No.22
28th March 2019

HardenStance Briefing

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

ETSI Secures Public Clouds for Telcos

- Along with the other cloud provider partnerships they're exploring, telcos should at least have the option of running public telecom network functions in public clouds. The new ETSI standard TS 103 457 provides a potentially important security bridge that would support telcos going in that direction.
- The new standard provides extra security for sensitive functions down to individual Virtual Machines. It introduces a trust hierarchy onto the flat admin architecture of public clouds so that only a subset of telco engineers or processes can access these sensitive functions.
- Standards continue to have a major role to play in telecom, including in security.

We're nowhere near it becoming a real-world commercial requirement any time soon but the European Telecommunications Standards Institute Technical Committee on Cyber Security (ETSI TC Cyber) has just released a new security standard to enable telcos to run their core public telecom services in – wait for it – public clouds.

Yes, that's potentially regular public telephony brought to you by your local telco running in Google Cloud Platform (GCP) or AWS. To say that telcos aren't in any hurry to go in this direction is an under-statement. Telcos operate under government license. If the public communications network goes down, people can't reach police, fire and ambulances services.

By allowing any administrator access to the root password, telco security argues that cloud security takes unnecessary risks.

Running public telecom network services out of a public cloud might not be at the top of the agenda but for some telcos, that could emerge as one of the many partnership models they are continuing to explore with cloud providers. Recent public examples, still focused very much on business services, include the following:

- Vodafone and Telefonica are among those telcos that have latched onto AWS' new Outpost product line. This runs AWS services on AWS-designed hardware that sits in the enterprise premises to support hybrid cloud models.
- One of Oracle's key messages at the recent Mobile World Congress in Barcelona was pitched at building its own 5G core network elements; layering their market-leading analytics portfolio on top of them; and selling 'slices' of these 5G cloud networking resources wholesale to telco partners.

Bringing a Telco-Grade Trust Hierarchy to Flat Admin Architectures

Among the critical security barriers to telcos using public clouds for core public telecom services today is the flat administration, single root, architecture of public clouds. Here there is still a big gap between the telco security and cloud security models.

By allowing any administrator access to the root password, telco security argues that cloud security takes unnecessary risks. Role Based Access Controls (RBAC) and Attribute Based Access Controls (ABAC) are fine as far as they go, telco security argues, but since administrators can still access the system root password to go to places they're not supposed to, this constitutes an unacceptable risk.

If telcos are going to run their public telecom network functions in a public cloud in future, ETSI TC Cyber prescribes new security tools that eliminates access to restricted areas altogether rather than merely prohibiting it.

These can be found in TS 103 457, Trusted Cross Domain Interface: interface to offload sensitive functions to a trusted domain. The new standard is not intended to be in any sense mandatory. Other approaches may also come to market but this one does at least have the merit of being a standard.

TS 103 457 is a set of tools in the form of security specifications that can be built into the design of telecom network functions. Now that these are being virtualized, they're referred to as Virtual Network Functions (VNFs). VNFs can, in turn, comprise dozens or hundreds of unique Virtual Machines (VMs) or even more containers.

The new ETSI standard assumes that telco VNFs can be classified according to one of two types of sensitivity:

- **Wholly sensitive:** A small subset of telco VNFs are wholly sensitive. If they are compromised, the whole telecom network is at risk. Hence they should only be managed by a small subset of highly trusted engineers operating in a wholly isolated zone with its own dedicated root of trust. Examples include a Home Location Register (HLR) and Authentication Centre (AUC) in 2G; the Home Subscriber Server (HSS) in 4G and IMS; and the new Authentication Server Function (AUSF) and Unified Data Management (UDM) in 5G.
- **Partially sensitive:** The vast majority of telco VNFs comprise a mix of VMs or containers, only a very small subset of which are sensitive (carrying billing data for example). In legacy telecom networks, the separation of sensitive functions is enforced in hardware such as via a separate card. In an increasingly software-driven network architecture evolving to 5G, another approach needs to be found.

Only a small subset of sensitive VMs or containers that make up a partially sensitive VNF would need to comply with this standard.

TS 103 457 provides specifications for designing VNFs so that differentiated access rights are embedded not just into each discrete network function or VNF but also at the more granular level of each discrete software component of a VNF (each VM or container).

Requiring each and every function, let alone each and every VM or container, to support this standard isn't necessary and would add a lot of unnecessary cost. In a public cloud environment all of the components of a wholly sensitive VNF would need to be TS 103 457 compliant. However, only the small subset of sensitive VMs or containers that make up a partially sensitive VNF would need to comply.

The presence or absence of TS 103 457-compliant software components in the network then maps directly to the telco's operations environment so that a subset of sensitive functions across all software components running in the network can only be manipulated by a trusted subset of engineers. The vast majority of engineers can nevertheless access the vast majority of software components that are non-sensitive.

The standard is best thought of as an underlying framework of specifications on which specific, still to be defined, services will be able to run. A useful analogy is to think of the architecture of high trust telecom services operating at four layers in a public cloud:

1 Some kind of Hardware Mediated Execution Enclave (HMEE). The obvious example is Intel's SGX which has some known issues but has already been embraced by ETSI and other telecom Standards Development Organizations (SDOs).

2 TS 103 457 then presents like a generic, service-enabling, framework of specifications. This framework allows the most sensitive functions to be isolated and treated differently.

3 On its own, TS 103 457 is nothing without a service to run on it. It now awaits the definition of specific network security applications to run on it. These could come from standards bodies or single entities.

4 Introduction, management and monitoring of appropriate segmentation in day-to-day telco operations.

At a point in the future when telcos start asking for it, compliance to TS 103 457 could therefore become something of a security-related differentiator for telecom software vendors that don't currently have one. From a networking vendor perspective it also offers the distinct advantage of requiring that only a small part of a VNF need be compliant rather than all of it.

Some criticism of global standardization either wilfully or absent-mindedly neglects the value of foundational specifications that are replicable and inter-operable.

Standards have a major role to play in security

Consistent with Briefings published in the last 12 months on the Anti Malware Testing Standards Organization (AMTSO) and NetSecOPEN, HardenStance believes that standards remain critical to the cyber-security community as a whole. In fact the work these two organizations are doing highlights how much more standardization can contribute to improving enterprise security - and as a matter of urgency.

In telecom circles it has become increasingly fashionable in recent years to question the value of global standardization or even blame it outright for the sector's failure to keep up with the pace of innovation in the cloud. Some of that criticism is justified. Some of it either wilfully or absent-mindedly neglects the value of foundational specifications that are replicable, inter-operable and aligned with government licensing requirements across hundreds of telcos in each of the world's nearly two hundred countries.

Telecom standards and telecom security standards remain core to the health of the sector. Whichever telcos are first to seriously contemplate public telecom services in a public cloud will look to see what globally recognized telecom security standards are there to help them – or indeed permit them – to execute on that.

More Information

- Contact HardenStance's Principal Analyst: patrick.donegan@hardenstance.com
- Register for free email notifications when HardenStance publishes new content.
- www.hardenstance.com
- HardenStance received no payment for publishing this Briefing.

HardenStance Disclaimer