The need for hardware-based security in mobile devices
The need for hardware based security

VERSION HISTORY

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Status</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>15 Mar 2017</td>
<td>Release</td>
<td>First release</td>
</tr>
<tr>
<td>1.1</td>
<td>24 Mar 2017</td>
<td>Update</td>
<td>Minor updates</td>
</tr>
</tbody>
</table>

TABLE OF CONTENTS

Why mobile security is important........................................................................................................... 2
Trustonic’s beliefs ......................................................................................................................................... 2
What is hardware-based security?.................................................................................................................. 3
More detail on the alternatives to a TEE? ....................................................................................................... 4
Where TEEs are in use today? ......................................................................................................................... 6
How do I use a TEE in my application? .......................................................................................................... 7
About the author ........................................................................................................................................... 10
WHY MOBILE SECURITY IS IMPORTANT

Securing mobile phones and other connected devices is becoming increasingly important, as these are now the primary means by which people access the web and other applications. Many people now rely on their mobile devices for a huge array of services, including banking, payments, work and personal communications (including voice, messaging and email), watching premium content, healthcare monitoring and much more.

There are many initiatives which require the use of a mobile device for user authentication. For example, in the European banking sector, the forthcoming PSD2\(^1\) initiative will propose the use of biometric authentication through a mobile device to be used for approval of most payment transactions, irrespective of whether that transaction was initiated on the mobile device. For this and other new services to become mainstream, they need to be trusted and secure and, in turn, appropriately secured devices must be utilized.

Like PCs before them, mobile devices are susceptible to numerous threats. Spyware can monitor user activity to gather passwords and sensitive data, malware can infect applications and users may deliberately or accidentally install root kits that undermine any security the operating system provides. Given the increasing use of mobile devices for sensitive financial and personal information, the need for strong security has never been greater.

TRUSTONIC’S BELIEFS

It is a well-known fact that modern mobile operating systems such as Android are so complex that they inherently have many bugs, weaknesses and security holes. They are, therefore, open to malware and device rooting, which compromise the security of normal applications. Therefore, best practice is to isolate and protect the most sensitive code and data and to keep it as small as possible, in order to remove the possibility that weaknesses could be exploited.

\(^1\) PSD2 is the second Payment Services Directive, designed by the countries of the European Union. This new EU directive will allow companies to give their customers the option of using third-party providers to manage their finances. It could revolutionise the payments industry, affecting everything from the way payments are made online, to what information is seen when making a payment.
Trustonic's fundamental belief is that, when developing applications, security-related code and sensitive data should be isolated and protected away from the main application. That sensitive code should then be executed in an environment that is known to be trustworthy.

Currently, most applications running on mobile devices are secured by pure software technologies running on the main device OS. Whilst software security can certainly provide a level of protection and reduce the risk of attack, it requires regular application updates to keep ahead of the hackers and other malware that may be resident on any given device. Most software-based security solutions using software obfuscation or white-box cryptographic techniques also produce a noticeable impact on the performance of an application, as these techniques add significant code overhead. Furthermore, most of the software security solutions are not sufficiently diversified per unique device and are, therefore, subject to very scalable attacks.

Trustonic believes that security by design, built from the hardware level up, is the best mechanism for properly securing applications. Software security does, however, have its place. It provides a certain level of security generically and offers security on mobile devices where hardware security features might not be accessible in a scalable and economical manner.

**WHAT IS HARDWARE-BASED SECURITY?**

Hardware-based security is enabled via a hardware-isolated execution environment for security sensitive code. This may be a separate physical processor, such as a smartcard (or secure element), a separate CPU, such as in Apple's secure enclave, or a hardware mode of the main processor, called a Trusted Execution Environment (TEE) such as that delivered by ARM’s TrustZone technology. A TEE running on TrustZone is an example of the technology used by Trustonic for its smartphone-class products.

Hardware-based security utilizes physical hardware technology to protect against attacks. There are several different types of hardware-based security that offer differing levels of effectiveness, but they all protect fully against Trojans and other software-based threats. These are the threats that most organisations are worried about, as they are both scalable and replicable. Software-based security can be thought of like a vaccination, it will protect to a certain level for a while, but will need updating on a regular basis. On the other hand, hardware-based protection can be thought of as a cure.

Traditionally, the most common hardware mechanism was a SIM-based solution, preferred by the mobile network operators. In this model, the SIM is the device that holds the keys and
performs cryptographic operations, but, as well as requiring a complex and costly TSM\(^2\) infrastructure, the SIMs themselves are limited in power and capacity. An alternative model is an embedded secure element, preferred by some handset OEMs. The embedded secure element is technically very like a SIM, but differs in that it is physically embedded into the handset. It also requires a similar TSM infrastructure if post-deployment updates are needed. Neither model is open or scalable and deployments are dwindling worldwide.

The Trusted Execution Environment (TEE) is a hardware protection mechanism, requiring no additional hardware to be installed into the device and, therefore, results in no additional bill of materials cost to the OEM. The TEE makes use of the device’s main processor which, in the clear majority of cases, can operate in a special operating mode, enabling the device to run two operating systems: the ‘real-world’ operating system (e.g. Android) and a ‘secure-world’ operating system (e.g. Trustonic’s Kinibi). These two operating systems are physically isolated from each other.

**MORE DETAIL ON THE ALTERNATIVES TO A TEE?**

**Secure Element** - In the banking and payments world, a secure element (SE) has typically been used to provide security. The secure element takes many forms, either on a smart card, a SIM or physically embedded into a mobile phone. As described previously, the secure element can provide secure key storage and a limited amount of secure processing, but access for an application provider to the secure element, whether embedded or as part of the SIM, is complex from both a technical and business model standpoint. Secure elements have very limited processing power, have access to limited amounts of memory and are restricted in their capabilities, as they are not directly connected to the different peripherals of the device.

The TEE has many benefits over secure elements. One of the major benefits to handset OEMs is the fact that there is no additional discrete hardware required, as the TEE is built-in on the main device processor. It therefore saves space and cost in the device, providing effective, affordable on-device hardware-based security.

**Software** - Software-based protection is another alternative and, whilst not as strong as a hardware-based security solution, offers a reasonable level of security and features. It does

\(^2\) A TSM, or Trusted Service Manager, is a solution designed to deploy secure credentials to SIMs or embedded secure elements. The TSM enables service providers to distribute and manage their applications remotely, by allowing access to the secure element in handsets.
The need for hardware based security

however suffer from several drawbacks; software protecting software is always prone to attack and, therefore, software-protected applications need to be regularly updated to keep ahead of the hackers. Software protection mechanisms, such as white-box and code obfuscation, can also have a level of performance impact on the application, as a large amount of additional code is required to deliver cryptographic and anti-tamper detection functions. In contrast, TEE-based applications run directly on the processor and have access to large amounts of memory. Trustonic delivers software-based protection as an integral part of its solution, thereby enabling protection across all available devices, not just devices with the embedded Trustonic TEE.

Android Key Store - Android provides applications with access to a TEE-backed key store, which provides effective protection against lost and stolen devices. However, it does not protect against software threats. Access to the key store also needs to be protected to stop rogue applications requesting the use of a protected key, thereby bypassing its effectiveness.
WHERE TEEs ARE IN USE TODAY?

Both Apple and Android rely on TEEs to secure their platforms, in fact Google now mandates the use of a TEE in Android to secure features such as biometric sensors, key storage and content protection. Many phone OEMs deliver system level trusted applications to provide capabilities around payment, secure content storage, DRM and other services. Samsung itself uses the Trustonic TEE to underpin its Knox security platform, to perform biometric matching as well as to deliver Samsung Pay services.

Trustonic believe that third-party applications should be able to gain access to the same level of protection as the OEMs and has worked hard to create the ecosystem that exists today, offering service providers with the ability to properly secure their applications on an ever-growing number of devices.

Samsung Pay is underpinned by Trustonic’s TEE. Both key storage and cryptogram generation are performed inside the TEE, delivering a card scheme-certified solution.

Samsung ARTIK is an integrated IoT platform designed to simplify the process of delivering and launching IoT products. It has the Trustonic TEE at its core, delivering strong security for any solution.

Symantec VIP is a one-time code generator that uses the TEE to securely store the keys and code generation functions. It offers users with a Trustonic TEE-equipped device a lower cost, faster and more convenient method of accessing corporate services.

Samsung SDS FIDO is a solution where a biometric face recognition function is performed inside the TEE and a FIDO authentication credential is released if the faces match.

Alipay & WeChat Pay utilize the Trustonic TEE to secure a fingerprint sensor, enabling trusted and convenient user authentication and transaction validation.

Koolspan uses the Trustonic TEE to add an additional layer of security, safeguarding the TrustCall application on end-user devices against malicious attacks, thereby adding hardware-based protection to secure voice and text communications.

Shinhan Card & Hana Bank use the Trustonic TEE to enable trusted and convenient one-time password on mobile to deliver premium banking services.
HOW DO I USE A TEE IN MY APPLICATION?

Whilst TEEs are used in almost all Android devices today, unless they are open, they are of no use to a third-party application vendor. Trustonic believes that an open ecosystem is vital to ensuring that application developers have access to hardware-based device security. Trustonic is the only vendor delivering third-party developers access to the TEE and delivers its TEE (called Kinibi) to silicon and device vendors, who embed it into the heart of their devices. Trustonic’s TEE has so far been embedded into over one billion devices and every one of these devices is capable of hosting third party-secured applications.

Applications can be developed that consist of both a real-world component (running on the main OS of the device like Android) and a secure-world component, a trusted application, running inside the TEE.

The functions to manage features like the general user interface, high-level communications and business logic would typically remain in the real-world Android application, whilst functions dealing with sensitive operations such as user authentication, communications encryption, cryptography and secure storage would be executed and protected inside the trusted application running inside the TEE.

Any Android application including malware is physically unable to “see” and modify what is happening in the trusted applications running inside the TEE. The security is delivered at the processor level and cannot be bypassed by software, even if the device is rooted. This level of hardware-based separation ensures that rogue applications like Trojans are unable to gather sensitive information from resident applications and, therefore, cannot interfere with them.

Multiple trusted applications, usually coming from different sources (OEM, different service providers) running in the TEE, are also completely isolated from each other. As well as embedding the TEE into the device, each device is loaded with a unique device key - a unique hardware-based root of trust. This unique identity is injected when the device is on the production line and guarantees the authenticity and security of each Trustonic TEE-enabled device.

Trustonic also delivers a Trusted Application Manager (TAM), which enables secure application deployment and lifecycle management. The TAM can be hosted by the service provider or by a trusted third party, delivering them control of deployment of applications.

3 Trustonic announced at Mobile World Congress in 2017 that its TEE has been embedded into over one billion devices. http://bit.ly/2mF8Nly
and credentials. The TAM, utilising the multiple application capability of the Kinibi TEE, is what delivers the capability to load secured applications into the device post-deployment.

Trustonic’s TEE delivers several unique functions that cannot be delivered through software or secure elements. One key feature is a Trusted User Interface (TUI). The TUI enables applications to use the touchscreen and display without the ability for other applications to eavesdrop. It delivers the ability to perform features such as a secure PIN or passcode entry screen, or a truly secure messaging application. Many messaging apps claim to be secure, but most are just securing the communications and therefore any Trojan running on the device could intercept the display or touchscreen and could gather data that way. With a TUI that is not possible.

![Figure 1 - TEE secured peripherals](image)

Trustonic ensures that its products are secure by submitting them to security evaluations performed by independent certification laboratories. The Trustonic TEE is the first to have successfully achieved Common Criteria security certification for a TEE, based on GlobalPlatform’s TEE Protection Profile. The Trustonic TEE is also compliant with the GlobalPlatform TEE configuration version 1.1. The Trustonic TEE will be undergoing FIPS certification during 2017.

---

4 GlobalPlatform (www.globalplatform.org) is an international body that defines standards around hardware security. Trustonic has been an active member in the working groups and has helped define many of these standards. Trustonic meets these standards and certifies its products against them. GlobalPlatform has more than 110 members including MasterCard, Visa, ARM, Apple, Gemalto and Samsung.
Trustonic delivers a secure ecosystem enabling handset manufacturers, mobile application developers and service providers to deliver secure applications onto mobile devices. Trustonic has been working for over four years with chip manufacturers, mobile phone OEMs and IoT industry vendors to embed security into the heart of their connected devices. Once in-situ, this secure platform can be used by the device manufacturer to secure system-level services, as well as by service providers to secure their applications that will run on the devices.

Figure 2 - Hybrid application deployment

If you have a need to deliver secure mobile applications to your employees or customers, then Trustonic can help. We provide a toolkit and training to get you started. When you develop your applications, you need to identify the security-critical parts and migrate those to a trusted application, using the Trustonic GlobalPlatform compliant API. A secured application, including a combination of hardware and software-based security, will be created. The application can then be published into the appropriate app store as usual and, at runtime on the end device, the highest level of security available will be deployed. Over time, as your customers upgrade their devices, more of them will be able to take advantage of hardware-based security.

To find out more about how Trustonic can deliver the best on-device security to your mobile applications, please email enquiries@trustonic.com or go to www.trustonic.com/contact to request a meeting.
ABOUT THE AUTHOR

Paul Butterworth, the Strategic Marketing Director at Trustonic, has 25 years of experience in the IT security and card payments industry. Currently, he is helping Trustonic to deliver ground-breaking products to the mobile security market. Prior to joining Trustonic, he spent four years at Proxama, a leading mobile wallet and proximity marketing organisation, helping to drive technology strategy and leading the R&D team. In previous roles, Paul worked for ViVOtech as the lead technical resource in Europe, helping to deploy TSMs into the market, for nCipher as the product lead for the payShield HSM and for Verifone in a pre-sales role for the eCommerce division. He has a wealth of experience in understanding the challenges organisations face around security and deployment of large-scale mobile solutions.

Trustonic is a technology company whose mission is twofold:

- To establish a common security platform embedded in smart connected devices
- To enable app developers to utilize these advanced security capabilities