No. 34
February 2020

HardenStance Briefing

Trusted research, analysis & insight in IT & telecom security **PUBLIC/SPONSORED**

Ericsson & Nokia Complete 5G CyberHack

Sponsored by Ericsson

HardenStance attended the world's first 5G cyber hackathon at Oulu University in Finland on November 29th - 30th 2019. The idea and organization came from Traficom, the Finnish regulator, supported by event specialist, Ultrahack. Here's what came out of it:

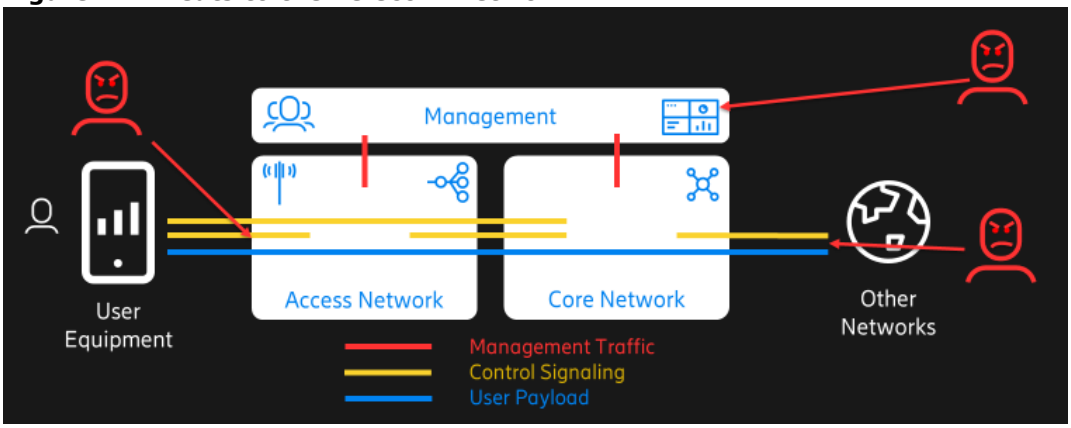
- For the first time ever, Ericsson and Nokia exposed their 5G infrastructure software to the ethical hacker community. Participants responded with valuable findings.
- As is entirely normal, hackers reported vulnerabilities or flaws in all three challenges involving a 5G NR product, 5G remote hospital and fixed wireless 5G use cases. Findings will be addressed in both vendors' R&D roadmaps.
- 5G cyber hackathons like this have an important role to play in assuring the security of the 5G network but they shouldn't be seen as any kind of panacea.
- Ericsson and Nokia should stage a second 5G CyberHack, perhaps in the US.

By far the most significant aspect of the world's first multi-party 5G cyber hackathon in Oulu on the last week-end of November 2019 is the simple fact that it happened. More than 80 ethical hackers from ten countries spent 24 hours picking holes in real commercial and pre-commercial 5G New Radio (5G NR), 5G Non Stand Alone (NSA) core and 5G Fixed Wireless Access products exposed to them by Ericsson and Nokia.

More than eighty ethical hackers from ten countries spent 24 hours picking holes in real commercial as well as pre-commercial 5G products.

Most of the hackers were cyber security professionals, most of them employees from a wide range of companies in different industries. Only a few were university students. This wasn't the first 5G hackathon. Verizon and AT&T have staged developer hackathons aimed at generating new 5G application ideas. Neither was it Ericsson or Nokia's first cyber security hackathon. They have each hosted their own hackathons in the past and will again in the future. However, these events are dedicated to finding vulnerabilities in things like external-facing web interfaces as well as Unix and Linux operating systems that are at the heart of what most hackers – white hat defenders as well as black hat adversaries - spend their time on. Until the event in Oulu neither of these vendors had

Figure 1: Threats to the Telecom Network



Source: Ericsson

ever actively participated in exposing their mobile network product hardware and software to this kind of organized external scrutiny; never on this scale; and never together with a view to combining to attract so many hackers from around the world.

So why the engagement with the hacker community in this way and why now? Obviously, cyber threats posed by organized crime, nation states and others didn't always pose the same level of business and societal risk that they do now. In the last couple of years, at the very start of the 5G era, the security of mobile network infrastructure software has come under particularly intense scrutiny from governments around the world. In particular, many governments are restricting or banning the use of Huawei and ZTE 5G kit in their country's networks on the grounds of cyber security risk.

It's only now that the expertise of the global ethical hacker community can start to be exploited to help make mobile infrastructure hardware and software more secure.

Embracing the Architecture and Protocols of the IT World

It's only now with 5G that the mobile network ecosystem is starting to embrace the distributed architecture and protocols that are widely used at scale by both good and bad actors throughout the IT world:

- 5G's new Service Based Architecture (SBA) is the mobile industry's own version of the well-established Service Oriented Architecture (SOA).
- Whereas 3G and 4G rely on the telecom sector's own SS7 and Diameter standards, mobile industry standards prescribe HTTP2 and JSON standards for 5G signaling.

Hence it's only now, with the greater adoption of IT industry norms, that the expertise of the global ethical hacker community can start to be effectively exploited by Ericsson, Nokia and the rest of the mobile industry ecosystem to help harden mobile infrastructure hardware and software. If, over the years, either company had made big open invitations to hackers to attack their 3G or 4G networks, there probably wouldn't have been many takers. That's because the balance of telecom and IT sector knowledge was still so heavily weighted towards the telecom sector.

Traficom and Oulu University Made Substantial Contributions

Not many regulators or universities are as lucky as Traficom, Finland's Transport and Communications Agency, or the University of Oulu to have two global 5G infrastructure leaders right on their doorstep.

These co-hosts of the event nevertheless made sure they exploited the local presence of Nokia and Ericsson to the full:

- Representatives from Finland's National Cyber Security Centre, which forms part of Traficom, came up with the idea for this event, branding it as an opportunity to "Safeguard the digital society". Traficom didn't just send a senior representative to come and congratulate everyone, pat them on the head, and go home either. No less than seven Traficom personnel were on site throughout the event, learning as much first-hand as possible. As a national cyber security agency, what better way to demonstrate to your Interior Ministry how seriously you are taking 5G security than by actively engaging in an event like this?
- Oulu University is one of Finland's leading universities for research in advanced technology, including in telecommunications. The University is also engaged in research into 6G and is one of the leading drivers of Finland's 6G Flagship research programme. As outlined on the next page, the University's own 5G campus test network was also used in one of the three challenges.

The Three 5G Challenges

Attendees were invited to participate in one or more of three distinct hacking challenges:

- a 5G New Radio (5G NR) product;
- a 5G network supporting eHealth applications across remote home and hospital environments;
- a 5G Fixed Wireless Access home router.

An initial phase provided a basic level of access to the network via the device's IP address and LMT interfaces being left open.

Challenge 1: The 5G NR 'Black Box' (Hosted by Ericsson)

Participants were given physical access to Ericsson's latest 5G NR product, supporting the company's latest, pre-commercial, 5G software. Participants had to assume the role of a service engineer in a telco with responsibility for operations and maintenance (OAM) for a new indoor radio. They were given access to the OAM interfaces of the baseband as well as to the remote radio unit (RRU).The hackers were steered towards finding vulnerabilities in the OAM, Local Maintenance Terminal (LMT) and traffic interfaces.

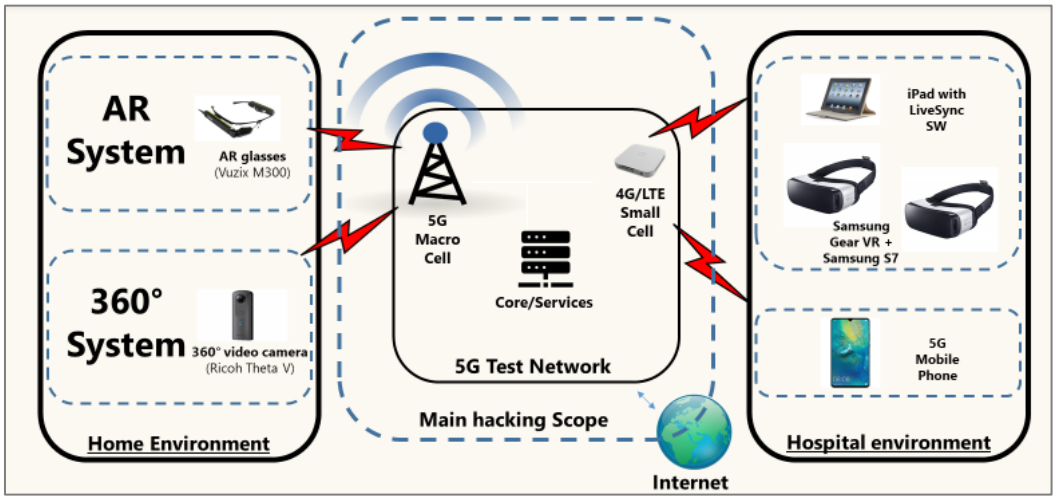
The challenge evolved in three phases over the 24 hours. An initial black box phase provided a basic level of access to the network via the device's IP address and via LMT interfaces being left open. A second grey box phase provided additional credentials, allowing participants to probe further into what was going across those interfaces. The third white box phase elevated the participant's access privileges from 'basic' to 'expert'. This allowed unrestricted access to OAM as well as LMT and traffic interfaces. In this phase, participants were also able to request access to the accompanying RRU.

Challenge 2: The Hospital Intrusion (Hosted by Oulu University)

As shown in **Figure 2,** this challenge was hosted on the Nokia-supplied 5G test network deployed on Oulu University's own campus. The network was divided into three domains:

- a nurse visiting a patient in their home, supported by Augmented Reality (AR) glasses. Digital data was collected via 360-video, close camera view and biosensors. Critical symptoms could be shown locally and remotely via an eHealth app.
- a hospital environment featuring a 4G iPad with LiveSync software, commercially available 5G Virtual reality (VR) glasses, and a 5G mobile phone for remotely viewing the home environment.
- a 5G NSA core providing the connectivity between the other two domains. The patient's home environment was connected to the core via 5G. The hospital was connected via a 4G small cell (in large part because iPads aren't yet 5G-enabled).

Figure 2: Oulu University's 5G Hospital Intrusion Challenge



Source: University of Oulu

Participants were invited to attack the 5G network leveraging soft spots in the peripheral devices, 5G devices and connected applications. They could also use any third party devices they might have brought with them. The challenge leaders steered hackers towards attacking the core network itself rather than spending time trying to break into the two home or hospital access domains or disrupting the eHealth app itself.

This challenge was split into two phases. In the first phase, home domain devices were not connected to the 5G network whereas they were in the second. The devices nevertheless used the same software in both phases.

The primary goal was to learn as much as possible about exactly how hackers approach the challenge of hacking into 5G networks.

Challenge 3: Fixed Wireless Access in The Home (Hosted by Nokia)

This challenge invited participants to hack into Nokia's 5G-enabled FastMile home gateway devices which are commercially available. The device was connected to a 4G core via a 5G NR access network. It was designed as a wireless challenge, meaning the goal was to emulate remotely accessing someone's home from a nearby street. For that reason, participants were not given physical access to the FasMile device itself.

This challenge was split into two phases. In the first phase, participants had to infiltrate the home's Wi-Fi network and capture a specific object. Having achieved that, the second phase then steered participants to find vulnerabilities or ways to compromise the admin interface of the Wi-Fi router. Nokia deliberately configured the FastMile product sub-optimally from a security perspective and modified the firmware. This was to make it easier for hackers to gain initial access to the network.

Event Outcomes and Learnings

At the closing award ceremony that took place on the Sunday morning, each of the three challenge organizers disbursed their €10,000 funds. The value of each hacker team's contribution was measured against the widely used CVSS scoring system to ensure objectivity in awarding prizes. Ericsson and Nokia each awarded €5,000, €3,000 and €2,000 prizes. Oulu University chose to award two prizes of €7,000 and €3,000.

These amounts might not sound very big in the context of the headline $1 million bounty Apple is now offering for finding the severest type of zero day vulnerability but that's not the right benchmark. Day to day bug bounty awards bear comparison with lottery prizes. Most of the prizes that are won are small, in the hundreds or thousands of dollars or Euros. Moreover, those rewards can often take days or weeks of work to earn. In that context, the chance to win a few thousand Euros split between two to four participants over a 24 hour period is a pretty good incentive, together with getting exclusive exposure to the latest and greatest new technology.

Responsible Disclosure Means What it Says

If you were hoping to read exactly what vulnerabilities were discovered during the Oulu event, prepare to be disappointed. Consistent with the core principle of responsible disclosure, these aren't being published in this briefing. Certainly, neither of the two vendors wanted nor expected that the event would identify major vulnerabilities (they both confirmed that it didn't, by the way). But neither were they focused on wanting to emerge as flawless. That's just not how the world of software development works.

Rather the primary goal was to learn as much as possible about exactly how hackers approach the challenge of hacking into 5G networks so as to factor that into their own software development practices from now on. The ultimate proof of this is that, as previously mentioned, Nokia went as far as deliberately configuring the fixed wireless access challenge sub-optimally from a security perspective. This was to make it easier for participants to gain initial access to the network and then go further to see what other flaws they could find and report back.

At the conclusion of the event, Ericsson and Nokia both expressed their satisfaction with the outcomes, confirmed that some flaws had been found, and committed to taking the findings back to their organizations and incorporating them into their R&D.

While they jointly participated in the event to create scale in participants, Ericsson and Nokia didn't share the findings of their own challenge with one another. If a major vulnerability had somehow been found that required a fix in 3GPP, for example, they would have collaborated together. However they saw no advantage in sharing what were minor flaws related to their own products.

In addition to the substance of the event and the outcomes it generated in terms of improving product security, there is also marketing differentiation to be had from this cyber hackathon for Ericsson and Nokia. This event sends an excellent message to governments, operators and businesses around the world that they are both upping their game in 5G product security.

The Oulu event is a potentially important breakthrough in formalizing the role of ethical hackers in the 5G security ecosystem at scale.

The Cyber Hackathon's Place in the 5G Security Ecosystem

Until now third party 5G vulnerability research has mainly been confined to small, isolated, teams of researchers working to find vulnerabilities without much active support from industry. The Oulu event is therefore a potentially important breakthrough in formalizing the role of ethical hackers in the 5G security ecosystem at scale.

Events like this shouldn't be seen as any kind of panacea, though. For example, most of the hackers in Oulu are likely to have been using fairly conventional tools and techniques such as buffer overflows, scripting errors and the like. Whilst these are very good for identifying known exploits, on their own they are of limited use for generating Advanced Persistent Threats (APTs) of the kind generated by nation states. Participants at hackathons also operate under time constraints which adversary groups sponsored by nation states and major criminal groups do not.

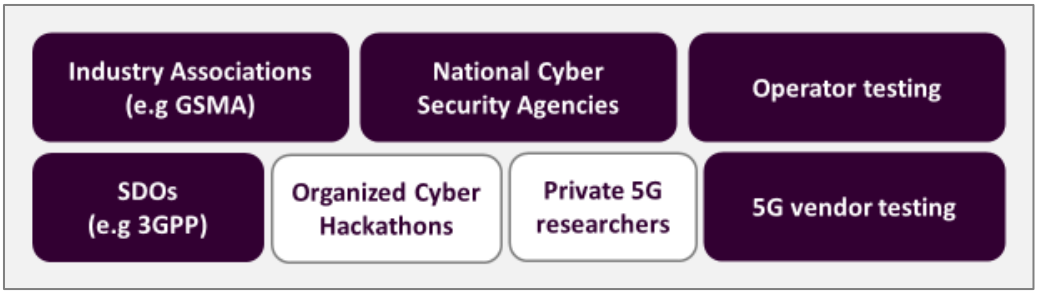
An Important Contribution to the Ecosystem, Not a Panacea

Rather than being seen as a panacea, events like this should be seen as an important new contributor to the 5G security ecosystem, alongside vendors, operators, industry associations and standards bodies like the GSMA Association and 3GPP, national cyber security agencies and private researchers. As shown in **Figure 3**, the Oulu event creates a clear opportunity for this model of 5G cyber hackathon to take its place in that ecosystem now. Ericsson and Nokia should consider a second one, perhaps in the US.

Greater collaboration is critical to closing the gap that exists between attackers and defenders in cyber security. Within the telecom sector, greater collaboration is evident in the expanded role the GSM Association (GSMA) is taking now in driving greater collaboration between operators, vendors and other stakeholders in cyber security.

The GSMA's work now includes building out the Network Equipment Security Assurance Scheme (NESAS) together with 3GPP. Where appropriate, Nokia and Ericsson should look at ways to share learnings from Oulu with these two industry bodies. ■

Figure 3: Key Participants in 5G Infrastructure Security



Source: HardenStance

More Information

- This HardenStance Briefing was sponsored by Ericsson
- Contact HardenStance's Principal Analyst: patrick.donegan@hardenstance.com
- Register for **free email notifications** when HardenStance publishes new content.
- www.hardenstance.com

About Ericsson

Ericsson enables communications service providers to capture the full value of connectivity. The company's portfolio spans Networks, Digital Services, Managed Services, and Emerging Business and is designed to help our customers go digital, increase efficiency and find new revenue streams. Ericsson's investments in innovation have delivered the benefits of telephony and mobile broadband to billions of people around the world. The Ericsson stock is listed on Nasdaq Stockholm and on Nasdaq New York. For more information www.ericsson.com

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a well-known voice in telecom and enterprise security, a leader in custom cyber security research, and a leading publisher of cyber security reports and White Papers. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, The Cyber Threat Alliance, The GSM Association, ETSI and TM Forum. To learn more visit www.hardenstance.com

HardenStance Disclaimer