Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 13, Issue 8

Securing the Modern Cellco

By: Mark Cummings

As the modern Cellco becomes more and more critical to society, new threats and vulnerabilities are creating new challenges. With the advent of nation state cyber attacks, Cellcos have become targets. At the same time, mobile networks are evolving from hardware-based components to more software-based components. Taken together, these two require strengthening internal security in two ways: changes in policies and procedures, and the extension of end-to-end orchestration to automated detection and response to intrusions and infections.

Changing threat environment

As wireless becomes the default last kilometer, IoT explodes, and autonomous vehicles arrive; the Cellco becomes increasingly critical to society. It used to be that the only significant threat to Cellco networks was from disgruntled employees or difficult labor actions. For example, a fiber-cutting incident in Silicon Valley that took out cellular service, many of the web services, and disrupted phone service for a day occurred when there was a labor action in the area prompting speculation that the two were related.

Now, the threat profile has expanded to include nation states. "*Zero Days*," was an HBO documentary on events surrounding the cyber attacks on the Iranian nuclear centrifuges. It stated that Iran, as a warning of potential reprisals to continued cyber attacks, launched a cyber attack on an Israeli Cellco. With apparently authoritative claims of Chinese and Russian cyber attacks and apprehensions about rogue states and terrorist organizations, there is growing concern for the vulnerability of infrastructure in general and Cellcos in particular. The Cellco is not only a key infrastructure element by itself, but it plays a critical role in the viability of most other critical infrastructures including water, transportation, oil and gas, electrical grid, emergency services - just to name a few. Because of this central role, the Cellco has become an increasingly attractive target.

Evolving vulnerabilities

Looking back in time, the Cellco was composed primarily of hardware components, now called by some PNFs (Physical Network Functions). Today Cellcos are moving to software-based

components. 2G base stations have 50 software settable parameters. 3G have 500. 4G have 6,000. And 5G is on the horizon. SDR (Software Defined Radio) is moving high-speed signal processing out of hardwired ASICs (Application Specific Integrated Circuits) into software. SDN (Software DefinedNetworking) is replacing hardware-based switches and routers with software running on industry standard general purpose computing platforms. NFV (Network Function Virtualization) is replacing hardware-based appliances in the ePC (Evolved Packet Core – the central site computing center that supports mobile network operations) such as the MME (Mobility Management Entity), Home Location Register (HLR), etcetera - all with software running on industry standard general purpose computing platforms. At the same time, value added services are moving to cloud implementations.

This transition to software-based network components creates new vulnerabilities. Disgruntled employees can insert rogue code. But failing to update policies and procedures creates another new vulnerability. An example of this can be seen in the recent attack on Deutsche Telekom.

At Deutsche Telekom it appears that when SDN switches and routers were deployed, the unused ports (~300) were left open and active, and that the attacker used these open and active ports as an entry point for a software attack on the network. It appears that what happened is as follows: Hardware-based switches and routers didn't have open ports, so the policies and procedures for deploying and provisioning them did not include shutting down open ports. When SDN components arrived for deployment, operations was told that they would function exactly the same as the older hardware-based components. At the data and operations levels they did. However, they had an industry standard general-purpose computing platform underneath. That platform defaulted to all ports being open. Since operations was under the impression that the SDN components would work just like the hardware components they were replacing, they used the existing policies and procedures. Those policies and procedures didn't call for closing unused ports, so they were left in default open configuration. It may also be the case that vendor documentation was not updated.

The take-away is that, as Cellcos move from hardware to software components, policies and procedures must be revised to minimize vulnerabilities in both the software functionality and the underlying platforms.

Policies and procedures updates are necessary but not sufficient

It is not wise to rely entirely on firewalls, virus checkers, and policies and procedures alone. Today, these represent a "semi-permeable membrane" akin to that of our skin. Just as our skin keeps out most invasive things, it can't keep them all out - just as humans need air and food, a Cellco needs customers and employees to survive. Thus, our bodies have a way of detecting and either quarantining or removing harmful invasive things. Cellco networks need similar capabilities. All too often, intrusions and infections are only discovered after a large segment of the network has been affected. Only then, are manual efforts initiated. The resulting damage can be severe.

The Deutsche Telekom example cited above is a case in point. Deutsche Telekom should not be criticized, but rather commended. Far too often, successful attacks are kept secret. This is done out of fear that releasing the information will damage the company or damage the reputation of individuals involved in identifying and recovering from the attack. The Cyber Security industry has long advocated for release of attack information so that we, as an industry, can learn about the attack vectors and better work together to protect ourselves. Unfortunately, this is a fight against human nature. Some have argued that there needs to be government laws and regulations forcing disclosure while providing anonymization. But here again, this has proven politically difficult. Some years ago, it was estimated that only approximately 10% of the illegal drugs smuggled into the U.S. were caught. So, a way to estimate the quantity of drugs is to multiply the amount seized by 10 fold. There may be a similar situation visa vie Cellco cyber attacks. We can reasonably assume that there are far more attacks than publicly reported.

Generally, attacks on Cellco networks start with penetration of a single network component and

then use that component to attack other components in the network. It is only after a critical mass of components have been compromised that severe damage to the network results. Because of the scale, complexity, and volatility of Cellco networks, what is needed is a very fast means of quickly identifying an intrusion or infection and preventing it from propagating or moving through the network. Trying manually to detect and respond fast enough to prevent damage has proven difficult. An automated system is needed, one that can identify attacks quickly and prevent them from spreading.

A network immune system

Ideally, a network system should respond like the human immune system acts when our outer defenses are breached. Companies are now offering security probes that can detect “infections”. To be effective in catching malignancies before they can spread, there has to be an array of these probes distributed at the edges of the network where attacks are most likely to start. Today, these probes can be so distributed, but they report their results back to a central manual operations center. In large, complex, volatile Cellco networks, these manual responses can’t be fast enough to prevent significant damage. What is needed is a way to automate and respond quickly where the attack is originating. This would be acting in a way similar to how our lymphatic system protects against breaches of our outer defenses.

Recently, there has been a significant amount of industry activity focused on end-to-end automated network orchestration (see “Collaboration Effort, Making Progress” *Pipeline*, January 2017). End-to-end network orchestration products are available or being developed by vendors, operators, and open source groups. Some are central site architected, but some have a combination of central and distributed capabilities. These central and distributed systems are akin to our nervous system complete with ganglions. Some of these orchestration systems seek to replace the entire existing Cellco operations environment and others are an overlay on existing operations.

The initial motivation to develop these overlay end-to-end orchestration systems was to reduce operations expenses that are increasing in a non-linear fashion. Over time, they were seen as also a means for quickly and efficiently delivering services both conventional and innovative. This became known as a composable services capability.

These overlay end-to-end orchestration systems can also be the means to automate the response to attack information from the security probes. Today, the security probes can quickly identify a breached component. The response is to remove that component from the network. A well-crafted, end-to-end orchestration system can connect to the security probes, accept alerts, and automate the response to infection detections. In this way, such a system becomes the immune system of the network.

We have seen how the increase in threats to and vulnerabilities of the Cellco are necessitating both new policies and procedures, and the automated network immune system described above. The network immune system is within reach and can be provided by connecting existing security probes to some of the end-to-end orchestration systems available now and those being developed.