CMER

Centre for Mobile Education and Research

Security and Mobile Devices

Week I

Overview

- Purpose of Security
- Application to Mobile Devices
- Threats to Mobile Devices
- Security and the Blackberry
- Threats against the Blackberry
- Planning Network Infrastructure
- Security Policies
- Blackberry Enterprise Solution Tools
- IT Policies

What is the purpose of security?

- There are three parts to a computer security system
  - Confidentiality
  - Integrity
  - Availability

Confidentiality

- Limits access to the data
- Only allows authorized users access to the data while preventing unauthorized users access to the information
  - Identify the user through physical or computer controlled methods
    - Physical means
      - Badges
      - usb/parallel adapter dongle
      - Biometrics

Confidentiality (Cont.)

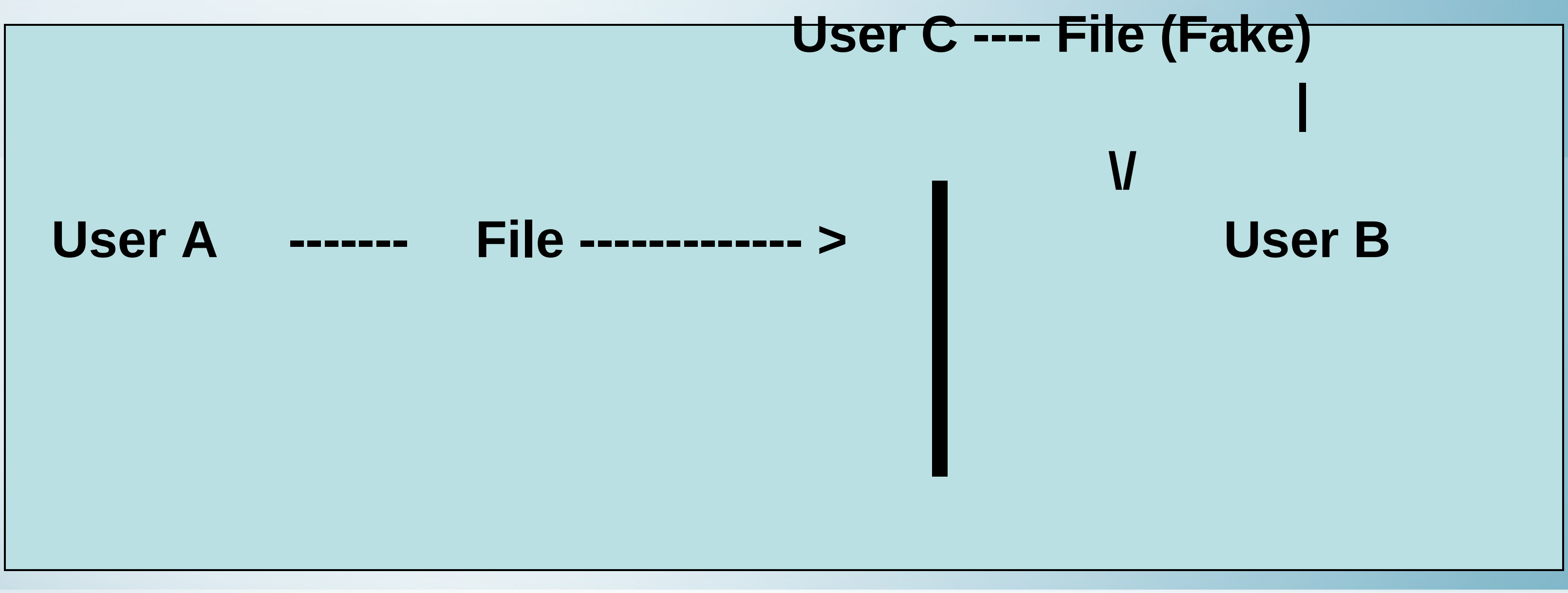
- Computer
  - username and password
  - Digital signatures or certificates
  - Smart cards

Integrity

- Verify the integrity of messages or files
  - Confirm that the information has not been modified whether accidentally or deliberately
- Verify the source of the information
  - The original data came from the correct point of origin and is not a fake

Integrity (Cont.)

– Example: user A sends a file to user B. User B needs to confirm that the file received DID in fact come from user A and that someone else (ie User C) did not intercept the file and replace the file that User A sent with their own file.



User C ---- File (Fake)

|

\/

User A ------- File ------------- > User B

Availability

- The information is availability as required
- Information must be accessible while at the same time restricting user's access based on their identity

How does it apply to Mobile Devices?

- This applies to any mobile devices that can be connected to a network
  - Ie Laptops, PDAs, BlackBerry Devices
- Security breaches and vulnerabilities on mobile devices are just as bad as security breaches on a computer.

How does it apply to Mobile Devices? (Cont.)

- When applying to a network, the network is only as secure as it’s weakest point. In this case, if security measures are not taken on the mobile device, then through it, a malicious user has the ability to gain access to your network through the device.

How does it apply to Mobile Devices? (Cont.)

- Vulnerabilities are not just restricted to the mobile device itself but can also be attribute to badly written mobile applications that do not take security measures

How does it apply to Mobile Devices? (Cont.)

- Example
  - John has a BlackBerry and he did not set up any type of security mechanism on his mobile device. One day while out to lunch, his BlackBerry was stolen ☹
    - Confidentiality:
      - Bad: The thief now has access to all of his data that is on the device
      - Worst: If he is on a corporate network and has access to the company data through his BlackBerry, the thief now has the same access to company sensitive information that John has.

How does it apply to Mobile Devices? (Cont.)

- Example
    - Integrity
        - Bad: The thief now has the ability to impersonal John through the device
        - Worst: The thief decides to implement malicious acts to company network since he now has access through John’s BlackBerry

Solutions

- Know about the threats that apply to mobile devices and the methods and solutions to neutralize them
- Keep security in mind when developing mobile applications

Threats to Mobile Devices

- There are various threats that can affect mobile devices and they can be summed up into two categories.
  - Passive
  - Active

Threats to Mobile Devices (Cont.)

- Passive threats
  - Passive threats are those that are not a direct attack but rather occur through indirect actions against an entity.
  - They work by gathering information such as traffic analysis or releasing message contents
  - An example of such a threat can be wireless attacks that work as traffic analysis and record data that is being transmitted and received by the mobile device.

Threats to
Mobile Devices (Cont.)

- Active threats
  - Unlike passive threats, active attacks take direction action against an entity
    - Viruses/Malware
    - Lost/theft

Security and the BlackBerry

- Applications and the BlackBerry
- Installing applications
- Malware
- Managing Risk

Third Party Applications and the BlackBerry Device

- Applications loaded on a BlackBerry have the ability to perform the following functions:
  - Communicate and share storage with other third party BlackBerry applications
  - Communicate with native BlackBerry applications
  - Access user information stored on the BlackBerry. Such information includes calendar entries, email messages, and contacts

Installing Applications on BlackBerry Device

- There are various ways to load an application on to a BlackBerry device
  - Downloading an application over the air through the wifi or cellular network from a website
  - Use the application loader found with the BlackBerry Desktop Manager and completing an installation though a connection to the computer

Installing Applications on BlackBerry Device (Cont.)

- push an application to the device wirelessly and install it automatically through the application loader remote function

Threats against BlackBerry Devices

- Applications that are designed with malicious intent to cause harm to computer systems are commonly known as malware and include the following:
  - Viruses
    - replicate themselves by attaching to legitimate applications on a computer

Threats against BlackBerry Devices (Cont.)

- Trojan horses
  - disguise themselves as or embed themselves within innocuous-seeming or trusted applications; to succeed, a Trojan horse application depends on the action of the device user, and therefore, it requires successful use of social engineering rather than the ability to exploit flaws in the security design or configuration of the target device

Threats against BlackBerry Devices (Cont.)

- Worms
  - replicate themselves to spread across networks and potentially overwhelm computer systems (a worm is self-contained and does not need to be part of another program to spread itself)
- Spyware
  - designed to log device user activities and personal data and send that information to the attacker

Threats against BlackBerry Devices (Cont.)

- Some malware attacks might target BlackBerry devices.
- Attackers might use malware to perform attacks that are designed to:
  - steal personal and corporate data
  - create a Denial of Service to make a corporate network unusable
  - access a corporate network using corporate BlackBerry devices

Managing risks on the BlackBerry

- There are various ways to manage and decrease the risk of these malware:
  - Plan the network architecture
  - Design security policies
  - Use The BlackBerry Enterprise Solution tools

Planning the Network Infrastructure

- When creating the network infrastructure, considerations should be made to protect the network components. It might have many connections to the Internet and to external systems, as well as network clients such as BlackBerry devices.

Planning the Network Infrastructure (Cont.)

- Consider separating the network infrastructure into digital zones, or segments, separated by firewalls, and restricting internal and external user access to those zones.
- multiple security products and methods might be required to protect each gateway from one section of the network to another and to and from the Internet.

Security Policies

- In addition to planning the infrastructure, security policies can be used to help protect the network.
  - Policies are a set of rules used by which to govern the actions of an entity. An entity can anything that connects to the network
  - Research In Motion offers two types of security policies for the BlackBerry Devices
    - IT Policy
    - Application Control Policy

Security Policies (Cont.)

- To maintain and enforce security policies, a subset of the security solution and security policies must be applied to each BlackBerry device
- This must be done since BlackBerry devices connect to the network and thus are an extension of the network.
- The security measures that are set up must be designed to not only protect the physical network, but also to protect the security of the BlackBerry devices.

BlackBerry Enterprise Solution Tools

- No matter how the application is to be installed on a BlackBerry Handheld, the BlackBerry Enterprise Solution (BES) includes tools created to let the administrator control the method of installation (manual or automatic) of application on the device.

BlackBerry Enterprise Solution Tools (Cont.)

- The BES allows the administrators to limit the amount of access for suspicious application and their resources to help avoid the spread of malware
- The tools that come bundled with the BES offers help to help prevent opportunities for attackers to use malware to access the network and BlackBerry devices.

BlackBerry Enterprise Solution Tools (Cont.)

- On computers, malware prevention requires processes that both detect and contain malware attacks. Detection is the process of determining whether or not a program is malware.
- Effective malware detection requires a comprehensive and frequently updated local database or a constant connection to a similarly qualified online database.

BlackBerry Enterprise Solution Tools (Cont.)

- While computers might have access to these databases, current mobile devices do not have enough storage space for a malware database and cannot guarantee a constant connection to the Internet.

BlackBerry Enterprise Solution Tools (Cont.)

- The BES is designed to use IT policies, application control policies, and code signing to contain malware by controlling an application’s access to BlackBerry device resources and applications.
- These methods are designed to prevent malware that might gain access to the BlackBerry device from causing damage to the BlackBerry device, its applications and its data, or to the network.

BlackBerry Enterprise Solution Tools (Cont.)

- The following methods below can be used control third-party applications installed on a BlackBerry
  - prevent BlackBerry devices from downloading third-party Java applications over the wireless network
  - requiring or preventing BlackBerry devices from installing specific third-party Java applications
  - controlling the permissions of third-party Java applications that exist on BlackBerry devices

BlackBerry Enterprise Solution

- By default, BlackBerry devices can install all third-party Java applications until you use one or all of these methods to control third-party Java applications on BlackBerry devices.

Policies

- IT Policy
  - An IT Policy can be seen as a global policy that applies to all the devices that implement the policy
- Application Policy
  - An application policy is a policy that applies only to a particular application that resides on the device
- When applying security policies, there are precedence that occur between the IT policy and the application control policy.

Policies (Cont.)

- Since IT policy rule settings apply to the device in general, IT Policies override application control policy rule settings.
  - Example: if you set the Allow Internal Connections IT policy rule to False for BlackBerry devices for which you also set an application control policy that allows a specific application to make internal connections, the IT policy rule setting overrides the application control policy rule setting and thus the application cannot make internal connections.

Policies (Cont.)

- The BlackBerry device revokes an application control policy and resets if the permissions of the application to which it is applied become more restrictive. BlackBerry devices running the BlackBerry Device Software Version 4.1 or later let BlackBerry device users make application permissions more, but never less, restrictive than what the BlackBerry Enterprise Server administrator sets.

Policies (Cont.)

- IT policy rules included with the BES are designed to allow the administrators to control the applications on the BlackBerry device.
  - They are designed to prevent BlackBerry devices from downloading third-party Java applications over the wireless network
  - Specify whether or not applications, including third-party Java applications, on the BlackBerry device can initiate specific types of connections

Types of IT Policy Rules

- Disallow Third Party Application Download
  - Specify whether or not the BlackBerry device can download third-party Java applications.
  - Cannot be used to allow or prevent the downloading of specific applications on the BlackBerry device.

- Allow External Connections
  - Specify whether or not applications, including third-party Java applications, on the BlackBerry device can initiate external connections (for example, to WAP, SMS, or other public gateways).

Types of IT Policy Rules (Cont.)

- Allow Internal Connections
  - Specify whether or not applications, including third-party Java applications, on the BlackBerry device can initiate internal connections (for example, to the BlackBerry MDS™ Connection Service)
  - Preventing all internal connections for all third-party Java applications turns off the use of the connection service on the BlackBerry device.

Types of IT Policy Rules (Cont.)

- Allow Third-Party Apps to Use Serial Port
  - Specify whether or not third-party Java applications can use the serial port or USB port on the BlackBerry device for communication.

Application Control Policy

- Designed to let you allow or prevent the installation of specific third-party Java applications on the BlackBerry device and to limit the permissions of third-party Java applications, including
  - the resources (for example, email, phone, and BlackBerry device key store) that third-party Java applications can access on the BlackBerry device
  - the types of connections that a third-party Java application running on the BlackBerry device can establish (for example, local, internal, and external connections)

Application Control Policy (Cont.)

  - whether or not an application can access the user authenticator framework API, which permits the registration of drivers to provide two factor authentication to unlock the BlackBerry device
- For example, you can control connections to your internal servers from third-party Java applications on the BlackBerry device using the following process:
  - Do not change the Allow Internal Connections IT policy rule

Application Control Policy (Cont.)

  - Create an application control policy that prevents the application to which it is assigned from making internal connections.
  - Apply the application control policy to a software configuration for a user or one or more user groups
- Assigned application control policy cannot use third-party Java applications to send and receive data from internal servers.

Application Control Policy (Cont.)

- One or more application control policies can also be applied to trusted third-party applications to create an allowed list of applications for specific application behavior.
- Example
  - allow BlackBerry device users to install only those applications
  - allow only those applications to perform specific actions

Types of Application Policy Rules

- Internal Domains
  - Specify the internal domain names to which the application can establish a connection.
- External Domains
  - Specify the external domain names to which the application can establish a connection.
- Browser Filter Domains
  - Specify the domains for which the application can apply browser filters to web page content on the BlackBerry device.
    - ie, specify google.com and yahoo.com as domains for which you allow an application to use a search engine browser filter on the BlackBerry device

Types of Application Policy Rules (Cont.)

- Disposition
  - Specify whether the application is optional, required, or not allowed on the BlackBerry device.
  - used to require that the BlackBerry device download a specific application or prevent the BlackBerry device from downloading an unspecified or untrusted application.
- Interprocess Communication
  - Specify whether or not the application can perform interprocess communication operations.
  - used to prevent two or more applications from sharing data and to prevent one application from using the connection permissions of another application.

Types of Application Policy Rules (Cont.)

- Internal Network Connections
  - Specify whether or not the application can make internal corporate network connections.
  - Used to allow or prevent the application from sending or receiving data on the BlackBerry device using an internal protocol
    - ie, using the connection service or
  - Used to require that the user respond to a prompt on the BlackBerry device to allow internal connections through the BlackBerry device firewall.

Types of Application Policy Rules (Cont.)

- External Network Connections
  - Specify whether or not the application can make external network connections.
  - used to allow or prevent the application from sending or receiving data on the BlackBerry device using an external protocol
    - ie, using a WAP gateway, public BlackBerry MDS Services, or TCP
  - used to require that the user respond to a prompt on their BlackBerry device to allow external connections through the BlackBerry device firewall.

Types of Application Policy Rules (Cont.)

- Local Connections
  - Specify whether or not the application can make local network connections
  - Example:
    - connections to the BlackBerry device using a USB or serial port

Types of Application Policy Rules (Cont.)

- Phone Access
  - Specify whether or not the application can make phone calls and access phone logs on the BlackBerry device.
  - Used to allow or prevent the application from making calls on the BlackBerry device or to require that the user respond to a prompt on the BlackBerry device to allow the application to make a phone call.

Types of Application Policy Rules (Cont.)

- Message Access
  - Specify whether or not the application can send and receive messages on the BlackBerry device using the email API.
- PIM Data Access
  - Specify whether or not the application can access the BlackBerry device PIM APIs, which control access to the user's personal information on the BlackBerry device, including the address book.

Types of Application Policy Rules (Cont.)

- Browser Filters
  - Specify whether or not the application can access browser filter APIs to register a browser filter with the browser on the BlackBerry device.
  - used to allow third-party Java applications to apply custom browser filters to web page content on the BlackBerry device.
- Event Injection
  - Specify whether or not the application can inject synthetic input events, such as pressing keys and performing trackwheel actions, on the BlackBerry device.

Types of Application Policy Rules (Cont.)

- Bluetooth Serial Profile
  - Specify whether or not the application can access the Bluetooth® Serial Port Profile (SPP) API.
- BlackBerry Device Keystore
  - Specify whether or not the application can access the BlackBerry device key store APIs.

Types of Application Policy Rules (Cont.)

- BlackBerry Device Keystore Medium Security
  - Specify whether or not the application can access key store items at the medium security level (the default level), which requires that the BlackBerry device prompt the user for the BlackBerry device key store password when an application tries to access the user’s private key for the first time or when the private key password timeout expires.
- Device GPS
  - Specify whether or not the application can access the BlackBerry device Global Positioning System (GPS) APIs.

Types of Application Policy Rules (Cont.)

  - Used to allow or prevent the application from accessing the GPS APIs on the BlackBerry device or to require that the user respond to a prompt on the BlackBerry device to allow access to the GPS APIs.
- Theme Data
  - Specify whether or not the BlackBerry device can use the custom theme applications

Types of Application Policy Rules (Cont.)

- User Authenticator API
  - Specify whether or not the BlackBerry device allows an application to access the user authenticator framework API.
  - The user authenticator framework allows the registration of drivers (currently smart card drivers only) that provide two-factor authentication to unlock the BlackBerry device.
  - Applies to the BlackBerry Device Software and third-party Java applications.