# SMS Security

## Malicious attacks are just around the corner. Are you protected?

*This paper examines how operators can leverage monitoring and advanced security techniques to protect their mobile subscribers, network and business.*

TEKELEC

5200 Paramount Parkway
Morrisville, NC 27560 (USA)
1-919.460.5500 or 1-888.628.5527

www.tekelec.com

This page intentionally left blank

# *Introduction*

The mobile messaging market is growing rapidly and is a very profitable business for mobile operators. Today, text messaging is the most widely used mobile data service on the planet with 72% of all mobile phone users worldwide, or 1.9 Billion out of 2.7 Billion phone subscribers at the end of 2006, being active users of the Short Message Service (SMS). The quote below from Portio Research, a respected industry analyst firm covering the mobile messaging market, says it all.

> "SMS has proved to be the industry's most successful non-voice service. Globally, SMS is expected to remain the most widely used messaging format for several years to come. With the adoption of 3G and increased bandwidth, operators are expected to continue lowering SMS prices, resulting in greater use."
>
> Source: Portio Research, 2006

The profitability of mobile messaging is under attack. Mobile SMS spam, spoofing and other SMS-related scams are a global problem. There are many incidents of rogue operators gaining unauthorized access to the SS7 networks of major service providers and routing millions of text messages into those networks. Congestion of the network becomes a concern when there is a sudden flood of messages coming into the network from bulk messaging providers, rogue operators, or from legitimate traffic caused by radio or television promotions or voting events. Quite often they are attempts at delivering massive volumes of spam into the network. Service providers often end up building new facilities to deal with the increase in messaging traffic – with no corresponding increase in revenue. And with spoofing there is great opportunity for fraud - coaxing users into providing sensitive personal data, which results in a financial windfall for the bad guy. In fact, there have been reports of spoofing cases where messages are sent disguised as official government announcements for emergencies.

Even though nothing catastrophic has happened in the wireless world, things seem to be changing for the worse. Current trends in mobile devices are raising the probability of attack. Devices have much more functionality than they used to – they have become small computers. They are more connected than ever, supporting more communications protocols and even offering full-blown Web access. And there are tens of millions of them on every continent on earth – except for Antarctica of course.

New spam threats will evolve, as more advanced services such as multimedia messaging service (MMS) and mobile instant messaging start to grow in popularity. The most current threat comes in the form of smartphones. Several security holes have already been found in the popular iPhone, launched in July 2007. The main lesson from the iPhone hack is that it only takes one security hole to compromise an entire cell phone. Similar vulnerabilities have already been exploited in cell phones supporting the Symbian, Microsoft, and Blackberry operating systems.

Operators are demanding spam control and anti-spoofing capabilities to protect their SMS network and subscribers. However, with current short message service centers (SMSCs), when customers have complaints regarding SMS, operators have no way of addressing those concerns other than turning off SMS capabilities to those particular subscribers. This is clearly not good news for revenues.

This whitepaper discusses how operators can leverage monitoring and advanced security techniques to protect their mobile subscribers, network and business!

## *Mobile Security Threats*

There are many security threats to mobile subscribers and operators. It is easy to sneak a virus as a Trojan attachment in an SMS message. There are, of course, other common and not-so-common ways to attack mobile devices, including denial of service (DoS) attacks that blast multiple inbound messages and block outbound calling as well as the usual spam and spyware that is already migrating from PCs to phones.

Before diving into specifics, here are the GSM Association definitions (IR.70 SMS SS7 Fraud Paper, dated February 2005) for the various types of SMS fraud.

- **Spam:** Spamming is an action where the subscriber receives an unsolicited SMS. An unsolicited SMS is one the subscriber did not request to receive. The act of spamming does not define the content but only the fact that the SMS was received without solicitation. The content of the spam SMS is incidental to the act. The spam SMS may take on various forms of content to include: commercial information, bogus contest and other message generally intended to invite a response from the receiver.
- **Spoofing:** The spoofing case is related to an illegal use of the HPLMN SMS-C by a third party. In this case, an SMS MO with a manipulated A-MSISDN (real or wrong) is coming into the HPLMN network from a foreign VLR (real or wrong SCCP Address).
- **Flooding:** The act of flooding is when a large number of messages are sent to one or more destinations. These messages may either be valid or invalid. The value or parameter used to define flooding is the extraordinary number of messages sent.
- **Faking:** A fake SMS is originated from a foreign SS7 network and is terminated to a mobile network. This is a specific case when SCCP or MAP addresses are manipulated. The SCCP or MAP originator (for example: SMSC Global Title, or A_MSISDN) is wrong or is taken from a valid originator.

### *Using SMS for Fraud, Flooding and Other Attacks*

SMS is a wonderful service for both subscribers and operators alike. Used properly it brings great benefits and joy to the masses. Unfortunately, in the wrong hands SMS can be used as a weapon. For example, mobile originated (MO) spoofing involves the illegal use of an operator's SMSC network by a third-party. The weak link that permits spoofing is more of a protocol vulnerability. The current protocol used for these transactions is SS7, which was developed for use between two trusted domains. The industry has meanwhile moved to a more open model where many networks interconnect with one another, opening the opportunity for exploitation of protocol weaknesses, resulting in fraudulent abuse. The SCCP/TCAP protocol lacks any form of authentication of handshaking prior to accepting a transaction from another operator. The networks depend on a very rudimentary screening process within their gateways to prevent unauthorized access, but these screening applications are typically not robust enough to prevent spoofing.

The sections below discuss some of the mean-spirited uses for which unscrupulous individuals can use SMS.

### *Fraud*

Many fraudsters are tied to organized crime or terrorist cells - and they are using SMS fraud to fund their operations. This means they are very well funded, educated, and have the ability to deploy very sophisticated networks for the purpose of defrauding operators. For example, premium rate service (PRS) fraud is where the subscriber pays a higher than normal per minute rate for a call in exchange for information (such as adult chat lines). PRS fraud in itself has become more and more sophisticated, incorporating a number of means for defrauding both subscribers and the operators - who are left paying for the events. PRS fraud has moved into the mobile messaging domain. Fraudsters will send subscribers an unsolicited SMS telling the subscriber that they have won a prize and need to call the following number to collect their prize. When they call the number in the text message they are billed a high amount. In Europe, PRS-related scams tricked unwitting subscribers to make calls that were billed as high as 300 Euros a minute, resulting in exorbitant fees incurred by the terminating carriers.

Fraud continues to grow as new technologies are developed, but it is always difficult to understand how a fraudster is going to use new technology until it begins. Without visibility to the messaging traffic, it is nearly impossible to identify and control fraud. In many cases, such as PRS fraud, operators are attempting to team together to identify when the traffic is hitting their networks so that they can shut down the traffic immediately, but many times they lack the tools needed to get visibility to this traffic, making it impossible to see and deal with fraudulent events such as those in real time.

## *Flooding and Denial of Service (DoS) Attacks*

There is another threat that messaging brings to wireless networks and it is especially troublesome. Tests have shown that service (both voice and messaging) can be denied to any cell site using a PC to generate thousands of text messages to that cell (or multiple cells), congesting the control channels used to establish connections with the wireless devices in that cell. The attack blocks both messaging and voice for a sustained period of time (as long as the messages are continuously sent). As few as 900 messages in a one hour timeframe can cause a significant outage. This is a very low number of text messages, especially if one employs bots (software applications more commonly used in automated attacks on networked computers) to carry out the attack. The bots can be spread to thousands of wireless devices, and used to generate text messages from these devices simultaneously. This method of attack would prove devastating, especially if carried out in synch with other forms of attacks.

## *Handset Viruses*

In the real world, most cell phone payloads propagate through direct user download (similar to downloading a Trojan horse from a random website). The second-most popular propagation mechanism is Bluetooth, and the third is SMS. Propagation really matters when it comes to malicious code, because getting to the victim is more than half the battle. Once it gets into a device it starts to do some pretty offensive things.

Devices have much more functionality than they used to – they have become small computers. They are more connected than ever, supporting more communications protocols and even offering full-blown Web access. There are tens of millions of them on every continent on earth. And just like computers, they can be infected with viruses. One of the first well known handset viruses was the Cabir virus, which debuted in 2005 and has now infected phones in over 30 countries. There are more than 370 known mobile viruses, most of which target the Symbian platform. (SOURCE: Mikko Hypponen, chief research officer at F-Secure).

So-called smart phones are clever enough to handle e-mail, instant messaging, database storage and video, but they're not necessarily prepared to fend off the inevitable viruses that come their way. With potentially hundreds of millions of these devices being shipped in the next few years, viruses pose a real threat to both carriers and consumers. The sheer volume of very private, sensitive, valuable information that people are carrying around in their handhelds is mind boggling and all of it is under attack constantly with almost no protection. Often the most sensitive data that is found on your cell phone is in your address book.  Bots accidentally downloaded to the cell phone can take control of the phone and send infected text messages to everyone in your address book. Extrapolate this concept to millions of infected phones all launching text messages at the same time and the network will certainly crash.

Why are cell phones so susceptible to viruses? Simple cell phones don't have kernels that separate root level privileges and critical system functionality from other kinds of code. This is similar to how Windows 95, Windows 98, and WindowsME were architected more than a decade ago. We're currently in exactly the same state of security in the cell phone world as the Internet was just before the debut of the Morris worm back in Nov 1988. The Morris worm, written by a student at Cornell University, was one of the first computer worms distributed via the Internet.

### *Future Threats*

People have already been defrauded out of a lot of their money through phishing attacks sent via SMS. Residents have been put into panic mode and initiated evacuation plans after receiving spoofed messages regarding a catastrophe. So what's next? New threats will evolve as more advanced services such as Messaging 2.0 and instant messaging (IM) start to grow in popularity. No one knows exactly what types of insidious schemes await us in the future.

## *Stopping SMS Threats*

### *Protecting Against Attacks*

Recent trends in mobile devices are raising the probability of attack. Current government oversight, operator procedures and technical solutions haven't kept up with wayward youths and criminal minds. Finding the perpetrator is difficult in all cases, and since the legality and jurisdiction of SMS spamming is still a grey area, legal action is not a viable option. Operators are left trying to identify when their network security is being breached and pursuing the perpetrators themselves.

In fact, some operators still don't feel that SMS spam is an issue, which usually indicates that they (the operator) do not have visibility to the traffic in their networks. In other cases operators do not necessarily want to know too much detail about problems in their network, because it can result in negative press. However, this attitude has changed significantly in the operator community given new competition, slowing revenue growth and less capital to invest. Fraud and security departments are now being given new directives to find revenue losses, which means they are now looking for new tools and applications to help them identify what they cannot see.

The threats are now clear enough and margins tight enough that operators can no longer assume that they can weather a storm of spam. Operators are finding they need to be watching the traffic coming in and going out of their networks and analyzing that traffic in real time to be able to stop the sophisticated attacks being seen today.

The most logical response to the mobile security threat is to use existing virus protection commonly installed on PCs. This won't work though because while the handheld devices are smart, they don't have the horsepower to run applications that slow up even high-capacity PCs. There are skinny versions of virus protection for cell phones, but they're not always effective because users either don't have the virus protection software installed or haven't taken the time to update the software in a long time. While consumers are asked to load up their own annual-fee virus protection programs for their desktops, operators are the first line of defense for mobile security.

A good starting place to protect the mobile network is the underlying signaling/transport network for SMS – the signaling system 7 (SS7) network. To better protect the SS7 network, Eurescom made three recommendations in their studies of SS7 vulnerabilities. These recommendations called for:

- Monitoring the call control network
- Screening messages to prevent unauthorized access
- Policing to ensure only authorized services are accessed

Not many of these practices are implemented today. Part of the problem is the reluctance to make a "risk management" investment. Also, with the absence of events to raise the alert level of service provider executives, it makes the business case even harder.

# Technical Challenges

## Finding the Threat

Before stopping any intrusions into the network an operator must be aware of the intrusions in the first place. If an operator is not able to verify the Quality of Service (QoS) for messaging, which requires the ability to trace a message end to end, then they most likely cannot see the problem. Although beyond the scope of this paper, operators can leverage network monitoring tools to identify attacks on their SMS network. Additional products can then be used to block the attacks.

## Solving the SMS Security Problem

With current SMSCs, when customers have complaints regarding spam, operators have no way of addressing those concerns other than turning off SMS capabilities to those particular subscribers, which negatively impacts revenues. Operators dealing with fraud and security issues can deploy a variety of devices to protect their SMS network from hostile spam attacks, DoS attempts, and even advanced techniques like spoofing. These devices range from STPs with screening (MAP/ISUP) capabilities and other security capabilities, SMS Firewall, and specialized niche solutions. This paper will focus on SMS Firewall security capabilities and use cases, which include:

- Spoofing
- Spam
  - Faking
  - Anti-flooding
  - Pattern detection
  - Content filtering
- SMS Home Routing

SMS Firewall detection triggers and filter settings should be adaptable in real-time, enabling network operators to react very quickly to new threats. The following paragraphs will discuss different SMS Firewall use cases and the respective operator benefits.

## SMS Firewall Use Case #1: Spoofing

SMS network and subscriber security is a big issue today with operators. With mobile originating (MO) spoofing, the "spoofer" typically pretends to be a mobile subscriber roaming in another country in an attempt to bypass the operator's mobile switching center (MSC) authentication processes. In

**Figure 1**, the SMS Firewall intercepts the MO message and compares the MSC location from where the message originates to the MSC location stored in the subscriber's profile, which is stored in the home network home location register (HLR). If the comparison shows two different locations, the message is considered to be an MO-spoofed message. It may be blocked or simply logged and then forwarded to the SMS network for delivery.

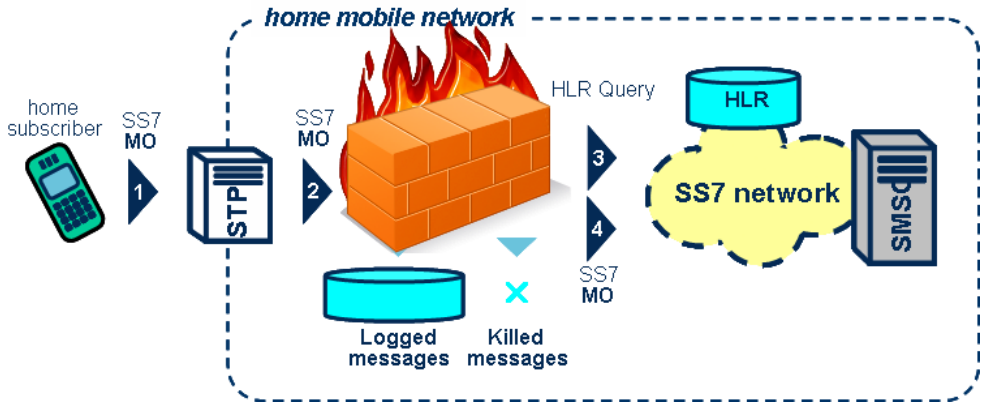


**Figure 1: SMS Firewall Use Case #1 – Spoofing**

### *SMS Firewall Use Case #2:– Spam*

Another prevalent security topic with operators is mobile terminating (MT) spam. MT spam includes the following:

- Faking
- Anti-flooding
- Pattern detection
- Content filtering

**Use Case 2A: Faking**

The SMS Firewall's MT spam solution resolves situations in which a foreign SMSC or a device pretending to be a SMSC is trying to 'spam' mobile subscribers with SMS messages. In a common 'spam' example, a mobile subscriber receives an SMS requesting that the recipient call a premium rate number to claim a prize that they supposedly have won. The spammer already has registered this premium rate number and collects all revenues generated by unwitting subscribers calling this number.

Figure 2 shows how an SMS Firewall can prevent this spamming scenario by intercepting the routing information request, generated by a foreign SMSC, by pretending to be the destination MSC/HLR. When the foreign SMSC forwards the MT message to the recipient's network, the SMS Firewall intercepts the message and checks for inconsistencies in the message headers and message content. If any consistencies are discovered, the message may be blocked.

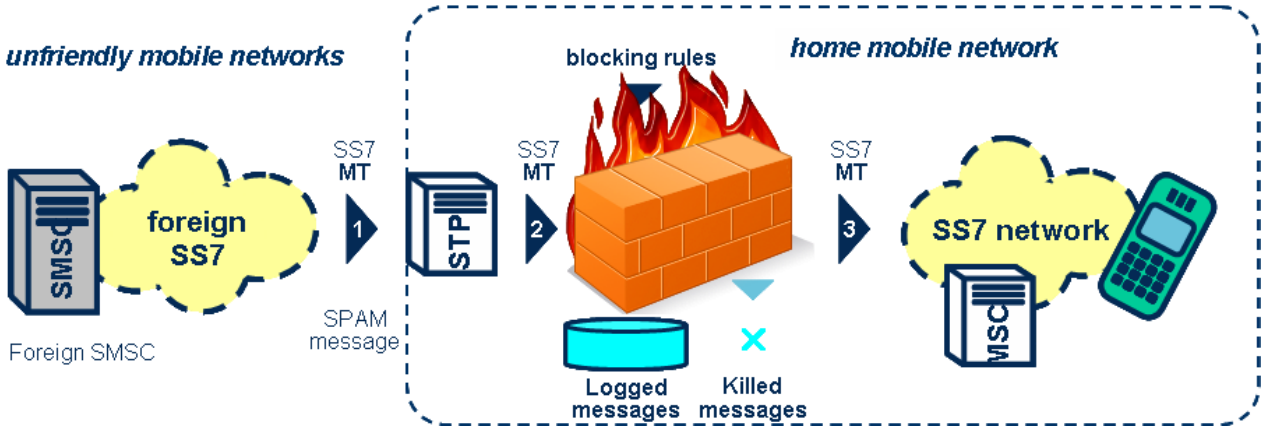


**Figure 2: SMS Firewall Use Case #2A - MT spam (Faking)**

**Use Case 2B: Anti-flooding**

The SMS Firewall flooding filter detects sudden increases in traffic from the same originator(s). It continuously monitors the short and long term traffic average (in messages per second) per originator (or range of originators). If the short term traffic average exceeds the long term traffic average by a considerable margin and for a long enough period of time, flooding is detected. The flooding condition remains until the short term traffic average drops below the level where flooding was detected initially. While flooding is detected, the flooding filter does not update the long term traffic average. The flooding filter has a number of settings for adjusting its detection behavior when a flooding event occurs as depicted in Figure 3.

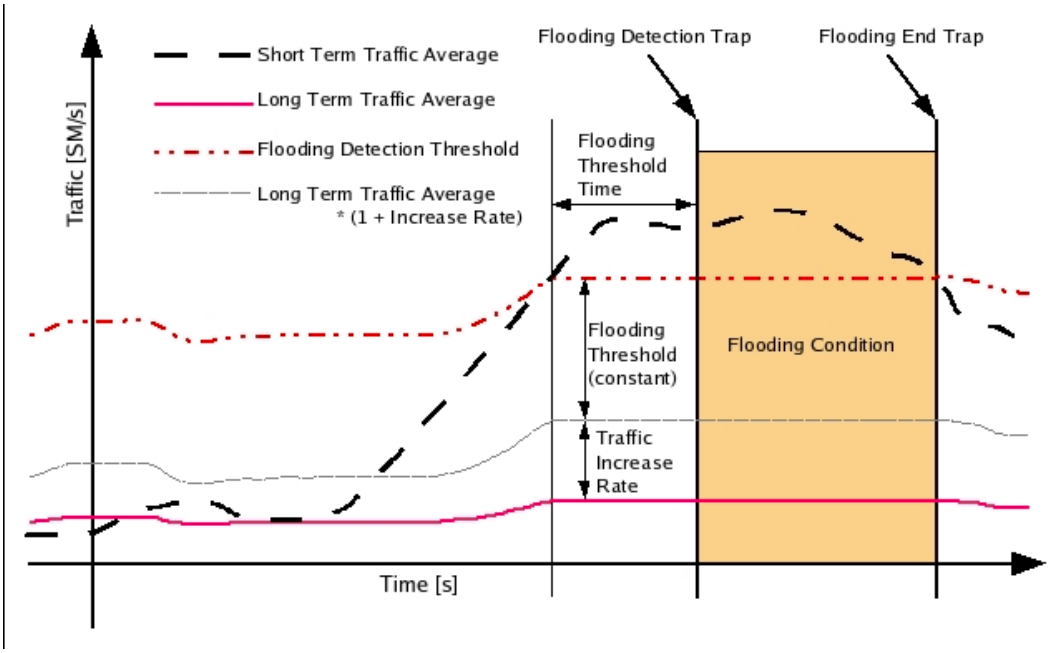


**Figure 3: SMS Firewall Use Case #2B – Anti-flooding**

**Use Case 2C: Pattern Detection**

The 'duplicates filter' detects messages which are (very) similar to a relatively large number of recent messages. Every time the duplicates filter is evaluated, it tries to detect groups of similar, recent messages that are large enough to be worthy of tracking (cluster detection). Each time such a group is detected, the duplicates filter starts a so called "cluster" for this group of messages, which starts tracking them closely (cluster matching). The duplicates filter measures similarity based on a comparison of features, except for a 'required similarity' of 100%, where a message must be an exact duplicate.

**Use Case 2D: Content Filtering**

The content filter detects messages that contain a word (or a phrase) from a provisioned list. The accuracy of the match can be configured and varies from an exact match to a match after normalization of the message. For each match, the word, phrase or the entire message can be modified. If at least one match was found, the filter yields TRUE. Normalization is applied to a string of tokens. Normalization collapses multiple identical tokens into one single token. For example, two consecutive tokens 2 (the L's of "dollar") are collapsed into a single token. In another example, after normalization, the strings "many dollars" and "maany dolar$s" are equal.

## *SMS Firewall Use Case #3: Home Routing*

Without the proper systems in place, roaming mobile subscribers are outside the protective shield of the home network SMS security and management capabilities. The result is that the customer may not have a consistent SMS experience while roaming in a foreign network. SMS home routing enables spam and spoofing protection implemented on the home network to be transferred to the visitor network experience and helps to reduce or eliminate the burden (on the roaming subscriber) of unsolicited marketing messages introduced by visits to the foreign network. Figure 4 shows how the SMS is routed to the home provider network for processing.

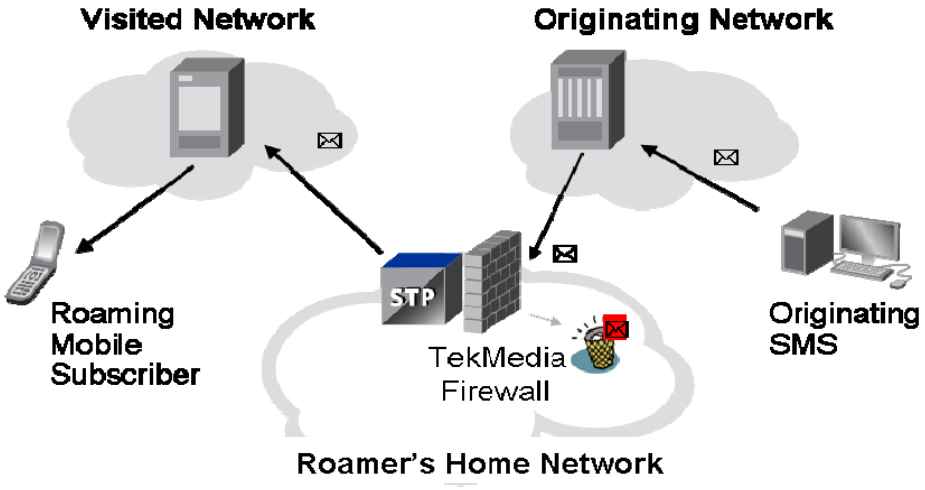


**Figure 4: SMS Firewall Use Case #3 - Home Routing of SMS Messages**

Because the home network operator screens messages sent to subscribers to prevent unwanted messaging, only the messages consistent with the subscriber experience on the home network reach the subscriber while roaming. In some instances, the home operator may allow a foreign operator to send "SMS Welcome" messages to roamers. These messages can educate a roamer about visited network services and can be screened on a pre-approved basis. In case no such agreement has been agreed and the visited network sends unsolicited "SMS Welcome" messages they can be stopped by the home network when home routed. Home-routing can be used to enhance a subscriber's experience and to improve their perception of the home mobile services carrier.

The SMS Firewall allows the operator to home-route all SMS messages that are sent to customers while roaming. The originating network is forced to send all SMS messages to the roamer's home network, with the benefit that the home operator can continue to offer subscribers a consistent messaging experience whether in mobile home zones or traversing foreign networks.

For an added benefit, the home network operator implementing an SMS home-routing solution is able to capture and/or reduce origination network inter-working charges. Depending on the network situation, the SMS home routing solution payback period is just a few months - due to reduced (increased) inter-working charges (revenues).

SMS home routing gives operators the ability to control the quality of service that they want to deliver to customers – wherever they are. This unified customer experience allows operators to differentiate themselves and can translate into increased subscriber average revenue per user (ARPU) for the home operator.

## *Tekelec Security Solutions*

Tekelec provides a suite of security tools that operators can use to protect their network, and which can be combined to create a solid security foundation.

### *Network Visibility for Finding Intruders*

Tekelec's Integrated Applications Solution (IAS) collects network signaling traffic such as SS7 and SIP, as well as MAP, ISDN, HTTP, FTP and more. The IAS solution gives operators the ability to filter the data and form reports and dashboards based on criteria they define. IAS gives service providers visibility to their networks to identify security breaches and unauthorized access. Because the solution is capable of providing end-to-end network usage data, service providers will be able to identify the source of network attacks, including:

- "Ping calls"
- Mass call events

- SMS flooding
- SMS spam and their originators
- Fraudulent access

Tekelec's IAS solution provides data usage in the form of reports and customized dashboards, accessible by any authorized user through standard browsers. This allows service providers to distribute information to several departments. Reuse of the network usage data prevents unnecessary capital expenditures for redundant systems supporting multiple departments.

IAS can be deployed with or without probes when integrated with Tekelec's industry-leading EAGLE® 5 Integrated Signaling System (ISS)—providing operators with significant cost savings, more efficient operations and a reduced footprint.

A Tekelec customer in France is using IAS to identify the top 50 originators of SMS messages who have broadband accounts. They have found that identifying this set of users always points them to spam originators.

## *Stopping the Intruders*

Once SMS spam and spoofing have been detected, Tekelec's TekMedia SMS Firewall can be used to actively block these messages. The Firewall solution provides unprecedented protection against spam, fraudulent messages and flooding of the SMS network. TekMedia SMS Firewall has two main components – Basic and Firewall Advanced Filters (FAF) – as shown in Figure 5. The basic component blocks incoming and outgoing spam by screening at the SCCP and MAP levels: providing correlation between MAP messages, and allowing for the active blocking of MO spoofing and MT spam messages.

The services provided by the second TekMedia component – Firewall Advanced Filters (FAF) - give insight into some of the specific problems SMS traffic is prone to. For instance, content filtering blocks banned words contained in the message payload. An example could be VIAGRA or (in its tokenized version) V1AGRA. Anti-flooding, meanwhile, detects and blocks abnormal increases in traffic, while pattern detection can detect and block frequent messages containing the same phrase and messages coming from consecutive originating numbers.

The SMS Firewall protects the service provider at two levels: through address analysis and content filtering. The address analysis function allows operators to identify and block messaging from operators using fake SCCP addressing or spoofed SMS addresses to gain access into their networks. It also offers control over bulk SMS providers sending large volumes of messages into the network.

The content filtering and analysis function allows service providers to perform a complex assessment of the content of messages, looking for specific text combinations or even the content type (premium content such as music downloads and picture files). Using Bayes filtering, TekMedia SMS content filtering adds another element of control over spam to further manage unwanted messages. When combined with the Tekelec IAS, service providers have the best-in-breed solutions for identifying and preventing fraudulent SMS and spam.

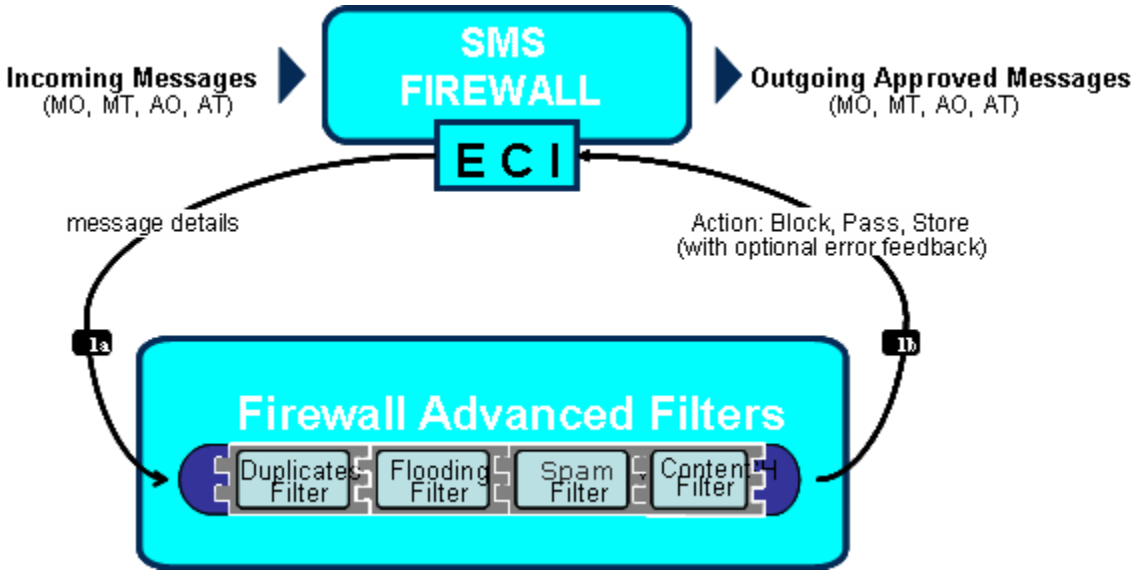


**Figure 5: TekMedia Firewall Advanced Filters (FAF)**

Tekelec has deployed the TekMedia SMS Firewall for a variety of SMS security use cases, including: SMS home routing; blocking SMS welcome messages; reduction of inter-connection charges; SMS spam control; anti-spoofing; and the complete set of TekMedia Firewall Advanced Features (FAF).

### *Screening the Threats*

The EAGLE® 5 ISS provides contextual screening to prevent certain types of Message Transfer Part (MTP) and Level 3 Network Management Messages from entering the network. For example, if a TFP is received by an STP, with the concerned point code of a network node that is not directly adjacent to the STP, the message is discarded. This is because the TFP should be coming from an adjacent node and never from outside the network. Any TFP coming from outside the network, with a concerned point code of an internal node, should be considered a threat and discarded immediately.

The EAGLE 5 ISS also includes screening of SCCP Subsystem Management (SCMG) messages with reference to network resources such as HLRs and number portability. SCCP screening provides the same methods of protection against attacks on network resources. It works in the same fashion as network security enhancements, examining each management message, and determining if the message should be received by the STP (is the affected subsystem adjacent to the STP).

## *Conclusion*

The messaging market is growing rapidly and has become a very profitable piece to the mobile operators' revenue puzzle. Unfortunately, growing security threats such as spam, spoofing, flooding (DoS attacks), fraud and handset viruses pose an increasingly significant threat to the mobile operator. Although these threats haven't made a big impact to operators' bottom lines yet, the security threats and seriousness of them will increase quickly, just as they did with PCs.

There are a variety of niche products beginning to come onto the market to help operators deal with these threats. What operators really need is a comprehensive strategy consisting of proper processes and network-wide security. Operators need visibility into their network to see the threat, the proper tools to stop the threat and the ability to fix any damage done by the threat.

Tekelec provides a suite of security tools that can help operators today. The Tekelec IAS can be used to show operators that their network has been infiltrated by a variety of threats. They can then use TekMedia SMS Firewall to actively detect and block many of these threats – including spam and spoofed messages. The TekMedia SMS Firewall can also be used for SMS Routing, for operators looking to expand the routing capacity of their SMS networks. And lastly, the EAGLE 5 ISS provides contextual screening to prevent certain types of threats.

## *About Tekelec*

Tekelec is a high-performance network applications company that is enabling the transition to IP Multimedia Subsystem (IMS) networks for service providers around the globe. With its experience at the intersection of network applications and session control, Tekelec creates highly efficient platforms for managing media and delivering network solutions. Corporate headquarters are located near Research Triangle Park in Morrisville, N.C., U.S.A., with research and development facilities and sales offices throughout the world.

For additional information on Tekelec's portfolio of products, please contact your local Tekelec sales representative or visit www.tekelec.com.

# *Appendix*

## *Glossary of Acronyms*

ARPU – Average Revenue Per User

DoS – Denial of Service

GSM – Global System for Mobile Communication

HPLMN - Home Public Land Mobile Network

HLR – Home Location Register

IMS – IP Multimedia Subsystem

ISUP – ISDN User Part

MAP – Mobile Application Part

MMS – Multimedia Messaging Service

MO – Mobile Originating

MSC – Mobile Switching Center

MSISDN - Mobile Subscriber Integrated Services Digital Network Number

MT – Mobile Terminating

MTP – Media Transfer Protocol

PRS – Premium Rate Service

QoS – Quality of Service

SCCP – Signaling Connection and Control Part

SIP – Session Initiation Protocol

SMPP – Short Message Peer-to- Peer

SMS – Short Message Service

SMSC – Short Message Service Center

SS7 – Signaling System 7

STP – Signaling Transfer Point

TCAP – Transaction Capabilities Application Part

TFP – Transfer Prohibited

VLR – Visitor Location Register