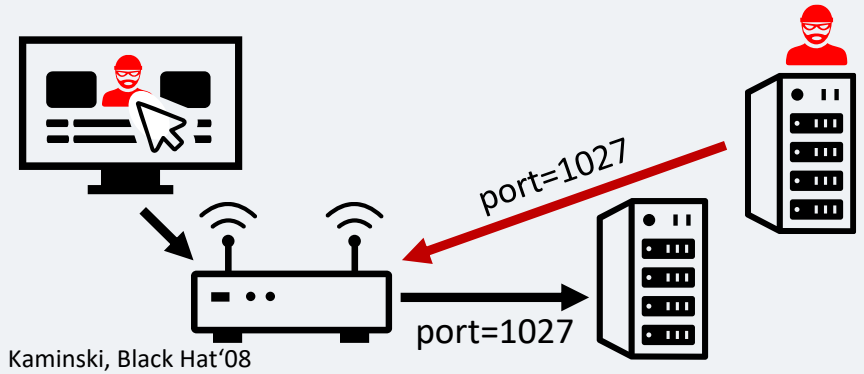
TXID forwarding

TXID value re-used from attacker-controlled query



Static UDP source port

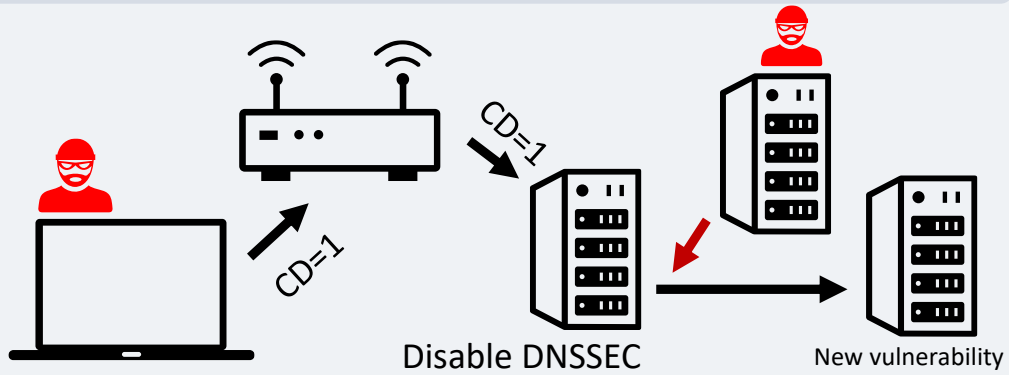
Static UDP port allows off-path injection



Kaminski, Black Hat'08

CD=1 forwarding

Checking disabled flag forwarded to disable DNSSEC



Black box evaluation: Scans and Lab tests

Internet-wide scans of 1.5M resolvers

- 8.1% of open resolvers vulnerable to misinterpretation
- Data suggested that these are forwarders

Forwarders in routers

- 36 physical devices tested
- 15 vulnerable to attacks

Ad-net study shows vulnerable routers are widely used

Vulnerability	Attacker Model	Impact	Vulnerable devices
Character misinterpretation	(a) Script	Cache poisoning	9
TXID forwarding	(b) Client	Cache poisoning	4
Static UDP source port	(a) Script	Cache poisoning	7
CD=1 forwarding	(b) Client	Disable DNSSEC	5

White box evaluation: What cause the issue?

Reverse-engineering router firmware

- Verified programming mistakes which cause the vulnerabilities

Many forwarders are not written professionally

- unmaintained open-source software from 2001
- PNRG for UDP port seeded with uninitialized device clock

Study of Github forwarders shows the same vulnerabilities in 8/10 cases

Shows that this is more a problem of less-popular DNS implementations, not only routers

Do we need DNS in routers?

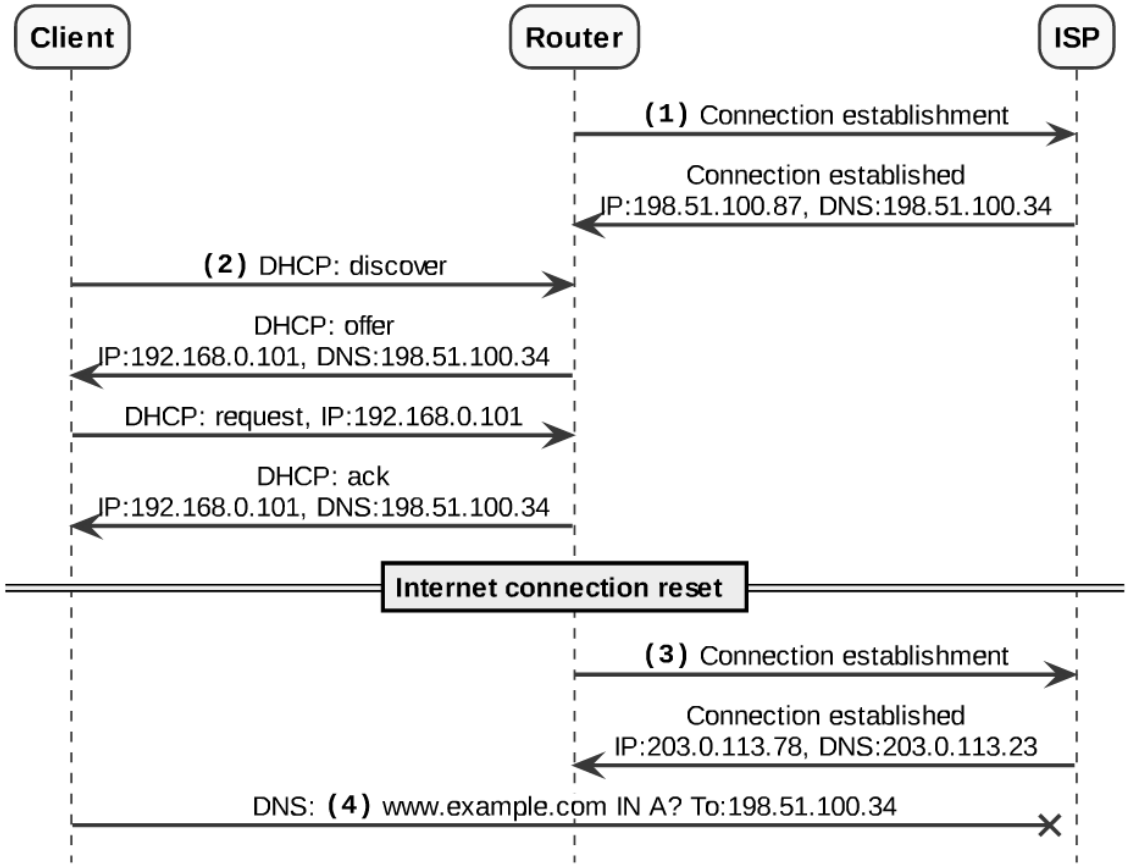
Do we need caching in routers?

- Not really. OSes and browsers contain their own caches.

Problem: Network management separation

- Clients expect DNS server IP in DHCP offer
- Router cannot communicate address changes to clients
- Forwarding needed to separate network configuration of internal network

Replace error-prone caching forwarders with NAT rules?



Disclosure and Conclusion

All vendors were contacted prior to publication

- 3 patched, 2 EOL, some with ongoing contact
- CVE-2022-{33988, 33989, 33990, 33991, 33992, 33993, 33994, 33995}, HWPSIRT-2022-82592

Open source implementations (used in routers)

- dnrd, dnsproxy-nexgen, totd (all unpatched cause of age)

Conclusion

- Cache poisoning still a problem in routers
- Vulnerabilities are wide spread and implementations are often not well built
- Removing DNS from routers might be a solution in some cases

Thank You!

Philipp Jeitner, TU Darmstadt/Fraunhofer SIT
philipp.jeitner@sit.fraunhofer.de

תודה רבה!

çok teşekkürler

谢谢

Merci beaucoup!

Thank you very much!

Dank je wel!

Vielen Dank!

Muchas gracias

ありがとうございました

Dziękuję!

zor spas

Grazie mille!

اشكرك