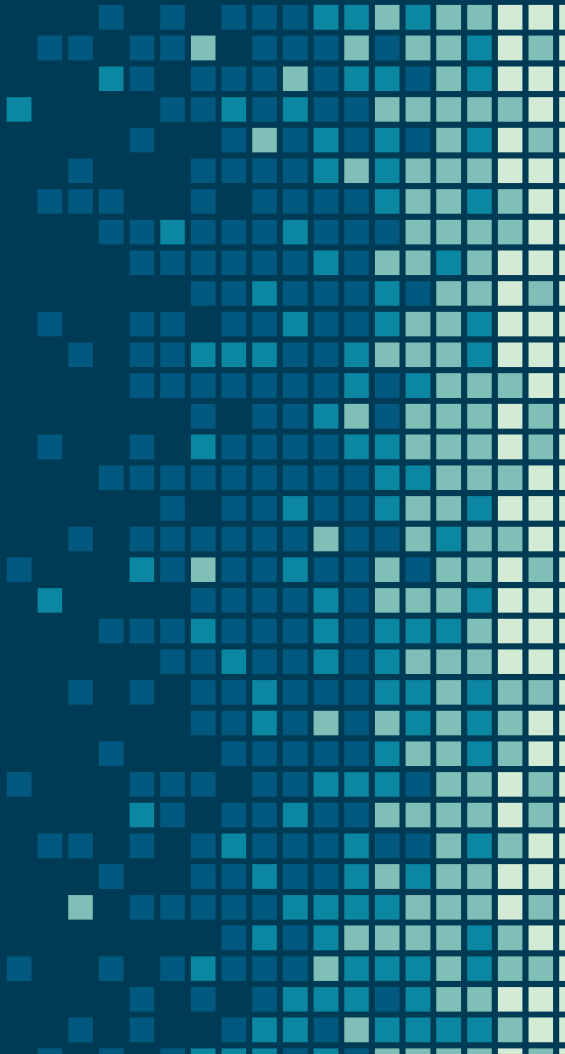
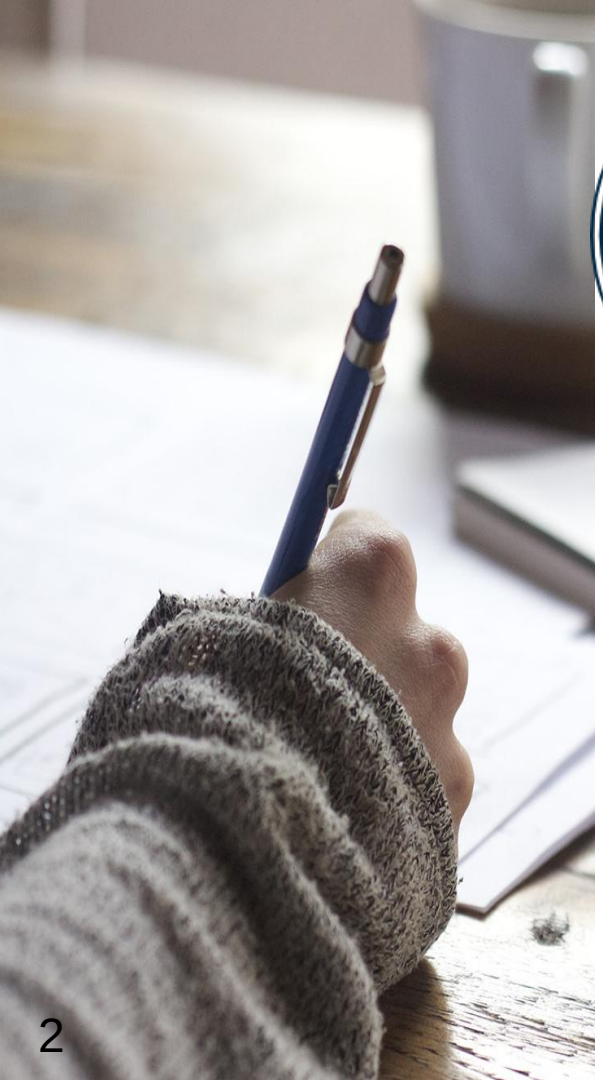
anatomy of a VoIP theft of service attack





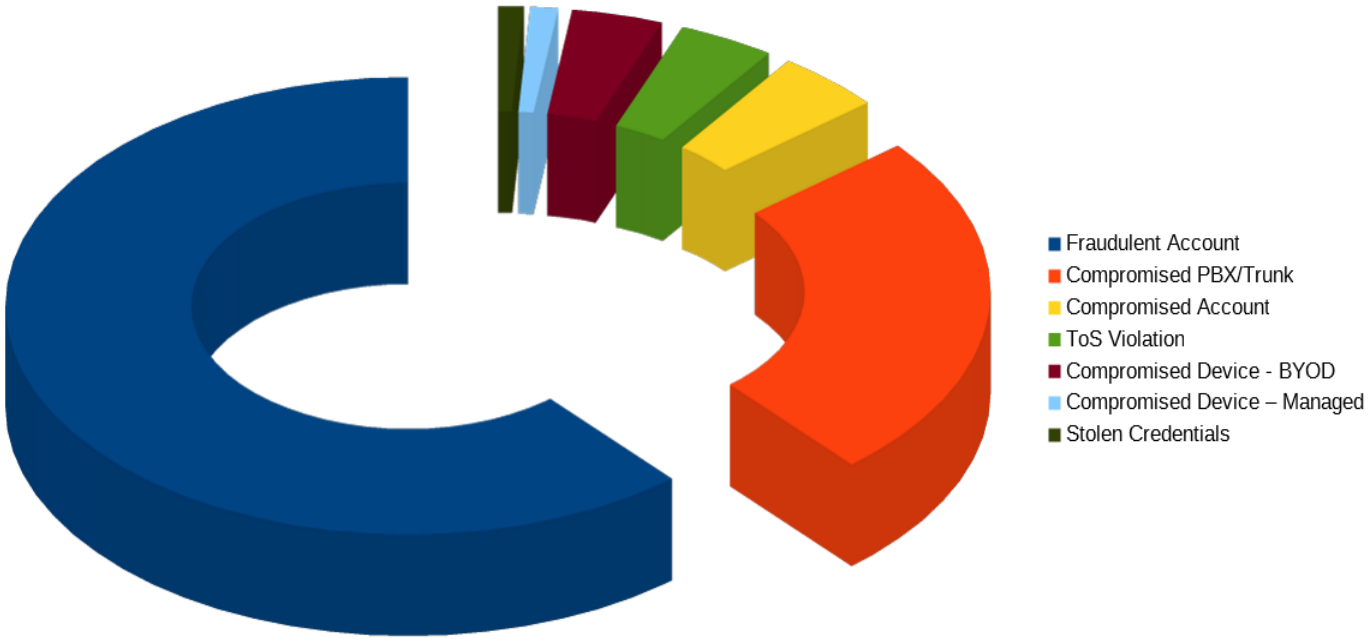
Iris Systems

Ryan Delgrosso
Principal

www.iris-sys.com

1.
where is it coming from?

how are fraudsters getting in?


Fraudulent Account
Compromised PBX/Trunk
Compromised Account
ToS Violation
Compromised Device - BYOD
Compromised Device – Managed
Stolen Credentials

2.
fraudulent accounts

who, and how

what are fraudulent accounts?

Fake Business

- It looks and smells like a new business lead.
- They will often pass the a cursory exam
- Credit card charges often go through for a month or two.

Stolen identity

- More common with residential services.
- Using stolen credit card to buy new service.
- Looking for app-based or BYOD service

Arbitrage

- Opportunistic customers using your plans against ToS
- Domestic dialer or intl resale
- Pass all validation (even credit/DUNS)

3.
compromised pbx/sip trunk

how do they get in? then what?

how do they get in?

Voicemail Hacking

Breaking into the voicemail system and using the callback feature

Extension Hijack

Break into a sip account with a weak password

Admin Hijack

The admin panel for the PBX is remotely accessible and an account has weak credentials

User Hijack

A user portal on the PBX with weak credentials is an excellent point of access to configure forwarding

Endpoint Hijack

IP Phones left configured with public internet access to admin pages are easy targets to setup forwarding or worse

API Hijack

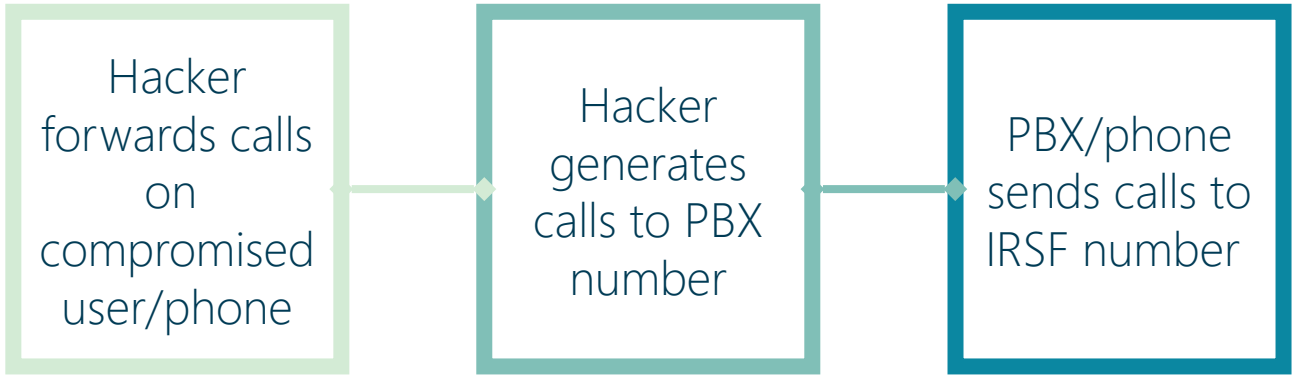
Nearly all IP PBX systems today have powerful API's and most are left with default setting

“it works because its right. its not right because it works”

customers frequently stop configuring their systems when calls start working, leaving holes behind.

voicemail hacking

call forwarding



call transfer

how to defend against this?

Be on the lookout for war dialing

Look for inbound sequential dialed calls that suddenly connect to the same number repeatedly

Tiered dialing

Impose choke-trunks for premium prefixes or block tiers of numbers all together as default

Prepaid

Prepaid services insulate the provider quite a bit as long as you are doing live-charging

User agent fingerprinting

Tracking user agents in signaling will let you get ahead of PBX versions that have been compromised

Pre turn-up scan

Scan your customers for basic vulnerabilities.

Deploy your own edge

Deploying an E-SBC and managing the surfaces of the customers equipment for them can alleviate a lot of this

4. compromised account

compromised hosted services

account portal break-ins

- provision new services to make fraudulent calls
- steal credentials to existing user accounts
- reset voicemail PIN and use callback feature
- provision mobile apps with user credentials
- access api and click-to-call functions
- access invoices for other fraud

myth: adding security increases user friction

service providers live and die by customer convenience

mitigating account break-in

Selective MFA

Make use of known computers and only MFA new ones.

Get geographical

Use geographical and proxy detection tools to separate wheat from chaff

https://www.maxmind.com

Passwords for people

Stronger passwords doesn't mean harder to remember passwords.

https://xkcd.com/936/

Rate limiting / Blacklisting

Track failed logins. Blacklist early and often for short times.

Red-teaming

Attack your own network. Find the weak links.

Aggregate logs

Know everything about your network. Even if someone gets in, have the info to figure out how.

https://www.elastic.co/elk-stack

5. compromised endpoints

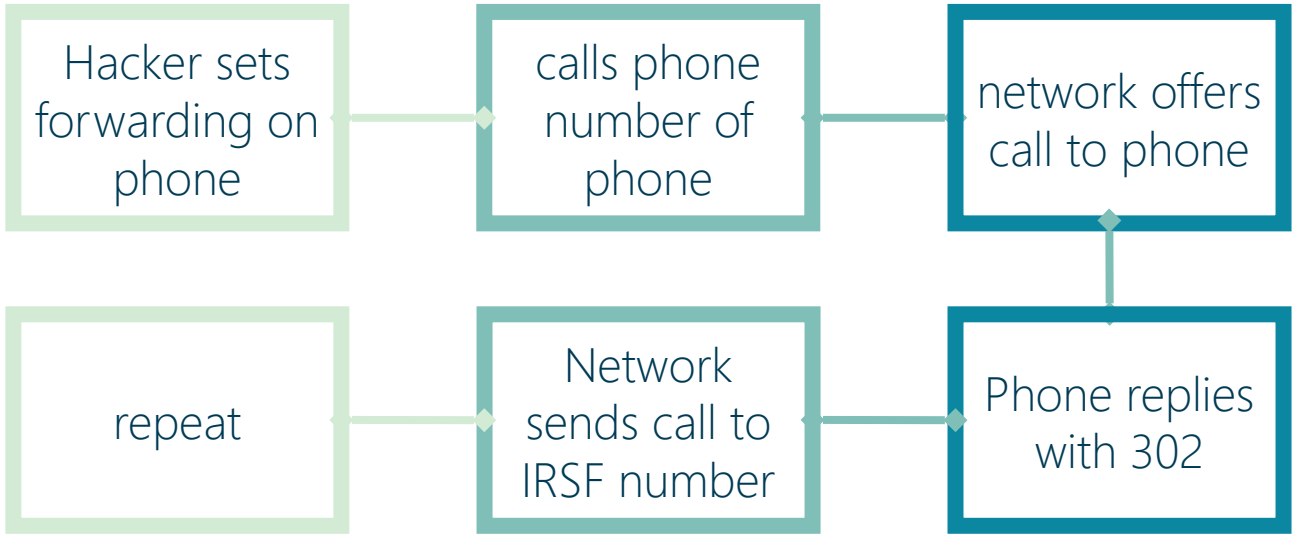
each phone is a battleground

“you cannot compromise a device if you cannot reach it”

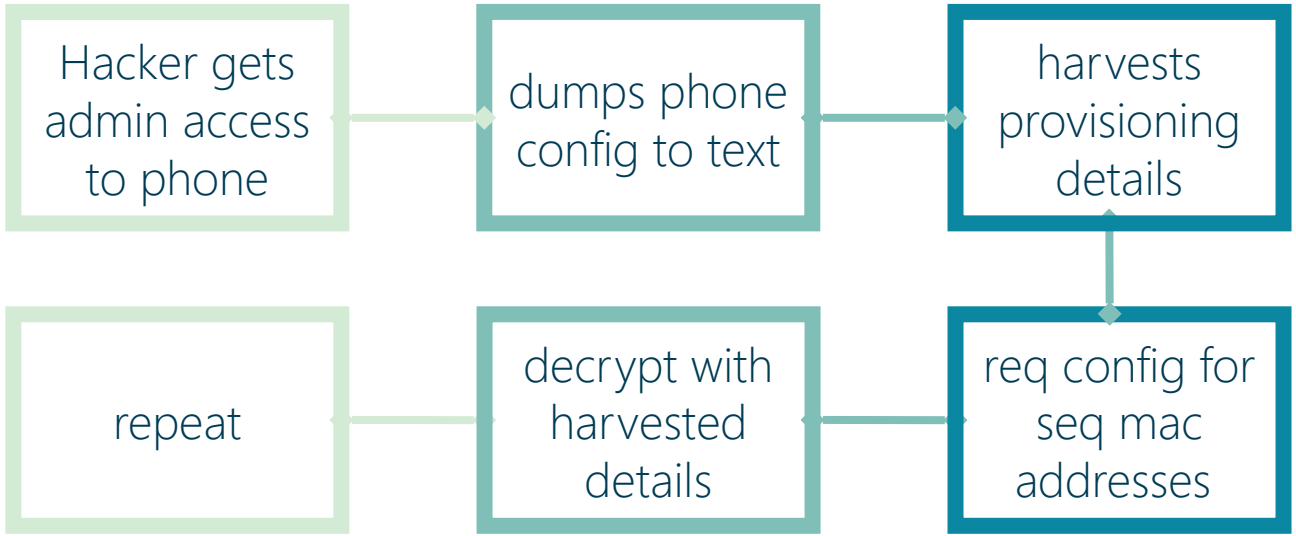
modern IP phones are a juicy target

- contains sip credentials, certificates and provisioning keys.
- limited security options due to hardware limitations
- starting to expose rich API controls for integration
- often have weak passwords for “ease”

sip 3xx forwarding



provisioning harvest attack



defending your endpoints

Out of band management

Use devices with strong management solutions. No more exposed devices and is a force multiplier for support.

Disable unused API's

You probably arent using that cisco web-dialer api. Disable it.

No public access

Never ask a customer to allow all traffic to a phone, and if that must happen make sure it gets closed after.

Certificates

Use certificates for provisioning (Client and Server). Its free now!

https://letsencrypt.org

Per-device credentials

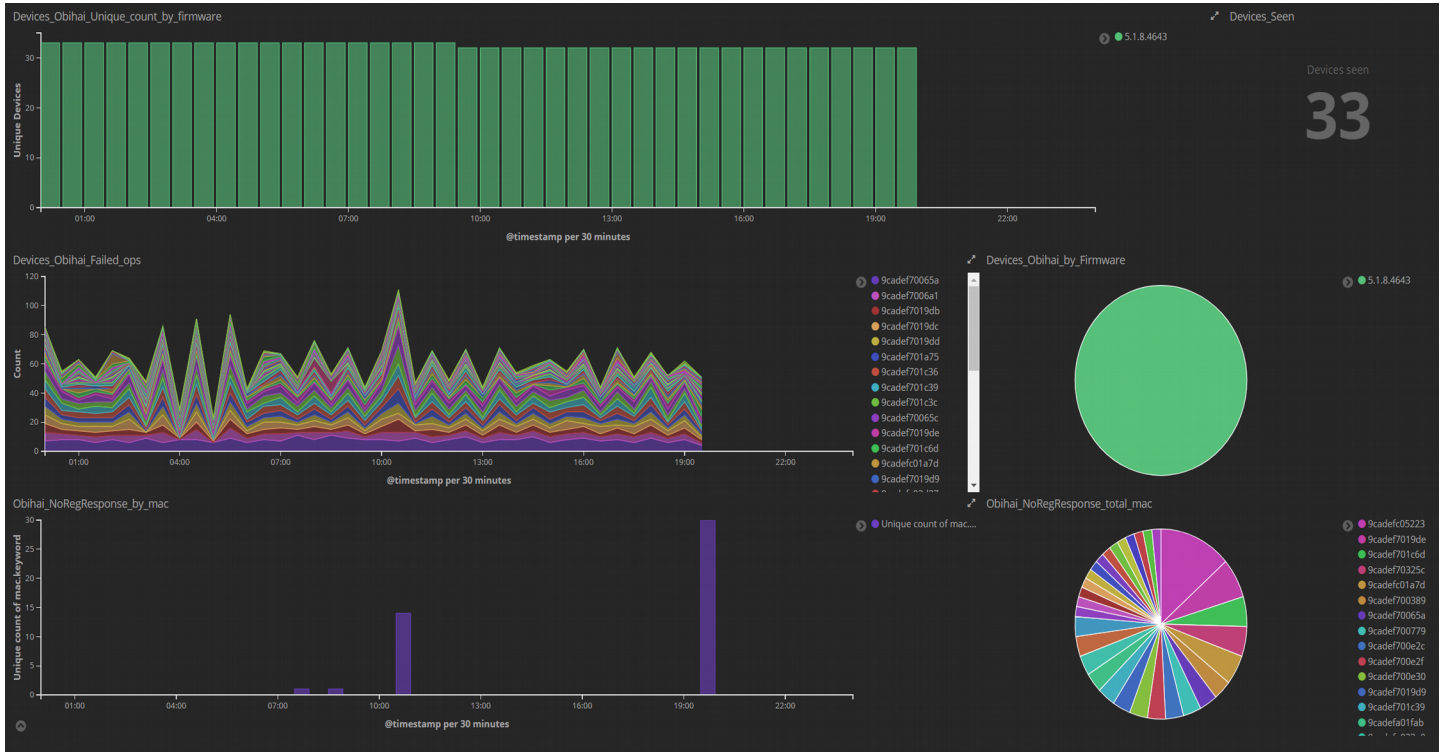
dont use global device passwords. Generate per customer or per-device passwords.

Aggregate logs

device syslog isnt just for troubleshooting. Its a force multiplier for management!

https://www.elastic.co/elk-stack

ELK stack logging



mobile app compromises

ITSP's with a mobile app are vulnerable through that app being run in a development emulator!

5.
free floating hostility

un-focused brute-force attacks

your network is under constant attack

Whether you are aware or not, millions of bots and low-level hackers are probing voice networks constantly looking for weak and predictable accounts

a multi-pronged approach is needed

strategies for surviving the chaos

Defense in-depth

Use a layered approach. Stacking SBC's behind security appliances, behind ACL's and RTBH services gives you multiple points to defend from.

Network intelligence

Know whats normal on your network. Investigate the abnormal. Unexplained seismic shifts are almost always bad.

Automated convergence

Things never go wrong when you're watching them. Your network needs to adapt and protect itself automatically.

THANKS!

Any questions?

You can find me at:

ryan@iris-sys.com

www.iris-sys.com