The Trusted Computing Group Mobile Specification:

Securing Mobile Devices on Converged Networks

White Paper

September 2006

Executive Summary

Mobile workers and consumers alike have increasingly numerous ways to access these networks – via data-enabled cell phones, smartphones, PDAs, ultra-mobile personal computers (UMPCs) and notebook computers. In many cases, these same devices can also access the thousands of WiFi hotspots which dot every major metropolitan area.

The near term benefit underlying the increasing use of smartphones and data-enabled cell phones is high-speed data access which can be used to browse the public Internet, connect back to a corporate network or even watch television. This access creates huge security concerns for both consumers and the IT managers tasked with guarding their companies' confidential information.

Over time, this increased access will have an impact on the type of information/data content which is exchanged on a daily basis – i.e., that content will increase in utility and value. Electronic financial transactions conducted via mobile devices will become a norm rather than the current exception, for example. This shift will, in turn, require ever greater platform integrity and protection for that content. There are no existing security solutions – in hardware or software – which can support security in this type of cross-network and cross-device environment.

Also consider that today the vast majority of white collar mobile workers carry at least two types of mobile devices – primarily cell phones and notebook computers. The use of smartphones and similar devices is increasing, but overall usage is still low as compared to cell phones. Indeed, only about six percent of the handsets shipped worldwide in 2005 were smartphones – that is approximately 51 million smartphones versus 809 million new cell phone shipments. By 2010, *i*GR expects smartphones to comprise approximately 21 percent of all mobile handsets shipped worldwide.

In this world of mobile broadband, IT managers have several primary concerns about wireless security. Namely, they want to make certain that their current, wired networks remain secure, and they want to ensure that only authorized and authenticated users are accessing that network. Finally, IT managers are concerned about the security of the data saved on those wireless devices – be they laptops, PDAs, cell phones or smartphones.

The fear, of course, is that the mobile devices will become compromised and either mined for confidential information or used as a base from which to launch an attack on a corporate network. Despite the existence of malicious software (malware) which can cause mobile devices to fail or bog down a mobile operator's network, the real security threats surrounding the increasing use of smartphones, data-enabled handsets and other mobile devices are rather pedestrian: loss and theft. There are several factors to consider when a device is lost or stolen:

- Replacement cost of the lost/stolen device.
- Cost of restoring data to the device – i.e., the time it takes for the IT staffer to reconfigure the device.
- Possible compromise of confidential data (personal and/or company), which could be almost anything depending on the device lost and the data kept on it – e.g., customer records (any industry), patient information (health care), etc.

- Possible breach in the security of the network to which the wireless device connects – e.g., if network passwords are stored on the device, then an unauthorized user could gain access to the network via an authorized device.

Mobile operators around the world are also gravely concerned about wireless security. They need to ensure that their subscribers are using secure devices both because it's good for their business – i.e., they can more readily launch mobile commerce related services – and because compromised handsets are a potential threat to the smooth functioning of their networks. Mobile operators are also always looking for ways to protect themselves from the revenue losses associated with cloned devices i.e., stolen mobile phones which are illegally resold.

There are numerous software-based ways to safeguard mobile devices – virtual private networks (VPNs), firewalls, on-device data encryption software and device management solutions, to name just a few. These types of solutions typically protect the data and or operating systems of the devices from attacks, but do little to protect the unique identity of a device such as a cell phone e.g., the International Mobile Equipment Identity (IMEI) number. These software-based solutions also cannot ensure the integrity and/or authenticity of the hardware platform on which they are running.

This whitepaper will provide an overview of the security threats facing mobile devices and the existing solutions for shoring up those security holes. It will also provide a look at a new technical specification from the Trusted Computing Group which has been developed to address the specific global needs of wireless and mobile security from both a consumer and enterprise perspective. These needs include:

- A hardware-based approach to mobile device security is significantly stronger than a software-based approach. Software approaches tend to be limited in scope and do not, to date, enable interoperability between different security applications, device platforms and/or data networks.

- A cross-platform and open security standard given the wide array of networks, devices, operating systems and applications in the converging world of wired and wireless data

- A solution which simultaneously provides protection for the user's information, the device itself, and the network operator's assets. For example, a hardware-based approach to security can help prevent mobile devices from being cloned – this protects the device and by implication the user and the mobile operator.

The Need for Mobile Device Security

With the advent of third-generation (3G) mobile broadband networks, wireless security is only getting more complicated. Globally, there are two types of mobile broadband networks are being deployed. One is the Universal Mobile Telecommunications System or UMTS, which is also known as Wideband-CDMA (W-CDMA). Cingular Wireless is the only U.S. carrier deploying UMTS – and they are jumping right to an enhanced version of UMTS called HSDPA or High-Speed Downlink Packet Access. Other mobile operators such as Vodafone and NTT DoCoMo are also moving in this direction.

In the United States and in several other regions, the other type of mobile broadband network being deployed is CDMA EV-DO, which is short for Code Division Multiple Access Evolution-Data Optimized. This type of network is being deployed by Sprint-Nextel, Verizon Wireless and several of the regional mobile operators such as Alltel.

Both of these networks allow cell phones, smartphones, PDAs, ultra-mobile PCs (UMPCs) and laptop computers easy access to the open, public Internet at DSL/cable modem-like speeds. This exposure to an untrusted network only heightens the requirement for strong security solutions.

There are five fundamental requirements for any type of data security, wireless included:

- Authentication, authorization and accounting (AAA): Although three separate topics, they are heavily inter-related. Authentication ensures that only valid devices and users access a given service. Authorization ensures that those valid users only access approved services. Accounting creates an audit trail of user activity that can be used at a later time, if necessary.

- Data integrity: Ensures that messages / data / communications are not tampered with while in transit or in storage (in memory on the device, for example).

- Privacy: Although related to data integrity, since a message which has been tampered with is no longer private, privacy also involves rules around what information can be shared among users, whether messages can be exchanged "in private," and the anonymity of users (if needed and/or desired).

- Nonrepudiation: Ensures that the parties to a transaction or communication cannot deny (i.e., repudiate) their involvement in the transaction. In the physical world, handwritten signatures often provide nonrepudiation.

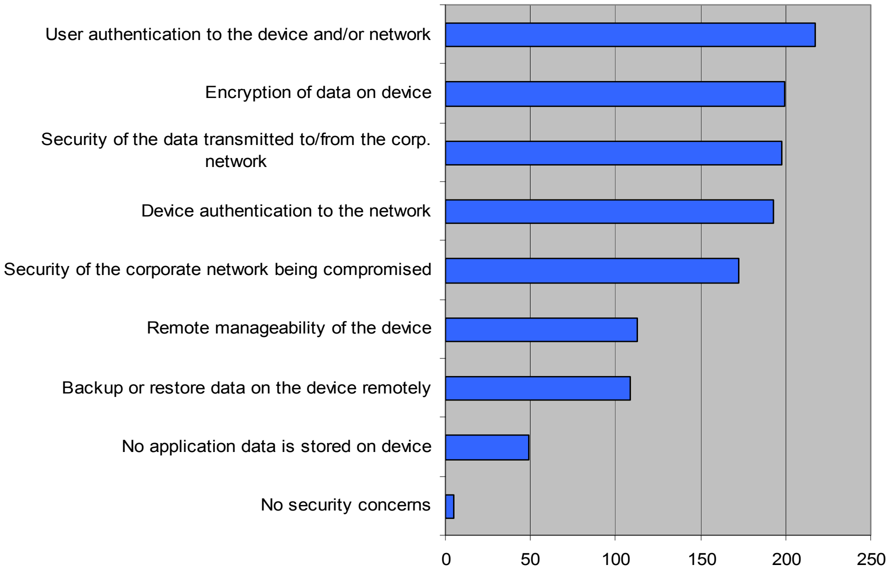
- Security policies: Company (or personal) policies which complement and/or shore up the actual security technology are key. A company security policy might mandate that all users must create passwords with 16 number and letter characters. A personal security policy might be: Keeping one's wallet in a front pant's pocket.

All of these factors are at play in the wireless and mobile device world. For example, mobile operators provide all of the above features to help safeguard their customers and themselves. For example, carriers provide AAA, data integrity (calls are not tampered with and are private), and the user cannot deny that their phone was making and receiving calls. How the user safeguards his/her phone is their own affair.

In the mobile broadband world, IT managers have several primary concerns about wireless security. As Figure 2 illustrates, IT managers want to make certain that their current, wired networks remain secure, and they want to ensure that only authorized and authenticated users are accessing that network. Finally, IT managers are concerned about the security of the data saved on those wireless devices – be they laptops, PDAs, cell phones or smartphones

Figure 2 is from *i*GR's 2006 survey of 406 IT managers working in large U.S. enterprises and corporation. Note that the respondents were asked to "check all that apply" in responding to the question: "What security concerns did you have about your wireless deployment?" As a result, the data in Figure 2 shows the most common responses among the respondents.

Figure 2: Wireless Security Concerns Among Enterprise IT Managers



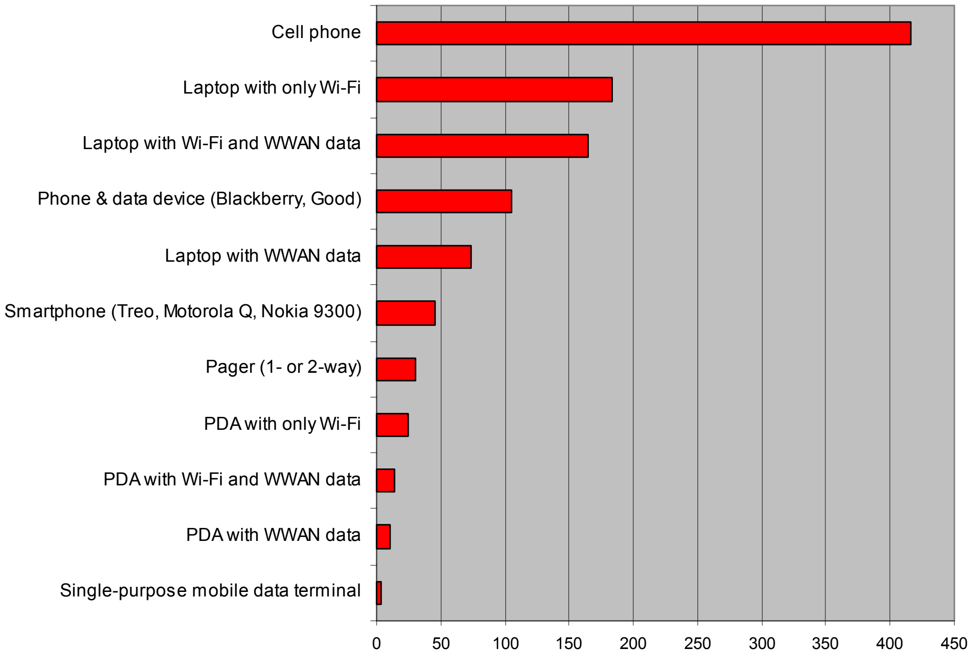
Source: *The Enterprise According to IT Managers, 2006*, *i*GR

Device Usage

Figure 3 is from *i*GR's 2006 survey of 503 mobile workers employed in large U.S. companies. The data in Figure 3 shows the most common responses among the respondents. Note that the respondents were asked to "check all that apply" in responding to the question: "What types of devices are used by mobile workers at your company?"

Note that 95 percent of the mobile worker survey respondents classified themselves as "white collar" mobile workers. The term "white collar worker" refers to employees who perform knowledge work, such as those in professional, managerial or administrative positions. This work usually does not involve manual labor and employees in these occupations are often expected to dress with a degree of formality.

Figure 3: Common Wireless/Mobile Devices in Use



Source: *The 2006 Mobile Worker Survey Report, i*GR, 2006

The mobile worker survey found the most commonly used mobile devices among mobile workers are:

- Cell phones: Clearly, cell phones remain the “default device” of most mobile workers. Those mobile workers not using cell phones are using BlackBerry-type devices or smartphones.

- Smartphones: Used by a much smaller percentage of the surveyed mobile workers. It is entirely possible, as *i*GR found in its survey of smartphone users, that a portion of the respondents to this mobile worker survey do not know what a smartphone is. So, they may be using a smartphone and not realize it or they might be using a “regular” feature phone (e.g., the Motorola SLVR) but think that it is a smartphone.

- Phone and data devices – e.g., RIM BlackBerry, Good Technology devices. These devices are essentially smartphones.

- Laptops with two types of wireless connectivity options: Laptops with only WiFi versus laptops with both WiFi and WWAN data. Laptops with only WWAN connectivity were used by a comparatively small percentage of the surveyed mobile workers.

- PDAs: PDAs are used by a small percentage of the surveyed mobile workers which represents a decline as compared to surveys conducted in previous years. This is likely due to two factors: the popularity of RIM BlackBerry and similar devices which incorporate PDA and mobile phone functions, the uptake (albeit slow at this time) in smartphone usage, the greater utility of a laptop as compared to a PDA.

Obviously, these devices are used in myriad ways. The basic use (voice communication) has since evolved into mobile devices which provide a broad array of communication, entertainment and business-centric functionality, such as:

- Rich features and function: Devices today are loaded with features – everything from AM/FM radios and WiFi / GSM roaming to iTunes players and TV players.

- Advanced form factors: Flip phones and smartphones with larger color screens, QWERTY keyboards, better battery life, faster processors, more memory and slots for removable cards. Handset manufacturers are also taking the flip phone form factors to new levels with slide and rotating designs. Not all of these designs make sense for mobile workers, but some are applicable in particular industries – e.g., Real Estate, where realtors might more highly value a camera-oriented smartphone.

- Advanced operating systems: Most mobile phones still run on proprietary operating systems – the device manufacturer's own OS or one from a third-party vendor. The emergence of devices with greater memory, better processors and more storage has increased interest in bringing the traditional OS into the mobile space. As well as smartphone operating systems from Palm, Microsoft, Symbian and ZTE, other companies now offer new operating systems for feature phones. A good example is Savaje with its Java-based OS. There is also much discussion of Linux in mobile handsets, but product plans remain unclear.

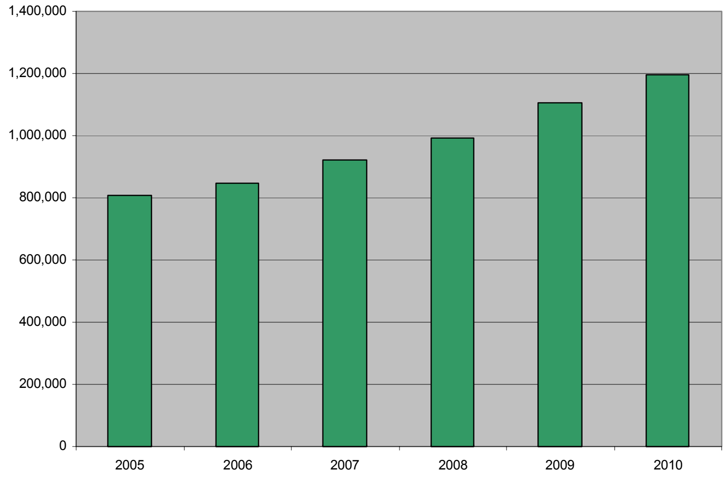
- WiFi/WWAN connectivity: Devices with integrated WLAN capabilities are of greatest interest to corporate users, since many companies have WLANs in place in their offices. It is likely that mobile devices with integrated WiFi will not enter mid- to low-end phones for a few years.

- More services and applications: The emergence of Java and BREW on handsets has opened up the market for innovative services and applications. To date, these development environments have enabled content and game creators to make more interesting games and applications, but these environments can also be leveraged by independent software vendors such as Salesforce.com who want to port their applications to mobile devices.

- Multimedia: Cameras are now included on a wide range of mobile devices to the point that there is little market differentiation to be gained by including a camera and image capability. Indeed, the reverse may be true (not including a camera), given corporate paranoia and industrial espionage. Full multimedia capabilities, including video (for messaging or possibly for conferencing or SWIS – "see what I see") will be the next major differentiators. Clearly, 3G networks are required to take full advantage of video – in addition to devices with longer battery life, more memory and higher processing power.

These trends have helped create huge growth in the wireless market, both in past years and down the road. The number of handsets shipped is growing rapidly as Figure 5 shows. In 2005, there were approximately 809 million new handsets sold worldwide. By 2010, *i*GR expects that number to rise to slightly more than one billion. Note that the following forecast excludes handsets which are sold as replacements for existing units and, obviously, to existing subscribers. In 2005, there were approximately 552 million replacement shipments. *i*GR expects that number to grow to slightly over one billion by 2010.

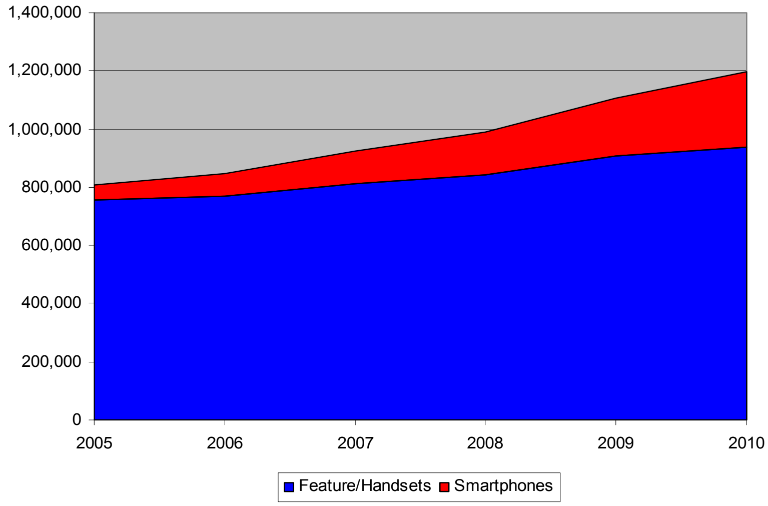
Figure 5: Total Worldwide Handset Shipments, 2005-2010



Source: *i*GR, 2006

Not all of these devices are smartphones, of course. Indeed, only about 6 percent of the handsets shipped worldwide in 2005 were smartphones. By 2010, *i*GR expects smartphones to comprise approximately 21 percent of all mobile handsets shipped worldwide, as Figure 6 illustrates.

Figure 6: Number of Smartphones Shipped Worldwide, 2005-2010



Source: iGR, 2006

Mobile Device Security Threats

The term “mobile malware” refers to malicious software such as viruses, worms and Trojan Horses (Trojans) that have been specifically designed to infect wireless handsets. There are several mobile phone viruses “in the wild” right now, but the majority of that malware only affects smartphones – and, for the most part, only smartphones based on the Symbian operating system (OS). One virus only affects WinCE devices – but Microsoft is long past WinCE so there is even less danger now than there was two years ago when Brador made headlines. The small target market for mobile malware is one of the reasons why it barely registers on the “threat meters” published by the leading anti-virus software firms.

The fear, of course, is that mobile malware will soon become far more dangerous to smartphones, wireless PDAs, laptops, the data resident on those devices, the wireless networks over which those devices communicate and the corporate networks, servers and/or personal computers with which those devices exchange information. Undetected malware on a smartphone could get transferred to a corporate network at which point it might be coded to activate and replicate itself.

The real security threats surrounding the increasing use of smartphones, PDAs with wireless connections and laptops are rather pedestrian: loss and theft. In the hands of someone with malicious intent, a stolen device could be used to launch an attack against the device’s owner, the enterprise to which the device belongs and/or the mobile operator on whose network the device runs. As a result, there are several factors to consider when a device is lost or stolen:

- Replacement cost of the lost/stolen device.

- Cost of restoring data to the device – i.e., the time it takes for the IT staffer to reconfigure the device.

- Possible compromise of confidential data (personal and/or company), which could be almost anything depending on the device lost and the data kept on it – e.g., customer records (any industry), patient information (health care), etc.

- Possible breach in the security of the network to which the wireless device connects – e.g., if network passwords are stored on the device, then an unauthorized user could gain access to the network via an authorized device.

- Alternatively, if the device identity itself can be altered, then it can be re-purposed to possible affect the network and to bypass network security mechanisms based upon that identity. This is typical of the so-called cloning threat wherein a stolen device is re-programmed with a new identity to bypass black-list enforcement.

Mobile Device Security Requirements

Improving device security, then, involves the creation of security policies on how to use wireless devices, what types of corporate-related information can be stored on them, and the implementation of technology which:

1) Encrypts data transmissions to and from the device.

2) Encrypts data on the devices themselves.

3) Protects the identity (IMEI) of the device from being changed (i.e., cloning the device for illegal resale and use)

4) Measures the trustworthiness of the hardware, OS and applications to detect an unauthorized configuration.

5) Allows IT staffers to deactivate, lock and/or wipe devices which have been stolen or lost. This is a feature of many device management software products.

6) Provides strong user authentication both to activate the device and to access the network. In the case of loss/theft, user authentication can slow or halt an attacker entirely.

7) Management functions on the device and on the back-end which allow IT staffers to centrally create, rollout, change and enforce their security policies. These management functions are only feasible to the extent to which a device itself can be authenticated and its own integrity ensured.

8) Password protection on all devices at power-on. Most mobile devices ship with this feature; device management software products can allow IT staffers to enforce the use of this feature (which many users never activate).

The relative ease with which smartphones and PDAs can be stolen or lost should also encourage enterprises to put in place security policies and best practices which govern the use of those devices. Obviously, these policies will vary across companies and industries. Doctors using PDAs or smartphones to hold patient data need to be extra careful so as to protect their patients' from inadvertent (or malicious) HIPAA violations. Similarly, mobile workers in the financial services industry might need more security on his/her device than a cable service technician using a phone to speak with his/her dispatcher.

As compared to laptop or desktop computers, achieving these objectives with smartphones, cell phones and/or PDAs is different for several reasons:

- There are more operating systems to support: Symbian, Palm, Windows Mobile. The OSes and product offerings from RIM and Good Technology incorporate their own security which is not reliant on third-party solutions.

- Mobile operators may control the WWANs, but they have no dominion over the public Internet. Data traffic that leaves a mobile operator's network is "in the clear" unless the user (or enterprise) has some security in place (e.g., a VPN or application-level security).

- Mobile operators also control what applications are loaded onto smartphones and cell phones which function on their networks. All applications and content available for purchase through a mobile operator's Web portal, for example, goes through a stringent approval process. They have somewhat less control over the applications used on a PDA with a WWAN data card and the emergence of smartphones with expandable memory slots has also created the potential for unapproved content to be loaded onto those phones. That said, if the mobile operator has the proper tools in place, it can prevent certain applications from running over their network – e.g., VoIP software on a laptop or PDA. A mobile operator would prevent these types of applications from running if the operator were not involved in the revenue chain associated with that service.

- The smartphone devices themselves have comparatively short battery lives, slow CPUs and less memory than laptops and/or desktop computers although their performance improves with each new generation of devices. Lower performance as compared to laptop or desktop computers can limit the types of security applications that can effectively be run on mobile devices. On the positive side, however, the disparity in performance has encouraged innovative solutions to mobile device security.

There are numerous software-based ways to protect mobile devices – e.g., anti-virus software, virtual private networks (VPNs) and firewalls. Another type of software solution is individual file, folder and/or hard drive. Once installed and configured, this type of software encrypts and decrypts any data on the device specified by the user in real-time. So, email and SMS can be encrypted, as well as contact information, Microsoft Office files.

Some of these products can also encrypt and decrypt information stored on removable media. File decryption can only be done by an authenticated user – a process which can be made transparent to the user. That is, the user logs into the phone and then has access to all his/her files.

Good security is not just based on software solutions, however. It also includes a companywide security policy which is strictly enforced and the assurance that the platform can and will enforce a local security policy which reflects the companywide security policy. Example tenets in such a policy might include:

- Password protection on all devices at power-on (at least); password enforcement software should be used to make sure users are not disabling that requirement. The number of password attempts should also be restricted.

- Some companies might want to use two-factor authentication for additional security.

- When the devices connect to the corporate desktop/laptop, the wireless port(s) should be disabled on the device.

- All devices must have AV software and be scanned for viruses before connecting to the corporate network.

- The devices should run personal firewall software to protect against intrusions.

- The devices can only connect to the corporate network via a VPN.

- Sensitive corporate information cannot be stored on the mobile device unless it is encrypted. This encryption could occur per file, per directory or the entire hard drive (really only applicable to devices with hard drives). “Sensitive information” is whatever the company says it is – patient record, customer information, press releases, contacts, etc. In some cases, enterprises might want to require bit wiping software to be installed on devices so that sensitive data can be deleted remotely or after repeated failed login attempts, for example. This software should delete all the data stored on the device, the data in RAM and any data on external memory cards that are plugged into the device,

- All devices must have the latest security patches installed. The onus here is on the IT department; they need tools that help them determine which devices can run what software and what version that software is on to then update the software appropriately.

- All devices must have a unique identity and a mechanism to demonstrate trust in their integrity claims.

Benefits of the Trusted Computing Group Mobile Specification

The Trusted Computing Group (TCG) has developed a specification to address the specific needs of wireless and mobile security. The goal of TCG has been to define a much stronger security solution based on hardware protection rather than more vulnerable software approaches. The specification also focuses on global interoperability between handsets and other platforms and will allow independent software vendors (ISVs) to leverage hardware-based security solutions in their products.

The scope of the TCG is greater than just mobile since, as a group, the TCG is involved in developing specifications that are relevant to many other computing areas such as infrastructure, PC clients, storage, peripherals, server and software stacks. The TCG's experience in those other, more mature industries is being applied to the specification being developed for mobile world. This cross-industry experience also helps improve cross-device functionality as it is applied to mobile devices. Although the first iteration of the TCG's specification only applies to mobile phones, in the future it could be extended to encompass other mobile devices such as laptops or UMPCs.

There are a large number of companies involved in creating the mobile specification, which include ARM, AuthenTec, Ericsson, France Telecom, Freescale, Hewlett Packard, IBM, Infineon, Intel, Lenovo, Motorola, Nokia, Philips, Samsung, Sony, STMicroelectronics, Texas Instruments, VeriSign, Vodafone and Wave Systems.

Note that the TCG is not developing applications or hardware, but a specification which defines the fundamental hardware functions and transactions that are key components of a trusted mobile computing model. Original equipment manufacturers (OEMs), silicon vendors and/or ISVs can then take that specification and develop specific hardware and software solutions to leverage the strengths of the TCG-developed specification.

With cooperation among the multiple vendors supporting the specification, the ultimate goal of the TCG mobile security specification is threefold:

- Significantly increase the overall strength of the security provided in mobile phones, including new protection for the handset itself,
- Provide interoperability between competing hardware/software solutions, and
- Provide end users with a trusted mobile computing ecosystem.

The hardware nature of the TCG specification forms the cornerstone of its security assurances. Software-based security standards and/or applications typically define what must be done to secure a protocol or an application. The TCG's specification goes a level deeper to address, in a standard and observable way, what must be done to secure the platform on which these protocols and applications depend.

The TCG explains the value of its specification through a series of "use cases" which all relate to the five basic tenets of security previously mentioned. Note, however, that the TCG specification is a technical spec and does not concern itself with company and/or personal security policies.

- Platform integrity: Ensures that the device is running authorized software and hardware. This provides the user with some surety that they are using a secure device. This relates to the basic security principle of Authentication and Authorization.

- Device authentication: Ensures that the correct device and/or user is accessing the appropriate services. This use case also relates to authentication and authorization.

- Secure software download: Allows users to securely download application software, updates, firmware and/or patches, and to verify that those downloads are trusted. This use case relates to data integrity as well as to authentication and authorization.

- Secure channel between device and UICC: This use case involves secure transfers between the UMTS Integrated Circuit Card (UICC) and Subscriber Identification Module (SIM) card. The goal here is to provide users a secure channel with which to store sensitive data on the UICC and then move that data between devices. This specification also works to prevent the transfer of malicious software from the SIM card to the device itself, as well as to prevent malware from gleaning private data from the device. Data integrity and privacy are key principles here.

- Software use: Ensure that the apps on a device do not do more and/or access data they are not supposed to – which relates to authentication, authorization and accounting.

- Proving platform and application integrity: A way to ensure that the user knows that they are using a secure device and applications which helps give the user a feeling of security and helps prevent them from using an untrusted device or malicious software.

- User data protection and privacy: Protect user data (e.g., contacts / address book, electronic wallets, identity, etc.) which relates to data integrity and privacy.

Summary

Wireless security is a key pain point for mobile operators and enterprises worldwide. This is in large part due to the common belief that wireless networks are inherently less secure than wired networks. In fact, wireless networks and mobile handsets and smartphones can be made every bit as secure as wired networks and the equipment which runs on them.

That said, achieving a high level of wireless network and device security today means relying on point solutions which are either proprietary and/or limited in scope. What is needed is an industry-wide, standardized and interoperable wireless/mobile security solution that does not limit the ability of either application developers or OEMs to innovate and compete effectively in the marketplace. This type of solution would also, of course, enable mobile operators and enterprise to address the security requirements of their subscribers and end users.

The TCG specification provides that underlying platform on which the industry can build robust wireless security solutions in a trust framework which is appropriate to the disparate platforms and endpoints of the converged network.

About *i*GR

*i*GR is a market strategy consultancy *focused* on the wireless and mobile communications industry. Founded by Iain Gillott, one of the wireless industry's leading analysts, we research and analyze the impact new wireless and mobile technologies will have on the industry, on vendors' competitive positioning, and on our clients' strategic business plans.

Our clients typically include service providers, equipment vendors, mobile Internet software providers, wireless ASPs, mobile commerce vendors, and billing, provisioning, and back office solution providers. We offer a range of services to help companies improve their position in the marketplace, clearly define their future direction, and, ultimately, improve their bottom line.

A more complete profile of the company can be found at www.iGR-Inc.com.

Disclaimer

The opinions expressed in this white paper are those of *i*GR and do not reflect the opinions of the companies or organizations referenced in this paper. All research was conducted exclusively and independently by *i*GR. This white paper was sponsored by Trusted Computing Group, but Trusted Computing Group personnel were not involved in the carrier interviews or in the ongoing research.