

MOBILE SECURITY—WHY THE TIME IS NOW

Mobile Carriers Must Implement Security Now to Protect the New Wave of Mobile Devices from a Variety of Security Threats

Table of Contents

Executive Summary	3
Introduction	3
The Changing Mobile Device	4
Opening the Mobile Device and Network	5
Mobile Devices	5
Mobile Networks	5
The New Wave of Applications	6
The Mobility Factors	7
Cybersecurity	7
Conclusion	7
About Juniper Networks.	8

Table of Figures

Figure 1: Mobile devices are evolving into multi-functional devices	4
Figure 2: Graphs depicting botnet and DDoS attacks	5

Executive Summary

Mobile security is quickly becoming essential for mobile carriers. As mobile devices and networks continue to evolve from second generation (2G) to broadband speeds and also become more open, security attacks on mobile networks and devices will likely increase substantially.

The global acceptance of smart phones, netbooks, PC cards/dongles, and other third-generation (3G) devices is enabling mobile users to access and generate more content and applications, many involving financial transactions. In addition, mobile carriers are opening up their networks from the traditional walled gardens. While this creates new revenue opportunities, it also opens the door to new security threats. While most hackers are still focusing on the fixed line or computer world, there is a perfect storm occurring in the mobile industry that makes it ripe for a bombardment of security attacks. This paper will discuss some of the key factors that are contributing to the increasing need for mobile security including:

1. Mobile devices—they are changing dramatically and are now as powerful as laptops and other computing devices.
2. Open devices and networks—services and applications have moved to IP and given the user more control, exposing the network and users to additional security risks.
3. Applications—thousands of applications with billions of downloads are now happening.
4. Massive increases in bandwidth from data services—these are increasing the number of attacks on network signaling and applications layers.

Mobile security has not traditionally been at the top of the priority list for most mobile carriers. However, as the mobile industry becomes similar to the fixed line world and the number of attacks continues to grow substantially each year, mobile operators need to pay more attention to securing their networks and subscribers. Without having a multilayer security architecture in place, mobile attacks could have a dramatic impact on the growth of the mobile industry.

Introduction

Mobile security is an area which mobile carriers have so far not given too much attention. However, that is now changing due to a variety of factors that are occurring in the mobile industry. Up until the last year or so, mobile users primarily used their mobile devices for voice communications, with little to no mobile data activity. Data applications that were available were contained in a walled garden and only available on the mobile carrier's network, thus closed off from the rest of the data world.

However, the walled garden mobile environment has now quickly changed as mobile devices are becoming more open. These open devices need open networks to get the full benefit of the openness of the device. This is pressuring mobile operators to open their networks and allow the mobile user to do more with their devices. This in turn has led to a new phenomenon in mobile applications, as mobile users can now access thousands and thousands of applications. Mobile commerce performed over these open mobile devices is also becoming much more prevalent, with many mobile users now getting more comfortable shopping or purchasing items with their mobile device. All of these things open the door for mobile carriers to drive new revenues. It also opens the door for new security threats that can potentially do harm to mobile users and to the carrier's revenue streams.

As smart phone sales continue to take off, the potential mobile targets for hackers to perform malicious acts in order to achieve financial gain will quickly outnumber those in the computer world. This time is approaching very quickly and mobile carriers need to prepare now to protect their networks and users from these new threats. The consequences of not implementing security could have devastating impacts on the future growth of the mobile industry.

The Changing Mobile Device

Times have changed dramatically since 1946 when the first mobile telephone call was made. For the first 60 years, there was really only one purpose for a mobile device—to conduct phone calls. This was a relatively simple process, and for the most part it was secure. Mobile carriers only had to worry about potential phone fraud but security was not something that was a high priority for them.

Over the past few years, there has been a wave of new mobile devices that run on 3G networks. These devices include smart devices, PC cards/dongles, and netbooks. In many ways, these new 3G devices are comparable to today's laptops or desktops, only mobile. While they are used for voice communications, they are designed for much more. A typical smart phone today is able to:

- Use 3G technology or Wi-Fi to access the data network at broadband speeds
- Access any website (many built for mobile) in an open environment
- Have access to thousands of mobile applications
- Synchronize emails, contacts, calendars, etc. with personal and corporate email systems
- Download and manage digital music, photos, podcasts, videos, and other multimedia

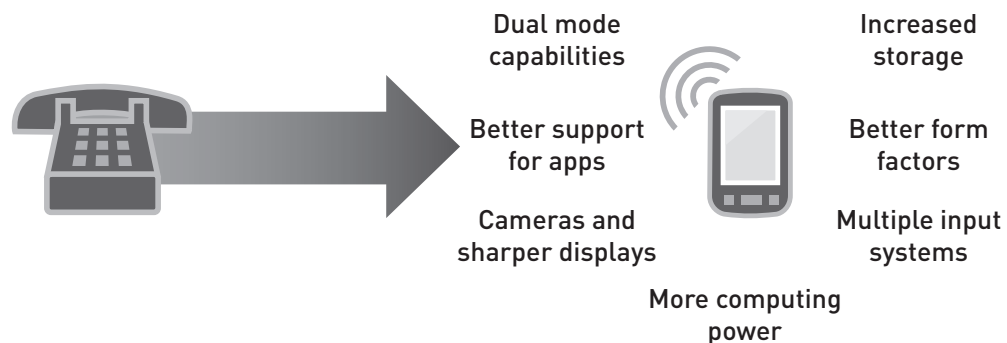


Figure 1: Mobile devices are evolving into multi-functional devices

The capabilities of new mobile devices enable the mobile user to perform a variety of functions. In fact, voice calling is quickly becoming less important. Other means of communicating, such as Short Message Service (SMS) or Multimedia Messaging Service (MMS), are quickly becoming more main stream. As the demand for enhanced functionality rises, smart devices will continue to become increasingly powerful. This will ultimately lead to an increase in security attacks—something about which the mobile carrier did not have to be concerned when voice calls were the mobile device's main function.

To understand the potential impact that security attacks might have on the mobile industry, one needs to look no further than the computer world. Service providers and enterprises spend billions of dollars each year trying to protect their networks and services from attacks. They are under constant bombardment from distributed denial of service (DDoS) attacks and new, more complex attacks such as botnets. While almost none of these attacks hits the mainstream news for security reasons, the number of attacks has increased dramatically in the past few years (see figure below). The mobile industry is likely to follow the same fate—as mobile devices become more and more like their wireline counterparts, they will be targets of a multitude of attacks. In fact, due to the dynamics of mobility and the sheer number of mobile devices, the mobile industry could be impacted far more than the wireline industry has been.

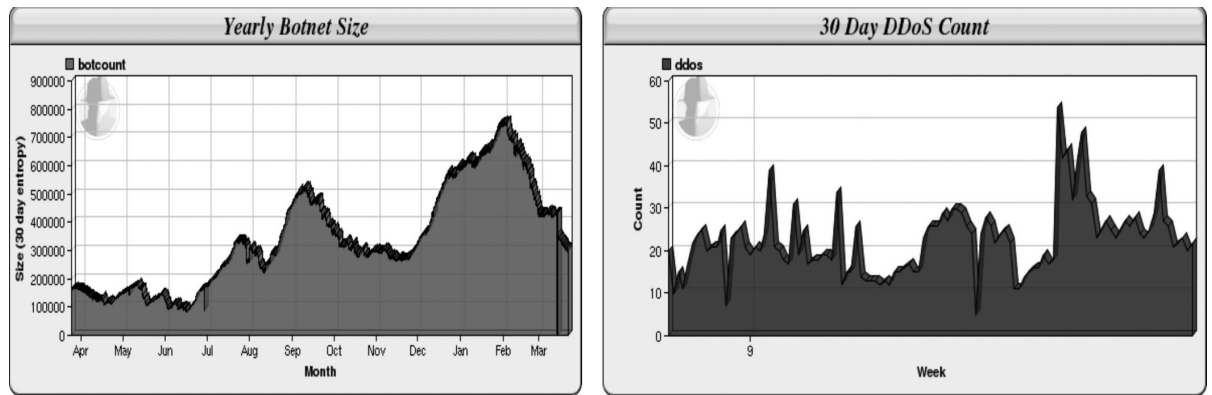


Figure 2: Graphs depicting botnet and DDoS attacks

Wireline networks have been the target of attacks for many years. However, the nature of attacks has evolved over the years. The initial focus was for the hacker to try to take down a service, such as a website, through techniques such as a DDoS attack. While these types of attacks are still common today, many hackers increasingly focus on trying to obtain some sort of financial gain. This includes trying to steal credit card information, social security numbers, or conduct service fraud, to name a few. Hackers can use this stolen information themselves or they can sell the stolen information on the black market for a significant price. The primary focus so far has been on fixed line networks. However, as the number of smart phones and 3G devices increase and the ability of these devices to conduct financial transactions increases as well, the hacker's attention will likely shift from wireline to also include mobile network attacks. It is imperative that mobile operators prepare now.

Opening the Mobile Device and Network

A second trend happening within the mobile world that has significant security implications is the increasing openness of mobile networks and devices. Opening things up provides opportunity for everyone—the mobile user, the mobile carrier, and also the hacker.

Mobile Devices

Before 3G networks, there wasn't too much trouble a mobile user could get into. The primary activity was simply placing and receiving voice calls. Mobile data was somewhat limited to the mobile operator's walled garden and also the relatively slow data speeds. While the subscriber could browse news stories and even download some content such as ringtones, all of the content was primarily kept under the mobile operator's control, thus limiting the exposure to security threats. However, as the mobile network and devices both become more open, the risk of security attacks will increase.

As previously stated, traditional mobile devices were closed devices. Users were not able to do much in terms of loading new applications or customizing their phones, and the user was mainly limited to the applications that were originally installed on their phone. While this is good from a security perspective, users are accustomed to the openness of the computer world and aren't satisfied with the limited nature of closed devices. Many mobile users get frustrated when going from an open computer device to having to use a closed mobile device. Therefore, the trend in the mobile industry is towards opening up the phone. Many of the smart phones are run on open software such as Android, Symbian, or Windows Mobile. These operating systems provide much more user flexibility in terms of loading applications and customizing the phone.

Mobile Networks

In addition to opening up mobile devices, mobile carriers are also opening up their networks. The days of the closed walled garden model are fading fast. Walled gardens are a way for the mobile carrier to control the content to which a mobile user has access. Walled gardens include static menus that allow the mobile user to access specific content and/or applications. This confines the mobile user to specific content, a big departure from the computer world.

Today's smart phones are now able to access the open mobile network. Aside from being able to support some plug-ins, smart phones are able to access a far greater amount of content and number of applications. This allows mobile users to access websites that they were not able to access in the walled garden model.

Along with the added flexibility of open devices and networks comes more potential harm. Installing a virus and other malware is much easier to do in these open machines and networks, as a mobile user can unknowingly download and install a virus assuming that it is a legitimate application. This can lead to stolen personal information including credit card numbers and more. As more and more mobile users migrate to smart phones and open themselves up to security threats in the process, mobile carriers need to find ways to protect them from harmful attacks.

There have already been many known cases of viruses found in smart phones. There have been viruses that attack the Safari Web browser of the iPhone that have caused problems for users. Viruses exploiting vulnerabilities in applications such as the Safari Web browser can cause a denial of service (DoS) attack. Mobile users simply browse to a website that contains the malicious virus script and the virus is triggered, eating up memory in your iPhone and causing it to crash. This is just one example of how open devices running on open networks can easily (and unknowingly) download a virus to render a mobile device useless. While these cases are not significant today, they do show that hackers are starting to take notice of the mobile industry and their attacks will only get more complex and damaging over time.

The New Wave of Applications

The new open devices are driving new applications that mobile users can download and subsequently run on a mobile device. This is familiar to the computer world but it is a relatively new phenomenon in the mobile world. As the number of smart devices increases, so too does the number of available applications. One example is the Apple iPhone. The iPhone has dramatically changed the mobile market by making available an unprecedented number of applications that are available to download and install on the iPhone. In just 9 months, iPhone users have downloaded over one billion applications. This is only the beginning of the application market and depicts the exploding demand for mobile users to be able to customize and run applications in a mobile environment.

The wave of new applications can cause alarm in a couple different areas. For one thing, while most mobile applications are still offered in a controlled environment, it's only a matter of time before hackers figure out a way to penetrate this market. With billions and billions of downloads occurring and thousands of applications, it's a big market that will eventually attract hackers. Secondly, many application developers charge a fee for their applications. This is driving a very large number of financial transactions over the network. According to Garner, Inc., the mobile payment industry will experience steady growth, as the number of mobile payment users worldwide will total 73.4 million in 2009, up 70.4% from 2008 when there were 43.1 million users. In addition, Gartner predicts that the number of mobile payment users will reach more than 190 million in 2012, representing more than 3% of total mobile users worldwide and attaining a level at which it will be considered mainstream.

Mobile commerce and mobile payments provide a significant opportunity for security hackers. As the number of mobile users conduct mobile commerce and become comfortable doing so, the number of potential targets will outweigh the wireline side. This will likely entice security hackers to focus attention on the mobile industry and target smart devices for financial gain. Knowing that hackers tend to go where the money is, this is certainly an area about which mobile carriers need to be concerned from a security perspective. If mobile users do not feel it is safe to purchase new applications, this lack of trust will have a dramatic effect on the growth of the mobile carrier's business.

As the mobile network evolves from 3G to high broadband speeds such as Long Term Evolution (LTE), mobile devices and the trend for applications will continue to increase. Broadband speeds will fuel this phenomenon and make security an even bigger challenge.

The Mobility Factors

One very interesting statistic that is bound to get the hacker's attention is the sheer size of the mobile market. The number of mobile devices hit 4 billion in 2008. By 2015, mobile numbers will outnumber fixed lines by a 9:1 ratio. A large percentage of these mobile devices are not smart phones and perform basic functionality within walled gardens. However, this will change as smart phones become more affordable and mobile network speeds increase to support even more applications such as streaming video. As this transformation occurs, mobile security will be increasingly critical, and it is something that mobile carriers need to start preparing for now.

In the computer world, users can take some action to protect themselves from certain things such as viruses. Users can install antivirus, firewall, and other software to help protect their machines from a variety of security exploits. Thus, there is the somewhat prevailing view that users can help themselves and are expected to share some security responsibilities with their service providers. When viruses or botnets successfully infect a large number of users, antivirus definitions and other means can be downloaded and installed to help defend these threats.

The mobile world today is much different. Mobile users do not place antivirus or spyware detection programs on their mobile devices. When a mobile-oriented virus is known, there is little that a user can do to protect a device. Thus, the entire responsibility for the containment for security threats is placed on mobile carriers, as they are the one source of protection that mobile users have to defend against any threats. At some point, this might change as mobile devices become more powerful and can handle processing intensive applications such as antivirus programs, but this represents a fundamental difference in how security defense is played out in the mobile industry versus the computer world today.

Cybersecurity

It is worth noting that cybersecurity has been an important topic in the United States recently. In fact, a recent study by the Center for Strategic and International Studies wrote, "Cybersecurity is among the most serious economic and national security challenges we face in the twenty-first century. Our investigations and interviews for this report made it clear we are in a long-term struggle with criminals, foreign intelligence agencies, militaries, and others with whom we are intimately and unavoidably connected through a global digital network; and this struggle does more real damage every day to the economic health and national security of the United States than any other threat." As the United States and other governments come to understand the threat security attacks present, it is imperative that mobile operators also understand the threat posed to their networks and subscribers.

Conclusion

The mobile industry is at a perfect storm when it comes to security. Phones are getting much smarter, mobile networks are getting much faster, and both phones and networks are becoming more open. All of these factors are contributing to billions of new application downloads and a much higher average revenue per user (ARPU) for mobile carriers stemming from data services. We are only at the beginning of this phenomenon, and mobile security will become a much bigger issue for mobile users, mobile carriers, and, unfortunately, for hackers as this trend continues to grow.

Similar to the way the computer world has been attacked by DDoS, viruses, and botnets, mobile carriers will also come increasingly under fire. Mobile attacks will be driven by the increase in open networks, open devices, and financial transactions conducted over the mobile network. It is difficult for mobile users to protect themselves, so it will be important for mobile carriers to move mobile security to the forefront, protecting their users and their revenue streams from hackers and the coming onslaught of security attacks.

About Juniper Networks

Juniper Networks,[®] Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.

Corporate and Sales Headquarters

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

Copyright 2010 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.