Volume 08, November, 2017

A SAMENA Telecommunications Council Newsletter

www.samenacouncil.org

SAMENA TRENDS

EXCLUSIVELY FOR SAMENA TELECOMMUNICATIONS COUNCIL'S MEMBERS

BUILDING DIGITAL ECONOMIES

Exclusive Interview 08

The Next Generation of Service Providers 34

Exclusive Interview

H.E. Eng. Salim Al Ozainah

Chairman & CEO

CITRA

THIS MONTH

REGIONAL PERSPECTIVES ON THE IMPACT OF TAXATION BOTTLENECKS IN TELECOMS

ARTICLE

Mobile Security, an Opportunity for Mobile Operators

The Challenge

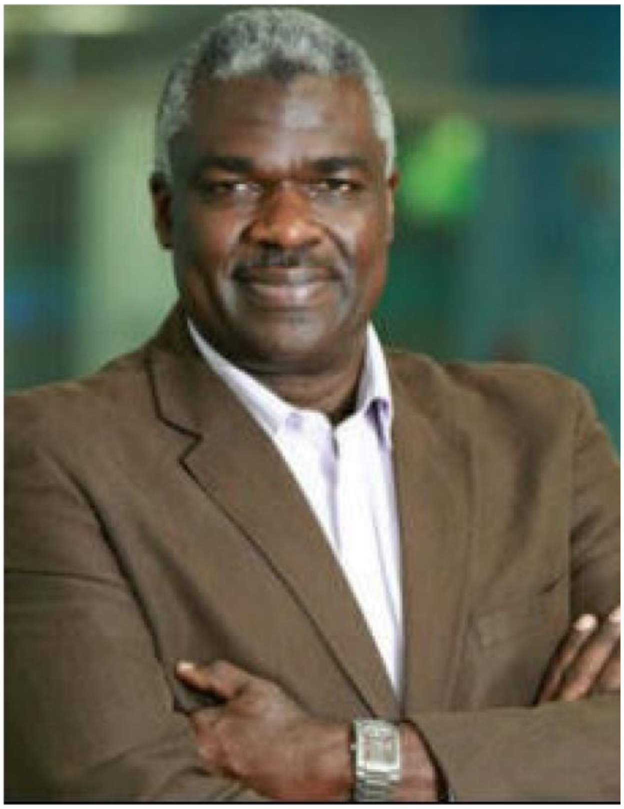
One word is on the mind of all CISO's and CIO's globally – Security! In a world rapidly moving towards ever greater interconnectivity, with 5G on the horizon and IOT becoming a reality, security is at the forefront. How do we become more open and retain security? How do we share more data and expose more end points and link our digital world yet still remain secure? How do we prevent this unleashed data from being abused and misused? What role can or should Mobile Operators play and what stake should they have in securing this interconnected future?

Cyber-attacks are increasingly threatening and costly. Studies show that they drain $450 billion annually from the global economy—a number that some project will reach $2 trillion by 2019.

Cyber-attacks are increasingly threatening and costly. Studies show that they drain $450 billion annually from the global economy—a number that some project will reach $2 trillion by 2019. Highly sophisticated attackers can hide their tracks for weeks, months and even years without being noticed.

Many enterprises manage device access to corporate resources, networks and identity, but they can't remediate a threat they can't identify. As more of our computing goes directly from mobile devices to cloud services, network threat detection solutions are ineffective since data often resides outside the corporate data center. Adoption of a non-signature based mobile threat detection software to protect your organization and its data is required. This fact is a serious and growing concern for all CEOs and CIOs.

Allowing employees to use their own devices can certainly improve productivity, but it also puts the organization at risk for additional security threats. Whether these devices are sanctioned or not through a corporate BYOD program, IT departments need to grapple with setting unified policies especially when it comes to securing mobile devices and the information they access.



Shuaib Mahmud
Chief Executive Officer
Staxx Solutions

Staxx Solutions

Security on the mobile device can be segmented into 3 principal areas:

- Device management, for policy enforcement, corporate application access and data segregation
- Threat detection
- Secure voice and messaging
- Addressing all three components provide a significant level of security that ensures that CIO's and CISO's are able to rest easy.

Mobile Security – The Opportunity

As Mobile Operators, the opportunity to move up the value chain for enterprise, consumers and prosumers means the delivery of critical value-added services. Identifying the right services will be essential to driving revenues, increasing profitability and reducing churn as technology continues to rapidly evolve. It is expected that mobile security spending will rise over the next 5 years reaching $73.5 billion a year as threats and losses continuing to increase globally.

Security is one of the essential areas in which Mobile Operators can play a key role. Becoming a key service provider in this area broadens the service portfolio and provides significant tangible value to customers in an area that is set for significant growth.

It is expected that mobile security spending will rise over the next 5 years reaching $73.5 billion a year as threats and losses continuing to increase globally.

Mobile Device Management: This area of security is probably best left to enterprise customers to manage through their internal IT, as policy rules, changes and end-user management could become more costly than it is worth for most operators to manage as a service. MDM products such as MobileIron offer a wide range of EMM solutions for enterprise.

Mobile Threat Detection: While managing employee devices doesn't make sense for every organization, securing devices does. Gartner recommends that security and risk managers, "Propose installation of an MTD product in situations where BYO users are unwilling to allow EMM supervision on personal devices". A logical provider of MTD is the mobile operators, offered as an enterprise service with a nominal per user monthly charge or direct to consumers as a package service for a nominal monthly fee. Gartner predicts that, "By 2019, 25% of mobile-ready enterprises will deploy mobile threat defense capabilities on enterprise-issued mobile devices". Key Enterprise customers include Finance, healthcare, energy, and government sectors.

Given the current mobile landscape, it is clear that the threat is real. Take the ongoing BankBot malware attack that is focused largely on Middle Eastern banks and their customers. BankBot is Android-targeting malware that uses fake overlay screens to mimic existing banking apps and steal user credentials. BankBot and other exploits aren't going away anytime soon, in fact they are increasing every single day. To ensure enterprise customers stay secure, operators should partner with mobile security companies like Zimperium that offer continuous, real-time cyber threat protection for both mobile devices and applications.

For a relatively small fee customers can have the peace of mind that their devices are fully protected wherever they might be. Products offered through Zimperium, the global leader in mobile threat defense (MTD) and the only provider of real-time, on-device protection against known and unknown threats, provides its z9 product for Mobile Malware. In addition to its proven effectiveness against zero-day device and network attacks, z9 is the only machine learning-based engine capable of detecting previously unknown mobile malware on-device without the delays and risks of cloud-based lookups. Zimperium provides the most integrated and scalable mobile threat defense platform. The solution delivers real-time, on-device threat detection for Android and iOS devices. To date, Zimperium's machine learning-based engine, z9, has detected 100 percent of zero-day mobile exploits without requiring an update. z9 protects devices and their data via the zIPS™ mobile Intrusion Prevention System app, and mobile apps and their sessions via zIAP™, the In-App Protection SDK.

Encrypted voice and messaging services are a concern of not just operators, but also a serious national security concern, as bad actors use these unregulated and unrestricted means to communicate globally and evade law enforcement and intelligence agencies.

The number of post-paid customers can be used as a yard-stick to determine the potential uptake of this service by consumers. The hurdle for enterprise customers is much lower as the inherent risks of BYOD users is already apparent and of growing concern, Financial services firms with mobile banking applications see MTD as a means to safe guard their customers and protect them from losses. MTD as a driver of revenue could be significant for operators seeking new value added services that are income generating.

Secure Voice & Messaging: Third party OTT VOIP applications enable smartphone users to talk and chat with one another with greater ease and near global coverage as long as the users at both ends of the connection use the same application. While these applications drive additional data consumption, from the operators perspective, the incremental data usage revenues do not make up for the erosion of traditional minutes revenue. Popular VoIP apps, such as WhatsApp, are free for download and use. The operators do not generate revenue from selling or using the service. Encrypted voice and messaging services are a concern of not just operators, but also a serious national security concern, as bad actors use these unregulated and unrestricted means to communicate globally and evade law enforcement and intelligence agencies.

OTT's that provide these services are reaping benefits by monetizing data or charging fees for the services that typically bypass the operator. There are certainly legitimate reasons for encrypted communications at an enterprise level and within governments. Conceivably this is where regulatory bodies should step in requiring non-enterprise VOIP services to be un-encrypted as the uncontrolled use by parties capable of terrorism and other nefarious activities can be coordinated globally evading law enforcement.

How do Operators benefit from secure communication? By offering secure voice and messaging as a service to enterprise customers. KoolSpan has partnered with several Operators around the world to develop service offerings of secure mobile communications for both voice and text. Operators offer these solutions initially to their business-to-business (B2B) customers, including government organizations, enterprises and even small and medium sized businesses (SMB). As demand accelerates, several leading carriers are also rolling out "prosumer" and consumer secure communications service offerings. The result? The operator is perceived as a Trusted Security Service Provider.

While secure communications services vary slightly from one to the other, they share a common foundation of end-to-end (E2E) encryption. However, KoolSpan's high definition (HD) audio quality and robust performance across a wide range of network environments exceeds the quality and performance of both regular calls and all other VoIP calls, so that users who are not satisfied with their free, "you-get-what-you-pay-for" app are willing to pay a nominal fee for KoolSpan TrustCall. End users are replacing WhatsApp with TrustCall because of the security and quality advantages.

Operators that build "value-add" packages around secure mobile communications can open up additional business and revenue streams as customers return for additional security services.

From a government security risk and compliance perspective, it is known which enterprises have deployed TrustCall, additional regulations could be applied to ensure each enterprise is vetted by authorities and approved for encrypted communication and messaging. The end result will be a profitable business for Operators, working fully in compliance with the requirements of government regulators.

Operators that build "value-add" packages around secure mobile communications can open up additional business and revenue streams as customers return for additional security services.

Bottom line, delivering services like MTD and TrustCall secure voice and messaging to B2B customers helps operators as they change their business model so that not only does it drive direct higher ARPU, but it also enhances the trusted provider relationship for operators with their customers, leading to multiple new revenue streams. Key points for operators to consider:

- Secure voice and messaging for the business market is an innovative service that provides new revenue streams
- MTD is a rapidly growing area of need in the Security space
- Adding security creates a strong competitive advantage
- Protecting confidential information exchanges brings new customers from competitors, reduces churn, and increases customer satisfaction

Contributors:
Nigel Jones, CEO Koolspan Inc.
JT Keating, VP of Product Strategy
Akhil Bhutani, GM of Middle East & Africa, Zimperium

References:

1. http://www.welivesecurity.com/2016/02/19/averagecost-cybercrime-rises-200-just-five-years/
2. http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-trillion-by- 2019/#421e63773bb0/
3. http://kbvresearch.com
4. http://bit.ly/2jlDgbt/ "How Telcos beat the Voice Minute Consumption Model"
5. http://Zimperium.com "Zimperium Announces World's First On-device Detection of Undetected Mobile Malware