Cisco
Customer Experience

Hello: I bring you announcements from other Autonomous Systems

Building SOC capability for telcos

Tim (Wadhwa-)Brown
Engineering Technical Leader, CX CoE Security
June 2023

Background

- I own(ed) an ISP
- I cut my offensive teeth testing various telecoms networks both in labs and in production
- I work closely with with MITRE and other interested parties

Why give this talk?

- We all rely on secure networks
- Working for Cisco, I’m a technical SME with an interest in keeping our telcos secure
- Purple is the new red

An approach

- Threat modelling
  - What do you have, what do you need?
  - Suggested use cases as output
- Threat hunting
  - Conduct threat hunts based on threat model
- Detection engineering
  - Combine telemetry from SIEM, queries (Sigma et al) and big data analytics
  - Define specific use cases where big data can identify threats that analysts can’t

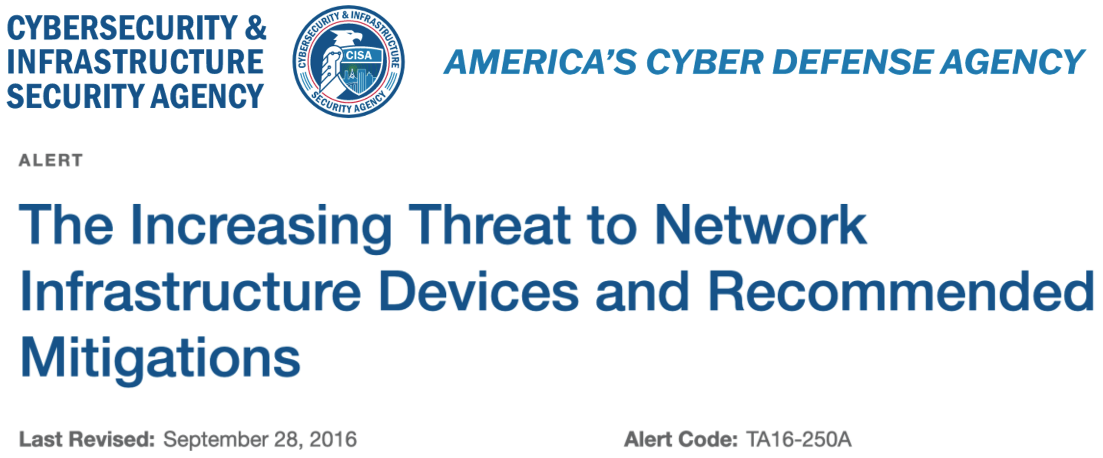
Where should we start?

Attacks in the wild…

Sep 2016

Risks to network infrastructure

- A network infrastructure device has:
  - Operating system
  - Free CPU cycles
  - Little / no end point detection
  - Vulnerabilities
  - Potentially overlooked
  - Potentially outsourced
  - Opportunities!!!



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

ALERT

The Increasing Threat to Network Infrastructure Devices and Recommended Mitigations

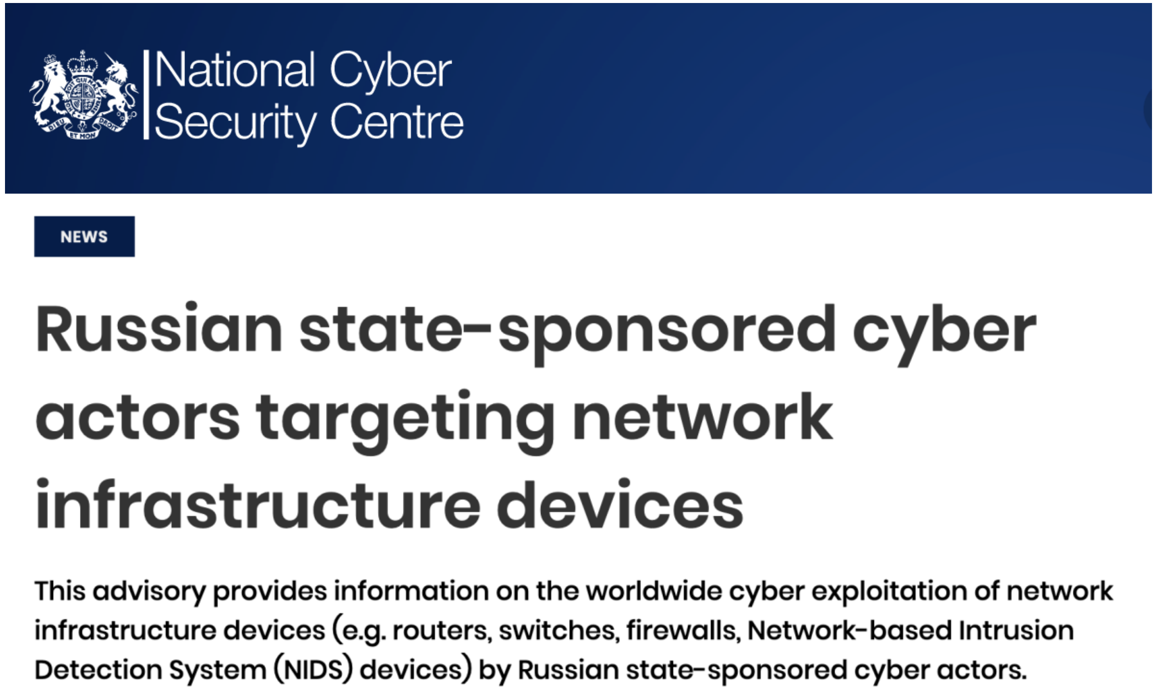
Last Revised: September 28, 2016

Alert Code: TA16-250A

Apr 2018

More activity

- “Russian state-sponsored cyber actors are using compromised routers to conduct man-in-the-middle attacks to support espionage, extract intellectual property, maintain persistent access to victim networks, and potentially lay a foundation for future offensive operations.”



National Cyber Security Centre

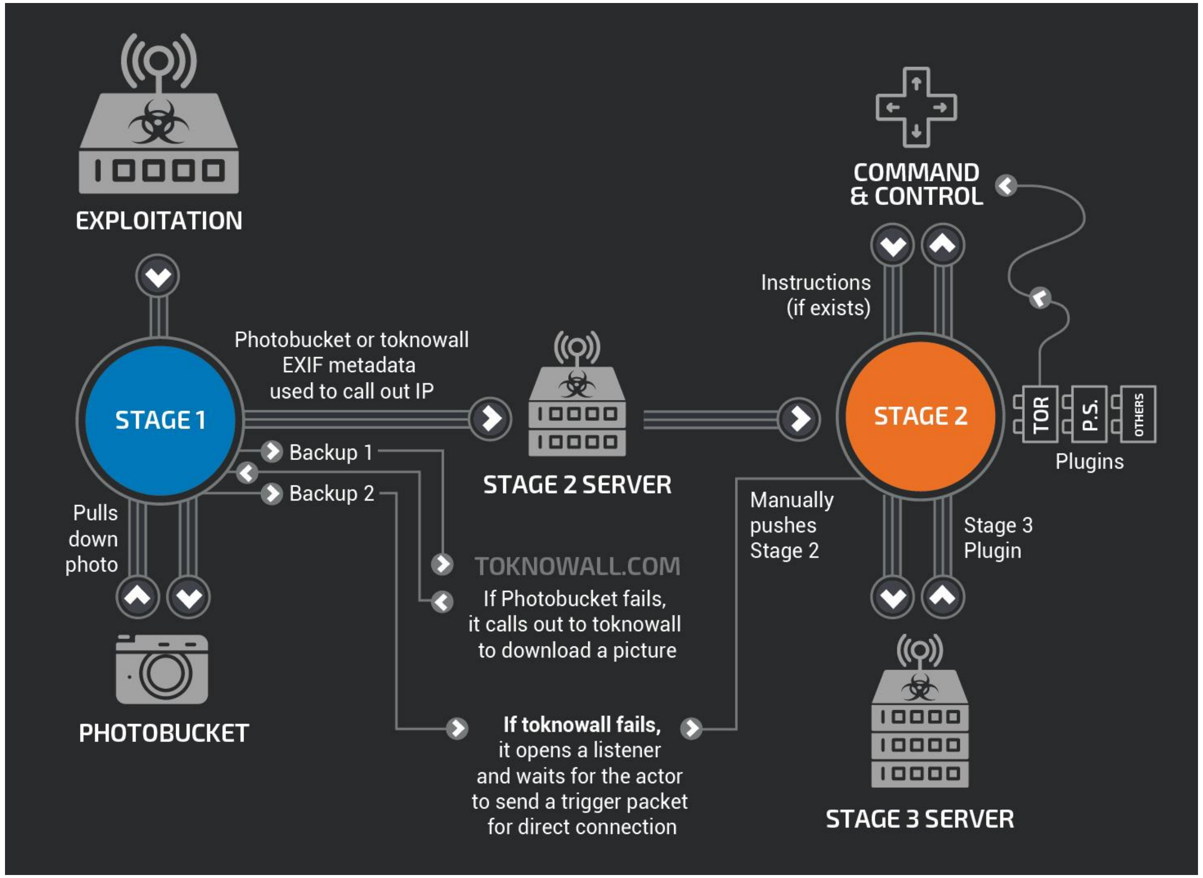
NEWS

Russian state-sponsored cyber actors targeting network infrastructure devices

This advisory provides information on the worldwide cyber exploitation of network infrastructure devices (e.g. routers, switches, firewalls, Network-based Intrusion Detection System (NIDS) devices) by Russian state-sponsored cyber actors.

VPNFilter

- Modular malware affecting 500 000 SOHO routers and network storage systems
- APT28’s broken RC4 implementation
- Identified modules hint at objectives


EXPLOITATION
COMMAND & CONTROL
Instructions (if exists)
Photobucket or toknowall EXIF metadata used to call out IP
STAGE 1
STAGE 2 SERVER
STAGE 2
TOR
P.S.
OTHERS
Plugins
Backup 1
Backup 2
Pulls down photo
Manually pushes Stage 2
Stage 3 Plugin
TOKNOWALL.COM
If Photobucket fails, it calls out to toknowall to download a picture
PHOTOBUCKET
If toknowall fails, it opens a listener and waits for the actor to send a trigger packet for direct connection
STAGE 3 SERVER

Modular functionality

- Stage 1 – Persistence via crontab, C2 via Tor or SSL
- Stage 2 – Execute commands, file upload/download, kill switch, proxy
- Modules:
  - Tor client
  - Wipe system, brick device.
  - Downgrade https to http, inject JS, redirect traffic, record credentials & tokens
  - Capture port 502 (Modbus) traffic
  - Subnet ARP scan, MicroTik network discovery protocol
  - SSH server, SSH connect, port scan IP range
  - Drop traffic, port forward, socks5 proxy, establish VPN to internal network
- Possibly additional modules, probably found most common.

June 2019 - Feb 2023

Cyclops Blink

- Modular malware affecting SOHO network devices
- VPNFilter v2
- Similar C2 weakness

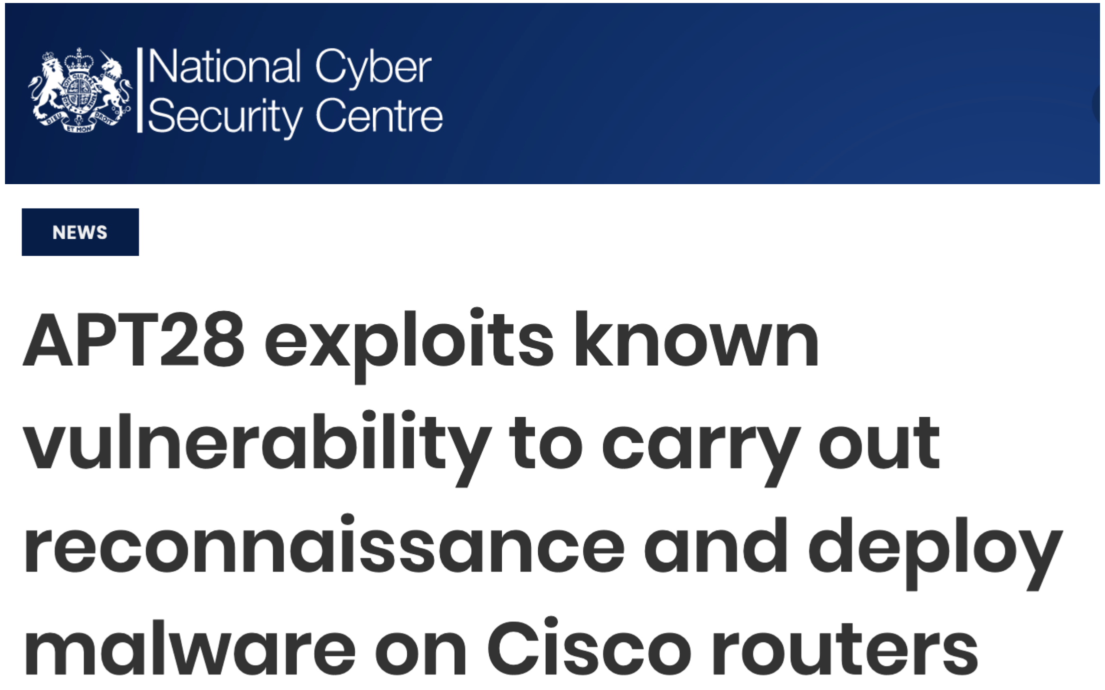
Modular functionality

- Modules:
  - System reconnaissance
  - File upload / download
  - Store & update C2 IPs
  - Update & persist
- Additional modules?

Apr 2023

Jaguar Tooth

- Exploitation of CVE-2017-6742, SNMP vuln
- Part of wider campaign against network infrastructure (not only Cisco)
- GRE tunnel creation, DNS hijack
- Modifying memory to reintroduce vulns
- Modifying configuration to make insecure
- Traffic capture, exfiltration & modulation
- Additional payloads
- Persist
- Scale & tempo give cause for concern



National Cyber Security Centre

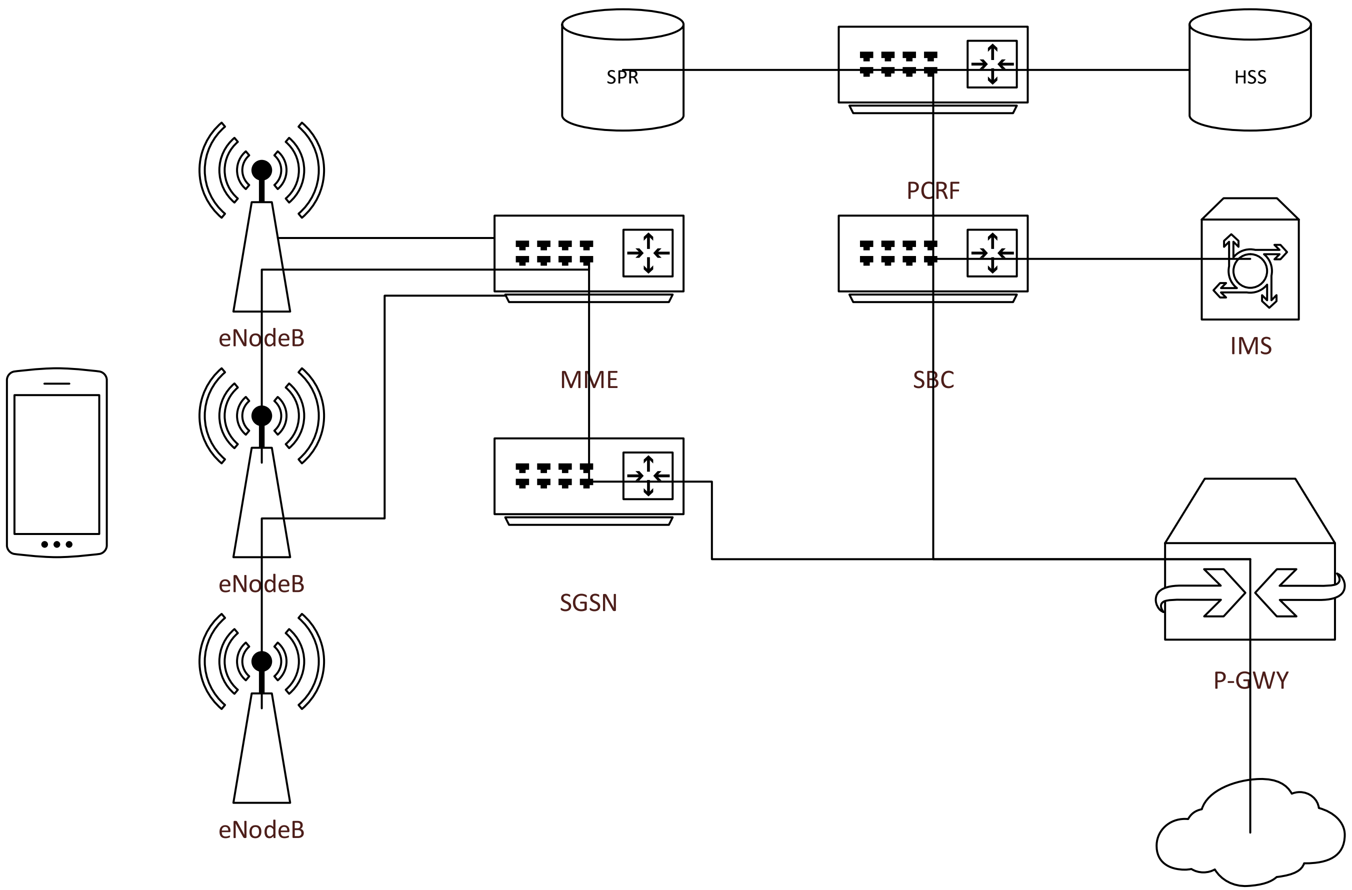
NEWS

APT28 exploits known vulnerability to carry out reconnaissance and deploy malware on Cisco routers

What do we know about mobile networks?

…and the threat landscape?

4G Mobile Core

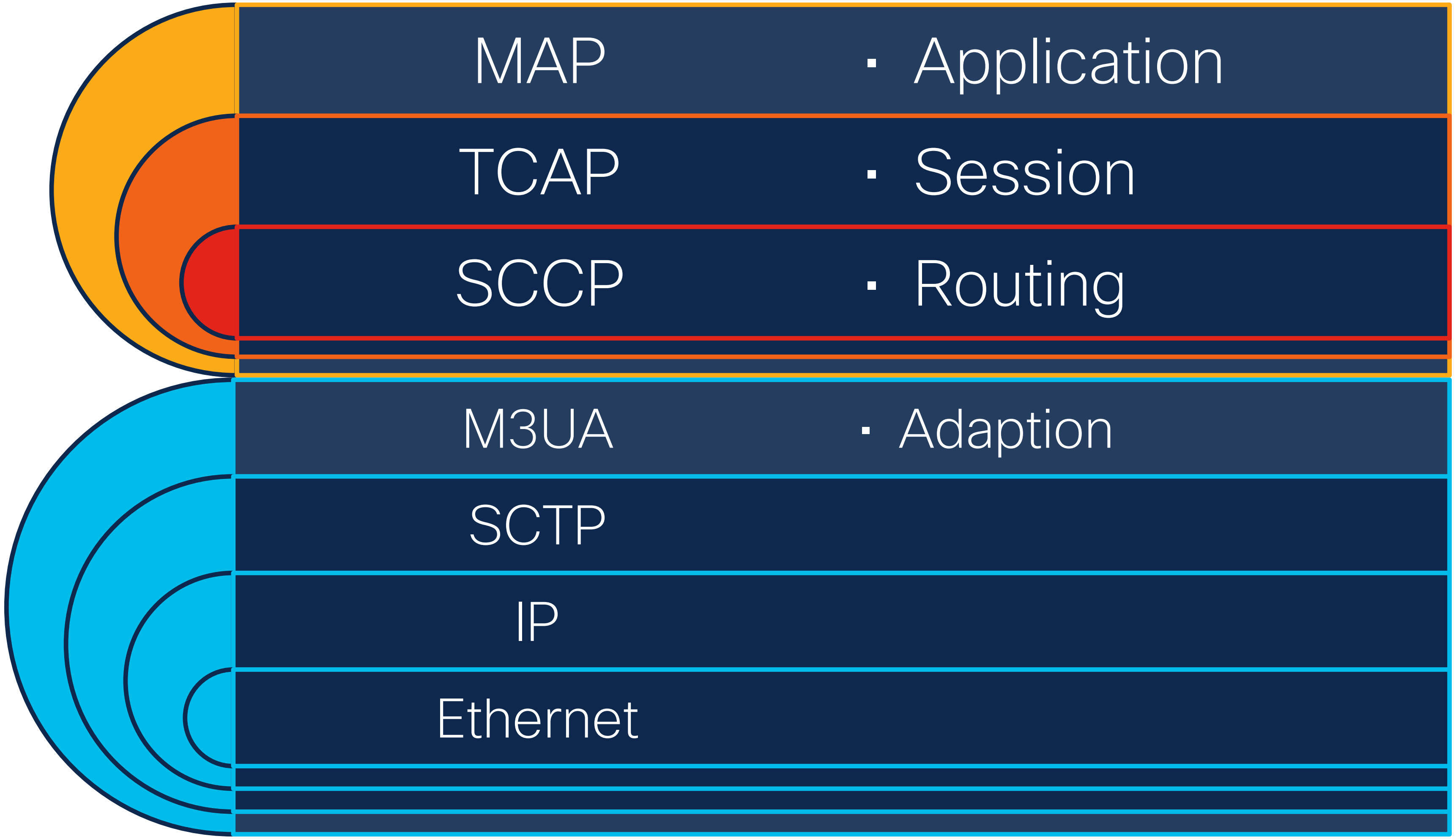


- HSS – Home Subscriber Server
- SPR – Subscriber Profile Register
- PCRF – Policy and Charging Rules Function
- PCEF – Policy and Charging Enforcement Function
- MME – Mobility Management Entity
- SGSN – Serving GPRS Support Node
- IMS – IP Multimedia Subsystem
- SBC – Session Border Controller

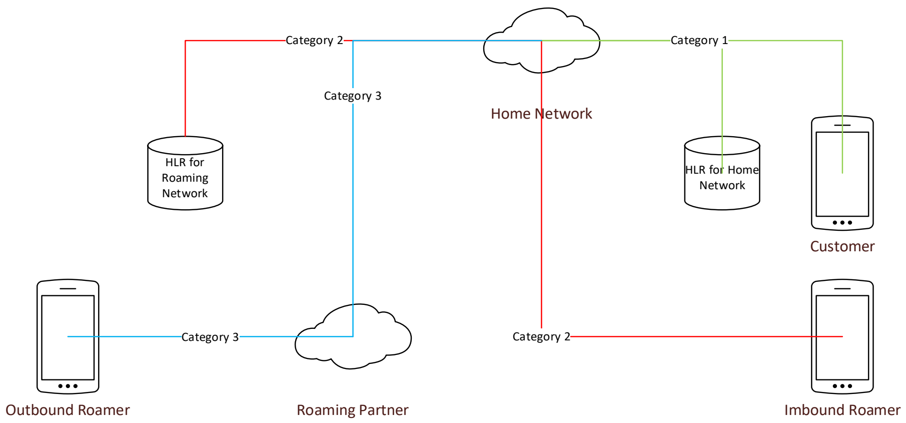
What does the control plane look like?

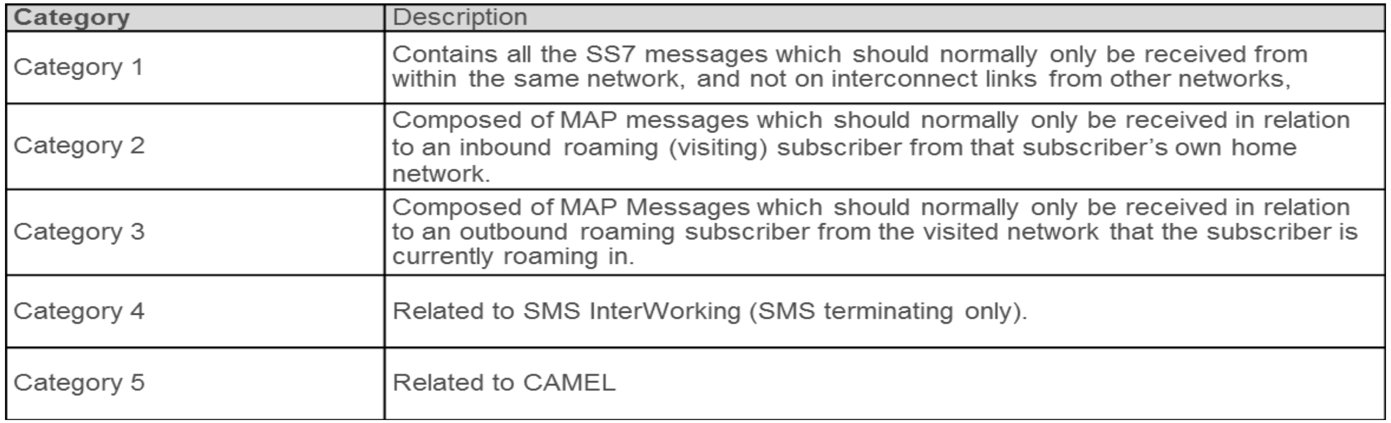
- SS7 and Diameter
  - AAA
- GTP-[UC]
  - Establishes tunnels

SIGTRAN and SS7 protocol stack



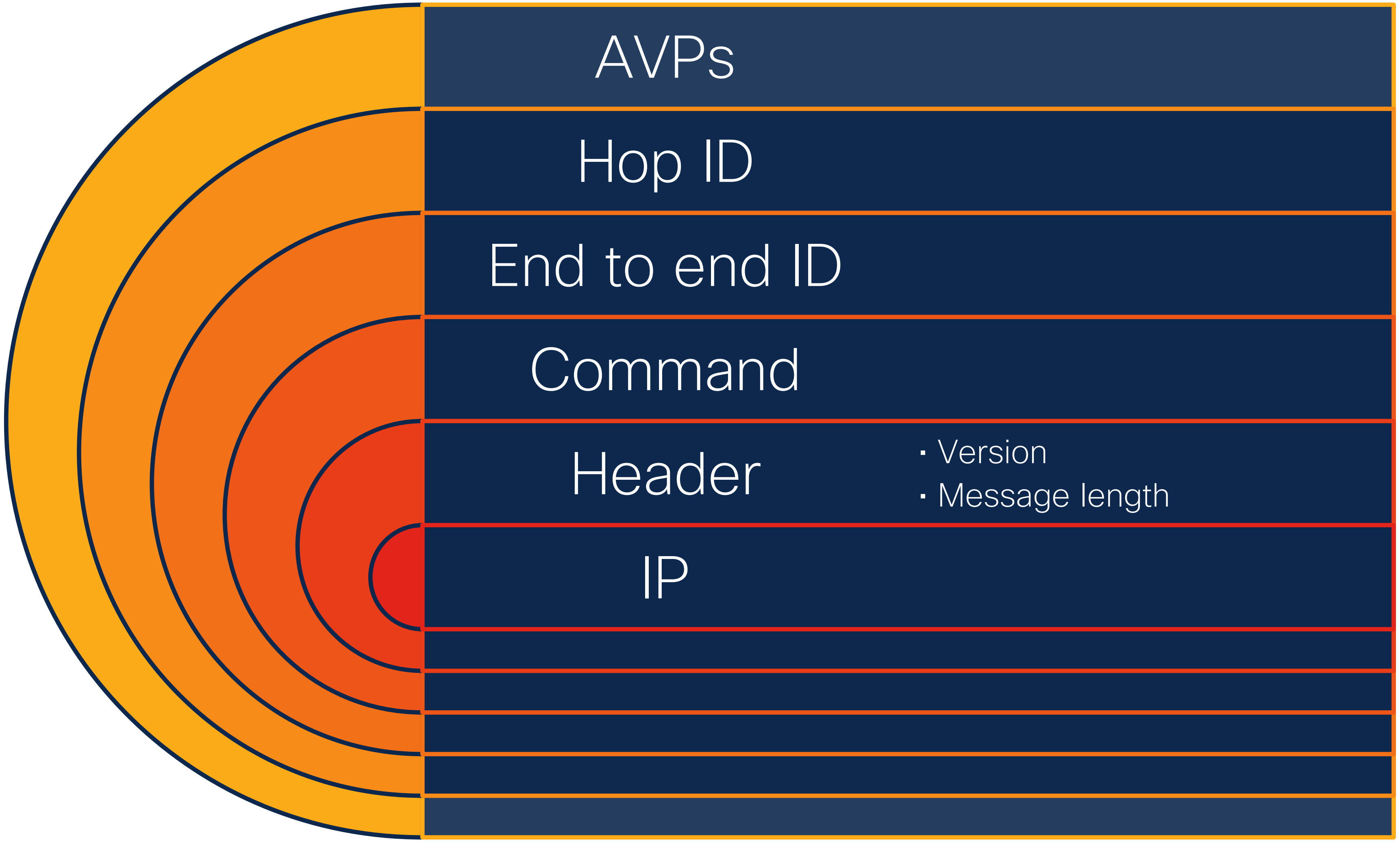
GSMA message categories





Category	Description
Category 1	Contains all the SS7 messages which should normally only be received from within the same network, and not on interconnect links from other networks,
Category 2	Composed of MAP messages which should normally only be received in relation to an inbound roaming (visiting) subscriber from that subscriber's own home network.
Category 3	Composed of MAP Messages which should normally only be received in relation to an outbound roaming subscriber from the visited network that the subscriber is currently roaming in.
Category 4	Related to SMS InterWorking (SMS terminating only).
Category 5	Related to CAMEL

Diameter protocol



AVPs

Hop ID

End to end ID

Command

Header

- Version
- Message length

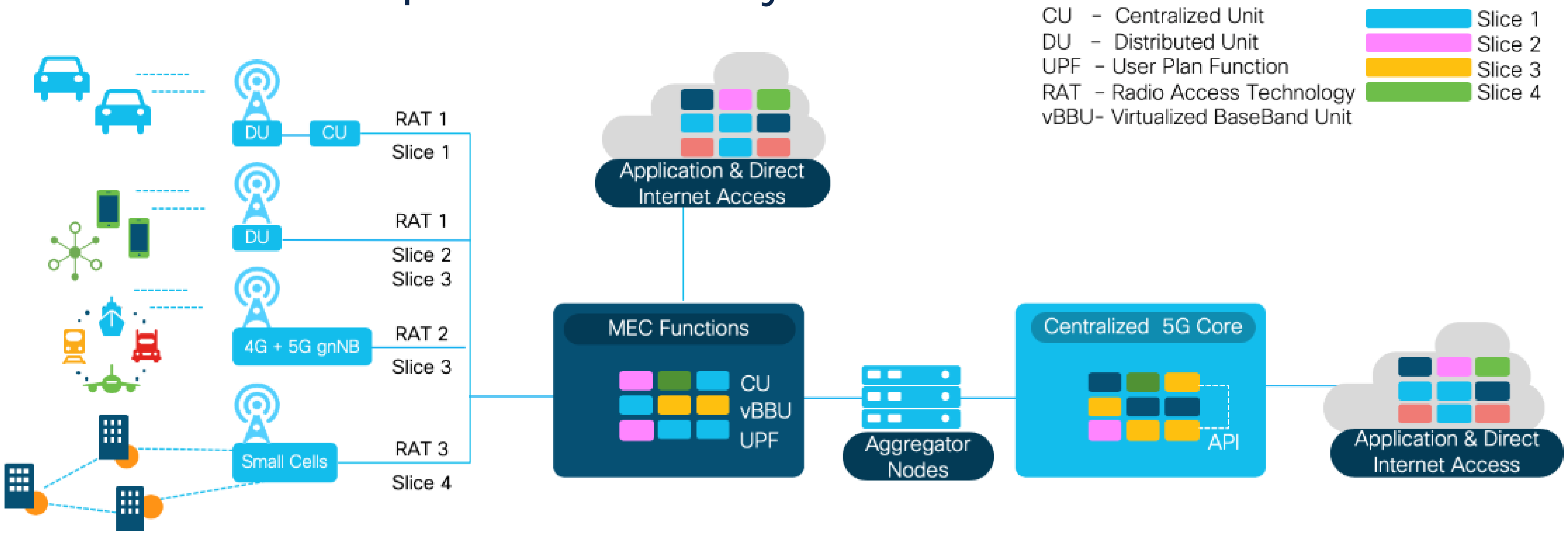
IP

SS7/Diameter mappings*

Diameter Command	Interface	Direction		SS7 Equivalence
Command Name	Name	Source	Destination	Command Name
Update-Location-Request	S6a	MME	HSS	Update-Location-Request
Update-Location-Request	S6d	SGSN	HSS	Update-GPRS-Location-Request
Cancel-Location-Request	S6a	HSS	MME	Cancel-Location-Request
Cancel-Location-Request	S6d	HSS	SGSN	Cancel-Location-Request
Authentication-Information-Request	S6a	MME	HSS	Send-Authentication-Information-Request
Authentication-Information-Request	S6d	SGSN	HSS	Send-Authentication-Information-Request

* Illustrative rather than a complete mapping of all operations

Threat landscape in today's mobile networks



CU - Centralized Unit
DU - Distributed Unit
UPF - User Plan Function
RAT - Radio Access Technology
vBBU- Virtualized BaseBand Unit

🟦 Slice 1
🟪 Slice 2
🟨 Slice 3
🟩 Slice 4

Device Threats

- SIM manipulation
- Cloning
- Bots DDoS
- Firmware Hacks
- Device Tampering
- Sensor Susceptibility
- TFTP MitM attacks

Air Interface Threats

- MitM attack
- Jamming

RAN Threats

- Rogue Nodes
- Insecure S1, X2
- Insecure Xx, Xn

MEC & Backhaul Threats

- DDoS attacks
- LI Vulnerabilities
- Insecure Sx
- Insecure N6
- CP / UP Sniffing
- MEC Backhaul sniff
- API Vulnerabilities
- Side Channel attacks
- NFVi Vulnerabilities

5G Packet Core & OAM Threats

- Virtualization
- LI Vulnerabilities
- Improper Access Control
- Network Slice security
- API vulnerabilities
- NEF vulnerabilities
- IoT Core integration
- Roaming Partner
- DDoS & DoS attacks

SGi / N6 & External Roaming Threats

- IoT Core integration
- VAS integration
- App server vulnerabilities
- Application vulnerabilities
- API vulnerabilities

Lightbasin

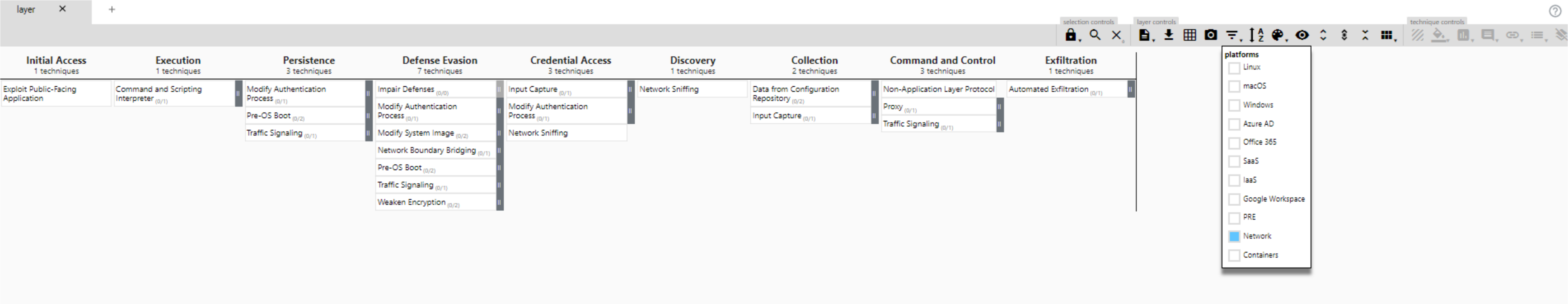
- Password spray w/ default vendor passwords
- Compromised an eDNS node
- Deployed PAM backdoor known as SLAPSTICK
- Utilised ICMP tunneling
- Used SGSN emulation software to support C2 activities in concert with TinyShell
  - Connect to nine pairs of International Mobile Subscriber Identity (IMSI) and Mobile Subscriber Integrated Services Digital Network (MSISDN) numbers
  - Established GTP tunnels
- Leveraged SIGTRAN for additional G2

Redressing the balance

Cyber hygiene is *critical*

There’s more though…

- https://mitre-attack.github.io/attack-navigator/
  - Create New Layer
  - Enterprise
  - Filters > Platforms > Network



Initial Access 1 techniques	Execution 1 techniques	Persistence 3 techniques	Defense Evasion 7 techniques	Credential Access 3 techniques	Discovery 1 techniques	Collection 2 techniques	Command and Control 3 techniques	Exfiltration 1 techniques
Exploit Public-Facing Application	Command and Scripting Interpreter (0/1)	Modify Authentication Process (0/1)	Impair Defenses (0/0)	Input Capture (0/1)	Network Sniffing	Data from Configuration Repository (0/2)	Non-Application Layer Protocol	Automated Exfiltration (0/1)
		Pre-OS Boot (0/2)	Modify Authentication Process (0/1)	Modify Authentication Process (0/1)		Input Capture (0/1)	Proxy (0/1)	
		Traffic Signaling (0/1)	Modify System Image (0/2)	Network Sniffing			Traffic Signaling (0/1)	
			Network Boundary Bridging (0/1)					
			Pre-OS Boot (0/2)					
			Traffic Signaling (0/1)					
			Weaken Encryption (0/2)					

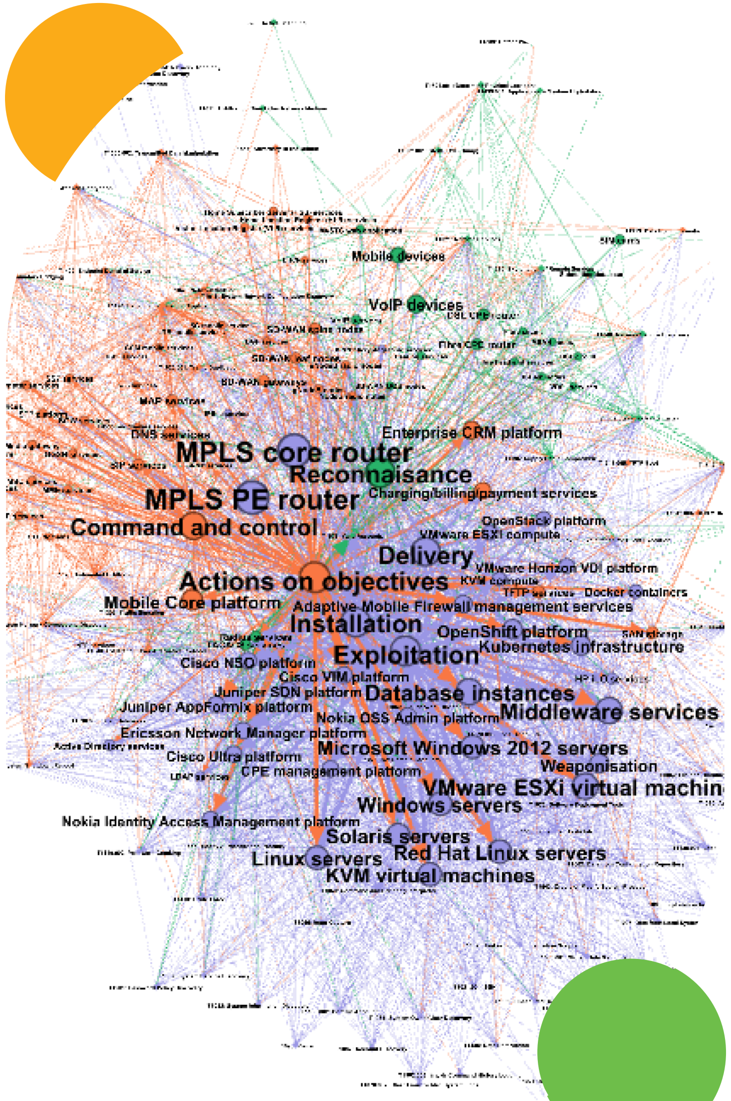
platforms
□ Linux
□ macOS
□ Windows
□ Azure AD
□ Office 365
□ SaaS
□ IaaS
□ Google Workspace
□ PRE
☑ Network
□ Containers

How do we go about building SOC capability for a telco?

- Threat model
- Manual hunts
- Automation

What does the threat model for a telco look like?

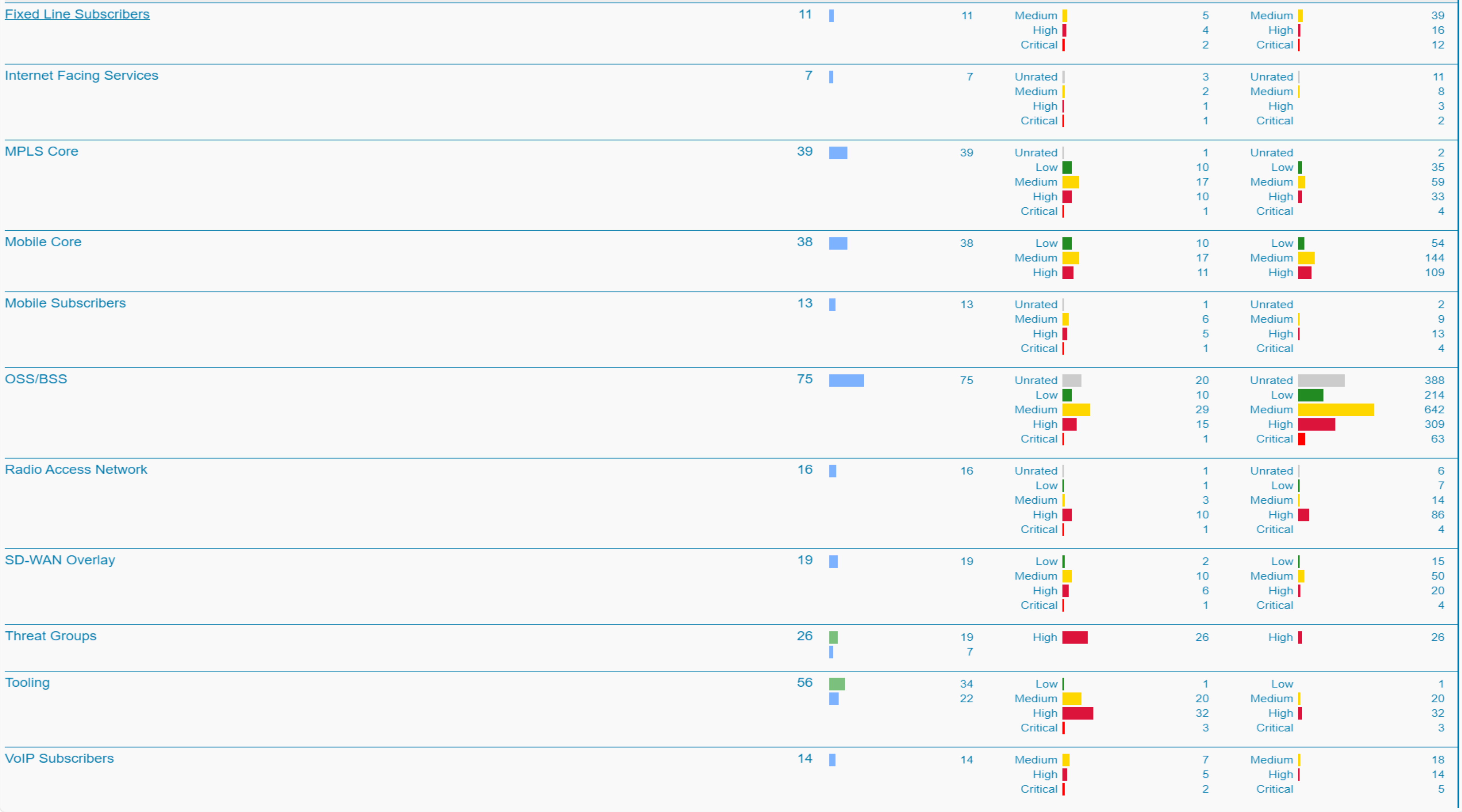
What might a telco graph look like?



- OSS/BSS
- Subscribers
- Routing and switching fabric
- Mobile networks

Useful generalisations

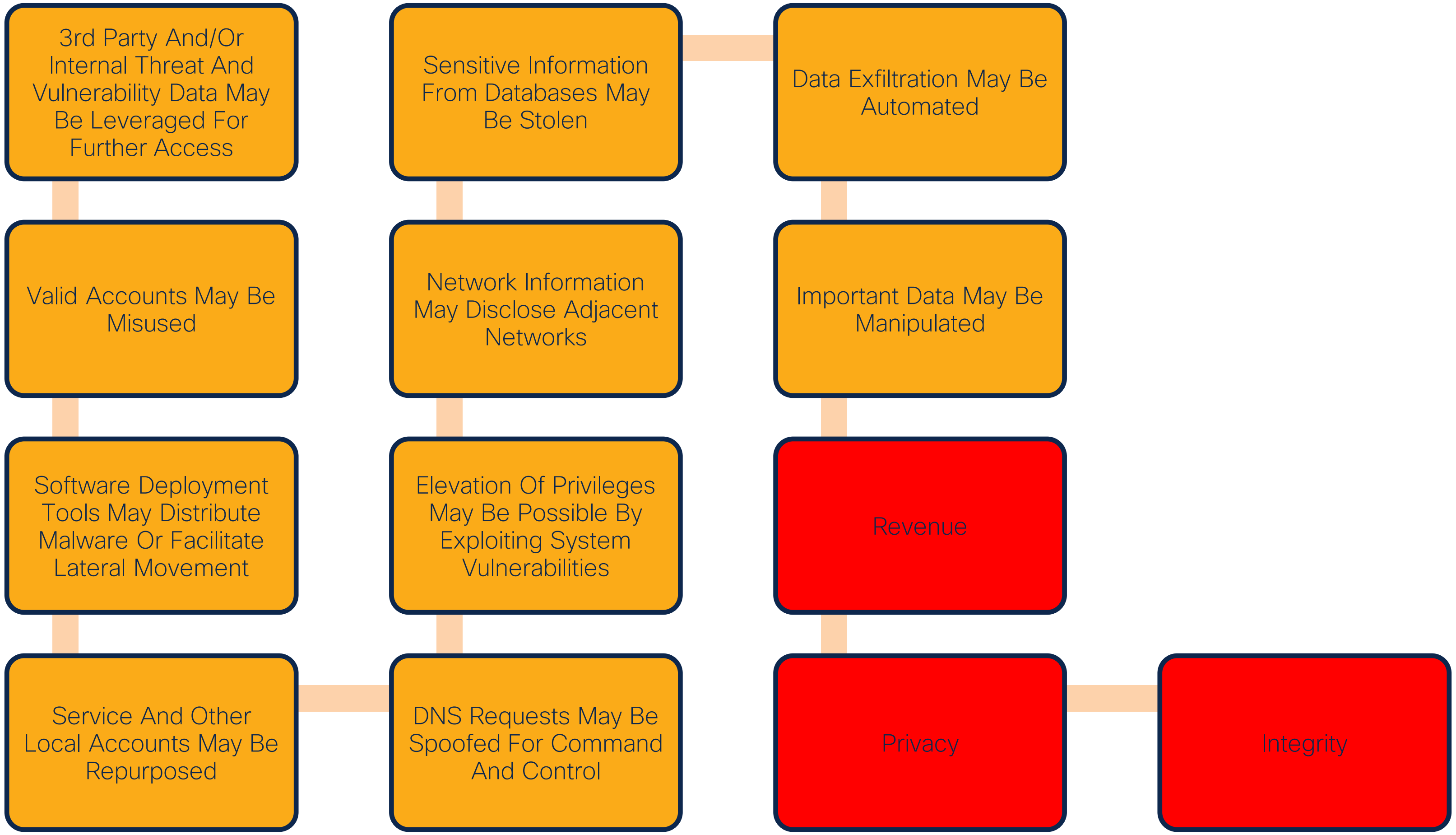
- Not all systems will be affected by all tactics
  - Initial access
    - Subscribers, maybe OSS/BSS
  - Impact
    - HLR, core routing and switching
- Use CVSS for scoring
  - Imperfect
    - Better than nothing
    - Captures properties of techniques quite nicely
- Think STRIDE
  - Enterprise and mobile techniques can be mapped into a telco specific equivalents
    - E.g. Most directory services are likely to have similar threat models, AD or otherwise



Fixed Line Subscribers	11	11	Medium	5	Medium	39
			High	4	High	16
			Critical	2	Critical	12
Internet Facing Services	7	7	Unrated	3	Unrated	11
			Medium	2	Medium	8
			High	1	High	3
			Critical	1	Critical	2
MPLS Core	39	39	Unrated	1	Unrated	2
			Low	10	Low	35
			Medium	17	Medium	59
			High	10	High	33
			Critical	1	Critical	4
Mobile Core	38	38	Low	10	Low	54
			Medium	17	Medium	144
			High	11	High	109
Mobile Subscribers	13	13	Unrated	1	Unrated	2
			Medium	6	Medium	9
			High	5	High	13
			Critical	1	Critical	4
OSS/BSS	75	75	Unrated	20	Unrated	388
			Low	10	Low	214
			Medium	29	Medium	642
			High	15	High	309
			Critical	1	Critical	63
Radio Access Network	16	16	Unrated	1	Unrated	6
			Low	1	Low	7
			Medium	3	Medium	14
			High	10	High	86
			Critical	1	Critical	4
SD-WAN Overlay	19	19	Low	2	Low	15
			Medium	10	Medium	50
			High	6	High	20
			Critical	1	Critical	4
Threat Groups	26	19	High	26	High	26
		7				
Tooling	56	34	Low	1	Low	1
		22	Medium	20	Medium	20
			High	32	High	32
			Critical	3	Critical	3
VoIP Subscribers	14	14	Medium	7	Medium	18
			High	5	High	14
			Critical	2	Critical	5

OSS/BSS

Example attack path for OSS/BSS



3rd Party And/Or Internal Threat And Vulnerability Data May Be Leveraged For Further Access

Valid Accounts May Be Misused

Software Deployment Tools May Distribute Malware Or Facilitate Lateral Movement

Service And Other Local Accounts May Be Repurposed

DNS Requests May Be Spoofed For Command And Control

Elevation Of Privileges May Be Possible By Exploiting System Vulnerabilities

Network Information May Disclose Adjacent Networks

Sensitive Information From Databases May Be Stolen

Data Exfiltration May Be Automated

Important Data May Be Manipulated

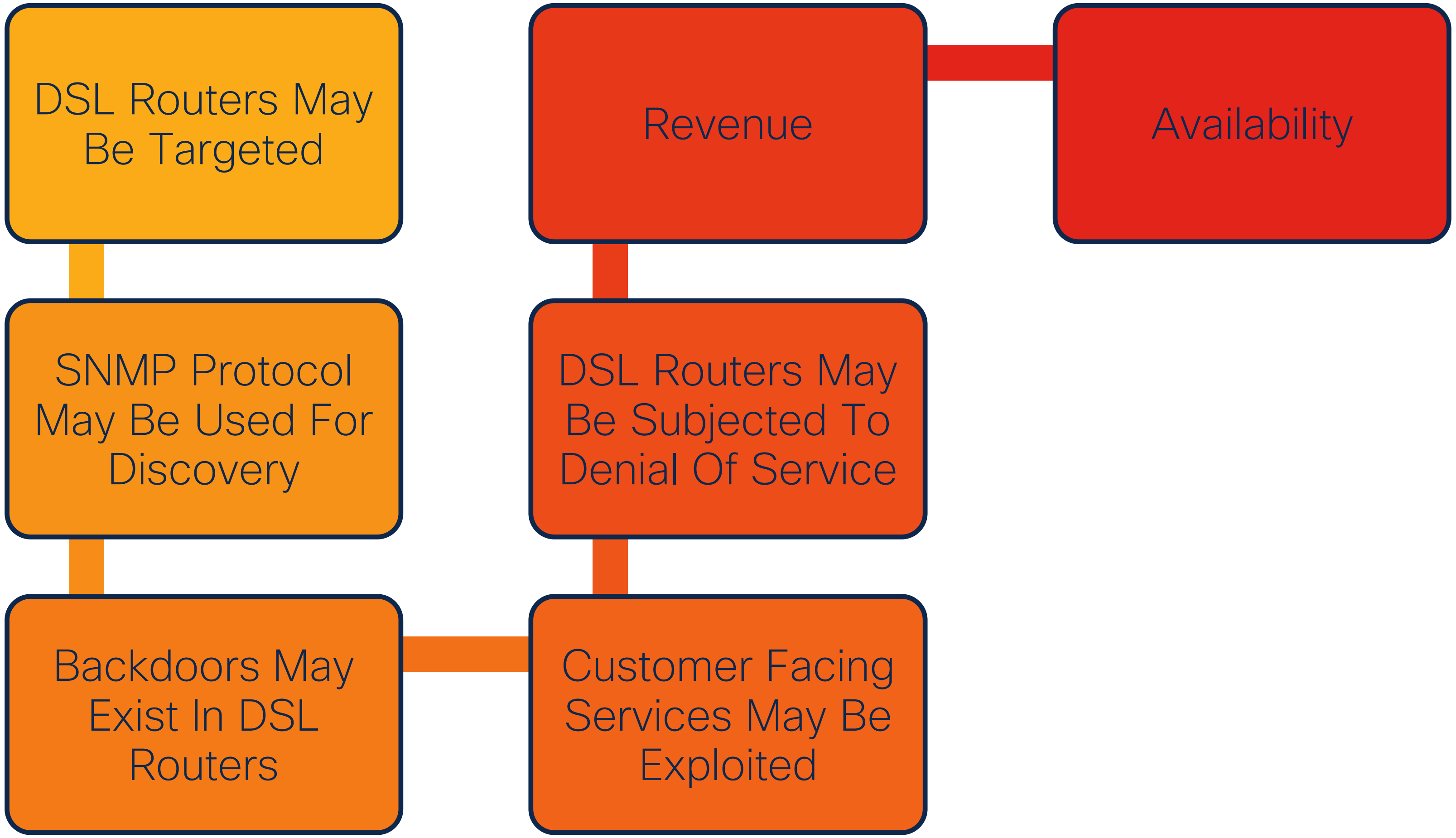
Revenue

Privacy

Integrity

Subscribers

Example attack path for fixed line subscribers



DSL Routers May Be Targeted

SNMP Protocol May Be Used For Discovery

Backdoors May Exist In DSL Routers

Customer Facing Services May Be Exploited

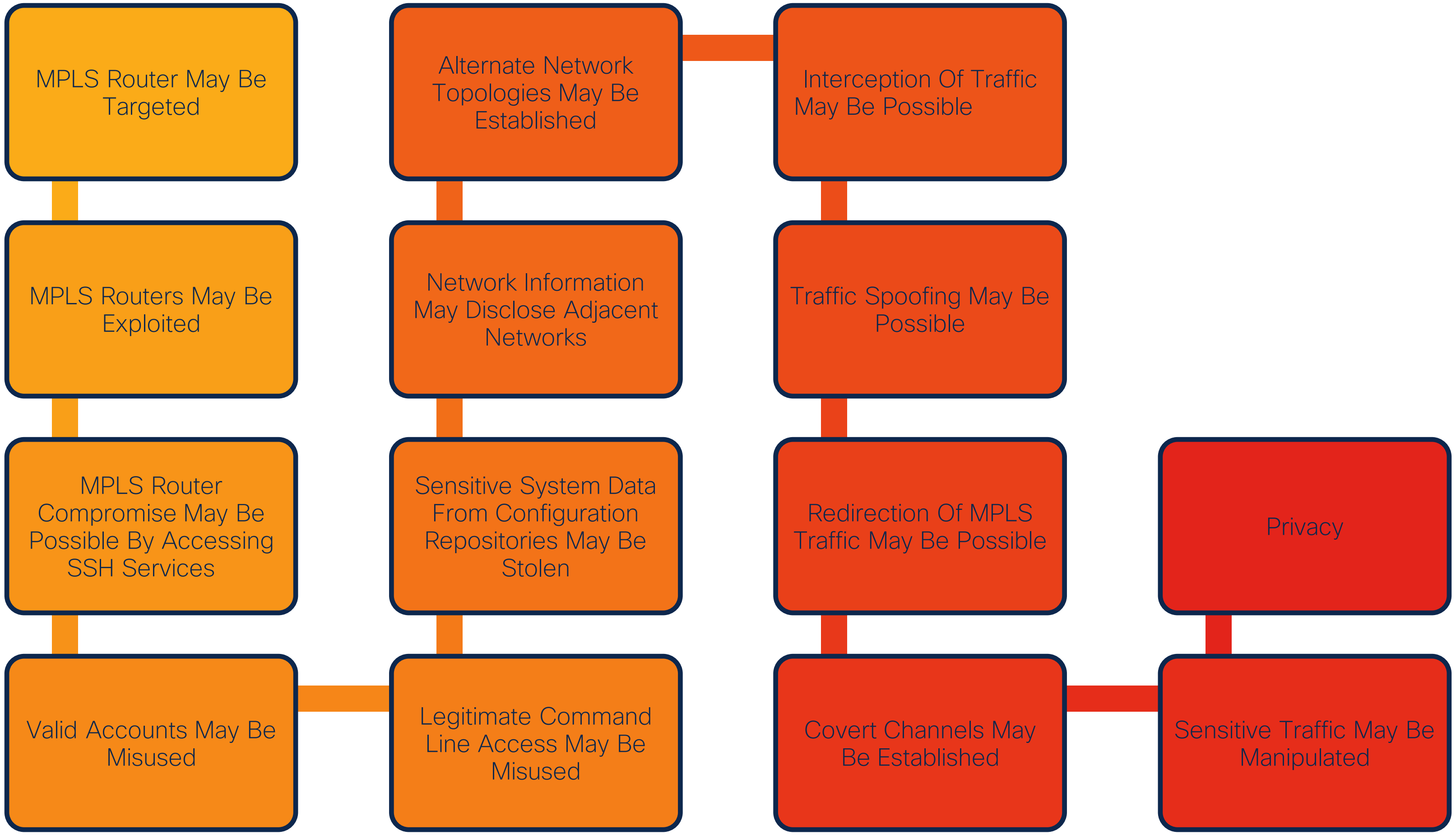
DSL Routers May Be Subjected To Denial Of Service

Revenue

Availability

Routing and switching

Example attack path for MPLS Core



MPLS Router May Be Targeted

MPLS Routers May Be Exploited

MPLS Router Compromise May Be Possible By Accessing SSH Services

Valid Accounts May Be Misused

Legitimate Command Line Access May Be Misused

Sensitive System Data From Configuration Repositories May Be Stolen

Network Information May Disclose Adjacent Networks

Alternate Network Topologies May Be Established

Interception Of Traffic May Be Possible

Traffic Spoofing May Be Possible

Redirection Of MPLS Traffic May Be Possible

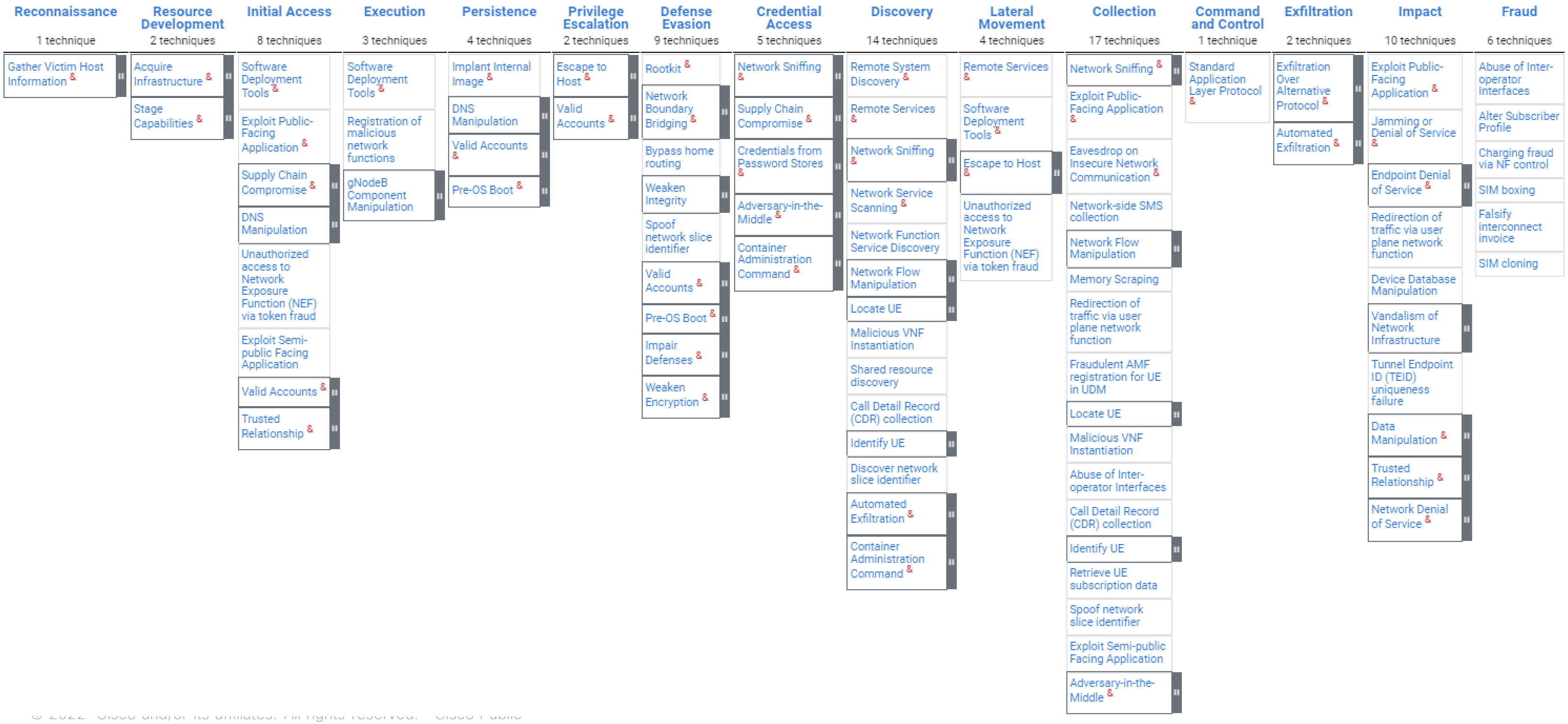
Covert Channels May Be Established

Sensitive Traffic May Be Manipulated

Privacy

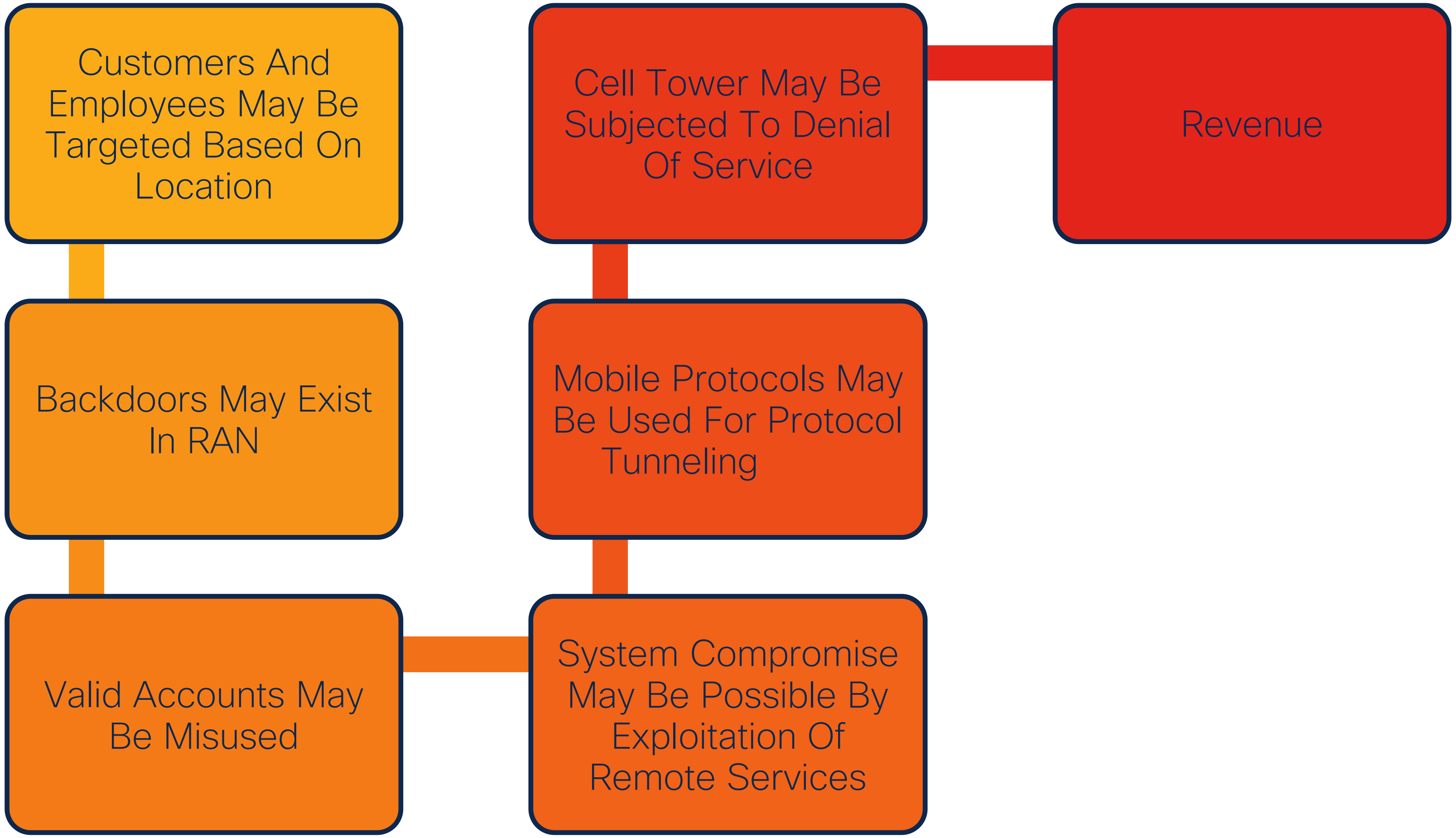
Mobile networks

Introducing MITRE’s FIGHT matrix



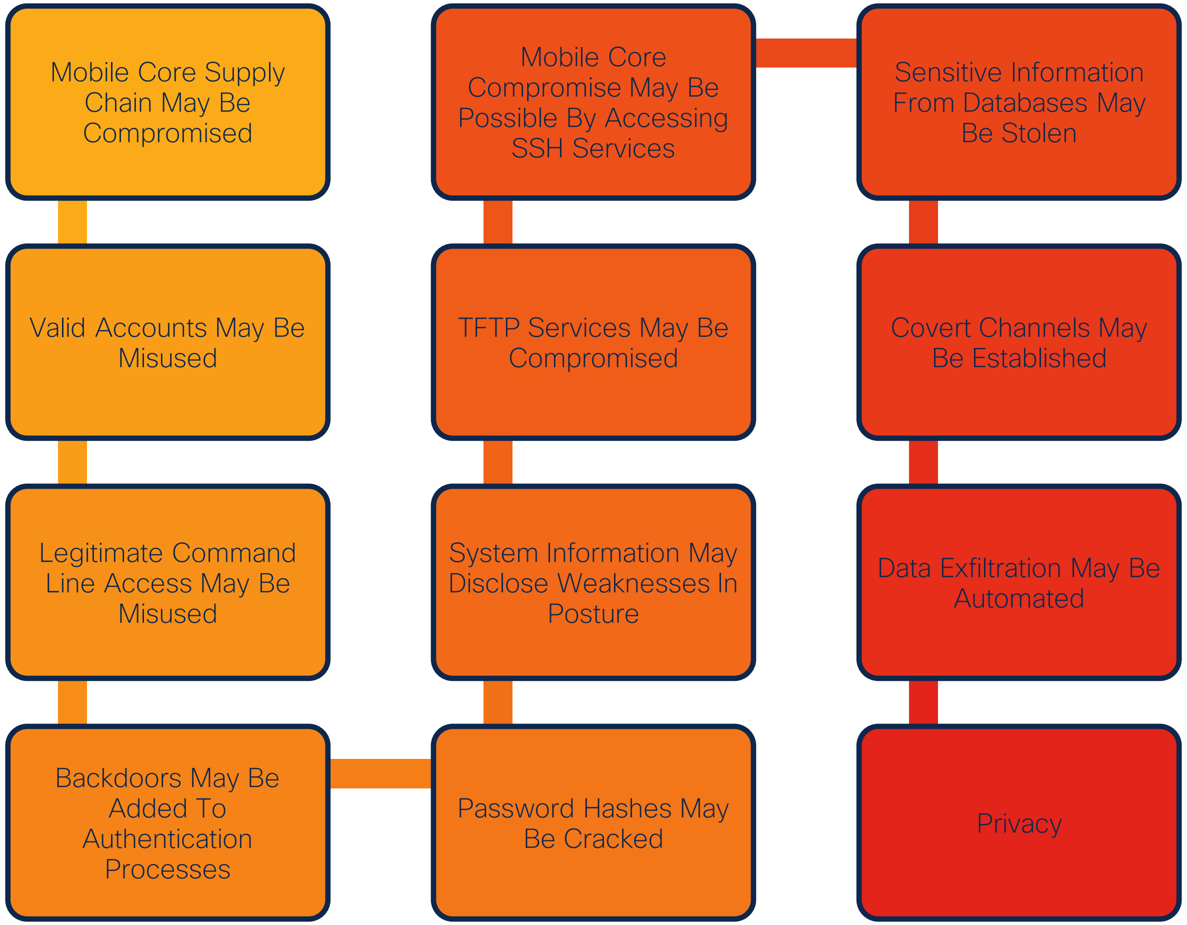
Reconnaissance 1 technique	Resource Development 2 techniques	Initial Access 8 techniques	Execution 3 techniques	Persistence 4 techniques	Privilege Escalation 2 techniques	Defense Evasion 9 techniques	Credential Access 5 techniques	Discovery 14 techniques	Lateral Movement 4 techniques	Collection 17 techniques	Command and Control 1 technique	Exfiltration 2 techniques	Impact 10 techniques	Fraud 6 techniques
Gather Victim Host Information &	Acquire Infrastructure &	Software Deployment Tools &	Software Deployment Tools &	Implant Internal Image &	Escape to Host &	Rootkit &	Network Sniffing &	Remote System Discovery &	Remote Services &	Network Sniffing &	Standard Application Layer Protocol &	Exfiltration Over Alternative Protocol &	Exploit Public-Facing Application &	Abuse of Inter-operator Interfaces
	Stage Capabilities &	Exploit Public-Facing Application &	Registration of malicious network functions	DNS Manipulation	Valid Accounts &	Network Boundary Bridging &	Supply Chain Compromise &	Remote Services &	Software Deployment Tools &	Exploit Public-Facing Application &		Automated Exfiltration &	Jamming or Denial of Service &	Alter Subscriber Profile
		Supply Chain Compromise &	gNodeB Component Manipulation	Valid Accounts &		Bypass home routing	Credentials from Password Stores &	Network Sniffing &	Escape to Host &	Eavesdrop on Insecure Network Communication &			Endpoint Denial of Service &	Charging fraud via NF control
		DNS Manipulation		Pre-OS Boot &		Weaken Integrity	Adversary-in-the-Middle &	Network Service Scanning &	Unauthorized access to Network Exposure Function (NEF) via token fraud	Network-side SMS collection			Redirection of traffic via user plane network function	SIM boxing
		Unauthorized access to Network Exposure Function (NEF) via token fraud				Spoof network slice identifier	Container Administration Command &	Network Function Service Discovery		Network Flow Manipulation			Device Database Manipulation	Falsify interconnect invoice
		Exploit Semi-public Facing Application				Valid Accounts &		Network Flow Manipulation		Memory Scraping			Vandalism of Network Infrastructure	SIM cloning
		Valid Accounts &				Pre-OS Boot &		Locate UE		Redirection of traffic via user plane network function			Tunnel Endpoint ID (TEID) uniqueness failure	
		Trusted Relationship &				Impair Defenses &		Malicious VNF Instantiation		Fraudulent AMF registration for UE in UDM			Data Manipulation &	
						Weaken Encryption &		Shared resource discovery		Locate UE			Trusted Relationship &	
								Call Detail Record (CDR) collection		Malicious VNF Instantiation			Network Denial of Service &	
								Identify UE		Abuse of Inter-operator Interfaces				
								Discover network slice identifier		Call Detail Record (CDR) collection				
								Automated Exfiltration &		Identify UE				
								Container Administration Command &		Retrieve UE subscription data				
										Spoof network slice identifier				
										Exploit Semi-public Facing Application				
										Adversary-in-the-Middle &				

Example attack path for Radio Access Network



Customers And Employees May Be Targeted Based On Location
Backdoors May Exist In RAN
Valid Accounts May Be Misused
System Compromise May Be Possible By Exploitation Of Remote Services
Mobile Protocols May Be Used For Protocol Tunneling
Cell Tower May Be Subjected To Denial Of Service
Revenue

Example attack path for Mobile Core



Mobile Core Supply Chain May Be Compromised

Valid Accounts May Be Misused

Legitimate Command Line Access May Be Misused

Backdoors May Be Added To Authentication Processes

Password Hashes May Be Cracked

System Information May Disclose Weaknesses In Posture

TFTP Services May Be Compromised

Mobile Core Compromise May Be Possible By Accessing SSH Services

Sensitive Information From Databases May Be Stolen

Covert Channels May Be Established

Data Exfiltration May Be Automated

Privacy

Let’s go hunting

Starting point

- Align to a Use Case Framework
  - Leverage understanding of real world threats that could affect you
  - Identify useful data sets from SIEM
  - Define questions we'd like to be able to answer
  - Provide use cases to data engineers as VAL

Example hunts on OSS/BSS

- AAA
  - Authentication failures
  - Malformed authentication
  - Use of local + console access
  - Use of default credentials
  - Use of shared accounts
  - Use of privileged access

- AAA
  - Use of unauthorized commands
  - Use of privileged commands
  - Use of FTP and TFTP
  - Credential modification
  - Weak credentials

Example hunts on MPLS Core

- MPLS + BGP
  - Control plane
    - Failed SSH authentication attempts
    - Failed SNMP authentication attempts
    - Weak credentials
    - Credential modification
    - Use of unauthorized commands
    - Use of (anonymous) FTP and TFTP
    - Config file transfer

- MPLS + BGP + control plane
  - Operationally
    - Failed BGP authentication attempts
    - Failed LDP, PCEP etc authentication attempts
    - Interface changes
    - System state changes

Example hunts on Mobile Core

- SS7 + Diameter + GTP
  - Location
    - Source operator
    - Destination operator
  - Protocol
    - Operation anomalies
    - Sensitive operations
      - IMSI enumeration
      - Subscriber profile enumeration
      - Subscriber location enumeration

- SS7 + Diameter + GTP
  - Protocol
    - Sensitive operations (cont’d)
      - Profile enumeration
      - Operator leakage
      - Traffic interception
      - Fraudulent billing
      - SMS interception + modification
      - Denial of Service
    - Malformed packets

How many events are too many for an analyst? ☺

- Consider the number of IPs operated
  - IPv4
  - IPv6
  - Millions of firewall events each day
- Consider the number of subscribers, phone calls and text messages
  - Hundreds of millions of events each week

Insert ML here ->

and here ->

How can we scale detection?

- ML based detection
  - For example
    - Events that are suspicious
      - Clustered by operations and properties aligned to threats
      - Statistical analysis of
        - Rare clusters
        - Increased cluster rates
        - Decreased cluster rates

Refining Use Cases

- Define use case
  - Provide questions
- Analyse data
  - Identify index and sourcetype
- Analyse data sets
  - Define queries
  - SIEM data model
  - Identify correlation points and pivots
- Iterate

Example threat description for mobile usage

- This UC is all about user equipment interacting with the network and the impact as seen on the control plane
- Operators should typically know the identity of handsets
- Visitors should only be interacting via the relevant gateways e.g. locally vs via international gateways etc
- The protocol implementations should largely be a known quantity and operators should typically not be expect anomalous operations from them
- The aim with this use case is therefore is to identify anomalous usage patterns, which do not fit into expected clusters
- This will primarily focus on protocol operations and network locations, rather than the specifics of individual pieces of user equipment

Example questions

- Has there been an increase in activity?
  - We would expect this to be seasonal, but a dramatic change on one particular day is worth investigating
- What is the baseline range of users and locations?
  - Have they changed?
  - Are they feasible?
- What is the baseline range of operations?
  - We mapped all the likely malicious operations into their offensive use cases
  - Have they changed?
  - Are they feasible?
  - Are any malicious?
- What is the baseline range of visiting handsets?
  - Have they changed?
  - Are they feasible?
- What happens when you put all of these different features together?

Key Fields

- IP Header Source Address
- IP Header Destination Address
- Gateway Hostname

- Protocol Operation
- Protocol Errors
- Source Operator
- Destination Operator

Every Use Case benefits from analytics, however…

- Fundamental challenges
  - SOCs often envisage communication of requirements as discrete logic
    - This doesn't really work for ML
  - Lack of familiarity with processes can hamper integration
    - This is a growing pain when deploying new capability
- Splunk performance
  - Source event generation volume too great
  - Source event generation frequency too great
- Data engineering
  - Insufficient data quality
  - Inability to effectively reliably correlate telemetry to security events
  - Lack of public human labelled data sets

Reasoning

- Feasibility can’t really be evaluated until data is onboarded into the data lake
  - Samples of log sources are no substitute for real live data
- Once the data has been onboarded, there is always the opportunity for custom statistical analysis
  - Primary aim of moving beyond SIEM should be to identify where ML can help

Conclusions

Improving the ecosystem

- https://github.com/SigmaHQ/sigma/tree/master/rules/network
  - Cisco
    - AAA
    - BGP
    - LDP
  - Huawei
    - BGP
  - Juniper
    - BGP
- https://blogs.cisco.com/security/new-forensic-investigation-procedures-for-first-responder-guides
- https://sec.cloudapps.cisco.com/security/center/tacticalresources.x

Final thoughts…

- Enterprise vs telco
- Operational interlock
- Analytics
  - Need to avoid selecting data from bulky data sources
  - Need to consider ML from the very start of the use case process
    - Align use cases to anomaly, forecasting and classification earlier
    - Where possible, identify open source labelled datasets from the outside
    - For non-ML experts…
      - Consider the questions you would like the model to be able to answer
- Testing

Questions?

twadhwab@cisco.com

Cisco
Customer Experience