



TECH BRIEFING

MOBILE SECURITY

Lines of defence

The threat to mobile security has not been as prevalent as for fixed devices, but as software downloads increase on handhelds things could get worse. Already operators are putting measures in place to tackle this and roaming fraud. By ROY RUBENSTEIN

This month will mark a key milestone in how mobile operators tackle global roaming fraud. The GSM Alliance (GSMA) set October as the target date for its 700+ member operators to go live with the ability to generate user roaming reports within four hours. The GSMA expects 83 operators to have implemented the Near Real-Time Roaming Data Exchange (NRTRDE) this month, with at least 30 more to follow quickly.

Mobile roaming fraud is extremely lucrative for criminals. Swiss firm Mach, which handles roaming records for mobile operators, claims it accounts for US\$5 billion, 10% of all telecoms fraud. Reducing the time taken to report user roaming activity from days to hours should improve fraud detection and curtail the fraudulent sums accumulated (see box).

The GSMA's initiative is an example of the continual ebb and flow between mobile operators and fraudsters. Another security threat with increasing criminal tendencies is malicious software (malware) attacks.

Until now mobile operators have been a step ahead of the attackers. While serious mobile virus outbreaks have occurred, widespread epidemics have been avoided, says market research firm Ovum. Mobile operators risk financial and brand loss, and potentially even customers, should the

balance tip in favour of the attackers.

The bad news is that malware attacks will increase as handsets and services develop, say analysts. Indeed operators are already witnessing greater activity.

"The iPhone with its flat rate has brought a lot more hackers on side," says Marcel Zumbühl, head of security at Swisscom. "Hackers interested in mobile phones have been at a low level but we are seeing it rising."

Moreover, underlying security trends are discouraging. According to IDC, whereas revenues from PC security software continues to grow, security software for wireless PDAs and mobile handsets remains weak, at less than 5% of all security software sales.

"There is a deepening gap developing with personal mobile devices," says Eric Damage, research manager, security products & services, IDC. "Growth in security software for mobile is below 2% per year for the main vendors while handheld devices will grow by 19% a year until 2012."

However, comparing mobile with fixed network security requires care. The threats facing mobile networks—spam messages, malicious software and denial of service (DoS) attacks—are similar to those of fixed networks. But because mobile operators' data services are relatively new, they have benefited from the fixed operators' years

of experience in addressing cyber attacks (*Total Telecom*, December 2007, p.40).

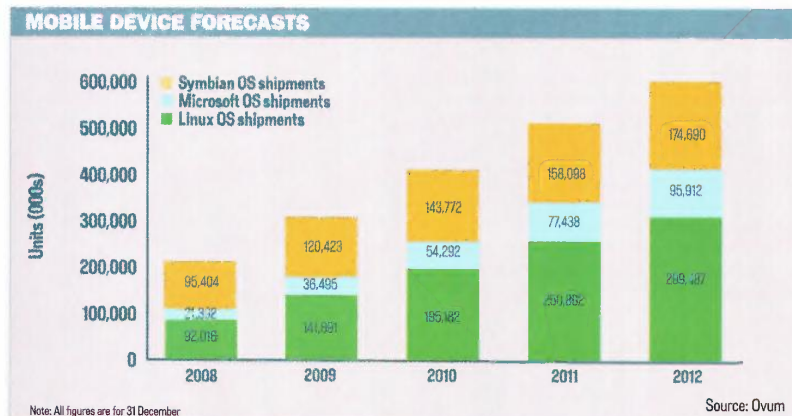
"The mobile industry has seen how the Internet has developed," says Janne Uusilehto, head of Nokia product security. "Operators and vendors recognise that if they don't take care they will follow [the experiences of] the Internet."

Mobile also has unique characteristics that aid operators to secure their networks. First, mobile communications is largely transaction-based, meaning that attacks must be paid for. "As an attacker, all you want is to make money," says Zumbühl. "The business case of any attack must be feasible." A distributed DoS attack must be paid for, as must SMS and Multimedia Messaging Services (MMS). However, while paid-for transactions help operators to deter attacks, it is also a hindrance if an attack leads to customers being charged for unwanted transactions.

"MMS is chargeable and there is a lot of infected MMS that can take hold in handsets and cause other problems," says Darren Turnbull, director of product management at security vendor Fortinet.

Commwarrior, first detected in 2005, is a notable example of a virus that spreads using MMS. "The payload deleted users' addresses then propagated using MMS, replicating the application via [the phone's] Bluetooth [wireless interface]," says Adam Leach, a principal analyst at Ovum. Commwarrior also sent SMS and MMS to spam other users. "Not only did it affect the handset, it increased the [user's] bill and made MMS traffic peak in the network," says Leach.

"MMS messages can lead to false revenue and loss of service; sent on to other operators it can also result in [an operator's] loss of reputation," says Turnbull at Fortinet. Spam emails can lead to loss of service and customer care issues. A user with an infected PC inadvertently sending spam via their 3G modem card will first become aware of a problem when their emails stop. "You report to your operator that you can't send email, but it's a mail server problem not a mobile issue," says Turnbull.





TECH BRIEFING

Fortinet has developed content inspection hardware that inspects messages and creates records based on the user's mobile phone number to determine whether they are spamming. The same applies to MMS messages. "All messages sent from a handset or received from an operator are checked to see if they have viruses," says Turnbull, "We can identify a virus, clean up the message and still deliver it."

Other techniques include monitoring an end point to see if it is sending multiple copies of the same message, and checking to see if the same message is propagated to multiple devices. To do this a hash of the message—effectively a unique signature—is created and stored. If the same hash reappears, it is the same message, and this alerts the operator to cache the messages and start security and fraud analysis.

Operators also say they are taking steps to counter spam. "In order to tackle MMS and SMS spam in the UK, Vodafone has launched the VSPAM initiative," says Bryan Littlefair, chief information security officer, Vodafone Group. "Customers who receive unsolicited messages can forward them to 87726 where we will then process them and take action where possible against the parties responsible."

The other notable difference between fixed and mobile that impacts network security is the operating systems used by the end devices. PCs connected to fixed networks are nearly always Windows-based. Handsets, in contrast, often use open operating systems, such as Symbian, Microsoft's Windows CE and Linux-based ones such as Google's Android.

"There is a huge fragmentation in software platforms compared to the PC," says Leach. Such diversity means specific malware is inevitably targeted at a particular handset category. Commwarrior, for example, originally targeted Symbian Series 60-based handsets.

That partly explains why 4,000 viruses target mobiles while PC viruses total 400,000, says IDC. "Malware cannot currently spread from one family of handsets to another unless there is significant compatibility," says Vodafone's Littlefair.

Leach at Ovum says Symbian has improved the security of its V9 operating system. It has also introduced an authentication scheme whereby only trusted third-party applications developers work with its operating system. "Since Symbian has done these changes, there have been no instances of malware," says Leach.

But things could get worse for operators. "As the mobile becomes open to software downloads, you expose the phone to the

TACKLING ROAMING FRAUD

An example of global roaming fraud is when a SIM card is stolen in one country and used in a second to call a premium number in a third. For example, a phone stolen in the UK may be used to make a call in France to a number in Italy, and it is the French operator that pays for the transaction before reclaiming the roaming payment from the UK service provider of the stolen phone owner. By the time this operator realises international fraud has occurred, the operation in Italy has disappeared.

Swiss firm Mach handles roaming records for hundreds of mobile operators, and offers its own fraud detection service that uses artificial intelligence techniques to detect unusual calling patterns within the data. In an attempt to help reduce fraud, five years ago it introduced a high-usage report service that details for operators users spending over \$100 a day. Such reports are generated within 36 hours compared to the normal 30-day period. But even a day and a half can be too long. According to Frank Jacobsen, Mach's director of business development, fraud, one operator experienced fraud of US\$800,000 between a Saturday night and Sunday morning.

The GSM Alliance initiative to produce usage reports within four hours will clearly help to tackle roaming fraud. Operators must amend their systems to produce and exchange record data within that time period. "The GSMA has fulfilled its mission," says Jacobsen at Mach. "It is up to individual operators and [security detection] companies to detect fraud before it happens."

Enterprises, meanwhile, face other network challenges. WiFi is now an integral part of corporate LANs and, unlike GSM, uses unlicensed spectrum which does not include built-in security for subscriber identification and billing. "Wireless' biggest benefit is its biggest problem: the signal goes everywhere," says Rachna Ahlawat, vice president of strategic marketing at WiFi specialist Meru Networks.

Meru designs WiFi networks based on multiple access points, and its systems include measures to counter security threats. To counter eavesdroppers that use a high-gain antenna beyond the building, for example, it has developed a product that alters the exiting wireless signal so it can't be decoded. "It [the received signal] appears as an innocuous message," says Joe Epstein, Meru's senior director of technology.

same problems seen with the PC," says Jörgen Lanto, vice president of portfolio management and technology at Ericsson Mobile Platforms.

Ericsson is a proponent of Java programming language-based applications and has developed a multimedia communication suite that enables instant messaging and video sharing between a handset user's contacts. "That type of application is very advanced," says Lanto. "If you don't have control of your environment then, in a theoretical example, you could download a client that would set up calls to 0800 numbers" and circumvent call costs.

Ericsson has adopted an approach similar to Symbian's: it is only possible to download certified Java clients onto a handset. It is using the approach for pre-commercial trials and will start widespread deployments in 2009.

Compared to the PC, mobile operating system providers are slower to issue software patches. "If a gap is identified it stays there longer, which means there is a longer window of opportunity," says Zumbühl at Swisscom.

For Ovum's Leach, operators must adopt a multi-tiered approach with security mechanisms in the network as well as within devices.

"Unlike some traditional signature-based detection systems, Vodafone's defence is also capable of detecting new viruses, and a turning point was reached

when the BeSeLo worm was released in late 2007/early 2008," says Littlefair. "Vodafone's intelligent defences picked up the new virus, and as a result it was Vodafone that provided samples to the antivirus vendors, not the other way around."

Swisscom uses Fortinet as part of its network security strategy to filter mobile malware directly in the network. In addition, it works with vendors to shore up any identified security flaws in handsets before they are launched. "This doesn't happen in the PC market," says Zumbühl.

"The key question [with security] is who is responsible," says IDC's Domage. "Telcos protect their networks, they don't protect their clients." He expects regulation to play a role in forcing operators to secure end devices: "The EC is aware of the gap and there will be a battle [between operators and the regulators] in Brussels."

Vodafone says its intelligent network detects and is capable of removing viruses and malware in transit across the network. "This capability is being extended to all Vodafone operating companies and currently covers most of the MMS traffic in Europe," says Littlefair.

Zumbühl at Swisscom is adamant that the network is the place to stop viruses, while devices more prone to attacks will also come with antivirus software. "As the mobile is more seen as a PC, it will become very natural to protect the mobile," says Zumbühl. ■