



Freddy Mangum, vice president of product marketing, Fortinet

Keep a tight lid on Pandora's box

The quest for greater ARPU has brought about new, open standards-based network architectures for fixed and wireless operators. However, this evolution towards IMS has opened a Pandora's box of security risks as telecom carriers come face-to-face with threats they were previously shielded from, writes Freddy Mangum, vice president of product marketing at Fortinet.

Carrier security is an issue rarely discussed in public, although the security stance among mobile network operators is actually very encouraging. As an industry, mobile operators treat the issue proactively, taking steps to protect entire core services infrastructures rather than merely leaving subscribers responsible for protecting their smart phones.

While altruism may well be a factor, the main reason for this posture remains ARPU. Mobile operators are on the cusp of realising truly mass-market penetration for pre-IMS (2.5G) services such as MMS that deliver advanced ringtones, games etc., and widescale disruption could mean those revenues – as well as accumulated brand equity – falling off a cliff. Market competition demands differentiation, and no mobile operator wants to be the odd-one-out when it comes to security – particularly with 3G, 4G, FMC and all-IMS networks looming so large on the horizon.

It's easy to underestimate the threat posed by mobile 'malware'. Criminal entities hardened by experiences in the fixed internet world have emerged and seek to defraud subscribers and/or carriers in an effort to extort monetary gain. Their activities have grown exponentially since 2004/2005 so that today, anything up to 5% of all mobile network traffic is currently being infected with some form of malicious code. Hackers typically gain access to pre-IMS networks through the application layer and silently exploit individual subscribers in the following ways:

Malicious Attack. Exemplified by the Skulls virus, this group of malware seeks to completely disable the infected device by removing or corrupting its system functions.

MMS Spam Threat. This involves cyber criminals posing as legitimate promoters of an illegitimate service or prize draw. Having mass-mailed MMS messages describing the promotion, individual recipients are invited to download an application installer in order to participate. Once installed, this software replicates itself to every number in the device's phonebook before sending unlimited numbers of



texts to the advertiser's account, thereby generating huge amounts of revenue. Victims only find out when they receive their monthly bill, or run out of credit.

MMS Service Threat. Similar to the threat above, this involves the richer media file structure inherent within MMS, capable of attaching application files (such as games), which can harbour malicious code. Examples include ComWarrior and Mosquito. MMS messages are also most likely to carry offensive, unsolicited content designed to cause maximum distress, particularly among juvenile users.

Smart Phone Web Browser Application Threat. This approach represents apparently normal applications that obscure a sinister side. Examples include RedBrowser, a free-of-charge messaging application containing a Trojan program that directs each message to a \$5-a-time premium rate number.


The opening up of the network and the growth of standard-based devices – both developments designed to facilitate greater services innovation and flexibility – have created challenges for mobile operators both at the application service layer and deeper at the core-IP network layer. Laptops, PDAs and smart phones that traverse fixed and mobile networks can cross-pollinate any threat developed through the medium of IP.

Defending pre-IMS networks therefore involves more than merely putting up network roadblocks. Operators understandably worry about network performance, service uptime and its effect on user experience, therefore care must be taken to ensure that legitimate network traffic is not delayed or mistakenly terminated. An effective security solution must analyse all traffic, make an appropriate determination in separating the good packets from the bad, and take action in 'real-time' to thwart nascent security risks well before they can impact network performance or disrupt service delivery.

Hackers are applying knowledge gained from years of attacking users on the fixed

network to conceive highly sophisticated mobile threats that can easily confuse or overwhelm security systems focused on countering specific types of threats. If these were just viruses, then the obvious solution would be an anti-virus filter. Unfortunately these blended threats often combine the characteristics of a virus, a worm, a DoS (Denial of Service) attack, blacklisted content or spyware, and they can morph very quickly once launched by the hacker.

Any deterrence solution therefore should employ a combination of identification and multi-layered analysis techniques coupled with rich, up-to-date security content to minimise false positives (where normal traffic wrongly triggers a response) and false negatives (where actual threats are missed) across the network. This approach centres upon taking full advantage of new technology advances to flexibly implement real-time application and core-IP layer protection from the full gamut of security functions; MMS antivirus, anti-spam, GTP firewall, web and content filtering, IPS, VPN etc. A flexible and modular yet unified approach in this regard is also critical, particularly in light of mobile operators' understandable sensitivity to the prospect of escalating operating costs or management overheads.

Operators understand that securing their current pre-IMS infrastructures is the surest path to ensuring safe migration to tomorrow's advanced, converged SIP-based applications and services. It starts with the implementation of a proven, high-performance carrier-grade (such as AdvancedTCA-certified) platform, configured to be constantly abreast of new multi-threat intelligence and capable of ensuring effective management and analysis. It carries on down the road to greater ARPU and lower risk. 

Hackers are applying knowledge gained from years of attacking users on the fixed network to conceive highly sophisticated mobile threats that can easily confuse or overwhelm security systems focussed on countering specific types of threats.

Swisscom Mobile - Fighting malware

Swisscom Mobile AG is the leading mobile communications services provider in Switzerland, operating several state-of-the-art wireless networks. It takes a hands-on approach to securing its customers against the considerable numbers of mobile malware that could reach end users through an array of communication vectors such as MMS, email or web traffic. To protect its 4.5 million customers from mobile cyber threats, Swisscom Mobile uses Fortinet's FortiGate-5000 chassis based systems and FortiGuard Antivirus, Intrusion Prevention (IPS) and Web Content Filtering subscription services.

"Our ongoing commitment to security is greatly benefited from Fortinet's technology, which continuously protects our customers from mobile malware and helps safeguarding the continuity of subscriber services," said Marcel Zumbühl, head of security at Swisscom Mobile.