Cybersecurity and its Effects on Telcos

JAVED SAMUEL
CYBER-SECURITY CONSULTANT
Cybersecurity Agenda

• Who are My Attackers?
• Telecos’ Cybersecurity Threats
• Telecos’ Customers Cybersecurity Threats
• Recommendations – What Can I Do?
• Conclusions
• Questions and Answers
Who Are My Attackers?

- Nation States
- Organized Crime
- Criminals
- Hackivists
- Insiders
Telecos’ Cybersecurity Threats

• Distributed Denial of Service (DDoS)
• Unaddressed Vulnerabilities in Software Applications and Network Devices
• Service Misconfigurations
• Malicious Insiders
Distributed Denial of Service (DDoS)

- Reduce network capacity
- Degrade performance
- Increase traffic exchange costs
- Disrupt service availability
- Use of vulnerable IoT devices in botnets to launch DDoS attacks.
- Cover for a deeper, more damaging secondary attack
Unaddressed Vulnerabilities in Software Applications and Network Devices

- **Application Vulnerabilities**
  - Injection Attacks
  - Authentication Bypasses
  - Cross Site Scripting

- **Network Device Vulnerabilities**
  - SYNful knock
  - Enable third-party access to network traffic
  - Access to sensitive data

![Image showing a webpage with a login prompt and two different authentication outcomes.](image)
Service Misconfigurations

• Publicly exposed GTP/GRX ports on devices
• BGP attacks where acceptance and propagation of routing information from other peers allows MITM attacks or denial of service.
Malicious Insiders

- Cheaper and easier to comprise a network with the help of a hired or blackmailed insider.
- Cybercriminals recruit insiders through two approaches
  - Entice or coerce individual employees with relevant skills
  - Trawl around underground message boards looking for an appropriate employee or former employee.
Telecos’ Customers Cybersecurity Threats

• Social engineering, Phishing Etc
• Vulnerable Kit
• Local Cells and SIM Attacks
Social Engineering, Phishing of Telecos’ Customers

- Target unaware or poorly aware subscribers and telecoms employees.
- Lack of user awareness and egress protections.
- Poor password handling and storage discipline.
- Use of Ransomware
- Lack of two-factor authentication
- Lack of user permission segregation.
Vulnerable Kits Provided to Telecos’ Customers

- Insufficient authentication
- Remote Code Execution from web scripts.
- Arbitrary device firmware modification due to insufficient consistency checks
Local Cells and SIM Attacks

- Attacker can gain complete control over devices that signal coverage inside buildings.
  - Can lead to call interception, service abuse or internal network access.
- Clone SIM cards
  - Use differential power analysis for the encryption key and extracting secrets.
  - This was thought to be impossible
Recommendations – Secure Your Network

• Use Multi-Factor Authentication
• Use Strong Passwords
• Segment Your Network
• Audit Administrator Access
• Secure All Keys and Secrets
• Harden All Devices
Recommendations – Secure Your Applications

• Use recommended authentication mechanisms
• Do not trust user input and implement robust server side checks
• Ensure that applications continue to verify their assurance of a user’s identity following authentication
• Using safe coding practices such as
  • Parameterized queries for database access
  • Use managed code for safe string handling
  • Pass an index to a list of files as a parameter, instead of an actual filename
Recommendations – Detect and Respond to Threats

• Implement threat detection and prevention tools
• Create and maintain an approved incident response plan
• Deploy reactive mechanisms to mitigate attacker’s progress
• Implement sufficient logging and auditing
Conclusions

• Security must be a core component of your entire enterprise
• Use both technical and non-technical solutions
• No quick-fix solutions will be completely effective
• Understand the changing threat landscape and react quickly
Questions and Answers

CONTACT INFO: JAVED.SAMUEL@GMAIL.COM