Interested in learning more about security?

SANS Institute InfoSec Reading Room

Wireless Mobile Security

This paper offers an overview of the current threats to mobile system data confidentiality, availability and integrity. It will present the data-centric security model as a key enabler for secure personal and business use of mobile devices. Finally, the incident handling model will be applied against mobile device security events in order to assess the model against this relatively new threat vector to the enterprise computing environment.

Mobile Security:

Current threats and emerging protective measures

GIAC (GCIH) Gold Certification

Author: Erik Couture, erikcouture@gmail.com
Advisor: Egan Hadsell

Accepted: December 3, 2010

Abstract

This paper offers an overview of the current threats to mobile system data confidentiality, availability and integrity. It will present the data-centric security model as a key enabler for secure personal and business use of mobile devices. Finally, the incident handling model will be applied against mobile device security events in order to assess the model against this relatively new threat vector to the enterprise computing environment.

1. Introduction

Advanced mobile devices, known as smartphones, are a class of devices built at their core around ease of connectivity and always-on accessibility of online services. These devices can offer many advantages in increased productivity and ubiquitous availability of personal, client and corporate data. There is no question of the power of the devices many of us now carry in our pockets; they are increasingly used not only for communication, but for carrying personal and sensitive business data and accessing remote network resources. As smartphones decrease in price, they are increasing rapidly in both power and functionality and their popularity has risen exponentially in the past 5 years. Fig 1 shows that very soon more then half the mobile phones in the US will be smartphones. Indeed, there are over 50 million smartphones (Roche and O'Neill, 2010) users in the US, this number having grown rapidly in the past 2 years.

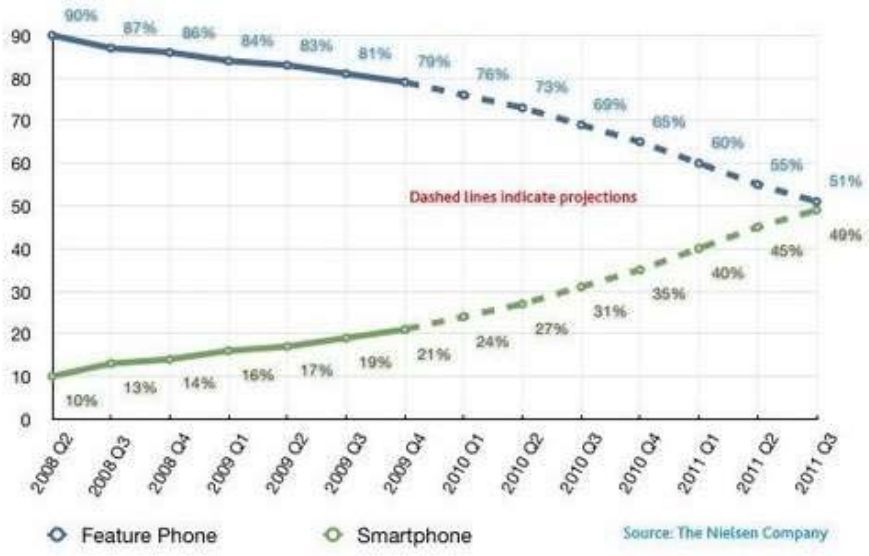

Figure 1 - Smartphone Market Penetration (Neilson, 2010)

These platforms are becoming increasingly similar to our desktop and portable computers, but it is their unique qualities in many respects, which demand special consideration for the distinct security risks they present. The proliferation of the 'app'; small single purposed applications, easily downloaded and installed, opens the platform up to malware, previously uncommon to the mobile phone arena. This app-based environment has quickly grown to transform the industry and has pushed users to much higher data usage and pervasive connectivity to the internet from their mobile devices. Increased IP network connectivity in itself brings a familiar raft of security challenges, well known in the desktop environment, but new to the relatively immature mobile operating systems. A number of existing technologies enable security professionals to ensure some degree of security in the implementation of these mobile platforms (encryption, VPN, firewalls, anti-malware scanners). These tools are familiar to all security experts, but the method in which they are applied to mobile devices differ significantly from the desktop and portable (laptop) computing environment. Merely

focusing on technologies however, misses the key vulnerabilities which plague mobile devices above other types of platforms; their frequent loss and theft, their misuse by employees, and unwillingness by management to take the appropriate policy and enforcement steps to ensure mobile security governance is enforced.

The large variety of mobile platforms, with disparate operating systems installed on dozens of different hardware platforms, imposes an extremely broad and challenging surface to defend. Constant changes in hardware and software configurations generate challenges with data security that is made particularly evident in the mobile arena as compared to the relatively more homogeneous desktop environment. This environment begs the question of whether the conventional wisdom of 'securing the network/platform' remains valid in a mobile environment. An option is looking at the problem from the perspective of the more recently popularized data-centric security architecture.

This paper will examine smartphone platforms in general, making reference to specific examples as necessary to illustrate categories of vulnerabilities. While it does not intend to provide an exhaustive taxonomy of specific threats, it will capture broad classes of hazards and propose enduring best practices to prevent and recover from mobile device security incidents.

2. The Mobile Threat Environment

The mobile device threat environment is not only growing in terms of raw numbers of personal users, but in penetration into the corporate environment. Only a few years ago mobile data devices were primarily in the hands of business executives and early

adopters. Now mobile data usage is trending into the mobile workforce; sales, management, service and nearly anyone who leaves the office. Remote connectivity is being used for all major classes of enterprise applications which portable laptops have been employing in the field for years; inventory management, sales, client record management, email and voice communications. The difference is that while laptops run familiar operating systems with similar application sets to the corporate office workstation, mobile devices run rapidly evolving and heterogeneous operating systems whose security has yet to be rigorously proven under the spotlight of focused hackers and security professionals.

As mentioned, the diversity of handsets, operating systems and their configurations, installed software and service providers makes establishing a security baseline drastically more challenging then even a heterogeneous Windows/Unix desktop environment, where mature security best practices and thorough expert knowledge exists.

A small survey of technically savvy group of security professionals revealed that "the type of unprotected data being carried would have serious repercussions to the organization should it be misplaced – from intellectual property (67%), customer data (40%) and employee details (26%)." (Sacco, 2007). There are certainly few individuals who carry this much data on their mobile devices, but increasing connectivity and integration into corporate networks means that a vast amount of data could be at risk by virtue of the less-secure portal into corporate systems potentially created by mobile devices.

In "The Top Cyber Security Risks" (SANS, 2009), the authors identify client-side

software as the number one current security vulnerability. The key takeaway is that while OS vulnerabilities have historically led in terms of exploit development, hackers are now focusing their energy at exploiting the vulnerabilities of applications such as Adobe Acrobat, Flash and MS Office. While these trends are particularly visible on the desktop front, it is likely that as mobile devices become more and more application centric, this attack vector will continue to develop. Indeed, the recent 'jailbreak' of iOS v4 was attributed to an issue in the way PDFs were rendered on the device, rather then some deep kernel or network stack level exploit.

Despite many proofs of concept and increasing research, hackers have thus-far largely ignored mobile platforms; a trend which is consistent with the evolution of hackers' motivation over the past decade of so. Whereas hackers were once inspired by curiosity and personal notoriety, the motivations have shifted almost completely to financial gain. Some common monetization methods have been the harvesting of massive worldwide botnets and mass theft of credit cards numbers and banking credentials. This ongoing large-scale theft of financial data can effectively 'harvest' more credentials then can currently be exploited or sold. As the idiom goes, "necessity is the mother of invention" and so far, there hasn't been a strong need to exploit mobile devices for use in botnets of for the personal or corporate information stored within. With the significant increase of data speeds and always-on connectivity, the former becomes more palatable as a means to leverage the world's hundreds of millions of mobile devices to send spam or launch denial of service attacks. The latter leaves to be proven, but as users entrust more and more valuable data to their phones, they can only become more desirable a target to cyber criminals.

A recent study of security professionals found that less the 2% had encountered a "serious incident" arising from a mobile device (Help Net Security, 2010 a), yet one third of the same respondents cited mobile wireless security as crucial, and one of their highest priorities. While the seemingly disproportionate reaction may be the effect of several factors (not the least of which might be hype and F.U.D (fear, uncertainly and doubt) by the security industry and press, this paper will strive to examine those threats and make sound recommendations, enabling security professionals to make informed investments into wireless security for maximum effect.

In the coming sections, I will broadly classify mobile threats into three categories: those resulting from the physical nature of small and highly portable mobile devices, those stemming from their ubiquitous connectivity and those originating with the prevalence of mobile software applications and malware.

2.1. Physical

The number one unique threat to mobile computing it physical loss or theft of the device. In a recent Pointsec survey (Bancroft, 2008) it was revealed that 85,000 mobile phones and 21,000 PDAs and smart phones were left on taxis in Chicago over a 6-month period. The seriousness of the impact of ease of loss of these tiny devices is exemplified time and again in the media with stories of lost devices (mostly laptops at this time) which resulted in the loss of millions of records of personal information. (Privacy Rights Clearinghouse, 2010)

The threat of actual data compromise following a device loss or theft depends on several factors; as many of the lost phones will be found by individuals who have no

interest in compromising the data within. The ease by which they can access the contents of the device and the ability to identify the possible value contained within are the primary factors in protecting data in this case. A worthwhile practice would be to include a contact telephone number or address labeled or permanently etched on the device, but not to give away the organization, or personally identifiable information. The mention (and follow through) on a sizeable reward should be strongly considered and mentioned on the label. The value of the reward should be measured against the true cost handling the loss incident; man hours, loss assessment, legal implications etc., and certainly be well above the market value of the device alone.

Assuming a subset of thieves and 'finders' of lost devices are at least somewhat technical and will be curious, it is likely some level of effort will be applied towards accessing the device. Phone-based attacks can often be foiled through use of challenging login pins and max-attempt lock out policies. It is shocking that in a survey by Credant Technologies (Credant Technologies, 2009) 56% of IT professionals admitted to not using a password on their smartphones. This most basic precaution being ignored by a particularly tech-savvy demographic goes a long way to support the requirement for centrally managed policy-based mandatory pin policies that may not be disabled at the user level. Policies should also be applied to ensure a short timeout before which the lock screen appears on the computer. As most smartphones now use a common USB interface, it is not unlikely that an enterprising individual will attempt to connect it to his or her computer. Auto mounting of the device should be disabled and important data at rest should be encrypted. There is a risk that casual finders divulge protected information, if it is of obvious value. There may be a sense of responsibility triggered to report that a

device belonging to (for example) a Government organization, holding personal records was handled and secured so poorly.

A smaller subset of thieves may have the skills and motivation to attack the device with specialized software or techniques. For example, it was recently shown that by mounting an iPhone via USB to particular computer operating systems would create a race condition that would allow the viewing of a large part of the iOS file structure. This was shown to be the case whether or not the iPhone's passcode lock was enabled. (Marienfeldt, 2010) A variety of phone forensics systems allow the motivated attacker to extract data from a device, even bypassing the screen lock in some cases. This raises the bar and reinforces the need to encrypt valuable on phone data as a matter of policy.

There is also risk of non-theft related misuse of the phone. A user may, for example, allow a family member to use his phone to get on the Internet or play a game. This may give an unintended user access to data or applications to which they are not authorized. Anyone who has seen a child inadvertently dial 911 can empathize with to the risk of accidental data exposure or device usage. In addition to user education, best practices may include application and data-level security, requiring additional authentication at time of access - beyond simple phone log-in.

Something of a devil's advocate, Marnix Dekker, an application security developer is quoted as saying: "A smartphone is a much more personal device then, for example, a desktop or laptop computer. You carry it around on your person, and rarely leave it unattended. In this aspect, it is a much more secure device than a PC." (Zorz, 2010) While this may have some merit, clearly the risk of data loss increases when dozens of

copies of corporate data exist in personal portable devices, as compared to physically centralized in a typical perimeter-defended enterprise network. Certainly the opportunities for physical access to computers in a locked building are less then those of mobile devices. Indeed many of the risks brought on by mobile computing exist because of their biggest benefit; portability (ISACA, 2010).

A point worth noting is the Subscriber Identity Module (SIM) card, which is generally removable from the device. These cards may hold subscriber data, contact lists and SMS messages and should be considered in mobile security policy. Devices should be managed such that these cards do not store any non-essential data, as any data stored can be easily read by anyone with access to the physical SIM card.

2.2. Mobile Network Security

One of the challenges of mobile device security are the numerous types of connectivity available on a current generation smartphone. The attack surface is broad and encompasses a trove of possible attack vectors. Not only do these devices possess cellular data capability, but also many have WIFI, Bluetooth radios and other specialty communications systems. When considering smartphone security, each one of these elements should be considered and addressed appropriately. Unlike locally constrained exploits (Bluetooth, Infrared, RFID) in which a user is vulnerable to people in his general vicinity, web tethered devices are a security game-changer as they are susceptible to being detected, scanned or otherwise attacked from anywhere in the world.

Cellular. A smartphone generally connects to the cellular network using one or many mobile phone technologies. It may transmit voice and text messages via legacy

(Global System for Mobile Communications) GSM means, while maintaining an always-on data connection via a Enhanced Data rates for GSM Evolution (EDGE) /High-Speed Downlink Packet Access (HSDPA)/Evolution-Data Optimized (EV-DO) connection. It is commonly known that the foundation stream ciphers employed in widely used GSM networks (A5/1, A5/3) are weak and broken. Most smartphones are built to support multiple RF bands and generations of technology, for ease of roaming on a wider range of networks. This may allow the possibility for a villain to somehow force a handset to register with a less secure protocol then it would normally choose; one which the eavesdropper can easily decrypt. It has been demonstrated (Nohl, 2010) that a hacker can create a malicious cell-site and locate it near the target phone the phone will then forward all traffic through it, allowing complete interception of voice and data streams. Capturing and decrypting voice and data connections however still remains non trivial, requiring a skilled and motivated hacker targeting specific users. This threat is worth noting, but remains at this time largely in the realm of a 'possible but unlikely' threat to most organizations.

SMS. A popular service protocol within the GSM standard, the Short Message Service has long been considered generally harmless. Misuse of SMS often amounted to nothing but unsolicited SMS spam directed at user handsets. While the most common use of SMS is messaging, the underlying protocol, Wireless Application Protocol (WAP) provides the ability to send network and phone configuration details over the mobile phone network. In their paper (Miller & Mulliner, 2010), the authors showed how techniques they developed to fake or 'inject' the transmission of SMS within a phone's protocol stack allowed them to send massive amounts of 'text messages' and permitted

them to bombard the phone with thousands of permutations of non-standard message formats. This technique, known as fuzzing, revealed certain cases when a particular message would result in a crash or some other unexpected outcome that can be leveraged to deny service to the phone user, or possibly inject malware onto the phone. The recipient's phone can even be hacked while in ‘sleep’ mode, and the exploit can be leveraged to retrieve the phone’s unique identification numbers, personal information or other data stored on the device. Variations of the hack are effective against Windows Mobile, Apple iPhone and Google Android. At the 2009 Blackhat conference, Miller showed how he could send a malformed SMS message and crash the recipient iPhone, generate a denial of service on the recipient handset, or execute arbitrary code. A potential weakness is that SMS messages are generally not blocked, firewalled or examined by network intrusion detection systems, and thus could constitute a simple circumvention of the best laid network security plans, providing a means through which to infect a device with malware while completely circumventing IP network connectivity and any protective measures in place. "SMS is an incredible attack vector for mobile phones," said Miller, "All I need is your phone number. I don't need you to click a link or anything." SMS remains largely unexplored and may, under scrutiny, reveal even other security vulnerabilities.

SMS is employed in some two-factor authentication schemes as a means to provide the user with a time-limited login token, supplementing the password he knows, with a second factor, the phone he physically has. This concept certainly makes sense as users often carry their mobile phones, but as SMS vulnerabilities become more prevalent, it would be wise to consider a more secure transmission medium for these one-time

authentication passwords, perhaps a messaging band that itself provides some measure of originator authentication.

Bluetooth. Bluetooth technology is most commonly used for connecting simple accessories such as headsets and audio headphones to mobile phones. Due to this seemingly innocuous usage, most users do not bother securing it. The protocol was created for Personal Area Networking, and has the ability to provide data access to the device and bridging connectivity to the device's other connected networks. Not unlike the exploitation efforts against SMS described above, hackers (Mahaffey et al, 2009) have designed a mobile framework they call Fuzzit that allows fuzzing 'testing' against various mobile phone communication protocols. Tools such as this may provide hackers easy access to a multitude of new, previously undiscoverable vectors over any of the wireless protocols discussed

WIFI. WIFI security threats are well known and multiple vulnerabilities have been published. These include severe weakness in WEP protocol encryption and man in the middle (MITM) attacks. Should a WEP network password be cracked, or a mobile phone connect to an open WIFI hotspot, the entire range of threats typically aimed at portable computers become relevant. In particular, MITM attacks launched at a number of vulnerabilities allow the opportunity for an attacker to inject himself in the data stream of a mobile device's network connection

Increasingly, mobiles are used to access corporate networks, exposing the so called "mobile security blind spot" (Skuler, 2009), the time in which a mobile device is disconnected form the corporate infrastructure and therefore is not synced with the latest

patches and security policies. In the blind spot, it is also impossible for the device to report it's own status, should it have been physically breached or stolen.

In Impersonation Attacks on a Mobile Security Protocol for End-to-End Communications (Dojen et al, 2010), the authors describe how crypto systems running over non-secure channels such as the internet or wireless networks can be exploited by impersonation attacks; these techniques could involve an attacker impersonating the initiating station, the destination host or a trusted third party to the communication. The technique they describe shows how weaknesses in typical communications protocols mean it is possible for an attacker to inject his own forged credentials in the authentication chain and become a trusted party to the communication. In practice, many types of man-in-the-middle attacks are possible over wired and wireless networks which reinforces the need for end-to-end encryption, such that a third party in the communication cannot access the protected data.

The unlocking or "jailbreaking" of iPhones in particular has been shown to open gaping vulnerabilities. Users intent or gaining more control over their devices effectively hack their own devices permitting them to apply patches that disable manufacturer and network operator controls. In the process, many of these jailbreaks open up root-level login accounts with default passwords and the phone begins broadcasting the availability of a remote SSH login service - useful in some cases but highly dangerous should the user not know enough to secure his root password. Typical SSH login attacks can be carried out by any device sharing the same WIFI network, as they would against any platform; and for the most part unobserved. The act of hacking a phone as described above also permits unsigned code to execute on the device, which makes a successful

malware installation far more likely and gives any malware root access to perform any manner of trouble.

2.3. Malware

It has already been established that mobile devices are in effect tiny, always connected personal computers; along with all the power, functionality and risks that come along with that distinction. The previous section on mobile network vulnerabilities outlined several weaknesses these devices have due to their connectivity, but these vulnerabilities are usually a means to an end. Malware can take root through any of these vulnerabilities and quickly 'own' a mobile device, as it would a desktop. There are a range of possibilities, from malware stealing personal and business data, to hijacking the device's connectivity; either to deny service to the user, or act on behalf of the hacker, for example to contribute to a distributed denial of service attack (DDOS). The latter example may currently be somewhat less tempting to hackers as the limited network throughput of mobile devices will be less effective when sending DDOS or spam traffic, for example. Mobiles however have the ability to bridge network modes and send SMS spam, for example, at the request of a WIFI/IP-connected bonnet.

As phones become more sophisticated and fully featured, the user's expectations will be to use them not only for business but for web surfing, banking, photography, and to run apps. There will be increasing pressure by users not wanting to carry a personal and a business device, or requesting to have the business device opened up to personal, lifestyle and entertainment applications. As with computer workstations user permissions should allow only authorized applications to be installed on the device, as unauthorized

apps are an easy threat vector for malware to piggyback into the system. Mobile management systems should perform routine audits of installed apps to verify no illicit applications have somehow been installed.

Some examples of existing mobile malware include:(Mobile Antivirus Researcher's Association, 2006)

- Mabir/Cabir virus: can infect Symbian OS via Bluetooth or SMS
- Dampig trojan: corrupts the system's uninstallation settings
- Commwarrior: tries to disable antivirus software
- Frontal virus: causes a total system crash of the phone

Individual variants of malware currently in the wild have been shown to effectively infect multiple types of platforms and spread through SMS/MMS, Bluetooth, or by SD flash memory card. Instances have been identified of malware subsequently infecting Windows workstations with a crossover trojans when synced with the mobile device.

At a recent hacker conference, researcher Jon Oberheide showed how he created a malicious application that he passed off as a collection of photos from an upcoming movie. It was downloaded by several hundred people on the first day, and brought along a rootkit that could contact a control server and download follow on malware. (Help Net Security, 2010 b) This proof of concept highlights a key vulnerability of mobile devices, the general lack of concern in the authenticity and trustability of applications that users will install with a few finger touches. Much of the hard fought healthy paranoia which has been drilled into user's consciousness with regard to their desktops are quickly

forgotten in the move the mobile environment.

When writing and distributing malware for any platform, what's most important to hackers is scale; if they write and inject their own malicious app it might only get downloaded a few thousand times.. if it self propagates like a worm, it could infect and 'own' thousands or more.

The smartphone market is dominated by 4 main platforms: Symbian (the most popular outside the US), iPhone OS, Windows Mobile and Google Android. Each platform poses its own challenges to the hacker and their widely varying security postures make any widespread cross-platform malware very complex. Even within the 4 platforms, wide differences in installed OS versions and vendor/carrier customization of operating systems add layers of complexity to successful large-scale exploitation.

Despite the viruses listed above, many of which are proofs of concept, the chances of being infected are currently remote (Fogie, 2008). Despite a decent set of security features in place on these platforms, a large minority of users is feeling limited in their free use of their devices. Mandatory code signing in particular is defeated through the so-called 'jailbreaking' process that allows users to install non-vetted (and often pirated) applications. In the case of iOS, estimates are that ~10% of devices are jailbroken, amounting to millions of phones which will run any code, legitimate or malicious, circumventing critical security measures. Indeed, users may be their own worst enemies as they may be creating a fertile bed for a future piece of malware that will take advantage of the largely neutered security environment they've produced on their devices.

Sandboxing techniques implemented by Apple and Google makes life harder on hackers, as they are designed to isolate the operating environment of individual applications. Open platforms and user 'jailbreakable' platforms have the potential of opening holes in the sandbox through negligent user behavior; either by inadvertently installing malicious applications or by clicking on 'allow' dialog boxes and giving unintentional access to malicious processes, as with traditional operating systems. Indeed, many 'baseline' applications shipping with the device may run as 'root', giving a successful app-level exploit full access to the device without the need for additional privilege escalation. The converse effect is also true; since the sandboxed environment prevents cross application interaction, it also increases the technical difficulty for security companies trying to develop anti-malware apps which are able to monitor all other running applications as well as the network stack, memory etc. According to a 2009 survey (Goode Intelligence, 2009), only 13% of users were running anti-virus/malware software. It is impossible to conclude how this is aggravated by system sandboxing, general lack of understanding of the risk, perception of low risk or simply user apathy.

It is worth noting that there is an industry of 'deliberate' spyware. Software packages such as Mobile Spy and Flexispy, marketed as means to monitor cheating spouses and employees, are available for most smartphone platforms. These packages exhibit the same features of malicious malware such as the ability to capture SMS messages, call logs, GPS locations and make recordings of voice calls. Anything that is possible through the use of this 'legitimate' software is also possible to an unsuspecting user.

A final consideration is whether mobile operating systems allow the user enough

situational awareness to truly understand the security risks he is facing. As very GUI centric and app-centric environments, there are virtual blinders put up such that the user generally doesn't see the underlying operating system, and many interactions he may have with a desktop system are limited or hidden altogether. While this construct may be partially necessary due to the simplistic user interface required by a smartphone, it is worth asking if too much is hidden from the user, causing too much trust to be placed in the system.

3. Emerging technologies for protecting mobile systems

Having looked at the many security challenges added through the introduction of mobile services to the IT environment, this section will explore how a paradigm shift of the way we consider security may be necessary to prevent future threats. In a recent publication considering future threats (Northcutt, 2009), the author writes "…to better influence business/compliance strategies - one of which will be to educate our communities that we need to be data centric not equipment, location or infrastructure centric." Indeed, this new approach does warrant attention in the enterprise, and in the mobile-enabled realm in particular.

3.1. Data-Centric Security

Platform-centric security, the current construct of network security in which defense in depth generates 'walled gardens' of security within the enterprise begins to wither when applied to mobile networks. Mobile data networks, by definition and design, necessitate access to core business data anytime and from anywhere, and in doing so,

breaks the normal bounds of security of a geographically fixed and physically secured network.

In their paper, “Elevating the Discussion on Security Management - The Data Centric Paradigm” (Bilger et al, 2007) , the authors develop the concept of data centric security, and describe it as a concept of protecting data, rather then devices. The concept of data-centric security should be quite familiar to anyone who has worked in the Defence industry or similar governmental organization. These groups have long employed the concept of tiered protective measures and access rights through the use of security classification and security clearance. As a matter of practice, files marked ‘SECRET’, for example, need to be stored in approved locked containers, or isolated on secure encrypted networks with no connectivity to the open internet. Indeed, different pieces of information are critical for different reasons; personally identifiable information of clients, corporate financial records and trade secrets all produce different implications should they become compromised. The real paradigm shift in data-centric security is to think of security measures in terms of the impact of a breach in the confidentiality, integrity or availability of every specific file, service, or other piece of data held by the organization. Only then can security measures be emplaced to protect the varying levels of data as deemed appropriate to its importance.

A simple practical example for the sake of comparison would be: in a platform/network centric security model, a user may have access to his entire corporate network through a single-factor-authenticated (e.g. password) VPN solution configured on his device. Once logged in, data and applications can be retrieved, run and pushed back to the corporate environment.

Platform-centric thinking defines layers of security so that in the example above: a user logs in to his corporate network using the same VPN. This suffices for access to personal data and sales data, which in this case is classified 'Level 1 - Protected'. Should the user select a 'Level 2 - Confidential' file or application, he would be required to authenticate using a second factor (e.g. his password and a one time PIN from a physical token). This additional authentication allows for the decryption of the file via a Public Key (PKI) Infrastructure service and flags the file as being non-locally-saveable on the device. Should the user request to view a 'Level 3 - Corporate Secret' document, the system might recognize the fact he is on a mobile device and deny the request altogether.

While this example discusses applying data classification meta-data to each file or application, this construct can, and should be moved down to the lowest practical level; each field in a customer information database can easily carry a classification tag, even fragments within a file can be flagged as being sensitive and treated separately from the remainder of the file.

In "Data Centric Security: Enabling business Objectives to drive Security" (Bilger, et al, 2006) the authors outline key classification questions when preparing for a data-centric security strategy;

- Where did the data originate?
- Who owns the data?
- Who controls the data?
- Who or what holds the data?
- What type of data is it?

One can then outline controls that can be applied to individual pieces of data;

- Who or what can use the data and for what purpose?
- Can it be shared, and under what conditions?
- Where will the data be kept and for how long?
- Does it need to be safeguarded at rest, when backed up, and/or during use?
- How can the data be disclosed?
- What subset can be disclosed?
- What protection must be implemented?
- Does the data need to be distorted or watermarked?

Instituting a multi-level data-centric model ensures the least amount of user hassle for most common data, and increasingly stringent requirements as the data becomes more sensitive. As with all security controls, a balance must be struck between the requirement for thorough security practices and usability. Depending on the technological implementation of data-centric security, the user may be required to (Talmor, 2010) answer some or all of the above questions, when saving a new piece of data. At a minimum they will have to select a permissions group (e.g. 'Finance') and a sensitivity level (e.g. 'Level 2 - Confidential)

A properly implemented user interface can make these steps largely transparent, and can default to commonly used values to minimize user interaction. Still, a successful system hinges on the user's participation in defining the protection requirements of a given piece of data or document. This workflow step cannot be circumvented, or a lazy user would opt out. Once data has been meta-tagged once however, the system can recognize the security requirements and apply the requisite protective measures automatically. Alternatively or collaboratively, software can scan the contents of a file

and assign a classification based on content recognition. This approach has flaws, but may be workable in certain data environments. Naturally, any data being entered into a database would assume the classification and releasability of the field in question and require little to no user interaction.

Any degree of security policy may be implemented based on the threat-risk assessment conducted by the organization. If it is considered overly risky, consideration should be given to data generated on the mobile device. While these mobile devices may not be used to generate long pages of textual documents, many have the ability to take photos, complete with geotagged location data, or record voice and video. Even the phone call register, contacts and calendar items of key executives may require scrutiny and necessitate some measure of attention.

3.2. Data Loss Prevention

Data Loss Prevention (DLP) is another emerging technology that shows promise in addressing some of the issues raised by mobile platforms. Vendors use several terms to refer to DLP technology: Information Leak Detection and Prevention (ILDP), Information Leak Prevention (ILP), Content Monitoring and Filtering (CMF), Information Protection and Control (IPC) or Extrusion Prevention System. Whatever the name, DLP is concerned with actively monitoring and protecting information at rest and in transit on a network.

DLP and data-centric security complement each other in many regards. The field or file level tagging of data with classification and permission markings allows DLP software to easily recognize data and control its flow as it travels through the network.

While ‘Level 2’ data might be allowed to flow freely anywhere on the geographically local wired corporate network, it can be prevented from transiting out through VPNs gateways, email servers, web browsers or other common modes of data exfiltration. Several DLP vendors recognize the stigma of employees feeling like they will be disciplined for making honest mistakes, and offer self-remediation features. A user might receive a pop-up which allows her to cancel the action she just initiated: “Are you sure you want to copy this Confidential file to this USB device?” or “Do you really want to email this data to an external email account?” This type of system educates the user, ensuring fewer involuntary accidental data breaches and reinforcing policy.

DLP can also allow an organization to maintain a positive inventory of each copy of protected data and manage the information’s lifecycle as it is created, transmitted and securely deleted. DLP products can operate, as describe above, as network based devices ‘sniffing’ layer 3 for particular traffic, or at the host level, sniffing individual workstations or mobile devices. A host-based client can inspect data as it is entered into local applications such as chat clients or encryptable email, where it might otherwise go undetected through a network layer device. DLP can also be set to search host inputs or network traffic for particular data, for example recognizing the format of a credit card number or financial record. While this can be useful capability, in practice accuracy may be highly variable based on the maturity and testing of the rule set. A poorly vetted rule set may correlate many false positives and negatives.

Data-centricity is a useful model for consideration when deploying mobile networks. With correct configurations and policies it can effectively address the data-at-rest issue of valuable information on lost mobile devices by either forcing immediate

secure deletion (self-destruct) after a short period of inactivity, or by not allowing it to be downloaded in the first place. Other technologies on the forefront are permitting creative solutions to this issue, while possibly injecting other challenges. For example, the availability of mobile broadband connections makes off-device (cloud) computing possible. A thin-client model can be employed over which only the screen image of the data is pushed to a mobile device in real-time, rather then the data itself. A remote desktop/VNC type connection to the core network can in this way simplify the playing field; a single application to secure on the handset, a single tunnel to the network, and volatility of the data the moment the connection is torn down.

A challenging question is in what manner an organization should implement security during inevitable mobile blind spots. Often, work still needs to be conducted out of wireless service areas. In these cases, very careful consideration needs to be given to ensuring only the minimal data required is stored locally on the device, based on predetermined confidentiality parameters. Encryption and deletion measures need to be emplaced to ensure high confidence of data-breach prevention should a security incident or device loss occur.

There is still much research to be conducted on these emerging technologies, but the trend is clear; more focus is required on securing the data, and less trying to build impenetrable perimeter defenses.

4. Mobile Incident Handling

The incident handling (IH) process (Fig 2) is well defined and broadly accepted in

the IT security world, and its six core steps will likely be familiar to many readers. It is an evolution from simple incident response, which focused only on reactive steps while ignoring prevention and lessons learned. As a whole, the system describes a formal workflow through which an analyst moves while preparing for, reacting to and learning from security incidents. Throughout the process, there is a strong emphasis on documentation, as this enables the critical final step of putting the experience to work addressing the root cause of the issue. As with more typical IH situations when well considered but rapid action is key, this is particularly true in the case of mobile system incidents, where significantly more of the incidents will involve the physical loss of a device. Speed is critical in minimizing lasting damage to corporate data and reputation.

Figure 2 - Classic Incident Response Model (CNSS, 2007)

This section will look at the typical IH process in the context of mobile security incidents. As previously discussed, mobile devices are becoming more like desktop workstations in many ways and are sharing some of the same vulnerabilities. The focus here will be on the particularities of mobile platforms and the challenges they bring to the standard way of thinking about IH.

4.1. Preparation

Preparation is the step where the majority of the work and time is invested, but also has the potential for the greatest payoffs in terms of return on security investment. The employment of best practices on your mail server and backend mobile management server can prevent many common security issues for a fleet of centrally managed mobile devices. The installation of anti-virus or anti-malware software directly on the device is also a possibility, if supported by the platform. Ensure consistent and timely rollout of security patches prevent exploitation from recently discovered vulnerabilities, although the platform may dictate the ease at which these can be rolled out.

Just as important is the preparation of supporting technology that will be connected to the devices. If the user will be syncing the device to a PC, proper security practices must be employed in it as well, as malware can be passed from one to the other. Backend support servers must be given consideration; Blackberry Enterprise Servers (BES) should be configured to take into account key configuration best practices. Microsoft System Center Mobile Device Manager servers and Exchange servers should be considered and configured to disable non-essential services and to cleanse mail messages from any possible spam, malware or nefarious links. WIFI-hotspots setup for enterprise mobile device use should be secured, as they can provide a wide open backdoor into an otherwise tight security perimeter. Devices themselves should be configured to only connect to trusted WIFI sources and not to just any open WIFI hotspot. If access to open or non-corporate access point is required, all data should be routed through encrypted VPNs for protected communications to the corporate infrastructure. Bluetooth headsets must be configured with complex and non-default pins to minimize the risk of

bluejacking/bluesnarfing. Key tasks for mobile device incident handling include:

- Perform a threat-risk assessment, and follow through - Consider the true value of what could be lost in a data breach and implement countermeasure and mitigations technologically and procedurally. The right mix of layered security and data-centric approaches will likely complement each other and ensure resources are applied to greatest effect, protecting the most critical data.
- Build your incident response kit - Ensure you have the cables and software installed and tested on your incident handling workstation. If employing a forensics tool such as Paraben or CELEBRiTE, ensure you've tested it with each device type and configuration and that you can extract data as required. As they don't all provide the same degree and breadth of analysis, ensure your choices of tools overlap and complement each other. Consider SIM and SD card forensics measures in addition to handset investigation tools.
- Prepare clean backups of recovery images for all platforms and review them regularly to ensure patch levels and application versions are up to date. These will greatly simplify the Recovery phase.
- Perform threat modeling - Consider all manner of possible incidents as outlined in section 1. Ensure clear processes exist for handling each step of the handling procedure for each type of device, from device loss scenarios and malware infection.
- Practice your processes and identify procedural or technological shortcomings, and resolve or work around them. Involve management, legal counsel and IT system administrators as planned to ensure they are familiar with these events and

the role they may be asked to play

Any security system will succeed or fail on the backs of the users. Ongoing training is critical to ensure understanding of the necessary limitations of their mobile devices and to securing buy-in from the users. It is only when users fully realize the true value of the data they are carrying that they will think twice about circumventing controls or policy.

4.2. Identification

It is during the identification phase that security events are logged and analyzed to determine if a security incident has occurred. An organization's identification process needs to take into account multiple levels of event detection; the network perimeter, the host perimeter, host-level and even data-level in a data-centric system. Normal IDS, IPS and firewall solutions will allow some measure of network perimeter identification, but mobile device host event detection could be challenging, unless properly configured mobile security software is installed on each device.

User training and awareness is key for early identification of mobile security issues. Whereas network/malware related issues may be detected centrally as they are on desktop platforms, many mobile security events/incidents may require user identification. Loss of control of a device or suspicious behavior needs to be reported early to allow responders to minimize exposure risk. Data-centric systems may have the benefit of positive data tracking, which may report specific data leakage (e.g. "A user has sent confidential data to an external email address" or "Document X has not been confirmed deleted by Device Y, as per a given policy.")

Security incidents may be reported directly by a user with a lost or stolen device, or

complaining of some non-typical behavior of his device. Awareness training conducted with users, administrators and help desk technicians prior to an incident will greatly increase each party's ability to recognize an incident when it happens.

Thorough documentation becomes imperative at this stage, and should include details of the original security event report and all follow-on analysis. Security management should develop and communicate incident identification processes in policy and make it simple and non-threatening for users to report suspicious indications and warnings of possible issues.

4.3. Containment

The goal of containment is to prevent additional harm to the network or loss of data. The major factor when dealing with mobile incident containment is the availability of the device. Unlike in server-based incidents, where a decision must be made at this stage whether or not to leave the system in operation due to critical operational service running, mobile containment should generally allow investigators to immediately seize the device and take it offline, preventing additional damage.

If it is physically available, it is recommended to isolate the device from the network immediately, to ensure that any threat that may be resident on the device is neutralized through physical segregation from the network. An RF-shielded Faraday bag may prove useful in these cases, as the device can remain powered up while investigators can be assured that it is not being changed remotely by malware, a hacker or even normal device management policy 'pushes' over the network. Assuming the device is available, forensic/investigation tools will generally allow imaging of the entire phone system and

data. In some cases, such as with certain versions on iPhone, full forensic imaging is not possible and a logical image will be a necessary compromise. Mobile forensic imaging is a complex field of its own and is outside the scope of this paper, but a few of the key mobile forensics techniques include:

- Ideal forensic acquisition is a full memory dump, which may be difficult in some cases. This process would include unused space and deleted files. Forensics packages such as EXACT, CELEBRiTE, and Paraben can provide full acquisition of many devices.
- Logical acquisition is useful, even if you get a full physical memory dump. The logical dump gives you the file structure rather then just a large blob as provided by a full dump. Each toolset, based on its features and acquisition method will capture a different set of logical files. If employing several tools, ensure file metadata matches between tools.
- SIM card forensics. Recovery of call logs and contacts from a device SIM card.
- Manual examination, or physically operating the phone, can be useful to verify details and completeness of a logical data dump.
- It may be necessary to conduct subsequent forensics on any computers/servers that the device was synchronized to. The workstation may contain backup images of the device, while a server's logs could reveal helpful entries about related network traffic to and from the device.

Once all possible data has been acquired, sound forensics methodology with thorough documentation will ensure the best possible understanding of cause and scope of the incident. The image can be compared to a known good image to determine changes

to system file integrity unusual registry keys, log entries or processes. While specific techniques for mobile device forensics is outside the scope of this paper, there are many excellent courses and books on the topic.

If the device is lost or stolen, a different approach is required. A necessary capability is a remote secure wipe of all data and settings on the phone. Your initial risk assessment performed during incident identification will educate a decision whether this is immediately required, or if device recovery should be first attempted. The remote wipe feature should provide the functionality of reporting an acknowledgement just prior to resetting itself, in this way you can be assured the wipe command was received and carried out. Device recovery may be desirable in cases where the risk of data breach is lower then the value of the unit. Several services including Lowjack and Apple MobileMe 'Find my iPhone' can help locate a device via GPS, and recovery may be possible in collaboration with local police.

Whether or not the device is present, it might be useful to contact the service provider and request all available data regarding the device; service logs of recent calls and other network activity can be helpful in identifying if a lost device has been breached, or if SMS messages (or other traffic) have been sent by malware. It would be wise to build a relationship with the service provider during the preparation phase, to clarify what information is available and how to go about requesting it.

4.4. Eradication

Eradication in a mobile device context is relatively simple. As most of these devices are easily imaged from backups, this is the preferred method for recovering from

nearly any incident. Indeed, if very little or no data is stored on the local device, the reimaging will re-establish a known-good baseline in minutes with virtually no risk of follow-on infection.

Typically, mobile devices storage is divided into two parts, an 'imageable' read-only partition for OS files and a user partition for applications and data storage. A complete device restore will wipe the entire device, thereby removing any chance of lingering malware. While there are known rootkits on mobile devices, there are none known to survive a complete device restore. It is therefore important to perform a restore and not just a recovery from a backup of the user partition.

The Eradication phase may necessitate follow-on attention to associated workstations and servers, if the device was synced or backed up while infected, these backups may be similarly infected and need to be deleted. The user's server-side email box and file storage should be scrutinized for traces of malware.

4.5. Recovery

Like Eradication, mobile Recovery is relatively straightforward. Once restored to factory settings, or the latest verified image, and all the appropriate security configurations have been installed, the device should be ready for operations. Depending on the incident or the nature of the data breach, one may consider swapping the device SIM card or phone number and/or issuing a different type of device, if the issue cannot be permanently resolved due to an unpatched hardware or software vulnerability.

4.6. Lessons Learned

Lessons learned are where the greatest value is added to the incident management process. It is only by documenting throughout the process, and analyzing the underlying meaning of all these notes that true intelligence can be gathered and applied.

The Committee on National Security Systems has proposed an alternative to the classic, linear incident handling process (Fig 3). They argue that often organizations may not work through the entire process, and therefore miss the critical reporting/documentation and lessons learned gathering. Instead, they propose a cyclical adaptation through the steps, with focus on the prevention and constant feedback throughout all steps of the process.

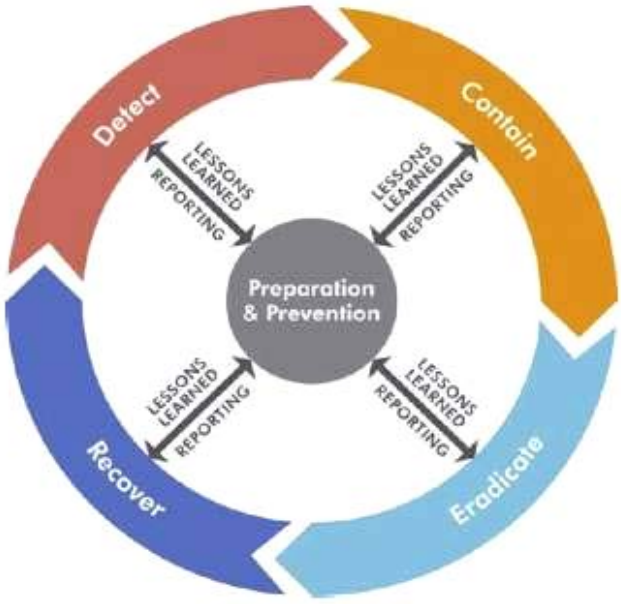

Figure 3 - Incident Management Model (CNSS, 2007)

This cyclical methodology makes sense in any environment, but particularly so in

the mobile environment as varied platforms and handling processes may be less familiar to IH staff. It will ensure that the incident management team will learn all they can about what caused the problem and feed back the appropriate recommendations to ensure the vulnerabilities are minimized going forward. It reminds the handlers to always be thinking about prevention and bettering not just internal processes and security technologies, but the incident handling process itself.

5. Conclusion

These highly connected and powerful portable communications devices are clearly here to stay. All signs point to an ever-increasing use of smartphones in replacing portable and desktop computers for many tasks. Most security conscious enterprises have had many years to develop robust security policies and implement technical and procedural measures to ensure security in the relatively controllable office paradigm. The rapid shift to the mobile model demands thorough data-centric threat-risk assessments, incident handling planning and preparation and user and administrator training. A holistic analysis of the mobile threat environment, giving appropriate attention to threats generated by the unique portability of the devices themselves and by their highly connected natures is necessary in any environment considering placing sensitive data on mobile networks. At the core of the security assessment and throughout the process of 'selling' procedural and technical mitigation solutions to senior management, the true cost of data leakage must be kept squarely in mind.

Many organizations are unwilling to dedicate time and money securing against threats that have not yet done damage; indeed there are plenty of existing security issues

to deal with on traditional workstations and servers. The unprecedented boom in the numbers of network-connected mobile devices shows growth unlike any other threat vector; each potentially breaches to your personal and business data. The pervasiveness of mobile systems could mean the first significant mobile-targeted malware could steal your core business data or take down your network through the sheer number of network ingress points. It is imperative that security practices are worked into mobile systems and policies as they are being rolled out and written. It is crucial you consider the impact of mobile devices to your incident response process, because incidents will certainly happen.

Effective security planning and implementation, with a focus on the areas of greatest concern can enable, not hinder, mobilization of corporate applications and access to crucial business data, leading to increased performance and productivity. Mobile security is truly a business enabler as it makes possible the powerful use of business data anytime and anywhere, a promise only partly fulfilled by decades of portable laptops, which really represented portable offices, not data access on the move, any time anywhere.

6. References

Bancroft, M. (2008) The Top 5 Stupid Things People Do With Mobile Phones. Retrieved from: www.csoonline.com/article/464722/the-top-5-stupid-things-people-do-with-mobile-phones. In reference to survey by Pointsec, 2008.

Bilger, M. et al. (2007). Elevating the Discussion on Security Management - The Data Centric Paradigm, 2nd IEEE/IFIP International Workshop on Business-driven IT

Management. In conjunction with IEEE/IFIP Integrated Management.

Bilger, M., et al. (2006). Data Centric Security: Enabling business Objectives to drive Security. IBM 2006.

Committee on National Security Systems (CNSS). (2007). National Information Assurance (IA) Approach to Incident Management (IM). Investment in Detection, Response, and Recovery Technology Working Group.

Credant Technologies. (2009).Mobile Usage Survey at Infosecurity Europe 2009. Retrieved from: http://www.credant.com/news-a-events/press-releases/353-it-security-professionals-passwords.html

Dojen, R.,, Pasca, V., Coffey, T. (2010). Impersonation Attacks on a Mobile Security Protocol for End-to-End Communications. Data Communications Security Laboratory, Department of Electronic & Computer Engineering University of Limerick, Ireland.

Fogie, S. (2008). Mobile Platform Malware Threat Overview. InformIT: Security Reference Guide. www.informit.com.

Goode Intelligence. (2009). Mobile Security 2009 Survey. Retrieved from: http://www.goodeintelligence.com/pdfs/news_release_191009.pdf

Help Net Security. (2010) a. Security pros say serious mobile device and social network breaches are rare. Retrieved from: www.net-security.org/secworld.php?id=9661

Help Net Security. (2010) b. Twilight app turns mobile phones into zombies. Retrieved from: http://www.net-security.org/malware_news.php?id=1383

ISACA. (2010). Securing Mobile Devices. An ISACA Emerging Technology White Paper.

Neilson Data. (2010). Smartphones to Overtake Feature Phones in U.S. by 2011. Retrieved from: http://blog.nielsen.com/nielsenwire/consumer/smartphones-to-overtake-feature-phones-in-u-s-by-2011/

Mahaffey,K., Hering, J., Lineberry, A. Fuzzit: (2009). A Mobile Fuzzing Tool. Black Hat USA 2009

Marienfeldt, Bernd. (2010). iPhone business security framework. Retrieved from: www.marienfeldt.wordpress.com

Miller, C., Mulliner, C. (2009). Fuzzing the Phone in your Phone. Black Hat USA 2009

Mobile Antivirus Researcher's Association. (2006). The Ten Most Critical Wireless and Mobile Security Vulnerabilities. Retrieved from: http://www.net-security.org/article.php?id=927

Nohl, Karsten. (2010) Attacking Phone Privacy. Black Hat 2010 Conference.

Northcutt, S. (2009). 2009 Security Predictions Retrieved from: http://www.sans.edu/resources/securitylab/2009_predictions.php

Privacy Rights Clearinghouse. (2010). www.privacyrights.org

Roche, Robert and O'Neill, Lesley. (2010) CTIA's Wireless Industry Indices, Semi-Annual Data Survey Results: A Comprehensive Report from CTIA Analyzing the U.S. Wireless Industry.

Sacco, Al. (2007). Retrieved from: www.cio.com/article/147000/Study_Average_Value_of_Business_Info_on_Travelers_Laptops_Equals_525K. Based on iBahn/FGI Research's study, April 2007.

SANS. (2009). The Top Cyber Security Risks. Retrieved from: www.sans.org/top-cyber-security-risks

Skuler, Dor. (2009). Eliminating the Mobile Security Blind Spot. Retrieved from: www.technewsworld.com/rsstory/66590.html

Talmore, E. (2010). Data-centric security. Retrieved from: https://www.infosecisland.com/blogview/4249-Data-centric-security.html

Zorz, Zelijka. (2010). Smartphone security risks and best practices research. Retrieved from: www.net-security.org/article.php?id=1492

Last Updated: October 22nd, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS San Diego 2017	San Diego, CAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, AE	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Milan November 2017	Milan, IT	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Amsterdam 2017	Amsterdam, NL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Miami 2017	Miami, FLUS	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Paris November 2017	Paris, FR	Nov 13, 2017 - Nov 18, 2017	Live Event
Pen Test Hackfest Summit & Training 2017	Bethesda, MDUS	Nov 13, 2017 - Nov 20, 2017	Live Event
SANS Sydney 2017	Sydney, AU	Nov 13, 2017 - Nov 25, 2017	Live Event
GridEx IV 2017	Online,	Nov 15, 2017 - Nov 16, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CAUS	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, GB	Nov 27, 2017 - Dec 02, 2017	Live Event
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZUS	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Khobar 2017	Khobar, SA	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TXUS	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, DE	Dec 04, 2017 - Dec 09, 2017	Live Event
European Security Awareness Summit & Training 2017	London, GB	Dec 04, 2017 - Dec 07, 2017	Live Event
SANS Bangalore 2017	Bangalore, IN	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Frankfurt 2017	Frankfurt, DE	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DCUS	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS SEC460: Enterprise Threat Beta	San Diego, CAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, NL	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SEC599: Defeat Advanced Adversaries	San Francisco, CAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Berlin 2017	OnlineDE	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced