清華大學
Tsinghua University

博士学位论文答辩
计算机科学与技术系

域名系统关键安全问题研究

指导教师：刘莹、段海新

答辩人：刘保君

2020年9月4日

汇报内容提纲

一、研究背景

二、研究现状

三、研究内容

四、工作总结

五、现有成果

互联网域名系统

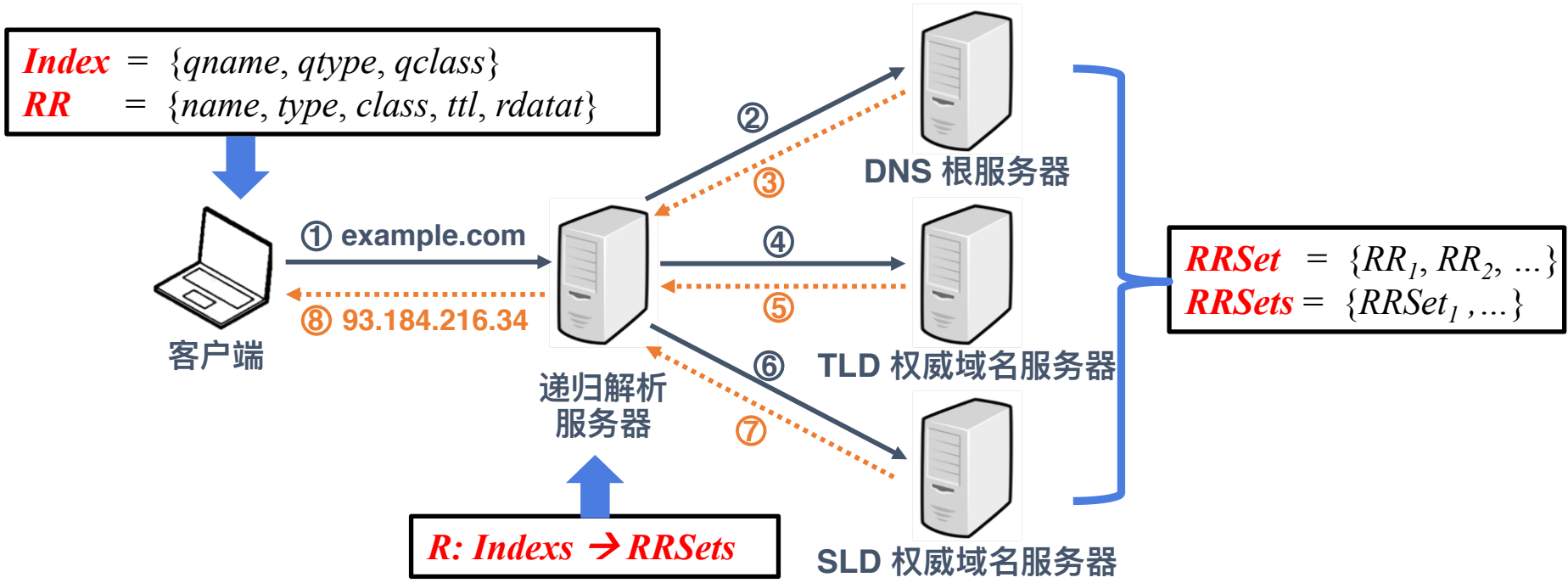
- 域名（Domain Name）
  - 基础需求：对网络空间的设备及服务进行命名（Naming）
  - 通用体系：域名是当前网络空间通用的“命名体系”之一

- 域名系统（Domain Name System, DNS）
  - 翻译转换：域名与主机地址之间的衔接纽带
  - 基础协议：绝大多数互联网上层应用获取网络资源的前提
  - 可扩展性优异：源自于层次授权的设计架构和简洁的协议格式
  - 安全性脆弱：研究人员持续发现大量域名系统安全隐患

- 学术界的研究热点
  - 网络安全领域顶级会议相关论文
    - 2020：7；2019：6；2018：6；2017：8；
  - 网络测量领域顶级会议相关论文
    - 2020：7；2019：7；2018：5；2017：2；

互联网域名系统架构

- 域名系统：全球最大的、统一的、开放的分布式数据库
  - 域名解析：客户端以索引值检索分布式数据库
  - 域名协议：与数据库交互的一种形式化语言描述



域名应用　域名解析　域名空间

域名系统的宏观技术演进脉络

- 持续演进中的域名系统
  - 域名空间范围的延伸
  - 域名协议功能的增强
  - 域名应用场景的扩展

类别	技术	RFC 文档
域名空间	IDNA	RFC 3492, RFC 5890, RFC 5891, RFC 5892, RFC 5893 …
域名协议	DNSSEC	RFC 2931, RFC 3110, RFC 3225, RFC 3226, RFC 4033 …
	Privacy	RFC 7858, RFC 8310, RFC 8484
	EDNS	RFC 6891, RFC 7828, RFC 7830
域名应用	DANE	RFC 6698, RFC 7218, RFC 7671, RFC 7672, RFC 7673
	DKIM	RFC 6376, RFC 6651, RFC 8463
	SPF	RFC 6652, RFC 7001, RFC 7208

自2000年以来，与域名系统相关的RFC技术标准文档简表
（Standard, Proposed Standard）

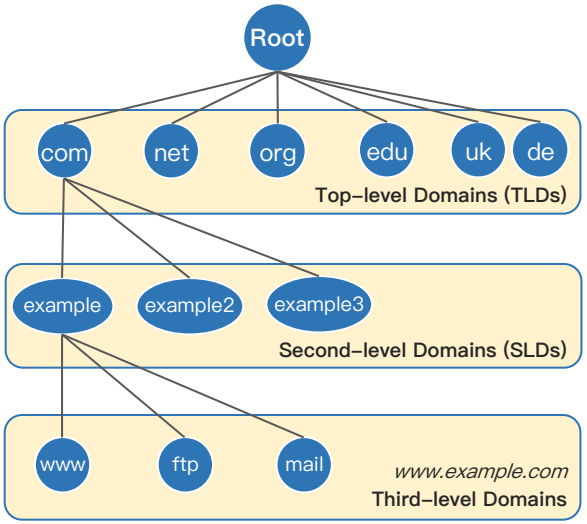
域名空间扩展中的安全威胁

- 域名空间标识符的扩展延伸
  - 新型通用顶级域（New gTLD）：如“*.google*”
  - 国际化域名（IDN）：如“清华.中国”

New gTLD

IDN

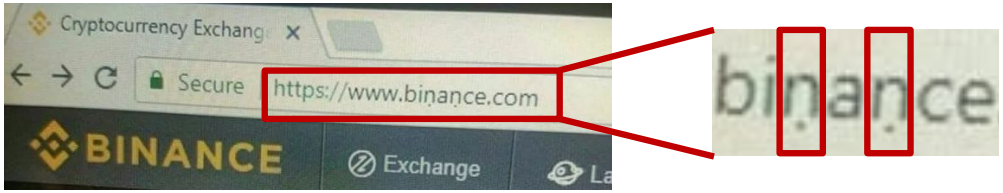
- 域名系统（分布式数据库）中节点定义的安全性
  - 域名标识符冲突（Name Collision）
  - 域名投机抢注（Opportunistic Registration）



<*letter*> ::= any the alphabetic characters **A through Z** and **a through z**

域名空间的国际化扩展

<*letter*> ::= any the characters belong to **Universal Coded Character Set**

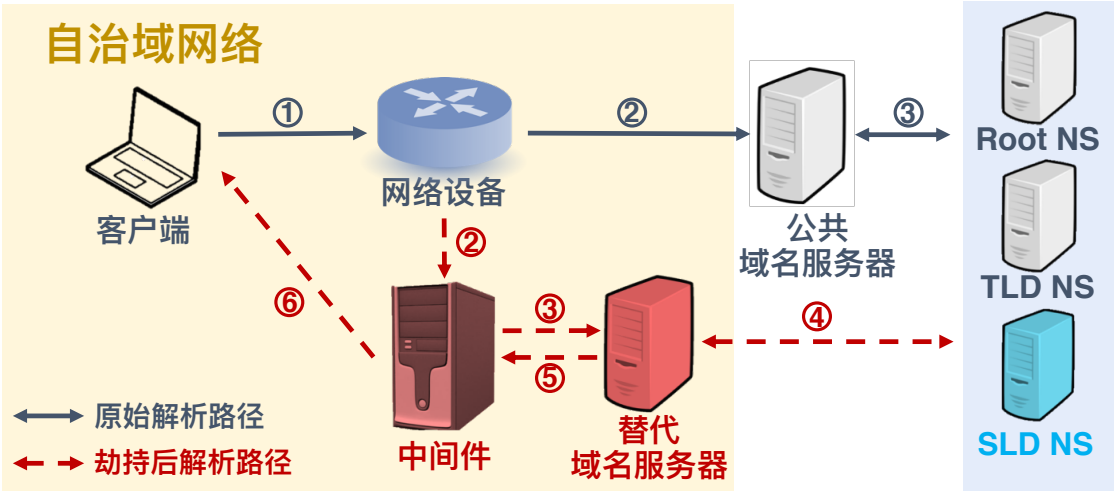


安全事件：2018/03/07，币安交易所遭遇钓鱼攻击

域名协议设计中的安全威胁

- 域名协议的明文传输设计导致解析交互过程易被劫持
  - 根源：缺乏内容完整性认证；缺乏对通信实体身份的认证
  - 协议增强：DNSSEC安全扩展，当前域名系统安全的最佳实践
  - 不足之处：部署进展缓慢；安全模型受限

- 域名系统（分布式数据库）中检索查询的安全性
  - 潜在的安全隐患：域名解析交互过程中的链路劫持问题

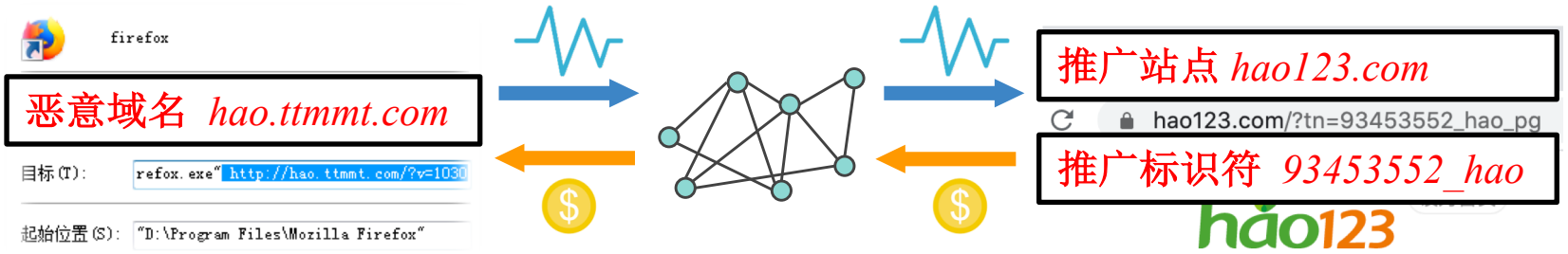


域名解析链路劫持威胁模型

域名应用管理中的安全威胁

- 域名滥用的检测方案
  - 域名滥用常见类型：互联网地下产业、僵尸网络C2、隐蔽隧道…
  - 检测方案常用特征：域名注册、域名词法、域名解析、网站内容
  - 不足之处：特征工程往往聚焦于特定攻击，模式特征难以迁移

- 域名系统（分布式数据库）中节点之间的关联关系
  - 案例：非法流量变现（主要角色：流量主 - 流量联盟 - 网站主）
  - 解决思路：衡量任意两个域名在域名解析层面的关联度，拓展现有域名滥用的检测方案



虚假流量主
恶意软件篡改用户浏览器主页

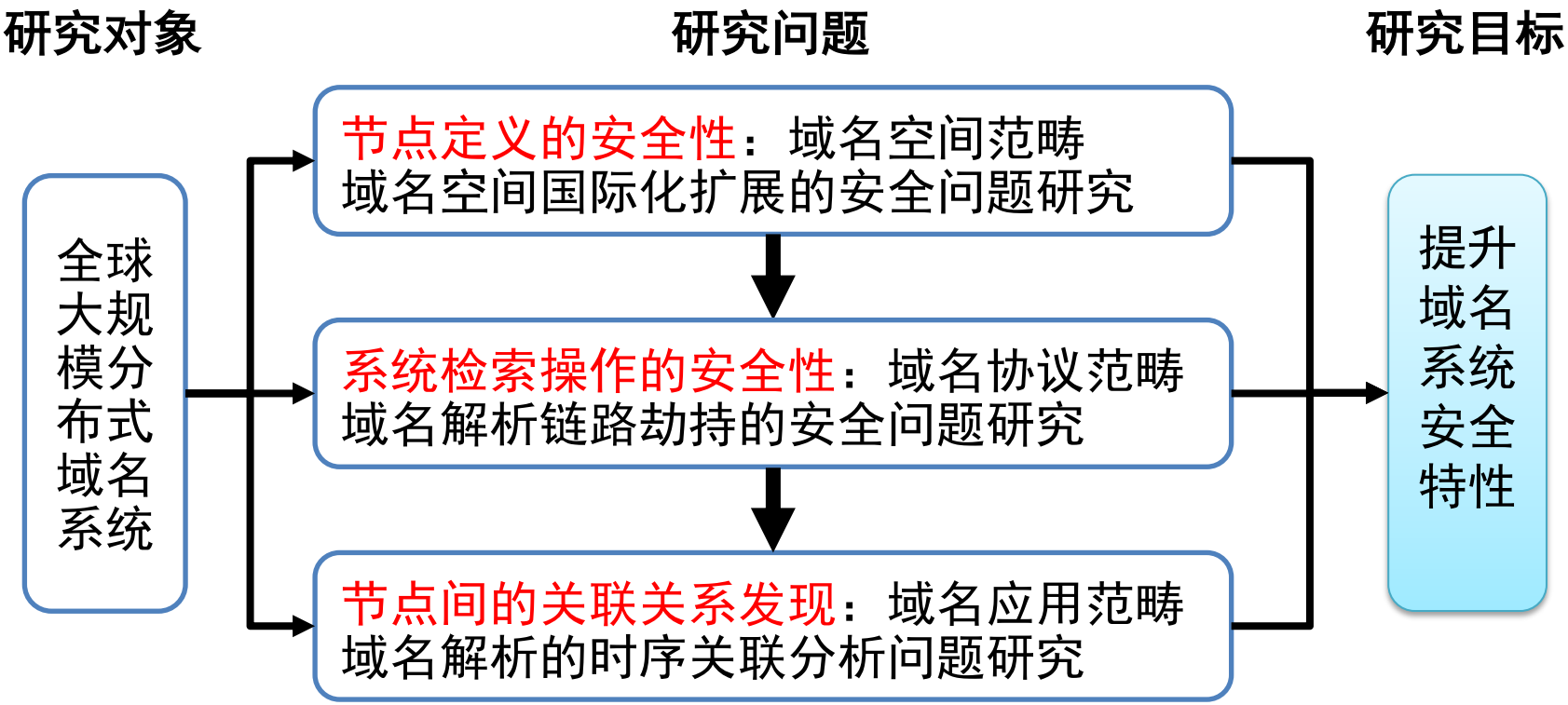
流量联盟
衔接流量主与网站主

网站主
依据流量来源支付佣金

研究问题及研究意义

❖ 研究意义

- 前提背景：域名系统是全球分布式系统的重要组成部分
- 科学问题：全球大规模开放分布式域名系统中，恶意节点及其隐藏关联关系的检测，以及域名解析交互(即系统检索操作) 的攻击发现
- 一般意义：增进大规模分布式网络系统设计原则方面的认知



汇报内容提纲

一、研究背景

二、研究现状

三、研究内容

四、工作总结

五、现有成果

域名空间扩展的相关研究

相关研究工作

- 新型通用顶级域（New gTLD）

类型	相关研究论文	研究问题
协议漏洞	[Chen, S&P 16]	域名冲突
软件测试	[Chen, CCS 17]	域名冲突
测量研究	[Halvorson, PAM 12]	域名注册管理现状
测量研究	[Halvorson, WWW 14]	域名注册意图
测量研究	[Halvorson, IMC 15]	域名注册意图
测量研究	[Kang, HotWeb 16]	CZDS数据分享服务

- 国际化域名（IDN）

类型	相关研究工作	研究问题
流量分析	[Holgers, USENIX ATC 06]	同形异义域名
案例分析	[Symantec Blog]	国际化域名滥用

研究现状小节

- 缺乏系统性对域名空间国际化扩展的安全研究

域名协议设计安全的相关研究

❖ 相关研究工作

- 域名劫持（返回恶意/不正确的应答响应）

攻击者所处位置	相关研究论文
权威服务器侧	[Liu, CCS 16] [Vissers, CCS 17] [Kalafut, IMC 10]
解析服务器侧	[Kuhrer, IMC 15] [Weaver, FOCI 11] [Ager, IMC 10]
网络旁路侧	[Dan Kaminsky, Blackhat 08] [Brandt, CCS 18]
网络中间人	[Chuang, IMC 16]
客户端侧	[Dagon, USENIX ATC 08]

- 用户隐私泄露

类型	论文
操作系统	[Chang, RAIM 15] [Kim, SecureComm 15]
用户网络访问习惯	[Kirchler, CCS 16]

❖ 研究现状小节

- 主要聚焦于域名解析查询与应答过程中“内容”层面的安全性
- 较少关注域名解析交互过程通信链路的安全性

域名滥用检测机制的相关研究

❖ 相关研究工作

▪ 常见检测方案

特征维度	相关研究论文
域名注册	[Hao, IMC 13] [Lever, S&P 16] [Hao, CCS 16]
域名内容词法	[Schuppen, Security 18] [Bigle, NDSS 11]
域名查询解析	[Khalil, AsiaCCS 16] [Antonakais, Security 11]
网站内容及拓扑	[Li, S&P 13] [Bermudez, IMC 12] [Wang, CCS 11]

▪ 域名关联关系

类型	相关研究工作	研究方法
DGA域名聚类	[Gao, Sigcomm 13]	基于NLP，将域名转为向量
沦陷主机发现	[Sato, Leet 10]	不同之间主机，域名查询相似性

❖ 研究现状小节

- 已有研究较少关注于域名查询请求的时间特征
- 已有域名关联方案考虑场景单一，模型不具有可解释性

汇报内容提纲

一、研究背景

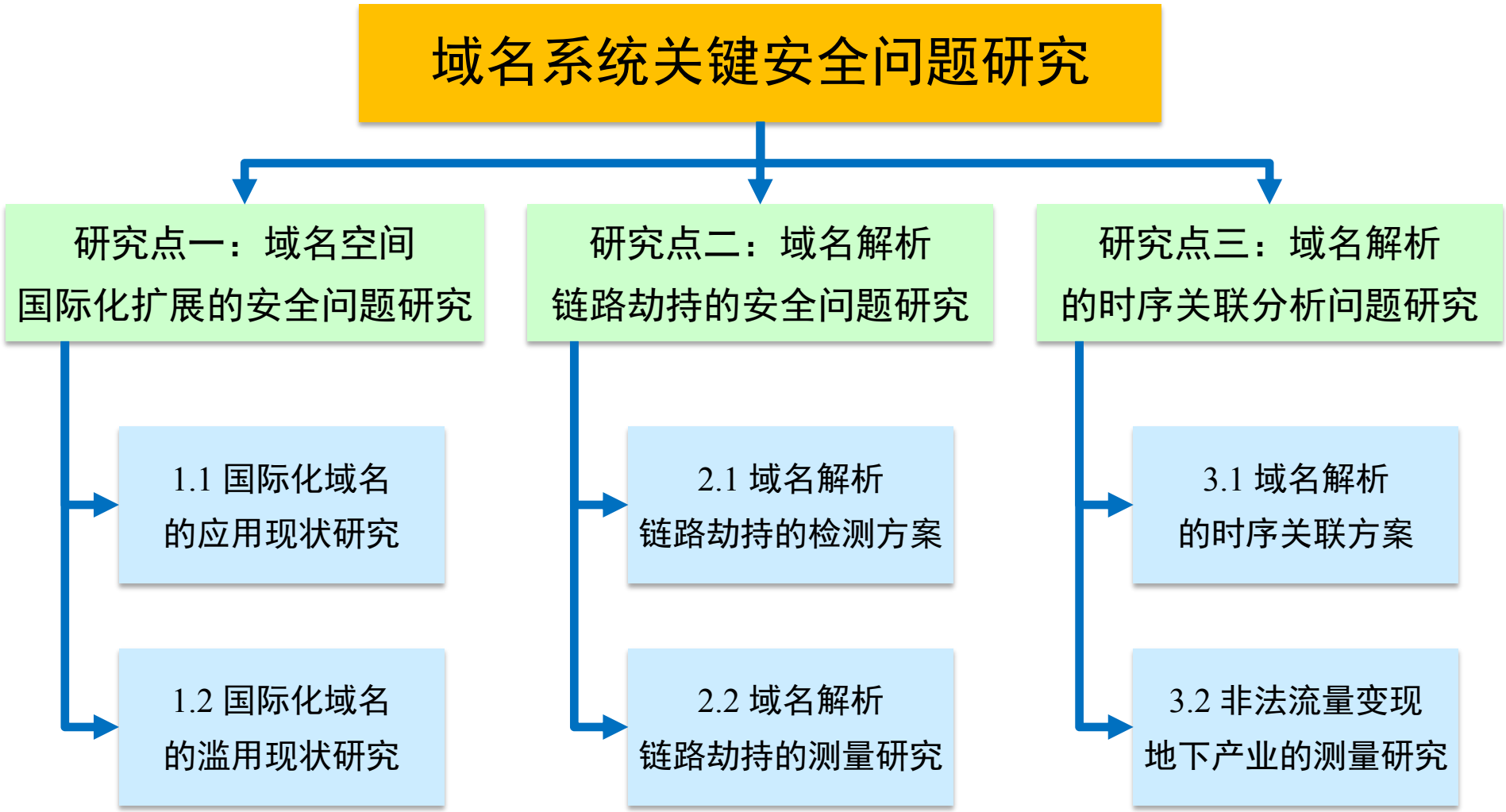
二、研究现状

三、研究内容

四、工作总结

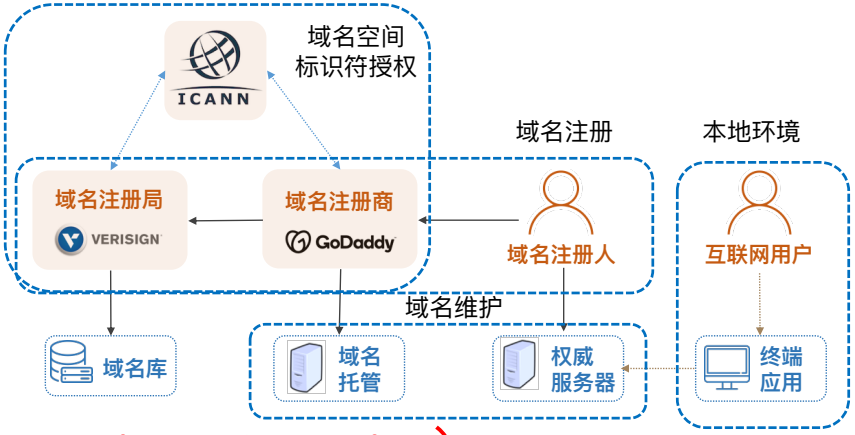
五、现有成果

研究内容总体框架


域名系统关键安全问题研究
研究点一：域名空间国际化扩展的安全问题研究
研究点二：域名解析链路劫持的安全问题研究
研究点三：域名解析的时序关联分析问题研究
1.1 国际化域名的应用现状研究
1.2 国际化域名的滥用现状研究
2.1 域名解析链路劫持的检测方案
2.2 域名解析链路劫持的测量研究
3.1 域名解析的时序关联方案
3.2 非法流量变现地下产业的测量研究

一、域名空间国际化扩展的安全问题研究

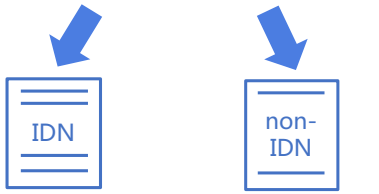
- 域名空间标识符安全体系
  - ICANN、注册局、注册商
  - 域名注册人、互联网用户
  - 其它：终端应用、安全厂商



- 研究方法：数据驱动安全（Data-Driven Security）
  - 主要数据：源自于域名顶级域权威服务器的区域文件
  - 辅助数据：Passive DNS，WHOIS记录，域名黑名单，SSL证书

ICANN

CZDS 数据分享计划

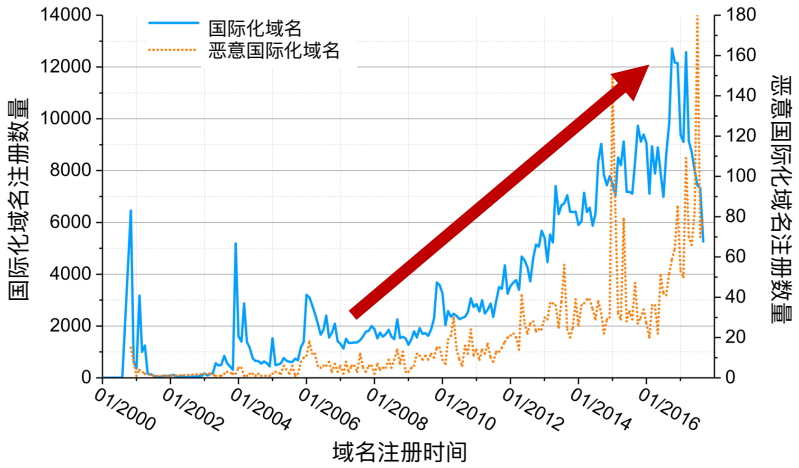


IDN 域名列表　　non-IDN 域名列表

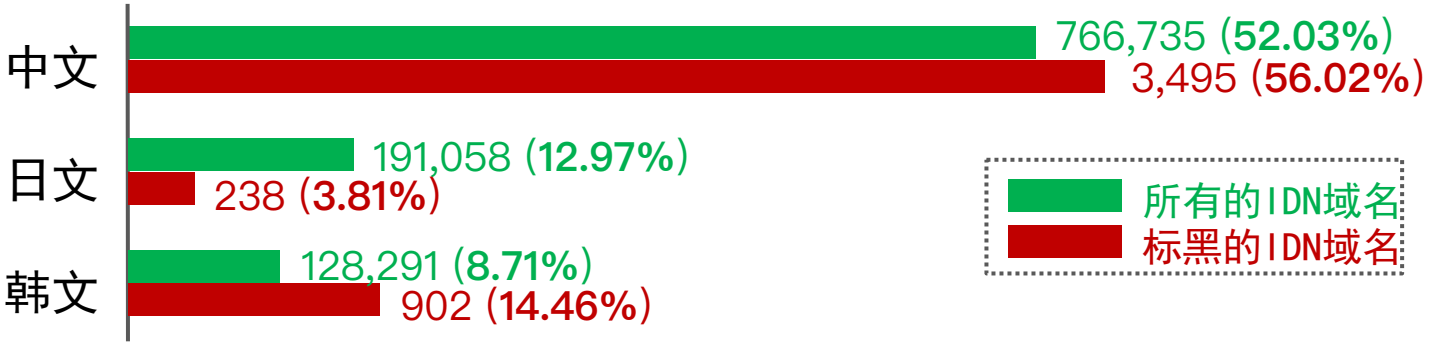
顶级域	快照日期	# IDN (SLD)	WHOIS	黑名单
.com	2017/09/21	1,007,148	590,542	5,284
.net	2017/09/21	231,896	131,573	746
.org	2017/10/05	25,629	19,271	59
iTLDs	2017/10/05	208,163	2,226	152
共计	--	**1,472,836**	**739,160**	**6,241**

国际化域名的应用现状测量研究

- 正面：国际化域名的规模持续增长，有助于互联网的多元化
  - 现象一：注册人倾向于长期持有国际化域名

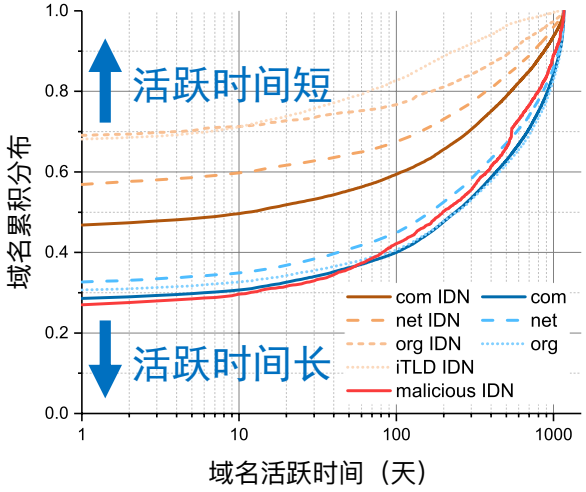


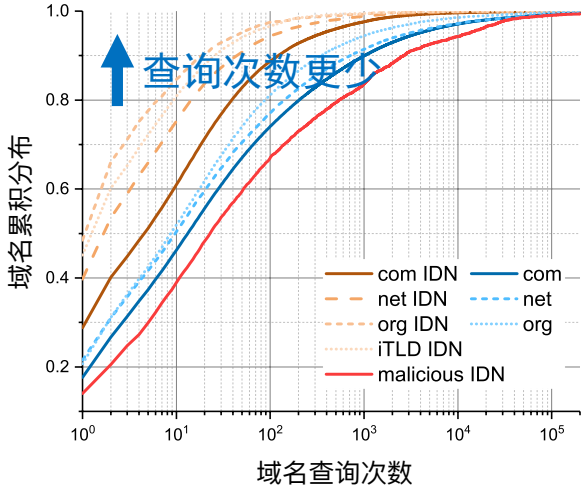
  - 现象二：亚洲国家在推广应用国际化域名中走在前列



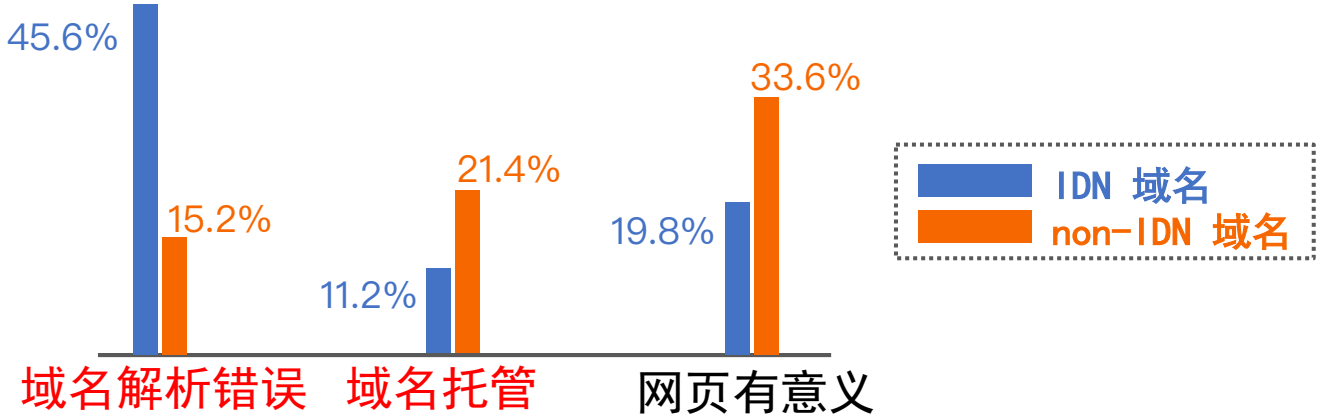
国际化域名的应用现状测量研究

- 负面：国际化域名对互联网的整体价值仍然较为有限
  - 现象三：国际化域名活跃时间更短，用户访问流量更少





  - 现象四：国际化域名的站点大多尚未托管有意义的内容

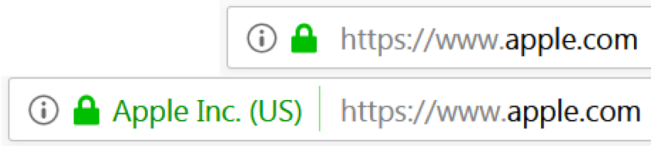


国际化域名的滥用现状测量研究

- 国际化域名滥用类型分析：基于安全厂商域名黑名单
  - 同形异义攻击（Homograph Attacks）
    - 部分检出案例

facebọok.com　faċebook.com　faceḅook.com　faceboôk.com
facebọok.com　fácebook.com　fâcêbook.com　facebooĸ.com
facebóók.com　fạcẹbook.com　fącebook.com　facebȯok.com

攻击目标：FaceBook官网



攻击目标：Apple官网

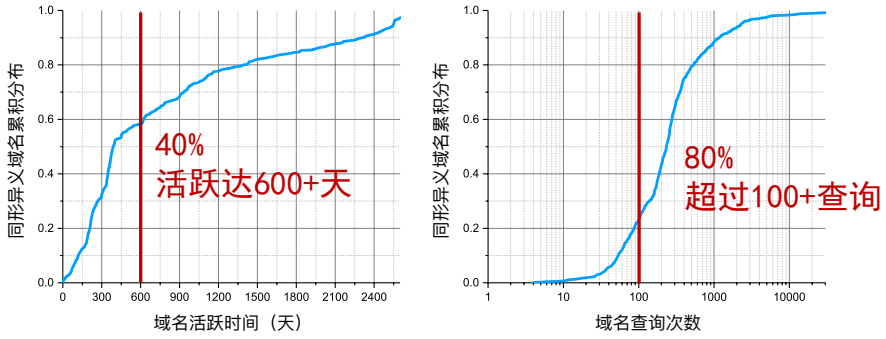
  - 域名语义攻击（Semantic Attacks）
    - 类型一：关键词组合（重点）
    - 类型二：关键词翻译

Punycode 编码	Unicode 编码	Punycode 编码	Unicode 编码
xn–icloud-uz2li34m.com	icloud 登录.com	xn–tfr361c12mbrq.net	格力空调.com
xn–icloud-1u6oy84r.com	icloud 登陆.com	xn–tlqpa605apxhf4c468i.com	北京交通大学.com
xn–apple-rq8mk98i.com	apple 邮箱.com	xn–ztsu95bbqz6hj.com	奔驰汽车.com

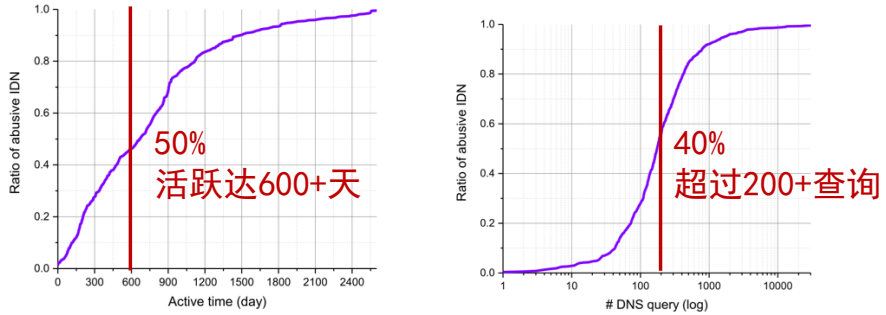
关键词组合型域名语义攻击　　关键词翻译型域名语义攻击

国际化域名的滥用现状测量研究

- 基于域名视觉相似度的国际化域名滥用检测
  - 已被注册的同形异义域名：1516个
    - 仅有少量域名被安全厂商检出 (100个)



  - 已被注册的语义攻击域名：1497个
    - 特点：活跃时间长；有一定规模访问量

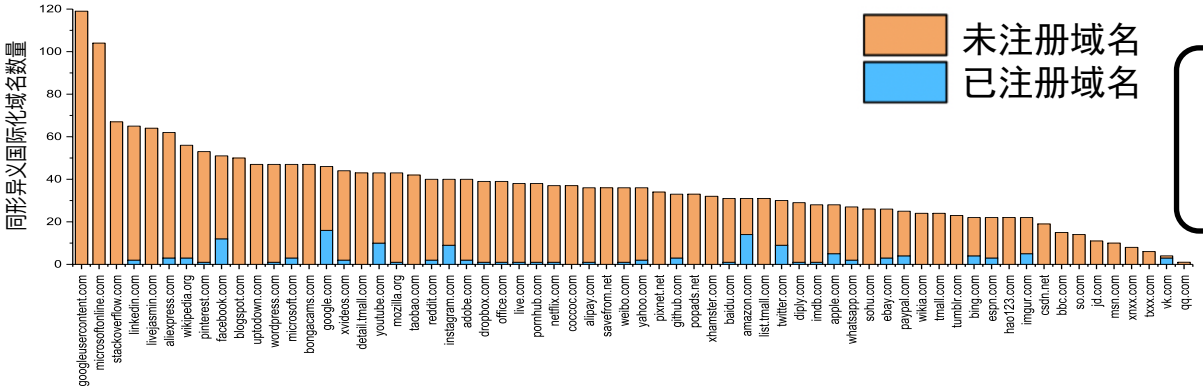


应对措施

安全厂商应考虑新型域名标识符特性，改进并完善现有的域名检测机制。

国际化域名滥用的潜在空间评估

- 同形异义国际化域名仍具有巨大的潜在注册空间
  - 系统至少发现42,671个国际化域名可用于同形异义攻击
  - 域名注册商并未对此类域名锁定，已有237个域名被注册



应对措施
注册局锁定/预留
存有争议的域名

- 热门终端应用渲染国际化域名的安全策略存在诸多缺陷

平台 / 浏览器	PC			iOS			Android		
	Ver.	iTLD IDN 支持情况	同形异义攻击	Ver.	iTLD IDN 支持情况	同形异义攻击	Ver.	iTLD IDN 支持情况	同形异义攻击
Chrome	62.0			61.0			61.0		
Firefox	57.0	需要前缀	可被绕过	10.1			57.0	需要前缀	可被绕过
Opera	49.0		可被绕过	16.0			43.0		
Safari	11.0			11.0			/	/	/
IE	11.0			/	/	/	/	/	/
腾讯	9.7			7.9	Unicode	网页标题	8.0	Unicode	about:blank
百度	8.7		可被绕过	4.10	Unicode	网页标题	6.4	不支持	网页标题
360	9.1			4.0		网页标题	8.2	Punycode	
搜狗	7.1		可被攻击	5.10		网页标题	5.9	Unicode	网页标题
猎豹	6.5		可被绕过	4.18	Unicode	网页标题	5.22		网页标题

应对措施
终端应用显示
提示信息

研究点一 工作总结

- 域名空间国际化扩展的安全问题研究
  - 测量分析：系统性提出域名空间国际化扩展引入的系列安全风险
  - 检测方案：基于域名视觉相似度，设计恶意国际化域名的检测方案
  - 防范措施：提出防范域名国际化扩展安全风险的解决措施
  - 研究论文录用于 **DSN 2018（CCF B类会议长文）**

- 促进国际化域名的后续相关研究
  - 为完善国际化域名的管理规范提供实证依据
  - 相关安全隐患被多个课题组研究跟进
    - [Yuta Sawabe, APAN 18]
    - [Le Pochat, PAM 19]
    - [Le Pochat, SPW 19]
    - [Chiba, RAID 19]

Table 3: Results of Comparing Properties

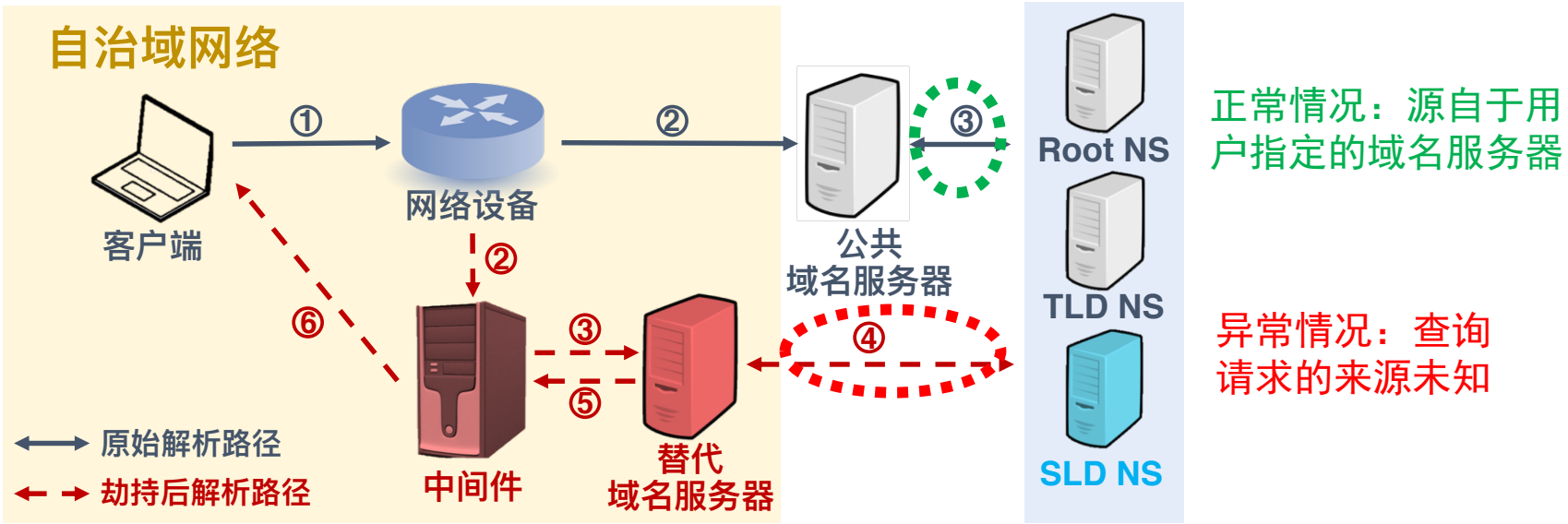
		Our System	Liu et al. [36]	Sawabe et al. [48]
Dataset	# TLDs (IDNs)	570	56	-
	# Domains (IDNs)	4,426,317	1,472,836	1,928,711
Targeted Brand	# Domains (English)	2,310	1,000	1,000
	# Domains (Non-English)	4,774	0	0
Deceptive IDN	Combo	●	◐	○
	Homo	●	●	●
	Homocombo	●	○	○
Method	Visual Similarities	●	●	●
	Brand Features	●	◐	◐
	TLD Features	●	○	○

●: Fully Covered, ◐: Partially Covered, ○: Not Covered

DomainScouter [RAID 19]

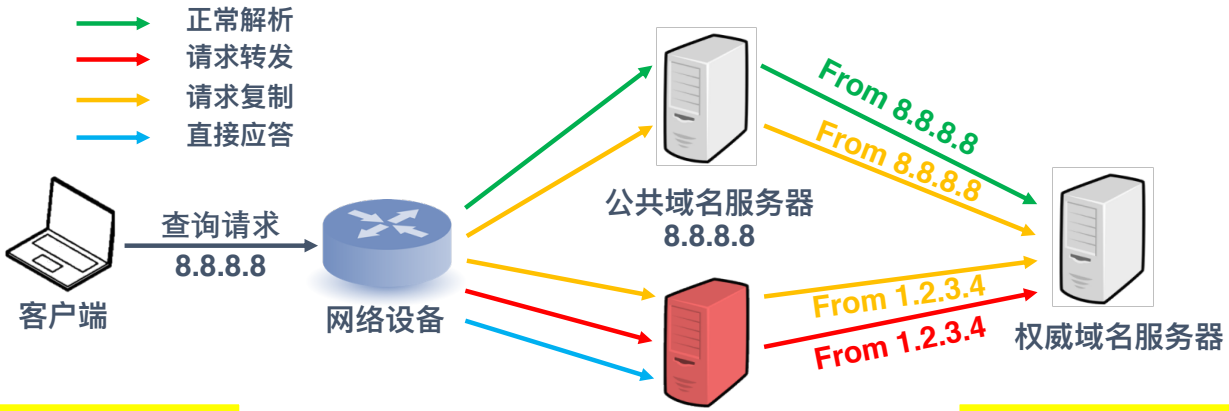
二、域名解析链路劫持的安全问题研究

- 威胁模型分析
  - 根源：域名协议缺乏对通信实体身份的有效认证
  - 现象：劫持者伪造数据包源地址，劫持用户查询请求
  - 关键区别：域名权威服务器一侧，域名查询请求的来源显著不同



域名解析链路劫持的检测方案

- 模型简化：重点关注域名解析的查询请求阶段
  - 链路类型：正常解析，请求转发，请求复制，直接应答



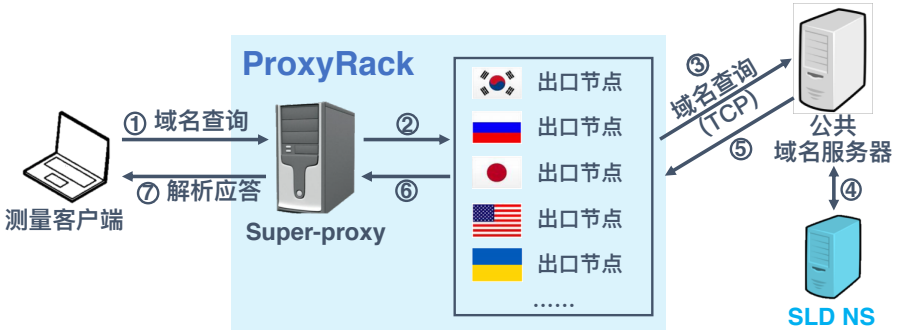
- 基本思路：“连点成线”
  - 挑战：现有测量平台在数据包构造能力和观测点分布存在不足
  - 挑战：公共DNS服务器的出口地址难以判定 【略】

实验数据收集与评估

- 第一阶段：基于ProxyRack商业代理软件设计网络测量平台
  - 复用活跃用户：保证实验观测点的合理分布
  - 构造探测数据包：支持SOCKS 5协议，允许自定义探测报文
  - 不足：仅支持TCP协议传输网络流量

平台	示例	构造DNS	观测点分布
HTTP代理	Luminati	NO	YES
广告网络	BitTorrent	NO	YES
硬件设备	RIPE Atlas	YES	NO
众包测量	Netalyzr	YES	NO

现有网络测量平台对比分析



基于ProxyRack的网络测量平台

- 第二阶段：与安全厂商合作，将测试内嵌网络调试模块
- 数据评估：共计获取全球148,478个IP地址的域名解析数据

实验阶段	查询请求	IP 地址	国家	自治域
第一阶段	1,652,953	36,173	173	2,691
第二阶段	4,584,413	112,305	87	356

域名解析链路劫持的实际影响

- 劫持规模：链路劫持现象普遍存在

198个自治域存在劫持（TCP）

61个自治域存在劫持

- 劫持特征：知名公共DNS更易被劫持

Google Public DNS 27.9%

OpenDNS 12.6%

ORACLE + Dyn 16.1%

EDU DNS（自建） 9.8%

APNIC Blog: One in four Google Public DNS requests are being intercepted.

域名解析链路劫持的实际影响

❖ 劫持策略：自治域之间差异显著

自治域	组织机构	请求转发	请求复制	替代解析服务器
AS4134	中国电信	**5.19%**	0.26%	116.9.94* (AS4134)
AS4837	中国联通	**4.59%**	0.51%	202.99.96.* (AS4837)
AS9808	**中国移动**	**32.49%**	8.85%	112.25.12.* (AS9808)
AS56040	**中国移动**	**45.09%**	0.04%	120.196.165.* (AS56040)

❖ 安全威胁分析

- 增加安全隐患：篡改域名解析应答响应内容
- 影响解析性能：劫持设备导致域名解析性能下降
- 隐私风险：用户难以察觉域名解析被劫持，难以排查网络故障

云南移动劫持域名解析案例

BIND
Berkeley Internet Domain Name

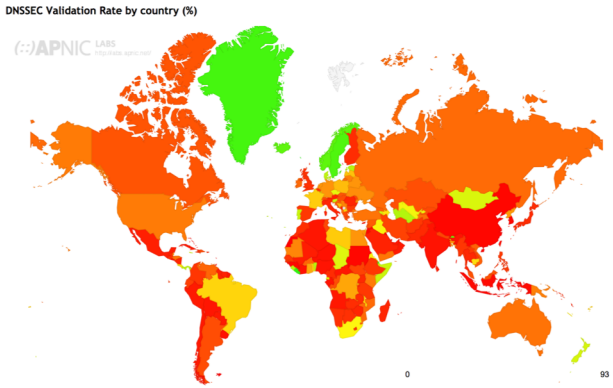
DNS软件版本过期十年

DNSSEC

不支持DNS安全扩展

域名解析链路劫持的解决方案

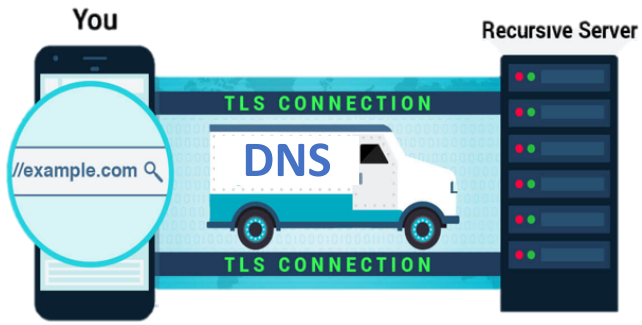
- DNSSEC的安全模型：关注数据完整性问题



US Validation Rate: 29.7%

CN Validation Rate: 1.2%

- 域名加密协议解决认证问题
  - RFC 8301: Resolver Authentication
  - RFC 7858: DNS over TLS
  - RFC 8094: DNS over DTLS
  - RFC 8484: DNS over HTTPS
  - ……

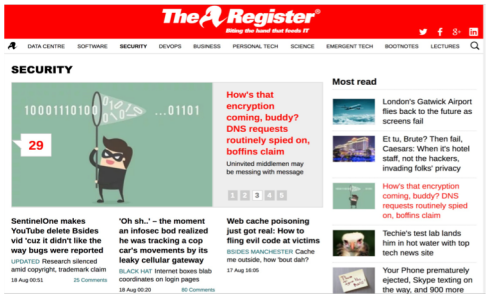


- 在线检测工具
  - 面向互联网用户：http://whatismydnsresolver.com

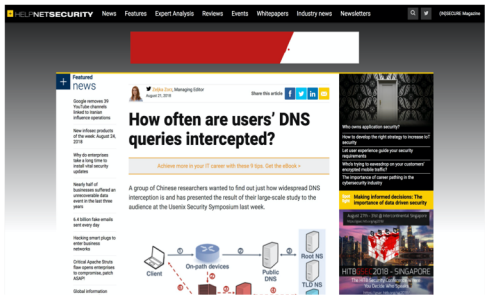
研究点二 工作总结

- 域名解析链路劫持的安全问题研究
  - 检测方案：提出大规模检测域名解析链路劫持的检测方案
  - 测量分析：首次证实全球互联网中普遍存在的劫持现象
  - 缓解措施：面向互联网用户，发布在线检测工具
  - 研究论文录用于 **USENIX Security 2018（CCF A类会议长文）**

- 研究论文在学术界与工业界的影响
  - 论文入选 DNS-OARC 30 和 ANRW 2019
  - 多家知名科技媒体报导：ACM TechNews, The Register …



The Register



HelpNet Security

HackRead

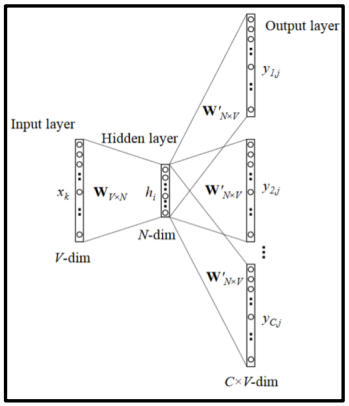
研究点二 工作总结

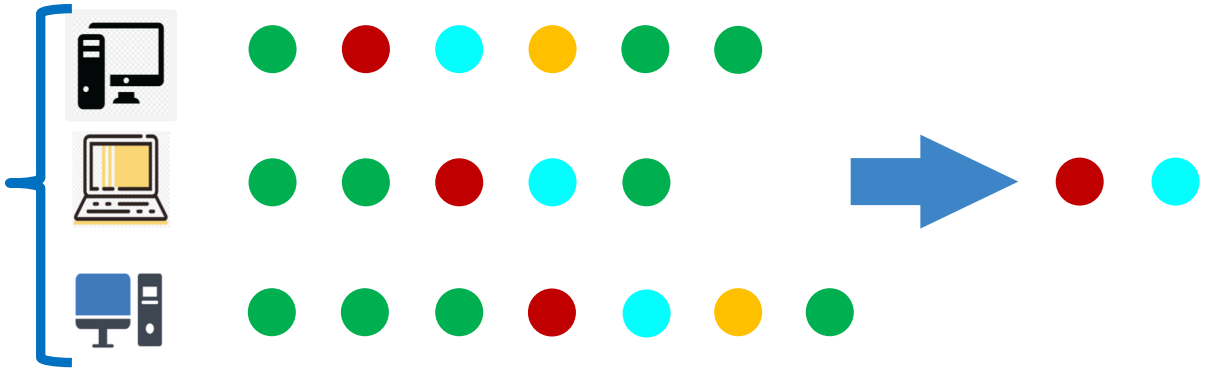
- 促进域名加密协议的研究与部署
  - Nick Sullivan：Cloudflare 研究院主任

- 后续研究工作
  - **[IMC 2019]**. An End-to-End, Large-Scale Measurement Study of DNS-over-Encryption: How Far Have We Come ?
  - 论文同时提名 **IMC 2019 最佳论文奖与社区贡献奖**
  - 论文获得 **IRTF 应用网络研究奖** (**A**pplied **N**etwork **R**esearch **P**rize)
  - 论文入选 DNS-OARC 31

三、域名解析的时序关联分析问题研究

- 域名解析的时序关联问题研究
  - 整体目标：可解释性强，适用于安全检测场景
  - 基本思想：使用概率统计模型，以支持度和置信度衡量关联规则
  - 性能瓶颈：针对频繁子集挖掘算法FP-Growth进行优化改进
  - 设计要素：引入滑动时间窗口，引入时间衰减因素，子域名归并





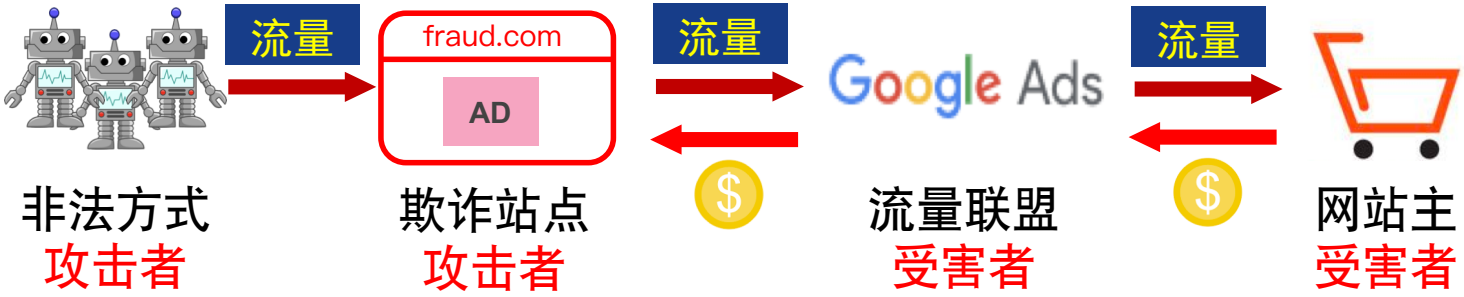
已有研究：基于NLP技术
计算域名间关联关系
缺点：可解释性不足

$$Support(d_i, d_j) = P(Query(d_i)\ Query(d_j))$$

$$Confidence(d_i, d_j) = P(Query(d_j) \mid Query(d_i))$$

非法流量变现地下产业

- 利益链分析



- 流量联盟类型
  - 电商流量联盟
  - 广告流量联盟
  - 导航流量联盟

amazon associates　ebay partner network
Google Ads　Microsoft | Advertising
hao123　360导航

- 已有研究工作的局限性
  - 基本以主动探测为主，针对特定欺诈类型，需要流量联盟深度配合
  - Honney ads [Dave, Sigcomm CCR 2012]
  - Inspection JS [Reis, NSDI 2008] [Thomas, S&P 2015]
  - Network probe [Dagon, USENIX 2008] [Kuhrer, IMC 2015]

基于域名关联分析的检测系统

- 关键模式特征：网站流量自动重定向

```
<HTML>

<style> a{ color:#FFFFFF;}</style>
<BODY>
<Meta name="Robots" Content="All">
<script src="http://s11.cnzz.com/z_stat.php?id=1259526277&web_i
<script language="JavaScript">
if(location.hostname=="bd.1141a6.com")
          location="https://www.baidu.com/?tn=90578459_hao_pg";
</script>

</BODY>
</HTML>
```

推广站点域名　流量主标识符

自动重定向，导致了域名解析之间的强关联

- TraffickStop系统设计：以被动分析为主
  - 设计方案：设计域名解析的时序关联分析方案

数据收集

DNS 数据

URL 数据

域名 WHOIS

域名关联

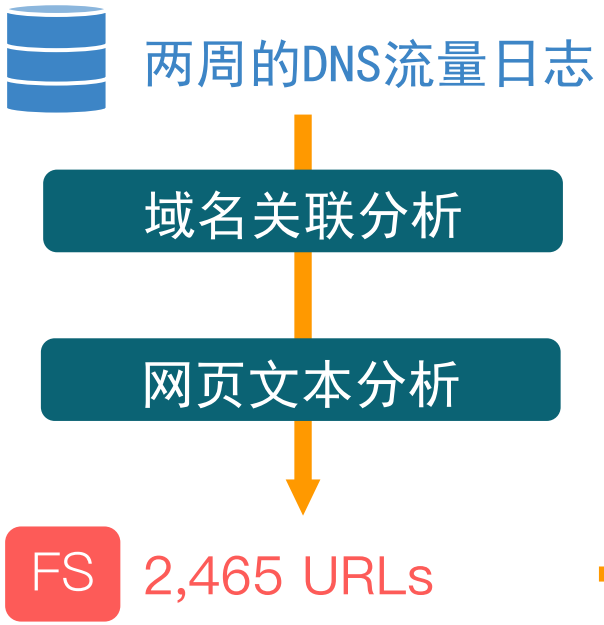
挖掘域名解析强关联关系

内容分析

分析可疑网页的实际用途

系统实现、评估

- 系统优势
  - 易于部署：依赖域名解析流量，以被动分析为主
  - 系统性能：分析两周共2310亿条DNS日志，耗时49小时



严苛的人工确认条件

A. 网站内容无意义或非法

B. 强制性流量重定向行为

C. URL必须包含推广标识符

72.7% accuracy (1,792/2,465)

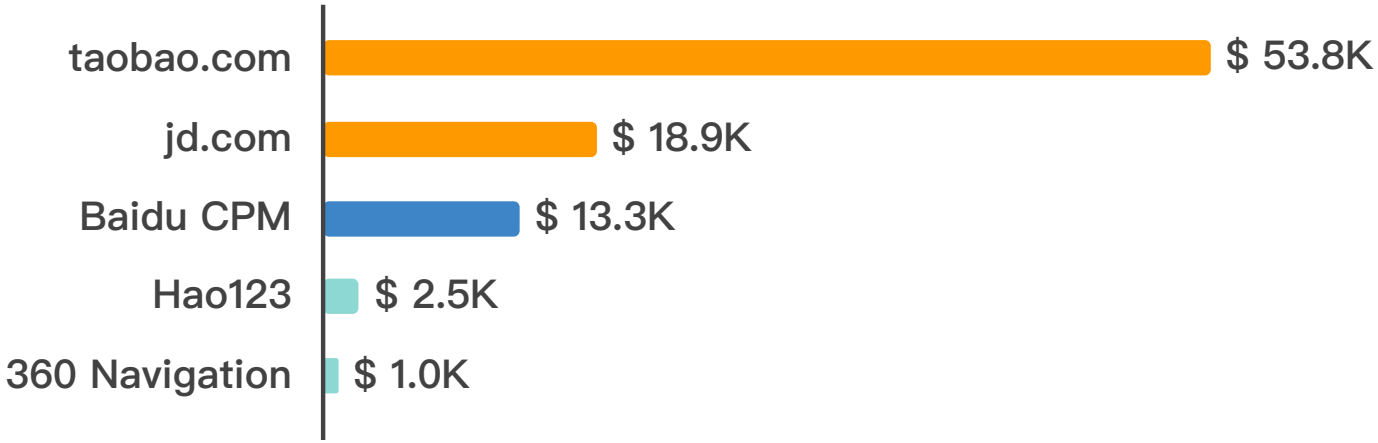
89.4%	电商流量联盟
67.5%	导航流量联盟
74.8%	广告流量联盟

非法流量变现的现实影响

- 网络流量的规模
  - 欺诈域名：1457个（以二级域名计）
  - 评估方法：根据一年的Passive DNS数据进行估算

53 Billion	100K+ Queries	300+ Days
欺诈域名DNS查询请求整体规模	96%+欺诈域名接收的DNS查询规模	85%+欺诈域名的活跃时间跨度

- 流量联盟的损失
  - 保守评估：网站主每天以流量欺诈，至少损失数千美元



研究点三 工作总结

- 域名解析的时序关联问题研究
  - 设计方案：设计域名解析的时序关联分析方案
  - 检测系统：基于域名关联分析，检测非法流量变现型地下产业
  - 测量评估：系统性测量评估非法流量变现产业的影响
  - 研究论文录用于 **EuroS&P 2019**

- 应用于安全事件分析
  - JS代码劫持
  - 浏览器数字货币挖矿脚本

汇报内容提纲

一、研究背景

二、研究现状

三、研究内容

四、工作总结

五、现有成果

论文工作总结

- 针对域名空间扩展中的安全威胁
  - 提出系列风险：阐述域名空间国际化扩展所引入的系列安全风险
  - 设计检测方案：设计恶意国际化域名的检测方案，促进后续研究
- 针对域名协议设计中的安全威胁
  - 设计测量方案：在全球互联网维度，大规模检测域名解析链路劫持
  - 评估实际影响：证实链路劫持普遍存在，促进域名加密协议部署
- 针对域名应用管理中的安全威胁
  - 提出域名关联方案：基于域名查询时序特征，衡量域名关联程度
  - 检测非法流量变现：检测流量变现型地下产业，评估实际影响力

一般意义而言，有助于解决全球大规模分布式系统中恶意节点的检测及关联问题，也有助于提升系统查询检索的安全性

汇报内容提纲

一、研究背景

二、研究现状

三、研究内容

四、工作总结

五、现有成果

论文发表（17篇）

1. [USENIX Security 18] Baojun Liu, Chaoyi Lu, Haixin Duan, Ying Liu, Zhou Li, Shuang Hao, Min Yang. Who Is Answering My Queries: Understanding and Characterizing Interception of the DNS Resolution Path. **CCF A类会议长文.**
2. [DSN 18] Baojun Liu, Chaoyi Lu, Zhou Li, Ying Liu, Haixin Duan, Shuang Hao, Zaifeng Zhang. A Reexamination of Internationalized Domain Names: the Good, the Bad and the Ugly. **CCF B类会议长文.**
3. [EuroS&P 19] Baojun Liu, Zhou Li, Peiyuan Zong, Chaoyi Lu, Haixin Duan, Ying Liu, Sumayah Alrwais, XaioFeng Wang, Shuang Hao, Yaoqi Jia, Yiming Zhang, Kai Chen, Zaifeng Zhang. TraffickStop: Detecting and Measuring Illicit Traffic Monetization Through Large-scale DNS Analysis.
4. [IMC 19] Chaoyi Lu, Baojun Liu, Zhou Li, Shuang Hao, Haixin Duan, Mingming Zhang, Chunying Leng, Ying Liu, Zaifeng Zhang, Jianping Wu. An End-to-End, Large-Scale Measurement of DNS-over-Encryption: How Far Have We Come? **CCF B类会议长文. IRTF Applied Network Research Award (ANRP) ! Nominee for Best Paper Award and Community Contribution Award !**
5. [CCS 20] Yiming Zhang, Baojun Liu *, Chaoyi Lu, Zhou Li, Haixin Duan, Shuang Hao, Mingxuan Liu, Ying Liu, Dong Wang, Qiang Li. Lies in the Air: Characterizing Fake-base-station Spam Ecosystem in China. **CCF A类会议长文. Corresponding Author.**

论文发表（17篇）

6. [CCS 17] Daiping Liu, Zhou Li, Kun Du, Haining Wang, Baojun Liu, Haixin Duan. Don't Let One Rotten Apple Spoil the Whole Barrel: Towards Automated Detection of Shadowed Domains. CCF A类会议长文.
7. [Oakland 19] Xianghang Mi, Xuan Feng, Xiaojing Liao, Baojun Liu, Xiaofeng Wang, Feng Qian, Zhou Li, Sumayah Alrwais, Limin Sun, Ying Liu. Resident Evil: Understanding Residential IP Proxy as a Dark Service. CCF A类会议长文.
8. [NDSS 19] Eihal Alowaisheq, Peng Wang, Sumayah Alrwais, Xiaojing Liao, XaioFeng Wang, Tasneem Alowaisheq, XiangHang Mi, Siyuan Tang, Baojun Liu. Cracking Wall of Confinement: Understanding and Analyzing Malicious Domain Takedowns. CCF B类会议长文. Distinguished Paper Award !
9. [NDSS 20] Ruo Guo, Weizhong Li, Baojun Liu, Shuang Hao, Haixin Duan, Jia Zhang, Kaiwen Shen, Jianjun Chen, Ying Liu. CDN Judo: Breaking the CDN DoS Protection with Itself. CCF B类会议长文.
10. [USENIX Security 20] Xiaofeng Zheng, Chaoyi Lu, Jian Peng, Qiushi Yang, Dongjie Zhou, Baojun Liu, Keyu Man, Shuang Hao, Haixin Duan, Zhiyun Qian. Poison over Troubled Forwarders: A Cache Poisoning Attack Targeting DNS Forwarding Devices. CCF A类会议长文.
11. [CCS 20] Mingming Zhang, Xiaofeng Zheng, Kaiwen Shen, Ziqiao Kong, Chaoyi Lu, Yu Wang, Haixin Duan, Shuang Hao, Baojun Liu, Min Yang. Talking with Familiar Strangers: An Empirical Study on HTTPS Context Confusion Attacks. CCF A类会议长文.

论文发表（17篇）

12. [USENIX Security 21] Kaiwen Shen, Chuhan Wang, Xiaofeng Zheng, Minglei Guo, Chaoyi Lu, Baojun Liu, Yuxuan Zhao, Shuang Hao, Haixin Duan, Qinfeng Pan, Min Yang. Weak Links in Authentication Chains: A Large-scale Analysis of Email Sender Spoofing Attacks. CCF A类会议长文.
13. [Journal of Tsinghua University 17] Shenglin Zhang, Ying Liu, Dan Pei, Baojun Liu *. Measuring the BGP AS Path Looping and Private AS Number Leaking. Corresponding Author.
14. [FOCI 18] Mingming Zhang, Baojun Liu, Chaoyi Lu, Jia Zhang, Shuang Hao, Haixin Duan. Measuring Privacy Threats in China-Wide Mobile Networks. CCF A类会议Workshop.
15. [SRDS 18] Run Guo, Jianjun Chen, Baojun Liu, Jia Zhang, Chao Zhang, Haixin Duan, Tao Wan, Jian Jiang, Shuang Hao, Yaoqi Jia. Abusing CDNs for Fun and Profit: Security Issues in CDNs' Origin Validation. CCF B类会议长文.
16. [SecureComm 19] Kun Du, Hao Yang, Zhou Li, Haixin Duan, Shuang Hao, Baojun Liu, Yuxiao Ye, Mingxuan Liu, Xiaodong Su, Guang Liu, Zhifeng Geng, Zaifeng Zhang, Jinjin Liang. TL;DR Hazard: A Comprehensive Study of Levelsquatting Scams. CCF C类会议长文.
17. [DSN 20] Weizhong Li, Kaiwen Shen, Run Guo, Baojun Liu, Jia Zhang, Haixin Duan, Shuang Hao, Xiarun Chen, Yao Wang. CDN Backfired: Amplification Attacks Based on HTTP Range Requests. CCF B类会议长文. Best Paper Award !

在投论文、参与项目

- **在投论文**
  - NDSS 2021 (CCF B类会议长文)，一作
- **参与项目**
  - 赛尔网络下一代互联网技术创新项目. IPv6环境下威胁情报感知平台. **项目负责人.**
  - 国家“十三五”重点研发项目. IPv6地址驱动的互联网安全管控体系结构和关键 机制研究.
  - 国家“十三五”重点研发项目. 地址驱动的网络安全管控体系结构及其机理研究.
  - 国家自然科学基金. 基于RPKI的域间源地址验证关键技术及部署优化研究.
  - 国家计算机网络与信息安全管理中心项目. 教育网基于IPv6真实源地址的跨境用户可信通道关键技术研究.
  - 中国信息安全测评中心项目. 安全通讯网络系统的设计与实现.

荣誉奖励

- 2020年，清华大学计算机系优秀博士毕业生
- 2020年，IRTF应用网络研究奖 （ANRP）
- 2020年，DSN会议最佳论文奖
- 2019年，NDSS会议最佳论文奖
- 2019年，IMC会议最佳论文奖与社区贡献奖提名
- 2019年，下一代互联网创新技术大赛，一等奖（9/287）
- 2018年，清华大学博士生国家奖学金
- 2016年，清华大学综合优秀奖学金

致谢

谢谢！

恳请各位老师批评指正！