互联网域名系统安全
国际学术研究前沿及趋势分析

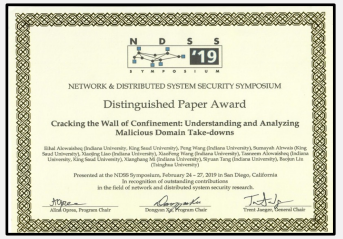
刘保君 助理教授

清华大学网络研究院

个人简介

- 教育与工作经历
  - 2022/12 - 至今　　清华大学网络研究院　助理教授
  - 2020/11 - 2022/11　清华大学网络研究院　博士后
  - 2015/09 - 2020/10　清华大学计算机系　　工学博士
- 主要研究方向
  - 互联网测量、网络基础设施安全、网络犯罪检测及对抗
- 学术荣誉以及学术会议重要奖项
  - 2020年 清华大学 “水木学者”
  - 2022年 ACM中国计算机安全分会 “学术新星”

网络研究应用奖ANRP



NDSS杰出论文奖

DSN最佳论文奖

互联网域名系统 -- 被遗忘的互联网基石

- DNS基本功能：域名字符串 ⇔ 主机地址
- 应用层的路由功能
  - 电子邮件路由（MX）
  - 内容分发网络（CDN）
- 作为信任锚点
  - 邮件发件人真实性的验证（SPF)
  - 数字公钥证书申请的验证

    Domain Ownership Validation
- 域名系统是互联网基础性服务，影响几乎所有上层网络应用的安全和稳定。

应用层流量调度

网站公钥证书申请

电子邮件身份认证

安全厂商威胁情报

近年来研究团队围绕互联网域名系统安全及测量开展的一系列工作

- *2018年*，测量发现全球范围内的大规模域名解析路径劫持现象（USENIX Security）
- *2019年*，测量全球范围加密域名协议的部署应用现状及安全缺陷（IMC，ANRP奖）
- *2020年*，发现针对DNS转发服务器的新型缓存污染攻击（USENIX Security）
- *2020年*，发现基于侧信道的DNS服务器新型缓存污染攻击（CCS，Best Paper）
- *2021年*，测量评估GDPR对域名注册数据WHOIS可用性的负面影响（NDSS）
- *2022年*，提出了一种算法透明、抗操控的域名流行度排名方法（USENIX Security）
- *2023年*，发现了域名授权机制安全缺陷，可致使恶意域名无法移除（NDSS）
- *2023年*，系统评估云服务平台中域名劫持接管的安全风险（ACM SIGMETRICS）
- *2023年*，发现了一种基于域名解析角色混用的新型缓存污染攻击（USENIX Security）

- *2018年-*，连续多年对全球域名解析服务开展安全性测量
- *2018年-*，持续收集并分析公共 DNS 114 域名解析日志

系统梳理互联网“域名系统安全研究”的前沿学术成果

梳理总结前沿学术研究成果
国际学术界关于域名系统安全研究趋势

- ✅ **域名协议设计与软件实现新型攻击面**
- ✅ 域名解析性能等测量研究工作
- ✅ 域名滥用行为检测与分析
- ✅ 域名安全监管机制相关研究

时间：2018年 - 2023年

安全论文检索：*https://secpaper.cn*

近五年国际网络安全研究四大顶会域名系统安全相关研究论文 -1/3

1. Philipp Jeitner and Haya Shulman. 2021. Injection Attacks Reloaded: Tunnelling Malicious Payloads over DNS. In 30th USENIX Security Symposium (USENIX Security '21). USENIX Association, Boston, MA, 3165–3182.
2. Markus Brandt, Tianxiang Dai, Amit Klein, Haya Shulman, and Michael Waidner. 2018. Domain Validation++ For MitM-Resilient PKI. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS '18). Association for Computing Machinery, New York, NY, USA, 2060–2076.
3. Xiaofeng Zheng, Chaoyi Lu, Jian Peng, Qiushi Yang, Dongjie Zhou, Baojun Liu, Keyu Man, Shuang Hao, Haixin Duan, and Zhiyun Qian. 2020. Poison Over Troubled Forwarders: A Cache Poisoning Attack Targeting DNS Forwarding Devices. In 29th USENIX Security Symposium (USENIX Security '20). USENIX Association, Boston, MA, 577–593.
4. Keyu Man, Zhiyun Qian, Zhongjie Wang, Xiaofeng Zheng, Youjun Huang, and Haixin Duan. 2020. DNS Cache Poisoning Attack Reloaded: Revolutions with Side Channels. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS '20). Association for Computing Machinery, New York, NY, USA, 1337–1350.
5. Keyu Man, Xin'an Zhou, and Zhiyun Qian. 2021. DNS Cache Poisoning Attack: Resurrections with Side Channels. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS '21). Association for Computing Machinery, New York, NY, USA, 3400–3414.
6. Tianxiang Dai, Haya Shulman, and Michael Waidner. 2021. Let's Downgrade Let's Encrypt. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS '21). Association for Computing Machinery, New York, NY, USA, 1421–1440.
7. Tianxiang Dai, Philipp Jeitner, Haya Shulman, and Michael Waidner. 2021. The Hijackers Guide To The Galaxy: Off-Path Taking Over Internet Resources. In 30th USENIX Security Symposium (USENIX Security '21). USENIX Association, Boston, MA, 3147–3164.
8. Amit Klein. 2021. Cross Layer Attacks and How to Use Them (for DNS Cache Poisoning, Device Tracking and More). In 42nd IEEE Symposium on Security and Privacy (SP '21). IEEE Computer Society, Washington, DC, USA, 1179–1196.

近五年国际网络安全研究四大顶会域名系统安全相关研究论文 -2/3

9. Philipp Jeitner, Haya Shulman, Lucas Teichmann, and Michael Waidner. 2022. XDRI Attacks - and - How to Enhance Resilience of Residential Routers. In 31st USENIX Security Symposium (USENIX Security '22). USENIX Association, Boston, MA, 4473–4490.
10. Xiang Li, Chaoyi Lu, Baojun Liu, Qifan Zhang, Zhou Li, Haixin Duan and Qi Li. 2023. The Maginot Line: Attacking the Boundary of DNS Caching Protection. In 32nd USENIX Security Symposium (USENIX Security '23). USENIX Association, Boston.
11. Eihal Alowaisheq, Siyuan Tang, Zhihao Wang, Fatemah Alharbi, Xiaojing Liao, and XiaoFeng Wang. 2020. Zombie Awakening: Stealthy Hijacking of Active Domains through DNS Hosting Referral. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS '20). Association for Computing Machinery, New York, NY, USA, 1307–1322.
12. Marco Squarcina, Mauro Tempesta, Lorenzo Veronese, Stefano Calzavara, and Matteo Maffei. 2021. Can I Take Your Subdomain? Exploring Same-Site Attacks in the Modern Web. In 30th USENIX Security Symposium (USENIX Security '21). USENIX Association, Boston, MA, 2917–2934.
13. Xiang Li, Baojun Liu, Xuesong Bai, Mingming Zhang, Qifan Zhang, Zhou Li, Haixin Duan, and Qi Li. 2023. Ghost Domain Reloaded: Vulnerable Links in the Domain Name Delegation and Revocation. Processedings of *The 30th Annual Network and Distributed Security Symposium (NDSS). Internet Society.*
14. Baojun Liu, Chaoyi Lu, Hai-Xin Duan, Ying Liu, Zhou Li, Shuang Hao, and Min Yang. 2018. Who Is Answering My Queries: Understanding and Characterizing Interception of the DNS Resolution Path. In 27th USENIX Security Symposium (USENIX Security '18). USENIX Association, Boston, MA, 1113–1128.
15. Nguyen Phong Hoang, Arian Akhavan Niaki, Jakub Dalek, Jeffrey Knockel, Pellaeon Lin, Bill Marczak, Masashi Crete-Nishihata, Phillipa Gill, and Michalis Polychronakis. 2021. How Great is the Great Firewall? Measuring China's DNS Censorship. In 30th USENIX Security Symposium (USENIX Security '21). USENIX Association, Boston, MA, 3381–3398.
16. Abhishek Bhaskar and Paul Pearce. 2022. Many Roads Lead To Rome: How Packet Headers Influence DNS Censorship Measurement. In 31st USENIX Security Symposium (USENIX Security '22). USENIX Association, Boston, MA, 449–464.

近五年国际网络安全研究四大顶会域名系统安全相关研究论文 -3/3

17. Alden Hilton, Casey Deccio, and Jacob Davis. 2023. Fourteen Years in the Life: A Root Server's Perspective on DNS Resolver Security. In 32nd USENIX Security Symposium (USENIX Security '23). USENIX Association, Boston.

18. Rasmus Dahlberg and Tobias Pulls. 2023. Timeless Timing Attacks and Preload Defenses in Tor's DNS Cache. In 32nd USENIX Security Symposium (USENIX Security '23). USENIX Association, Boston.

19. Yehuda Afek, Anat Bremler-Barr, and Shani Stajnrod. 2023. NRDelegationAttack: Complexity DDoS attack on DNS Recursive Resolvers. In 32nd USENIX Security Symposium (USENIX Security '23). USENIX Association, Boston.

20. Wei Xu, Xiang Li, Chaoyi Lu, Baojun Liu, Jia Zhang, Jianjun Chen, Tao Wan and Haixin Duan. 2023. TsuKing: Coordinating DNS Resolvers and Queries into Potent DoS Amplifiers. In Proceedings of The 30th ACM SIGSAC Conference on Computer and Communications Security (CCS '23).

21. Fenglu Zhang, Baojun Liu, Eihal Alowaisheq, Jianjun Chen, Chaoyi Lu, Linjian Song, Yong Ma, Ying Liu, Haixin Duan and Min Yang. 2023. Silence is not Golden: Disrupting the Load Balancing of Authoritative DNS Servers. In Proceedings of The 30th ACM SIGSAC Conference on Computer and Communications Security (CCS '23).

22. Samuel Schüppen, Dominik Teubert, Patrick Herrmann, and Ulrike Meyer. 2018. FANCI : Feature-based Automated NXDomain Classification and Intelligence. In 27th USENIX Security Symposium (USENIX Security '18). USENIX Association, Boston, MA, 1165–1181.

23. Eihal Alowaisheq, Peng Wang, Sumayah A. Alrwais, Xiaojing Liao, XiaoFeng Wang, Tasneem Alowaisheq, Xianghang Mi, Siyuan Tang, and Baojun Liu. 2019. Cracking the Wall of Confinement: Understanding and Analyzing Malicious Domain Take-downs. In 26th Annual Network and Distributed System Security Symposium (NDSS '19). Internet Society, Reston, USA.

近年来域名系统安全学术论文的基础信息统计与分析

- 论文所录用的学术会议
- 该领域的主要研究机构

序	学术会议	论文
1	USENIX Security	13
2	ACM CCS	7
3	NDSS	2
4	IEEE S&P	1

序	研究机构	论文
1	Tsinghua University	8
2	TU Darmstadt	5
3	University of California, Riverside	3
4	University of Texas at Dallas	2
4	Bar-Ilan University	2
4	University of California, Irvine	2
4	Indiana University	2
4	King Saud University	2

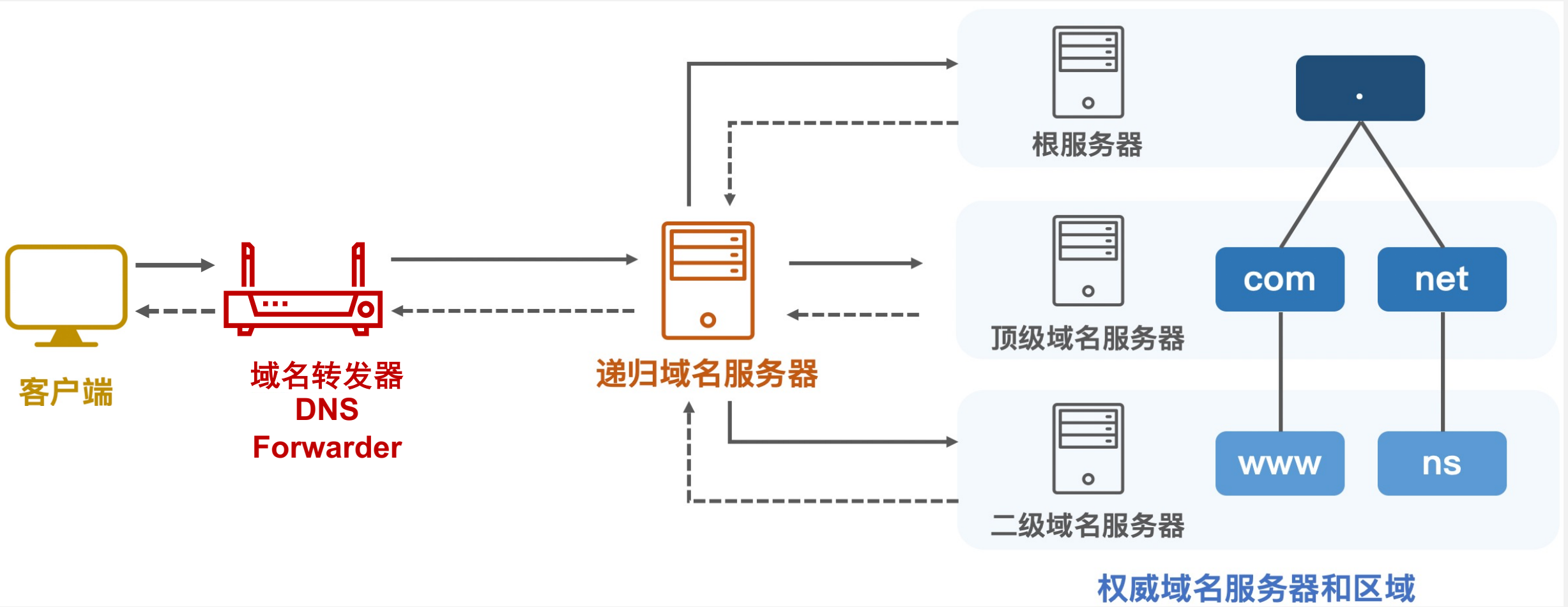
内容提纲 – 三类主要研究话题

话题一： **新型域名缓存污染攻击** （10篇）

话题二： **域名授权机制安全威胁** （3篇）

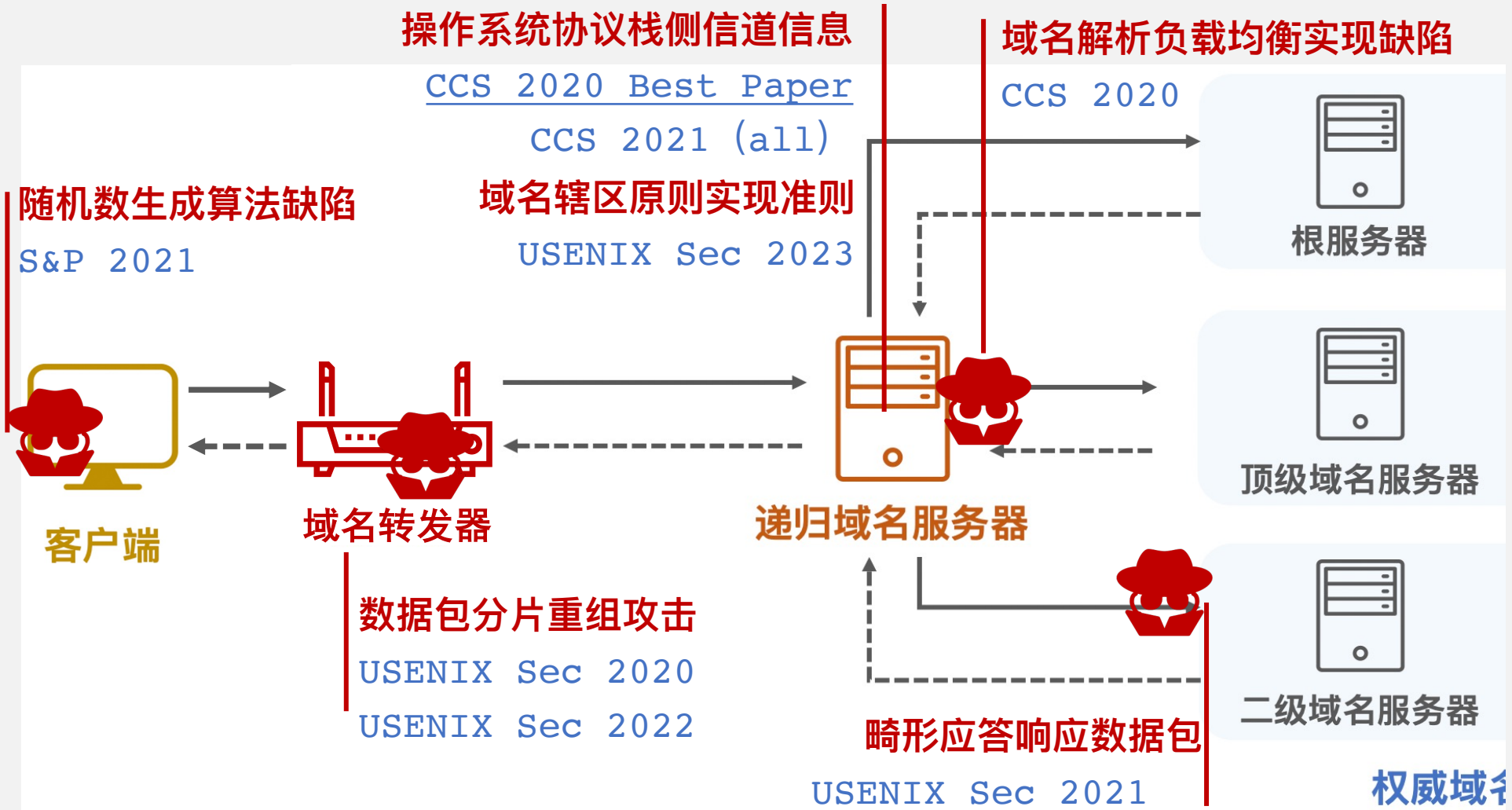
话题三： **域名解析流量规模操控** （3篇）

新型域名缓存污染攻击 -- 安全威胁模型的延展



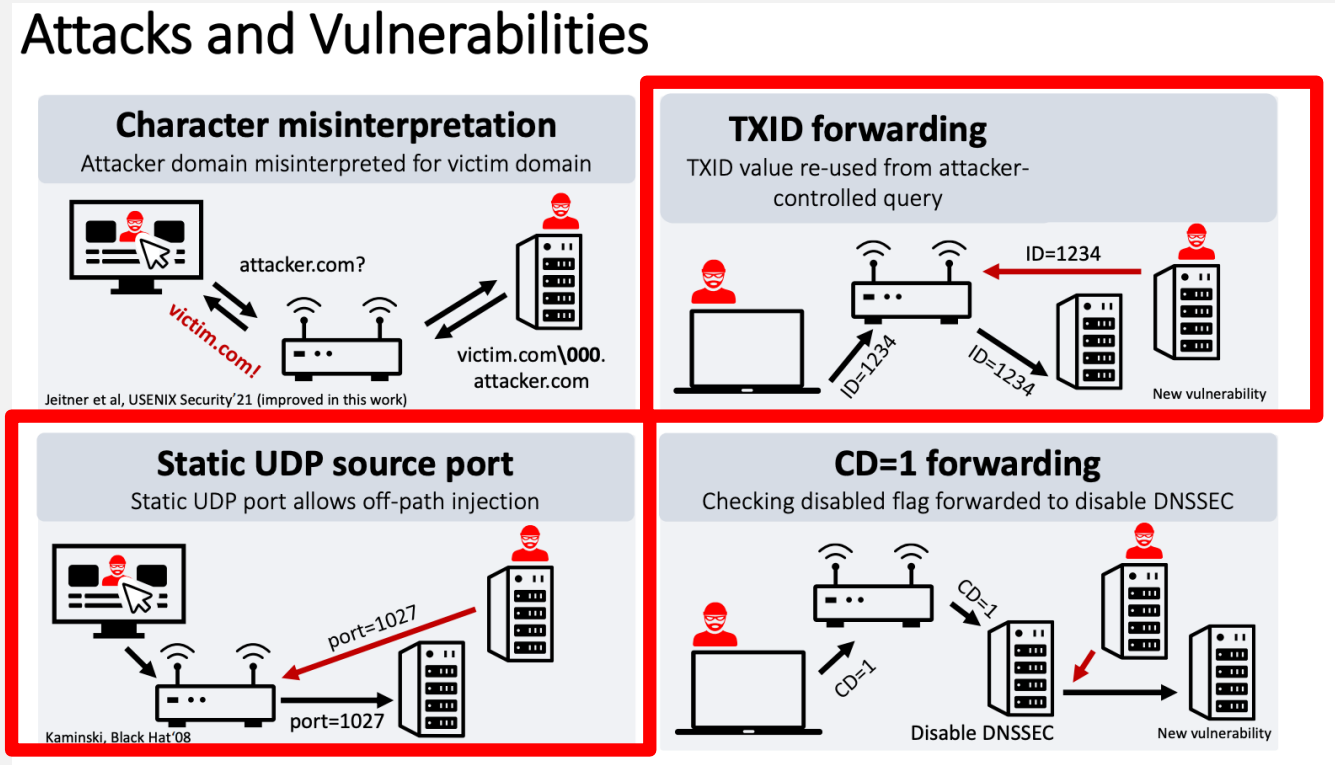
域名解析环节涉及到的主要角色

新型域名缓存污染攻击 -- 安全威胁模型的延展



一、针对 DNS 转发器的缓存污染攻击 （1）

仍有部分 DNS 转发器的代码实现，不遵循最佳 RFC 安全实践
- 域名解析报文交互过程：TXID随机化不足，采用静态源端口

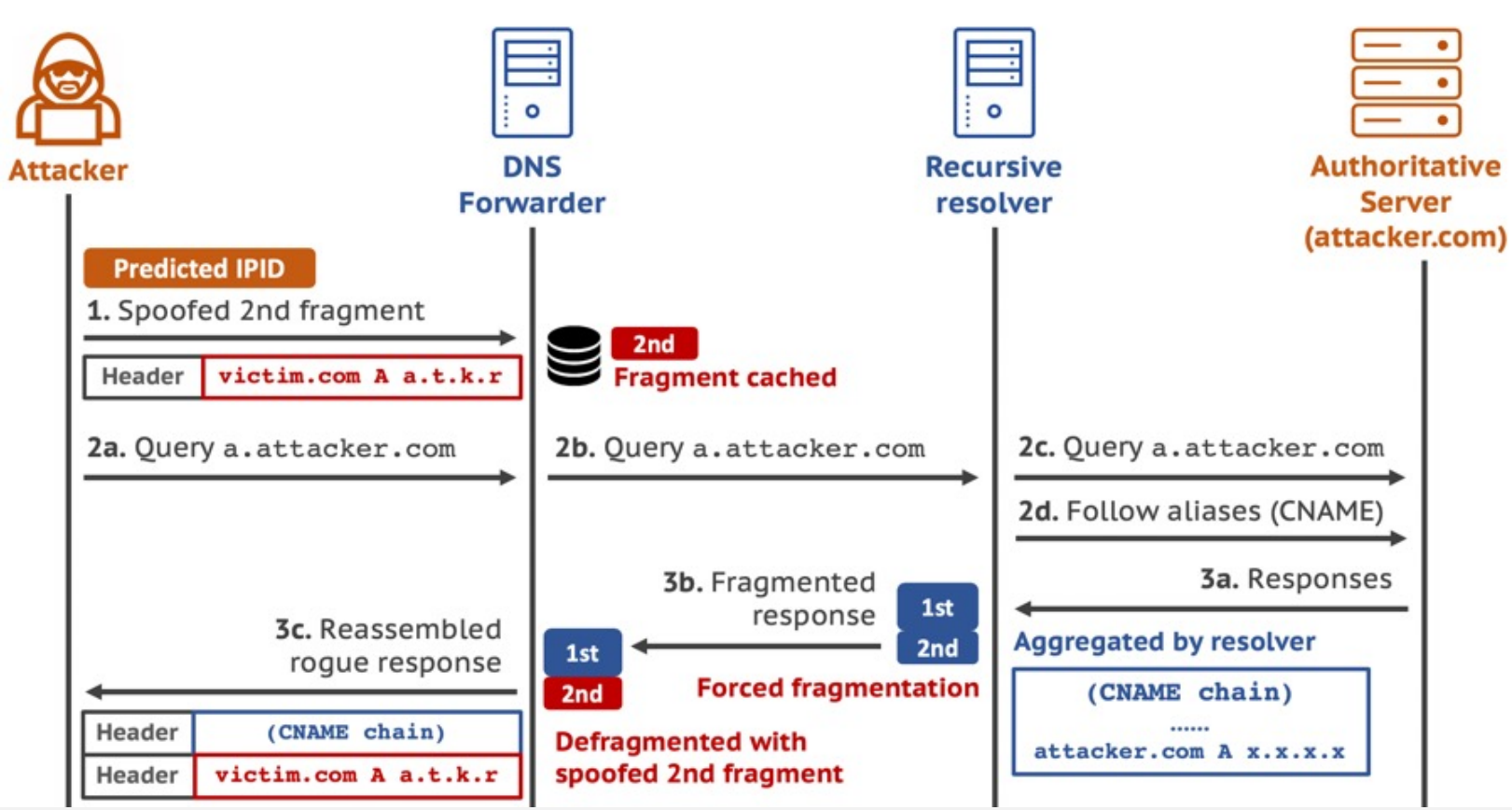


* USENIX Sec 2022. XDRI Attacks - and - How to Enhance Resilience of Residential Routers.

一、针对 DNS 转发器的缓存污染攻击 （2）

基于数据包分片重组的新型DNS缓存污染技术，影响7%互联网用户

影响了2款主流DNS软件，8家常见的路由器硬件厂商



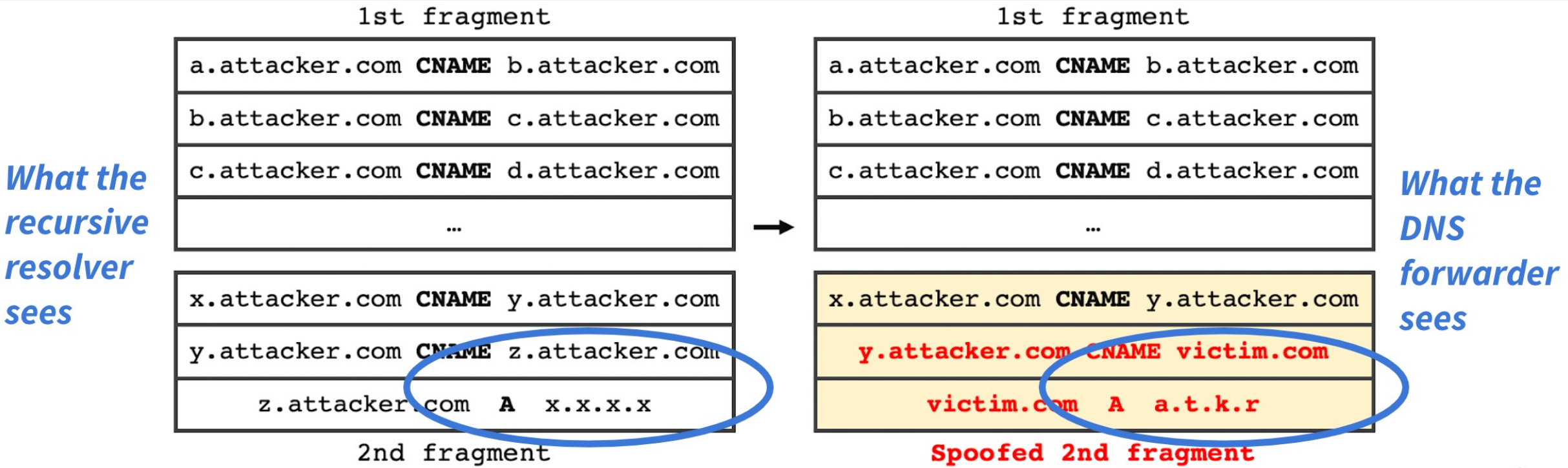
研究团队入选
GeekPwn极棒名人堂

* USENIX Sec 2020. Poison Over Troubled Forwarders: A Cache Poisoning Attack Targeting DNS Forwarding Devices.

基于数据包分片重组的 DNS 转发器缓存污染攻击

基于数据包分片重组的新型DNS缓存污染技术，影响国内7%的互联网用户

该漏洞影响了2款主流DNS软件，8家常见的路由器硬件厂商



* USENIX Sec 2020. Poison Over Troubled Forwarders: A Cache Poisoning Attack Targeting DNS Forwarding Devices.

如何放大域名缓存攻击的危害，寻求影响更上层的网络服务?

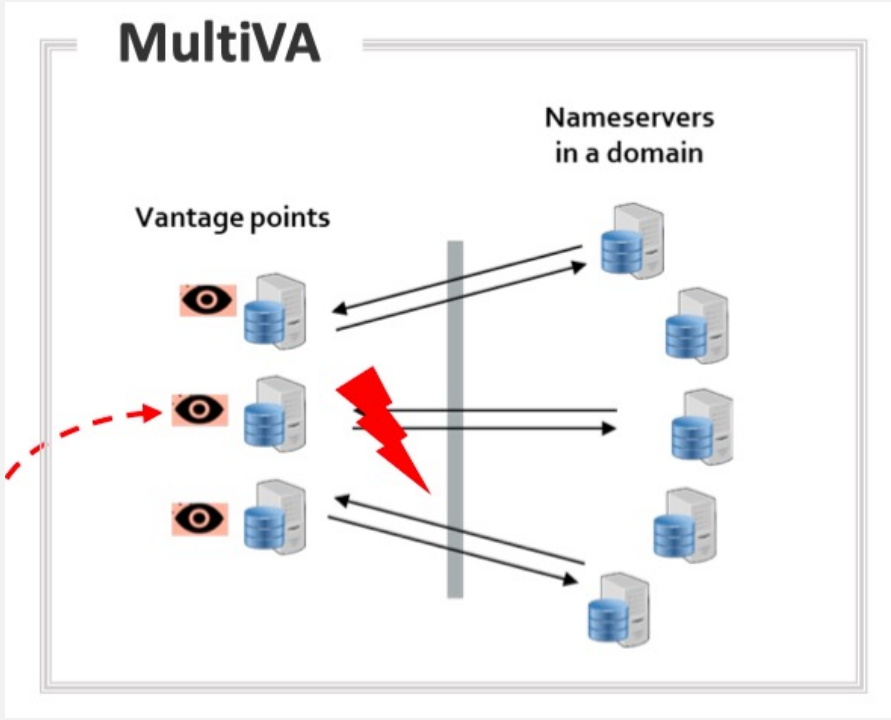
利用域名缓存污染攻击，冒充知名域名所有者，申请数字签名证书

Domain Validation

Who owns that domain?

"On the Internet, nobody knows you're a dog."

https://www.flickr.com/photos/ben_lawson/155595430
CC BY-NC-ND 2.0



研究证书颁发机构域名所有权验证的缺陷，提高缓存污染攻击的成功率。

* CCS 2018: Domain Validation++ For MitM-Resilient PKI.
* CCS 2021: Let's Downgrade Let's Encrypt

内容提纲 – 三类主要研究话题

话题一： 新型域名缓存污染攻击（10篇）

话题二： **域名授权机制安全威胁** （3篇）

话题三： 域名解析流量规模操控 （3篇）

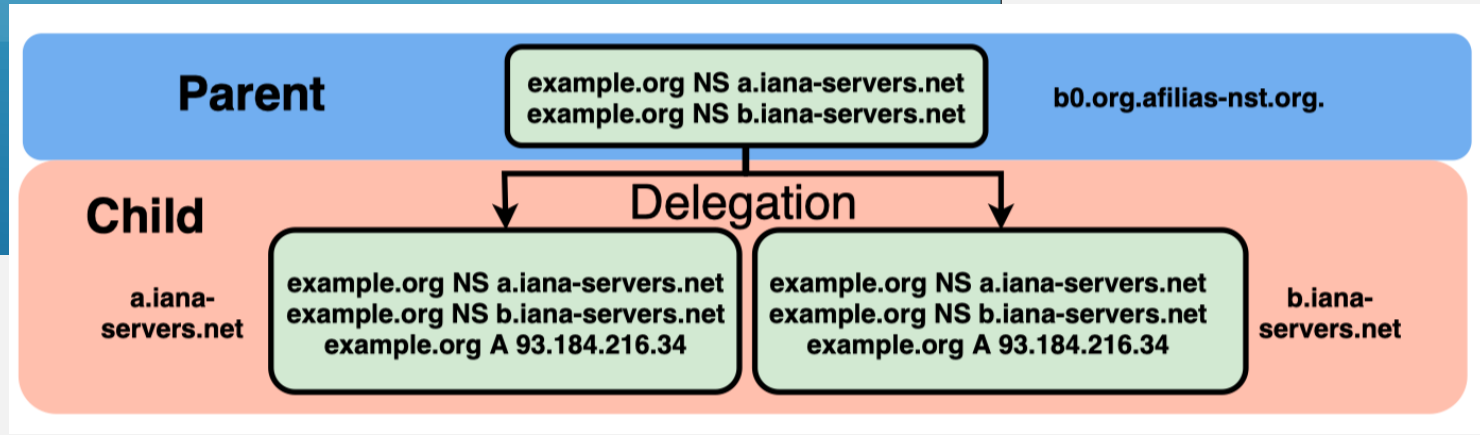
域名空间的层级授权机制： 父域与子域授权记录的冲突

A key mechanism that enables the DNS to be hierarchical and distributed is delegation

The DNS hierarchy is organized in parent and child zones typically managed by different entities

Different zones need to share common information (NS records) about which are the authoritative name servers for a given domain.

DNS AND DELEGATIONS



* PAM 2020, When parents and children disagree: Diving into DNS delegation inconsistency

安全风险一：域名解析链中的隐蔽劫持

一类特殊的域名授权记录配置现象

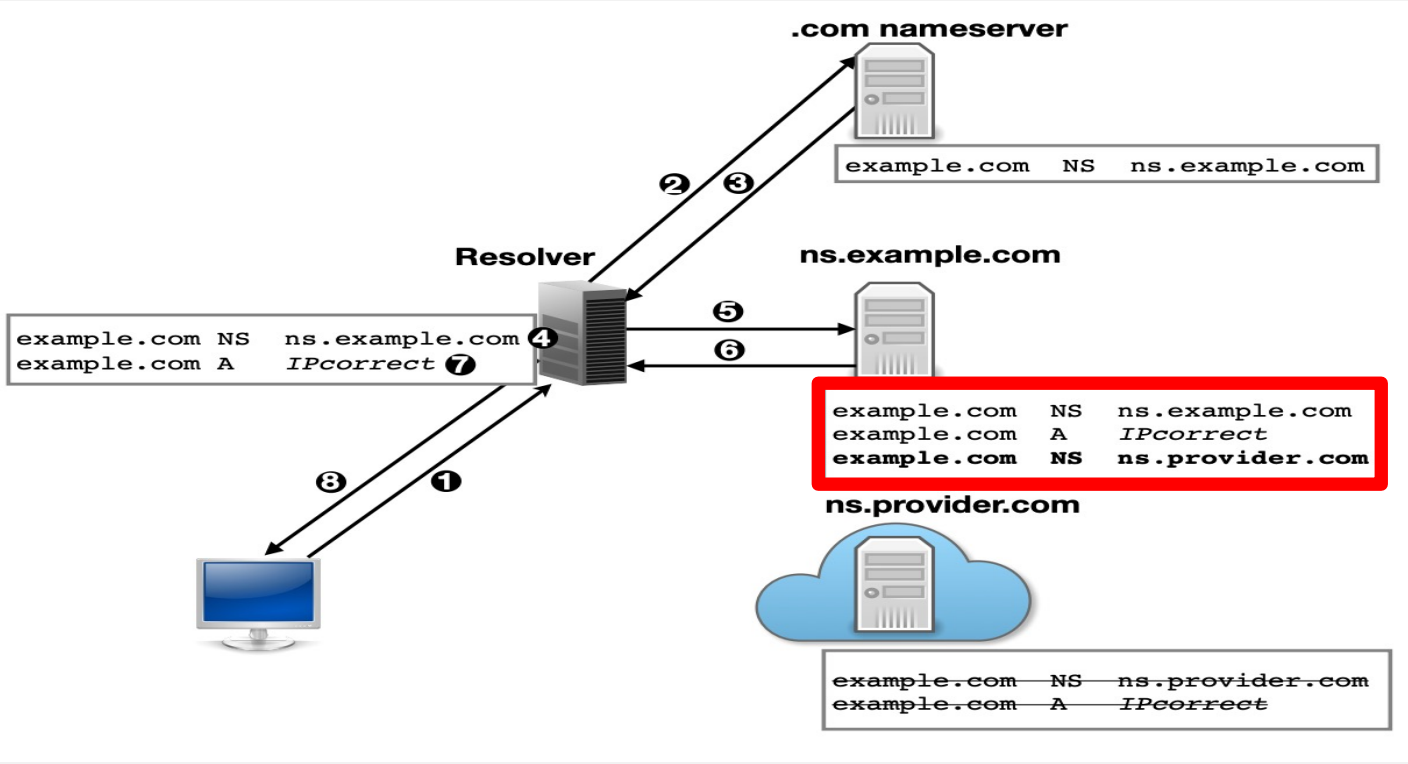
- 父域授权记录

  example.com NS ns.example.com

- 子域授权记录

  example.com NS ns.example.com

  ~~example.com NS ns.provider.com~~



云服务时代下，域名解析托管愈发普遍，引入了僵尸授权记录现象。

* CCS 2020. Zombie Awakening: Stealthy Hijacking of Active Domains through DNS Hosting Referral.

安全风险一：域名解析链中的隐蔽劫持

一类特殊的域名授权记录配置现象

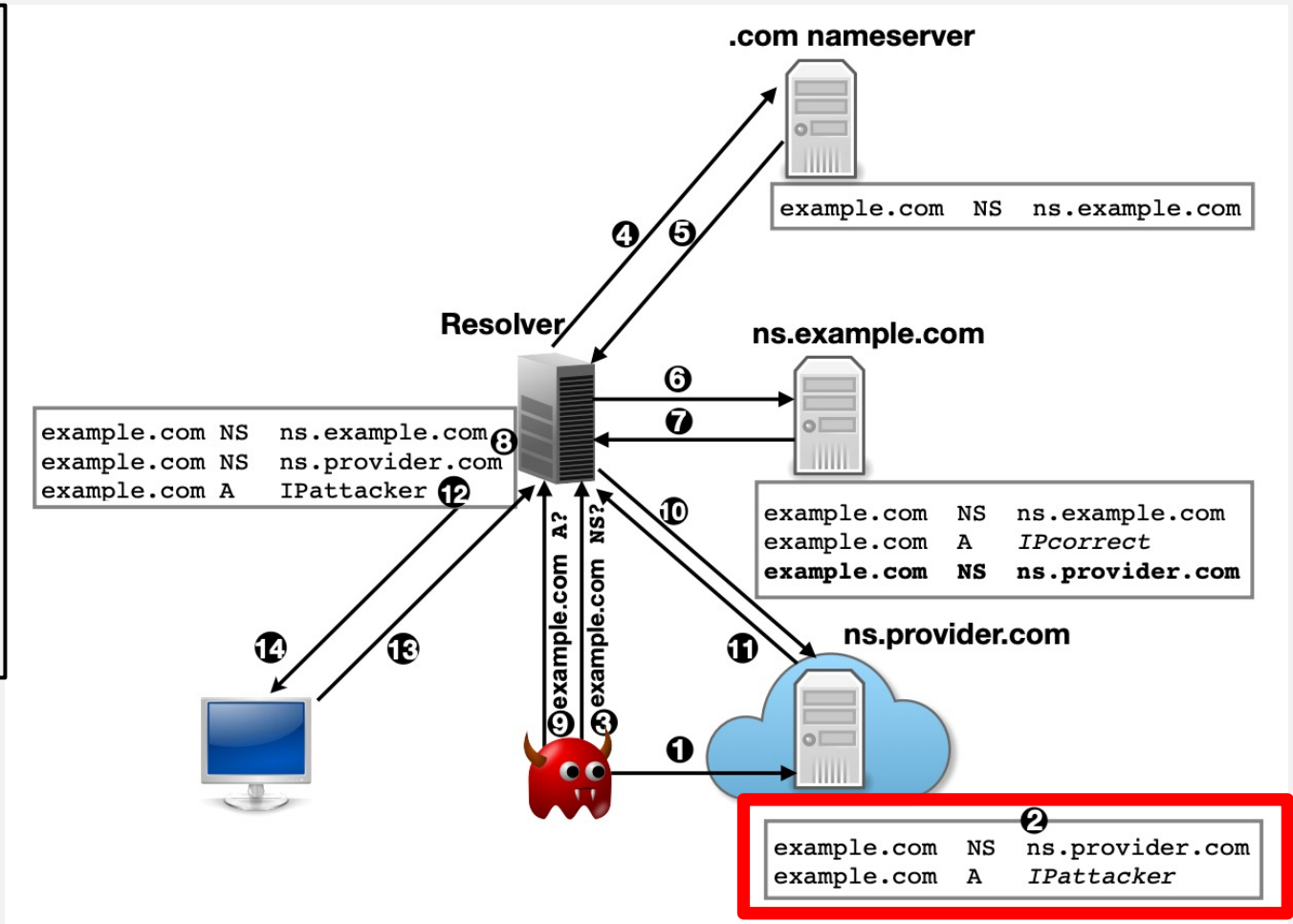
- 父域授权记录

  example.com NS ns.example.com

- 子域授权记录

  example.com NS ns.example.com

  example.com NS ns.provider.com



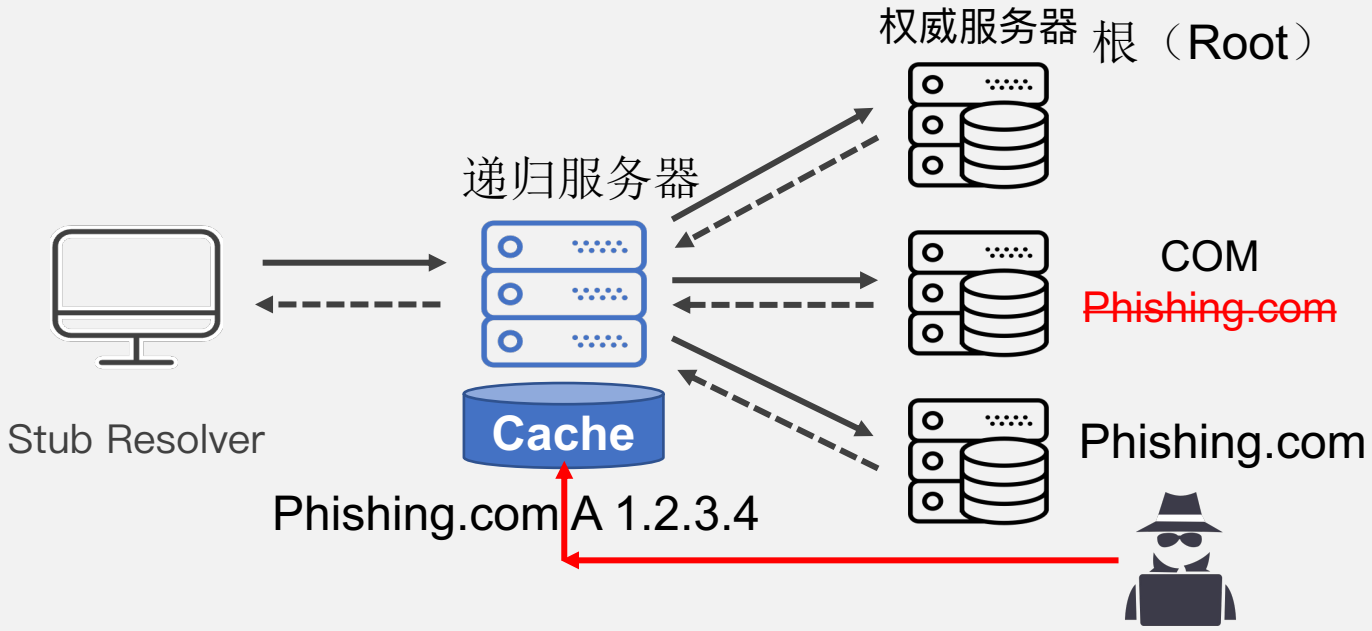
唤醒僵尸：攻击者接管僵尸记录，进而控制目标域名的解析链。

628个知名域名受到上述攻击影响。

* CCS 2020. Zombie Awakening: Stealthy Hijacking of Active Domains through DNS Hosting Referral.

安全风险二：无法从网络空间移除的幽灵域名

- 幽灵域名（Ghost Domain）：被删除的域名却可以持续存活
- 域名协议设计的缺陷：应当优先遵循父域记录，还是子域记录
- 现象：缓存服务器与权威服务器授权记录的数据不一致问题

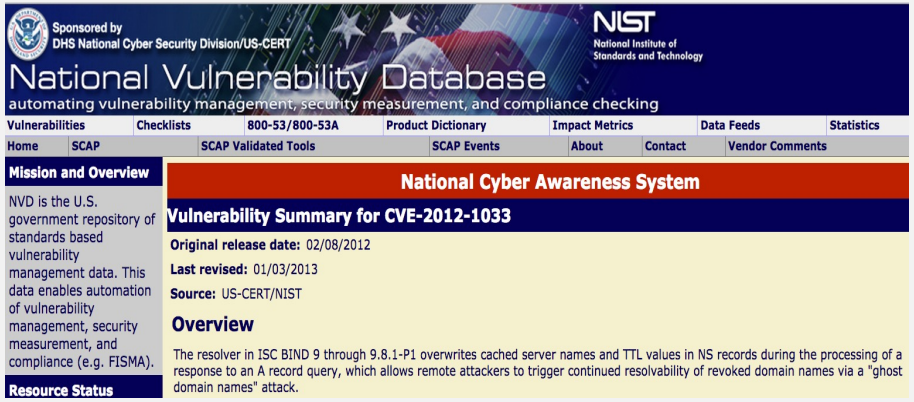


攻击者注册了一个恶意域名phishing.com, 被用户举报后，父域COM删除授权记录。

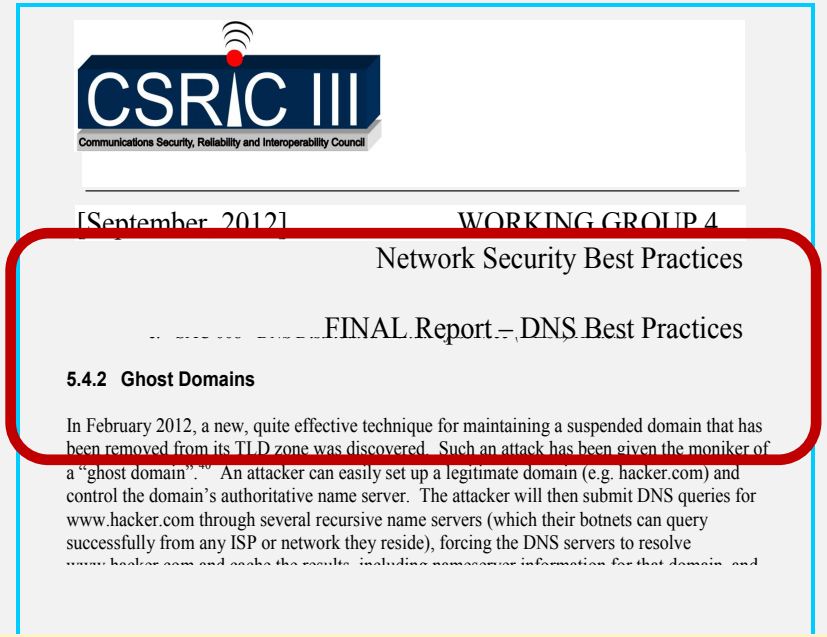
但是，攻击者可以利用协议漏洞操控递归服务器，使phishing.com持续存活。

安全风险二：无法从网络空间移除的幽灵域名

- 论文发表在网络安全顶级学术会议 NDSS 2012
- 美国国家漏洞库收录，10个DNS厂商发布补丁
- 美国联邦通讯局（FCC）安全工作组将Ghost domain写入2012年安全最佳实践（Best Practice）报告



美国国家漏洞库收录（CVE-2012-1033）
10个域名软件厂商发布安全补丁



美国联邦通讯局（FCC）安全工作组
写入安全最佳实践报告

内容提纲 – 三类主要研究话题

话题一： 新型域名缓存污染攻击（10篇）

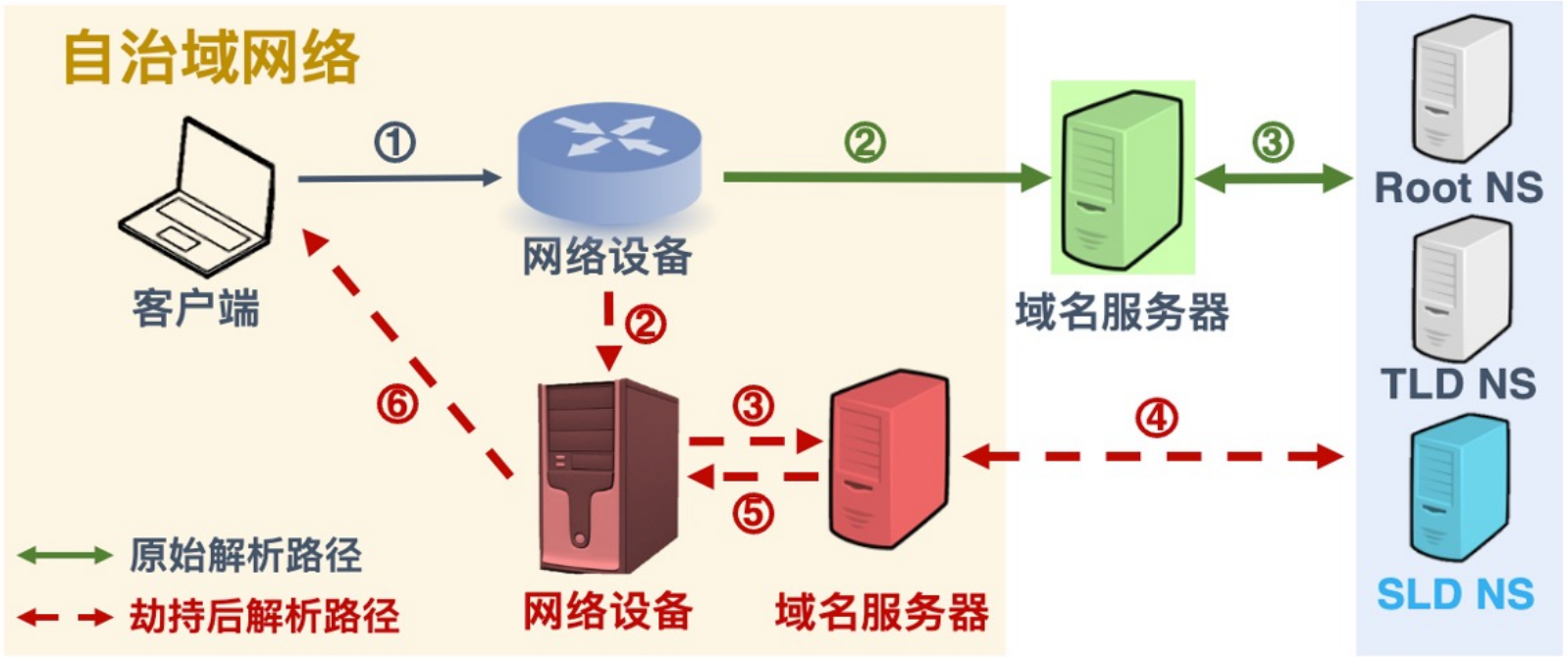
话题二：域名授权机制安全威胁 （3篇）

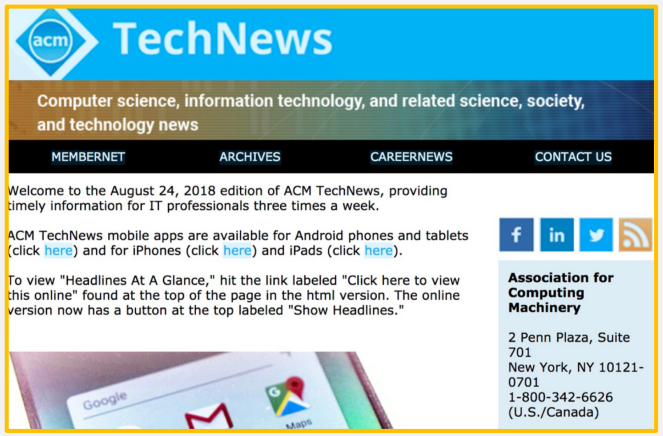
话题三：**域名解析流量规模操控** （3篇）

一、发现大规模域名解析流量操控现象

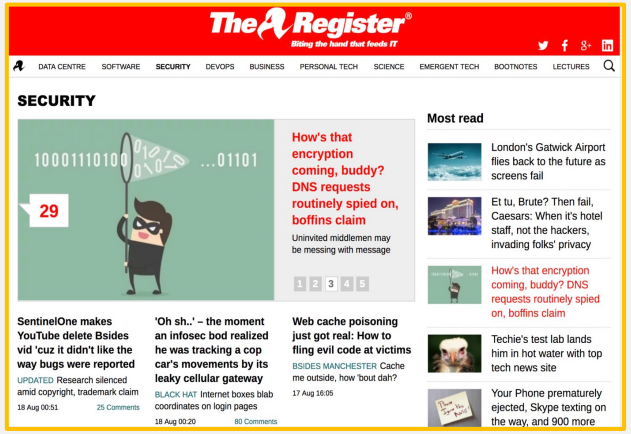
域名协议设计之初缺乏通信实体身份认证机制

劫持者可操控域名通信链路，破坏解析交互过程





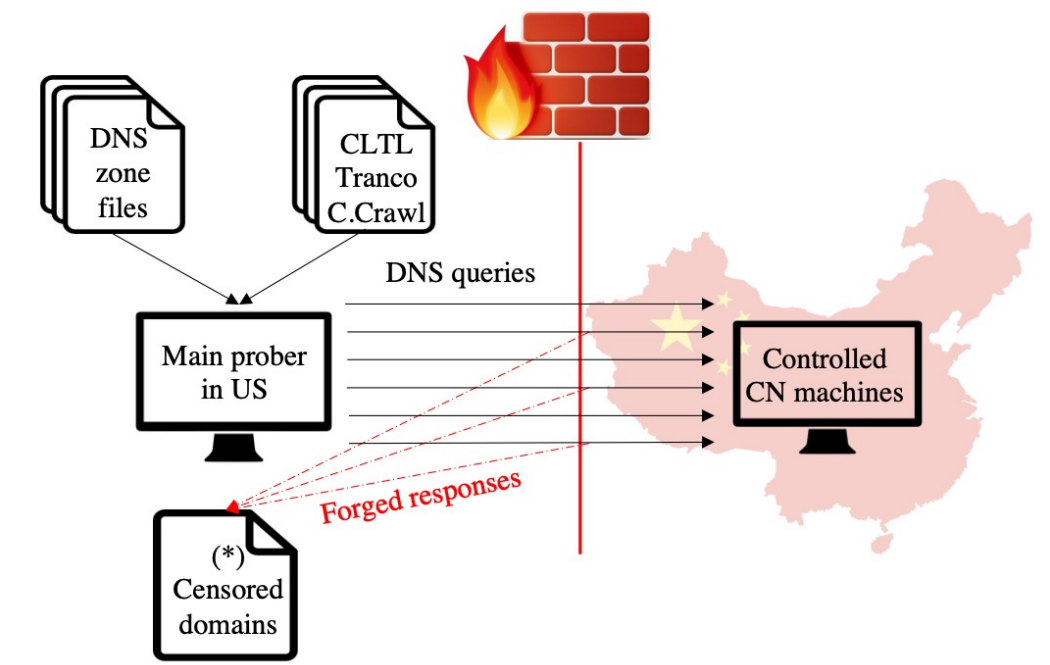
ACM TechNews

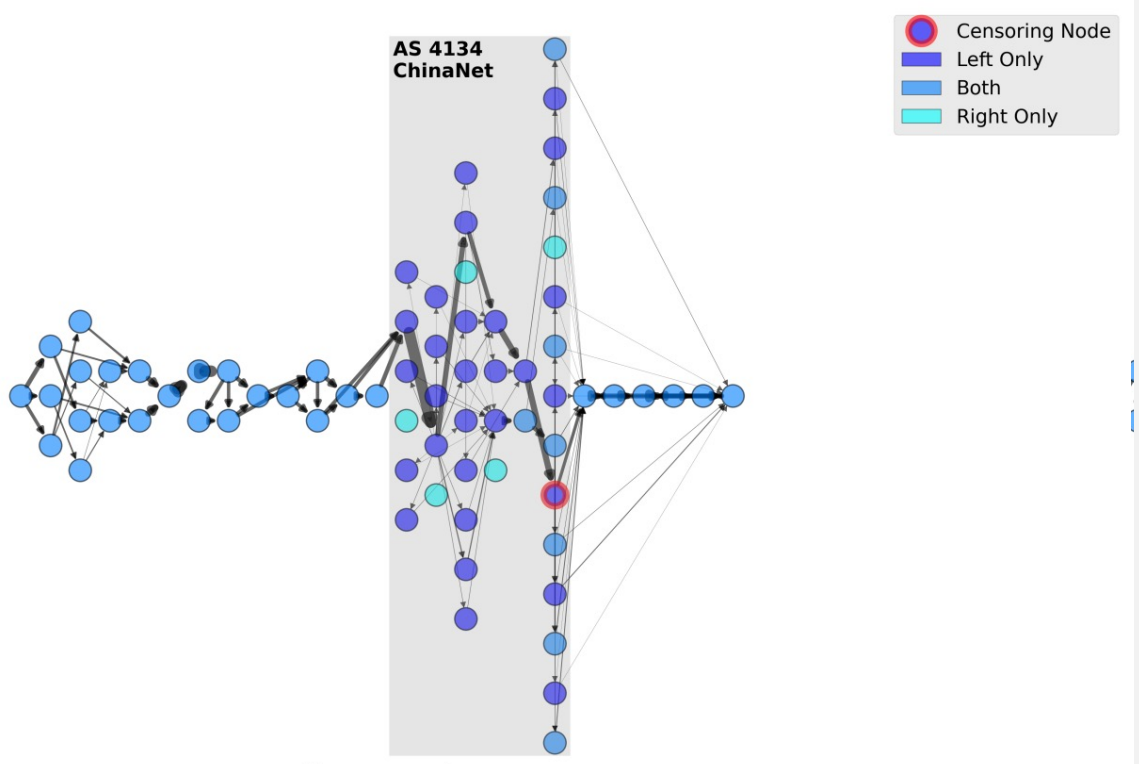


The Register 网站首页

* USENIX Sec 2018. Who Is Answering My Queries: Understanding and Characterizing Interception of the DNS Resolut

二、 深入理解网络审查策略 DNS Censorship





全球范围哪些域名正在遭受审查

审查节点所处的路由拓扑环境

* USENIX Sec 2021. How Great is the Great Firewall? Measuring China's DNS Censorship.
* USENIX Sec 2022. Many Roads Lead To Rome: How Packet Headers Influence DNS Censorship Measurement.

未来互联网域名系统安全研究的趋势展望 （人工版本）

针对域名系统基础设施安全性的分析，呈现出从黑盒走向灰盒化趋势。围绕域名解析交互过程的形式化验证，可能会发挥不容忽视的作用。

互联网流量集中化背景下，云平台域名解析的安全性将愈发受到关注。

无论是对于学术研究还是现实世界的攻击，利用域名基础设施的安全缺陷，进而寻求影响、攻击与之相关联的网络基础设施将会更加普遍。

THANKS

刘保君 助理教授

清华大学网络研究院

lbj@tsinghua.edu.cn

Scan the QR code to add me as a friend.