ORACLE®
COMMUNICATIONS

An Oracle White Paper
February 2017

The State of Telecommunications Security

ORACLE®

The State of Telecommunications Security Today

We use our devices for everything—working, shopping, banking, healthcare, and more. Our digital lifestyle generates large volumes of metadata that crosses mobile networks – metadata that is valued by those lurking in the darkest corners of the web. According to Cisco's Visual Networking Index, global mobile data will grow at a compounded annual growth rate of 53% between 2015 and 2020. As the emerging trends of wearable tech and the Internet of Things (IoT) take off with consumers and enterprises, the volume of this data is set to explode. Low cost microcontrollers and 2G chipsets for network access in IoT devices will allow these technologies to become ubiquitous.

All the data being generated through successive waves of innovation is flowing over a global telecommunications network that was designed in a different era. This network of networks, once run by a small club of telecommunications companies on the basis of shared interests among peers, is now open to virtually anyone. Interconnection – the linking of two or more networks for the mutual exchange of traffic – used to require a hard-wired circuit terminating at a physical address. With the widespread adoption of Internet Protocol (IP)-based interconnection, now virtually anyone can purchase or gain access.

Today, malicious actors take advantage of the assumption that any company seeking to interconnect and gain access to networks can be trusted. Service providers have also become targets themselves, with network breaches almost doubling. Meanwhile the hacker community has been busy publishing new research on wireless vulnerabilities, and productizing hacking tools for sale on the Dark Web.

Despite these concerns, security remains an afterthought throughout the telecommunications industry. Many executives struggle with justifying the cost of implementing security in the network, without sufficient evidence that can be used to build a business case. If their network has not been compromised, they would rather spend that capital on new technology. They are not convinced that they have a problem, and many believe that this problem will go away as the industry moves to 5G and virtualized networks.

The reality is starker. The exploits being publicized by media and talked about at hacker conferences are not going to go away. These exploits demonstrate a much deeper problem in our world's telecommunications networks. The network doors have been left open and unlocked, and anyone can purchase access to the command and control of any network in the world.

Interconnect Abuse is Rampant

Researchers have uncovered both evidence of criminal abuse of telecom networks as well as tool kits that are being sold on the dark web to exploit these networks. German computer scientist Karsten Nohl showed *60 Minutes* last spring how he could remotely spy on a mobile phone used by U.S. Representative Ted Lieu. Using only Lieu's cellphone number, Nohl was able to listen to Representative Lieu's calls, determine his location, and obtain a list of numbers that he had called. The attack took advantage of a largely open global mobile network know as Signaling System No. 7 or SS7, which is used to connect carriers to facilitate global roaming, texting, and other communications. While SS7 has received much of the attention, other protocols including Diameter are also vulnerable to similar attacks.

We are at a critical juncture as the hacker community begins productizing their hacking tools. The security industry has watched this trend unfold in the world of IT. Exploits begin with scripts, followed by toolkits, and finally products and services centered on these exploits. Once this process is fully underway, anyone with bitcoin and an Internet connection can use these products and services. The telecommunications industry, new to cyber security, still does not realize the threat it faces.

While an earlier generation of hackers stole services or used the network to carryout denial of service attacks, this generation has figured out that masquerading as a peer and accessing telecommunications interconnects directly provides an elegant vector for criminal activity. Malicious actors are abusing interconnect privileges to locate individuals, intercept messaging, and eavesdrop on calls. Many actors with differing motivations from disruption, terrorism, espionage, or theft now have the capability to abuse the trust model that currently governs the telecommunications industry.

A Security Model Built for a Bygone Era

Before the adoption of IP-based interconnections, Telecommunication Service Providers were a small club of known entities with significant barriers to entry as a trusted peer on the network. Securing the network against threats was simpler, and often problems could be fixed with a phone call to a friendly engineer at another phone company. Now, telecommunications companies are expanding their business and offering new ways for content providers and other service providers to directly interconnect with their network and provide services to subscribers. But with a growing number of connections, the challenge for a telecommunications company is how to manage network access and the permissions that go with that access. For decades interconnect partners were allowed to connect directly into a telecommunication service providers network because they were known, and trusted. Now, interconnect partners can be anyone.

Compounding the problem, the industry has moved away from fixed circuitry that required a physical address to connect. Today, the industry has moved to an all-IP infrastructure, allowing much easier access from anywhere in the world. The barrier of access has been lowered by not having a physical separation, using common protocols, and a growing percentage of the population fluent in software programming. An IP connection is all that is needed in today's interconnect environment, rather than a fixed circuit connecting point A to point B. Providers that believe they are limiting access by vetting their interconnect partners have a false sense of security; they are still connected to other networks, and they have no visibility into the security measures of downstream partners.

Many companies do not use direct connections into their networks, choosing instead to use an aggregator, or hub provider. These aggregators provide a single interconnection point for the service provider, eliminating the need for them to negotiate hundreds of interconnect agreements. However, this also opens up another attack vector, where rogue networks can masquerade as legitimate service providers connecting through these very aggregators. This means aggregators themselves must reexamine their networks to ensure they are providing protection for their down stream customers, a challenge requiring detailed knowledge of each customer's business to be effective.

Despite this move from a largely fixed set of trusted partners to a world where interconnects are rife with a fluid mix of untrusted partners, the legal and technical arrangements remain the same. Contracts for interconnect often do not limit what a partner is allowed to access within the network or limit whether they can provide access to their network partners. This has created an untrusted chain of access. Network gateways where access control is implemented have little to no policies enforced at the interconnect, allowing everyone who connects full rights to the network. Technical controls for monitoring are almost non-existent. Criminal hackers know this all too well.

Adapting Best Practices to Telecom Security

Telecommunications service providers must move beyond the trust model that has governed network access for so long. As telecommunications networks move to an "All-IP" infrastructure model, adopting best practices for securing information technology networks can address many of the security risks observed on the networks today. Telecommunications companies have not implemented security controls in the network like they have in the data center. Most telecommunications service providers have not instrumented their network to monitor for violations of policy by interconnect partners. Access control has not been implemented and encryption is not being used at the interconnect. The industry does not differentiate between interconnect partners, giving full access to all partners under a one-size fits all model.

Adopting best practices from IT networks will be no easy task. Only a handful of people globally have experience maintaining core infrastructure – with its attendant uptime and reliability requirements – and expertise in the tools and techniques used in IT systems security. As the state of the art moves to Network Functions Virtualization (NFV) and Software Defined Network (SDN), security will be even more challenging. To address these challenges, telecommunication service providers should build a security plan around existing standards for IT security. They should then focus their efforts on increasing knowledge of who their interconnect partners are and what network privileges they are allowed. Once this understanding is gained, it should be followed by identifying the technical and business risks associated with interconnect partners. With a clear understanding of privilege and risk, telecommunication service providers can begin to implement security controls that monitor for and prevent the interconnect abuses that have become common.

Five Steps to Building an Interconnect Security Plan

Telecommunication service providers should build a security plan that begins by adopting best practices in IT security and adapts them to the specific needs and biggest risks for telecom networks. While supply chain or business partner risk is increasingly being recognized as a crucial component for IT security, in telecommunications it is fundamental. Because interconnect partners have access to your network, your network is only as secure as your least trustworthy interconnect partner. The five-point plan provided below can address risks to telecommunications networks holistically, focusing on areas that require special consideration in the context of telecommunications:

1. **Adopt a Standard and Stick to It.** The International Standards Organization 2700 series and the National Institute of Standards Cybersecurity Framework divide the world between them. There are other standards with merit. Choose one, and begin the process of implementing it. You will not be able to implement everything, and it will take time, but you need to start someplace and stick with the program.
2. **Implement 'least access' privileges.** Provide access at the lowest level and to the fewest resources necessary. Implement policies that can be enforced by technical means. Only allow the level of access absolutely required and do not grant unfiltered access to anyone. Verify that only authorized entities can connect through use of digital signatures, certificates or shared secrets.

3. **Collect event logs from all systems on a regular basis.** The most common excuse heard is that logs are erased or written over before they can be reviewed. This means that breaches could go undetected for a long period. Use immutable audit logs to record every event and validate access against agreements. Store logs for a minimum of one year.
4. **Monitor all activity on critical systems.** If you do not have visibility to all the traffic coming into your network, you have no idea what is happening. Also, do not forget to monitor your internal assets. Many times, misuse is from insider threats misusing the network themselves or sharing passwords to critical systems to grant outside sources access to the network.
5. **Know your customer (and know their customers).** Beyond technical controls, the most important thing telecommunications companies can do to protect the integrity of their networks is to practice due diligence on their interconnect partners and to pass down requirements to their interconnect partners.

Time for action

We should no longer be guessing about network abuse. There is sufficient evidence now that networks are being accessed and abused for nefarious activities. Service providers should be implementing multi-layered security program to prevent ongoing theft of subscriber data, and exposure of sensitive personal information. The industry can no longer "patch" the issue by implementing limited protection to solve the immediate exposure and not addressing the larger problem of network access.

Service providers should be moving aggressively towards monitoring and analytics as they do in their IT networks, equaling these investments and tailoring them for telecommunications networks. It is time for the telecommunications industry to take action and protect its networks, subscribers, and the very corporations and organizations that depend on reliable and secure communications. The time for action is now.

The State of Telecommunications Security
October 2016
Author: Travis Russell

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com

Oracle is committed to developing practices and products that help protect the environment

Hardware and Software, Engineered to Work Together