McAfee | informa telecoms & media

Mobile Security Report 2009

Mobile Security Report 2009

Methodology

McAfee commissioned Informa Telecoms & Media (ITM) to conduct an online survey in November and December 2008. ITM canvassed mobile device manufacturers for their opinions on key aspects of mobile security.

An email invitation, guaranteeing anonymity to the individuals participating in the survey, was sent to mobile handset manufacturers and the software and hardware component vendors that supply them. More than 30 international mobile device manufacturers responded.

In addition to completing the survey, participants were given the opportunity to participate in follow-up interviews carried out by ITM. The purpose of the in-depth, confidential interviews was to complement, verify, and expand on the survey results.

This summary incorporates responses from both the online questionnaire and the interviews.

CONTENTS

Executive Summary

The mobile industry is going through a period of unprecedented consolidation, both at the carrier level and among hardware and software vendors.

Attempts to make the mobile ecosystem more user friendly have shown early signs of success. New players in evolving markets have successfully managed to close the gap with more developed markets, both in terms of the breadth of mobile service offerings and the range of devices available to subscribers.

Regardless of international consolidation, however, there have been few innovations anywhere able to generate significant new revenue streams. Despite ongoing efforts to grow the market with new services and functionality, voice and data access remain the main revenue generators—though often with less attractive returns than a few years ago. At the same time, barriers to entry have emerged that prevent the development of new business models.

One of these barriers is security.

Attacks on mobile networks and devices have grown in number and sophistication. This has had a negative impact on how market participants perceive the reliability of existing mobile security solutions. This is particularly apparent in the areas of mobile payments and mobile commerce (m-commerce). Devices, applications, and even networks are not sufficiently secured to allay users' concerns.

For many respondents to our survey, device manufacturers are seen as being in the frontline when it comes to providing security. They are at the forefront of balancing control with innovation, a dynamic that often determines the mobile ecosystem for as long as a complete lifecycle of a given device. This is why the *McAfee Mobile Security Report 2009* is taking a closer look at manufacturers' security experiences, their concerns and priorities, and their approach to the major security challenges that lie ahead of them in the near future.

We hope you find the *McAfee Mobile Security Report 2009* interesting and valuable.

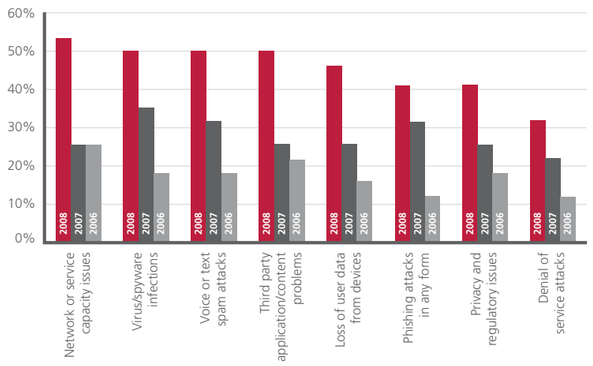
Victor Kouznetsov
Senior Vice President , McAfee Mobile Security

"The growth of multimedia applications coupled with the opening of mobile operating systems will be the tipping point for mobile security issues."
– Mobile Device Chipset Vendor

Reality Check: The Situation Today

For mobile device manufacturers and the software and hardware vendors that supply them, malware and malicious content is only one of many mobile security issues that need to be dealt with. New threats, including those that compromise users' data or privacy, have emerged, targeting widely supported services such as text messaging and even voice.

Mobile Security Issues Reported, 2006 – 2008



Source: Informa Telecoms & Media

Figure 3-1. The increase in security issues experienced by mobile device users from 2006 to 2008; percentage of respondents.

At the same time, mobile hackers using traditional coding practices have developed an increased level of sophistication. Throughout 2008, McAfee® Avert® Labs noticed a dramatic upswing in complex attacks targeting lower-level device functionality. Some of these have challenged the entire platform security concept of several vendors. Early security threats from independent young hackers have turned into sophisticated, profit-oriented attacks driven by experienced criminals. There also continues to be a high level of threat of infections from existing malware variants as vulnerable device models have entered secondary life cycles. Figures 3-1 and 3-2 illustrate manufacturers' experiences with the most common mobile security threats over a period of three years.

Within the last 12 months, manufactures have reported increased security issues across all threat catagories.

Development of Incidents

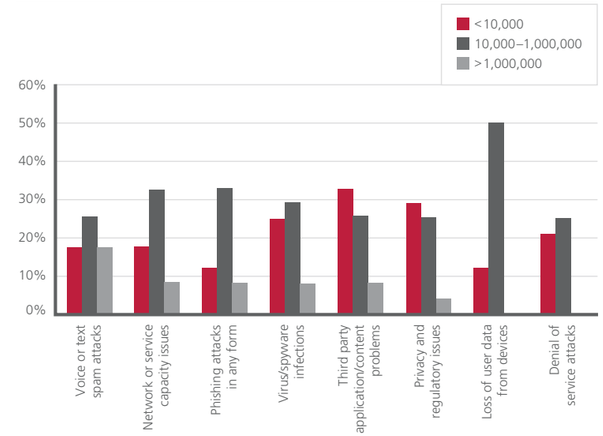
Within the last 12 months, vendors have reported increased security issues with third-party applications and content. During this time, McAfee Avert Labs has seen a strong increase in the sharing and downloading of user-generated content and mobile applications in the developing markets of the Middle East and Asia. The vulnerabilities on devices or networks created by applications with unintentional malicious code can be as severe as those deliberately created by mobile malware hackers. Interviewees have repeatedly reported cases of prematurely released applications causing severe network capacity issues, as well as crashed or locked devices. In some cases, hackers have been able to get unauthorized network access at the users' expense.

More than 40 percent of vendors have experienced all the types of security incidents listed in Figure 3-1 except domain name system (DNS) attacks. In addition to general security issues causing network or service capacity problems on the carrier side, viruses and spyware as well as voice or text spam attacks have grown to considerable levels throughout 2008.

Number of Devices Affected

As voice and text services are supported by almost all mobile devices, voice or text spam attacks have hit the greatest number of devices. Supporting findings from Figure 3-1, security issues arising from third-party applications and content have impacted a considerable number of devices. Phishing attacks and traditional problems with malware have also affected a surprisingly high number of mobile devices in the past 12 months.

Number of Devices Impacted by Security Incident Category



Source: Informa Telecoms & Media

Figure 3-2. The number of devices affected in each incident category over the last 12 months; percentage of respondents.

The Impact of Mobile Security Incidents

If security is not an integral part of mobile device and platform development, security incidents can have dire consequences for vendors' businesses. Figure 4-1 shows participants' experiences with mobile security issues and how these issues impacted internal functions and third-party developer relations.

Impact on Manufacturers' Businesses

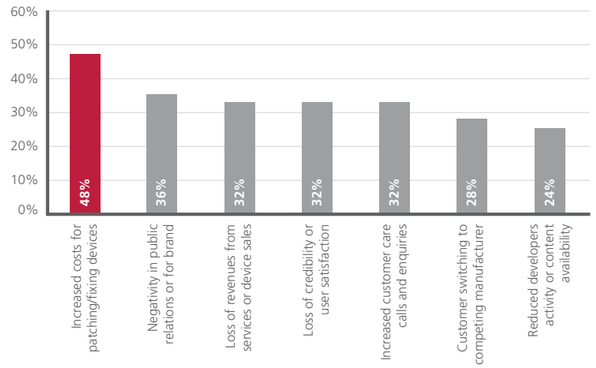
While mobile devices and services are still relatively safe, individual incidents have already had a significant impact on manufacturers' businesses. Almost half of participating vendors mentioned increased costs for patching and fixing devices. More than a third suffered from negative public relations or other brand damage followed by loss of credibility and user satisfaction. Recent experiences with releasing new mobile handset platforms, such as Android, have demonstrated how costly, complex, and annoying it can be for manufacturers, carriers, and users to distribute security solutions and patches for devices out in the field.

Surprisingly, participants reported a very weak connection between increase of incidents and third-party developer activity. In fact, most previous security incidents have prompted device manufacturers to introduce platform security and limit third-party applications to those vendors fulfilling stringent technical and liability conditions. This initiated a considerable decline in developer activity and innovation output, for example, for the Symbian operating systems and other platforms—a trend not reflected in Figure 4-1.

"Wireless devices make use of precious resources as far as the communication infrastructure is concerned."

– Mobile Device Chipset Vendor

Manufacturer's Business Areas Impacted Most Significantly by Mobile Security Incidents



Source: Informa Telecoms & Media

Figure 4-1. Significance of the perceived impact of previous security incidents on manufacturers businesses; percentage of respondents.

Focus Areas of Mobile Security Research

Results from interviews with manufacturers and component vendors enquiring about their top mobile security concerns showed close alignment with findings from McAfee research conducted among mobile operators at the beginning of 2007[1] and mobile consumers in early 2008[2]. Problems in PC environments, which are now accessible by mobile devices, are now top-of-mind concerns among mobile device manufacturers, operators, and mobile users.

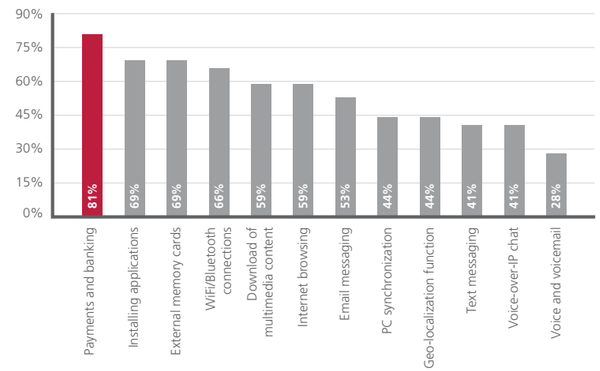
"Testing applications is not really our concern and it's not our business to deal with those issues."

– Mobile Network Operator

Areas of Highest Mobile Security Concern

Concern about mobile banking and payments security was mentioned most often by mobile device manufacturing companies. Initially introduced for the fixed line world, financial transactions have traditionally been a high attack and concern area. Today, service providers, banks, and PC manufacturers recommend the installation of personal protection products (often at no cost for the user.) But the situation is different in the mobile space. While mobile banking services are growing rapidly in developing countries, where other payment methods are rare, mobile devices continue to lack sufficient protection features.

Mobile Usage Areas with Highest Security Concern for Manufacturers



Source: Informa Telecoms & Media

Figure 5-1. The security concern level for various mobile device functions.

[1] *McAfee Mobile Security Report 2007,* Research among 200 mobile operators about their experiences with mobile security incidents.

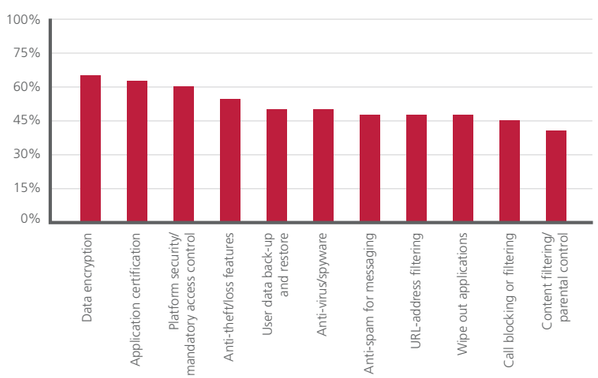
[2] *McAfee Mobile Security Report 2008,* Research among 2000 consumers in Japan, United Kingdom and United States about their mobile security concerns on mobile devices and mobile services.

"Downloading security patches for wireless operating Systems should become a transparent process."
– Mobile Device Chipset Vendor

"Reliability and trustworthiness of applications will become more of an issue."
– Mobile Device Chipset Vendor

Compounding the problem is the fact that additional protection features can't be installed on many devices once they have left the factory. Other top areas of concern for mobile manufacturers are downloading and installing applications and multimedia, and exchanging information or content via external memory cards. With manufacturers' limited control of voice, voicemail, and text messaging services, these areas are of least concern, despite the increase of related incidents discussed in Figure 3-1.

Security Features Implemented on Today's Mobile Devices



Source: Informa Telecoms & Media
©2009 Informa UK Ltd.

Figure 5-2. The security features included in at *least one* of participating vendors' device models; percentage of respondents.

Security Features Development

Fortunately, most mobile device manufacturing companies do deploy or plan to deploy security solutions addressing the concerns shown in Figure 5-1.

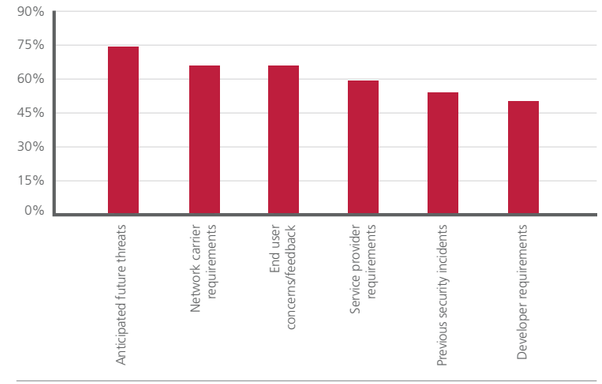
Figure 5-2 suggests that manufacturers have started to implement additional security features in some of their devices. However, interviewees confirmed that these were mostly limited to smartphone devices representing the minority of mobile device portfolios. The most commonly deployed security features are mobile device data encryption solutions, followed by mobile application certification, and platform security in the form of mandatory access control (MAC).

Recent attacks on various manufacturers' platform security features have made it clear that MAC alone is a very vulnerable approach if it is not complemented by other proactive security technology. In fact, the increased focus on platform security did not prevent security issues related to third-party applications and content (Figure 3-1). Relevant mitigating solutions such as anti-malware or other dynamic content security solutions—including the ability to wipe out certain applications—have not received equal deployment to date.

An Approach to Mobile Security

As mobile devices become increasingly multi-functional and connected to other guarded and unguarded networks, McAfee sees the need for additional security measures on the application, device platform, and network level. With limited control over the network domain, manufacturers are carefully examining security developments and threats to their platforms. However, past experience with previous security incidents has provided them with very limited guidance as to where to expect the next attack. Figure 6-1 reveals the drivers behind the consideration of proactive mobile security solutions at the device level.

What Drives Manufacturers to Implement Security Features on Mobile Devices



Source: Informa Telecoms & Media
©2009 Informa UK Ltd.

Figure 6-1. The most important drivers for integrating and offering mobile security in devices; percentage respondents.

"Subscribers are suffering, but it is mainly the carriers that complain."
– Mobile Device Manufacturer

"It is surprising how little pressure enterprises put on mobile device manufacturers to apply their security policies."
– Member of Standardization Group

Drivers for Security Deployments

Devices make mobile services and mobile content consumable. More services spark more device sales and more device sales will trigger more services. To keep the mobile ecosystem of service and device usage intact, manufacturers need to position their platform so that it attracts continuous innovation by developers and content producers. All of them demand universal access rights to fully utilize the power of today's devices. At the same time, these rights can be just as easily abused for malicious purposes that may impact a manufacturer's brand, trust, and revenue. Security helps device manufacturers balance control with open platforms that invite innovation.

At the same time, network operators, service providers, and, of course, users, have their security needs as well. Users want to be free to do what ever they like on their devices, but networks cannot always rely on consumers to make the right security choices. Here again, balancing end-user requirements with security policies at the network or device platform side requires additional, easy-to-manage mobile security solutions.

The Preferred User Experience

Mobile users want to be empowered with tools and information that can help them enjoy their devices and choose from the diverse mobile service and content offerings available today. However, detailed security options, warnings, and prompts have traditionally not been successful in empowering users and delivering the required security at the same time. Meanwhile, threats change continuously, making managing security a complex task.

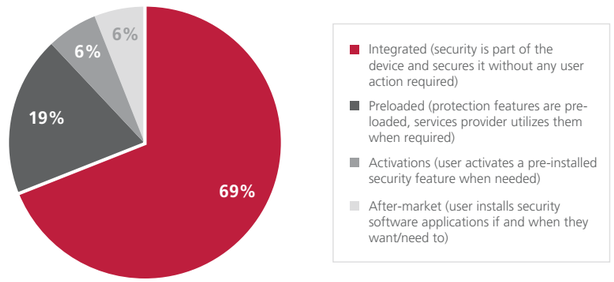
The majority of mobile device manufacturing companies (69 percent) believe that device-integrated security is the most effective and efficient way to protect devices, carriers, and users at the same time. This means protection should be part of the device, so it is secure without any additional user action required.

Nineteen percent of manufacturers believe that preloaded protection is appropriate, supporting the trend that mobile security shouldn't be a user's choice but rather should be professionally managed as a part of communications vendors' business discipline. Combining those groups leaves a minority of just 12 percent who believe users should bear the responsibility of proactively seeking their own security.

Three quarters of handset manufacturers and device component vendors excluded users from their business model for mobile security. Manufacturers want to be in control of security for their devices and are, therefore, including security technology as preloaded and prepaid functionality or services.

Manufacturers have to manage their own business risks and have started to create security requirements that go beyond those requested by carriers. The cost for protecting devices, services, and content is, therefore, expected to be borne by manufacturers and carriers according to the majority of survey participants.

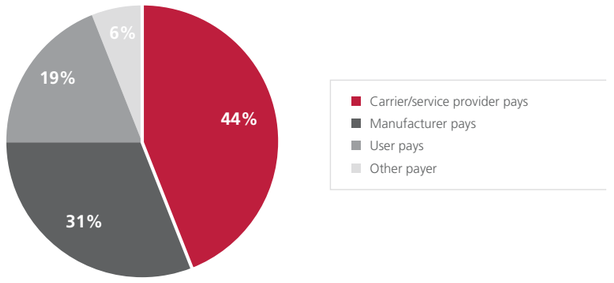
How to Secure Devices and Deliver Mobile Security to the Market



Source: Informa Telecoms & Media

Figure 6-2. The manufacturers' preference for handling security and deliver secured devices to the market.

Who Should Bear the Cost for Securing Mobile Devices?



Source: Informa Telecoms & Media

Figure 6-3. The manufacturers preferred business models for deploying core level mobile security on devices.

"We use inbuilt security on our devices to prevent other applications and malware being downloaded."
– Mobile Device Manufacturer

"The majority of users are not in a position to make intelligent security decisions based on warnings and prompts."
– Member of Standardization Group

Summary and Outlook

Mobile device manufacturers are experiencing more mobile malware attacks than ever before and spending more time and money on recovery from these attacks.

Infections from existing malware variants remain at a high level. Most issues reported today effect carriers' network capacity, indicating the type of business risks that may result from a security incident.

But manufacturers have experienced their own issues with installing applications, handling user data, and patching security solutions for devices out in the field. Manufacturers have mentioned that the increased cost for resolving problems was the most significant effect from previous mobile security incidents.

For more than 70 percent of manufacturers, mobile security is necessary in anticipation of future threats. Attacks on networks and devices are more sophisticated than ever. The recent increase in the level of sophistication of attacks has raised concerns about security for many existing and emerging services.

Manufacturers want to be in control of security for their devices. About 75 percent prefer to include security technology as a preloaded and prepaid functionality or service on their devices, limiting user interaction and responsibility.

Most commonly deployed security measures include mobile encryption solutions, application certification, and platform security in the form of mandatory access control (MAC). However, the recent attacks on multiple vendors' platform security have demonstrated the need for complementary security technology, such as dynamic content security, including the ability to wipe out or block malicious or unwanted content or services.

Fortunately, McAfee has been closely monitoring the mobile security landscape since 2001 and has developed solutions to protect manufacturers and operators. McAfee Integrated Content Security has been shipped on more than 100 million mobile devices, placing us in a unique position in the global marketplace.

McAfee Mobile Security Solutions

Effective protection of networks, devices, applications, and content is necessary to safeguard a user's current and future experience, lower adoption barriers, and protect mobile players' businesses and brands. To achieve success in the market, new services, such as mobile payments or mobile localization, will require multiple levels of security.

McAfee® mobile security products and services help mobile device manufacturers and network operators take proactive measures to stay on top of these developments and to not only prevent costly disruptions, but also prepare their environment for the level of security required by new service offerings.

For more information visit:
http://www.mcafee.com/mobile

About McAfee, Inc.

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee is relentlessly committed to tackling the world's toughest security challenges. The company delivers proactive and proven solutions and services that help secure systems and networks around the world, allowing users to safely connect to the Internet, browse and shop the web more securely. Backed by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security.

About Informa Telecoms & Media

Informa Telecoms & Media is the leading provider of business intelligence and strategic services to the global telecoms and media markets through two key strands.

Providing business critical information—ITM products offer innovative formats and powerful channels to meet customers' real business needs, with research services, reports and consultancy that guides the decisions of over 10,000 leading decision makers.

Creating communities—ITM actively fosters and empowers the communities it works with, promoting debates and sharing best practice, solving problems and stimulating innovation through its magazines, online portals, large exhibitions, focused conferences and networking lunches.

McAfee®

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com