A Big Win/Win: Protecting Mobile Users While Boosting Revenue:

The Benefits of Providing a Real-Time Cloud Service in Malware Threat Protection for Consumers & SMBs

By Dan Baker, Technology Research Institute (TRI)

Sponsored by, Allot Communications

The mobile business has probably never been tougher. Operators today are being hit by challenges from all directions:

- Costly LTE and bandwidth rollouts have been great for users, but have not contributed to big revenue gains;
- Traditional voice, SMS, and other IP services are steadily being gobbled up by OTTs;
- Profitable roaming charges are now being undercut by regulators in some regions; and,
- New mobile and OTT competitors continue to enter the market.

Service Selection: Network Technology vs. Value Added Services

So how can operators win in today's brutally competitive climate?

Well, I think the strategy is no different than it's been in the past. The winning operators are the ones who choose and deploy compelling services that boost revenues and profits.

Now "compelling service" is obviously a moving target. A service that's a star today may be a dog tomorrow. Look at mobile's history: voice mail, ringtones, call forwarding, 2G and SMS. Each of those services had its day in the sun, and then faded. Some services died because they lost their value or went out of date. Other services became universally available, and therefore lost their power to differentiate and generate revenue.

Having a winning service is also a matter of timing: if you can deploy LTE one year before your competitors, that's a great advantage. However, if you're not careful or your timing is wrong, you could deploy expensive network before consumers are willing to pay for it. And that could spell big trouble.

To be sure, the choice of network technology (3G, LTE, etc.) varies greatly by market. In some regions of the world, 3G is a relatively new service. And we can expect the strongest carriers to be the first to deploy advanced networks because taking the technology lead is their strategy.

The reality, of course, is that investments in network technologies are planned years in advance. And in the near term, the only place where product marketers have real power to boost revenue is in **value added services**.

But there's a problem here too. Since most value added services are IP-based today, they are quite vulnerable. OTTs are quite adept at replicating and more cheaply delivering just about any "killer IP service" a mobile operator dreams up.

So this raises the fundamental mobile operator need for value added services that are useful, sticky, and can't be easily knocked off by the OTTs.

The Opportunity in "Real-Time Cloud Services"

Increasingly, I feel, mobile operators will turn to the cloud to find compelling services. Now I hasten to add that by "cloud," I'm not referring to plain vanilla cloud computing such as Amazon AWS and Microsoft offer.

Rather, the best cloud opportunity for mobile operators is in **real-time cloud services** that leverage a mobile operator's unique capability to perform in-line network analytics, and then react to events through network policy.

Such in-line cloud services are now emerging in applications such as: content caching at the mobile edge, mobile device security, and enterprise service assurance. And no doubt, many others applications are coming soon.

Now in this paper I'm going to discuss one such real-time cloud service in depth: **mobile user security**. This is a proven cloud service that is already widely deployed at several global operators:

Network In-Line Malware Blocking and Web Surfing Protection for Consumers and Small/Medium Businesses

It's instructive, I think, to look at this service – not just for the many benefits it brings to the problem of malware protection – but as **representative** of many real-time cloud services to come. These services are very well suited for the unique capabilities mobile operators bring to the larger communications ecosystem.

So let's discuss Security as a Service: what the service entails, the nature of the security threat, its benefits, and the advantages it brings to the operator.

An Attractive Real-Time Cloud Offering: Mobile Security as a Service

To begin, Security as a Service enables mobile (and fixed) operators to provide anti-malware protection through a network in-line service powered by Deep Packet Inspection (DPI).

Leveraging the intelligence and threat signature databases of leading security firms, the service protects the mobile users when they surf the web or use data services. Designed to serve enterprise, Small Medium Businesses (SMBs) and consumers, it blocks all kinds of malware that can damage mobile devices and cause the loss of personal content. The service also delivers powerful anti-virus and anti-phishing capability for email (SMTP, POP3, IMAP) and web traffic.

The service includes Parental Controls that assure child-safe browsing: parents determine the websites and content that their children can access, as well as the hours and amount of time they spend online.

In a moment, I'll discuss this value-added service in greater detail, but first, here's a quick rundown of its benefits:

- It attacks a growing problem: mobile security -- Mobile phones are increasingly vulnerable to cyber-security attacks. The service blocks malware attacks and also gives parents and businesses extensive control over web surfing.

- The time is right for 24/7 mobility protection – We live in a world where mobile users are constantly on-guard. As people move their banking and work lives to smartphones, their fear of viruses, phishing, bank fraud, and children being bullied has intensified. Even regulators welcome a simple and economic way to protect consumers and SMBs – it's the socially responsible thing to do.

- The service protects the user transparently -- The security service is a zero touch solution: the consumer or business user never has to fuss with manual updates or download because the operator takes care of that in the cloud. What's more, no IT expertise is required to manage the service.

- **It better guarantees user satisfaction while lowering on-going costs –** Security problems can be deadly to customer loyalty and satisfaction. By ensuring users have good protection, you avoid later headaches and reduced costs from people contacting your call center to get help. An ounce of prevention is worth a pound of cure.

- **It's a money-maker –** Through a multi-tenant capability that scales to millions of mobile users, the service can deliver a very profitable service. For the operators who have deployed the service thus far, the uptake is generally in the 15 to 20% of subscribers range.

- **It's economical to maintain –** Being an in-line cloud service, the service can be efficiently maintained and kept up-to-date with the latest malware signatures and website categorizations.

- **It offers keen operating advantages over device-resident software –** Maintaining security in the cloud means it doesn't degrade the mobile experience or tax the battery and there's no need to download security updates.

- **It's future technology friendly –** The service is not limited to mobile phones alone and can be extended to any device that contains a browser. What's more, vendors are delivering SDN/NFV compatible integration.

- **It is essentially OTT-proof –** Being a real-time, in-line network service, malware protection is delivered exclusively by the operator itself rather than an OTT.

OK, those are the many advantages of this in-line security service. Now let's discuss some of these issues in greater detail. Let's begin by discussing the cyber security threat itself.

The Cyber Security Threat in Mobile

Cyber security is a well-known issue on personal computers, and it's now steadily migrating to become a big issue on mobile devices as well.

Alcatel-Lucent's Motive Security Labs estimates that in 2014 a total of 16 million mobile devices worldwide were infected by malicious software – or malware. Finding malware infections in mobile devices increasing 25 percent over the previous year, the Security Labs also claimed that the high infection rates of Android devices alone caught up to Windows laptops as the "primary workhorse of cybercrime".

Some of the specific mobile user threats include:

- Downloading unprotected apps -- Apple and Google protect the apps that are downloaded through their app stores. But for browsing, there's no built-in protection on the mobile phone. What's more, if the phone is "jailbreaked", then it can download unsecured apps, games, and malicious advertising (or malvertising)

- Fraudulent phone calls to premium rate numbers – According to the anti-fraud association CFCA, the hijacking of phones -- to make premium rate calls at $10 a minute and more – costs telecoms $10.8 billion a year. Once criminals drop malware Trojans on the mobile phone, they make use of the conference calling feature in mobile phones to make, say, six simultaneous phone calls. Over a weekend, the charges can sometimes add up to $100,000 or more.

- Mobile banking fraud – In a 2013 mobile consumer study, Javelin Strategy & Research found "banking Trojans" to be the most prominent of mobile threat, making up 95% of mobile malware. The fraudsters' objective, of course, is to monitor SMS traffic and steal authorization codes and passwords to execute payments and money-transfers from user bank accounts.

- Future mobile technology threats – We can expect greater threats as new mobile technologies arrive. For instance, one emerging standard is Voice over LTE or VoLTE, an advanced means of transmitting mobile voice calls over data. However, researchers at Kaspersky Labs found that hackers can fool VoLTE and send ordinary data packets masqueraded as 'the high priority' signal or voice packets.

The Value of Zero Touch Mobile Security: Especially for Consumers & SMBs

As real as these mobile threats are, research suggests that mobile users are ill-equipped to manage the problem themselves. In fact, users are notoriously careless about security:

- A Ponemon Institute study commissioned by IBM found that 67% of large organizations allow their employees to download unverified, personal apps on their work devices.

- Gartner has also raised the alarm flag in a 2015 study. They say: consumer demand for security tools has "not yet emerged" and that endpoint protection software is "not a consistent practice" yet for most mobile platform users.

- Another issue is **outdated OSs for the device** in question. Updates are not always convenient or available – and users don't pay enough attention to ensure the updates are obtained.

In truth, this lack of security preparedness varies quite a bit depending on the category of mobile user. In general, we can say:

- **Large to medium sized enterprises are the most secure** because they have IT departments who manage security for a living;

- **Small businesses are vulnerable**: a typical firm of 100 employees or less has no professional IT or security person; and,

- **Individual mobile consumers are highly vulnerable** to malware attacks because many have no virus or malware protection at all.

Clearly the small business and consumer are the most at risk. And the beauty of a Security as a Service is ideal because it makes up for a mobile user's lack of knowledge or attention. The service runs completely transparent to the user. There's nothing the end user needs to install.

In this way, a security service has a big advantage over device-resident software and apps. All updates are done in the operator's network. The subscriber doesn't have to download an update file like as you would for anti-virus protection on a PC.

Another key benefit of security as a service is that battery usage and service quality is not affected.

A Money Making, Low Maintenance Service

There's no question that the market for mobile security solutions will grow – the sheer volume of mobile activity and the growing business use of mobile phones almost guarantees the need.

A 2015 **Silicon Valley Bank** report estimates that more than 1 billion employee-owned smartphones and tablets will be in the workplace in 2018. Gartner believes that by 2018, 70% of mobile professionals will conduct all of their work on personal smart devices.

So if there's money to be made in mobile security solution, the beauty of a cloud security service is that it enables operators to go after this business and win a big share of it.

Several operators today sell in-line malware blocking service as a premium offering. And because of the high perceived value of phone security, subscribers are willing to pay extra for it. One tier 1 operator with 10 million subs charges 1 to 1.5 Euros a month per subscriber for the service.

Once a certain threshold of users is achieved, the service is highly profitable. Operators who offer the service generally experience a 15% to 20% uptake of subscribers ordering the service.

The initial cost is generally not high because the solution runs on general purpose servers -- and those can be re-purposed for other uses. It's generally sold as a pay-as-you-grow service and some vendors even offer it on a revenue share basis, taking away almost all the financial risk.

The service is supplied by a Security-as-a-Service (SECaaS) vendor who maintains the content filtering database on its own. For anti-virus signatures, a license is obtained from anti-virus experts such as Kaspersky or BitDefender. In fact, the operator can choose to run multiple filtering engines.

Now in certain countries, such as the UK, the regulator actually requires all operators to deliver a content filtering service to mobile users. Generally, the consumer gets the service free of charge. And the service protects the mobile user from accessing content, such as – terrorist sites, illicit content, and the like.

Implementation is Easy -- and the Technology is Future Friendly

Security as a Service is designed for mass market service deployment. The service scales massively to millions of subscribers, and through multi-tenancy, it provides a personalized service for individual subscribers.

Complete with customized reporting and management capabilities, the service is integrated with back office systems. For instance, the service is inserted in-line in the operator's network and identifies customers via integration with CRM and the radio access network via DIAMETER.

The solution is completely software based, so there's no issue of obsolete hardware. And it's fully compatible with NFV and can be controlled through a service management or an orchestrator.

The service is also device agnostic. It doesn't matter what software version or brand of handset is used. In addition to mobile phones, it can also filter content for an XBox, a smart TV, tablets, and other devices. As long as the device browses, it can be protected. The platform itself is extensible, so if tomorrow you want to secure your IoT environment, you can have the platform extended to do that.

Conclusion & Recommendations

As we've seen, there's a lot to like in Security as a Service. It's an excellent fit for many mobile operators for a number of reasons. It serves a genuine mobile user need, it can profitably be offered at a low monthly fee, it offers zero touch convenience for the user, it is superior to device-resident software, and it's a sticky service that cannot be easily knocked off by an OTT.

What's more, Security as a Service is a sterling example of a real-time cloud service – a promising new category of value added services that mobile operators can really take to the bank.

As you scan the vendor market for Security as a Service solutions, here are some quick suggestions:

1. Choose the right type of supplier – Domain experience in security is important, of course, but experience in implementing, maintaining, and scaling a network in-line cloud service for millions of mobile users is even more important.

2. Investigate financing options – Suppliers are offering Security as a Service as either pay-as-you-go or shared-revenue models. A good supplier should be able to provide whatever you prefer: a low-risk or low-cost solution.

3. Security Reporting – Keeping full details about malware and attacks is key to fine tuning and improving an operator's service. Advanced SECaaS includes granular reporting and an ability to keeps tabs on what malware was blocked to whom and when, etc.

4. Personalization – In a security service equipped with multi-tenancy, security settings and URL filtering can be personalized. This feature is not yet common, but operators find it a highly desirable addition.

About Allot Communications

Allot Communications (NASDAQ, TASE: ALLT) is a leading provider of security and monetization solutions that enable service providers to protect and personalize the digital experience. Allot's flexible and highly scalable service delivery framework leverages the intelligence in data networks, enabling service providers to get closer to their customers, safeguard network assets and users, and accelerate time-to-revenue for value-added services. We employ innovative technology, proven know-how and a collaborative approach to provide the right solution for every network environment. Allot solutions are currently deployed at 5 of the top 10 global mobile operators and in thousands of CSP and enterprise networks worldwide.

About Technology Research Institute

Dan Baker is Research Director of Technology Research Institute (TRI), an analyst firm that has been following telecom software markets since 1994. Baker is editor of TRI's on-line magazine, Black Swan Telecom Journal. He also contributes to Pipeline, Vanilla Plus, and CommsRisk. For 21 years TRI has authored dozens of syndicated reports, its latest, a 239-page study entitled, Telecom Fraud Management Software, Services & Strategies.