Cloud infrastructure actual security challenges ...from Telecom perspective

Gábor Csordás – Security Architect @Nokia
Challenges and transformation of cloud security

Technological transformation towards cloud nativeness & business model evolution
- legacy bare metal (DSPs, ATCA) → virtualization → cloudification → container infrastructure (embedded into VMs or bare metal)
- Convergence towards IT (also on application level)
- Wide usage of OSS (Open Source Software)
- Degradation in security perception when transforming from VM based to container based architecture
- Moving from private to public cloud →
- Paradigm shift: Perimeter protection + DMZ → zero trust philosophy → each product as a standalone component must be secure enough

5G relevance: cloud native (CNF based + orchestrated) productized also for public-cloud deployment, wide usage of OSS components
Cloud security - Infrastructure vs. application-level security

• Infrastructure layer:
  Wide usage and convergence* of Telco infrastructure in Telco environment:
  (virtualization techniques, cloud platforms, containerization)
  Using the IT-based environments in Telco also inherits their vulnerabilities
  Most of the known vulnerabilities are targeting the infrastructure layer
  • low hanging fruit, huge install base
  • prerequisite for the more sophisticated, application-level attacks
  • widely documented, automated tools available

• Application layer:
  Requires special, application and/or environment specific information and knowledge
  • vulnerabilities typically not shared within the general security community
  • telco standards and architectures
  • signalling protocols
  • solution specific implementation details (topology & architecture)

A real sophisticated cyberattack typically involves both the infrastructure layer and the application level.

*Telco applications might need some improvement in commodity IT infrastructures (e.g., real-time scheduling requirements, HA- improvements)
Quick case study – highly sophisticated attack methods

**Spectre & Meltdown**
Hardware vulnerabilities allow programs to steal data which is currently processed on the computer.

https://meltdownattack.com/

(hyperthreading – protection method in the hypervisor – performance penalty of protection vs. thread level – exploiting the stolen data – decision for mitigation based on the business model transformation)

**L1TF:** A speculative execution side channel cache timing vulnerability, potentially allowing unauthorized disclosure of information residing in the L1 data cache.


Foreshadow – Intel CPUs Affected By L1TF Vulnerabilities - Swascan
Quick case study – Erosion of trust because of legacy protocols

**SS7 attacks:** Compromise and intercept voice and SMS communications on a cellular network. Legacy protocols designed for isolated environments. Later moved to convergent infrastructure.

- [A Step by Step Guide to SS7 Attacks - FirstPoint](firstpoint-mg.com)

**Syniverse:** Handles 740 billion text messages annually for carriers around the world including Vodafone, AT&T, T-Mobile, Verizon and China Mobile.

- [Syniverse quietly admits it was hacked for five years | Light Reading](https://lightreading.com/security/syniverse-quietly-admits-it-was-hacked-for-five-years-1418913087)
- [Who is Syniverse, anyway?. One of the world’s largest SS7 hubs was... | by David Allen Burgess | Telecom Expert | Oct, 2021 | Medium](https://medium.com/telecom-expert/who-is-syniverse-anyway-one-of-the-world-s-largest-ss7-hubs-was-11532f252f57)

→ Still trusting in SMS based Multi-factor authentication?

**The Facebook story** (no indication for being a victim of an attack, but BGP is used by other clouds as well, hosting telco applications) & **poisoning** (ARP, BGP, etc) type of attacks

OSS - Curse or blessing?


Focusing on security related drawbacks:

Attractive target for cyber attacks:
- usage of outdates SW
- OSS included everywhere (infra + application)
- public documentation of vulnerabilities (pros+cons)
+ widely available vulnerability scanners working based on vulnerability databases (e.g. CVEs*)
- SLA challenges (directly included OSS vs. re-packaged OSS)
- extremely fast inflation of being vulnerability-free

“You become responsible, forever, for what you have tamed.”

Need for SVM (Software Vulnerability Management) and for systematic hardening

*The mission of the CVE Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities

CVE - CVE (mitre.org)
Thank You