EXECUTIVE SUMMARY

Mobile network security has always been a multi-layered issue, but it is becoming ever more complex in the transition to mobile broadband. Until recently, the mobile industry has been relatively removed from the threat of cyber-attacks. While low-level fraud has been with the mobile industry since its inception, until now it has been possible to treat it as a minor irritant.

Several things are now happening at once to increase the threat to mobile networks. Cyber-attacks are gaining a higher profile in the communications industry, as well as across society in general. Meanwhile, the rollout of advanced mobile broadband services has put mobile operators on the road toward becoming full data-oriented ISPs, which will expose the mobile network to a variety of new security challenges. On the network side, the transition to end-to-end IP represents a paradigm shift in risk management. And after an incredible 20 years, the first A5/1 GSM encryption algorithm is finally looking vulnerable to being cracked in a potentially significant way.

So where mobile network security was once taken for granted, operators, infrastructure vendors, handset vendors, and application providers are being called to account as never before and asked for reassurance, near-term solutions, and long-term roadmaps that will ensure that the next 20 years of the mobile industry's evolution are built on as secure a platform as the first.

Vendors of network security products such as firewalls and intrusion protection systems, as well as solutions for mobile handset security, report strong demand for their products. While the network security product landscape is extremely rich and diverse, the one thing all these dedicated products share is that they are there to compensate for the vulnerabilities inherent in the primary network infrastructure.

In contrast, this report looks at what primary infrastructure vendors can do to correct the security vulnerabilities in their own RAN, switching, router, and transmission equipment, as well as introduce new security features into their portfolios. The report focuses on the secure development and design practices, as well as security feature roadmaps, of the primary incumbent infrastructure vendors that account for the lion's share of mobile operators annual capex on network infrastructure: Ericsson, Nokia Siemens, Alcatel-Lucent, Juniper, Tellabs, and Huawei. Cisco Systems was also invited to participate, but formally declined to do so.

Drawing on responses to a detailed Heavy Reading survey, the report explores variations in these major vendors' security practices relating to the product development process itself. It looks at best-practice design features in specific products that enable operators to protect their networks and potentially reduce their dependence on dedicated security products. The report also highlights specific vendors that are showing leadership in key areas of securing primary network infrastructure products.
Because of this approach, the report does not cover the market in dedicated security products and solutions, such as security firewalls, intrusion detection and intrusion prevention systems, SBCs, other security gateways, and test equipment. The report does not address issues relating to the security of end-user devices, nor the security of the operator's customer-facing portals, which have featured prominently in recent security breaches.

**Next-Gen Security Strategies for Mobile Network Infrastructure** is focused on what can be done to secure the mobile network infrastructure itself. It examines security best practices among the primary suppliers of mobile infrastructure equipment, analyzing their internal product development processes and the measures they take to prevent breaches of those practices. The report explores security-first product design features relating to the specific requirements of the mobile network, including the design of testing methodologies, logging mechanisms, and ease of patch implementations. The report also presents the challenges and vendor roadmaps for supporting 3GPP security features, such as the A5/3, SNOW, and EEA1/EEA2 algorithms, as well as IETF protocols such as IPV6.

For a full list of mobile network infrastructure vendors profiled in this report, [click here](#).

While networks are constantly subjected to low-level attacks, such as email and SMS spam, until now the mobile network has been at the margins of the new generation of more severe attacks and attack threats motivated by organized crime, nation-states, political, and terrorist groups. Some of the more high-profile attacks on smartphones over the last 12 months are profiled in the excerpt below.

**Excerpt 1: Recent Attacks & Vulnerabilities Impacting Mobile Broadband**

<table>
<thead>
<tr>
<th>TARGET (DATE)</th>
<th>VULNERABILITY</th>
<th>ASSESSMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android (August 2010)</td>
<td>Trojan horse discovered in Russia. Sending SMSs to premium-rate phone numbers without the owner's knowledge, resulting in money exiting the user's account.</td>
<td>Application was not available from the Android marketplace, so it was non-trusted.</td>
</tr>
<tr>
<td>iPhone (August 2010)</td>
<td>Malicious code can be hidden in fonts that automatically load when a user opens a PDF file, allowing hackers to take control of the device.</td>
<td>Being fixed.</td>
</tr>
<tr>
<td>iPhone &amp; Android (July 2010)</td>
<td>LookOut Mobile Security's Apps Genome research finds that 14 percent and 8 percent of free apps available on the iPhone and Android can access people's contact data.</td>
<td>Number of applications affected is disputed, but there is no doubt that the vulnerability exists with many of them.</td>
</tr>
<tr>
<td>Symbian (July 2010)</td>
<td>Netquinn, a mobile security company, claims 100,000 devices impacted by a Botnet virus that sent messages containing URLs linked to malicious sites to all the contacts of the address book.</td>
<td>Symbian says there is no evidence that the software is behaving as a Botnet, that its certification has already been withdrawn, and that users have a fix anyway.</td>
</tr>
<tr>
<td>AT&amp;T (June 2010)</td>
<td>Brute-force attack on 100,000 iPad users who had their email addresses stolen via a vulnerability in a feature on AT&amp;T's Website.</td>
<td>AT&amp;T turned off the Website feature.</td>
</tr>
<tr>
<td>Vodafone Spain (March 2010)</td>
<td>3,000 of Vodafone's HTC Magic devices found to have the Mariposa Botnet malware installed via the phone's memory card.</td>
<td>FBI involvement with Spain's Guardia Civil. Security practices addressed by Vodafone.</td>
</tr>
<tr>
<td>AT&amp;T (January 2010)</td>
<td>Users accessing Facebook admitted to the wrong Facebook accounts without needing to enter any user credentials</td>
<td>AT&amp;T network issue.</td>
</tr>
</tbody>
</table>

Source: Heavy Reading
Report Scope & Structure

Next-Gen Security Strategies for Mobile Network Infrastructure is structured as follows:

Section I includes a full executive summary and report key findings.

Section II outlines the different kinds of security attacks that are being perpetrated against computer software and network infrastructure.

Section III explores the specific security challenges and vulnerabilities of fixed and mobile network environments, as the growing complexity of traffic types in these networks makes it increasingly difficult to distinguish malign from benign traffic.

Section IV provides a high-level perspective on a multi-layered approach to securing the mobile network, singling out the securing of primary infrastructure elements. It describes the opportunity for vendors to differentiate themselves via more secure development practices, secure equipment design features, and support of standards-based security features specified by 3GPP and IETF.

Section V examines best-practice internal product development processes in the telecom equipment industry, outlining how vendors can tighten the security credentials of the final product they ship to customers via secure development processes relating to code compilation, sharing of code with partners, and protecting the development process from unauthorized intrusion.

Section VI examines best-practice processes in secure product design, including trends in the application of software virtualization techniques to mobile network infrastructure, systems design for transaction logs, patch implementation processes, and security testing.

Section VII evaluates the key security features in industry standards roadmaps – including 3GPP security standards, such as the new air interface encryption algorithms and IETF security features relating to the IPv6 and IPsec standards – and considers their implications for mobile networks and the outlook for feature availability and deployment in the mobile network.

Section VIII considers the growth in application-layer attacks and analyzes the 3GPP’s GAA application-level authentication mechanism and vendor roadmaps for supporting it.

Section IX profiles and analyzes the strategies of six major primary infrastructure vendors as regards their secure development practices, approach to secure equipment design, and support of standards-based security features specified by 3GPP and IETF.

The report is essential reading for a wide range of industry participants, including the following:

- **Network operators:** What catalysts are altering the network security landscape, and what measures are available to stay ahead of the security curve? Which infrastructure vendors are in the best position to meet your needs for next-generation mobile network security? How does the evolving business model for mobile services alter the security environment? What pressures are governments likely to exert on operators to ensure that their networks can withstand the most serious cyber-threats? How can network operators improve their operational security practices and better educate users on security issues?

- **Equipment vendors:** How do your secure development practices, product designs, and implementation of security features in primary network elements compare with those of your competitors? What opportunities do primary infrastructure vendors have to differentiate their network security value proposition for mobile operators? How do your competitors prioritize security in their product design philosophies and go-to-market strategies? How will the security feature roadmaps of the 3GPP and IETF influence how mobile operators evaluate and select their primary infrastructure vendors?
Investors: Which vendors are best placed to serve the security needs of next-generation mobile network service providers? How will the developing requirement for security at the application level as well as the network level influence winners and losers in this critical market? How has the increased involvement of organized crime and politically motivated organizations (including both nation-states and terrorist groups) changed the security landscape? How does the outsourcing of R&D activity by major vendors to foreign countries and third-party partners complicate network and application security?

Next-Gen Security Strategies for Mobile Network Infrastructure is published in PDF format.