



## **Batten Down the Hatches**

By Monica Allevan

March 1, 2007

Wireless Week

So far, U.S. wireless operators have been spared from a major, network-crippling attack, and they've succeeded in preventing hackers from harming their networks. But as the industry moves toward an all-IP scenario, security-related concerns could become even greater.

Often included in references to the 4G vision, end-to-end IP systems will require careful balancing acts on the part of network providers, say some security specialists. "I think that's part of the balancing act the industry is going to have to walk – opening things up to users," says Tom Kershaw, vice president of next-generation networks and database services at VeriSign. "The more you open it up, the less control."

No one is suggesting operators think twice about their all-IP routes. Far from it. Security specialists recognize the need to offer as many services as possible to meet end-user demands in an emerging all-IP world. And plenty of safeguards are put into place at the infrastructure level, from authentication to encryption. Yet operators already appear to have their share of lesser-known security breaches in present-day systems.

### **MORE ATTACKS**

Globally, mobile operators are finding more malware attacks than ever, and they're spending more time and money on recovery, according to a recent Informa Telecoms & Media study, which was commissioned by McAfee. Twice as many mobile operators spent more than \$200,000 on mobile security in 2006 compared with 2005, the study found. The study involved more than 200 operators worldwide and was carried out in the December-January timeframe.

Operators cited business areas most affected by serious incidents as customer satisfaction (29%), followed by network performance (25%), revenue recognition/billing (22%), customer service (21%) and public relations (15%). "It can take some time to realize the effect on the network performance," says one unnamed mobile operator executive in the report.

Although much attention previously was focused on the device and solutions for end-users, McAfee is no longer targeting consumers with solutions to help themselves, according to Jan Volzke, senior marketing manager, mobile security at McAfee. That's in part because the incidents no longer are applicable just to smartphones and devices; increasingly, threats are aimed at more mass-market handsets. McAfee's target now is mobile operators. "Security at the network level gives you immediate protection for all subscribers," Volzke says.

The big fear, security experts say, is that a security breach will happen in the network and then spread, taking service quality down with it. If a carrier experienced a severe outage or attack, for example, it would be difficult to recover and regain customer confidence.

In the Informa study, respondents were asked to rate the priority they gave to a range of issues. The most important issue by far was network intrusion, with almost 70% giving it high priority and more than 90% giving it high or medium priority. More than 50% of operators in all regions rated network intrusion as a high-priority issue.

Of course, McAfee conveniently offers solutions to protect operators from impending threats. Are they necessary? In terms of network infrastructure, security measures are built in, and that goes for upcoming-generation systems as well, says Li Mo, chief technical officer at ZTE USA, which supplies network infrastructure. "We're building a lot of those capabilities into the border controllers," he says. "It could be made as secure as anything." Detection mechanisms also are incorporated to isolate problems and make sure they don't spread within the network.

#### END-USER LEVEL

While safeguards are built into networks, professionals in the communications security industry almost universally agree that another big piece of the puzzle boils down to end-user behavior. That's why companies such as Orange Business Services offer solutions such as its Secure Mobile Pass. A simple Internet connection is sufficient to access company resources, and a security policy can be applied on a per-user basis instead of a per-device basis, explains Guillaume Freyburger, enterprise mobility product manager at Orange Business Services.

Like other solutions, Orange's Secure Mobile Pass is based on Secure Sockets Layers (SSL), which enables privacy and security between two communicating applications through encryption.

Eventually, the idea is to move IP all the way to the base station, which can present more issues related to security, including denial of service attacks, where hackers prevent a network from being used as it is intended for legitimate users. But the move to an all-IP architecture is incremental, notes Constantine

Polychronopoulos, Bytemobile founder and chief technology officer. More security solutions are in the works today, and more will evolve. In addition, individual solutions continually will need to address specific functions, such as preventing denial of service attacks or virus monitoring.

In some ways, the mobile Internet faces some of the same challenges as the online Internet. In theory, there's a mechanism in place – locking the device. "Nobody does that," Kershaw says. People rarely log out of their PC, leaving it susceptible to anyone walking by. The same applies to phones, which come with locking mechanisms. "The vast majority of the problems are end-user related," he says. So companies such as VeriSign offer education for employees. But that only goes so far, and it's back to the drawing board to build measures into both networks and devices.