InZero Technologies

Patented WorkPlay Technology™

What happens in one OS stays in that OS

1. IN A NUTSHELL

The WorkPlay Technology was specifically created to overcome a fundamental architectural vulnerability of mobile devices: shared device resources. Existing methods to protect data through various data access separation methods – user permissions, containers, passwords, encryption, etc. – share the same system resources (a single kernel, RAM, drivers, storage). This makes the device susceptible to malware that can achieve "Escalation-of-Privileges" ("EoP") to obtain the credentials to access all device data, including network access rights.

We attacked this problem at its core, by using ARM TrustZone Secure World to create multiple (2 or 3) operating systems ("OS's"), each **complete** with its own full set of resources, and **inaccessible** by another OS, meaning any malware in one OS **cannot** access another OS.

This critical separation of multiple, complete OS's does not hinder device use. Each OS operates normally, and the user switches between OS's in a few seconds, picking up where it left off.

The WorkPlay eliminates the need to purchase multiple devices, and makes IT admin management considerably easier, since it eliminates any need to manage the user's personal apps.

In this way, WorkPlay TrustZone offers Security, Simplicity and Savings.

2. WHY WE CREATED WORKPLAY

The Quintessential Attack – It Only Takes One

One clever phishing attack, luring unwitting employees.

In the OPM's case, the attackers used fake OPM domains to convince victims to give up passwords. Not only did the $5B "Einstein System" fail to thwart it, a breach was only discovered **after** a second successful attack.

There was more. A few months later, the stolen data was used to breach the DoD.

> ***"The most unnerving part of the current state of government it security is that there's no way to know the extent of breaches."*** *(arstechnica.com, June 2015)*

The OPM attack should have come as no surprise, just another in a series of massive similar attacks going back a decade, against Government agencies and large enterprises. It's not getting better. After the much publicized TJMaxx breach back in 2007, we've seen much worse in recent years in US agencies and huge companies like Home Depot, Target, Anthem, JPMorgan, SONY and others.

Did we mention attacks stealing government data for years before detection? "Cleaver" and "APT 28/Pawn Storm" are two examples. The original OPM attack apparently started in 2014.

With all the emphasis on cyber security and constant introduction of newer and newer products. . .

3. HOW CAN THIS BE?

For several years now, well-known vendors have promoted endpoint security that safeguards organizational networks no matter what the user is doing. Powerful, impressive convincing and comforting product names are used–"KNOX", "IronKey", "TrustWave" –to suggest that sensitive data was well-isolated and protected against user activity that might run into a malware exploit.

100 Carpenter Dr.
Sterling, Virginia 20164

The beat goes on. New and improved solutions are constantly announced. Legacy vendors even team up to promote their combined effectiveness, like *"BlackBerry and Samsung Partner to Provide End-To-End Security for Android" (BB release Nov. 13, 2014).*

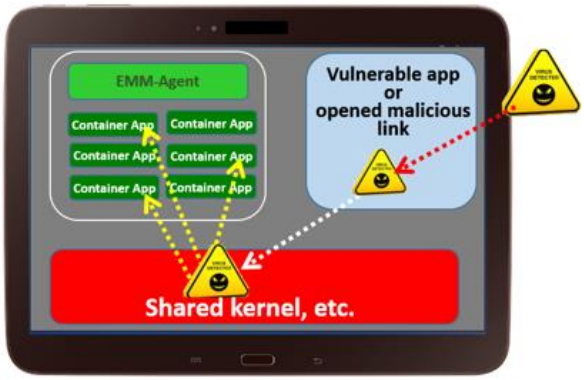
Yet this past summer, researchers published a scathing critique of the Samsung KNOX product, detailing how the latest iteration (v. 4.3) was no more secure than the original (v. 1.0), marketed with much fanfare over three years ago. *(http://www.zdnet.com/article/israeli-researchers-poke-holes-in-samsung-knox-security-system/)*

Meanwhile, despite increasing cost and complexity for more and more layers of products, **the most basic risk of breach remains:** Malware can still reach the user's privileges–taking over the user's endpoint device to access sensitive network data.

This is because, as the KNOX researchers reminded, so long as the kernel and other system resources are shared, they are accessible by malware that can find and use the privileges:

> *"if you can subvert the kernel . . . you have achieved the ultimate elevation of privilege (EoP) exploit." (March 24, 2016 sophos.com report on Android CVE-2015-1805 flaw.)*

And sometimes, in a clever and convincing phishing attack, it's even easier because the user unwittingly gives them up. Like we said, ask the OPM.



4. THINK THIS KIND OF ATTACK IS NOW A THING OF THE PAST?

The breach of the Democratic National Committee was more of the same. Once again, a phishing attack. No surprise. There is no reason for cybercriminals to stop these attacks. The Dark Web reports that the value of a health care record is $25 each. Think of that when a breach is reported of just a few thousand victims, much less the enormous theft of a well-known breach like Anthem Insurance (over 70 million records.)

And the constant use of growing social media apps only heightens the risk. Since 2015, cyber-attacks were launched against Anthem, DHS, OPM, FBI, White House, SONY.

5. HACKERS ATTACK THE FLAW TO GAIN NETWORK ACCESS. WE ATTACKED THE FLAW TO ELIMINATE IT. HERE'S HOW.

Standard dual persona configurations, like containerization, include an architectural weakness of sharing resources that creates escalated privileges risk.

In addition, this structure is, of course, especially vulnerable to the clever phishing exploit that lures the user into giving up authentication credentials to access the organization network.

Our solution: WorkPlay eliminates the inherent flaw, and does so in very small code, readily verifiable.

100 Carpenter Dr.
Sterling, Virginia 20164
www.inzerosystems.com

Here's how:

(1) WorkPlay creates Hardware-enforced separation of Operating Systems, one OS being active at a time.

(2) These OS's are created so that:

- one OS cannot access another
- so malware in one cannot access another - regardless of gaining escalated privileges in one OS
- so even if a user unwittingly gives up passwords in one OS, an intruder cannot access the network access keys stored in another OS.

(3) Switching between OS's, by simple user action like pressing the switch icon or other desired method, takes a few seconds.

(4) On switching, the inactive OS resumes where it left off.

(5) Each OS operates normally, as if it were the only OS in a device, including allowable typical apps and security, with IT admin control through MDM/EMM.

(6) WorkPlay requires only ARM TrustZone, and adequate storage for intended use.

At bottom, WorkPlay does at the hardware-level what cannot be done at the software level.

6. WE DON'T DECIDE USE CASES

WorkPlay was so named for the most obvious use case: one OS for work, a truly separate OS for personal use – a scenario still much needed for BYOD or for organizational use where business data requires high-level isolation, like government, healthcare, finance, etc.

But WorkPlay is use-case agnostic.

Please visit our website for examples of many, common-sense, use-case scenarios. WorkPlay can be used for any purpose where genuine domain separation is necessary or helpful.

InZero Technologies, LLC

100 Carpenter Dr.
Sterling, Virginia 20164
www.inzerosystems.com