ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

The Hijackers Guide To The Galaxy: Off-path Taking Over Internet Resources

Tianxiang Dai, Philipp Jeitner, Haya Shulman, Michael Waidner

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

Overview

- Digital resources and providers
- Taking over resource holders' accounts
- Vulnerable customers
- Potential resource manipulations
- Vulnerable resources
- Countermeasures & Conclusions

Digital resources and providers

Access to resources via SSO accounts

Provider datasets

RIRs AFRINIC APNIC ARIN LACNIC RIPE

Registrars Godaddy Namecheap Networksolutions enom name.com Alibaba Amazon Gandi Namesilo Google OVH

Cloud (IaaS) Amazon Azure Alibaba Google IBM Tencent Oracle DigitalOcean Linode IONOS Hostwinds OVHCloud Vultr CloudSigma

Certificate Authorities IdenTrust DigiCert Sectigo GoDaddy GlobalSign

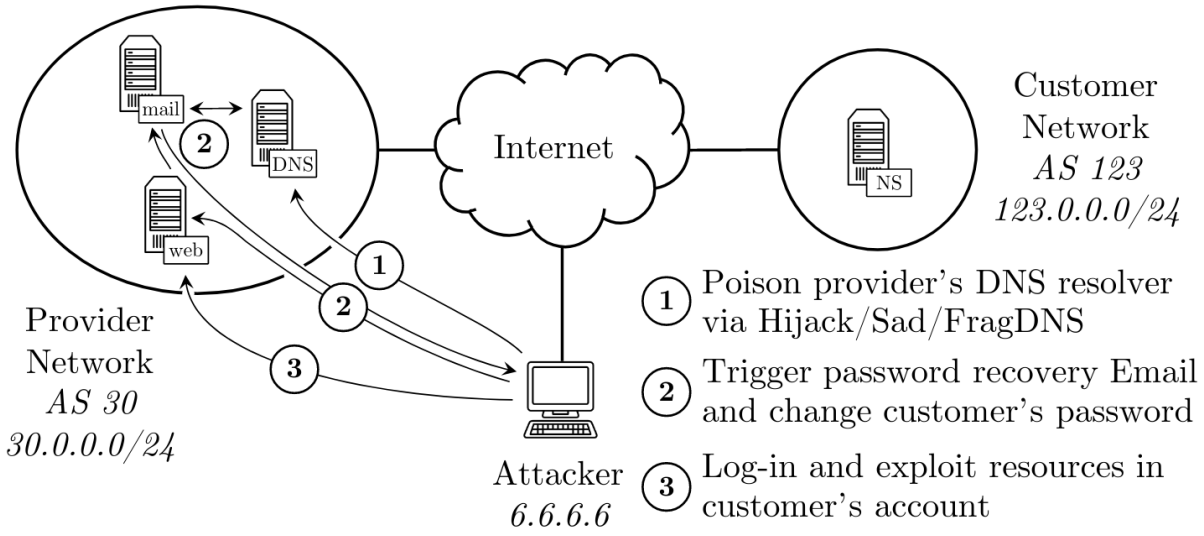
Customers datasets

- 75% of customers of RIRs (Local ISPs)
- 100K-top Alexa

Attacking providers

Taking over accounts from off-path

- Take over accounts via password recovery:
  - Poison DNS cache for victim domain
  - Trigger password recovery for victim domain
  - Reset password and take over account



How to poison cache?

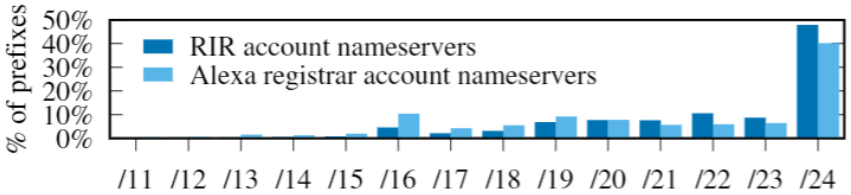
- On-path lookup interception
- Off-path:
  - BGP prefix hijacks
  - Side channels
  - IP fragmentation

Vulnerable providers	BGP sub-prefix	Side-channel	Frag-ment
RIRs	5/5	0/4	3/5
Registrars	11/11	0/9	11/11
Cloud providers	11/14	4/13	14/14
CAs	5/5	0/2	5/5
Total providers	**27/30**	**4/24**	**28/30**

Vulnerable Customers

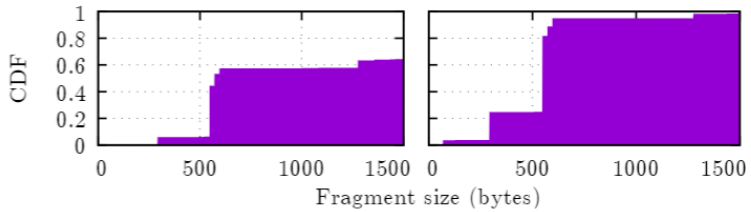
- Accessibility of customers‘ account details
  - 75% of ASes have email addresses listed in WHOIS
  - 11% of Alexa 100K domains
  - Account identifiers can also often be guessed

How to poison cache?
- On-path lookup interception
- Off-path:
  - BGP prefix hijacks
  - Side channels
  - IP fragmentation

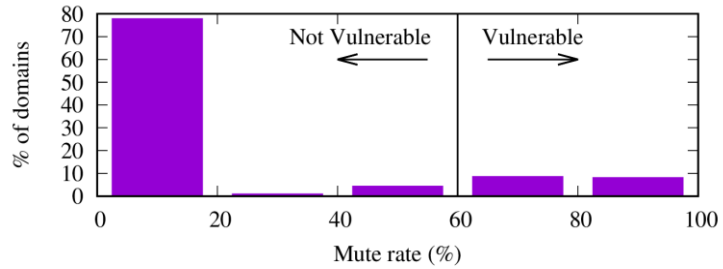


Networks vulnerable to sub-prefix hijacks

- Nameserver configuration:
  - 11-56% of accounts vulnerable



Domains with fragmented responses



Domains vulnerable to side channel attack

Manipulation of resources under providers

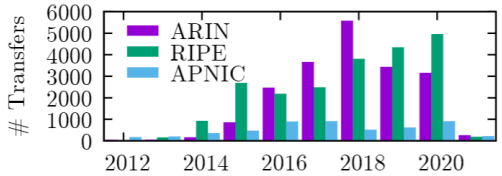
Test case: attacks via SSO account of LIR under RIPE NCC

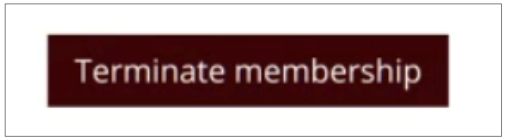
- **RPKI manipulation: create/remove/modify ROAs**
  - Disrupt propagation of BGP announcements
  - Expose to BGP hijacking
- **RIPE DB manipulation**
  - Allows impersonation of LIR representatives
  - Refused BGP peerings, dropped routers, degradation of conectivity
- **User, role and contact management**
  - Create new users (admin/operator)
  - Modify LIR contacts/details
  - Terminate LIR membership
  - Modify LIR organisation, address, VAT
- **Transfer of IPv4 resources**
  - Sell resources to a third party

Additonal Validation	Attack		RIRs	Registrars	IaaS	CAs	Outcome / Attacker use
RIRs	Account transfer/delegation		✓	✓	✓	✗	permanent control
No	Changing the account details		✓	✓	✓	✓	permanent control
RIRs	Close the account permanently		✓	✓	✓	✓	DoS
No	Disabling Email alerts		✓	✓*	✗	✓*	remain stealthy
RIRs	Resource transfer		✓	✓	✓	✗	permanent control
			✓	✓	✗	✗	sell resources
No	Resource return / deletion		✓	✓	✓	✓	DoS
CAs	Purchase new resources		✓	✓	✓	✓	financial Damage
			✓	✓	✓	✓	anonymous usage
No	Control / Modify Resources	Whois DB	✓	✓	✗	✗	facilitates hijacking
		VMs	✗	✗	✓	✗	various
		NS records	✗	✓	✗	✗	traffic hijacking
No	Create new ROAs/certificates		✓	✗	✗	✓	facilitates hijacking
No	Create invalid ROAs		✓	✗	✗	✗	DoS
No	Revoke certificates		✗	✗	✗	✓	DoS

RIPE DB manipulation

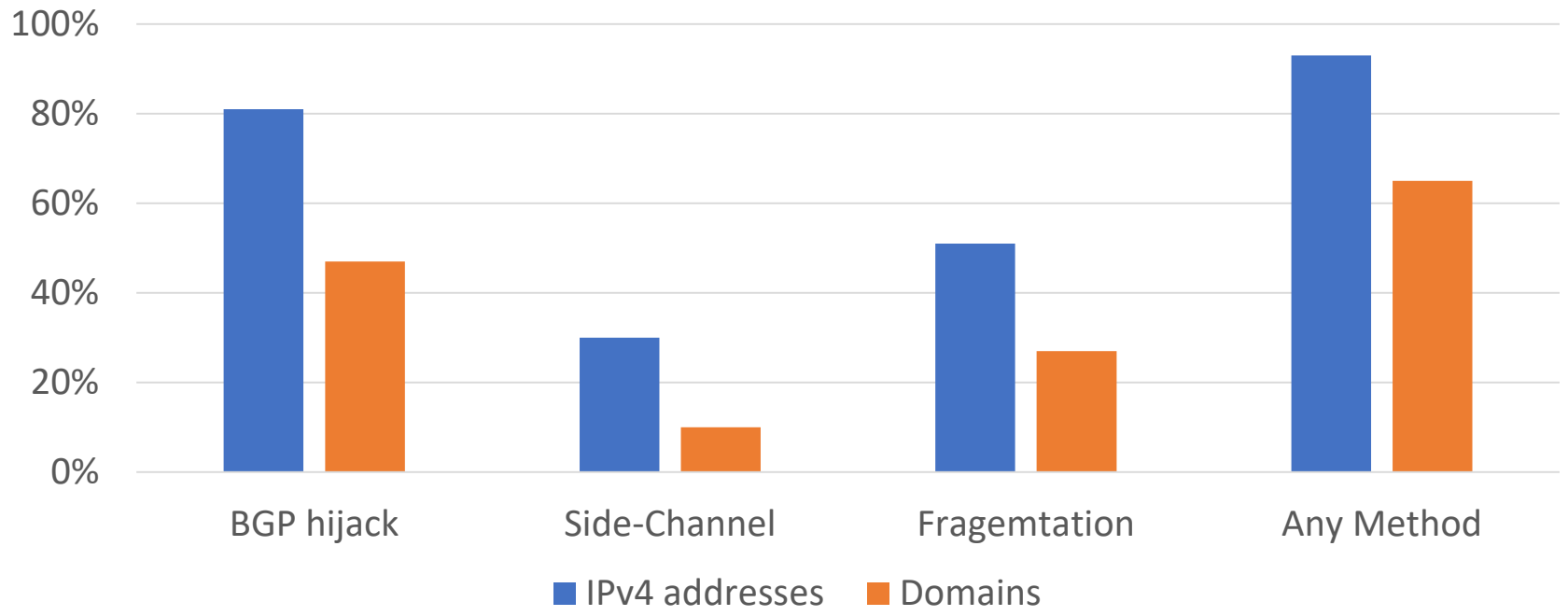
IPv4 Transfers per week:





IPv4 transfer

How many resources are vulnerable?



Resource	BGP hijack	Side-Channel	Fragmetation	Any Method
IPv4 addresses	81%	30%	51%	93%
Domains	47%	10%	27%	65%

Recommendations for countermeasures

Taking over accounts

Problems

Easy access to infrastructure, account details are public

Countermeasures

- ✓ Hide public account details
- ✓ Separate system for high-privilege accounts
- ✓ CAPTCHAs
- ✓ DNSSEC

Manipulating resources

Problems

Modifications are easy, stealthy and fast

Countermeasures

- ✓ 2-Factor authentication
- ✓ Account notificiations
- ✓ Account access restrictions
- ✓ Manual review/waiting time for transactions

Conclusions

- Resource databases are poorly protected
  - adversaries can take over the accounts and can manipulate them
- Attacks against accounts are practical
  - Large fraction of providers and customers are potentially vulnerable to off-path attacks
  - Even interesting for on-path attackers (nation adversaries, etc.)
- Fixes exist, but are not enforced
  - Strict authentication might drive customers away?

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