Mobile Security Risks

Ch 8

Topics

- Risks, threats, and mitigation strategies inherent to mobile device infrastructures
- Incident response

- Wireless media itself has several inherent risks.

Rogue Access Point

- Unauthorized access point operating in violation of policy or to attract unsuspecting users.
  - May be set up to entice users so that the hackers can obtain user credentials and other sensitive data .
- Often rogue access point named similarly tolegitimate access point.
- May broadcast an SSID similar to a legitimate wireless network.
  - Tricks users into attempting to connect to the fake access point.

Rogue Access Points

- User connects to the access point and authenticates.
  - Then, uses the access point as if it were the legitimate one.
- Often found in corporate environments to circumvent corporate security policies or placed by hackers to use the above described techniques to acquire sensitive data.
- Often seen in settings such as Internet cafés, bookstores, coffee shops, and restaurants that provide free wireless access to its customers.
  - An evil twin duplicates the legitimate wireless network.
- An attacker may offer a rogue access point that has a stronger signal than the legitimate one.

More Rogue Access Points

Figure 8-1
A rogue access point masquerading as a legitimate one

- Often used to carry out man-in-the-middle attacks.
- Figure 8-1 shows a wireless client that has found two different access points with the same SSIDs.
- One is an evil twin.

Denial-of-Service (DoS) Attack

- Variety of methods.
- One method includes sending deauthentication traffic to both the client and the access point in an effort to cause them to reauthenticate.
  - Attacker sniffs connection.
  - Hopes to capture the four-way handshake that WPA and WPA2 use to authenticate the client to the access point.
- When the deauthentication traffic is sent, it disrupts the connection between the client and access point.

DoS Methods

- Another method is to use a rogue access point that overpowers the legitimate one.
  - The transmit power set to a higher level than legitimate AP.
- Also there are devices and software that can be used to travel through the different wireless frequencies, sending disruptive traffic to any wireless network in the vicinity.
- Practice of disrupting signals between clients and wireless access points is called jamming.
- In most countries, jamming is illegal.

Wardriving, Warwalking, and Warchalking

- Wardriving an older practice.
- In wardriving (war walking), a person would drive around looking for unprotected wireless networks, noting details about them, such as location, signal strength, channel, and what type of security they used.
  - While the legality of wardriving isn't always clear, because the attacker may just be surveying the available wireless LANs in the area, actually connecting to them and using them usually is illegal.
- Laws regarding wardriving and connecting to WLANs vary from state to state, and from country to country.
- Warchalking is also an older practice, not really seen much anymore.

Figure 8-3 Preparing to go wardriving

Wireless LAN Security Protocols

- WEP uses very weak and repeating initialization vectors that can easily be intercepted and used to crack the WEP key.
- Because of this, use of WEP is discouraged.
- WPA and WPA2 are considered much stronger security protocols.
  - They can also be exploited through the use of weak keys or easy-to-guess passphrases.
- Other wireless LAN security methods, such as MAC filtering and SSID hiding, are relatively ineffective.

Weak Keys

- Weak encryption keys can help an attacker wage an interception attack on encrypted communications.
- Weak keys have the same effect as weak passwords; if they do not use large, complex character spaces and obscure characters for the password, they can be easily broken.
- Weak keys can be created by uninformed users, or by software that has not been implemented correctly.
- Algorithm used in encryption systems can also affect whether or not weak keys are used.

Encryption

- For example, in WEP, the key is limited in length and also in implementation.
- While WEP uses RC4 as its streaming protocol, it does not use a large initialization vector, and repeats this initialization vector frequently.
  - Makes it easy to intercept and crack the key(s).
- Even in WPA2, a weak or easy-to-guess password can be easily intercepted and cracked.
- Figure 8-5 shows a screenshot of the results of using the Aircrack-ng suite of tools to break a weak encryption key in WPA.

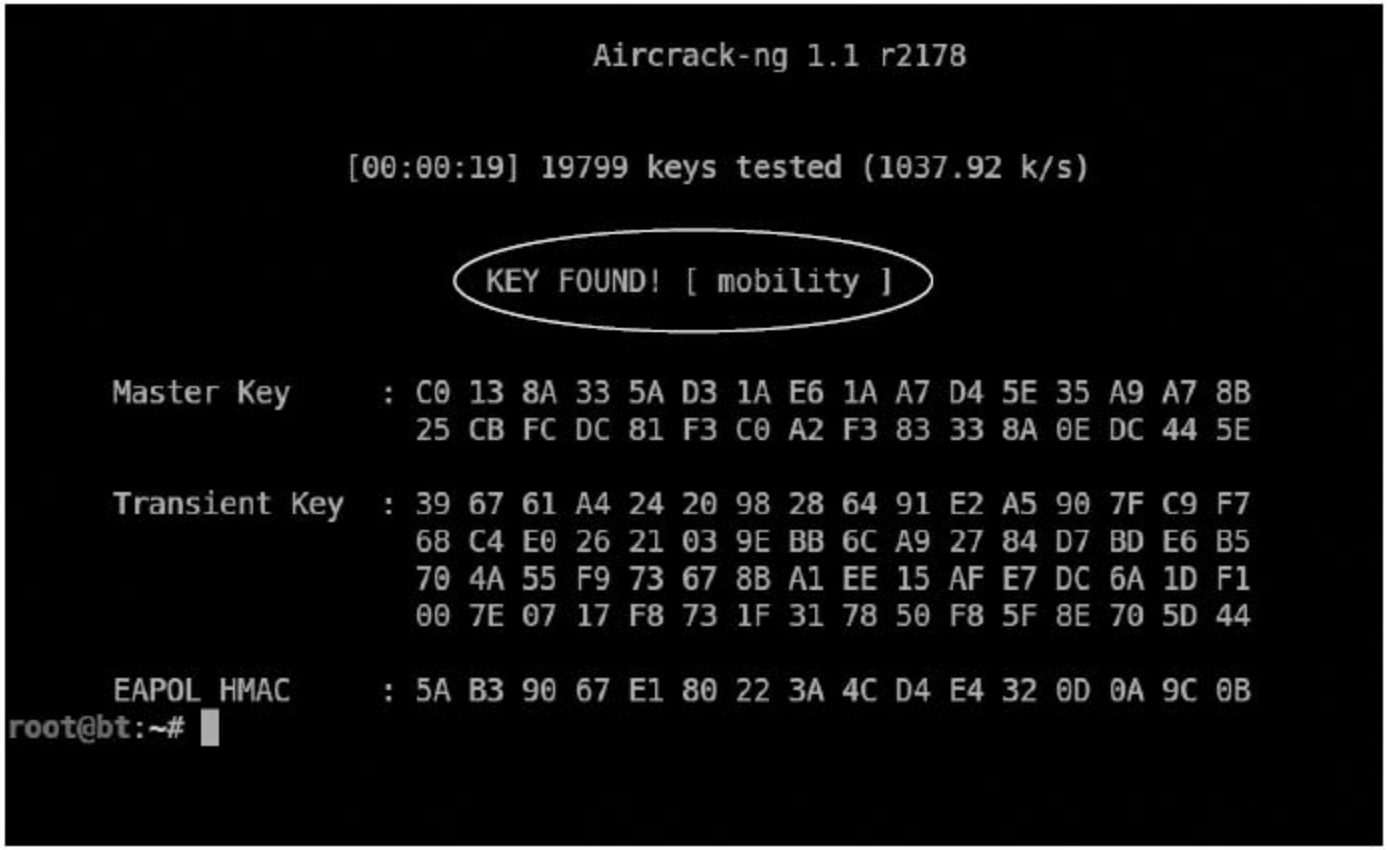


Figure 8-5 Aircrack-ng breaking a weak key in WPA

Man-in-the-Middle Attack

- MITM involves attacker that can intercept communications between the transmitter and receiver.
  - Can be used in several different ways.
- First, the attacker can intercept plaintext communications and either eavesdrop on the conversation or alter any intercepted data before retransmitting it to the unsuspecting receiver.
  - In encrypted communications, somewhat more difficult.
- Typically, attackers take advantage of weak encryption algorithms, weak keys, or a weakness in the implementation.

MtM

- Once the attacker has circumvented the authentication and encryption mechanisms, and entered the communications stream, they intercept traffic simply to eavesdrop, or modify data between the sender and receiver.
- Each user believes that he is communicating directly with the other party, when in reality, they are both communicating with the attacker.
- Because there is another party in the middle, delay in communications can be introduced, and data can be corrupted or modified.

MTM

- Several variations, including shutting one of the parties completely out of the conversation or hijacking the session.
- MITM attacks may be difficult to detect.
  - Although the delaying communication and verifying data transmissions on both ends may indicate that this attack is being carried out against the users.

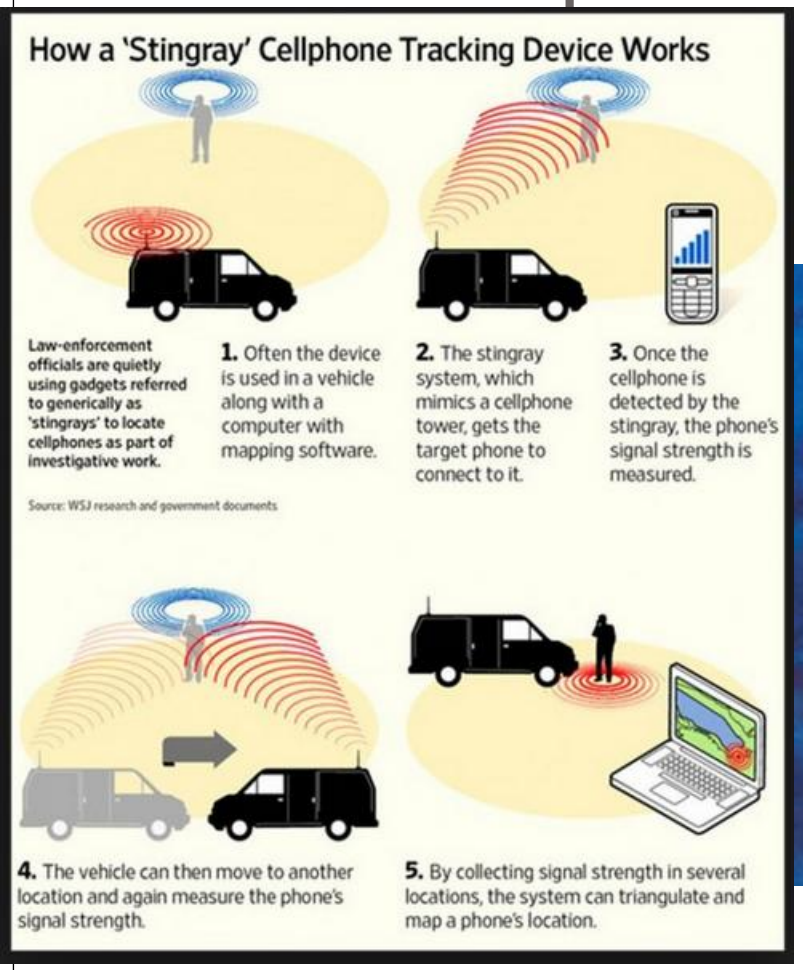
Tower Spoofing

- Involves spoofing a carrier's tower and infrastructure causing a cellular device to use it instead of the normal tower equipment.
  - Requires overpowering the nearest legitimate cell signal, causing the cellular device to lock onto it instead.
  - Equipment used in tower spoofing can also be used to eavesdrop on any conversation, even if it is encrypted.
- In some cases, the equipment can be used to fool the device into turning off encryption completely.

Tower Spoofing

- Equipment required to spoof a cellular signal tower can be expensive.
  - 2010, demonstrations given by security professionals showed how a determined hacker with some resources could purchase the equipment necessary to perform these types of attacks, for under US $1500.
- Law enforcement reportedly using it..
- Since 2010, there have been numerous court cases highlighted in the media questioning the admissibility of evidence obtained from cell signal interception.

Tower Spoofing: Stingray



A device called a "Stingray" has been reported by the media as used by various federal, state, and local law enforcement agencies to intercept a suspect's cell traffic using tower spoofing equipment and techniques.

Software Risks

- Includes untrusted or compromised mobile applications.
- For the most part, software risk kept to a minimum by controlling the source of apps, and through strict requirements on selling apps in the respective app stores from each vendor.
- Once mobile devices proliferate the market space, new risks specific to mobile devices, as well as older risks that have always plagued computing, are appearing…

App Store Usage

- For the most part, getting software from legitimate application stores run by the major vendors is usually secure.
- Different vendors have different developer requirements in order to get an app into the app store, include security requirements as well.
- Apple and BlackBerry are monolithic, strictly controlling all aspects of both the device and the apps that run on it.
  - Apple, for example, is extremely strict in terms of how developers must create an application that is sold in iTunes.

Android Applications

- Android, on the other hand, is based upon a multitier model, where the devices are developed separately from the applications, and even the operating systems that run on them.
  - There are variations in the Android devices' operating system that require developers to develop differently for each variation.
  - What may run on devices sold by one vendor isn't necessarily guaranteed to run on another vendor's device.

Mobile Apps

- Amazon's Kindle devices can only get apps from the Amazon Appstore.
- Additionally, Android apps aren't always subject to strict developer guidelines like Apple and BlackBerry apps.
  - Doesn't necessarily mean they are less secure, but this can cause issues for secure development.
- Security weakness that exists with app stores is essentially getting apps from unapproved or unofficial sources.
- Some sources, however, are not so legitimate, and are usually unapproved by the vendors, manufacturers, and corporate customers.
  - In some cases, you can get just the app, but getting it to run on the device may be problematic, as some of these apps require root-level access to the device.
  - Typically not allowed on most consumer devices unless the device is rooted.

App Sources

- When getting apps from questionable sources, problems include apps that contain malware, apps that steal personal data and transmit it to a third party, or apps that can even be used as hacking tools.
- Additionally, some apps require replacing the operating system with one that's not approved by the vendor, which not only invalidates the warranty on most devices, but also could cause the device to be unstable and not operate properly.

Malware

- Name given to malicious software, whose purpose is to infect the host and damage, destroy, or steal data.
  - Can also be used to wage network attacks.
- Several different malware classes, including viruses, Trojans, worms, spyware, keystroke loggers, and others.
- Can be used to steal authentication credentials, such as passwords, and send them back to the attacker, or it can be used to cause denial-of-service attacks against entire networks.

Virus

- malware that can be transmitted via files or executable software from device to device.
- We typically think of viruses as only living in the Windows-based PC world, but there have been instances of viruses specifically constructed for some mobile devices, such as laptops, tablets, and even smartphones.
- One important aspect of a virus is that it is not self-executable, nor is it self-replicating.
- Virus must be acted upon by a user or an external process in order to execute.
- It also must be copied in some form to another media or device in order to be replicated; it is incapable of replicating itself (unlike worms).

Trojans

- Malware, that infects a host masquerading as a useful program. Then executes when program is executed, performing all manner of malicious activities.
- Can be used to steal data, such as authentication credentials, passwords, credit card numbers, and other sensitive data, and transmit it back to the attacker.
- Mobile devices, such as desktop PCs, have been hit by Trojans.
- Examples of mobile device Trojans include Gingermaster and Droid KungFu.
  - Two Trojans that work on various versions of Android devices.
  - Both of these Trojans attempt to gain root access to the device and exfiltrate data from the device.

Worm

- Unlike a Trojan or a virus, a worm has the ability to self-replicate across network.
- This is why worms are very difficult to eliminate once they have infected the victim network.
  - When one host is cleaned, it may be plugged back into the network, only to be re-infected when the worm spreads across the network from another infected host.
- Examples of famous desktop PC worms include the Morris Internet worm (the very first worm), MyDoom, and the Win32 Conficker worm. Mobile device worm examples include Cabir (for Symbian OS devices), and Ikee, which was the first identified worm affecting Apple's iOS devices.
- Note that Ikee, like most malware, requires that the device bejailbroken.

Spyware

- Designed to spy on users and possibly steal data, such as passwords, credit card numbers, and so on.
- Can be used to observe a user's actions on a host, such as surfing the Internet, typing a document, or any other activity.
- Activities that spyware records could be saved as pictures, video, or keystrokes.
- Can also record activities, dump them to a list, and send them back to the attacker.

Jailbreaking

- Form of privilege escalation..
- Allows a user to install software not normally allowed, such as apps that don't come from the manufacturer's legitimate app store,or applications that don't meet legal or quality requirements of the device manufacturer.

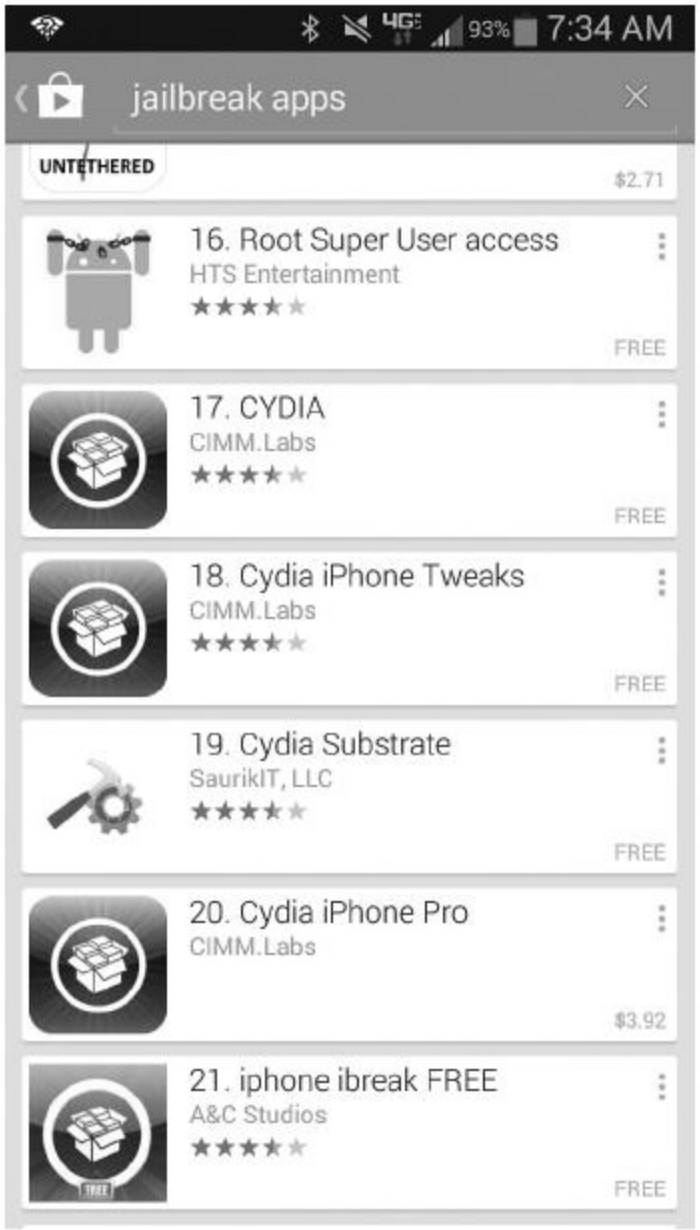
Jailbreaking

- For example, some iPhones that use AT&T as a service provider can't be used to tether (which means to allow another device to use their Internet connection).
- Jailbreaking an iPhone can unlock that functionality and allow other devices to use the iPhone's connection to the Internet.
- Normally not supported by the manufacturer .
  - Typically voids device warranty.
- Additionally, the manufacturer or service provider, if they detect that jailbreaking has taken place on the device, can prevent the device from connecting to their services.

Bricking

- In some cases, jailbreaking fails, and device is rendered non-operational.
  - Usually this can be fixed by restoring the device completely using a backup; however, this also removes the jailbreaking software.
  - Rendering a device non-operational due to jailbreaking is popularly called "bricking" the device.
- In rare occasions, bricking a device can be permanent.
- As you can see from Figure 8-6, there is no short supply of jailbreaking apps, for both Android and iOS.

Figure 8-6
A short list of jailbreaking apps for Android and iOS



Rooting

- “Rooting” similar to jailbreaking.
- When an Android device is rooted, it means that the user now has full administrative access to the lower-level functionality.
- Useful in that it allows the user to perform functions on the device that they would not normally be able to, and access functions that may be prohibited by the device manufacturer.
- Again, as in the case of jailbreaking, this is done to install software that could otherwise be used on the device, or to unlock functionality from a device.

Key Logging

- Process by which software, or hardware, captures and records keystrokes sent to a device from the keyboard.
- Hardware keystroke loggers usually plug into a port, such as a USB port, or even in-line with the keyboard itself.
  - Designed to be small and unobtrusive.
- When plugged into a wired keyboard, simply look like an extension of the keyboard connector.
- Hardware keystroke loggers may or may not have the capability to send data over the network.
- Often, simply sit and record keystrokes until the attacker is able to surreptitiously retrieve the device.

Unsupported OS

- Some rogue applications downloaded from not-so-legitimate sources may not run on stock operating system.
- Solution some determined users find for this is to install a replacement operating system on the device, one that allows uncontrolled access to hardware and root level permissions.
- Unsupported operating systems may have been developed from hacking into the legitimate operating systems' source code, altering the way it allows access to its kernel from users and applications.

Risk

- From an enterprise perspective, jailbreaking or rooting should not be allowed on devices that connect to the enterprise infrastructure or access corporate data.
  - Risks of malware or data loss from the device are too great.
- Additionally, from a practical perspective, unsupported operating systems could be problematic to manage with the Mobile Device Management (MDM) infrastructure.

Device Cloning

- Basically creates a duplicate of a smart-phone.
- Enables hacker to impersonate the legitimate device owner.
  - Includes making and receiving phone calls, text messages, and accessing data.
- Cloning device enables hacker to eavesdrop on legitimate communications.
- Typically, to clone a device, a hacker has to have almost the exact same model and specifications as the target device, as well as access to a device backup file, or access to sophisticated phone configuration and programming software.

Cloning

- Sometimes, an enterprise can maintain software-based device clones, in the form of virtual machines or devices, for testing applications and configuration changes.
- In some security infrastructures, these virtual devices can actually be linked to the actual physical ones, receiving configuration updates and synchronization from the physical device and vice versa.
- These virtual devices should be secured in a controlled area so they are not accessed by unauthorized persons.

Device Theft

- Theft of mobile devices is obvious threat.
- Theft a low tech threat, often carried out during a moment of opportunity, though sometimes planned.
- When a mobile device is stolen, it is subject to being used and examined by the thief.
  - Until theft has been detected, and the device is either reported as stolen, or the services turned off.
- One of the largest threats is unauthorized access of data.
- Unless the device is protected with a personal identification number or other authentication method and encrypted, a thief can retrieve any of the data stored on the device by the user, including contacts, phone numbers, and so on.

Critical Data

- Increasingly, critical data such as usernames and passwords, credit card numbers, and other personal data is being increasingly stored on mobile devices.
- Frequently, users have email accounts or bank accounts set up on the device.
  - May allow the thief to easily access these accounts and use them for malicious purposes.
- Sensitive data may be posted to social media sites.
- In the event that a corporate-owned device is stolen, the thief can access sensitive or proprietary information, or even gain access to the corporate network through any network connections or email connections that are set up on the device.

Device Loss

- Along the same lines as device theft, losing a device causes similar issues.
  - Although not a malicious act like theft, losing a device can also mean losing data.
  - Anyone finding the device may go through it to view the data stored on it, and this can result in unauthorized access.
- Even if the device is not found by anyone, just its loss could mean a loss of data if critical data was stored on the device and not backed up anywhere.

Data Loss Mitigatoin

- In order to prevent data loss from device theft or loss, implement device encryption and remote wipe capabilities as a preventative step.

- Device location through GPS services, as well as remote lock and remote alerts can also be used to prevent data loss from devices that are stolen or lost.

Organizational Risks

- Risks are may incur due to policy, planning, or even implementation of the mobile device infrastructure, and include a variety of items such as BYOD implementation, personal device security, use of removable media, security, control and wiping of personal data, and the infiltration of unknown and unmanaged devices into the network.

BYOD Ramifications

- Organization must balance the security requirements of the network infrastructure against the users' personal privacy and right of ownership over the device.
- Problem occurs when the device is used to access corporate data, which then may be stored or transmitted from the device.
  - Company still owns that data, but the user owns the device.
- Question how much control should the organization has over the users' personal device?
  - For example in some organizations, users must consent to allowing the organization access to their device and to wipe the device remotely if it is lost or stolen.

BYOD: Security vs. Control

- Users may have to consent to organization being able to limit activities user is allowed to do on the device or what resources they are allowed access.
  - For example, an organization that allows a user to bring their own device into work and connect to the corporate infrastructure may require the user to connect to the corporate proxy server and firewall, so the organization can control what content on the Internet the user accesses.
- Organizations must determine how much risk is involved with BYOD, and what mitigating factors can be applied to those risks.
- Users, likewise, must determine if being able to use corporate resources over their personal devices is worth the potential invasion of privacy and giving up control over their device to the organization.

Securing Personal Devices

- Device security is a responsibility of both the organization that owns a device and the user.
- Includes mitigating risks, such as malware, device theft, wireless risks, and software risks.
- Mobie device is not always connected to the infrastructure in order to monitor it and update it, and the organization doesn't always have full control over the device, especially when the user has it in their possession away from the office.
- Additionally, some of techniques require a mobile device infrastructure implemented in the organization that can be used to control mobile devices.
  - Some require specialized software and management devices on the network.

Removable Media

- Organization must balance use of removable media with security risks.
- In addition to establishing a policy on removable media, the organization should also establish technical controls, including the data loss prevention controls.
- Organization should also look at removable media encryption.
  - In addition to encryption, the organization can enforce only approved, corporate-issued media to be used in the device.
- As a last resort, the organization could also ban removable media so that the only place that corporate data resides is on the device itself, which can be remotely encrypted or wiped.

Wiping Personal Data

- One security solution, and a potential security issue, is wiping personal data from mobile devices.
  - If the device is corporate-owned, only a minimum of personal data should be stored on it.
  - However, if it is a user-owned device, and is allowed to connect to the corporate network, there may be issues with wiping a user's personal property.
- If the device is lost, the organization would definitely want to remotely wipe the device in order to ensure that there was no unauthorized access to corporate data.

Policy Considerations

- This is an issue that has to be closely examined before it is implemented, and it should be formally stated in the security policy for both users and the organization to adhere to.
- Users should be educated on the policy.
  - Cautioned about the importance of backing of personal data, as well as the risk of losing data.
- Users should carefully consider risks involved in using personal devices on the corporate network because ultimately, the organization has a responsibility to protect its information assets.
- One solution to this particular issue may be in using data containerization techniques

Unknown Devices

- Unknown devices should be carefully controlled using any of several techniques.
- One such technique is to use a network access control (NAC) device that doesn't allow any device to connect to the corporate network unless it has gone through a quarantine process, which serves to identify and authenticate the device, determine what software is running on it, and limit its connectivity until the user obtains the proper permission to connect it to the corporate network.
- Another technique is the use of virtual LANs, which involves forcing unknown devices to connect to a quarantined VLAN, with no connectivity to the main network.
  - Once the device is identified, it can be assigned to a less restrictive VLAN within the organization.
- Mutual authentication requirements are yet another technique.
  - Authorized devices may have to use the corporate-issued PKI certificate, for example, to identify themselves and authenticate to the network or authentication server.
- In addition to technical measures, policies should be developed regarding the authorization process for introducing new devices into the network.

Mitigation Strategies: Antivirus

- Typically, at the enterprise-level, centralized anti-malware infrastructure exists that provides protection to the entire network in the form of anti-malware servers that automatically update all devices with the latest anti-malware software and signature files.
  - However, because of the mobile nature of some of these devices, this isn't always practical.
  - In some cases, a hybrid solution of centrally managed anti-malware services, and decentralized antivirus solutions, used on a limited individual basis, may be the answer.
- Network access control solutions can ensure that when a device attempts to connect to the network, it is checked for the latest anti-malware signatures and updated as necessary before being allowed to connect to the network.
- In the case of user-managed solutions, when necessary, policy, network access control, and other technical solutions may be needed to ensure users are updating their own devices in a timely manner.

Figure 8-7
Antivirus app for Android

- Figure 8-7 shows an example of user-level antivirus software for an Android device.

Software Firewalls

- Software firewalls are typically installed on individual hosts, and as such, are normally used to protect the host itself from network-based threats.
- Now, while a network-based firewall also serves the same function, it's essentially used to protect the entire network from a wide variety of threats.
- Because different hosts may be running different applications or processing different types of data at varying sensitivity levels, network firewall may not catch threats specific to what the host requires.
- A software firewall is typically installed into an existing operating system.
  - There are firewalls that are integrated with the Windows, for example, but there are also ones that exist as third-party products that can be installed.

Linux Firewalls

- Linux also has firewall packages built into its operating system, as do most of the other OSes available.
- Unfortunately, there is a surprising lack of software firewalls for mobile devices in general, but mobile devices often rely on other security measures to compensate for this shortfall.
- But they do serve as a second line of defense for the host, and are part of any good layered defense-in-depth security design.

Figure 8-8
An Android firewall app

- One example of a software firewall for Android is shown in Figure 8-8.
- Firewalls construct rules to filter specific traffic coming into the host.
- Software firewall packages work at the very basic level and can't possibly keep out every single network threat that the host is exposed to.

Access Levels

- Organization need to determine sensitivity levels for each type of data.
- Based on the sensitivity levels, access can be assigned to different users or groups of users based upon their need to access data, the equipment that processes it, and the areas in which it resides.
- These factors could be things such as security clearance, proper identification of the individual, and the need-to-know the individual may have.
  - If an individual doesn't possess any one of these things, then the organization may deny him access to the area or computing asset.
- Policies regarding access should be formally developed and implemented by the organization.
  - Procedures for granting access to sensitive areas and data should also be implemented and followed.
  - Access levels for individuals should be documented, especially for highly sensitive data.

Permissions

- Permissions may be applied in different ways, depending upon the data itself, how it is accessed either on the local machine or across the network, and how the operating system itself implements access control.
  - For example, in a Linux or Unix-based system, the basic permissions for a file or directory include read, write, and execute.
- In a Windows system, however, a wide variety of granular permissions can be used for both folders and files.
- Some of these permissions are specific to accessing the data locally while sitting at the host, and other sets of permissions are geared toward accessing the data across the network.
- Permissions are assigned based upon the access control model in effect on the system.
  - In a mandatory access control model, the system assigns permissions based upon the individual's security clearance and labels assigned to the data.
  - In a discretionary access control model (the most common), the creator or owner of the asset has the discretionary power to assign permissions to anyone he or she chooses. In a role-based access model, permissions are assigned to specific roles rather than individuals.
- The access control model in use determines both who can assign permissions and how they can be assigned.

Permissions

- Permissions can be explicitly assigned, which ensures that an individual or group will be able to access a data object and perform the tasks they need.
- Permissions can also be denied explicitly, so that an individual will never get permission to the data object, regardless of other permissions they may have.
- Permissions should be documented and reviewed on a periodic basis to ensure that they are still required for an individual to perform their job.

Host-Based and Network-Based IDS/IPS

- An intrusion detection system (IDS) is a device used to detect malicious traffic or unauthorized access.
- A host-based intrusion detection system is typically a software package that is installed on a device that protects the host itself. It can be installed as part of a combination package that includes a host-based firewall and anti-malware software as well. In the case of a network-based intrusion detection system, it is a device that is strategically placed at various points on the network in order to detect malicious network traffic and unauthorized network access. It can be used to detect hacking attempts or denial-of-service attacks.
- Some of these devices are also intrusion prevention systems (IPS), and when detecting malicious traffic or attacks, they reroute traffic or dynamically block traffic based upon port, protocol, or IP address. Most intrusion systems perform both functions in terms of detecting and preventing attacks.

IDS/IPS Systems Work in Different Ways

- Some systems are signature-based, meaning that they are loaded with known attack signatures or rules describing known bad network traffic.
- The signature-based systems have to be periodically updated with current signatures and rule sets. Other systems are known as anomaly-based systems, and must learn the unique traffic patterns inherent to the network they are protecting.
- Usually an administrator will allow them to run in a "learning mode" for a while, where they do not actively detect or prevent malicious traffic; rather, they learn what kind of traffic is typical for the network. When actively detecting and preventing malicious traffic, they will take action or alert based upon traffic that does not meet known traffic patterns.
- For example, if there is an unusual amount of traffic at 3 a.m. on the network, where there normally isn't any at that time, the IDS/IPS will perform actions based upon its rule set, which may include blocking the traffic, rerouting it, or sending an alert on the traffic.
- Anomaly-based IDS/IPS systems usually must be adjusted or fine-tuned whenever changes to the normal network traffic patterns occur, such as installation of new network devices or services that may generate new traffic unknown to the IDS/IPS.

Application Sandboxing

- Sandboxing is a method where applications are run in a restricted memory space and not allowed to interact with other applications or certain hardware.
  - Operating system may have an abstraction layer that interacts with the application and transfers data to the device components as needed.
- All modern mobile operating systems implement some form of sandboxing.
- Another form of sandboxing—called virtual sandboxing—can be used to create sandboxes from existing memory and storage space for apps or processes that the user chooses.

Application Sandboxing

- In effect, this is user-level sandboxing, and uses third-party software instead of the operating system to create these virtual sandboxes.
- Of course, apps that are not controlled using sandboxing may be dangerous because they often run with the full access permissions and rights of the user.
- Potential for damage to data, other apps, or the operating system.
- Note that application sandboxing isn't a panacea for mobile device security.

Data Containers

- Containerization of data is a technique used to separate one class of data from another.
- There may be sensitive data that should not intermingle with other types of data so this data is separated into its own restricted area and cannot be accessed except by certain applications, users, and processes.
- Most common implementation is the separation of corporate data from personal data.
- Usually seen in an organization that allows BYOD in the mobile infrastructure.

Data Containers

- Created to separate corporate and private data so that each can be managed separately in terms of access control, restrictions, encryption, and so on.
- This can be implemented on the device level, as well as in the larger infrastructure, such as mass storage areas that contain device backups.
- Containers are not only used to separate data, but also corporate and private applications as well.
- Policies used in data containerization can also control and enforce restrictions on unauthorized applications and data use, to include copying and pasting between applications and email of corporate data to personal email accounts, for example.

Advantages

- One advantage to data containerization is the ability to selectively remove corporate data from the device at will while not harming personal data.
- Other advantages include the ability of the employee to do everything on one device without having to carry, maintain, and care for a corporate-owned device as well as their own device.
- Choice of devices beyond what the enterprise offers.
- Privacy from the corporate IT personnel and infrastructure.
- An MDM infrastructure used to secure BYOD implementations is required to effectively establish and maintain data containerization.

Trusted Platform Modules (TPM)

- A hardware device, typically implemented as a firmware chip on the mobile device board itself, which provides security functions.
- Functions are usually focused on cryptographic functions.
- A TPM can also control boot-level authentication into the device prior to even loading the operating system.
- If a TPM's encryption and authentication functions are enabled, this can provide extra layers of security in the event the device is lost or stolen.

TPM

- Usually requires very sophisticated equipment and physical possession of the device before it enters the market in order to compromise a TPM.
- Makes it a very secure alternative to software-based authentication and encryption measures.
- Additionally, the TPM or device can be controlled through the use of software on the device that communicates directly with the enterprise infrastructure.
- This enables the MDM infrastructure to load and change certificates, encryption keys, and so on remotely for the device.

Content Filtering

- Method of restricting the types of data and files that can either enter into or exit from a device or network.
- Used to prevent users from downloading certain content, such as music files, video content, or executable files.
  - Filtering usually performed by a security gateway device, such as a firewall or proxy server, although it can also be restricted on the device level.
- Can operate on a wide variety of parameters, including file extensions, sizes, application types, and so on.

Filtering

- Content can also be filtered based upon the end device or even the user account involved.
- Additionally, filters can be placed upon the source of the content, effectively blocking certain domains, sites, and IP addresses from delivering content to a device or network.
- Content filtering can also be used to prevent sensitive data from leaving the organization.

Data Loss Prevention DLP

- Encompasses policies, techniques, and technologies used to prevent loss of an organization's sensitive data.
  - Could include loss through data breaches, hacking, and even unauthorized exfiltration of data by insiders, whether their motivation is malicious or not.
- Techniques used by DLP are based upon monitoring and detecting potential data loss while the data is in use, being transmitted, or even in storage.
- Normally a formalized program within large organizations.

DLP

- Incudes normal information security, policy, user training, data sensitivity categorization, and so on.
  - Other normal security measures, such as authentication, access control, and encryption are also used in DLP.
- Other techniques used outside the normal security controls include content filtering for traffic leaving the infrastructure, as well as detection algorithms designed to detect massive information removal from databases and other electronic stores.
- Metadata marking can also be used in DLP.
- Content filtering can be applied in DLP to make use of keyword searches, or filtering on data sensitivity labels, if they are applied in the file's metadata.

DLP

- DLP highly depends upon the ability of the organization to classify data in terms of sensitivity and identify that data in some way.
- This might be accomplished using sensitivity labels (as used in a mandatory access control model) and through the use of file metadata, as well as other access controls, such as additional authentication methods and encryption.
- Data use and handling controls should also be used for data deemed as protected under the DLP program.
- Could include the storage of sensitive data in restricted folders, databases, or media, as well as additional operational procedures for accessing and using this data.
- DLP can also make use of physical controls, in that highly sensitive data may only be stored and processed in certain areas and on certain systems that are not connected to the network, or have no external media connections enabled (such as optical media drives removed and USB ports disabled).

Device Hardening

- In defense-in-depth, there are several layers of security at various points in the infrastructure, including at the perimeter, the device, hardware, software, and even user controls.
- Device hardening is another layer of security that can be used to prevent malicious action or data loss.
- Device hardening involves securing the device through configuration and software control.
- Mobile device hardening is no different from hardening standard desktop PCs or a server, as far as the concept goes.

Hardening

- Like traditional devices, hardening an enterprise mobile device also involves locking down its configuration, controlling unauthorized access, allowing the user to perform only those actions that are necessary for them to do their jobs, and software control.
- How it is implemented may be slightly different because of the operating system, apps, and multiple functions involved.
- Each of these functions should be looked at for hardening, including cellular telephone use, communications and Internet access, software installation, and user permissions.
- Unnecessary ports, protocols, and services should be removed or disabled, as should unneeded software.
- Vendor-approved security patches should also be installed after proper testing in the environment to ensure that the latest security vulnerabilities are mitigated.

Antivirus Software Kept up-to-date.

- Device hardening should be based upon security policy, which, of course, varies with each organization, as well as the degree of freedom allowed the user.
- There also may be different device hardening policies based upon whether it is an organizationally owned device versus a user-owned device. In any case, device hardening is one layer of the defense-in-depth strategy that should be used.
- Some of the more common device-hardening techniques for mobile devices include requiring a strong passcode, setting the "autolock" feature on the device, and requiring encryption for the device and removable media.
- Additionally, keeping the device updated with the most current OS versions and patches is also strongly recommended.
- Rooting or jailbreaking shouldn't be done on the device.

Physical Port Disabling

- Might include infrared ports, USB ports, SD card slots, Bluetooth, and cameras…
- Disabling the physical use of ports can help keep the device secure, especially if they are not needed or present security risks.
  - For example, while smartphones may be permitted in certain secure areas, their cameras and their ability to take pictures may not be. Disabling the camera itself might prevent data exfiltration from malicious insiders who may photograph sensitive equipment, areas, or documents.
- If external media is not permitted or is restricted, disabling USB ports and media slots should be considered.

Incident Response

- Security incidents include hacking, data theft, unauthorized information access or modification, malware, and even equipment theft and sabotage.
- Incident response is used to help an organization prepare for, respond to, and recover quickly from events that can harm the infrastructures, equipment, data, personnel, and business.
- Incident response is considered necessary to fulfill the due diligence and due care responsibilities for the organization and help prevent, or at least reduce, legal liability.

Preparation

- Preparation involves establishing an incident response policy that directs risk management in terms of sudden, unexpected events that may occur, as well as the formation of an incident response team. Preparation also involves establishing an incident response plan and then testing that plan periodically to ensure that it works.

Policy

- Unless policy is created and promulgated down to the organization, there's no structure in terms of determining whether something is acceptable or not, or there is no direction to perform any action or adhere to any governance.
- Incident response policy dictates what incident response is for the organization, how important it is, who is responsible for the incident response program, and so on.
- As with all security policies, and incident response policy does not tell you how something will be done, just that it must be done, why, who is responsible for it, and what requirements it must meet.
- Typically, incident response policies are created and approved at top levels of management with consultation from lower-level supervision and even technical personnel.
- Incident response policy should, at a minimum, include the types of events that the organization will respond to, who is in charge of the incident response program, and the priority and criticality of response, and it should direct that the incident response plan and team be formed.

Incident Response Plans

- Incident response plans are based upon the organization's commitment of resources to potential threats.
- The response plan should include procedures and actions for a wide variety of threats, including malware infections, critical service outage, data loss, malicious insider actions, as well as hacking attempts.
- Some threats will have common actions and procedures, such as notification and escalation to key personnel, enacting different security protocols, and so on.

IR

- Others may require very specific actions to be performed, depending upon the threat or incident.
- An incident response plan should dictate who the key incident response team members are, as well as their roles during an incident.
- Could include the incident team leader, area supervisors, technicians, and even administrative personnel.
- Each role should have defined duties and actions, as well as procedures for each that the individuals must perform from the outset of the incident.

Testing Incident Response Plans

- Once you have created the plan and have buy-in from management, as well as resources dedicated to it, people have to be trained on it.
- Periodic training is required to make sure everyone stays familiar with the plan and what their responsibilities are during an incident.
- Some personnel may require specific training if their duties are very critical or highly technical.
- Others may need to be trained if their incident response duties are not part of their normal day-to-day duties.

Outsourcing Considerations

- Organizations frequently use outside providers for a wide variety of services, including cloud storage services, infrastructure services, and so on.
- It is critical that any outsourced services be included in your incident response planning.
- You should ensure that service level agreements (SLAs) are written such that incident response is included in them, and the third-party organization knows what its responsibilities are with regards to incident reporting and response.
- The SLAs should specify how incidents are dealt with, how your organization is notified of incidents, and what steps the provider will take to both prevent and respond to them.
- Incidents you may be concerned about include service interruptions and outages, and especially security incidents.

Response

- It may be impossible to plan for every single small thing that can go wrong during an incident.
- This means that the plan must be solid in terms of procedures, yet flexible enough to make changes based upon unexpected conditions when they occur.
- If the team has also been adequately trained, and the plan periodically exercised, these unexpected events can be kept to a minimum.

Incident Identification

- The first part of the response is the identification of the incident.
- This may occur several ways, from a customer or user that notices something unusual on the network, or through an alert from a security device, such as an intrusion prevention system.
- It can also come from outside the organization, such as the upstream service provider, or even a law enforcement agency in the event of something like a large-scale cyber-attack.
- You can even discover an incident through normal troubleshooting of what seems to be at first an innocuous network problem. In any case, once the incident has been identified as a security-related incident, the incident response process should be activated.
- The incident response plan should identify who gets notified based upon different events that occur on the network and whether the incident response team should be activated or not.
- It should also identify immediate actions that should be taken as part of triage to determine the nature and scope of the incident, as well as any first response actions that should occur.

Determine and Perform Policy-Based Response

- The incident response plan, as part of the policy it supports, should drive the response effort.
- When an incident is identified, the key actions should be notification, triage, first response, and sometimes even containment.
- Containing an incident may require some time in the involvement of the entire response team, but the initial actions taken to contain possible security incidents are critical in terms of data loss prevention or compromise.

Reporting Incidents

- Once the incident has been responded to and contained, the team should assess the damage to the infrastructure and data, and report it.
- This may be an ongoing effort while the response is still occurring, or after the incident has concluded.
- In any case, the response effort may have to be escalated as well if the team cannot handle it due to technical ability or scope of authority, or if it extends to outside the company's infrastructure, such as with an Internet service provider. The incident also may have to be escalated to law enforcement officials if it affects breaches of privacy, violations of the law, or certain protected systems, such as banking, medical, and interstate commerce systems.

Esclation

- Escalation should be a determination that is made by the incident response team lead, as well as upper management. The incident response plan should include thresholds or specificscenarios leading to incident escalation.
- It's important that the incident and all the facts surrounding it be documented as quickly and as accurately as possible.
- This would include information about how the incident was discovered, the actions the first responders took, the actions of the incident response team, and what the ongoing status of the incident is if it has not been resolved.
- Documentation will be of critical assistance in the event the incident is escalated, and may be required by governance or law.

Documentation

- Documentation surrounding the event could include artifacts such as security and system log files, network traffic captures, and even configuration files or details from various systems.
- It also may include statements from customers, users, and incident response team members regarding the incident, what was observed, and what actions were performed by each. In the event of a physical incident, such as equipment theft or destruction, even security camera video footage can be included as documentation.
- In any case, anything that helps to add to an understanding of the incident should be included.

Questions???