SEGF WG MEETING

GSMA

Latin America

BOGOTÁ • 18 - 19 MAY 2016

Sponsored by

araxxe Syniverse *We make mobile work* XURA

Security and Fraud Working Group
Wednesday, 18 May
WORKING AGENDA

Time	Contents
09.00 – 10.00	**Opening. Introductions and recap** Chair: Luis Miguel Hurtado Zabaleta, Telefonica Deputy Chair: Jose Gilberto Fragoso, America Movil Lucas Gallitto, SEGF Coordinator, GSMA Latin America
10.00 – 10.30	**Fraud Manual** Round table to update the fraud manual with the inputs of all Latam operators.
10.30 – 11.00	**Coffee Break**
11.00 – 12.30	**Hot Security Issues** All Latin American Operators present a brief update on key security issues in each of the markets. One presentation per country. This gives all members visibility on what is going on in other countries in the Region. Argentina: Marcelo Scarabel (Telecom Personal) Ecuador: Mirka Leon (Telefonica) Brazil: Helio Cabral (Telefonica VIVO) México: Gilberto Fragoso/Gabriel Arenas (AMX) Chile: Nelson Cid (ENTEL) Peru: Aldo Romero (Claro) Colombia: Nelson Bermudez (Tigo-UNE) Venezuela: Luis Rogelio Ugarte (Digitel)
12:30 – 14:00	**Lunch break**
14.00 – 14.30	**IMEI Security Weakness Reporting and Correction** Presentation and revision of the procedure to report IMEI security weakness. **Speaker:** James Moran, GSMA
14.30 – 14.50	**SS7 and Interconnect Security** • SS7 security research and vulnerabilities • Impacts for mobile operators and their customers • Recommendations to operators • GSMA action **Speaker:** James Moran, GSMA
14.50 – 15.30	**Advanced Persistent Threats (APTs) and Advanced Malware** In Advanced Persistent Threats (APTs) and targeted attacks, the attacker uses a myriad of tools and techniques to breach into an organizations' network, steal sensitive information and compromise its operations. These include exploitation of application vulnerabilities to silently infect computers; malicious Java applications which bypass existing security and exploit prevention controls; advanced malware that enables remote access and control of corporate computers; and access to corporate resources using credentials stolen through spear phishing schemes. **Speaker:** Gilberto Fragoso / Gabriel Arenas, AMX
15.30 – 16.00	**Coffee Break**
16.00 – 16:30	**The use of SIEM for the treatment of internal fraud and its evolution toward security intelligence tools applied to fraud prevention** Security information incidents as data leakage, non-compliance with security policies, misuse and/or abuse of computing resources of the company are a critical component in many cases of internal fraud. The use of Security Information and Event Management Systems (SIEM) was traditionally used for managing anomalies in networks, but now are used by the Department of Information Security and Fraud Prevention to expand the vision in the fight against internal fraud taking advantage of the big data. **Speaker:** Luis Miguel Hurtado, Telefonica
16.30 – 17.15	**New regulation related to handset theft in Colombia** The theft of mobile phones, is the crime with the largest number of affected people in Colombia. The regulator, the Ministry of ICT and the local trade association have been developing strategies to reduce this crime. Several control measures have been implemented which include changes in the reporting process and suspension stolen mobile phones, identification and control of invalid, not approved, modified, unregistered and duplicated IMEIs. This presentation aims to present and analyse the measures that have been implemented to fight against this crime. **Speaker:** Carlos Lemus, Telefonica Colombia
17.15 – 18.00	**Finding the right approach in cyber threat intelligence**

	Today the organization needs to be more focus in what threats are trying to penetrate and steal information; find the correct way to detect and classify the threats, puts the organization in the way of response correctly in case of incidents. In presentation We abord topics like CyberIntelligence , profiling and attribution. **Speaker:** Patricio Sanchez - SCITUM

Security and Fraud Working Group
Thursday, 19 May
WORKING AGENDA

Times	Contents
09.00 – 09.45	**Securing the Internet of Things** IoT services can only scale if they are secure, and the security of any service is only as good as its weakest link. The GSMA has developed IoT security guidelines to promote best practice for the secure design, development and deployment of IoT services. A proven and robust approach to address typical cybersecurity and data privacy issues associated with IoT services will create trusted, reliable services that can scale as the market grows **Speaker:** Fernanda Vaqueiro, Security Information Manager, Oi Brazil (or other TBD)
09.45 – 10.15	**Fraud by changing simcards and bank fraud** Latin America, like the rest of the world remains as victim of bank fraudsters who perform Customer Identity theft in the changes of Simcard. This phenomenon, which is originated in the gaps of processes of our new fast-growth-digital-culture, has made it easier for our customers to be attacked and harmed when they use self-management channels and other facilities originally designed by the Telco Operators to give a better customer experience. The challenge is big, both for telecommunications companies and to financial institutions, in order to have better control strategies and timely communication that reduce the impact. **Speaker:** Angela Calderon, Telefonica Colombia
10.15 – 10.45	**Coffee Break**
10.45 – 11.30	**Cybersecurity Services and Cyber Intelligence Tools** **Tacyt demo**: Monitoring and analysis of mobile threats. Tacyt monitors, stores, analyzes, correlates and classifies million mobile apps with big data technology adding thousands of new applications every day. **Speaker:** Diego Espitia, Eleven Paths
11.30 – 12.00	**Mobile Money** Introduction What is mobile Money? - Industry Status - Industry status in Latin America Mobile money for regulatory perspective - Best practices - Risk mitigation **Speaker:** Jose Sanin, GSMA
12.00 – 12.45	**Wrap-up** - Next conference calls format - How KPIs info gathering is working - Blacklisting. Way of working among operators. **Proposal to discuss presented by Telefonica Argentina** - Next steps - Next meetings - AOB
12.45 – 14.15	**Lunch break**
14.15 – 14.50	**Integrated Interconnect Fraud Detection Approach** Interconnect fraud is no more limited to traditional SIM Boxes. There are today more fraud schemes and bypass techniques are more sophisticated. Telecom operators need an integrated approach to tackle interconnect fraud globally. Some case studies: - SIM Box: how to deal with counter-detection and white-lists? - Ghost Trunks: how to detect fraud cases slipping below the radar?

	- OTT Bypass: is it only about Viber? - SMS Fraud: does A2P SMS mean more revenues or more fraud? **Speaker:** Fidel Aponte, Araxxe	
14.50 – 15.25	**A Review of Alternative Global Fraud Statistics** Mutual understanding between global operators on fraud trends provides powerful insight for improved predictability. Following the CFCA's valuable survey results, we consider an alternative source of global fraud data to see what more we can learn. **Speaker**: Maximilian Goldberg , Syniverse	
15.25 – 16.00	**Securing the vulnerabilities exposed in SS7** Vulnerabilities in mobile networks' SS7 signaling have been publicly demonstrated and these vulnerabilities impact every network. Through its support of the GSMA Fraud and Security Group, independent testing of multiple networks' security and by working with operators to secure their networks, Xura will share the insights gained and key lessons learned, addressing: • How signaling networks can be attacked, how security varies and why no network is currently secure. • Quick and fixes: What are they? What are their limitations. • How to design effective, long-term signaling security into the network. **Speaker:** Mark Windle , Xura	
16.00 – 16.30	**Coffee break**	
16.30 – 16.50	**Abuse and revenue loss in mobile data. Causes and Recommendations** Abuse and frauds in mobile data is currently one of the main concerns for mobile operators. This issue have many different causes, some related to internal weaknesses and other from external and persistent attacks over specific vulnerabilities of each network. • Analysis of the main causes of revenue loss and miss invoicing in mobile data services. • Methodology proposal to reduce misconfigurations, abuse and fraud risks in mobile data. • Solution model, application examples and tools. **Speaker:** Osvaldo Torres, TI-Gestion	
16.50 – 17.10	**Innovations in SIM Box Detection** Best Practices in the fight against SIM Boxes and innovations in detection methodologies with regard to the entire interconnect path: voice, OTT and SMS. **Speaker:** Emmy Leger, Sigos	
17.10 – 17.30	**An Inner view on SIM Card security evolution** How operators can take advantage of the features already existent or defined in the different SIM card standards, going from state of art SIM security features, moving from 3G to LTE on IMS services and extending to eSIM using remote provisioning. **Speaker:** Carlos Tomero, Gemalto	

Sessions colored in blue are CLOSED, only OPERATORS can participate