From the Magazine: The Fine Art of Mobile Security in a Dangerous Age

Andrew Berg

If you haven't heard, digital security is a big deal, and the security of information on mobile devices is of utmost concern. The bad guys are getting smarter, their attacks more complex and the sensitive data they're after increasingly resides on that miniature computer you have in your pocket.

Shlomo Kramer is the co-founder, president and CEO of digital security firm Imperva. He's also the seed investor for a company called WatchDox, which specializes in document storage and encryption.

Kramer says the security landscape continues to change along with the devices we use and the kinds of threats faced by IT departments and end users alike.

"Mobile malware is much more dangerous than malware on your PC or Mac," Kramer says. "Simply because, [the mobile] is a much more personal device. The malware can record the physical conversation in the room. It can report on your physical location at any point in time. It has access to any payment transaction you might do on the mobile device."

That said, Kramer believes the industry has moved to the second phase in mobile security. The first, he says, was figuring out how to manage the device. He explains that now that we have the devices locked down, the applications and documents need to be secured as well.

"Mobile application and data security are in with the early adopters who are wrapping their arms around these challenges," Kramer said, adding that as usual security lags behind the threat.

Kramer says that the recent leaks about the NSA's surveillance program have taken the message about security to a broader audience. He says the same thing happened a few years ago on the PC side of things.

"An example would be the disclosure laws of seven or eight years ago, where you started seeing companies that had to disclose when they'd been breached," Kramer says. "Quite frankly they'd been breached before, but these headlines started to alert a broader audience to the fact that these things happened. And that by itself

had a significant influence on the security market.”

Securing Documents

One of those companies that is wrapping its arms around document security, is the previously mentioned WatchDox, in which Kramer has an interest.

Ryan Kalember, chief product officer for WatchDox, says his company believes that sensitive data needs to carry protections with it wherever it goes. With that philosophy, Watchdox targets large enterprises, servicing around 100 of the Fortune 1000 companies.

From an end-user perspective, WatchDox does loos very much like a Box or a Dropbox, but Kalember says his company differentiates by what it does with the information stored on the platform.

“The piece of content gets a couple of things,” Kalember explains. “It gets encryption everywhere it goes, not only in transit from point a to point b, but also when it’s in use, open in Microsoft Word being edited or for example open within a mobile app.”

Part of the premise of WatchDox’s business is that networks and applications will always be hackable, which makes the protection of sensitive information through unique encryption of the utmost importance.

Kalember said the recent leaks by Edward Snowden and the subsequent fallout were actually very useful for WatchDox.

“You have fairly large providers in our space, like Box—their general counsel last week said we’ve gotten [FISA] requests but not an overwhelming amount. That should be terrifying for anybody who’s a Box customer that doesn’t want their data ending up in the hands of the government,” Kalember says.

Kalember says that the folly of other providers—Dropbox, Box, SkyDrive—is that they all encrypt with the same key, which means that when the government comes a knocking those companies have set up a way to decrypt that data and turn it over upon request. The most recent Snowden revelation may have proven that the government doesn’t even need any help from those companies to decrypt that information.

"The latest revelations about encryption and mobile devices are an excellent reminder of why the basic security most technology providers offer is not enough for the data you really care about,” Kalember says. “Using strong encryption at the file level and controlling your own encryption keys is still the best way to keep your

information safe, from the NSA or anyone else for that matter."

Watchdox makes about 80 percent of its revenue from on-premise data, which Kalember says puts the control of a company's data in its own hands, as opposed to a cloud provider, where the owner of the information may not even know that a request has been made on that data.

The Snowden leaks have been so effective in raising consciousness around security and privacy that even the government itself has perked up its ears and reached out to WatchDox.

"Since the Snowden leaks, we've gotten our first two public agencies as customers," Kalember said, adding that the company couldn't publically name them just yet.

As an example of the consequences of not protecting and encrypting data, Kalember points to the case of Dr. Hong Meng, a DuPont chemist who was jailed for fourteen months after he allegedly emailed himself a Word document, which contained a breakthrough process on the development of Organic Light-Emitting Diode (OLED) technology.

"Dupont valued that document at $400 million," Kalember said. "They caught him, but they lost the IP."

Bottom line for Kalember is that the security paradigm built around protecting the network is quickly collapsing. He uses the analogy of Indian Jones to describe the shift towards data protection.

"You have to make it through all these tasks. It's tough to get it. It's tough to craft a phishing email of this one executive who you know has this particular document. But when they're actually going to get the thing that really matters, when they finally get to the holy grail of data, it doesn't set a boulder coming after them, it's just sitting there, because it's just a file. Some of the highest profile breaches have been just like that."

The Network and the Internet of Things

On the opposite side of the coin from Kalember is Vann Abernathy, senior product manager for a company called NSFOCUS, which is aims to defend the network at the perimeter, but also identify malware and other things that compromise systems and networks.

"Remembered when everyone shifted to the PC?" Abernathy asks. "It was a revolution. Everything in the office changed when we shifted to PCs. That same kind

of revolution is happening now as we shift to mobile devices."

Abernathy says that as more and more of the daily workflow shifts to the tablet and the smartphone, the risk of serious security breaches vastly increases.

"All of the big banks now have some flavor of mobile banking. So even in your personal life you're starting to adopt workflows that use your smart device," he says.

Abernathy says that the fundamentals of security haven't changed. The same principles that apply to safeguarding a PC need to be applied to those using a smartphone.

In the past, Abernathy has written about the possibility of using smartphones as bots for a Denial of Service (DoS) attack, a scenario he says is presently unlikely. Still, he notes that one of Anonymous' favorite programs—Low Orbit Ion Canon—for launching DoS attacks is now available through the Google Play store.

"It's right there in Google Play, and they've actually embedded it in other programs," Abernathy says.

Abernathy may not be far off with this scenario. According to McAfee's 2013 Threats Report, "once criminals discover a profit-making technique that works, they're likely to reuse and automate it."

For example, McAfee's report notes Android/Marketpay.A is a Trojan horse program that buys apps from an app store without user permission. We're likely to see crooks take this malware's app-buying payload and add it to a mobile worm.

Abernathy thinks that one of the biggest challenges facing mobile security is the end user's generally lax attitudes towards the problem. Abernathy relates a recent trip to a conference where he was speaking and he asked for a show of hands from those who had some form of security software on their phones. He didn't get many hands.

"You wouldn't dream of owning a PC without anti-virus, but when you're on a smartphone? The problem is we don't know what we don't know," Abernathy says. "Once the criminals figure out how to monetize breaking into the phones, then it's going to be the wild, wild West. Then it's on."

In the end, however, what keeps Abernathy up at night are the unmanned devices connecting to the network, whether that be a freight tracking module or a GPS system in an in-dash system.

“The whole thing with mobile devices and the Internet of Things, I think we're creating so many additional endpoints, and we're bringing so many different devices into both corporate workflow and normal everyday human interaction workflow that the vectors for attack are growing exponentially,” Abernathy says. “And I don't think any of us truly have a handle on how to stop it except for doing things like installing Web application firewalls.”

Applications

MobileIron is one of the major names in mobile device management and it recently put out its latest iteration of its Anyware platform, which brings together MDM, and application and document security into a single, cloud-based platform

Ojas Rege, vice president of strategy for MobileIron, says the goal of Anyware is to ensure that any business can go mobile securely and in a timely manner.

"The beautiful thing about Anyware, is that it takes less than a minute for a user to be fully configured and have access to all their applications and content,” says Rege.

The system allows users a consumer-friendly App Store-like experience. Administrators can approve a catalog of apps to Anyware’s enterprise applications store allows IT departments to get the right mobile apps to the right employees through a private app catalog customized by a group or user. The same can be done for pieces of content, such as documents, images and presentations.

Administrators can block untrusted devices and wipe business apps when required, which Rege says can offer the advantage of ensuring privacy and security simultaneously Rege says management of content across an organization can be tricky, as the IT administrator is rarely the one creating the content. With Anyware, MobileIron has tried to give the administrator granular controls of distributing and sharing content amongst many users. .

“So I can say, this person can publish content to these sets of users. Or this person can actually set administrative policies across all of these users,” Rege explains.

MobileIron’s is just one example of an approach to mobile security that builds off management of the device and expands to secure both documents and applications.

New Threats

Regardless of which angle a company takes on mobile security, the key appears to be vigilance. The bad guys will continue to come up with novel ways to compromise

data, as well as networks. The McAfee report referenced earlier reads like a horror story, wherein our most private data and sensitive information is compromised through some of the latest and most highly-anticipated technologies out there.

Take NFC for instance. Sure, it could prove to be a slick way of connecting to your car stereo or paying for that candy bar, but could it also be the perfect opening for a digital pickpocket?

McAfee argues that attackers will create mobile worms with NFC capabilities to propagate (via the “bump and infect” method) and to steal money. “Malware writers will thrive in areas with dense populations (airports, malls, theme parks, etc.). An NFC-enabled worm could run rampant through a large crowd, infecting victims and potentially stealing from their [mobile] wallet accounts,” the report states.

Such is the material for an IT administrator’s nightmare. And yes, it may sound a bit cloak-and-dagger, if not straight out of a Philip K. Dick novel. But the threats are as undeniable as this industry’s innovative approaches to thwarting them.