SecurityGen
Telecom Security. Transcending Generations.

Cybersecurity Perspective on the Top MWC 2023 Themes

MWC 2023 is over. With over 88,000 attendees, it was a mixed bag of displays and discussions around foldable phones, emotional robots, LTE-connected Moon Rover to the metaverse, 5G, AI and sustainability topics. The industry leaders and followers have showcased their products and services for a few days in front of bewildered or bored observers. The show witnessed several presentations and discussions on industry topics.

Let's see what is trending and review it from a cybersecurity perspective.

There Has Been a Significant Shift Towards Openness Announced - the GSMA Open Gateway Initiative

This is an attempt to generate interest and invite software developers to participate in creating new use cases for wireless communications, including 5G. The idea is to create a common API that provides universal access to operator networks to request specific capabilities, such as lower delay, higher speed, and different slices, to guarantee a better user experience. Software developers can create new and exciting applications that will have massive success among subscribers, thus helping to generate new revenues and share them with telecoms. This is a reasonable business hypothesis that is worth trying.

From a cybersecurity perspective, openness also brings some challenges. However, once these challenges are addressed and resolved, they make the technology stronger, more developed, and more trusted. The security of APIs is a well-defined area, so we do not expect dramatic cybersecurity changes in protecting networks equipped with Open Gateways. However, we will observe incidents resulting from security misconfiguration and failures following common-sense best practices like OWASP API security.

Thirty More Countries to Launch 5G Services in 2023

It has been announced that 5G connections are expected to double over the next two years, and the same is expected to happen with 5G roaming. This results from the significant growth of 5G subscribers and enterprise adoption. If the forecast is correct, there will be more than 120 countries where you can benefit from a 5G connection by the end of this year, and we will enjoy it! But what does it mean in terms of protection for subscribers and data security?

Unlike previous mobile network generations, 5G is designed from the ground up to be flexible and open for integration with multiple external systems. Thanks to security research, we know that such architecture that enables this flexibility and easy integration can also make 5G vulnerable and exposed to threats and hidden vulnerabilities, leading to different hacks like data leakage or denial of service.

The challenge for operators is guaranteeing a quick network rollout without leaving security in the back seat. Security is cheaper and more efficient if it is embedded into system design. Hopefully, no one will feel alone in this journey, with multiple industry initiatives launched to support the secure adoption of 5G networks, such as those driven by ENISA in the EU and NIST in the US.

Private Cellular Networks to Proliferate to More Industries

Since the time of LTE, it has been possible to build small-scale mobile networks for enterprise purposes. However, there were only so many reasons to do so, as the cost and complexity were way off compared to Wi-Fi, for example. Times have changed, and with new technologies and suppliers ready to make the construction, it's getting more and more convenient for a large organization to make a choice and build its own 5G network, especially when the scale is large, such as in the case of seaports, production lines, logistics centers, etc. For these purposes, it is almost perfect - coverage is excellent, signals are never lost, highly reliable, etc.

For network guys, it sounds like a dream. Is it the same for security professionals? Yes and no. Cybersecurity continues to suffer an ongoing shortage of skilled workers, especially in areas requiring specific expertise, such as telecom or industrial security - which looks exactly like this case. Private network evangelists say these networks are kind of isolated, but this argument is weak as the threat landscape is always broader than simply connectivity to the internet. In general, the usage of new wireless technology doesn't protect an enterprise better or make it more vulnerable. Cyber-resilience is achieved only through well-planned measures, and no silver bullet exists.

AI is Reshaping Telecoms

AI completely stole the show at the end of last year, and people started prophesying the end of the professions of software developers, novelists, and painters. So, what is its impact on telecoms? Here is a slightly convoluted quote, but it probably describes the expectations quite well: "It will enable all-in-one, software-defined, AI-driven, cloud-native, fully programmable, energy-efficient, future-proof, zero-emission, and glutted-free… something!"

Something is not a joke; AI has been used for Radio Site planning for years, primarily to fulfill the challenge of small cells and indoor coverage on the 5G allocated bands. AI models may, however, be improved by adding some site security prediction to the models. This means that AI has already proven to be practically implementable in many areas, and now it is a question of creativity as to how vendors, developers, and telecoms will utilize it further.

Let's narrow it down and imagine the implementation of AI in software-defined networks and applications. It can provide advanced threat detection, and even more interesting, AI can be used to automate responses to security incidents, such as shutting down a compromised system or blocking traffic from a suspicious source. But it can also increase system complexity and be vulnerable to attacks on the AI systems themselves. So the most probable forecast is that it will have both positive and negative effects on cybersecurity, just like implementing any new technology. We must focus on maximizing the positive impact while mitigating potential issues.

The Debate around Open RAN

While keeping a safe distance from the companies committed in favour (and against) the project, it was good to see what has evolved and the blocking points that remain to be cleared.

vRAN is a no-brainer at this point while we watch chipset companies racing to provide the required performance. Early-stage deployments were limited in subscriber density, and this may be the game changer that enables bringing the technology to bigger cities and expanding its usability. That's how you build scale and open doors for pure software solutions over standard hardware.

Openness is still an issue. And it may have been affected by the perception of lower security established in 2021. As a company performing RAN security assessments, we understand that security relies on resilient products, good practices, and controls. That means that with the right amount of effort, Open RAN can be as secure as the established RAN solutions. On the other hand, without the combination of the three, commercial networks based on standard RAN may also turn out less secure than projected.

Compiled by Team SecurityGen

If you may wish to know or discuss any of the topics just drop a note:

contact@secgen.com