The IoT Security Opportunity

By: Mark Cummings, Ph.D., Bill Yeack

Today's profusion of IoT devices opens an entire realm of new security problems for both the user and providers. Telecommunications providers are uniquely positioned to address these critical issues. Doing so requires the deployment of an automated dynamic security orchestration service—and represents a new, highly profitable revenue source that will deliver CSP benefits to investors, customers, regulators, and employees.

Today, many telcos have profitable MSSP (Managed Security Service Provider) offerings for their large enterprise and government customers. Recently, there has been a wave of IoT devices and systems sold to consumer and SOHO (Small Office Home Office) markets. Given the blitzkrieg of cyberattacks by organized crime, nation state pirates, and neighborhood petty criminals, these devices and systems cry out for dynamic security orchestration services. Communications Service Providers (CSPs) are uniquely positioned to provide these services—and have a responsibility to do so. This is because only CSPs have both the reach and the visibility to provide these services.

Yet challenges abound. Current MSSP services are highly manual, akin to the plugboard switching of early telcos. To effectively protect the consumer and SOHO markets, dynamic orchestration must be automated, meaning a move to automated switching. With such an automated dynamic orchestration platform, this service has the potential to become a large and highly profitable new revenue source.

A look at the origins

Taking a step back yields a broader perspective. The consumer and SOHO digital markets grew out of the PC and the Internet. The PC, Internet, and web are still important, but three other factors have come into play and a fourth is on the horizon. First, the PC is no longer directly connected to the Internet. It is now linked to Wi-Fi and other wireless network access points. Second, the overall amount of information and the percentage share of consumer and SOHO information stored and delivered digitally has mushroomed. Whether on PCs, attached storage of one type or another, or in the cloud, the overwhelming percentage of critical data as well as entertainment is stored and delivered digitally. Third, to this is added a host of IoT devices. These devices connect to the Internet via local wireless. They include smart thermostats, smart light bulbs, digital door locks, video surveillance systems, baby monitors, health monitoring systems, health intervention systems, children's toys, smart irrigation systems, other types of environmental sensors, other automated controls, and so on. Add to this array smart speakers that connect to digital assistants on the web. Finally, with the rise of 5G, the volume of traffic and data will grow dramatically, and even the best security approaches in widespread use today will become overwhelmed. And IoT is not yet using even today's best security approaches.

Digitization brings new complexity and threats to security

One group in the SOHO market has had a particularly intense increase in digitization. This is the medical niche, including doctor's offices, clinics, and hospitals. In medical environments, DoS (Denial of Service) and other forms of intentional or unintentional

disruption can have life-threatening consequences in addition to the financial impacts of data exfiltration.

This evolution from the PC to IoT has produced profound improvements in productivity, ease, and quality of life. But it has also greatly enlarged the attack surface and extent of possible damage from cyberattacks. The increase in the attack surface has not gone undetected by criminals.

It seems the mass media reports every day on some large organization getting hacked. But the situation faced by the consumer and SOHO markets often goes “under the radar.” This underreporting can lead to a false sense of security. Sometimes, though, indicators leak out. For example, several years ago, it was reported that electronic car theft was on the rise: thieves had exploited vulnerability in wireless key fobs’ interfaces, and these crimes were now exceeding the number of physical break-ins nationwide. This indicates that not only does the nation state pirate have the capability to perform cybercrime, the neighborhood crook does as well.

Now, with the profusion of IoT devices, crooks can not only steal your identity, they can break into your home or small office and steal whatever they want. The loss might include physical items as well as critical family and business records, and there can be unintended collateral damage. Irreplaceable family photos can be lost, basic functions of the physical home or office can be damaged, and more. For someone with health problems, or who is working in the medical industry, the damage can even be (or have) life-threatening repercussions.

Rules for basic security

The United States FTC has become so concerned about consumer and SOHO IoT devices being shipped without adequate initial security that it created some rules to require basic password security. Let’s look at an example. In the Netherlands, a farmer put smart-Internet-connected tags on cows. Hackers took control of the unused cycles (the overwhelming majority) to mount DDoS attacks (Distributed Denial of Service, which involve bombarding a system with so many simultaneous connects or transactions that it collapses, forcing the system owner to pay ransom). The cow tags numbered in the hundreds. When hackers started using thousands of baby monitors and children’s toys to mount DDoS attacks, the FTC was compelled to take action.

These rules are a good start, but they do not come close to solving the problem. Having the most basic security in IoT products when they are shipped is good. What is truly needed is a way to configure these products in a secure fashion in the context of the suite of products (including gateways, etc.) in a physical or virtual location. Because of software updates, new product additions, and more, “configure and forget” is simply not good enough. There must be a way to reconfigure devices and products to meet changing conditions. Even the best set-up cannot be assumed to be 100 percent effective in keeping hackers out. There must be a better way to detect successful breaches and remediate them.

Looking at CSPs and the potential

Today, CSPs are the primary way that users in the consumer and SOHO markets connect to the Internet. As such, they touch each user’s Internet portal. Furthermore, they have geographically distributed resources—very important for technical reasons discussed below. Finally, they already have a billing relationship with the users. This puts them in a unique position to launch a cost-effective service to protect, detect, and remediate cyberattacks. Finally, many of them already have experience offering security as a service (SASS, more commonly called MSSP). The challenge is that these MSSP services, being highly manual expensive offerings, don’t scale to the consumer and SOHO markets.

Moving to these markets requires a very large increase in scale, complexity, and volatility. Corporate-focused MSSP services are already:

- Drowning in behavioral data that is key to detecting attacks that get through the

outer defenses;
- Struggling with the profusion of products, layers of technology, and generations;
- Running as fast as they can to keep up with the speed of change.

Moving to these new markets will break them. Moreover, consumer and SOHO users typically do not have an IT department to do initial set-up, configuration, and reconfiguration, let alone handle remediation. What is needed is an automated technology base that CSPs can use to handle these functions effectively and efficiently.

The only effective way to provide crucial automation

That brings us to distributed dynamic orchestration, which is the only effective way to provide this automation. The easiest way to think about orchestration is as a third layer. The first layer is the data or operational layer. This is where things get done. The second layer is the management layer, where the work of managing the operation of the underlying subsystems goes on. The third—or orchestration—layer is where the other two layers are configured and observed to make sure that they are working well together. In this observation, orchestration watches for failures and acts (remediates) to fix them. These failures can be the result of naturally occurring problems or from cyberattacks.

The orchestration layer must be dynamic, because the underlying data and management layers are constantly changing (as a result of software updates, new products and technologies, and more). In addition, the nature of cyberattacks is also constantly changing. Therefore, orchestration must be able to respond effectively to things that have not, and cannot, be fully anticipated or scripted in advance.

Finally, orchestration has to be distributed because of the volume of behavioral data. Without the behavioral data, it is very hard to find the attacks that have penetrated the outer defenses. With today’s attack volume, even a small percentage that gets through the outer defenses represents a very large number. So, it is critical to identify them very quickly (in some cases, in less than 19 minutes). Trying to capture, hold, and analyze all the behavioral data in consumer and SOHO markets in central site systems is impossible. It takes too long to get the data there. And once there, it takes too long to find “the needle in the haystack.”

The only feasible way is to geographically distribute both the data and the behavioral analysis. This way, local systems only have to deal with relatively small amounts of local data. And, when necessary, the local systems can work cooperatively. Distributing also has very positive impacts on privacy, among other issues.

With automated distributed dynamic orchestration, plus the existing access to portals and distributed resources, CSPs would be able to quickly capture a new high-profit revenue stream. Pricing would most likely be tiered, starting with low-end consumer and moving up into SOHO. This would help with overall CSP profitability, which is especially important in the face of regulatory and antitrust pressure on existing product pricing. Maybe even more importantly, such an offering would position CSPs to show that they are meeting their responsibility to society. The social responsibility aspect would have a positive impact on employee morale. Thus, deploying such an automated dynamic orchestration service would deliver CSP benefits with investors, customers, regulators, and employees.