Compiled by Przemek (Shem) Radzikowski – shem@drshem.com – http://drshem.com

Cloud Security Alliance (CSA) Congress Berlin 2015

Conference Notes

1. Siani Pearson (HP Enterprise) – Science Lead (quick introduction)
2. Daniele Catteddu – OCF-STAR Program Director Cloud Security Alliance
    a. **Digital Single EU Market** [mr junker]
        i. Aims to break down national silos in telecoms regulation in copyright and data protection legislation, in the management of radio waves and in the application of competitive law
        ii. Better online access to digital goods and services.
        iii. An environment where digital networks and services can prosper
        iv. Reinforce trust and security in digital services
        v. Enhance the Digital Economy, Cloud, Computer and other data services
        vi. Many organizations are still struggling in moving to cloud, changing existing suppliers/carriers etc.
    b. Public Consultation – Input from general public welcome
        i. http://Ec.europa.eu/eusurvey/runner/Platforms
3. Frederic Gittler (HP Enterprise A4Cloud Project)
    a. **Cloud for Europe** – trusted cloud services for European market for public admin
    b. **PICSE** – procurement innovation for cloud
        i. Pre commercial procurement (PCP)
        ii. Setup European procurers platform

iii. Build on collaborative model from Helix Nebula to engage with providers and customers for cloud

iv. Make procurement for cloud services simpler

c. **SLA-Ready** – Make Cloud SLA readily usable in the EU private sector

i. Avoid take it or leave it attitude by providers

ii. Avoid lack of privacy and data security

iii. Avoid Provider lock-in and lack of standardization

iv. Avoid Jurisdictional issues and law

d. **A4Cloud** – accountability for cloud and other future internet services

i. The project has built methods and tools which combine:

1. Risk analysis
2. Policy definition and enforcement
3. Monitoring
4. Compliance auditing
5. A4clooud.eu – reference architecture

e. **SPECS** – secure provisioning of cloud services

i. Develop and implement and open source framework to offer Security as a service based on SLAs and security parameters

1. Enable user=centric negotiation of cloud SLA
2. Monitoring in real-time the fulfilment of SLA
3. Enforcing SLA to keep sustained QoSec

f. Why are some organizations still not going into the cloud?

i. Ongoing Legal barriers and legal uncertainty

ii. Data encryption and where data lives is still an issue

iii. Classification of data into three levels may help (high, med, low)

1. All these discussions are around PII – but what if we used homomorphic encryption and let the end user be the holder of keys for their own data. Many of these problems stems from the fact that there is no body that end users/companies/governments trust to hold/store the private keys.

4. Said Tabet – Senior Technologist – office of CTO – EMC Corp – Ireland

a. Governance accountability compliance in the cloud workshop

b. Beyond cloud – connected devices, embedded systems, IoT plus cloud

c. Accelerated pace of adoption in recent years

d. Rise of Hybrid Cloud

e. **SPECS** – **ViPR** provision of storage on S3.

f. Classification of security levels.

g. Privacy Level Agreement (PLA) – v2 compliance - big push on this.

5. **Bruce Schneier – What to expect in next 12 months**

a. Seeing a variety of attackers, you'll hear a lot of cyber war talk

b. People being herded to move to the cloud, devices, phones, and soon the desktop OS

c. Can't tell difference between APT (advanced persistent threat) i.e., Government or State vs an individual player in basement of the house – they all use the same tactics – "when you're attacked in cyber space you can call any number of people to help you – but the legal regime depends on two things, legal jurisdiction and why someone attacked you.

d. **Relative security** – how secure are you compared to the other guy. Most hackers will go after the easiest target. APTs on the other hand, "want" to get something and are prepared to engage well-protected infrastructure.

e. Most hacking is political hacking, non-financial hacking, e.g.: Sony having everything published, Ashley Madison database leak etc.

f. Time from **Theft** of data to **Monetization** is very short, now reaching days, rather than months

g. Governments getting more involved in privacy policies. Some are asking us to violate our privacy policies in the name of security.

h. The big are getting bigger.

i. Buyers can't tell the difference between bad products and good – the bad will drive out good products. The most secure products are not going to win because there are too many products on the market which only confuse the end users.

j. **Prospect theory** – loss aversion: risk averse when it comes to gains but risk seeking when it comes to losses. Seeing this in security space more and more, particularly when the cost of security is on the rise and threats keep getting larger.

k. **People matter during response to a threat**. You can automate most of the things about security, but not during response phase. You can't outsource decision making, how to you respond, what should you do now? During security response there is a change in who is in charge – from technology to people. (Zurich airport analogy – bomb joke)

l. **OODA loop** - Mr John Boyd - US Air Force – Observe, Orient, Decide and Act – Some players are already starting to apply this to cybersecurity. Originally used during combat operations. https://en.wikipedia.org/wiki/OODA_loop

6. Panel: **Cloud Trust and Security Innovation**
    a. Nathaly Rey – EMEA Head of Trust, Google for Work
        i. Cloud policy is being driven by government and large enterprise. This is good for SME because their cloud platform operates at the same level as security-demanding clients.
        ii. Security by tickbox – in past, policy was too prescriptive without giving any thought to individual organizational needs. Frequently, one size does not fit all.
    b. Said Tabet, Senior Technologist, CTO Office EMC
7. Thomas (Microsoft)
    a. How do we attract people into government rather than fancy private sector companies? Population is getting older and we need to ensure that intellectual knowledge remains in the public sphere.
8. David Lenoe, Director, Secure Software Engineering Adobe Systems
    a. What happens **When Security Tools Collide**
        i. Crowd Source – security via community has had some good results for Adobe.
        ii. Signal Sciences
        iii. Bugcrowd – Broad skills and niche areas
9. NIST Presentation – NIST Cloud Computing Program
    a. Cloud computing reference architecture **NIST SP 500-292**
    b. → developed with CSA TCI
    c. NIST Rubik's cube – a security matrix
    d. Heat MAP -- 50-299 heat map of aggregated CIA security indexes
10. **Akamai Threat intelligence** at the cloud – CDN – Content delivery network
    a. Or Katz, Principal Security Researcher @or_katz
        i. DDoS attacks are on the rise and are now starting to be seen as a smokescreen for the "real" or "secondary" attack and ultimate exfiltration of data.
        ii. Security becoming a game of Hide and Seek – playground for Akamai Cloud network
        iii. Find malicious activity and create actionable threat intelligence
        iv. 170,000 servers, 750+ cities, 92 countries
        v. 2 trillion hits per day

vi. 260+ terabytes of compressed daily logs

vii. 15-30% of all web traffic

b. Ezra Caltum Senior Researcher @aCaltum

i. Have seen **brute force attacks up to 10,000** password attempts per hour using distributed cloud networks. Current countermeasures don't cope well since Distributed-brute-force using only a few attempts per hour per source IP does not trigger current thresholds. In order to detect brute force patterns the scope of monitoring needs to be expanded across many cloud environments.

ii. Most botnets are running on the same network/cloud as target

iii. Most botnets were active at least 2 months before being detected

iv. **Tactical control** – block any login attempts initiated from detected botnet

v. **Strategic controls** – adjust security control brute force rate mitigations.

vi. GEO intelligence – restricting geo location isn't easy since it cuts out a considerable users of service

vii. Present threat intel – detection based on cross targeted correlation

viii. Future threat intel – forecasting based on patterns

ix. Summary – cloud can give unique actionable threat intelligence when we are able to utilize **cross-target correlation data**

11. Marillano - **State of the art analysis** – **Spanish & Peruvian Chapters** (CSA)

a. Why they go to the cloud? When they do, are they happy with services they receive?

b. Consumers don't care about the location of CSP / datacentre

c. Why people move back from the cloud (out of the cloud)

i. Cloud is maturing so this is strange, why is this happening?

ii. Out of cloud and private cloud – unsatisfied with service and inability to fully migrate data

iii. People are moving out because they aren't happy with service

1. Unclear yet as to what are the reasons?

iv. Shadow IT occurrence

1. Impossible (45%), doesn't happen (25%), already happening (5%)

v. Uses of Cloud Services

1. Mail (70%), storage (50%), web (45%), erm/crm (25%), business sw (25%), others (3%)

vi. Do you know about certification - Certifications (CCSK 50%) –

12. **Waverly Labs** - CSA **SDP Software Defined Perimeter Working Group** – Huanita (Open source code project for software defined perimeter to defend cloud applications from DDoS
    a. DHS Problems – largest department in US
    b. SDP aims to be able to withstand 1TB throughput
    c. SDP Control & ID Planes are separate (input from OWASP working groups) – similar architecture to SDN controllers / SDN switching plane.
    d. Monitoring Service and Logging is part of the spec
        i. Volume
        ii. Connection close events
        iii. Num of open connections
        iv. Messages per second etc.
    e. SDP - What's different
        i. Standardization of "need to know"
        ii. Device attestation before authentication
        iii. Mutual TLS
    f. **Single packet authorization** (SPA) is used to initiate any and all communication
    g. **Blackens the server**: the server will not respond to any connections
    h. Open Source SDP – Anti-DDoS assumptions
        i. Easy to spoof millions of IP addresses
        ii. Not easy to spoof millions of phone numbers or authenticated devices
        iii. Stack multiple factors together to verify access
        iv. Verify first, then the login (reverse the process)
    i. Hard problems (what we are looking for are legitimate packets and dropping everything as quickly as we can):
        i. Filtering
        ii. APIs between components
        iii. Using existing open source components
    j. Port knocker (we want to minimize it down to only 32 bytes)
    k. Possible to join the open source team (14 people on conf calls)
13. EU cloud initiative
    a. PPP, public private partnership

   b. C-SIG cloud select industry group
   c. European cloud partnership (ECP)
   d. E-identification and services (eIDAS) regulation
   e. Network and information security (NIS)
   f. General Data protection regulation (GDPR)
   g. EU Cloud Stragecy for Certification
      i. Cloud Certification schemes list
      ii. Cloud Certification Metaframework
   h. Cloud for Europe
   i. Helix Nebula Science Cloud
   j. European Commission Cloud1 – ready for consumption by Dec 2015

14. Walking the talk – Marnix Dekker – CISO team, European Commission
   a. Marnix.dekker@ec.europa.eu (philippe.merle@ec.europa.eu)
   b. 3600 employees in IT in EC / 50,000 employees
   c. 1600 systems / centralized and decentralized / 500 million euro budget
   d. At IT department (aka DIGIT) :
      i. 160 million spent 'centrally', of which 100 million is spent on infra
15. Radu Popescu-Popescu, president ICAM and one of the founders of Fraunhofer
   a. Gave background on Fraunhofer institute and ICT/Security efforts
   b. IoT – estimate 50 billion by 2010, 200 billion devices by 2020
   c. We are coming into a world where devices, are instrumented, interconnected, and intelligent – SMARTER world.
   d. **IPfication** of devices – "the most profound technologies are those that disappear" – zero-gateway architecture,
      i. Industrie 4.0/Industrial Internet/Internet of Everything IoE, Internet of Things IOT/ Cyber Physical Systems
      ii. Top 10 Cyber threats on ICS, Industrial control systems
   e. **IoT - Cisco is working on a FOG project**, analogous to Cloud – which tries to cloudify / **fogify** commodity devices/appliances/factories. http://www.cisco.com/web/solutions/trends/iot/fog-computing.html
   f. **Fata morgana effect** (mirage) – there is no secure system, we can improve but we never achieve a completely secure system

i. Solution – **learn, how to live in an insecure cyber space**, rather than hope, technology could provide 100% secure system

g. Security by Design – dream or reality – a statement designed to silence people who want answers. The manufacturers don't want you to know that they don't have a bulletproof solution to the security problem.

h. What is trust without identity… identity of persons, objects, services -- of everything? This leads to a certification o everything in the space of **Cyber Physical (CP) Systems**

i. Radu.popescu-zeletin@fokus.fraunhofer.de

16. Matthew Goodrich – Director FedRAMP, US GSA, OCSIT GSA – General Services Administration

    a. USG Approach to Cloud and a Need for Common Standards

    b. **800 series of NIST documents** (853 security catalogue)

    c. Had to put together a way which would allow the government to trust each other

    d. (837 series easy to understand)

        i. Select auth controls

        ii. Identify the risk and authorize it for us

        iii. Continuous monitoring etc.

17. Gwendal Le Grand, director of technology and innovation, French data protection authority

    a. CNIL – three guides in English , PIA Tools, PIA Methodology, Measures for the privacy risk treatment

18. **SAFECode** (Software Assurance Forum for Excellence in Code) – http://www.safecode.org/about-safecode/

    a. Software runs all sorts of hardware

    b. Jeep urged to update cars to stop hackers

    c. "if you put software on a donkey, you can hack the donkey"

    d. Most software developers have great university degrees, but next to no formal security training.

    e. SAFECode/training

        i. Secuire memory handling

        ii. Threat modelling

        iii. Xss etc…

    f. **Common Criteria** isn't something you need in this day and age, twenty years too late.

g. Darknet – **TheRealDeal** and other exploit resources

h. Life Expectancy - "Attesting to software security is the same as attesting that you won't die in the next five years"

19. **Emerging Approaches in a Cloud** –Connected Enterprise: Containers and Microservices

    a. Anil Karmel, Co-founder and CEO, C2 Labs, Co-Chair, NIST Cloud Security Working Group

    b. Hybrid cloud is becoming the defacto norm

    c. Relative to 2006, cybercrimes increased by 782% / new malware detected every 3 minutes

    d. **Mosaic effect** – two pieces of info, put together mean something to someone

    e. Microservices – highly decoupled and modular with services organized around capabilities (example, Docker)

20. Krishna, CTO Netskope

    a. How data can be breached in the cloud – pushing his own company agenda and tools.

21. **Quantum computing** – quantum protection

    a. Although quantum computing promises huge gains in processing, we still have the problems of standard PKI, such as Quantum key distribution (QKD)

    b. Quantum-resistant (notice that algorithms for encryption and signatures

    c. CSA Quantum-safe security working group

22. **Shittu O. Shittu** – SIEM, state of logging and event management

23. Patrick Kerpan – CEO cohesive networks

    a. Overlay networks will become the norm

        i. Hardware you can't get to; and

        ii. Hypervisors you don't control

    b. Limit of users access

    c. Google / BeyondCorp have already assumed that the internal network is as dangerous as the internet. They are making appropriate changes to their infrastructure to address these.

        i. Overlay networks to the rescue…

    d. IoT is not the internet of things, it will be the **internets of things.** Meaning, every IoT connected device will operate on an abstracted

    e. Organizations will run overlay networks over trunks out on the real internet.

f. It's called the cloud because it's so far away…. We continue to mistakenly think that hypervisors will be able to solve all our problems.

Przemek (Shem) Radzikowski
Independent Security Architect & Researcher
shem@drshem.com