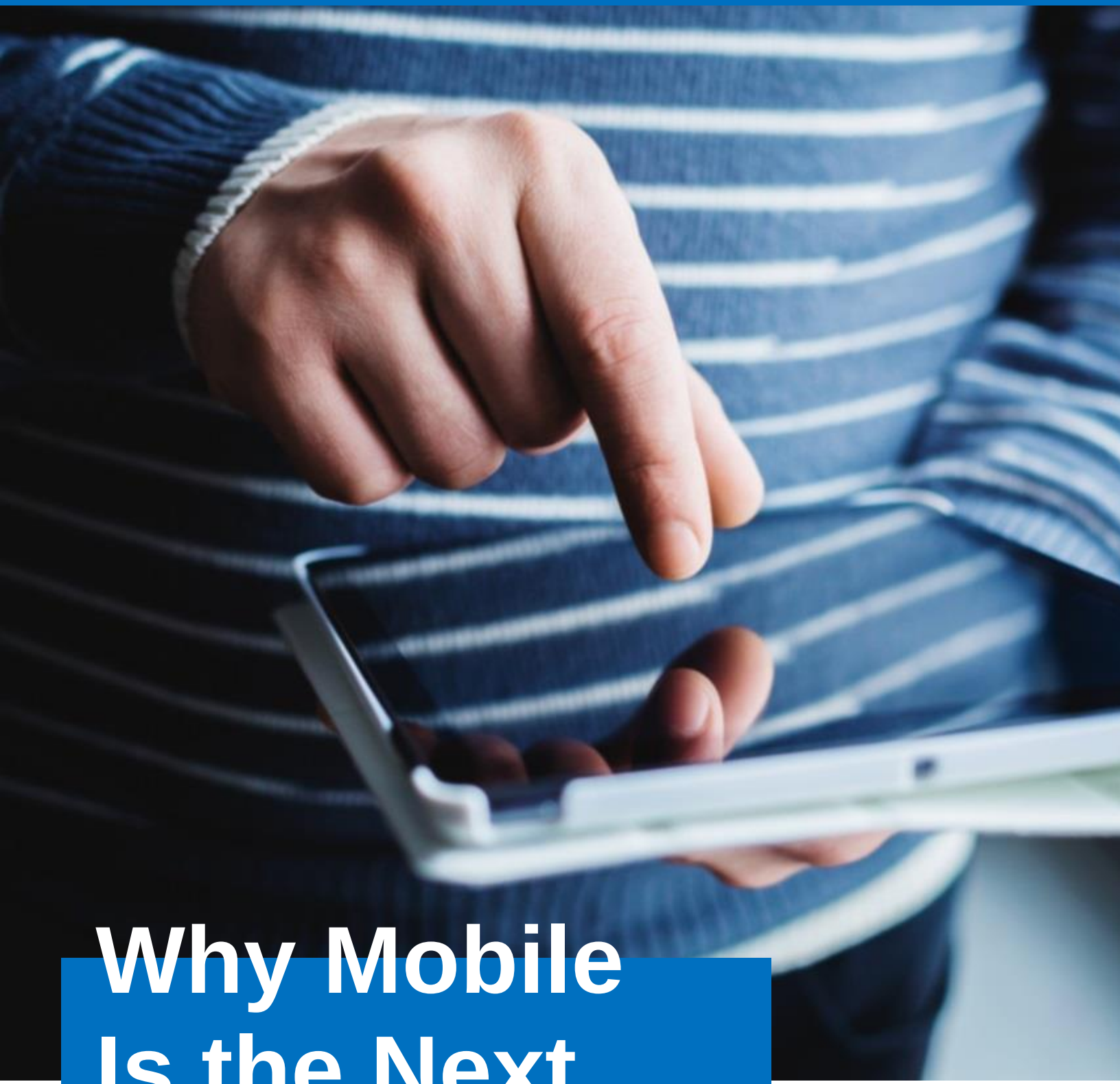
Entrust®

Entrust.com
1-888-690-2424
Entrust@Entrust.com



Why Mobile Is the Next Digital Identity

Enterprises Migrate to Mobile Platforms as Security, Convenience & Functionality Converge

Contents

The Era of the Mobile Identity

How can this growing acceptance of the mobile platform — across geographies, verticals, cultures and even age groups — be leveraged and extended to secure traditional digital identities in both the physical and online spaces?

It starts with the development of mobile platforms, where proven security was deliberate from the draft stages. This wasn't always the case with today's desktop PCs, where legacy techniques such as application-hooking still leave windows of app-to-app communication that may be exploitable by well-funded criminal organizations.

Another critical shift is the comfort level end-users have with their personal mobile devices. Executing tasks and making decisions is the norm, which now leads to greater adoption of mobile security controls.

Even the most novice users are quite adept at navigating the operating systems on today's smartphones. This global understanding was never so universal on the desktop.

"A mobile device can be the key to unlocking the potential for cross-over access to services, as well as being able to hold multiple IDs or credentials," said ABI Research Practice Director John Devlin. "In this respect, it is the central piece for convergence between online and offline identities ..."[1]

This white paper explores the birth of the mobile platform, identities shifts in trust, and explains specific technical reasons that mobile devise are more secure than today's standard desktop PC.

[1] "Could Mobile ID Be the New Killer App?" John Devlin, ABI Research, September 24, 2013.

Birth of a Mobile Computing Platform

It's hard to remember life before the first capable smartphone. It's similar to recalling an era before the Internet.

Even years later, June 29, 2007, still marks the beginning of a technology evolution. And it's not even hyperbole. Everything from checking emails, looking up movie times, watching TV shows, playing games and, yes, even making phone calls, changed when the first-generation Apple iPhone hit the market.

Google and Microsoft soon followed suit with Android and Windows Phone operating systems, and the market exploded.

The Introduction, Then Acceptance of BYOD

It was this consumer-driven shift that directly influenced the enterprise, sparking a critical shift in policy that allowed employees and staff to use powerful, consumer-level smartphones and mobile devices for work-related purposes.

It did take a handful of years to achieve critical mass, but consumer-owned mobile devices ushered in bring-your-own-device initiatives — more commonly known as BYOD — across the world.

This wide-spread adoption placed an entirely new computing platform into hands across the world in a relatively short time, especially when compared to the original acceptance of the first desktop-based PCs marketed to consumers in the early 1980s.

The Evolution of the Mobile User

Since the traditional PC is such a lucrative target for nefarious criminal organizations, hackers and nation-state attackers, the shift to the more secure mobile platform is a logical one — even if it does take some convincing.

Thankfully, user experience and security are no longer mutually exclusive, which often has been one of the biggest challenges of consumers adopting stronger security controls.

The average user is now experienced enough — and likely completely fatigued by unsecure username and password schemes — that they're ready to embrace newer security capabilities provided by mobile devices, operating systems and applications.

> "The average user is now experienced enough that they're ready to embrace newer security capabilities provided by mobile devices, operating systems and applications."

As the mobile user continues to evolve and mature — sometimes owning and using as many as three mobile devices — they demand that banks, governments, retailers and other organizations embrace mobility.

Supporting this stance, a recent Forrester report, “Mobile Authentication: Is This My App? Is This My User?” suggests more than half of users (52 percent) now rely on three or more devices. In fact, 60 percent of the devices are used for both personal and business use.[2]

Malware on the Rise

What’s shocking, however, is that enterprises still aren’t taking targeted, malware-based attacks against their organization seriously.

According to a May 2013 report by Kaspersky Lab, 90 percent of surveyed organizations underestimated the number of new malware strands found daily.

Even worse, only 6 percent recognized the serious nature of malware — particularly against enterprise data and identities.[3] According to Kaspersky Lab, almost 200,000 new malware strands appear globally each day.

Mobile Devices are More Secure

But even with sandboxed mobile applications, secure operating systems and savvy mobile users, the perception remains that mobile devices aren’t computers to be taken seriously — and, as a result, aren’t as secure.

In fact, the complete opposite is true.

Whether used for secure physical and logical access, authenticators for digital identities, platforms for soft tokens or even as tools to verify desktop-based transactions to defeat malware, mobile devices, by default, have a better security posture than today’s standard PC.

[2] “Mobile Authentication: Is This My App? Is This My User?” Andras Cser, Chenxi Wang, Forrester Research, December 5, 2012.
[3] “Global Corporate IT Security Risks: 2013,” Kaspersky Lab, May 2013.

Mobile Devices: Fighting Inaccurate Perceptions

While the security of mobile devices continues to fight an inaccurate perception, the reality is quite clear: mobile devices possess stronger security architecture when compared to PCs.

When properly managed and protected, mobile devices serve as a formidable platform for securing digital identities and online transactions. Despite the growing reliance on mobility, IT decision-makers still incorrectly believe traditional PCs are more secure than mobile devices.

To gain additional insight on this issue, Entrust commissioned Forrester Consulting to publish a report, **"Mobility Helps Enterprises Enter a New Age."**

Of those who responded to the Forrester Consulting survey, some 71 percent either somewhat or strongly agreed that desktops/laptops are secure, as opposed to 43 percent that said mobile devices are secure.[4]

Shift in Thinking

The innovation in mobile security solutions could be the catalyst for the changing perception in the enterprise. According to the Forrester study, enterprises are investing more in mobile, and are making mobile security a high or critical priority.

This is an important shift as the true power of mobility isn't yet being realized. The use of mobile capabilities that actually increase security or streamline business — mobile commerce (10 percent), partner/supplier applications (12 percent) and customer-specific applications (14 percent), for example — is decidedly lower amongst responders.

Once mobile devices are properly secured, leveraged and managed, more and more enterprises will embrace mobility as a standard business component.

The commissioned study found that IT decision-makers were migrating to mobile because of flexibility over traditional authentication (68 percent) and the ability to adapt to threats (64 percent).

In contrast, the study found that 50 percent of enterprises have implemented, but are not expanding, very basic access to email and calendars from mobile devices.

Of those same responders, access to network systems (42 percent) and supporting collaboration (36 percent) marked other accepted use cases.

[4] "Mobility Helps Enterprises Enter a New Age," Forrester Consulting (on behalf of Entrust), April 2013.

Mobile Advantages over Traditional PCs

Despite media reports on mobile devices being insecure, mobile OS architectures offer a level of security that is above desktop operating systems.

Desktop malware — performing malicious app-to-app process migration, native keyboard key-logging and Zeus-style memory-hooking — is not being found in mobile malware samples. Plus, specific mobile vulnerabilities usually have a short lifespan.

As for Android, malware usually targets specific hardware, firmware and OS versions, which greatly reduces the viability and lucrativeness of large-scale infections.

Today's mobile devices are more secure thanks to a multilayered approach that's core to the development of mobile operating systems. Applications installed on mobile devices are digitally signed and/or thoroughly vetted.

Legitimate applications also are sandboxed, meaning they can't share or gain access to each other's information — an important trait that helps defend against advanced mobile malware.

The strength of mobile platforms is further augmented by third-party security capabilities. Solutions that offer digital certificates, embed transparent OTPs, or provide application-specific PIN unlock options further bolster device security.

Confidence in Mobile

- **Signed/Vetted Applications**
- **Application Sandboxing**
- **Embedded Security** *(e.g., digital certificates, PINs to unlock apps)*
- **Biometrics** *(e.g., fingerprint, voice, facial recognition)*
- **Alternate Technology Available** *(e.g., GPS, IP-Geolocation, Device Identity)*
- **Enterprise-Ready Security Containers**
- **Fragmented Ecosystems Harder to Target**
- **Future Technology Offer New Security Paradigms and Features** *(e.g., Trusted Execution Environment, Secure Elements)*

Signed/Vetted Applications

Mobile applications from official stores are digitally signed with certificates to authenticate the source and verify the content integrity of the application.

Code-signing certificates provide assurance that customers are installing code or applications as they were intended. This helps protect the various mobile platforms with varying success.

For example, Apple does not allow apps to be installed on an iOS device unless it originates from the official Apple App Store. Plus, apps from the Apple App Store must be code-signed before being approved by Apple for public distribution.

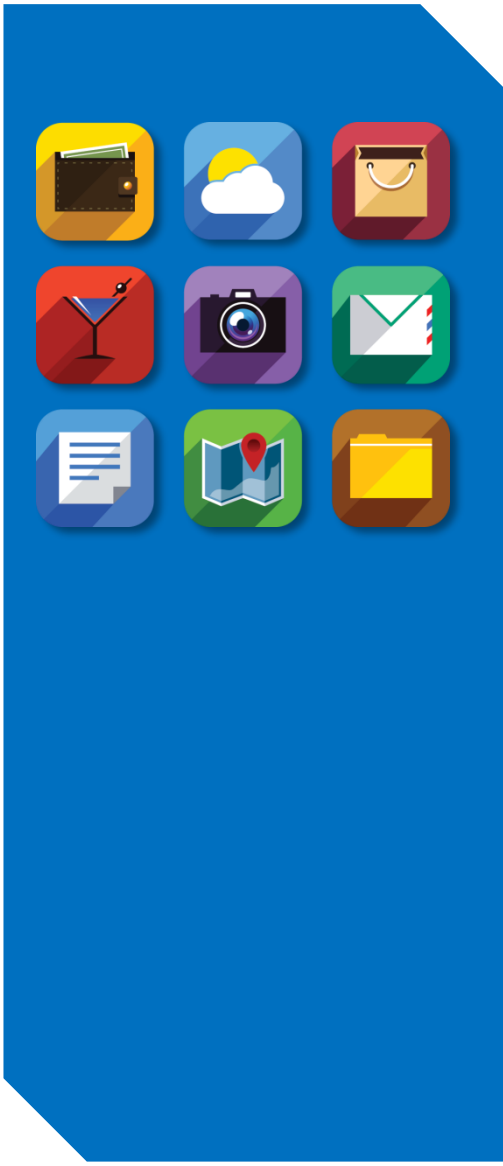
Installing or embedding malicious code on non-jailbroken iOS devices is extremely difficult. In fact, there have only been a handful of remotely successful examples, none of which executed any kind of malicious activity.

Contacts and photographs have been compromised, but that's been the extent of recorded breaches.

In comparison, the Android operating system permits the use of side-loading apps from beyond the Google Play store. To date, this is the major source of malware and primary reason Android is afflicted with malicious attacks.

The Google Play store is not as well scrutinized as the Apple App Store, but Google is getting better and reacts quickly when malware is found.

Application Sandboxing



Applications for today's popular mobile operating systems — namely Apple iOS, Google Android and BlackBerry — are secured via an architecture called sandboxing, which means they cannot communicate with each other. This reduces, and in some cases eliminates, data-sharing.

For example, a gaming application's data is completely separate from other apps (e.g., banking, social). Therefore, due to the sandboxing architecture, the applications don't use the same memory space. And if malware is installed on an Android device, sandboxing limits or eliminates its ability to interfere with the memory space of another application.

In desktop operating systems, many applications share memory space and will typically use a type of 'DLL API hooking' that is completely normal for standard functions.

Unfortunately, desktop malware is able to hop between application memory spaces with great ease. Thus, the application architecture of desktops isn't as secure as the sandbox architecture of many mobile operating systems.

To date, the industry has not seen malware outside of a lab environment that has been able to move between memory spaces on mobile operating systems, which were engineered from the ground up with built-in application isolation.

The Zeus virus, for example, is desktop malware that hooks the memory space of your desktop browser to perform man-in-the-browser (MITB) attacks, which are not possible on mobile because the browser is an isolated or sandboxed application.

However, man-in-the-mobile (MITMO) attacks are still possible as this vulnerability isn't the fault of the hardware or mobile operating system, rather the shortcomings of browsers and/or vulnerabilities in the website itself.

Application communication on Android and iOS is executed through *intents* or, more simply, "subscribed forms of communication."

As a malicious criminal group or hacker, you cannot write malware that will manipulate another application without that application requesting permission to be manipulated. Conversely, this is the opposite on desktop environments, which are, more or less, free-for-all-environments.

Embedded Security

Many basic security controls already in use today include PINs to unlock devices or applications, as well as digital certificates. The latter provides strong device and identity authentication to enable secure Wi-Fi or VPN access.

Organizations also may leverage digital certificates on mobile devices to enable secure email (S/MIME) communication.

Available Alternate Technology

Besides PINs, biometrics (e.g., retina or fingerprint scans, facial recognition) may be a better alternative in the near future to be able to access a mobile device.

Enterprise-Ready Mobile Security: Personal & Corporate Containers

Somewhat new to the market, mobile handset companies are releasing enterprise-ready features included on devices.

Two of the most recent — **Samsung Knox** and **BlackBerry Balance** — allow IT departments to control corporate data and policies in a secure container separate from the end-user's personal data.

This helps organizations enable BYOD while minimizing legal risk and/or data leakage concerns.

Biometrics

In September 2013, Apple introduced the Touch ID fingerprint authentication reader as part of the company's iPhone 5s. It was the first major U.S.-based mobile manufacturer to incorporate a consumer-level fingerprint scanner since Motorola released the Atrix 4G in 2011.

Soon after the device was released, Touch ID received much criticism for being easily bypassed. Germany's Chaos Computer Club was the first to claim to have circumvented Apple's new Touch ID biometric fingerprint sensor.[5]

More recently, Samsung unveiled and released the Samsung Galaxy S5 with an integrated fingerprint sensor. And as with Apple's Touch ID, weakness were discovered with the Samsung product.

"Attacks on fingerprint biometric systems are relatively difficult to carry out," said Alan Goode, founder and managing director of Goode Intelligence. "Mobile device manufacturers and service providers are turning to biometrics because they can enhance the usability of the authentication experience — this must not be altered."[6]

It's important to remember the security baseline Apple was implementing with Touch ID, which was not intended to be the gold standard for identity-based security.

Its goal was to remove inconvenience to increase consumer adoption of a basic security measure, but also pave the way for more advanced biometric authentication in the future. And it's absolutely a step up from current security measures such as passcodes, patterns and photo unlocks.

Regardless of the low-level "hack," consumers' biometric data for Apple Touch ID remains absolutely secure.

It's still encrypted on a segregated secure element — Apple brands this as the Secure Enclave — on the mobile device's chip and is never transferred, shared or otherwise communicated or shared with Apple, iCloud or the cellular provider.

"In the torrent of the billions of words already written about Touch ID, very, very few people have really understood just how revolutionary this really is," said Forbes contributing writer Brian Roemmele, founder and CEO of 1st American Card Service.[7]

"Apple not only has developed one of the most accurate mass produced biometric security devices, they have also solved critical problems with how the data from this device will be encrypted, stored, and secured."

Apple's Touch ID

In September 2013, Apple introduced the Touch ID fingerprint authentication reader, building one of the largest consumer install bases for biometric authentication.

[5] "Apple Touch ID fingerprint tech 'broken', hackers say," BBC, September 23, 2013.
[6] "The Samsung Galaxy S5 fingerprint sensor has been spoofed - what can be done to prevent it," Alan Goode's Blog, Alan Goode, April 16, 2013.
[7] "What Is Apple's New Secure Enclave And Why Is It Important?" Brian Roemmele, Forbes (Quoro), September 18, 2013.

Fragmented Ecosystems

Mobile ecosystems are organized and categorized based on the operating system in use, specific hardware, firmware versions, etc. These wide variations cause fragmenting of the ecosystem, which makes it more difficult for malware authors to target large-scale user populations.

If a hacker, online criminal or other malicious group wants to deploy malware to attack mobile devices, they're only able to target a specific sub-set of mobile users.

While a mobile OS developer may push an update to the handset providers, the providers still have to make it available to the end-user.

In theory, three different users, owning three different mobile devices, could be using three different OS versions with different patches — all on the same carrier.

This decreases the attack surface in one regard, but makes it possible for the user to rely on out-of-date software that could be compromised.

A recent Juniper report[8] had some additional data that supports vulnerabilities around mobile fragmentation.

It stated, "According to Google, as of June 3, 2013, only four percent of Android phone users were running the latest version of the operating system, which provides mitigation against the most popular class of malware measured by the MTC that makes up 77 percent of Android threats."

[8] "Juniper Networks Finds Mobile Threats Continue Rampant Growth As Attackers Become More Entrepreneurial," Juniper Networks, June 26, 2013.

Mobile Security for Today — And Tomorrow

Forward-thinking security organizations already offer you certain advanced mobile security capabilities that are proven to stop malware, authenticate devices and enable business.

Going a step forward, it's important to keep an eye on the next phase of mobile security — controls or technology that will shape the mobile landscape for the next five to 10 years.

Device Certificates

As previously mentioned, device certificates provide strong identity authentication to enable secure Wi-Fi or VPN access.

When using certificate-based security on mobile devices, organizations can defend themselves against unauthorized sharing of Wi-Fi passwords. These certificates can be unique for each device they are provisioned.

Digital certificates may be provisioned and managed through a variety of methods. Whether deployed via cloud or on-premise models, organizations may select the method that best suits their security needs, budget and environment.

Transparent Identity Authentication

Unfortunately, some security practices may create usability barriers, which end up frustrating user populations. In order to introduce security, but maintain acceptable usability, organizations opt to embed transparent security technologies.

When mobile app developers leverage embedded technology, they may simply use a mobile software development kit (SDK) that allows them to build their apps with strong transparent security.

With respect to authentication, developers may embed transparent application/user authentication into a mobile application.

Whether in the form of a one-time passcode (OTP) or an x.509 digital certificate, a credential can be requested by an authentication mechanism to ensure the authenticity of a mobile application. This helps ensure transactions are being performed with legitimate applications.

The credential may also be leveraged to sign a transaction back to the authentication mechanism so the transaction's authenticity is verified, commonly referred to as transaction verification. The user may have to do as little as "confirm" or "cancel" to accept or decline a transaction.

By not requiring the user to actively input an additional authentication factor, the user experience is greatly increased and the steps to executing a secure transaction reduced.

Additional security measures may be embedded to detect jailbreaks or bootloading, and to transmit data over a secure (encrypted) out-of-band channel to the authentication mechanism.

Simplify the User Experience

By not requiring the user to actively input an additional authentication factor, the user experience is greatly increased and the steps to executing a secure transaction reduced.

Transaction-Signing

Qualified digital signatures are able to legally authorize transactions, increase efficiency and enable new business services in both enterprise and customer processes.

With digital-signing built into mobile applications, organizations eliminate the need for complex client-side software and expensive signing tokens — all while delighting customers with new, convenient services.

Multipurpose Mobile-Based Virtual Credentials

Organizations will be able to eliminate hardware tokens, passwords and even physical access cards with an always-on-hand smartphone. Embed smart credentials on employee smartphones to create trusted identity credentials for stronger, more convenient enterprise authentication.

Mobile smart credentials use near-field communication (NFC) or Bluetooth standards to securely access computer workstations, network resources, data, cloud applications, physical doors or buildings, and also enable users to digitally sign transactions and encrypt data.

Device Capabilities

Organizations that opt for a more dynamic platform approach may introduce or change mobile security controls as technology improves — camera, voice channel, GPS or touch patterns, for example — with little or no adverse effects on the environment or user population.

> *“It is also important to remember that while the population of malicious mobile software is growing rapidly, it still remains smaller than threats to computers.”*
>
> **— Third Annual Mobile Threats Report**
> **Juniper Networks**
> **March 2013**

Secure Elements

The secure element of a mobile device is the complete or partitioned portion of a chip found on a SIM card, Micro SD card or embedded in the chipset of the mobile device itself.

The secure element provides higher-assurance security for the storage of applications, cryptographic data and confidential information. As is achieved with advanced smartcards, secure elements feature tamper-resistant measures and advanced cryptographic features to make exploitation of the sensitive data stored in the chip difficult.

By leveraging a secure element, a user can be confident in the security and privacy of their identity and transactional data — all beyond the security and privacy offered by sandboxed applications.

Trusted Execution Environments (TEE)

Trusted Execution Environments (TEE) differ from secure elements in that the software runs in an isolated environment from the primary operating system, which is called the “rich OS”.

The TEE can utilize the secure element for higher-assurance transactions and may act as a bridge between the rich OS and the secure element. The TEE is often used for the execution of sensitive transactions/data that requires advanced security measures.

What is the Trusted Execution Environment?

The Trusted Execution Environment, or TEE, is a secure area that resides in the main processor of a smart phone (or any mobile device) and ensures that sensitive data is stored, processed and protected in a trusted environment.

The TEE's ability to offer safe execution of authorized security software, known as 'trusted applications,' enables it to provide end-to-end security by enforcing protection, confidentiality, integrity and data access rights.

— Global Platform

> Read More

Recognizing Mobile Vulnerabilities

Consumers and enterprise decision-makers alike can be swayed by misguided media reports. Some educated concern about mobile security is rational, but mobile-based attacks to date are only gaining access to photographs, contacts, calendar items and SMS capabilities, the latter being the most concerning.

SMS Attacks a Real Concern

SMS-based malware Zeus-in-the-Mobile (ZITMO), and its variants, demonstrates how SMS redirection can exploit Android-based mobile devices for illegal financial gain.

Another example, known as premium-rate fraud, leverages SMS-based malware to actively make money for the attacker by having the targeted Android device automatically text an SMS pay service.

Because of end-user comfort and trust in text messages, SMS-based malware should not be underestimated. It's strongly advised that organizations consider the risk and exposure of SMS-based security controls, including SMS OTPs, for sensitive or high-risk transactions. Unfortunately, these channels now present a security risk.

Defending Against App Cloning

Many application developers tie data to specific device hardware to defend against application cloning, which may be used for nefarious attacks.

If malicious groups attempt to clone properly secured applications to another device, the application will detect a change in hardware and stop functioning properly.

This helps prevent applications from being used on another device, and requires credentials to be re-enrolled and re-encoded due to the change in hardware, or at the end of the credential's lifecycle.

> *While mobile devices are technologically more secure than traditional PCs, decision-makers view mobile devices as insecure because of media reports and the small size and personal nature of the devices.*
>
> **— Forrester Consulting**

Jailbreaking, Rooting & Sideloading

Despite the efforts of OS developers, users often desire more versatility and customization, regardless of the ramifications. Many of today's most ominous malware strands target security voids created on jailbroken or rooted devices.

However, most jailbreaks are written by well-meaning coders or hackers who simply wish to extend the functionality of mobile devices. It's also important to remember that jailbreaks on iOS devices are not possible without physical connection since the release of iOS 4 in June 2010.

To date, it's not possible for an iOS device to be jailbroken without physical access to the device — and with a very obvious series of steps.

Because of this, there's low that criminals will be able to leverage social engineering methods to manipulate an unsuspecting end-user into jailbreaking their device in hopes of introducing malware.

Jailbreaking a device — often to circumvent digital rights management (DRM) or to use media and applications without paying — **does not** automatically introduce malware. The device's native security, however, is completely removed.

Jailbreaking & Bootloading

Jailbreaking is a term that applies to the Apple iOS platform. Android *bootloading* is the act of downloading and installing a version of the operating system that has been altered or manipulated to remove developer restrictions or other controls.

Jailbreaking involves a series of exploits against the iOS operating system, initiated through physical access to the device, wired to a desktop computer.

Jailbreaking gives the user the option of installing unauthorized, unsigned applications for greater customization, but does introduce many new security vulnerabilities.

“Many of today's most ominous malware strands target security voids created on jailbroken or rooted devices.”

Rooting

Rooting is popular among Android users and provides “root access” to either portions or all aspects of mobile devices using the Google Android operating system.

It’s similar to jailbreaking, but does not necessarily mean the user has gained full root access to the entire device.

This enables the user to remove or circumvent system controls, applications and settings to execute unauthorized applications or perform other actions that require administrative controls not available on a stock device (except for the Google Nexus, which ships rooted for developers).

It is also used to circumvent carrier restrictions for upgrading the Android operating system. Users who want a newer operating system than the one installed will often root their device to upgrade the operating system.

Sideloading

Derived from well-known terms of *upload* and *download*, *sideloading* is the act of Android users downloading applications from unknown sources outside of the Google Play store.

There is a setting within the Android OS that allows a device to sideload applications.

Unfortunately, sideloading is a major source of malware and dramatically increases the risk exposure of end-users and organizations alike.

Mobile Mitigates Risk, Enables Efficiency

As the use of mobile devices and applications grows — and mobile (BYOD and corporate-issued) initiatives become more commonplace — so do the security risks and attacks targeting user identities, intellectual property, customer data and financial assets.

To effectively mitigate risk, enable true efficiency and satisfy customer expectations in the mobile environment, organizations must ensure mobile devices and related identities are secure — but in a way that minimizes user barrier and frustrations.

Once secured, organizations then have the opportunity to leverage mobile devices to improve security in other parts of the business.

With the growing dependence on mobile devices to execute business operations, organizations are urged to provision solutions that not only address security needs, but also ensure the mobile experience is simple from an end-user perspective.

For the Enterprise

In the enterprise, secured mobile devices are effective, popular and may be leveraged as a virtual employee identity to securely access computers, applications, cloud services and even physical doors. In high-risk situations, mobile may be leveraged to provide identity-assured transactions that effectively defeat malware-based attacks.

For the Financial Customer

In contrast, smartphones may be used to empower customers to better secure online transactions and defeat malicious fraud attacks that attempt to highjack customer accounts.

This movement holds the promise of safe, convenient and always-in-hand solutions to secure identities and transactions across various environments.

This two-pronged approach — first **secure** the device, then **leverage** it to improve security — is an effective method to reduce business risk and introduce new, innovative transactional services that improve the user experience for customers and employees.

Strength of Cryptography

The link between cryptographic security and strong identity is essential to understanding security in a modern information system. Cryptography binds information to the identities of those who are accountable for its preservation.

This enables effective prevention, detection and deterrence of criminal acts by both internal and external actors, despite the presence of vulnerabilities in the extended network.

The underlying system is strong, requiring only changes in the cryptographic variables over time in response to evolving threat conditions.

As technological advancement and computing power advances, it is inevitable that cryptographic strength will need to stay mathematically out of reach.

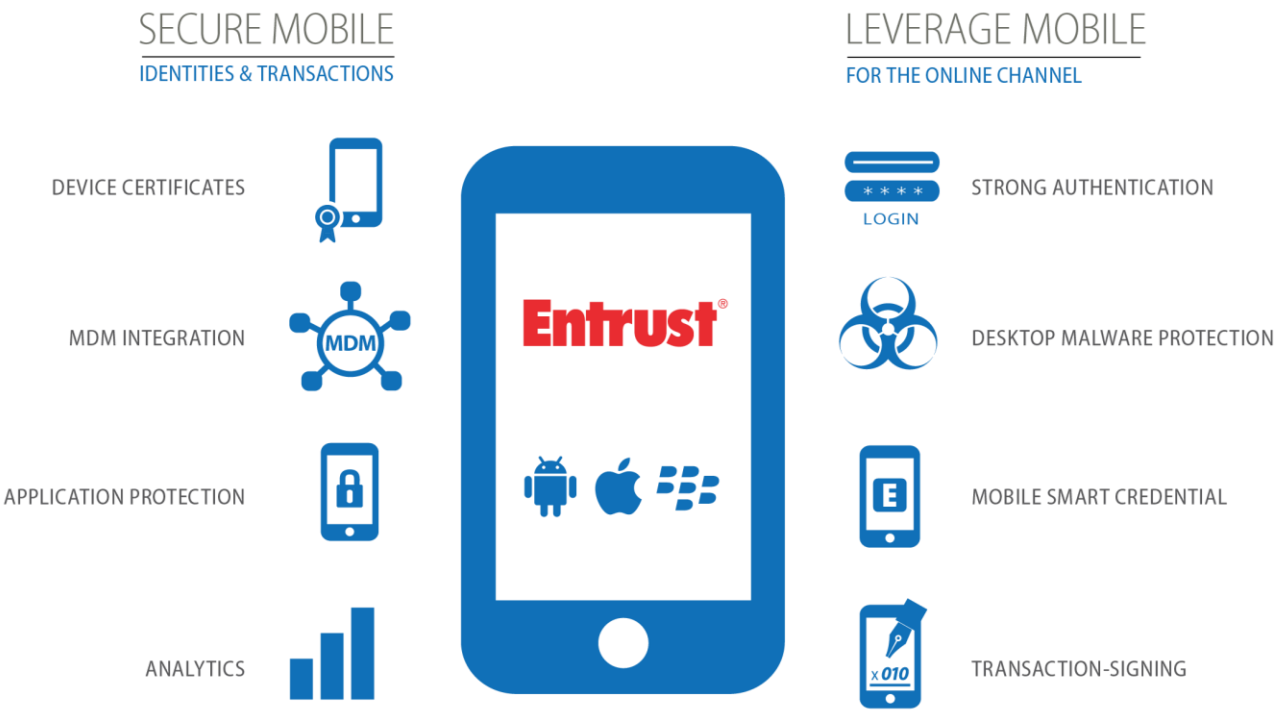
This is why, for instance, the use of 1024-bit RSA keys is no longer prudent and is being deprecated in favor of 2048, and why the MD5-based hash algorithm was discontinued years ago.

The active involvement of an open community comprising academia, government and industry to maintain the understanding of evolving attack vectors and cryptanalytic techniques is essential to the maintenance of this piece of the critical infrastructure.

Secure Mobile, Leverage Mobile

Entrust offers a number of capabilities that not only help secure mobile identities and transactions, but also empower organizations to leverage mobile devices to improve overall security and streamline business processes.

Security controls are increased across all channels, enabling more convenience for employees and customers alike.



Secure Mobile Identities & Transactions

With the growing dependence on mobile to execute business operations, organizations are provisioning solutions that not only address security needs, but also ensure the mobile experience is simple and unencumbered.

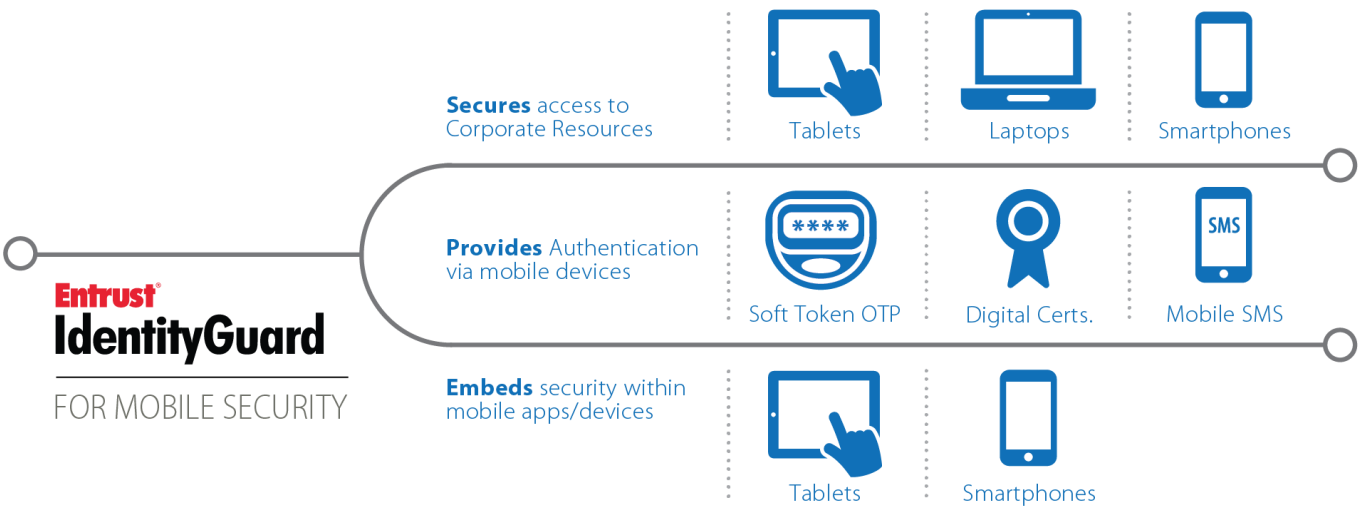
Entrust solutions authenticate mobile devices connecting to a network, encrypt and digitally sign mobile email communication, embed identity protection into mobile applications, and monitor transactions to detect fraudulent or unauthorized activity.

Entrust also offers a range of on-premise, hosted and pre-integrated mobile device management (MDM) capabilities to suit your needs.

Leverage Mobile for the Online Channel

Using mobile devices for strong authentication and identity-assured transactions is the secure, practical and cost-effective approach to enable organizations to unlock the power of mobile computing.

Entrust offers a number of solutions to defeat malware and secure access to logical, cloud and physical resources.



Embrace the Mobile Security Movement

The proliferation of mobile devices is front and center for virtually all organizations, in both employee and customer communities.

In fact, 526 million mobile devices and connections were added in 2013 alone. Globally, mobile data traffic grew 81 percent during that same time.[9]

This momentum will not slow. Organizations must prepare to better leverage mobile devices as a secure channel for communications, information exchange and transactions.

Within the enterprise, mobile helps streamline business processes, increasing responsiveness and efficiency. In contrast, mobile also presents tremendous opportunities to engage customers and provide new and differentiated services.

Whether it's for banking, online services or Web-based transactions, this shift has forced financial institutions, e-commerce companies and any organization with an online presence to re-think how they service customers — particularly from the mobile channel.

[9] "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013-2018," Cisco, February 5, 2014.

Research Methodology

The cited Technology Adoption Profile was commissioned by Entrust.

To create this profile, Forrester leveraged its Forrsights Budgets and Priorities Tracker Survey, Q4 2012, Forrsights Hardware survey, Q3 2012, Forrsights Workforce survey, Q4 2012, Forrsights Workforce survey, Q2 2012, as well as its Forrsights Security survey, Q2 2012.

Forrester Consulting supplemented this data with custom survey questions asked of 50 senior technology decision-makers in North American companies with 2,000 to 10,000 employees. The auxiliary custom survey was conducted in January 2013.

Entrust & You

More than ever, Entrust understands your organization's security pain points. Whether it's the protection of information, securing online customers, regulatory compliance or large-scale government projects, Entrust provides identity-based security solutions that are not only proven in real-world environments, but cost-effective in today's uncertain economic climate.

Entrust offers software authentication platforms that strengthen security in a wide range of identity and transaction ecosystems. Government agencies, financial institutions and other enterprises rely on Entrust solutions to strengthen trust and reduce complexity for consumers, citizens and employees.

Now, as part of Datacard Group, Entrust offers an expanded portfolio of solutions across more than 150 countries.

Together, Datacard Group and Entrust issue more than 10 million secure identities every day, manage billions of secure transactions annually and issue a majority of the world's financial cards.

Entrust's award-winning software authentication platforms manage today's most secure identity credentials, addressing customer pain points for cloud and mobile security, physical and logical access, citizen eID initiatives, certificate management and SSL.

For more information about Entrust products and services, call **888-690-2424**, email **entrust@entrust.com** or visit **entrust.com**.

Company Facts

Website: www.entrust.com
Employees: 359
Customers: 5,000
Offices: 10 Globally

Headquarters

Three Lincoln Centre
5430 LBJ Freeway, Suite 1250
Dallas, Texas 75240

Sales

North America: 1-888-690-2424
EMEA: +44 (0) 118 953 3000
Email: entrust@entrust.com