Mavenir Keynote

Think Smarter – Secure communication
Innovate Services

By Mohamed Issa
Regional Head of Africa Sales
The “New” Mavenir: Combining Market Leaders

Combining three industry-leading companies to establish a key player in evolved, cloud-proven networking solutions

Innovate: Transform: Succeed
The “New” Mavenir: **Snapshot**

- **350+** Carriers
- **17** of **top 20** TIER 1 CARRIERS GLOBALLY
- **3+ BILLION** Mobile Subscribers
- **150+** COUNTRIES
- **10 BILLION** Monetization Requests Annually
- **2,200+** EMPLOYEES Worldwide
- **37%** Share of VoLTE / VoWiFi in the U.S. and Canada
- **71%** Share of VoLTE / VoWiFi in France, Germany, UK
- **75%** Share of RCS in the U.S. and Canada
- >**50%** Share of global messaging

**Industry’s LEADING TECHNOLOGY**

With World’s First VoWiFi, VoLTE, and RCS

**Leading VoWiFi / VoLTE, RCS and Messaging RCS Market Share**

Source: Based on GSMA, GSA, TeleGeography and Mavenir (July 2016) – Number of launched Mobile operator networks "LTM as of q3'16."
Mavenir’s Innovative Market Firsts

VoWiFi
- World’s first Commercially deployed IMS-based VoWiFi
- Fully supported mobility between LTE<->VoWiFi

VoLTE
- World’s first Commercially deployed VoLTE
- World’s first Commercially deployed fully virtualized VoLTE network

RCS
- World’s first Commercially deployed RCS5 solution
- World’s first Commercially deployed fully virtualized RCS network

Messaging
- World’s first Commercially deployed SMS
- Solutions handling nearly half of the world’s text/multimedia messages

Multi-Line Multi-Device
- Disruptive Network-based solution using the carrier as a platform for innovation.
Strategy and Solution Details
Mavenir’s Key Solution Areas

5G
- NFV/SDN Optimized Network Elements
- 5G Capable Core Network
- Mavenir Cloud Range MANO (Management and Orchestration) Suite
- Mavenir SmartC-RANTM Solution

IoT
- Core and Access Infrastructure Provider
- IoT GW (w/Partner)
- Vertical Use Case Solutions (Elder Care, Connected Car)
- NaaS (Network as a Service)

Advanced Communications
- Voice, Video, Advanced Messaging Products
- Multi-Line, Multi Device Service Delivery
- Continued Service Innovation
- Innovative Platform for Service Providers (Open APIs, SDKs)

Security
- SS7 Firewall & Diameter Firewall - Signaling Security
- SpamShield - Spam & Fraud Control
- SBC (A/I SBC Products) – Session Border Controllers for Access and Interconnect
- Security Gateway – RAN <-> Operator Core Link
Security

- Mavenir’s security solutions are built to protect CSPs’ networks from sophisticated security threats. Mavenir’s highly efficient and topographically independent solution, provides 360-degree security and privacy protection, addressing many types of signalling network attacks, as well as spam and fraud exploits, providing advanced, real-time detection of malicious traffic alongside smart prevention mechanisms. Mavenir provides complete control to mobile operators over the messaging stream, signalling interfaces, and borders of the network.
Revenue leakage

- Devices are stolen in the other countries
  - Usable after hard reset
- No import tax is paid
- No tax is paid by the selling entity
- No taxable after sales/support business
- Better mobile network usage
Securing the mobile world

- Prevent Mobile phone crime and phone smuggling
- Secure mobile communication, and guarantee high quality service
- Creating New revenue streams to governments as well as attracting foreign investments via enabling fair competition
Governments Worldwide Are Losing The Battle Against Smartphone Theft

02/21/2014 04:59 pm ET | Updated Jan 25, 2014

Welcome, Guest!  Sign In/Nairaland | Search | Recent | Your
Meta: 1,462,618 members, 2,796,485 topics. Date: Friday, 15 April 2016 at 08:56 AM

Nairaland Forum
Nairaland Forum / Science/Technology / Phones / Most Stolen iPhones Are In Africa (955 Views)
SHOCKING: iPhones Are New EXLIBRIS! / The Modestious Success Of Apple iPhones - Why iPhones Are So Popular? / Apple Set To Launch Kill Switch For Stolen iPhones (132,142 @ 14)

Most Stolen iPhones Are In Africa - Phones - Nairaland
Nairaland Forum / Science/Technology / Phones / Most Stolen iPhones Are In Africa (955 Views)
Most Stolen iPhones Are In Africa by Adeniyi008 || 23Apr '10 at 02:37 PM

How To PLACE TARGETED ADS on Nairaland
How To PLACE TARGETED ADS on Nairaland

How To PLACE TARGETED ADS on Nairaland

How To PLACE TARGETED ADS on Nairaland

How To PLACE TARGETED ADS on Nairaland

How To PLACE TARGETED ADS on Nairaland

Most Stolen iPhones Are In Africa by Adeniyi008 || 23Apr '10 at 02:37 PM

Ever since cell phone carriers created a national registry of stolen phones on Nov. 1, it's become much harder, if not impossible, to reactivate one in the U.S. That's the good news. Here's the bad: The database isn't likely to rob thieves of the desire to steal your phone.

All major U.S. cell phone companies, including Verizon (VZ), AT&T (T), T-Mobile, and Sprint (S), are now sharing the serial numbers of stolen phones through the registry. If your SIM numbers on cars, these unique IDs are branded onto the hardware of the device and are hard to tamper with. If a thief has to pop out a SIM card and use a phone purchased from one U.S. company to sign up for service with another, the serial number will automatically show up as belonging to a stolen phone. Courtesy ecmtm:

The WCO and GSMA signed agreement to combat mobile device fraud

The WCO and GSMA signed an agreement to collaborate in the fight against the counterfeiting and fraudulent trading of mobile devices. The partnership will focus on the integration of the GSMA’s mobile device database with the WCO’s IPM mobile platform that will allow Customs officers global real-time product information and enable them to assess the authenticity of device shipments on their own.

"The trading of counterfeited mobile devices is a global issue that has a number of严重的 consequences in its victims such as safety concerns related to the release of substandard devices as well as on impact on the reputation and revenue of right holders," said John Hofman, CEO, GSMA Ltd. "This collaboration with the WCO will allow Customs officers to access the most accurate information available on bona fide phones data that will help in the fight against the trade of counterfeit devices."

The GSMA admits the allocation of IMEIs via Type Approval Codes (TACs) and earns the world’s authoritative database of registered devices. The WCO’s IPM web and mobile platform is a global security gateway that allows Customs officers to verify the authenticity of products online. It also allows manufacturers or right holders to share relevant product information which is made available in real-time to Customs authorities that can add this information to their consignment checking procedures.

"The integration of the GSMA’s database into our IPM platform is an important step in the fight against counterfeit and illicit bauded mobile devices. We are very proud to be able to work in partnership with GSMA as well as manufacturers of mobile devices, making available to Customs officers around the world, through our IPM platform, information and product details that can effectively assist our day-to-day operations," said Kurtis Mikampe, Secretary General of the WCO.
The challenge

- Big brands regulate prices for the new handsets
- Phone smuggling becomes a big business
- Increases crime, Phone thefts
- Revenue leakage due to customs avoidance and Smuggling
- No support for the smuggled devices – risk to consumers

Standard 3GPP operator solutions do not help!

- Mobile crime has become a serious problem that needs to be tackled!!!
XURA approach - *Monetising Security*

Structural solution to the problem on all levels

- Regulation and the law
- Technical enforcement
- Financial benefit
An IMEI check is initiated by the network for:

<table>
<thead>
<tr>
<th>Mobile originated short message</th>
<th>Supplementary service operation,</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile terminated short message</td>
<td>Location update with a new visitor</td>
</tr>
<tr>
<td>Location update/periodic location update</td>
<td>Mobile originated voice call</td>
</tr>
<tr>
<td>Emergency calls</td>
<td>Mobile originated data call</td>
</tr>
<tr>
<td>IMSI attach</td>
<td>Mobile terminated voice calls</td>
</tr>
<tr>
<td>Mobile terminated USSD (Unstructured Supplementary Service Data),</td>
<td>Mobile terminated data calls</td>
</tr>
<tr>
<td></td>
<td>GPRS/Data attach</td>
</tr>
<tr>
<td></td>
<td>GPRS/Data PDP context create</td>
</tr>
<tr>
<td></td>
<td>SMS delivery over GPRS/Data</td>
</tr>
</tbody>
</table>
Registration and Grace Period

When switching on the handset for the first time, and if the handset was never registered, a notification will be sent by the system to the subscriber to inform them about the necessity to register the phone to be able to continue using the handset, and the handset is then given a temporary access.

- **White List**: containing all IMEIs whose type has been approved
- **Black List**: containing all IMEIs that are stolen, illegal or otherwise faulty
- **Grey List**: containing IMEIs that in grace period
Benefits

**Subscriber**
- Guaranteed quality of the equipment
- Protection against theft
- Less crime and more safety
- No fake premium phones

**Government**
- Additional tax income
- Import tax protection
- Allowing fair competition by eliminating Grey market
- Attract foreign investments from global brands,
  - Civil safety

**Operator**
- Protection for equipment sale revenue
- Better service quality with elimination illegitimate handsets
- Known equipment on the network
Signaling Security challenges

Exposing Signaling is **Necessary**
- Global Communication between subscribers on different networks
- Roaming
- Vulnerabilities Exist
- Evidence of Malicious Activity

Network Evolution is **Inevitable**
- NFV
- LTE, IMS, VoLTE, RCS
- IoT and SDN
- Growing risk of Harmful Accidental Signaling

**Signaling Security Is Essential**

SS7  →  Diameter  →  SIP
Our Signaling Security Solutions

**Understand**

What vulnerabilities does your network expose?

**Monitor**

How do others interact with your network via signaling?

**Vulnerability Audit**

Understand which vulnerabilities your network exposes

**Offline Signaling Analysis**

See potential external threats reaching your network

**Passive Monitoring**

Automatic threat detection with powerful near-real-time analytics

**Active Monitoring**

Enhanced stateful and interactive detection rules

**SMART Support Service**

The Security Management and Response Team (SMART) Support Service
- provides periodic audits and analysis of signaling
- proactively alerts customers to new threats
- provides recommendations to address concerns.

**Maintain**

Leverage expert services to maintain and enhance network security

**Enforce**

Implement a solution to enforce your signaling interaction security policy

**Active Filtering**

Full firewall to detect and block harmful signaling and prevent fraud

**Offline Signaling Analysis**

Automatic threat detection with powerful near-real-time analytics

**Vulnerability Audit**

Understand which vulnerabilities your network exposes

**Understand**

What vulnerabilities does your network expose?

**Monitor**

How do others interact with your network via signaling?

**Vulnerability Audit**

Understand which vulnerabilities your network exposes

**Offline Signaling Analysis**

See potential external threats reaching your network

**Passive Monitoring**

Automatic threat detection with powerful near-real-time analytics

**Active Monitoring**

Enhanced stateful and interactive detection rules

**SMART Support Service**

The Security Management and Response Team (SMART) Support Service
- provides periodic audits and analysis of signaling
- proactively alerts customers to new threats
- provides recommendations to address concerns.

**Maintain**

Leverage expert services to maintain and enhance network security

**Enforce**

Implement a solution to enforce your signaling interaction security policy

**Active Filtering**

Full firewall to detect and block harmful signaling and prevent fraud
Our Signaling Security Products

Monitor

- SS7 Firewall
- Correlation module
- Diameter Firewall
- SIP Firewall
- XA Analytics

Enforce

- Powerful, near real-time Monitoring and Analytics
- DISC
- SIP

Understand

- Signaling Security Expertise
- SMART professional Support services

Maintain

- SMART professional Support services
Mavenir Delivers on Key Criteria

<table>
<thead>
<tr>
<th>Our customers need</th>
<th>Only Mavenir delivers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure network operation</td>
<td>Expertise and Experience</td>
</tr>
<tr>
<td>Subscriber protection</td>
<td>Powerful Analytics</td>
</tr>
<tr>
<td>Fraud prevention</td>
<td>Fast, Safe Resolution</td>
</tr>
<tr>
<td></td>
<td>Powerful Protection</td>
</tr>
<tr>
<td>Core network stability</td>
<td>Proven Reliability</td>
</tr>
<tr>
<td></td>
<td>Flexible Integration</td>
</tr>
<tr>
<td>Maximum return on investment</td>
<td>Own Signaling Stacks</td>
</tr>
<tr>
<td></td>
<td>SS7, Diameter, SIP security</td>
</tr>
<tr>
<td></td>
<td>Intuitive Operation</td>
</tr>
<tr>
<td></td>
<td>NFV-ready</td>
</tr>
</tbody>
</table>

- Intelligence about network threats and how to mitigate them
- Quick reaction to protect against new threats without introducing risk to network operation
- A solution that has minimal impact on existing systems and introduces no new risk to core signaling
- Make one investment in a future-proof solution, with low operational costs
Messaging Fraud impacts subscribers, enterprises and operators

**Poor user experience**
- Inability to interact with the application
- Delivery failure when roaming
- Variability in delivery QoS

**Reduced network service availability**
- Subscribers in cells congested by SIM Boxes
- Roamers in networks connected via links congested by A2P messaging
- Subscribers calling/messaging others in networks connected via congested links

**Poor subscriber satisfaction**
- Poor A2P user experience
- Service availability problems
- Increased volumes of SPAM and malicious content enabled by low cost delivery

**A2P Messaging Revenue Loss**

Losses from SMS fraud up to $6 Billion annually
Communications Fraud Control Association, 2016
Our Spam and Fraud Solutions provide 360° cover

- “Open” Messaging Centre
- Spoof Home Subscriber
- SIM-Box or Relaying App On-net
- SIM-Box or Relaying App via Grey-Route
- Application connected via Grey-Route
- Fake Messaging Service Centre

Control Every Route

- Complex Indeterminable Rules
- Rapid Evolution of Detection Rules
Machine Learning and Rule Evolution are Key Differentiators

- **Determinable Rules**
  - New bypass techniques emerge
  - Revenue Loss Continues
- **Complex Ever-changing Rules**
  - New bypass techniques almost IMPOSSIBLE
  - Revenue Loss Stopped - Quickly & Effectively

- **Delay**
  - More traffic bypasses

- **Manual Rule Definition**
  - Manual + High-cost
- **Manual Traffic Analysis**
  - Complex variations (sources and content)

- **Complex set of rules required**
  - Dynamic Complex Rule Evolution
  - Automatic

- **Real-time Machine Learning**

- **SpamShield**

- **Traditional Methods** vs **SpamShield**

- **Control Every Route**
  - Complex Indeterminable Rules
  - Rapid Evolution of Detection Rules

- **Revenue Loss Continues**
- **Real-Time Analysis**
  - Stops Bypass FASTER

- **Delay**
  - More traffic bypasses
Innovation
#catalystforinnovation