Will Proposed Standard Make Mobile Phones More Secure?

Neal Leavitt

Smart phones are becoming increasingly popular. Offering Internet connectivity, they function like minicomputers and can download a growing variety of applications and files, store personal information such as credit card numbers, and even conduct financial transactions.

But as smart phones become more sophisticated, they are also becoming targets for hackers and virus writers. "Because of increasing e-commerce capabilities, there is more value migrating to these devices," said Roger Kay, president of Endpoint Technologies Associates, a market analysis firm.

The Trusted Computing Group (www.trustedcomputinggroup.org), an organization with more than 100 members—including component vendors, software developers, and network and infrastructure companies such as Intel, Motorola, Nokia, Samsung, VeriSign, and Vodafone—is working on a set of specifications and building blocks for mobile- phone security.

The TCG system would integrate data security into smart phones' core operations, rather than implementing it via add-on applications.

The TCG's Mobile Phone Work Group has published 11 use cases that,

along with a set of technical requirements, will guide the specification work, slated for completion next year.

The proposed standard would protect user data and transactions, as well as enable intellectual-property (IP) protection, a feature the entertainment industry wants before making popular content available for mobile devices.

Nonetheless, the technology faces several potential hurdles.

For example, Seth Schoen, staff technologist for the Electronic Frontier Foundation (EFF), a digital-rights group, said consumers may not like usage restrictions imposed by the technology's IP protection.

DRIVING FORCES

The smart-phone market is growing rapidly. Market research firm IDC predicts that by 2008, vendors will sell more than 130 million of the devices, representing 15 percent of all mobile phones.

Market research firm Canalys said global smart-phone shipments through the first half of this year were more than 12 million, 105 percent more than during the first six months of 2004. Last year, said the ARC Group, a market analysis firm and consultancy, smart phones accounted for only 3 percent of global handset sales.

As smart phones have improved their data handling capabilities, customers are increasingly using them to conduct online and, via digital wallets, in-person purchases, as well as to store corporate, financial, and other important information.

Thus, hackers are targeting them more for attacks.

Until now, security has not been a primary focus for phone makers because the devices were used mainly for voice communications and messaging, explained Mikko Hypponen, director of antivirus research for security vendor F-Secure.

Vulnerabilities

About 90 viruses, worms, and Trojan horses currently target smart phones, as Figure 1 shows. Hypponen said the malware can destroy or corrupt data on a device or make the information inaccessible; make applications inoperable; or even send out messages without users' knowledge, for which providers can bill them.

Malware can spread itself from device to device via a phone's Bluetooth short-range connectivity capabilities, executables attached to multimedia messages, and infected removable memory cards.

Mobile devices can also pick up malware by synchronizing with an infected PC or downloading infected files from the Internet via a mobile network.

Information theft is also a concern. The most common way people steal data on a device is by taking the device itself, noted Ed Moyle, founding partner of the Security Curve market research firm.

Several utilities let attackers intercept material sent wirelessly from devices via Bluetooth, explained Marcus Sachs, a computer scientist at SRI International,

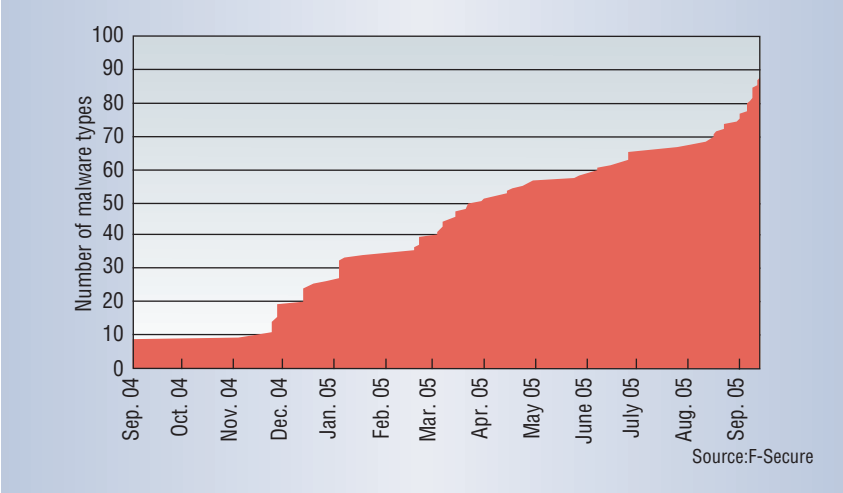

Figure 1. The number of malware types targeting smart phones has risen rapidly from less than 10 in September 2004 to about 90 a year later.

a contract research institute, and deputy director of the US Department of Homeland Security's Cyber Security R&D Center.

And in the future, malware will be able to steal information and send it to hackers, noted Aaron Davidson, president of antivirus vendor SimWorks.

Current mobile-phone security

Current mobile-phone security includes service providers' network-based malware defenses and malware protection on individual handsets, said Todd Thiemann, director of device security marketing for antivirus company Trend Micro.

Additional approaches protect against data theft and other problems. For example, noted Moyle, screen locks prevent thieves from accessing information from stolen devices, cryptographic software keeps unauthorized users from reading data on a phone, and PC-based products don't allow the migration of critical material to a handset.

Devices are also increasingly including authorization capabilities, said F-Secure's Hypponen.

Many prior security approaches for smart phones have been based on companies' proprietary approaches, noted Janne Uusilehto, who chairs the TCG's Mobile Phone Work Group and is head of Nokia's Product Security Technologies Team.

However, proprietary software won't work on all platforms.

WHAT TCG DOES

The TCG's smart-phone specification calls for hardware to support features similar to those of the Trusted Platform Module (TPM) chip used in PCs and servers.

The TCG said it won't divulge details of the technology behind its smart-phone system until it finalizes the initial specification next year. However, information about the TPM chip for PCs, servers, and laptops, described in the "Inside the Trusted Platform Module" sidebar, offers some ideas.

The TCG will have to adapt TPM technology because mobile phones are much smaller than PCs and are already full of circuitry and thus don't have room for another chip.

"It might be necessary to adapt the functionality of the TPM by integrating it within some other chip that's already in a mobile phone," explained the EFF's Schoen.

Integrating the circuitry with existing silicon would also minimize the TPM technology's added cost, said Endpoint's Kay.

Schoen noted that it would be more difficult to upgrade the TCG's hard-wired hardware-based security system than a software-based one. But hardware-based security is harder to modify and break than its pure-software counterpart, Security Curve's Moyle added.

However, Trend Micro's Thiemann said, a hardware approach would limit a company's flexibility in choosing phones if the device it prefers to use doesn't support TCG specifications.

Meanwhile, Moyle noted, the TCG's open approach will enable standardization and interoperability. And providing a technology foundation for companies to build on will enable them to bring products to market faster, said the TCG's Uusilehto.

TCG smart-phone use cases

The TCG's 11 use cases indicate its smart-phone security system will enable:

- mechanisms to ensure that no one has tampered with a device's hardware and software;
- device authentication to protect and store owner-identity-related information and thus determine whether a thief or other unauthorized person is trying to use a phone;
- IP protection to restrict use of third-party content;
- the safe download of updates, patches and other software;
- secure channels between different parts of the phone—such as a subscriber identity module and the processes that use the SIM's data—to prevent keystroke logging or other types of tampering by malware;
- the secure download and subsequent management of digital tickets, which represent proof that a user has the right to access network-based resources;
- the secure execution of payments made via a mobile phone;
- the ability to determine that downloaded software is safe and to

remove or at least not execute unsafe software; and
- ways to prevent unauthorized parties from accessing or viewing information stored on a device.

IP protection

The TCG specification would include IP protection that would keep users from playing, copying, and transferring content such as music, video, games, and software in ways that violate terms set by the company providing the material.

Proponents say that IP protection could encourage content owners to make video, audio, games, software, and other material available for use on smart phones. This could lead to new services for customers and generate revenue for content owners and cellular service providers.

Opponents contend this excessively limits the way individuals can use the content they buy and their devices.

Device control

Service providers and handset vendors could use TCG technology to get more control over devices. For example, said the EFF's Schoen, the technology could let service providers keep ring-tone or application vendors from selling material for use on a smart phone unless they pay carriers a fee.

"This is just one example of a business model that involves restricting how customers can use phones and charging customers for things that don't actually have a cost to the carrier," said Schoen.

POTENTIAL PROBLEMS

Integrating TCG circuitry into a phone or making the technology work with the handset's software could be a significant engineering challenge because most devices have limited memory, power, and processing resources, noted SRI's Sachs. "Any time you add cryptography or other security features, you increase storage requirements and the load on the processor," he explained.

Inside the Trusted Platform Module

The technology behind the Trusted Computing Group's (TCG's) secure platform for smart phones will be based on the Trust Platform Module, designed for use in PCs, servers, and laptops.

The TPM is a motherboard-mounted cryptographic processor with a unique digital signature. It provides the basic building blocks for higher-level security functions such as authorization, access control, and file encryption and decryption.

The TPM chip—which protects motherboard traffic and communications between the CPU and a network—stores public encryption keys, digital certificates, passwords, and other credentials.

"In essence, the system cryptographically seals off the parts of a computer that deal with data and applications and gives decryption keys only to outside programs that the TPM chip deems trustworthy," said Janne Uusilehto, who chairs the TCG's Mobile Phone Work Group and is head of Nokia's Product Security Technologies Team.

The system doesn't decide whether code is safe. Instead, it identifies users; their computing systems, based on their TPM chip's unique identifying digital signature; and the applications or data they want to run. Trusted agents then consult directory services to determine whether the users are authorized to run the applications or data on the protected system.

The TPM concept was developed by the Trusted Computing Platform Alliance, the TCG's predecessor. According to the TCG, computer makers such as Dell, Hewlett-Packard, and IBM have shipped more than 17 million TPM clients.

Meanwhile, Schoen said, customers may be angry about the IP and application-download restrictions that TPMs enable. Mobile phone users, he explained, expect a lot of freedom with their devices.

"The specification will help cell phone companies decide who can publish software or media for your phone and even whether you can load documents on your phone," he said.

The TCG's Uusilehto said the Mobile Phone Work Group will likely approve its smart-phone specification in the first half of 2006. The group would then make the document public, and manufacturers could begin adopting the technology.

TCG adoption, like TPM support, may be slow, noted Trend Micro's Thiemann.

Endpoint's Kay predicted widespread adoption won't begin in earnest for 12 to 18 months after the introduction of the specification because e-commerce, a major driver for the technology's adoption, won't start migrating to phones until then.

According to Schoen, adoption may occur even more slowly due to consumer concern about the usage restrictions the technology will enable.

Added SRI's Sachs, "If there are devices that don't have the restricting software but work just as well, then consumers won't buy the ones with TCG inside." ■

Neal Leavitt *is president of Leavitt Communications (www.leavcom.com), a Fallbrook, California-based international marketing communications company with affiliate offices in Brazil, France, Germany, Hong Kong, India, and the UK. He writes frequently on technology topics and can be reached at neal@leavcom.com.*

Editor: Lee Garber, *Computer*, l.garber@computer.org