ADVANCING MOBILE TECHNOLOGIES

WITHOUT SACRIFICING SECURITY

Properly configured, mobile can be safer than on-prem devices.

Our smart phones know us as well as—or even better than—we know ourselves. From when we arise in the morning to when we go to bed, our mobile devices act as the proverbial "fly on the wall," observing and recording what we do, and when and how we do it.

But for government and enterprise CIOs and IT security managers, this intensely personal relationship between employees and their portable devices—essentially handheld supercomputers—presents a new combination of challenges.

The more data these devices collect or share, and the more they serve as conduits to enterprise systems, the more attractive they become to criminals. Targeted mobile cyber attacks, having rarely occurred a few years ago, are on the rise.

For instance, McAfee Labs reported a total of 16 million mobile malware attacks in the first quarter of 2017 alone. That number is small compared to the billions of attacks on enterprise networks, but it has increased quarter by quarter. Spyware, botnets, and click fraud are also emerging threats to these devices, potentially endangering the security of individuals, businesses, and government agencies.

This uptick in mobile breach attempts makes state-of-the-art security a must, especially, in the age of Bring-Your-Own-Device, for the government sector—and is one reason why the U.S. Department of Defense (DoD) and National Security Agency have both approved Samsung Galaxy devices running the Knox security system as fit for government work. Their decisions offer a significant counterweight to common perception that Android-based devices are less secure than other brands. In fact, it confirms that Knox-equipped Samsung devices are among the most secure.

> "Building a chain of trust, from hardware through bootloaders to the device's operating system, ensures that your agency's data is protected before the Android OS even starts."

It also demonstrates that mobility does not have to mean sacrificing security.

True, portable computing devices can be lost or stolen, and many mobile apps lack adequate security features. But innovative technologies including derived credentials, behavioral analytics, and containerization—all features of the Knox platform—offer superior user authentication and multi-layer data/network protection at the transactional level, embedded in the Samsung hardware, for the most comprehensive suite of cutting-edge security services on the market today.

GUARDING THE GATE

The first challenge for mobile security is ensuring that only the authorized individual is using the device. Phones and tablets are too often lost or stolen, and laptops left unattended can be easily be viewed by unauthorized eyes.

To address these risks, federal agencies including DoD have issued Personal Identity Verification or Common Access Cards (PIV/CAC) to verify personnel identity in a variety of situations, including when employees log into government networks and sign documents digitally. But inserting CAC cards into a physical reader connected to a mobile phone or tablet can be cumbersome.

Knox's derived-credential technology eliminates the need for a physical card by placing verified identity credentials directly and securely onto the mobile device, much as mobile-pay systems do away with the need to make payments using a plastic credit card. This technology offers the added benefits of making identity verification more convenient, and preventing unauthorized logins.

But derived credentials and authentication tools such as biometrics offer only a one-time, "snapshot" form of user verification. Once the user has passed the initial test and gained access, the device and everything on it become fully available for viewing and use.

Behavioral analytics promises to change this paradigm. By learning user behavior—understanding and identifying browsing habits, messaging syntax, and even how the user holds the phone—tools designed to capture how a device is used can provide the equivalent of a continuously-authenticating security "video," (compared to one-and-done "snapshot" tools) to detect interlopers transaction by transaction.

> Knox's "nested" containerization approach... can be configured to create a small ecosystem of intermeshing apps inaccessible by others. It allows double-encryption at any point—because there's really no such thing as too much security.

Security technologies in platforms, including Samsung Knox, take authentication even farther than just protecting your employee and agency data while it is at rest, in use, or in transit. Knox can authenticate at the transaction level by verifying not only the person performing the transaction, but also the permission to perform it at that exact time and location. If a user tries to execute a sensitive transaction in a hostile location, the device may disallow access to that operation (while continuing to allow other uses).

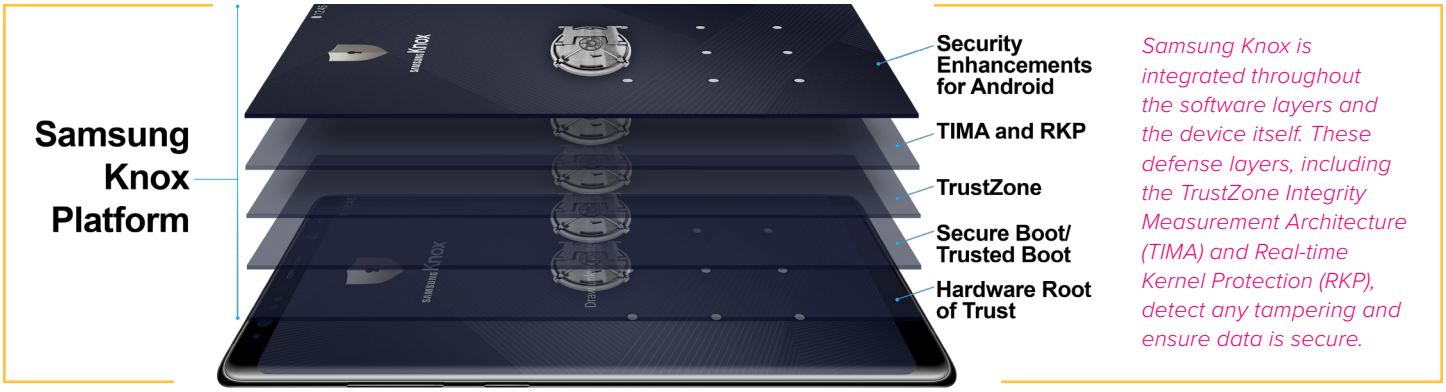
DIVIDE AND CONQUER

As an increasing number of organizations allow personnel to bring their mobile devices to work (BYOD)—as many as 50 percent by 2018, according to Mobile Business Insights—agencies may wish to use platforms such as Knox to place virtual "containers" around their data, limiting access.

Containerization allows enterprise IT directors to build 'walls' on mobile devices that can:

- "sandbox" apps, controlling how they interact with the mobile device ecosystem
- isolate a device to perform a single function
- divide work data from personal data
- set apart everyday apps and information into modes or silos separate from those where work-related data and documents reside

One often-overlooked benefit of containerization: when agency personnel use devices in "work only" mode, they experience fewer distractions and tend to be more productive.



Samsung Knox is integrated throughout the software layers and the device itself. These defense layers, including the TrustZone Integrity Measurement Architecture (TIMA) and Real-time Kernel Protection (RKP), detect any tampering and ensure data is secure.

Not all mobile devices use container technology in the same way. Some create containers at the operating system level. Others, such as Knox Workspace, take full advantage of ARM architecture by compartmentalizing the most sensitive information and processes, and storing them in a "trust zone" or "secure world," according to Craig Ano, leader of Samsung's Federal Technical Team. Knox's approach, using hardware-based security, makes it superior to operating system level security.

Building a chain of trust, from hardware through bootloaders to the device's operating system, ensures that your agency's data is protected before the Android OS even starts. Then, Knox continues to build that security chain and allows solution providers to do the same, for example, enabling a mobile device management tool to secure transactions.

Knox goes even further by offering a "nested" containerization approach that allows "sandboxing, " or isolation of a single application. The technology can containerize two apps so that they know only about each other, and nothing else on the device. It can be configured to create a small ecosystem of intermeshing apps inaccessible by others. And it allows double-encryption at any point—because there's really no such thing as too much security.

Of course, a device is, at its heart, only as secure as its hardware. Applications and even operating systems may be vulnerable to attack, but when security is "baked in" to the device, cybercriminals must breach an impenetrable layer to reach them. During Knox's continual verification and authentication process, its one-time warranty "fuse," when tripped by an intruder, shuts down access or even switches off the device, preventing added attempts. This unique hardware-based security sets Samsung and its Knox platform head and shoulders above the rest.

KNOWLEDGE IS POWER

The fact is, most enterprises use only a small portion of their phones' capabilities, leaving them much more vulnerable than they need to be. Many of Knox's features go unused because administrators lack an understanding of how to configure its settings, and of all the possibilities for doing so.

In this case, knowledge is power. Agency CIOs and IT security managers who inform themselves will certainly find that the perception of mobile devices in general, as being less secure than PCs is no longer valid. Samsung Knox, for instance, has five government certifications, including an MDFPP validation through NIAP/Common Criteria, assuring agencies that they can safely deploy Samsung devices (with containers, or without).

The idea that mobile technologies risk sacrificing security and privacy for the sake of convenience is widespread, but inaccurate. Although 34 percent of respondents to a recent survey by Dimensional Research said they think mobile devices are less secure than PCs, when properly configured these devices can actually be more effective than their larger digital brethren.

As FireEye president Kevin Mandia has noted, mobile phones cannot be traced to an IP address as can happen with PCs, and so are more difficult to infiltrate. Modern technologies including derived credentials, behavioral analytics, and containerization also provide added layers of security that PCs do not offer.

If your mobile devices could talk, what secrets would they tell? Advances in mobile security, properly configured, can ensure that what happens on your phone, stays on your phone—for your eyes only.

This article was produced by fedscoop | cyberscoop for, and sponsored by, SAMSUNG.