Cutter IT Journal

The Journal of Information Technology Management

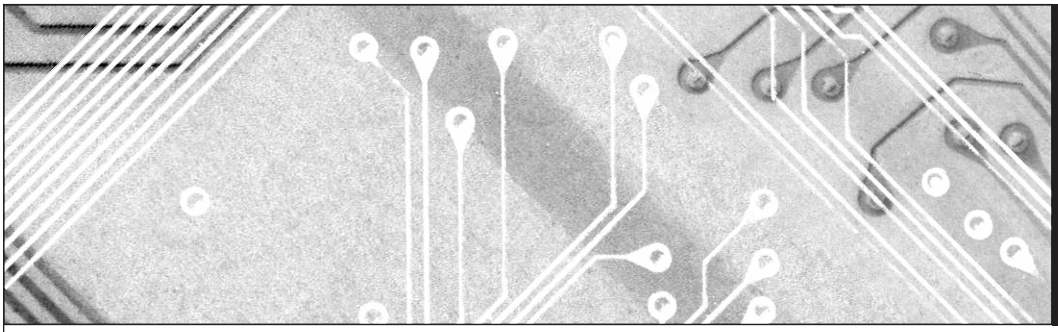
Vol. 27, No. 12
December 2014

"Every innovative service created and offered to the marketplace of individuals and businesses creates another vector for an attack that compromises the infrastructure that provides the service."

— Sebastian Hassinger, Guest Editor

Mobile Security:
Managing the Madness

CUTTER CONSORTIUM



Cutter IT Journal

About Cutter IT Journal

Part of Cutter Consortium's mission is to foster debate and dialogue on the business technology issues challenging enterprises today, helping organizations leverage IT for competitive advantage and business success. Cutter's philosophy is that most of the issues that managers face are complex enough to merit examination that goes beyond simple pronouncements. Founded in 1987 as *American Programmer* by Ed Yourdon, *Cutter IT Journal* is one of Cutter's key venues for debate.

The monthly *Cutter IT Journal* and its companion *Cutter IT Advisor* offer a variety of perspectives on the issues you're dealing with today. Armed with opinion, data, and advice, you'll be able to make the best decisions, employ the best practices, and choose the right strategies for your organization.

Unlike academic journals, *Cutter IT Journal* doesn't water down or delay its coverage of timely issues with lengthy peer reviews. Each month, our expert Guest Editor delivers articles by internationally known IT practitioners that include case studies, research findings, and experience-based opinion on the IT topics enterprises face today — not issues you were dealing with six months ago, or those that are so esoteric you might not ever need to learn from others' experiences. No other journal brings together so many cutting-edge thinkers or lets them speak so bluntly.

Cutter IT Journal subscribers consider the *Journal* a "consultancy in print" and liken each month's issue to the impassioned debates they participate in at the end of a day at a conference.

Every facet of IT — application integration, security, portfolio management, and testing, to name a few — plays a role in the success or failure of your organization's IT efforts. Only *Cutter IT Journal* and *Cutter IT Advisor* deliver a comprehensive treatment of these critical issues and help you make informed decisions about the strategies that can improve IT's performance.

Cutter IT Journal is unique in that it is written by IT professionals — people like you who face the same challenges and are under the same pressures to get the job done. *Cutter IT Journal* brings you frank, honest accounts of what works, what doesn't, and why.

Put your IT concerns in a business context. Discover the best ways to pitch new ideas to executive management. Ensure the success of your IT organization in an economy that encourages outsourcing and intense international competition. Avoid the common pitfalls and work smarter while under tighter constraints. You'll learn how to do all this and more when you subscribe to *Cutter IT Journal*.

Cutter IT Journal®

Cutter Business Technology Council: Rob Austin, Ron Blitstein, Tom DeMarco, Lynne Ellyn, Israel Gat, Vince Kellen, Tim Lister, Lou Mazzucchelli, Ken Orr, and Robert D. Scott

Editor Emeritus: Ed Yourdon
Publisher: Karen Fine Coburn
Group Publisher: Chris Generali
Managing Editor: Karen Pasley
Production Editor: Linda M. Dias
Client Services: service@cutter.com

Cutter IT Journal® is published 12 times a year by Cutter Information LLC, 37 Broadway, Suite 1, Arlington, MA 02474-5552, USA (Tel: +1 781 648 8700; Fax: +1 781 648 8707; Email: citjeditorial@cutter.com; Website: www.cutter.com; Twitter: @cuttertweets; Facebook: Cutter Consortium). Print ISSN: 1522-7383; online/electronic ISSN: 1554-5946.

Subscription rates are US $485 a year in North America, US $585 elsewhere, payable to Cutter Information LLC. Reprints, bulk purchases, past issues, and multiple subscription and site license rates are available on request.

Opening Statement

by Sebastian Hassinger, Guest Editor

Security in the IT realm is a very complex issue to deal with, largely because the very attributes that create vulnerabilities are the main creators of value for individual users, businesses, and society itself. Just as the value of a network increases as the square of the number of nodes on that network, so too does the probability of a bad actor exploiting the network to his or her own ends. Every innovative service created and offered to the marketplace of individuals and businesses creates another vector for an attack that compromises the infrastructure that provides the service.

Hardware advances also increase security risks. If computing power doubles every 18 months, the threats to trusted encryption technologies increase accordingly. The cheaper digital storage becomes, the more of our sensitive data we store, to mitigate the risk of loss through technology failure by having copies of our most valuable data on our own drives and in the cloud. These giant aggregations of financial and personal data create mouth-watering targets for those inclined to unethical and criminal behavior.

Declining prices of computing power, storage, and network traffic have put immense power in the hands of more people than ever before. A tiny startup can compete with a giant conglomerate, and a pupil in the developing world can access the same educational resources online as one in the developed world; but so too can a teenager with too much time on his or her hands and an unformed moral compass wreak as much havoc on a global enterprise as a state-funded "cyber warrior" attacking the military infrastructure of an enemy nation.

The complication comes not from recognizing those risks but in trying to mitigate them. In a classic case of "throwing the baby out with the bath water," any blunt force solution to the problems described above also jeopardizes the enormous value created on the other side of the equation. Constraining access to a network both creates a dichotomy of "haves" and "have nots" and diminishes the potential value of that network. Limiting the services allowed on the nodes of a network similarly reduces potential innovative value creation.

This was the situation at the beginning of our transition into the current mobile age — Internet-connected personal computers and servers vulnerable to all manner of exploits with some Band-Aid solutions available, each posing significant tradeoffs with regard to usefulness and value creation. If you locked down your corporate network to the maximum level of security, you would effectively isolate yourself from the world and doom your business to a slower rate of growth than your less safe peers in the market. However, most IT departments struck a workable balance, allowing email and Web traffic, sniffing at packets and ports, scanning for viruses, encrypting data, monitoring logs for breaches, and enforcing adequate levels of authentication for access to services.

Just as the value of a network increases as the square of the number of nodes on that network, so too does the probability of a bad actor exploiting the network to his or her own ends.

And then mobile happened. Long predicted, the mobile revolution still took the community of IT professionals off guard. Initially, it seemed that the mobile computing market was limited in scope — the Windows CE, Palm OS, Symbian, and even BlackBerry OS devices too expensive and unwieldy to appeal to more than a minority of users. Then the iPhone happened, striking a remarkable balance between Apple user friendliness and carrier-subsidized price point, and the era of the smartphone began. In the span of seven years, mobile has arrived with unprecedented velocity. As one article in this issue notes, there is now a smartphone for one out of every five individuals currently alive on earth.

This astonishing adoption curve has yet to reveal its ultimate ramifications for human society and the global economy, but at this stage, one implication is very obvious — the teetering balance struck by enterprise IT in the networked PC era is not working anymore. In fact,

we seem to have been thrown into a state of extreme volatility.

The networked PC-era balance of access to services and data against securing the same assets seems to drive mobile users away in droves. Ranjeet Vidwans, author of our first article, picks up on market data that 61% of enterprises have deployed three mobile apps or fewer, and 60% of enterprise users have stopped using mobile computing at work completely. In his article, Vidwans explores the reasons behind this dynamic and finds that the freedom of using one's own personal mobile "anywhere" device has raised the bar substantially for the enterprise. Poor capacity planning that causes performance issues and traditionally conservative security measures that create friction for the user with just a few minutes to spare — a "niche" work opportunity, as Vidwans calls it — exists in stark contrast to the ease of use of all the personal services that exist on the phone.

His exploration extends beyond outlining the root causes of poor adoption to offering a methodical approach to turning the tide in the enterprise's favor. On the security front, Vidwans identifies the top priorities for security efforts as a way to focus restrictions into the highest-impact areas. In this way, IT departments can put the minimum amount of obstacles in users' way for the greatest security benefit. In terms of scale, he provides a valuable guide to understanding the infrastructure required to provide adequate performance for your mobile apps. He offers very valuable advice regarding what he calls "visibility" as well — increasing your understanding of who is using your mobile apps and in what ways, and what you can do with that data to create a positive feedback loop for adoption.

All these efforts will be of little use, however, without a focus on the core attribute that has driven the startling adoption of mobile computing in the first place: user experience. Apple's success with the iPhone wasn't dependent on raw computing power or any particular technical innovation — mostly Apple assembled the hardware and software that existed in the market but with a hugely improved user experience. Indeed, the iPhone user experience was so much better than what people were used to that it propelled the phrase "user experience" into general parlance. Vidwans's core point is that enterprise IT departments need to take that lesson to heart and place far greater emphasis on the overall experience of their users when it comes to mobile. If they don't, users will do as the mobile do — move away.

The paucity of mobile adoption in enterprises should be deeply troubling to the senior management of these firms as it isolates them from a key driver of value creation and productivity. If they do solve that part of the equation by "loosening up" the corporate security grip over the user's experience, though, the balance will tend to swing too far in the other direction. Here again, the best practices of the PC era will not serve the IT department well.

In our next article, Andrew Hoog takes a look at the IT department's natural instinct to focus on the threat of malware. One might think that, as a key threat in the PC era, malware represents the main vulnerability in the mobile space. However, Hoog identifies a much more dangerous attack vector, one that is intimately tied to the personal freedom that attracts users to mobile: apps. Mobile apps are the user's means of customizing his or her mobile toolbox, adding just the features and attributes desired in the palm of a hand when and where they are needed. The attraction of mobile apps has created a mighty software economy, with Apple's and Google's marketplaces containing over 1.2 million apps each.

With that proliferation, Hoog says, it is not necessary for the criminal element to find ways to surreptitiously hitch a ride on a legitimate application, system component, or Web page. Merely build a game, utility, or other app and put it in the way of the user. Once installed and given permissions to the resources on the phone, a "leaky" app with ulterior motives is free to take advantage of the relatively unsophisticated security model of mobile OSes and the naive trust of the user who doesn't suspect his or her digital, mobile familiar has been possessed by those who seek to do harm.

UPCOMING TOPICS IN CUTTER IT JOURNAL

JANUARY

Bob Benson and Piet Ribbers

Improving Trust and Partnership Between Business and IT

FEBRUARY

Balaji Prasad

People Architecture Defines Enterprise Architecture

There are enterprise solutions, Hoog notes, that take a "containerization" approach — seeking to create a lockbox of sorts on the device where enterprise data can remain unmolested. Like Vidwans, he also finds the benefits outweighed by the cumbersome nature of the technology. Instead, Hoog's solution is an holistic approach to security based on some very pragmatic insights and a reliance on policies and education. Recognizing that this is an interim step, the article concludes with an exploration of an innovative approach that seeks to create an algorithmic representation of the holistic policies, resulting in a quantitative measure of "secureness" that can be used to gauge actual risk levels and modify exposure accordingly.

Zeroing in on the massive throngs of apps noted by Hoog, the authors of our next article, Naser Mohamed Al Ali, Dima Alhadidi, and Zakaria Maamar, take a closer look at ways to evaluate the trustworthiness of apps before installing them on a device. Interestingly, they find that a linguistic analysis of the licensing terms provides valuable metadata that can be used to gauge the risk associated with a particular app. Their analytical approach combines manual and programmatic data collection on two axes: horizontal and vertical. Horizontally, they examine the same app across multiple platforms, and vertically, they test a group of apps from the same category, messaging, on a single platform.

The results are intriguing, especially when cross-referenced with the resource access each app requests upon installation. The article suggests a promising new approach to security. Instead of focusing on the parasitic entities known as malware — which, as Hoog points out, are not the greatest danger in the mobile ecosystem — we may see emerging methods of preemptively scoring the level of risk represented by individual, seemingly legitimate apps.

Even with greater guidance regarding the trustworthiness of individual apps, however, the risk still hinges on the actions of individual mobile users. For Anjali Kaushik, author of "Mobile Security from a Practical Perspective," this is of critical importance. If the mobile revolution was sparked by the allure of greater individual freedom of movement, timing, feature customization, and usage in general, that freedom can't be curbed without reducing the value of mobile itself. Therefore, Kaushik highlights not just the technologies that can improve mobile security and privacy, but also the user behaviors that need to be modified or eliminated to effect real change.

According to Kaushik, it is necessary for technology providers and IT departments to deploy strong authentication and robust encryption and all the rest of the infrastructure of security, but it is not sufficient. All it takes is one user to install one app with a hidden agenda and then to use that app inside the corporate firewall, or one user to run the corporate mobile app on a bogus Wi-Fi hotspot that is running deep packet inspection and a man-in-the-middle attack. In other words, the corporate user is no longer inside the glass house where the IT department wields control. The paternalistic approach of attempting to restrict new freedoms merely drives the users further away. The risks to security worsen.

However, in the midst of this grim landscape, we see hope. The new mobile freedom is germinating a sense of self-reliance in users. Recent controversies such as high-profile privacy leaks of celebrities' photos and similar stories have gained enormous coverage in the press and loom large in mobile users' minds. They see themselves at risk, personally. This is an opportunity for tutelage that users' employers should seize. Better digital hygiene can reduce risks and let a user rest easier. And it can provide IT security directors with a glimmer of light at the end of a very dark tunnel.

Sebastian Hassinger is a Senior Consultant with Cutter Consortium's Agile Product & Project Management *practice. He has worked in the IT industry for over 25 years both in large corporations and as an entrepreneur and has provided product strategic consulting for large and small firms alike. Mr. Hassinger founded two ISPs; helped launch several startups, including a Vietnam-based Agile development shop specializing in Web and mobile applications; and held senior product strategy and business development roles with IBM, Oracle, and Apple. He currently serves as COO for Brewbot, a startup building a beer-brewing appliance. Mr. Hassinger holds MBAs from Columbia University and London Business School, is a published author, and holds over a dozen software and business model patents. He can be reached at shassinger@cutter.com.*

Driving Enterprise Mobile App Usage:
Moving from Stuck to Secure, Scalable, Usable — and Productive

by Ranjeet Vidwans

So you've deployed mobile email and calendar apps to your users. But you haven't yet achieved the vision of an über-mobilized workforce working anytime, anywhere, at the speed of business? Take comfort — few organizations have. They're running into the new security, scalability, visibility, and user experience (UX) challenges that are inherent to mobile devices and work styles. Understanding these challenges and applying the best practices I suggest here can get your enterprise on the road to full mobile productivity.

WHERE THINGS STAND

The actual state of enterprise mobility is far behind the promise. A May 2014 IDC report[1] found that 61% of the *Fortune* 500 have deployed only three mobile applications to their users. A recent Mobiquity-commissioned consumer survey[2] found that nearly 60% of employees stopped using their enterprise mobile apps and reverted to waiting until they were back at their desks to perform particular business functions. Ouch. What's worse, among users who continued using their enterprise mobile apps, 26% of smartphone users and 19% of tablet users said that they actually became *less* productive.[3]

What's going on? In a nutshell, users are not adopting mobile enterprise apps. Without user adoption, the entire enterprise mobility business case falls apart. Bear in mind that this already assumes that the apps organizations are trying to deploy are rich, attractive, and usable. After all, these would normally be the same apps that an employee would use at a desk in the office. So the reasons behind low adoption rates must stem from other factors.

THE FOUR CHALLENGES IMPEDING ENTERPRISE MOBILITY

Experience with large enterprise customers indicates that four challenges commonly hamstring enterprise mobility initiatives. Failing to address these challenges creates a situation in which you will be hard-pressed to deploy any mobile apps. And addressing them ineffectively ensures that any apps that you do deploy will quickly be relegated to the mobile dustbin.

The four challenges are:

1. **Security.** Security has traditionally been the primary showstopper for mobile enterprise app deployment. Many IT organizations already are burdened with escalating malware, data leakage, and other cyber threats. The thought of extending sensitive enterprise apps and data to mobile users and devices that they do not control has prevented many businesses from deploying mobile enterprise apps.
2. **Scale.** Mobile apps have a high impact on the network; usage patterns require that VPN connections be established and torn down rapidly.
3. **Visibility.** App owners don't know if or how their apps are being used. Actual usage data is scarce or buried.
4. **User experience.** Mobile users work in "niche time" — a few minutes here, a few seconds there. Most enterprise mobile apps have burdensome enrollment and authentication processes that are required to secure sensitive enterprise data but frustrate and discourage users.

Understanding and overcoming these four challenges will optimize your chances of executing a high-value mobility rollout. So let's look at the solutions available to remove these obstacles to your enterprise mobility strategy.

Security: The Supreme Balancing Act

There has always been tension between security and user adoption. The more tightly an organization tries to protect its digital assets, the more difficult it becomes for legitimate users to access and use them. Historically, organizations have been able to mandate the requisite level of security because end users had no choice but to go along with whatever was required. Mobility alters this dynamic.

Mobility requires a higher level of security than traditional endpoints such as desktops and laptops. Mobile devices are more likely to be lost or stolen. At the same time, users commonly use both personal apps and work apps on their mobile devices. Personal and corporate apps residing on the same device increases the risk of a rogue app running on an employee-owned device with corporate access.

There are a number of ways in which an organization can make sure that its mobile apps are delivered in a tight security envelope that minimizes the risk of security incidents, such as data loss, data leakage, and inappropriate access to sensitive systems:

1. **Use strong multifactor authentication** to identify your users. To truly unlock business value from mobility, you need to mobilize high-value business workflows. Instead of thinking about mobile email, think about a senior VP approving a multimillion-dollar purchase order. To securely mobilize business transactions, make sure that users are authenticated with multiple factors such as digital certificates, tokens, or biometrics.
2. **Protect your data at rest** to make sure that applications are secure even if a device is lost or compromised. The vast majority of users use their mobile devices primarily for personal and recreational apps. This fact dramatically increases the risk of an untrustworthy app being colocated with your sensitive apps and data. Assume from the start that the device is compromised, and make sure that your data is secured as strongly as possible. This means making your apps the control point of your security strategy by making them "self-defending," instead of relying solely on your enterprise mobility management (EMM) or mobile device management (MDM) infrastructure.
3. **Use per-app VPN connections** to connect to your network. This is the best way to ensure that only *your* apps are connecting to *your* network. It helps eliminate the risk of user error or malfeasance by a rogue app that could potentially compromise anything on the device. It also limits exposure at the app level. If an app is compromised for any reason, you can shut it down quickly, with total confidence that your other app connections have not been put at risk.
4. **Use a hardened appliance** to terminate mobile VPN connections. A hardware appliance is a physically secured environment for processing high-security transactions. This is a key requirement if your organization is subject to regulatory compliance requirements such as PCI, HIPAA, or SOX. In particular, ensure that your mobile VPN gateway has been through rigorous security validation and certification, such as FIPS 140-2 certification, so that you can demonstrate compliance.
5. **Enforce rich security policies** to protect your infrastructure. There are many types of policies that most commercial and government organizations require to protect themselves adequately. Here are a few to keep in mind:
   - *Implement jailbreak/rooting[4] detection* to enforce additional controls that define how compromised devices are (or are not) allowed to access your network.
   - *Enforce app expiration* so that certain apps are issued only on a temporary basis and are deleted, along with their data, when the validity period has passed.
   - *Institute email enforcement policies* that require secure data to go through your authorized mobile email client for the purposes of audit and data leakage protection.

Scale: Think an Order of Magnitude Higher

While the concept of mobile scale has been discussed for years, connected enterprise mobile apps take the concept to a new level.

First, there's the issue of mobile sizing. Mobile apps connect to your network through your existing VPN infrastructure or through a dedicated mobile VPN (mVPN) gateway. Most organizations "right-size" their VPN infrastructures for traditional devices based on calculations such as these:

- I have 10,000 employees/users.
- Only 35% of them will ever be remote (3,500 connections).
- Only 30% of those users will connect simultaneously (~1,000 connections).
- To be safe, I'll double that number (2,000 connections).

Using this approach, the VPN infrastructure is sized for a number of concurrent connections corresponding to a fraction of the overall user population. However, mobile enterprise apps operate according to completely different calculations:

- I have 10,000 employees/users.
- 100% of them will be mobile. In fact, some of them may even use my mobile apps while in the office (10,000 connections).

- Each device has, on average, 2.5 apps that may be in use simultaneously over a per-app VPN (25,000 connections).
- Peak loads can be higher, and each user might have multiple devices.

In the mobile world, scale has to be expressed as a significant multiple of overall user population.

The second factor that increases mobile scale estimates is connection churn. Mobile VPN usage patterns are different from traditional laptop VPN patterns; they require connections to be established and torn down rapidly.

For example, during a short break to go out for a cup of coffee, a user may access the same application several times to check the status of a pending purchase order. During this time, he may start on the office Wi-Fi network, transition to a 4G network, move to the coffee shop's Wi-Fi network, and then go back to the 4G network. Each of these transitions will cause the VPN connection to drop and rapidly reconnect.

Another driver for connection churn is idle timeout. In a traditional scenario, an employee may step away from her desk for 15 minutes but then come back and work. In a mobile scenario, if the employee hasn't touched an app in 5 or 10 minutes, she's likely off doing something else and won't be back for some time. That connection should be dropped quickly.

Examples like these demonstrate the need for an extremely scalable infrastructure that can rapidly establish secure connections and dispose of them at high levels of churn.

Handling this level of connection volume and churn effectively requires a hardware appliance. Such an appliance can deliver the rapid connections, optimized throughput, and cryptographic acceleration needed to support mobile scalability.

Visibility: Using Analytics to Improve Mobility Insight

Part of the reason that connected enterprise mobile apps are not yet broadly adopted is because application owners don't know if or how their apps are being used. An enterprise app store can provide data about the number of downloads for a particular app. However, actual app usage data is scarce and is usually buried in uncategorized HTTP and HTTPS traffic.

As you plan your mobile strategy, incorporate mobile analytics. Be sure that, at a minimum, you can obtain the following types of data from every mobile app you deploy:

- User
- Location
- Device type
- App
- Device posture (jailbroken, managed vs. unmanaged, etc.)

Having this data will help you improve the security posture of your organization and plan for future mobile investments. It will also enable you to:

1. **Implement richer security controls.** Mobile analytics data empowers you to incorporate mobility and location attributes into your preventive and detective security policies. For example, you may allow a purchasing manager to approve a purchase order from his mobile device, but not if he's doing so from a remote location while simultaneously logged in at his desk. Or you may allow certain apps to be accessed only by managed devices that are under the control of your EMM or MDM infrastructure.
2. **Build better mobile apps.** Mobile analytics data provides deeper insight into which mobile apps are being used most widely, by which types of users, and in which scenarios, enabling you to assess more accurately which apps are driving value for your organization. You can then retire apps that are not being adopted and "double down" on the types of apps that truly help move the business forward.
3. **Implement chargeback models.** Another business benefit of app and user insight is that you can monitor how mobile employees use your mobile infrastructure. With this data, you can demonstrate the value of your mobile investments and set up interdepartmental chargebacks to share the cost of mobility among those groups that use mobility the most.

User Experience: If You Do Nothing Else …

Security, scale, and visibility are critical, but your efforts will be in vain if you don't deliver a superior user experience. I've already assumed that you're building fabulous apps. Now I'm talking about how users securely access and use those apps.

Unlike a mandated application on a laptop or desktop, a user can simply choose to not use a mobile app. This is what leads to high rates of mobile app abandonment. Most enterprise mobile apps today require an onerous enrollment process and a cumbersome authentication experience that demands constant reauthentication. Users — understandably — become frustrated and find it easier to do tasks back at the office. Part of this

frustration derives from the different way in which employees work when they are mobile as opposed to when they are at a desk.

NTT DoCoMo first used the phrase "niche time" to describe how mobile users interact with their devices and apps.[5] Niche time refers to those small pockets of time — in line at the airport, walking to their car, waiting for their lunch partner to arrive — when users whip out their devices and "do something." These pockets of niche time are extremely short, lasting from seconds to perhaps a few minutes. The "something" users do is typically texting, email, Facebook, or Instagram, but it could also be a small work task like approving an order, submitting a leave request, or responding to a work ticket.

In contrast, the typical laptop VPN access process might take 1-2 minutes, after which the user can access work email, data, and applications for the remainder of the session — anywhere from 30 minutes to all day. This is a tradeoff that users are accustomed to and happy to make.

A mobile environment that requires users to connect to a VPN with manual authentication, unlock a secure container on their device, and manually log into any business apps they wish to use is not acceptable for a scenario in which the length of the session is also 1-2 minutes. The unacceptable becomes intolerable when users are asked to repeat this experience every time they try to access an enterprise mobile app, and so they stop using those apps.

When shaping your mobile strategy, it is critical to create an authentication and connectivity experience similar to that of consumer apps. Set up your infrastructure with the following in mind:

1. **Make the enrollment process as smooth as possible** for your end users while preserving the requisite level of security. For example, allow them to use their existing network login for initial authentication and use their own email account as a second factor. The process should be intuitive to the point of requiring no training and little or no documentation. It should also be relatively bulletproof, to avoid triggering an avalanche of calls to your help desk.
2. **Make authentication seamless.** For strong authentication, implement the use of biometrics or digital certificates, rather than tokens, to reduce or eliminate user intervention. Even when using biometrics or certificates, make sure that the second factor is completely transparent to the end users, so that from their perspective they're logging in using only a single credential — ideally, a familiar credential such as their Active Directory login.
3. **Deliver mobile single sign-on** and parlay that easy authentication experience to all other connected enterprise mobile apps. Multiple sign-ons are another source of friction and frustration that can be eliminated to optimize the user experience.
4. **Enable transparent reconnection.** Implement a solution that will allow you to simultaneously enforce aggressive idle timeouts while transparently reauthenticating users after an acceptable period of time. It can be as simple as choosing an idle timeout length and specifying a number of manual logins. This will give you the security benefit of quickly eliminating unnecessary connections while also delivering the perception of an "always on" connection to your enterprise. An idle timeout of 5 minutes, combined with one manual login per day, tends to be the sweet spot of usability and security.

READY?

Enterprise mobility clearly offers promise. As you set forth on your mobile journey, use the suggestions provided here to eliminate security, scale, visibility, and usability obstacles on your path to success.

ENDNOTES

[1]Hoffman, Ben, and Jean Philippe Bouchard. "The State of Mobile Enterprise Software in 2014: An IDC Survey of Applications, Platforms, Decisions, and Deployments." IDC, 2014.

[2]"Employee Mobile App Satisfaction Report." Mobiquity, October 2013.

[3]Mobiquity (see 2).

[4]Jailbreaking is the process of removing mobile device vendors' limits on their devices, such as by installing non-vendor-approved software or changing system settings. Rooting is the process of gaining root access to a device, which frequently results in compromised devices or problems with functionality.

[5]Mizukoshi, Yutaka, Kimihide Okino, and Olivier Tardy. "Lessons from Japan." The Boston Consulting Group, 2000.

Ranjeet Vidwans is VP of Marketing at Mocana, a mobile security firm. Mr. Vidwans has spent most of his 20-year career in the information security arena. Most recently he was VP of Marketing and Business Development at Identropy, where he led the company's rebranding and the launch of a new identity-as-a-service product offering. Mr. Vidwans has previously held leadership positions in business development, product management, and marketing at various enterprise security software startups, four of which were successfully acquired by blue chip firms like Oracle, Cisco, and CA. Mr. Vidwans holds a bachelor's degree from Rutgers University, where he was part of the elite "Five Year" program. He can be reached at RVidwans@mocana.com.

Mobile's Biggest Threat? It's Not What You Think

by Andrew Hoog

According to the International Telecommunication Union, the number of mobile devices in use now exceeds Earth's human population.[1] As a recent Harris poll attests, an estimated 80% employees are using their personal mobile devices for work,[2] even if just checking email or receiving alerts, and this number is sure to grow.

As we witness the end of traditional workplace computing and the rise of BYOD, enterprises are scrambling to put effective mobile security policies and strategies in place. But many of these measures are based on combating yesterday's traditional computing threats and do little or nothing to mitigate the biggest risk facing BYOD workplaces.

MOBILE MALWARE ISN'T THE ISSUE

To date, many mobile security policies — like their predecessors in traditional computing — have been focused on combating malware. Malicious code is a foe IT departments understand well, as the industry has been fighting viruses for more than a quarter-century. However, the mobile ecosystem is fundamentally different from that of a networked computing environment, and what was successful there won't protect the BYOD enterprise.

This is partly due to the permission structures for mobile operating systems. Apps are sandboxed, meaning that even an antivirus app can't access another app's storage or memory on most devices. In addition, while Android does allow some shared storage, malware detection typically only alerts you if there's a problem; it does nothing to remediate the threat and remove the app, making it a clumsy, incomplete solution.

The more fundamental problems, however, are of speed and scale. Malware detection operates by scanning apps and devices against a database of previously used malicious code. But the mobile ecosystem evolves too quickly for this strategy to be effective. Apple and Android currently offer more than 1.2 million apps each through their official channels (a number that doesn't include the additional millions of apps available through third-party marketplaces).[3] More apps are being released every day — Apple alone adds around 60,000 new apps monthly.[4] Considering the vast numbers of apps offered through Google Play and iTunes, these vendors do an admirable job of keeping malware out of their stores. At NowSecure, we often warn users who wish to jailbreak their devices (i.e., modify the operating system, typically to install apps offered outside official channels) that they are far more likely to end up downloading bundled malware from a third-party app marketplace.

With this boom in apps comes a boom in criminal innovation — attackers are constantly finding new ways to inject malicious code into apps and devices through simple evasion and obfuscation techniques. A recent Northwestern University study concluded that the most popular mobile antivirus programs were "susceptible to common evasion techniques" that rendered them largely useless.[5] Anti-malware strategies also suffer from assuming a reactive defensive posture. They depend on identifying a "known bad" and are consequently never going to be proactive — but the speed at which the mobile space evolves means anti-malware simply can't react quickly enough anyhow. Even the VP of Symantec admitted as much in an oft-quoted interview with the *Wall Street Journal*, where he declared antivirus "is dead."[6]

The bad news is that mobile anti-malware won't protect your enterprise. The good news? Mobile malware isn't your biggest problem anyway (more on that below).

WHAT ABOUT CONTAINERIZATION?

Containerization is a mobile device management (MDM) enterprise security strategy that has gained some traction in recent years. Containerization seeks to isolate corporate data on a device by storing it separately from whatever personal data a user might have on his or her phone or tablet. This allows companies to occupy and control a certain space on the device without having the kind of access many users find intrusive. It also lets them protect, encrypt, revoke access to, and

wipe corporate data on the device while leaving all other user data intact, which is especially useful when an employee leaves the company.

Containerization is cumbersome, however, as it creates another layer between a user and his or her device, and is in some quarters looked upon as the kind of top-down solution that makes individual users feel disempowered. What excites users about mobile is quick access to information, and containerization puts a damper on that.

To be fair, containerization goes some way toward mitigating targeted attacks. But the reality is that a determined attacker can *always* find a way into a device. Ironically, though, the container itself may act as a data-rich beacon for the most sophisticated attackers. Knowing that's where the good stuff is stored, attackers will focus their efforts on that area of the device.

Rather than positioning containerization as one layer of the security onion, proponents usually promote it as a comprehensive solution for the enterprise. Yet it does nothing to protect its users from the most pervasive threat to the mobile ecosystem, which is ...

LEAKY APPS

Aside from physically losing a device or having it stolen, unsecured or "leaky" apps — those applications that expose private user data — represent the biggest, most pervasive security risk facing BYOD workplaces today.

Many IT professionals (and most individual users) are surprised to hear this. Most assume that apps offered through Google Play and iTunes from reputable companies — including large financial institutions, well-known retail outlets, or established gaming and entertainment companies — are basically safe. Occasionally a high-profile app with security flaws will make the news,[7] but the vast majority go unreported by the media. And because there have been no headline-grabbing, massive security breaches in the mobile space like those that we've seen at Target, Home Depot, and elsewhere, users seem willing to take their chances.

When it comes to apps, though, they're gambling more than they realize — and the odds aren't in their favor.

At NowSecure, we recently tested 100 of the most popular apps offered through Apple's App Store and Google Play. These included apps in many categories — messaging, social networking, finance, entertainment, and productivity. All were apps from companies you've likely heard of, and none had any visible red flags that would give users pause before installing them on their devices.

The apps were tested for common security concerns, such as where they stored sensitive data, whether said data was encrypted in storage and while in transit, what sort of authentication methods the apps used, and other well-established security issues covered in the industry-standard Common Vulnerability Scoring System (CVSSv2).[8] We found that *60% of apps* tested had flaws serious enough to earn a high risk rating in one or more of these categories.

Let's think about that number for a moment.

Google claims the average global smartphone user downloads 26 apps onto his or her device[9] (though a more recent study showed that the typical Android user has 95 apps installed[10]). Let's say you're in a BYOD enterprise with 100 employees, all of them average global smartphone users. To achieve true BYOD enterprise security, you would have to be able to trust the security of some 2,600 apps. (Obviously, there would be some overlap in the apps your employees use, so this number would be lower in reality.) And as our study reveals, 60% of apps come with serious security risks, so your midsized enterprise could see its sensitive data exposed through any of 1,560 leaky apps.

With no watchdog body to evaluate apps and help consumers make educated choices, we're all basically in the dark when it comes to the apps we're entrusting with our most sensitive information.

Still considering just taking your chances? OK, but realize that failing to mitigate the risks these apps present means exposing your enterprise to loss of data, loss of customer trust, violation of regulatory statutes, and ultimately loss of revenue. Remember, too, that the cost of remediating the average data breach is US $8.3 million and rising.[11]

HOW DID IT GET TO BE LIKE THIS?

In short, because we let it.

As consumers, we haven't placed much value on security when it comes to mobile apps. Read app reviews at Google Play or iTunes, and you'll almost never see users question why an app would need location sensor permissions, much less point out that it stores login credentials in clear text on the device. With no watchdog body to evaluate apps and help consumers make

educated choices, we're all basically in the dark when it comes to the apps we're entrusting with our most sensitive information.

Tech moves fast — especially in the mobile space — and the biggest reward often goes to those who get there first. As such, speed-to-market typically trumps robust security testing in the app development cycle. The attitude among many vendors seems to be, "Meh, if people complain about security, we can patch holes in the next version." But that's of little comfort if you fall victim to a zero day exploit, and many users are slow to install updated releases.

We can't begin to achieve mobile security in the enterprise if we're still depending on outmoded strategies based on the traditional computing paradigm.

Another problem is that many apps — especially free ones, and especially games — depend solely on advertising to make money. (It's worth remembering the adage "If it's free, *you* are the product.") Even assuming a vendor has implemented strong security measures (a big assumption), the third-party advertising networks mining user data often fail to encrypt this data in transit. For evidence, look no further than Edward Snowden's revelations that the NSA was harvesting unencrypted user data leaked by advertisers on the blockbuster Angry Birds app.[12]

SO WHAT CAN WE DO?

Mitigating risks to your enterprise requires taking a layered, holistic approach to mobile security. It's less about implementing restrictive, top-down initiatives and more about educating your coworkers so they can take charge of their own device security and thereby become your first line of defense. At NowSecure, we like to refer to the four major areas of mobile security as the SCAN principle — systems, configurations, apps, and network.

You need to make sure your coworkers are running the most current version of a device's operating system, as many attackers take advantage of known problems in outdated versions. To mitigate configuration risks, you should discourage employees from jailbreaking their phones. You also need to make sure they are implementing strong passcodes — and encourage them not to reuse the same login credentials across multiple sites and services.

On the app level, users should only be downloading apps from the official marketplaces. Though this won't protect them much from leaky apps, they will be far less likely to encounter malware. They also need to keep updated and make sure they are running the latest versions of apps so they are not vulnerable to known exploits.

And if you're designing your own apps, there are a host of best practices you should implement during the development cycle,[13] including avoiding the storage of sensitive data on the device, not using crash logs,[14] ensuring SSL/TLS certificates are properly validated, using strong encryption, and much, much more.

When it comes to networks, users must be strongly discouraged from using unsecured Wi-Fi hotspots, as attackers can intercept traffic from their device and mine it for sensitive data. Painful though it may be, unless they are sure that the Wi-Fi connection at their favorite coffee shop is secure, they should instead connect using their data plan.

While educating your coworkers on the SCAN principle will do much to achieve BYOD security, protecting against insider threats will require your IT department to have some level of visibility into these devices. This doesn't mean implementing an intrusive, Big Brother–type spying program, but it does mean knowing exactly (and only) what you need to: how much risk does this device present to the company? Finding the answer to that question will bring you a long way toward enterprise mobile security.

A MORE SECURE MOBILE ECOSYSTEM

BYOD is here to stay, but we can't begin to achieve mobile security in the enterprise if we're still depending on outmoded strategies based on the traditional computing paradigm. Nor will we make much progress if we rely on magic-bullet, top-down solutions that negatively impact end users.

Creating a more secure mobile ecosystem going forward means increasing awareness surrounding mobile security issues in general, but especially those posed by leaky apps. As app developers, we need to build robust security testing into the development cycle to ensure that we're part of the solution and not part of the problem. As consumers, we need to place greater demands on vendors to create apps that don't put users' sensitive information at risk. We can start by more closely following public vulnerability disclosures, uninstalling leaky apps until these threats are remediated, and cautioning others about these flaws. And as IT professionals, we need to help educate coworkers about the threat leaky apps represent and implement proactive strategies to address those risks.

As described earlier, one way companies have sought to strike the delicate balance between enterprise security and individual privacy is through containerization — basically creating a walled garden of sorts on the device wherein all the corporate data resides. The company can then secure this data (and wipe it from the device if need be) without accessing any other areas of the phone.

Another approach involves giving users an app that allows them to monitor their own device. It could provide them with security alerts about leaky apps and let them know how much of their traffic is encrypted, what countries and organizations their device is sharing data with, and whether the connections they are using are secure. Using this data, the app could calculate an overall numeric security score. Company IT departments could then use their own version of this program to unobtrusively request these scores — without accessing any other individual user data — and react appropriately when a user reaches a predetermined level. For example, if a user's score goes below 75 (out of a possible 100), the company could prevent that user from accessing corporate email from the device and send the individual a notice to resolve any outstanding issues.

Attackers will always be innovating new exploits as new technology and techniques become available. But by working together, we can all make their jobs a lot more difficult and a lot less lucrative.

ENDNOTES

[1]"World to Have More Cell Phone Accounts than People by 2014." SiliconIndia, 2 January 2013.

[2]Cobb, Stephen. "BYOD Infographic: For Security It's Not a Pretty Picture." We Live Security, 4 April 2012.

[3]Perez, Sarah. "iTunes App Store Now Has 1.2 Million Apps, Has Seen 75 Billion Downloads to Date." TechCrunch, 2 June 2014.

[4]Perez, Sarah. "The App Store, Six Years Later." TechCrunch, 10 July 2014.

[5]Rastogi, Vaibhav, Yan Chen, and Xuxian Jiang. "Evaluating Android Anti-Malware Against Transformation Attacks." Northwestern University, Department of Electrical Engineering and Computer Science, March 2013.

[6]Yadron, Danny. "Symantec Develops New Attack on Cyberhacking." *The Wall Street Journal*, 4 May 2014.

[7]González, Ángel. "Starbucks iPhone App Vulnerable, Security Specialist Says." *The Seattle Times*, 15 January 2014.

[8]NVD Common Vulnerability Scoring System Support v2 (CVSSv2) (https://nvd.nist.gov/cvss.cfm).

[9]Fox, Zoe. "The Average Smartphone User Downloads 25 Apps." Mashable, 5 September 2013.

[10]Sawers, Paul. "Android Users Have an Average of 95 Apps Installed on Their Phones, According to Yahoo Aviate Data." The Next Web (TNW), 26 August 2014.

[11]Fobert, Joe, et al. "Cyber and Data Security Risks and the Real Estate Industry." AIG, 2013.

[12]Robertson, Jordan. "Google+, 'Candy Crush' Show Risk of Leakiest Apps." Bloomberg GlobalTech, 29 January 2014.

[13]"Secure Mobile Development." NowSecure, 2 December 2014.

[14]"Avoid Crash Logs." NowSecure, 26 November 2014.

Andrew Hoog, CEO of NowSecure (formerly viaForensics), is a recognized leader in mobile security. Author of two books and with two patents pending, Mr. Hoog cofounded the company with a mission to make the mobile ecosystem safer for all. NowSecure now counts four of the five largest financial institutions as well as Fortune *500 companies and the US government among its clients, and it employs researchers and developers across Europe and the Americas. The company was also recently named to 2014's* Fortune *5000. When not breaking and fixing things, Mr. Hoog enjoys great wine, science fiction, running, and tinkering with geeky gadgets. He can be reached at ahoog@nowsecure.com.*

Privacy of Mobile Users: Pitfalls and Recommendations

by Naser Mohamed Al Ali, Dima Alhadidi, and Zakaria Maamar

On-the-move smartphones have become the de facto means for communication and Internet usage today. In general, there has been major growth in the lucrative market of smartphones. According to Heather Leonard, author of the "Mobile Insights" column at *Business Insider Intelligence*, "By the end of [2013], 1.4 billion smartphones will be in use.... With the world population at 7 billion that will mean one phone for every five people in the world."[1] People have quickly embraced smartphones; they provide access to online services anytime, anywhere, and to anyone.

Unfortunately, there are risks associated with this "uncontrolled" embrace of smartphones, especially when people do not pay attention to the installation terms and conditions of smartphone apps. According to University of California, Berkeley researcher Erika Chin and her colleagues, "To help protect users while selecting applications, it is important to understand each step in the mobile application installation process."[2] Most apps require for their proper and efficient use that users grant them access to several in-built smartphone services and/or other apps. Some apps might not even inform users of the data collection that happens during installation. This data could be related to call logs, phone and email contacts, a device's identifiers, and so forth. Jay Patel of Vrinsoft Technology reveals that "59% of application publishers are not informing the users about their data collection."[3] He adds that only 15% of the apps he studied are "perfect" in the sense of making users aware of what data they collect and for what purposes. Most users only skim through the installation terms and conditions. Some do not even try to read them; they simply click!

To illustrate the madness of smartphone app adoption from a privacy perspective, we carried out a set of experiments that investigate the installation of apps on a specific smartphone (same platform) and then on multiple smartphones (different platforms). We refer to these experiments as "vertical" and "horizontal," respectively. Out of these experiments we put forward some recommendations that should help smartphone users deal with this madness.

WHAT DO YOUR APPS REVEAL ABOUT YOU?

Latest-generation smartphones are amazing; they handle real-time data, alert their users to traffic congestion, advise on physical exercise, and so on. At the same time, these smartphones threaten users' privacy when they access personal information like location, contact lists, phone logs, and messages. Researchers at the University of New England in Australia stress that "in order to achieve a high level of privacy, the user should be given the authority to control the privacy settings when he/she receives or requests a service related to his/her personal information."[4] Yet an examination of 101 popular software applications for iOS and Android smartphones shows that "56 transmitted the phone's unique device ID to other companies without users' awareness or consent; 47 apps transmitted the phone's location in some way; 5 sent age, gender and other personal details to third parties."[5] This is downright scary and shows that a lot of data is transmitted without the user's approval, although the user acknowledges the risks of installing the app.

In 2011, a *New York Times* report indicated that Apple iPhone and iPad devices were collecting users' geographical location data and storing it for a period of 12 months. Immediately, Apple released a software update to fix the issue and apologized for the same.[6] In addition, the *Wall Street Journal* conducted a study of apps for iOS and Android platforms and discovered that the majority of the collected personal information — ranging from age, gender, and location to phone identifiers — is provided to third parties without the user's consent. Many apps included in the *Wall Street Journal* study did not offer written privacy policies.[7]

To ensure proper handling of privacy, users have a role to play. They need to pay careful attention to apps' policies in terms of what data will be collected and shared, what access needs to be granted to these apps, when updates happen, and the like. Some policies do not contain legal terms and conditions, while others blindly copy other apps' policies without any adaptation. According to California Attorney General Kamala Harris, "Recent studies ... have found many mobile apps did not provide

users with privacy policy statements at all. This represents not just a failure in transparency, but it also suggests a lack of attention to the apps' privacy practice."[8]

PRIVACY ANALYSIS

To demonstrate how easily the privacy of mobile users is put at risk, we carried out a number of experiments on smartphone apps. Our testing consisted of three phases: app and smartphone selection, analysis of apps' legal terms and conditions, and app deployment on smartphones.

App and Smartphone Selection

First, we established the criteria for selecting both apps and smartphones. These included popularity, existence of fees, possibility to deploy across many platforms, and similarity in terms of functionality. The apps we selected are WhatsApp (version 2.11.399), Telegram (version 1.9.4), Viber (version 5.0.2), and Talkray (version 1.104):

- **WhatsApp** supports communication through messages between parties. It allows sending and receiving of messages, images, audio, and video.
- **Telegram** is known for its speed and security. Telegram users can exchange encrypted and self-destructing messages, images, video, and documents.
- **Viber** allows the exchanging of instant messages and is used to text messages and exchange photos, video, and audio media.
- **Talkray** is the fastest free calling and messaging app. Talkray users can send messages and pictures or call friends across the world.

The smartphones that we selected are Samsung Note 3 (Android 4.4.2), iPhone (iOS 7.1.2), and Torch 9800 (BlackBerry 6.0.0.546).

Analysis of Apps' Legal Terms and Conditions

The end-user license agreement (EULA) establishes a legal framework between a user and a software application. Several agreements are available online, while others are only accessible prior to installation. However, due to the complexity of EULA text, people tend to accept it without paying attention to how applications they install could put their privacy at risk.[9] Our analysis of apps' legal terms and conditions included two parts: a manual reading through of terms and conditions and an automatic parsing of terms and conditions using specialized tools.

Manual Analysis

To simplify the process of understanding apps' legal terms and conditions, we divided the terms and conditions into the following categories (see Table 1 on the next page):

- **Privacy and data collection.** Does the app provide a privacy policy to help users make informed decisions about whether or not to use the app?
- **Installation and functionality.** Does the app provide step-by-step installation guidelines or procedures?
- **Upgrade or update.** Does the app send upgrade or update notifications whenever it has a new feature?
- **Monitoring.** How does the app track utilization of its services after installation?
- **Data management.** How does the app store, secure, use, and/or transfer the users' personal information?
- **Advertising.** Does the app collect information for commercial purposes on behalf of third parties?

Automated Analysis

We selected EULA License Analyzer Beta Version (www.spywareguide.com/analyze/analyzer.php) to automatically analyze the terms and conditions of our four selected apps. This tool works by looking for specific words in an app's policy, allowing users to specify some activities and display the number of occurrences of these activities (see Table 2 on page 17).

App Deployment on Smartphones

We divided the last step of the analysis into two experiments: one vertical (with different apps on the same smartphone) and one horizontal (with the same app on different smartphones). These are shown in Figure 1 and Figure 2, respectively, on page 17.

In the vertical experiment, WhatsApp, Telegram, Viber, and Talkray were installed on a Samsung Note 3. They were downloaded from the Android Play Store using the first author's Gmail ID to sign in. Table 3 summarizes the access permission requests per app (X stands for "access to," while — stands for "no request").

In the horizontal experiment, WhatsApp only was installed on a Samsung Note 3, iPhone 4, and Torch 9800. Table 4 summarizes the access permission requests per smartphone (X stands for available, 1 stands for prompt, and 0 stands for not applicable).

Table 1 — Summary of EULAs for the Selected Apps

Categories	WhatsApp	Telegram	Viber	Talkray
Privacy and data collection	• Users should have mobile phone numbers. • App does not collect names, addresses, or email addresses, just mobile phone numbers. • Users must be 16 years or above. • App periodically accesses the mobile phone numbers.	• There is no data sharing. • Phone number is used as a unique identifier. • Permission is sought before syncing contacts. • App stores user's contacts to notify the user as soon as one of user's contacts signs up for Telegram.	• Users should have mobile phone numbers. • Users may add a user number to their address book, and the user name will be shown as registered to Viber. • The service does not record any call while communicating with other users. • The service may communicate with phone's SMS inbox for service activation. • Users must be under 13 years or above.	• User personal phone number and/or Facebook/ email ID can be requested for registration purposes. • App collects general information in server log files, such as the user's IP address. • Users must be 13 years or above.
Installation and functionality	• Users should not attempt to reverse engineer or modify any part of the service. • App allows the use of sniffers such as Ethereal, tcpdump, or HTTPWatch. • App does not recommend using unsecured Wi-Fi or other unprotected networks.	• Messages in secret chats can be ordered to self-destruct.	• Not applicable	• Not applicable
Upgrade or update	• Whenever there is an update, the app will send a notification to users.	• Not applicable	• From time to time, the policy may be revised. • App encourages users to visit the website and review the policy periodically to be aware of any modifications and changes. • If users want to remove their username, they can contact the Viber support team.	• Changes may be made to this policy from time to time. Talkray reserves the right to make these changes without any notice to the user.
Monitoring	• WhatsApp will remove all content and status submissions if properly notified that such content or status submission infringes on another's intellectual property rights.	• Not applicable	• App may disclose information about user for national security, law enforcement, or other issues of public importance.	• Not applicable
Data management	• Not applicable	• All data is stored and encrypted. • There is no storage for log messages in secret chat. • Users are allowed to delete their accounts only on deactivation page.	• Not applicable	• Not applicable
Advertising	• App does not send marketing messages or commercial content without the user's consent. • App may share personally identifiable information with third-party service providers to the extent that it is reasonably necessary to perform, improve, or maintain the WhatsApp service.	• App does not share user's data with anyone.	• Service uses third party in order to send users an authentication SMS.	• Goods and services of third parties may be advertised and/or made available on or through this app.

Table 2 — Summary of Apps' Terms and Conditions Automatic Analysis

Activities	Sentences Flagged per App			
	WhatsApp	Telegram	Viber	Talkray
Reference to advertising	6	0	1	4
Reference to tracking or monitoring of usage	20	0	11	5
Reference to removal restrictions or procedures	Not applicable	Not applicable	Not applicable	1
Reference to removal restrictions or removal rules by third-party tools	Not applicable	Not applicable	Not applicable	1
Software could expose users to content that may be offensive, indecent, or objectionable in their local community	Not applicable	Not applicable	Not applicable	2
No warranty on performance of software	Not applicable	Not applicable	Not applicable	1

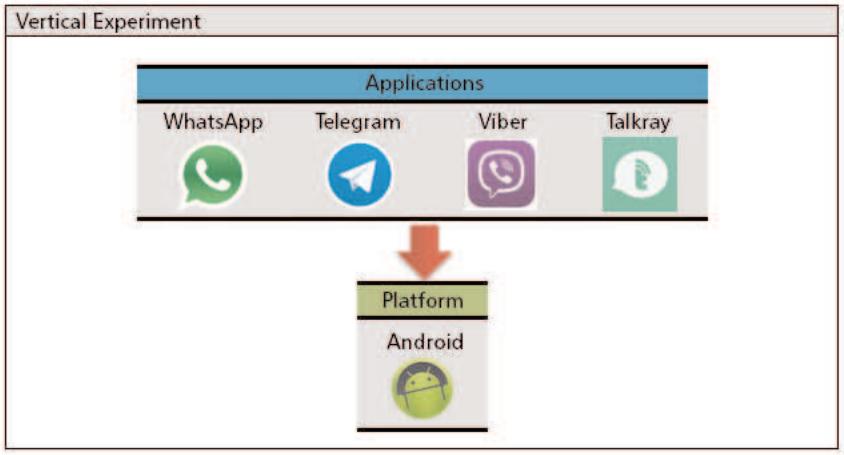


Figure 1 — Different apps on the same platform.

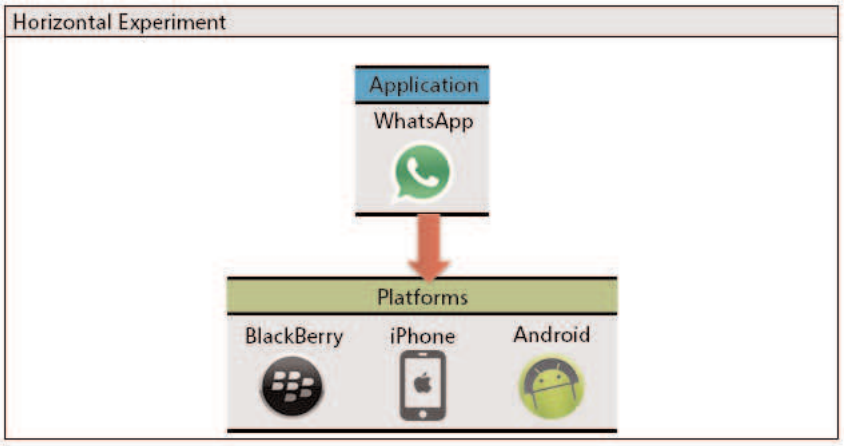


Figure 2 — Same app on different platforms.

Table 3 — Summary of Apps' Permissions for Samsung Note 3

Permissions	WhatsApp	Telegram	Viber	Talkray
In-app purchases	X	—	X	—
Device & app history	X	—	X	—
Identity	X	X	X	X
Calendar	X	X	X	X
Contacts	X	X	X	X
Location	X	X	X	X
SMS	X	X	X	X
Photo/Media/Files	X	X	X	X
Camera/Microphone	X	X	X	X
Wi-Fi connection information	X	X	X	—
Device ID & call information	X	X	X	X

Table 4 — Summary of WhatsApp's Permissions on Multiple Platforms

Permissions	Samsung Note 3	iPhone 4	Torch 9800
In-app purchases	X	0	0
Device & app history	X	0	1
Identity	X	X	X
Calendar	X	0	0
Contacts	X	1	X
Location	X	1	1
SMS	X	0	0
Photo/Media/Files	X	1	1
Camera/Microphone	X	1	1
Wi-Fi connection information	X	0	X
Device ID & call information	X	X	X

RECOMMENDATIONS

Understanding apps' legal terms and conditions is extremely important in order to make users aware of any potential risk. Our manual analysis of the apps' legal terms and conditions was not straightforward; it required understanding each term and condition. Indeed, we noted that some apps' privacy policies contain similar descriptive terms although these apps have different functionalities. Some apps' privacy policies are not clear about communication with third parties' apps or what activities they might offer, as they might use or store personal information for other purposes. This could expose a user's personal information in the future.

The success of an automated analysis depends on identifying the appropriate activities that a tool such as EULA License Analyzer will look for in legal terms and conditions documents. During our automated analysis, we noticed that most apps' privacy policies focus on advertisement, tracking, and monitoring. We also observed that platforms like iOS and BlackBerry are more restricted than Android in terms of permission controls.

When they are installing an app, users may not pay attention to every single detail of the app's privacy policies. Some platforms such as iOS and BlackBerry give users control over permission requests. Both always notify the user of access permissions before accessing users' phone services. Android, on the other hand, tends to offer less user control. To summarize how different platforms deal with user permissions, we observe the following:

- Android apps require users to either grant or reject access requests. If users reject them, they will not be able to download the app.
- iOS requests its users' consent by making them sign in using their ID account. Once an app is downloaded, users can manage the permission from iOS privacy control.
- BlackBerry allows its users to modify apps' permissions before installation. The apps prompt users for permission whenever necessary.

To protect your mobile privacy, we offer the following recommendations:

- Be fully aware of apps' terms and conditions and read users' comments and the feedback on each app before downloading it.
- Download apps from reliable sources and ensure that the URL does not redirect to a different source.
- Check the authenticity of the app developer and permission details before installing an app.
- If abnormal activity on the app is detected, remove it or flag it as inappropriate.
- Download "My Permission," a tool available for the Android platform.[10] It can help monitor apps' permissions and protect personal information.
- Set PINs and passwords to protect personal data stored on smartphones.
- Accept updates and patches to your smartphone's software.
- Encrypt sensitive data that you store on an SD card.

PARTING THOUGHTS

People have become addicted to smartphones for communication and access to different online resources. Many smartphone apps collect and share personal data so that they can offer better services to users, but many also abuse this access and thus put user privacy at risk. Making users aware of apps' legal terms and conditions is a must. Policies should be presented in a way that is easy to read and understand. Finally, users must be given more control over apps so they can make decisions about what information they want to — or don't want to — share.

ENDNOTES

[1]Leonard, Heather. "There Will Soon Be One Smartphone for Every Five People in the World." *Business Insider*, 7 February 2013.

[2]Chin, Erika, et al. "Measuring User Confidence in Smartphone Security and Privacy." *Proceedings of the ACM Symposium on Usable Privacy and Security (SOUPS'2012)*. ACM, 2012.

[3]Patel, Jay. "The 75% of Mobile Applications Are Seeking to Access User Data." WhaTech, 16 September 2014.

[4]Aldhafferi, Nahier, Charles Watson, and A.S.M. Sajeev. "Personal Information Privacy Settings of Online Social Networks and Their Suitability for Mobile Internet Devices." *International Journal of Security, Privacy, and Trust Management*, Vol. 2, No. 2, April 2013.

[5]Thurm, Scott, and Yukari Iwatani Kane. "Your Apps Are Watching You." *The Wall Street Journal*, 17 December 2010.

[6]Helft, Miguel. "Jobs Says Apple Made Mistakes with iPhone Data." *The New York Times*, 27 April 2011.

[7]Thurm and Kane (see 5).

[8]Harris, Kamala D. "Privacy on the Go: Recommendations for the Mobile Ecosystem." California Department of Justice, January 2013.

[9]Mateen, Faisal, and Irfan Hussain. "Automated Analysis of End-User License Agreements." Master's thesis. School of Computing, Blekinge Institute of Technology, Sweden, 2011.

[10]See https://play.google.com/store/apps/details?id=com.mypermissions.mypermissions&hl=en.

Naser Mohamed Al Ali is a network/security specialist working for the UAE government. He also is CEH, ECSA, and ITIL v3 certified. His research interests include hacking and privacy. He has a master's degree in cyber security from Zayed University in Dubai, U.A.E. He can be reached at m80004329@zu.ac.ae.

Dima Alhadidi is an Assistant Professor in the College of Technological Innovation at Zayed University, Dubai campus. Dr. Alhadidi's research interests include computer security, aspect-oriented programming, software engineering, secure distributed computing, and cloud computing. She has a PhD in computer science and software engineering from Concordia University, Canada. She can be reached at dima.alhadidi@zu.ac.ae.

Zakaria Maamar is a Professor in the College of Technological Innovation at Zayed University, Dubai campus. His research interests include mobile computing, business process management, and social computing. Dr. Maamar has published several papers in peer-reviewed journals and conference proceedings. He has a PhD in computer science from Laval University, Canada. He can be reached at zakaria.maamar@zu.ac.ae.

Mobile Security from a Practical Perspective

by Anjali Kaushik

New technological developments — such as the Internet and mobile usage and the connectivity they bring — are shaping the way business is transacted today. Together they bring a sense of independence from time and location and convenience as never experienced before. The accelerated use of the Internet and mobile has enabled a dramatic rise in online activity. The acceptance of mobile commerce for shopping, healthcare services, and travel is greater than ever.

As Internet and mobile usage continues to rise, however, the threat of cyber crime also grows. Mobile malware is becoming very advanced and rapidly reaching parity with PC malware. Recent technological developments have enabled seamless integration between traditional desktops and mobile devices. Unfortunately, a majority of users do not realize that most of the threats (e.g., phishing attacks) they face online using traditional devices can also hound their mobile experiences. Similar to PCs, mobile devices can be hacked, compromised, and enslaved to send spam messages and conduct other attacks. They can be exploited to extract information on where people have been, pictures they have taken, call log details, and much more. This is valuable and private data for people.

Further, due to the growing BYOD phenomenon, corporate data is readily available to employees on their personal devices. Therefore, mobile security is a serious issue both from an individual and organizational perspective.

THREATS THAT ARE UNIQUE TO MOBILE

What is disturbing is the potential for higher-impact privacy breaches through mobile devices compared to a PC. For instance, the amount of data that mobile app developers can send out to advertising networks after a user has downloaded one of their free apps is immense. Secondly, most apps — like those of e-commerce or ticketing companies — ask for access to user details like text messages, images, location, contacts, and so on. Some smartphones do not allow a user to download an app if they deny access to this information.

Smartphone users are also vulnerable to infectious Trojan viruses, which steal vital information from the personal device and can even illegally send SMSes to those on the mobile contact list. The malware may be bundled with legitimate applications and infect the smartphone. After a virus successfully infects a smartphone, basic information about the phone (e.g., IMEI number, device ID, device type) is compromised, and the malware can even install spyware on the targeted device. The virus can steal contacts and pictures, track the device's location, steal passwords, illegally access text messages, crash the complete system, steal personal banking information (when the user is logged in), install other spyware, and defend itself by disabling the device's firewall and antivirus program.

A device can also be compromised when its user visits a seemingly legitimate website that in fact contains a trap to infect the device by installing a piece of malware. Hackers can then operate networks of such compromised devices (i.e., "botnets") to attack other websites. In this way, the device may become a node in a botnet, with the attacker gaining access to and controlling such interconnected devices to launch spam and other forms of cyber attacks. Sophisticated cyber criminals may use botnets to launch coordinated attacks against vulnerable websites in order to steal credit card information. Credit card security is one of the most important components of online commerce security.

Mobile devices are also exposed to physical threats like theft, which helps users of malicious intent to get at the private and sensitive information stored in the devices. And since mobile devices are so ubiquitous now, and many of them have access into corporate networks, the risk is greater. A compromised mobile device may provide "back doors" through which hackers can gain entry to the corporate network and create problems.

Advanced Persistent Threats on Mobile Devices

Today it is not just governments and large organizations that fall victim to cyber attacks; specific individuals within organizations can also be targeted. In one such attack, the malware involved "targeted executives

and high-ranking individuals in the finance, engineering, and oil industries as well as those in politics, embassies, and militaries."[1]

An advanced persistent threat (APT) is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. The motive behind such threats is to steal confidential data and information from a specific person. In a simple attack, the intruder tries to get in and out as quickly as possible in order to avoid detection. In an APT attack, the goal is not to get in and out, but rather to achieve ongoing access to sensitive data and information. Developers of APTs firstly look for vulnerabilities within the system. After that, APTs evaluate the security controls that protect the system and try to come up with a plan in order to exploit the vulnerabilities. This entire process takes an incredible amount of time and research and may go on for months.

As these attacks become more targeted, they are also becoming more personalized. Cyber criminals are hitting smartphones and tablets with malware that is persistent and sophisticated. Such malware can infect systems through spear-phishing e-mails and messages that entice victims to open files that have a trap. Spear phishing refers to emails and messages that are specially crafted to target a particular company or person. Such emails/messages appear to be sent by organizations or individuals from whom the potential victims would normally get messages, so as to make them believe that the communications are genuine. This makes spear-phishing attacks much more deceptive than phishing attacks.

MOBILE SECURITY: MITIGATING THE RISKS

Companies offering Internet-based products and services or online mobile services to their customers should use effective authentication mechanisms for high-risk transactions involving access to customer information or movement of funds to other parties. For the company, it is also important to protect stored cardholder data and encrypt transmission of cardholder data across open, public networks as per popular standards such as PCI DSS. Areas of concern for online commerce can be minimized once the industry gives adequate focus to security issues. This is an important step so that customer trust in online transactions is protected.

There are a variety of technologies and methodologies that can be used to authenticate customers online, such as customer passwords, personal identification number (PINs), digital certificate using a public key infrastructure (PKI), physical devices such as smart cards, one-time passwords (OTPs), and others. An effective authentication system is necessary for compliance with requirements to safeguard customer information, to prevent money laundering and reduce fraud, to inhibit identity theft, and to promote the legal enforceability of electronic agreements and transactions.

Smartphones are getting more advanced, and the ways to attack them are getting more sophisticated. You need to be cautious, especially when making a financial transaction from a smartphone. In most cases it's better to choose a browser over an app, as the Web programs, being older, have been tested more thoroughly and are less likely to contain bugs.

That said, a browser is vulnerable to one risk that an app is not. While an app may have malware embedded into it, sessions on the browser can be taken over by a hacker through a man in the middle (MITM) attack. When a transaction is being made, a bot (a compromised machine used to hack) sends a message to a hacker that the session has started. The hacker will hijack the session and make transactions from the user account. The user will not know about the transaction until he or she gets an intimation of it from the other party with whom the transaction is being conducted. Therefore, smartphone users need to be careful both when downloading apps and/or using apps through a browser.

In an APT attack, the goal is not to get in and out, but rather to achieve ongoing access to sensitive data and information.

For added protection, use a longer password containing multiple character types and change it frequently. Some banks ask for a verbal password; that way if the bank calls the phone that's being used to access the account, a person who doesn't own the phone (and thus doesn't know the verbal password) won't be able to continue. A few other security suggestions for mobile users include:

- Keep the operating system and apps updated. One way to safeguard against malware is to decline the prompts for system updates and go through smartphone settings to check for system updates.
- Download applications and other information from trusted sources and official app stores only. Do not click "install" on a pop-up from a third-party Web page.

- Pay attention to the data that is shared through applications.
- Log out of sites after making a payment. Don't store the ID, username, or password on the phone and avoid financial transactions when on a public Wi-Fi.
- Avoid using m-wallets, as they can be used as a conduit for fraudulent transactions. In the case of m-wallets, the mobile payments are made through a third party, and the risk of fraud is higher.
- Avoid giving out personal information. If you get requests via email or text for account information, contact the business directly to confirm.
- Install a security app. A good security app can warn about risky websites and enable users to remotely locate, lock, alarm, or wipe a lost device. Avast! Mobile Security & Antivirus, Lookout Mobile Security, McAfee Mobile Security for Android, Kaspersky Internet Security for Android, and Norton Mobile Security are some options.
- For files stored on Internet-based storage services such as iCloud and Dropbox, make sure you have a strong password and turn on a second layer of protection, often known as two-step verification.

Apple, Google, and other tech firms have been trying to portray themselves as reliable custodians of their users' personal data after it was revealed that the US National Security Agency had been prying into user emails and other communications as part of its anti-terrorism efforts. Likewise, Apple is having to do some damage control on the security and privacy front after hackers accessed and distributed personal photos that various celebrities had stored on Apple's iCloud service. Apple now allows for the use of passcodes, fingerprint identification, and additional tools for hiding or securing sensitive photos and documents stored on the phone.[2]

CONCLUSION

As the usage of mobile devices grows in the individual and organizational space, the threat landscape is also becoming deeper and multidimensional. Unless individuals and organizations deploy appropriate controls, security issues will arise. Since the use of mobile devices introduces risk to the organization and individuals, an holistic and methodical approach should be used to define this risk on an ongoing basis. This will help ensure that controls exist to maintain both the security and usability of mobile devices.

ENDNOTES

[1]Goodin, Dan. "Nation-Backed Malware Targets Diplomats' iPhones, Androids, and PCs." Ars Technica, 10 December 2014.

[2]"How to Hide Data on Smartphones, from iPhones to Samsungs." Express Computer, 23 September 2014.

Anjali Kaushik is an Associate Professor of Information Systems at the Management Development Institute (MDI), India. She has almost 20 years of consolidated experience in the area of IT business consulting and research in both the corporate world and academia. Prior to joining academia, Dr. Kaushik headed the vertical research group in IDC (India) Limited. She is also a regular consultant to the government of India for various projects related to strategic planning, policy making, monitoring and impact assessment on e-governance, and cyber security. Dr. Kaushik has authored five books with major publishers and has more than 15 published research papers in various journals. She holds a PhD from Delhi University in the area of information systems planning. She can be reached at anjalikaushik@mdi.ac.in.

ACCESS TO THE EXPERTS

Cutter's Inquiry Program

Get Guidance and Answers from the Best Minds in the Business

Cutter's Access to the Experts Inquiry Program, available to Cutter Consortium Enterprise Suite clients, provides you with astute analysis and advice directly from Cutter's renowned experts. Every inquiry is fielded by a Cutter Senior Consultant or Fellow with hands-on expertise addressing IT challenges at organizations worldwide. You'll get insightful answers to your questions from the pros, based on real-world experience, which is markedly different from what other analyst firms provide.

Answers You Can Put Into Action

Clients can leverage the hours with Cutter's experts in many ways. Allot some of the inquiry time to the CIO, pairing him or her with a top Cutter business-IT strategist for monthly brainstorming sessions. Or set up monthly calls for your Director of Enterprise Architecture with one of Cutter's EA experts. In either case, the arrangement allows the two of them to build a rapport and gives the Cutter expert a growing understanding of the issues your enterprise is facing. The Cutter expert quickly becomes a valuable advisor. You can also submit email inquiries to Cutter. A Cutter Senior Consultant or Fellow with relevant hands-on expertise will answer your question directly, either in writing, by phone, or both ways if that better meets your needs.

From advice on your governance strategy from Cutter's Enterprise Risk Management & Governance expert Bob Charette, to counsel on integrating Agile approaches into your existing project management methodology from Israel Gat; counsel on how to spread the culture of innovation throughout your enterprise from innovation expert Rob Austin; input on creating and deploying your enterprise architecture from EA expert William Ulrich; advice about how to protect the personally identifiable information (PII) your organization collects from privacy guru Rebecca Herold; to advice on how to uncover IT cost-reduction opportunities from IT strategy expert Bob Benson, Cutter's team of experts is uniquely positioned to provide you with solutions.

While some inquiries may be answered informally by our experts, others will require research and further conversation in order to provide the best advice. But in each and every case, you'll get one of the best minds in the industry working on your problem right away.

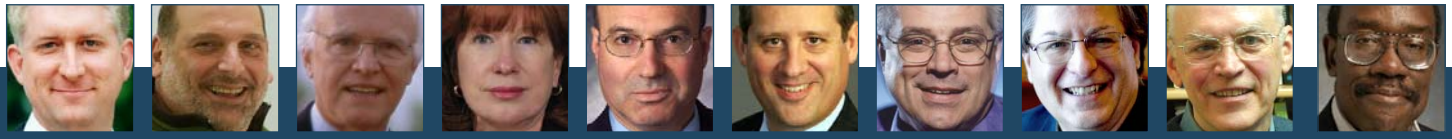
Your Client Research Manager

Every Access to the Experts client organization is assigned a client research manager who will field your inquiries, matching the right expert to your inquiry. Your client research manager ensures that your questions are answered promptly and he or she handles the logistics for teleconferences. We dedicate the time to coordinating the communication, so you can concentrate on getting the answers you need.

For More Information

For more information on Cutter Consortium, contact us by:

Tel: +1 781 648 8700
Fax: +1 781 648 8707
Email: sales@cutter.com
Web: www.cutter.com
Mail: 37 Broadway, Suite 1, Arlington, MA 02474-5552 USA



Rob Austin | Ron Blitstein | Tom DeMarco | Lynne Ellyn | Israel Gat | Vince Kellen | Tim Lister | Lou Mazzucchelli | Ken Orr | Robert Scott

Cutter Business Technology Council

About Cutter Consortium

Cutter Consortium is a truly unique IT advisory firm, comprising a group of more than 100 internationally recognized experts who have come together to offer content, consulting, and training to our clients. These experts are committed to delivering top-level, critical, and objective advice. They have done, and are doing, groundbreaking work in organizations worldwide, helping companies deal with issues in the core areas of software development and agile project management, enterprise architecture, business technology trends and strategies, enterprise risk management, metrics, and sourcing.

Cutter offers a different value proposition than other IT research firms: We give you Access to the Experts. You get practitioners' points of view, derived from hands-on experience with the same critical issues you are facing, not the perspective of a desk-bound analyst who can only make predictions and observations on what's happening in the marketplace. With Cutter Consortium, you get the best practices and lessons learned from the world's leading experts, experts who are implementing these techniques at companies like yours right now.

Cutter's clients are able to tap into its expertise in a variety of formats, including content via online advisory services and journals, mentoring, workshops, training, and consulting. And by customizing our information products and training/consulting services, you get the solutions you need, while staying within your budget.

Cutter Consortium's philosophy is that there is no single right solution for all enterprises, or all departments within one enterprise, or even all projects within a department. Cutter believes that the complexity of the business technology issues confronting corporations today demands multiple detailed perspectives from which a company can view its opportunities and risks in order to make the right strategic and tactical decisions. The simplistic pronouncements other analyst firms make do not take into account the unique situation of each organization. This is another reason to present the several sides to each issue: to enable clients to determine the course of action that best fits their unique situation.

For more information, contact Cutter Consortium at +1 781 648 8700 or sales@cutter.com.

The Cutter Business Technology Council

The Cutter Business Technology Council was established by Cutter Consortium to help spot emerging trends in IT, digital technology, and the marketplace. Its members are IT specialists whose ideas have become important building blocks of today's wide-band, digitally connected, global economy. This brain trust includes:

- Rob Austin
- Ron Blitstein
- Tom DeMarco
- Lynne Ellyn
- Israel Gat
- Vince Kellen
- Tim Lister
- Lou Mazzucchelli
- Ken Orr
- Robert D. Scott