Security Conference 2022

GSMA Device Security Certification

James Moran

04/10/2022

Fraud an Security Group in a Nutshell

FASG Mission

Centre Of Expertise

Drive industry management of mobile fraud and security

Trusted Environment

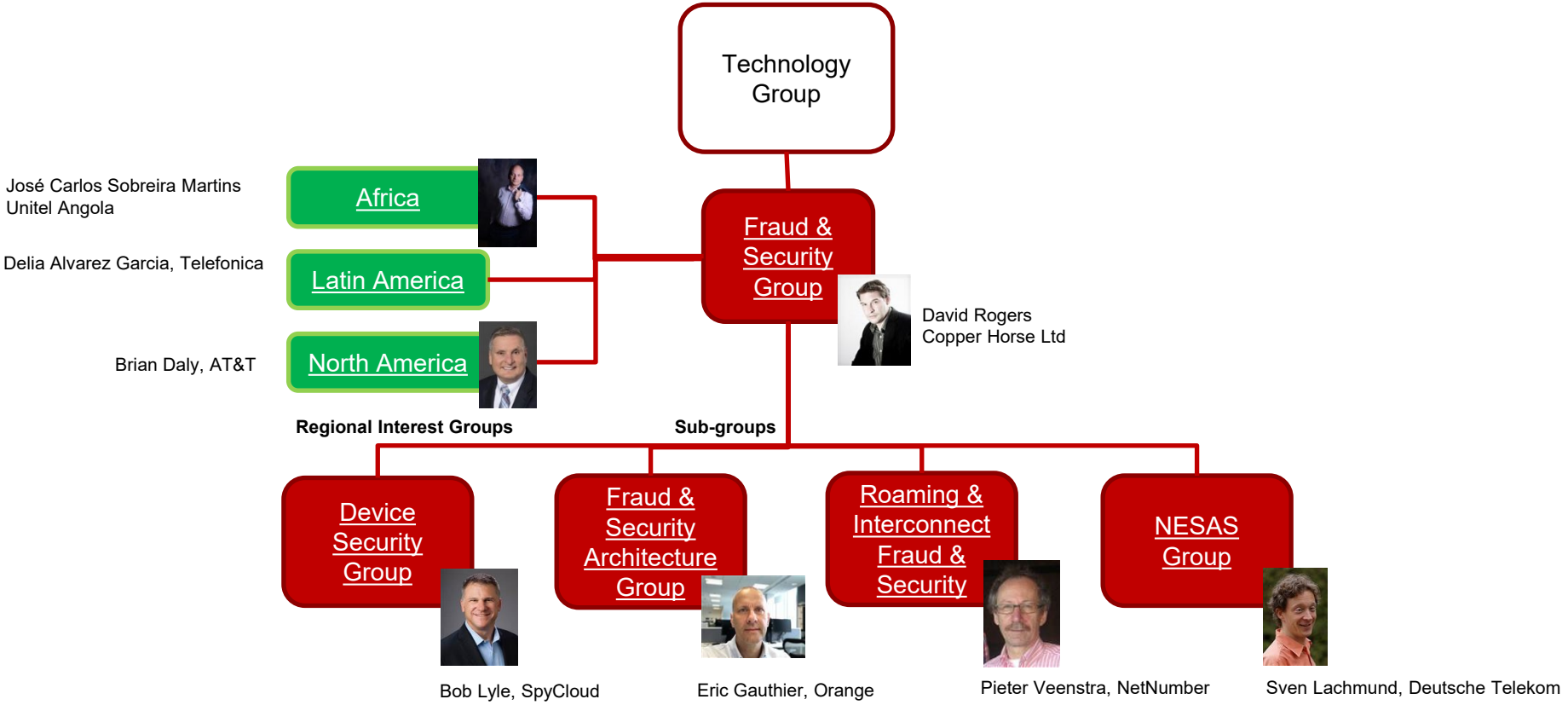
Provide a trusted environment for discussing fraud and security matters.

Increase Protection

Mobile operator technology & infrastructure

Customer identity security and privacy

FASG Structure and Leadership



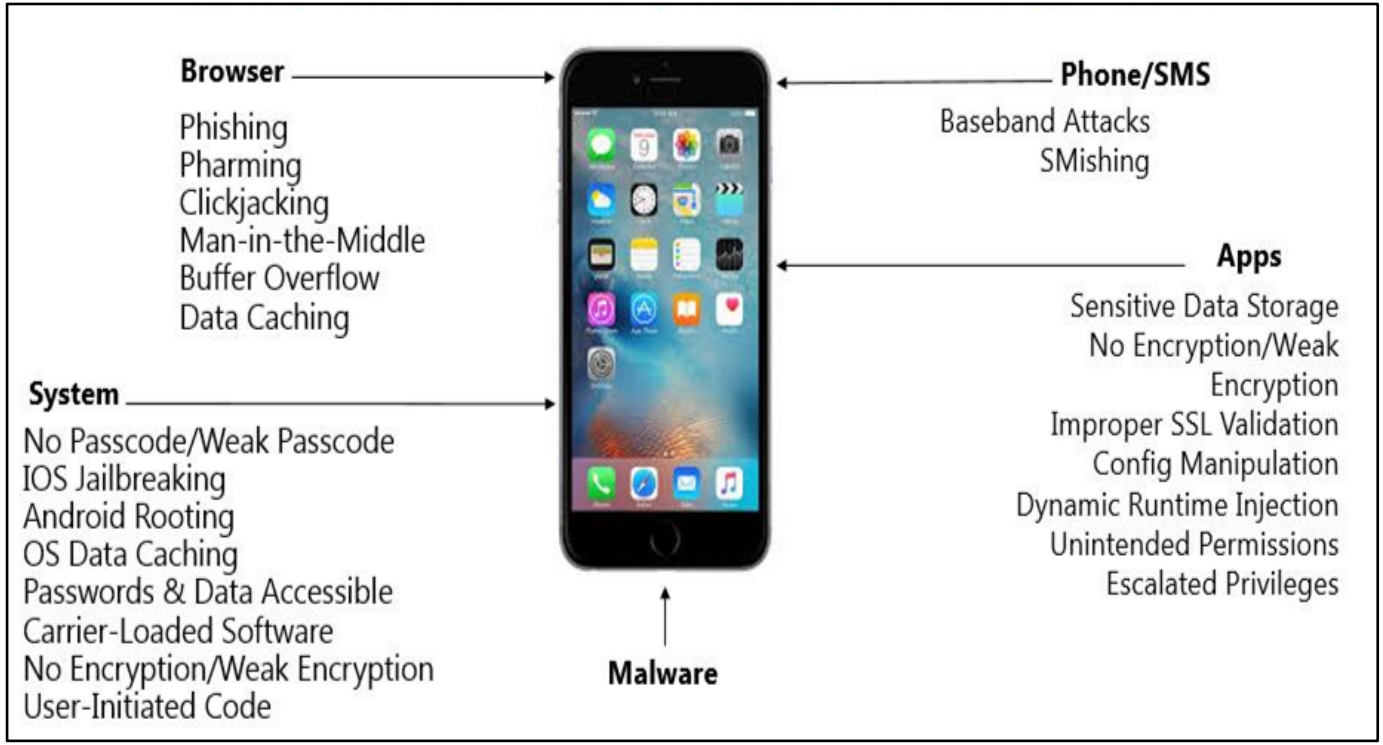
Device Security Group

- Be the centre of expertise on mobile and IoT device security
- Identify, classify and work to address common device security issues
- Tackle cross-platform and cross-sector security issues
- Address end-to-end device ecosystem aspects
- Monitor and respond to reported emerging threats
- Build relationships with device security experts and key stakeholders
- Maintain and develop materials on mobile and IoT device security
- Develop industry standards & recommendations/best practices as needed
- Liaise with relevant external standards bodies
- Promote and communicate the importance of device security
- Promote the use of the IMEI Database to share stolen device data

Trust in a Complex Environment

Reputation

Maintain industry reputation and trust in mobile operators and services



Need for Mobile Device Security Transparency

- Data shows that consumers & enterprises both care about built-in security & upgradeability
- Consumers rate security validation as a top 2 purchase driver across all age ranges
- Enterprises rank security & security updates as their top 2 purchase drivers
- Both stakeholder groups need transparency in order to make purchasing decisions

Too little?

Just right!

Too much!

Existing Device Security Enablers

- BSI – OEM Requirements for Smartphone Security – catalogue of OEM requirements describing basic device equipment and implementations for secure operation
- NIAP/NIST Mobile Device Fundamentals – certification specification to evaluate how devices defend against real world threats
- ETSI EN 303 645 / TS 103 701 – describes how conformity assessment is performed in a structured way, applies to IoT devices

Google Work Item Proposal to DSG

- Explore feasibility of a mobile device security certification scheme to address the following
  - Current lack of understandable information about device security capabilities
  - No independent security certification programs focused on consumer mobile devices
- Proposal is to develop a scheme to present security capabilities in a ‘nutrition label’ to increase transparency and facilitate benchmarking
- Overall objective is to raise the security bar with a focus on privacy, lifecycle support and data protection
- ETSI TS 103 732 Consumer Mobile Device Protection Profile to serve as the security requirements specification
- Scheme likely to be well received by stakeholders looking for devices to support sensitive applications

GSMA Mobile Device Certification Working Party

- Proposal, as a certification activity, falls under GSMA AA.35 and approval will be necessary for enabling work to be undertaken
- Working party established to identify and develop enablers required to establish and support a mobile device security certification scheme
- Two work streams running concurrently with weekly calls;

Technical	Business
Gap analysis of TS 103 732	Market assessment
Define assurance levels	Consumer research
Define lab requirements	Scheme set up and ongoing costs
Define ‘nutrition label’	Scheme funding
Define directory requirements	Legal structure

- Participation open to all

Certification Scheme Needs

Potential to Leverage Existing Capabilities

Missing piece

3 ETSI does not have a certification scheme by design

ETSI TS 103 732

2 In November 2022 ETSI launched a Consumer Mobile Device (CMD) Protection Profile (PP) as a Test Specification

The CMD PP is a fairly low bar that every GMS device should pass. As a result we would propose creating an Advanced Assurance Annex (AAA)

ETSI EN 303 645

1 Designed to prevent large-scale, prevalent attacks against smart devices that cybersecurity experts see every day. Supports a good security baseline for connected consumer products, provisioning a set of 13 recommendations. **Provides a basis for future certification schemes.**

ASAP Android Security And Privacy

Synergies with Existing Resources

- Use of ETSI TS 103 732 protection profile that defines security requirements – similar to NESAS use of 3GPP SCASes
- Use of NESAS test laboratory competency criteria and accreditation by ILAC member national accreditation bodies in accordance with ISO/IEC 17025
- Use of eSA model for the appointment of certification bodies, relationships between stakeholders and governance of their activities

GSMA Mobile Device Certification Progress

- Competitive landscape analysed and need for dedicated scheme identified
- Presentations received from complementary schemes such as SESIP, PSA, NESAS, eSA, etc.
- Gap analysis of TS 103 732 completed and changes proposed and submitted to TC CYBER
- 3 assurance levels defined
- Lab accreditation requirements documented
- Certification principles drafted
- Consumer survey outline presented

Competitive Landscape Review

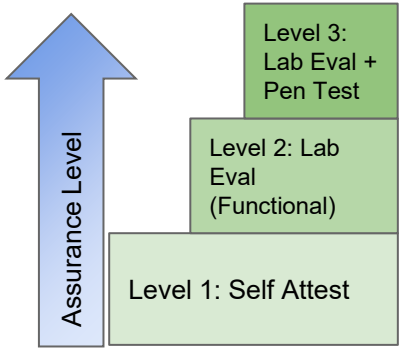
Competitive landscape can be broken up into 3 buckets:

- Smartphone specific certification schemes
- IoT Product Certification schemes
    a. Country
    b. Industry
    c. Lab
- IoT Component Certification schemes

No scheme currently exists that meets work item goals

Assurance Levels

- 3 assurance levels proposed;
  - Level 1 – self attest
  - Level 2 – Lab evaluation (functional)
  - Level 3 – Lab evaluation and pen test



- Keep security requirements and assurance levels separate
- Similar to EU CSA levels (Basic, Substantial, High) but not a 1to1 mapping
- Allow OEMs to choose if they want to also evaluate against a national scheme
- Will investigate how to use component evaluations to streamline efforts (e.g. PSA & SESIP)

Test Lab Requirements

- Requirements and standard against which accreditation is to be assessed documented
- Model adopted by NESAS will be re-used – fundamental requirement is that the lab must be ISO/IEC 17025 accredited
- Security objectives, test lab assets and threats, competency criteria and accreditation process defined
- Test labs must demonstrate their technical competence, and that of their personnel, to execute the role
- ILAC outreach will be undertaken to ensure MDCERT is understood and that accreditation can be achieved

Certification Principles

- High level certification principles documented
- Model adopted by eSA will be adapted for re-use – fundamental requirement is compliance with ISO 17065
- Certification body role and responsibilities defined, covering certification activities, test lab licensing, test lab alignment, etc.
- Certification process described – three phases – submission, evaluation and certification
- Certification methodology document to be created to provide more detailed description and guidance
- Certification validity periods and triggers to be further discussed and finalised

Other Scheme Enablers

- Scheme set up enablers identified – marketing resources, branding, website/directory, operational support
- Scheme funding has been discussed and is under consideration by GSMA Managed Services
- Contractual relationships, dispute management and certification support needs identified
- Directory requirements being defined – what to publish, who can publish, who maintains, active vs historic lists, discrepancy remediation, etc.
- ‘Nutrition label’ design to be discussed and drafts produced for consideration

Consumer Research

- Research proposals presented by Google to survey consumers and key opinion formers
- Targe groups include consumers, tech press, general press and policy makers
- Markets and sample sizes are being worked on – likely to include NALA, MENA, APAC, China
- Seeking to identify;
  - Goals and priorities
  - Pain points and frustrations
  - How we can solve their problems
- Question formulation ongoing

Conclusion

- Need for an independent mobile device security certification scheme is recognised
- Opportunity to develop and provide a one stop location and single source of truth
- Scheme will deliver information and demonstrable value for mobile device users
- Scheme should avert the emergence of isolated and fragmented national approaches
- Current work is drafting a proposal that will ultimately require GSMA ISAG approval for any scheme to be developed

Participants welcome – email jmoran@gsma.com


QUESTIONS?