May 2014

An eBook from the editors of FierceWireless

Keeping Wireless Networks & Devices Secure

Thank you to our sponsors:

CLOUDMARK®

f5

Editor's Note

By Sue Marek
Editor-in-Chief /// *FierceWireless*

Smartphones have become dramatically more sophisticated over the past few years making them more similar to tiny computers than phones. But that sophistication has led to vulnerability – making today's smartphones just as susceptible to malware and security breaches as your typical laptop or desktop PC.

Google's Android operating system has been a primary target for a lot of mobile malware. In fact, according to Juniper Networks' research, about 92 percent of mobile malware threats in 2013 were aimed at Android.

Premium SMS is another area of vulnerability. All major U.S. operators are involved in the GSMA's Spam Reporting Service which proactively addresses global messaging threats. Nevertheless, spammers continue to try to get unsuspecting consumers to provide their bank account information via SMS.

Meanwhile, Wi-Fi networks, which are increasingly used by mobile operators to offload their cellular traffic, have made great strides to diminish their susceptibility to security threats. In fact, experts say that many popular applications that consumers use in public Wi-Fi hotspots, which were once thought to be a high security risk, now use secure SSL for encrypting data end-to-end making them much more secure.

However, one area of big concern is the Internet of Things. With the potential of all types of devices and gadgets being connected wirelessly, experts say there is a huge risk for security threats. And those threats could be particularly dire if, for example, a hacker tapped into an automobile sensor system and was able to control car functions, like brakes. Or even worse, a hacker was able to tap into a medical device, like pacemaker or insulin pump, with potentially dire consequences.

Network operators and the entire wireless ecosystem will likely always be faced with combatting network and device security issues. The challenge is to stay one step ahead of the hackers and keep security breaches to a minimum.

In the latest ebook from *FierceWireless*, "Keeping Wireless Networks and Devices Secure," we take an in-depth look at the various security threats to mobile networks and devices and the solutions that wireless operators are deploying to prevent them. ■

Wi-Fi Gets Its Game On

Wi-Fi advocates say the technology has made huge strides when it comes to the simplicity and ease in making it more secure.

By Monica Alleven

Wi-Fi has come a long way since the 1990s, when it was designated a second-class citizen by many mobile operators and skeptics of unlicensed spectrum. Fast forward to 2014, and not only is Wi-Fi deemed secure enough for Fortune 100 companies, but mobile service providers are using it to share the traffic burden and operate their own Wi-Fi networks.

That might not be surprising given the ubiquity of Wi-Fi. While 66 percent of tablets lack cellular connectivity, all have Wi-Fi, and smartphones without Wi-Fi are an oddity, notes Senza Fili Consulting. According to the Cisco Visual Networking Index (VNI), the amount of traffic offloaded to Wi-Fi from LTE was 54 percent at the end of 2013 and will be 56 percent by 2018.

Security: Mixed Bag

Clearly, Wi-Fi is here to stay in a big way, and efforts are underway to further improve its security—and perceptions thereof. The FBI as recently as 2012 issued a warning to travelers abroad who were being targeted via Wi-Fi in hotels. Instead of legitimate connections, they were getting "spoofed" into thinking they were logging into a secure site when in fact the perpetrators were stealing passwords and other sensitive information.

Wi-Fi generally is believed to be more susceptible to security threats when it's free in public places, like coffee shops or airports, because it's "open." Hackers can set up fake Wi-Fi hotspots with names like "Free Wi-Fi" and steal passwords and other information. Experts warn users to make sure they use only SSL-encrypted services, denoted by https:// instead of http:// or use a VPN to log in.

But some say Wi-Fi gets a bad rap. Dave Fraser, CEO of hotspot aggregator Devicescape, said reports citing security issues around public hotspots are "completely overblown." Some of the most popular applications that consumers use in coffee shops and cafes are Facebook and Google, which use secure SSL for encrypting the data end-to- end, he said.

Having said that, he added, it's incredibly important that the data sent on behalf of mobile operators is secure, "so we help them layer on security." Devicescape aggregates public Wi-Fi access points to create what

feels like a single network. "We basically make the Wi-Fi experience feel just the same as cellular," Fraser said. The company works with about 39 operators, mostly Tier 2s and 3s in the United States, including U.S. Cellular and Republic Wireless.

Hotspot 2.0 to the Rescue

To make Wi-Fi roaming easier and more secure, the Wi-Fi Alliance created Hotspot 2.0, an interoperable Wi-Fi authentication and handoff technology that enables automatic roaming between Wi-Fi hotspots. The Wi-Fi Alliance offers a certification program for Hotspot 2.0 devices under its Passpoint brand.

This past April, Time Warner Cable staked the claim as the largest Passpoint-enabled network in the United States, offering the technology on 33,000 access points in its markets. TWC said the new service uses "powerful encryption technology" to ensure customers get the same level of protection on TWC's public Wi-Fi network that they get with their in-home TWC Wi-Fi connection.

For years, the industry talked about how the processes and procedures for using secure Wi-Fi needed to be simplified, said Boingo CTO Derek Peterson. Typically, the process involved getting a WPA key, entering passwords and/or searching for network names and SSIDs. "That whole concept of Wi-Fi has been challenging for people who are not technical," he said, adding that sharing passwords, a common practice, isn't ideal when you're talking about security.

Hotspot 2.0 addresses those issues, making the process more automatic for the end-user. "The real challenge is not technical, it's a business challenge," he said, acknowledging that consumers are accustomed to free Wi-Fi and changing that paradigm is difficult. Operators need to either get their customers to pay for it or include it in a bundled offering.

Boingo has carrier offload agreements with three of the four biggest mobile carriers in the United States. Eventually, the company expects to generate significant revenue from Hotspot 2.0 by acting more like a traditional roaming partner.

"We basically make the Wi-Fi experience feel just the same as cellular."

DAVE FRASER, CEO DEVICESCAPE

Earlier this year, Boingo launched its Passpoint Secure networks at more than 20 airports throughout the United States, including Los Angeles International, New York's John F. Kennedy and Chicago O'Hare airports. The airport networks are accessible to Boingo subscribers using Passpoint-capable Apple mobile devices running iOS 7 and Macintosh laptops running Mavericks OS X (10.9). The company plans to add Android and Microsoft as well, Peterson said.

"This [Hotspot 2.0] is going to take time, of course. Like anything, there's a ramp-up time," Peterson said.

"We're trying to help people and the industry get to where it needs to go."

Good enough for government

While Wi-Fi advocates might argue among themselves as to how secure various Wi-Fi networks are today, they can agree that great strides have been made in the ease and simplicity of using secure systems.

Is it secure enough for the White House? "I would venture to say yes," said Mads Lillelund, general manager for ADTRAN's BlueSocket division, which pioneered the virtual WLAN controller market. "I could almost walk into an enterprise and hack their wired networks faster than I could hack their wireless network."

That's because many enterprises leave their wired networks open in conference rooms so that anyone can come in and use them, thereby leaving them exposed and susceptible to nefarious acts and characters, he said. In a secured enterprise Wi-Fi network, either users are allowed access to the network or they're not.

"I could almost walk into an enterprise and hack their wired networks faster than I could hack their wireless network."

MADS LILLELUND, GENERAL MANAGER FOR ADTRAN'S BLUESOCKET DIVISION

Mathew Gast, director of advanced technology for Aerohive Networks, author of "802.11ac: A Survival Guide" and security task group chairman at the Wi-Fi Alliance, offers a different perspective. Because government IT uses a different class of requirements, such as classified vs. unclassified and various levels of security clearances, a better question than the White House test is whether Wi-Fi is secure enough for transmitting sensitive financial and healthcare information, and the answer to both is "yes," he said.

Security is like wine in that it gets better with time, he said. If it stands the test of time and survives countless attempts to hack it, it's probably worth keeping. ■

In-Network Security is Critical to Safeguarding Mobile Messaging

By Neil Cook, CTO, Cloudmark

Evolving threats in the mobile landscape create an increasing need for in-network solutions to protect endpoint devices. Threats such as the ability to remotely root SIM cards and phishing (both via SMS) affects trust in mobile communications for both consumers and businesses. Current endpoint solutions alone are not enough to protect mobile devices from today's attacks. The result of these threats directly affects general usage and services like two-factor authentication.

In 2013, security researcher Karsten Nohl disclosed one such shortcoming in endpoint mobile security. This attack allowed an advisory to easily root and gain full control of any DES-encrypted SIM card over-the-air via an SMS. The attack relied on the relative weakness of encryption on older, legacy SIM cards that are still widely used globally. A malicious update like this must be pushed over SMS and through the operator's network to reach the device. Conversely, an in-network whitelist of trusted sources for SIM updates could easily nullify this update and any future version of this attack by simply intercepting delivery of the messages to the handset.

A typical end user is unable to stay responsibly informed about the multitude of ever-changing mobile threats that pose security risks to endpoint devices. This lack of knowledge, combined with subscribers' inherent trust for mobile communications, creates a potent attack vector for social engineering, which has not gone unnoticed. During the first quarter of 2014, 46 percent of all reported unsolicited SMS in the U.S. were documented as forms of malicious phishing attempts. The rising popularity of these messages suggests that spammers are gaining success in tricking users. Here is an example of one such phishing attempt:

*"(Beneficial Bank) 4224 81** **** **** Debit Card Limited Due To Fraud. Call: 877 684 6966"*

Network filtering plays a fundamental role in disrupting these types of abusive phishing messages from ever reaching endpoint devices by prohibiting the delivery of unwanted or malicious SMS. Moreover, this solution is more effective than relying on phone filtering apps that are highly susceptible to mobile malware and consume precious battery life and processing power.

With the proliferation of malicious SMS, network security is vital to retaining subscribers' trust in mobile messaging. Without a multi-pronged response to these continuous attacks, confidence in mobile messaging may begin to erode as it did with email security – exacerbating a shift towards app-based or hardware token two-factor authentication methods. Therefore, malicious SMS attacks give rise to the need for greater in-network security measures to insulate subscribers from threats. ■

Securing the Internet of Things is no easy matter

There are currently just a few real examples of attacks on IoT devices, but it's time to do the preventative work to stop future damage.

By Nancy Gohring

It's already begun: Hackers are targeting the Internet of Things.

In January, security company Proofpoint reported that it had discovered an attack that sent more than 750,000 malicious email messages from 100,000 devices including smart TVs, home routers and at least one connected refrigerator.

Proofpoint reported that it thinks this was the first proven IoT cyberattack.

Late last year, Symantec discovered a worm that seemed designed to try to target IoT devices, although it hadn't succeeded in actually doing so.

Both attacks harnessed traditional paths to monetization, like spam, indicating that malicious code writers are transferring proven methods in the PC and phone worlds to the IoT. They're just starting to try to figure out how they might benefit from IoT attacks.

Kaspersky Lab sees additional evidence that hackers are spreading their wings. It's seeing an expansion of attack techniques toward embedded firmware. So far, the attacks have been targeted at devices such as routers but the shift indicates that hackers are focusing on new technologies of the kind that are used in IoT devices. "It's moving away from a Windows focus and toward embedded devices, which is what the Internet of Things is made up of," said Kurt Baumgartner, principal security researcher at Kaspersky.

Security researchers have demonstrated much more alarming possibilities too. A few years ago, university researchers pointed out vulnerabilities in automobile sensor systems that could allow hackers to track vehicles remotely or potentially do more damage by controlling many different functions, like the brakes.

Researchers have also shown that it's possible to hack medical devices, such as pacemakers and insulin pumps, with potentially dire consequences.

All of this activity points to a need to secure the fast emerging IoT ecosystem.

IoT startup frenzy challenging to security

While vendors in the IoT market are starting to talk about how to do so, there are challenges slowing down their progress.

One issue is that IoT is a hot market, attracting the startup community. "These startups with great ideas rush to get all these ideas implemented in a product. Then they get acquired. In turn, their lack of attention to security details gets pushed out by these larger companies snapping them up," Baumgartner said. Sometimes the new products aren't even using the most basic security techniques, like SSL for authenticating connections with backend servers, he said.

Another reason that security is overlooked is because in many cases the sensor needs to be very low cost to support the business model. "When every cent counts, you may not be able to justify putting in a powerful enough processor to do something like encryption," said Bret Hartman, CTO of Cisco's Security Group.

Plus, some devices are designed to be in the field for a very long time and may not be able to be updated remotely. "All these endpoints may very well have flaws or vulnerabilities built into them that somebody might be able to exploit," Hartman said.

Even when devices like TVs or streaming devices such as a Roku box can be remotely updated, doing so isn't easy. Nest, the connected thermostat, caused a customer uproar earlier this year when a software update created problems for some users, including the loss of Wi-Fi connectivity. The update wasn't security-related, but the scenario highlights that pushing out changes isn't easy and can cause new problems. "That's one of the risks when you start updating things," said Eric Hanselman, an analyst at 451 Research.

Open standards are appealing

All is not lost, however. Vendors are working on using the same kinds of techniques that they use to fight malware on PCs and phones to prevent hackers from disrupting the IoT.

"These startups with great ideas rush to get all these ideas implemented in a product. Then they get acquired. In turn, their lack of attention to security details gets pushed out by these larger companies snapping them up."

KURT BAUMGARTNER, PRINCIPAL SECURITY RESEARCHER AT KASPERSKY LAB

On the device end, Kaspersky is pushing for open standards around technology that would build security functionality in low resource environments, Baumgartner said.

In addition, vendors should create expectations so that end users are aware that security may be a problem and that updates may come to ensure the security of the devices, Hanselman said.

But sometimes it's just not possible to add many kinds

of protection to the device. "There's no place to put security, say, in a light bulb," Hartman said.

As a result, Cisco is working on expanding its existing network products to encompass the IoT. "We focus a lot today on the network fabric," he said. In the IoT "it's the same basic principle. So it's watching how the refrigerator communicates with the thermostat. We have network devices that permit that visibility."

"If you're talking about millions of devices in the network, you can't do things manually any more."

BRET HARTMAN, CTO OF CISCO'S SECURITY GROUP

Those network devices analyze traffic to look for unusual patterns. When they detect odd behavior, they can isolate the device to limit the damage it can do.

Cisco is working on more ways to automate this process because of the scale of IoT devices that are expected to proliferate. "If you're talking about millions of devices in the network, you can't do things manually any more," Hartman said.

The added layers of security will cost money and, particularly on the consumer device end, vendors are usually reluctant to raise costs for end users, Hanselman said. Unfortunately, users typically aren't prepared to pay extra for security until real problems have occurred that show the risk.

"Selling security has always been about catalyzing events," Hanselman said. "Take a look at Heartbleed. Lots of passwords were changed that wouldn't otherwise." ■

Android: The Center of the Mobile Malware Universe

Android continues to attract the bulk of mobile spam. But Android 4.2 will create a malware roadblock.

By Nancy Gohring

Over the past couple of years, there are a couple of trends around mobile malware that have been easy to count on. One is that even as the volume of mobile malware grows at a faster rate than many would have thought possible, Android continues to be the primary target.

In the year ending March 2013, the total amount of mobile malware that Juniper Networks' Mobile Threat Center found grew 614 percent. That compared to a 155 percent increase in 2011.

Of the mobile malware that Juniper found in 2013, 92 percent was aimed at Android.

Another fact in the mobile malware environment that's been easy to count on is that the predominant kind of attack has been to use malware to send premium rate SMS messages. The malware sends a premium rate SMS from the infected phone to a number controlled by the attacker. The phone user gets charged for the message and the attacker profits.

Juniper found that these premium rate SMS attacks made up 73 percent of all malware that it found.

However, experts now say that they expect to see changes in the kind of Android malware to come in the future.

"What we saw in the early days was a complex testing of capabilities, things you could do with Android malware," said Troy Vennon, director of Mobile Threat Center Research for Juniper Networks. But in late 2012 that all changed and malware authors focused predominantly on the premium rate SMS method. It became clear that this was a solid moneymaker and so attackers largely quit experimenting with other techniques.

Android 4.2 creates a malware roadblock

Now though, a new roadblock may soon make it harder for the premium SMS attack to succeed. With version 4.2 of Android, Google added a feature that requires

users to confirm that they know they're sending a premium rate SMS message.

The premium SMS malware "could all but be removed if the user base would get the security update Google is trying to push out," Vennon said. The problem is that the Android ecosystem is notoriously slow to deliver operating system updates. Version 4.2 was released in late 2012 but as of early May only around 35 percent of Android users have it, according to Google.

"Not a lot of cybercriminals have switched over to seriously making money in mobile yet."

KEVIN MCNAMEE, DIRECTOR OF ALCATEL-LUCENT'S KINDSIGHT SECURITY LABS

As the premium rate SMS door slowly closes, malware writers are starting to look for new possibilities.

Juniper is starting to see examples of ransomware, where malware appears to be antivirus software and locks the device, preventing further use unless the user pays from $10 to $100, Vennon said.

Another new technique is malware that does Bitcoin mining unbeknownst to the phone's user, said Armando Orozco, senior malware intelligence analyst at Malwarebytes, a popular Android anti-virus app available in the Play Store.

"What's interesting about those is I believe it's not your typical malware authors," he said. It's clear from the way the code is written that the authors are likely traditional app developers who think they may have found an easy way to make some money via bitcoin mining, he said.

Lookout reported finding a few of these mining apps hidden in the Google Play store in April.

Alcatel-Lucent doesn't expect bitcoin mining to become particularly widespread in the mobile world, however. "The phone platform is not that good for bitcoin mining because it doesn't have the CPU power you'd want and it drains your battery quickly," said Kevin McNamee, director of Alcatel-Lucent's Kindsight Security Labs.

A newer kind of malware he's starting to see allows someone to use another phone as a proxy to surf the Web. The point is to let the remote user surf anonymously, he said. In addition to potentially racking up big data usage bills, this technique could be troublesome if the remote user is visiting sites that could raise concerns among law enforcement authorities. In that case, it looks like the phone owner is visiting those sites.

He hasn't seen many denial of service attacks launched from mobile phones but said the potential for such attacks is there and the consequences could be alarming. They could cripple the mobile networks, he said.

Malware attacks are still rare

Despite the alarming statistics around the growth of

mobile malware and the emergence of these new kinds of attacks, the chances of getting infected are still quite low. “Not a lot of cybercriminals have switched over to seriously making money in mobile yet,” McNamee said.

It’s difficult to get a handle on total infection rates since most of the research comes from vendors and they can only study malware that impacts their own customers. But Alcatel-Lucent’s Kindsight Security Labs estimates that .55 percent of mobile phones were infected by the end of 2013, and 60 percent of those were Android phones. Vennon said Juniper estimates closer to a 4 percent infection rate. That compares to around 9 percent in the Windows PC world.

Part of the reason for relatively low infection rates is the way that Android malware spreads. It’s primarily through social engineering, Vennon said, meaning that end users are somehow tricked into downloading the malware.

One of the most common ways that happens is when malware writers trick users of third-party app stores into thinking they’re downloading legitimate apps. Because North American users tend to stick with the Google Play Store, they’re less likely to get infected than people in other regions. Phone users in Europe, the Middle East and Asia, favor the third party app stores.

“It doesn’t seem like the owners of those sites really care to keep them clean,” Orozco said.

When Malwarebytes first rolled out its app in October last year, it thought maybe 90 percent of users would come from the U.S. In fact, only around 60 percent are from the U.S., he said. The rest of its users are spread out around the world, including in places like Malaysia and Vietnam.

While sticking with the Google Play store isn’t a fool proof way to avoid malware, it can help. So can anti-malware products, which operators are increasingly preloading on Android devices to try to help keep users safe. In addition, companies like Alcatel-Lucent’s Kindsight offer network based security systems that monitor networks for malware. ■

Dynamic Multi-Layered Security

By Leonid Burakovsky, Senior Director of Strategic Solutions, F5 Networks

Service Providers (SPs) are increasingly having to deal with the types of security incidents and attacks that traditional Internet Service Providers have been experiencing for years. Incidents of service degradation and even complete outages resulting from security attacks are increasing, as well as the overall threat of potential manipulation and exposure of user and network control information

The rapid growth of 4G-LTE enrollments is a game changer and is significantly altering mobile network security. High bandwidth networks are more vulnerable to DDoS attacks, and the openness of LTE network protocols exposes SP networks to a larger number of threat vectors than previous generation networks. These threats are now rapidly increasing and potentially compromising both user data and network signaling information that controls all advanced broadband voice and data services. Attackers are also more different than ever, and predominantly part of large sophisticated criminal organizations that are designing attacks to fall under the radar of SPs in a low and slow manner.

Diameter is an open signaling protocol that is heavily used in 4G-LTE networks and can be thought of as the network's critical nervous system which needs to be optimized and protected. Future SP revenue growth will rely on delivery of new advanced services such as Voice over LTE (VoLTE) which are projected to drive significant expansion of signaling traffic, and it is more important than ever to address control plane security for Diameter, DNS and SIP. DNS-level attacks, DNS amplification attacks, and DDoS cache poisoning are other forms of increasing signaling attacks on SP networks that are negatively impacting revenue.

Current SP security infrastructure leverages multiple single-purpose hardware platforms from several vendors where changes to security policies are done manually, reactively, and tactically. But to deal with the quickly evolving nature of security attacks SPs need to change from their traditional approach to design and implement a longer term strategic security framework. Dynamic multi-layered defense must be considered.

Multi-Layered security is an architectural innovation that addresses all aspects of potential vulnerabilities rather than having to rely on niche point products that may address just one or very few security vulnerabilities. The whole ecosystem of devices, network and applications should be considered. Everything from access control and device management to identity management, network signaling, and radio access security—all should be included in a comprehensive multi-layered defense.

SPs need to leverage the ability to change security policies dynamically based upon individual user and application characteristics in real time. By combining dynamic security with a multi-layered approach, SPs will be able to detect attacks in one location and efficiently apply security enforcement in another location.

In order to adequately address their rapidly evolving security challenges, SPs should define and implement a long term strategic security framework to proactively stay ahead of potential attackers. There is a great deal at stake for Service Providers—network integrity can severely impact their reputation and long term revenue. ■

Network Security: Keeping the Sharks at Bay

Denial of service attacks can happen on every layer of the network. That's why many security experts recommend a multi-layer approach.

By Monica Alleven

Just when you thought it was safe to go into the ocean, along comes a movie like "Jaws," or, perhaps more scary, the more recent made-for-TV movie "Sharknado." In the world of mobile network security, the shark in the water looks a lot like DDoS, or distributed denial of service attacks that could be lurking in any one of the millions of mobile devices out there.

With the dramatic rise in smartphone and tablet usage comes a whole new generation of phones that are just tiny computers. In DDoS attacks, hackers distribute malware to computers to create botnets that can be activated like an army when they want to attack. Because Android is an open source platform, it's generally considered more vulnerable than Apple's iOS. One of the early cases of a Trojan horse taking over Android phones involved an infected Hello Kitty screensaver.

"The phones become attackers in DDoS," said David Hobbs, director of security solutions at Radware. "We've seen a tremendous rise in denial of service attacks," with upwards of almost 28 percent of problems in computer security related to DDoS.

"If you think about having 100,000 phones that are infected, that are roving on a carrier network, where their IP address can change at any moment depending on which tower they're connected to, it's almost impossible to detect and lock the attacker based on where they're coming from," he said. That means nefarious command and control centers can use infected phones to attack stock exchanges, financial institutions and others.

"The landscape that wireless providers have to take a look at is how do they detect what's known good traffic vs. known bad traffic."

DAVID HOBBS, DIRECTOR OF SECURITY SOLUTIONS AT RADWARE

Denial of service attacks can happen on every layer, said Lenny Burakovsky, senior director of strategic solutions at F5 Networks. That's why he advocates a multi-layer security concept; the vast majority of vendors are

designing a niche product to solve a niche problem, he said. That said, he does see the industry moving in the right direction, albeit slower than he'd like to see. Companies like IBM are starting to accept the concept of multi-layered security vs. niche products, he noted.

Known vs. unknown

Knowing what is a legitimate use of the network and what's coming from bad actors is always a challenge for operators, and such discussions can quickly venture into net neutrality territory. Operators need to determine good from bad when it comes to security threats, but consumers typically don't want them snooping into the content of their messages.

Operators "have done a great job hardening and building infrastructure above and beyond what you see a single retailer do. That's something they've been doing for many years."

KAYVAN ALIKHANI, SENIOR DIRECTOR OF TECHNOLOGY AT EMC'S RSA SECURITY

"The landscape that wireless providers have to take a look at is how do they detect what's known good traffic vs. known bad traffic," Hobbs said. "They have to have distributed denial of service protection technologies on their network" that can handle both voice and video and still provide a high level of service, "so they have probably some of the tougher jobs in maintaining service to their customers."

The situation can even come up when operators' own data center customers are testing their security systems. For example, a data center customer may conduct a test to see how its networks react to a DDoS attack, and the operator needs to know if that's just a test or actually a hostile act being conducted by someone else. "These are the complexities they have to be focused on, and it's a lot more difficult that it was 10 years ago, that's for certain," Hobbs said.

While smartphones and tablets represent intelligent computing capabilities to the wireless networks, there's the other extreme as well. For mobile devices with limited computing and power resources, such as sensors, it's difficult to deploy a strong cryptographic approach to protect communications between sensors, according to Dacheng Zhang, leader of the Open Networking Foundation's security discussion group. He also points out that encryption comes with costs. Encryption should be provided only when necessary because it will cost computing resources to decrypt packets and may affect the deep packet inspection (DPI) capability of security devices, he said.

The revelations about the NSA collecting millions of phone records heightened interest in technologies that are more "surveillance-proof," he said. Some people have discussed how to use opportunistic encryption, which is encryption without authentication, to make surveillance more expensive, Zhang said.

New habits, new threats

Years ago, mobile phone users with basic voice phone service didn't have the same concerns they do today.

Consumers carry their smartphones around all day, getting email and updates from social accounts like Facebook and Twitter. Granted, their information typically isn't as sensitive as say, a healthcare provider or financial institution, but they also don't want their personal accounts getting hacked. Storages/transfer services that are commonly used by the general public also don't always have the strongest security measures put in place, said Kayvan Alikhani, senior director of technology at EMC's RSA Security. He declined to name any specific storage providers.

Attacks like the one that accessed retailer Target's customer information are becoming more alarming, but when it comes to storing customer records and data, wireless operators are well-versed in that department, Alikhani said. Operators "have done a great job hardening and building infrastructure above and beyond what you see a single retailer do," he said. "That's something they've been doing for many years." Thanks to the ongoing threat of security breaches, no doubt they'll continue doing so for many years to come. ■

SMS Remains Trendy with Spammers

The underlying complexity and popularity of SMS make it susceptible to security threats.

By Monica Alleven

Despite the onslaught of over-the-top (OTT) messaging applications that do an end-run around carriers' SMS services--operator-driven SMS is not dead, a fact that doesn't go unnoticed by spammers.

Because SMS spam is a worldwide problem, operators are attacking it on an international scale. Back in 2012, the GSMA established its Spam Reporting Service (SRS) to proactively address global messaging threats. All the major U.S. carriers are involved in the GSMA's SRS.

Consumers are encouraged to forward spam messages using the short code "7226," which spells "spam" on most phones. Those messages go to a clearinghouse powered by messaging security software provider Cloudmark, which analyzes the SMS traffic and reports back to operators.

Phishing for dollars

Lately, Cloudmark has been seeing a lot of bank phishing, where someone tries to get a person's account details with a call to action, often using the area code in a regional community bank's geographic area.

"[Carriers] don't want to deal with having to refund people" for fraudulent amounts, so if someone sets up a premium rate service, "first of all, the carriers will look at them carefully to make sure they're a legitimate business, and secondly, they will delay that payment to make sure they don't get any complaints about fraudulent use of that service."

ANDREW CONWAY, RESEARCH ANALYST AT CLOUDMARK

The "you've-won-a-free-cruise-to-the-Bahamas" message remains popular as well, but it's actually a time-share selling scheme and consumers who fall for it get hit with a lot of other charges that aren't "free," said Andrew Conway, a research analyst at Cloudmark who happens to be based in the Bahamas.

Another ruse that's been around for years involves malicious apps that send premium rate text messages. In the U.S., "the carriers are all over this," Conway said. "They don't want to deal with having to refund people" for fraudulent amounts, so if someone sets up a premium rate service, "first of all, the carriers will look at them carefully to make sure they're a legitimate business, and secondly, they will delay that payment to make sure they don't get any complaints about fraudulent use of that service."

"[SMS] was never really designed to be massively secure."

DAVID COHEN, PRINCIPAL CONSULTANT AT ANALYSYS MASON

Message Interception in 2014

For many years, the gold messaging standard was BlackBerry, then supplied by a company known as Research In Motion (RIM). It successfully garnered corporate and government contracts, and for a time, it was thought to be so safe even foreign governments couldn't use it for surveillance purposes. But BlackBerry's decision last year to strike a pact with India's government on its intercept requirements ended that reputation, even though the company said the surveillance requirements didn't pertain to its Enterprise Server customers, said independent security consultant Shaun Murphy.

The underlying complexity and popularity of SMS, along with the different transports available, make it susceptible to security threats. "It would be very hard for me to say that SMS is or ever could be secure," Murphy said, noting that governments like India and China are hostile toward encryption of any kind, including for SMS.

Prior to Edward Snowden's revelations about the National Security Agency (NSA) last year, analysts like Murphy and those who work on a daily basis with information security "all sort of knew … that there are programs out there" like the NSA's, Murphy said, noting a series of books by James Bamford chronicling the NSA's capabilities. Snowden's revelations provided additional verification that governments could get their hands on pretty much any sort of communications platform if they so desire, he said.

That speaks to the current situation with service providers. "You're relying on a provider to say 'our systems are secure, we encrypt our data, we encrypt our servers'--whatever it is--and that's what a lot of providers have done now," including Google, he said.

"But in reality, the problem that we're seeing is the journey--what's the overall journey from one person communicating to another person, or an enterprise communicating within itself? You have all these different vendors now that have questionable practices and questionable content … That's a huge concern. That's where we need to look at it," Murphy said.

In terms of what governments are able to see, it boils down to the terms of service between the customer and the application or service provider, and that varies

greatly by country, Cloudmark's Conway said. In the aftermath of the NSA and the Snowden reports, "I think there's some very clever people who are busy redesigning the Internet" to make it less susceptible to government snooping, and "that will make spam filtering more difficult," Conway said.

Is OTT messaging more susceptible to security threats? "Sometimes you'll see OTT messaging being exploited, where someone will find a vulnerability and go out and start exploiting the system in high volume," but because the OTT application is controlled by a single company, it's identified relatively fast. "We tend to see bursts of spam on OTT networks, but then it gets shut down fairly quickly," Conway said.

Someone Is Always Listening

The bottom line is SMS doesn't come with guaranteed message delivery, much less a high level of security clearance. "It was never really designed to be massively secure," said David Cohen, principal consultant at Analysys Mason. "There is no inherent security in SMS itself."

Cohen advises anyone who uses SMS to consider it akin to having a conversation in a bar. Most likely, if two people are having a conversation, no one else will care about what they're saying. But you never know when someone might be eavesdropping, so it's wise to say only things you don't mind someone else overhearing.

"Security is an ongoing management process," Cohen said. "That's something security professionals are aware of. It's a bit like insurance for something that might happen." ■