RAMA UNIVERSITY

www.ramauniversity.ac.in

FACULTY OF EGINEERING & TECHNOLOGY

MOBILE SECURITY

LECTURE -8

Umesh Kumar Gera
Assistant Professor
Computer Science & Engineering

OUTLINE

- What is mobile device security?
- Why is mobile device security important?
- What are the benefits of mobile device security?
- How does mobile device security work?
  - Establish, share, and enforce clear policies and processes
  - Password protection
  - Leverage biometrics
  - Avoid public Wi-Fi
  - Beware of apps
  - Mobile device encryption
- MCQ
- References

WHAT IS MOBILE DEVICE SECURITY?

What is mobile device security?

Mobile Device Security refers to the measures designed to protect sensitive information stored on and transmitted by laptops, smart phones, tablets, wearable's, and other portable devices. At the root of mobile device security is the goal of keeping unauthorized users from accessing the enterprise network. It is one aspect of a complete enterprise security plan.

Why is mobile device security important?

With more than half of business PCs now mobile, portable devices present distinct challenges to network security, which must account for all of the locations and uses that employees require of the company network. Potential threats to devices include malicious mobile apps, phishing scams, data leakage, spyware, and unsecure Wi-Fi networks. On top of that, enterprises have to account for the possibility of an employee losing a mobile device or the device being stolen. To avoid a security breach, companies should take clear, preventative steps to reduce the risk

What are the benefits of mobile device security?

The Mobile device security, or mobile device management, provides the following:

- ❑Regulatory compliance
- ❑Security policy enforcement
- ❑Support of “bring your own device” (BYOD)
- ❑Remote control of device updates
- ❑Application control
- ❑Automated device registration
- ❑Data backup

Above all, mobile device security protects an enterprise from unknown or malicious outsiders being able to access sensitive company data.

How does mobile device security work?

Securing mobile devices requires a multi-layered approach and investment in enterprise solutions. While there are key elements to mobile device security, each organization needs to find what best fits its network.

To get started, here are some mobile security best practices:

1. Establish, share, and enforce clear policies and processes

Mobile device rules are only as effective as a company's ability to properly communicate those policies to employees. Mobile device security should include clear rules about:

- What devices can be used
- Allowed OS levels
- What the company can and cannot access on a personal phone
- Whether IT can remote wipe a device
- Password requirements and frequency for updating passwords

HOW DOES MOBILE DEVICE SECURITY WORK?

2. Password protection

One of the most basic ways to prevent unauthorized access to a mobile device is to create a strong password, and yet weak passwords are still a persistent problem that contribute to the majority of data hacks. Another common security problem is workers using the same password for their mobile device, email, and every work-related account. It is critical that employees create strong, unique passwords (of at least eight characters) and create different passwords for different accounts.

3. Leverage biometrics

Instead of relying on traditional methods of mobile access security, such as passwords, some companies are looking to biometrics as a safer alternative. Biometric authentication is when a computer uses measurable biological characteristics, such as face, fingerprint, voice, or iris recognition for identification and access. Multiple biometric authentication methods are now available on smart phones and are easy for workers to set up and use.

HOW DOES MOBILE DEVICE SECURITY WORK?

4. Avoid public Wi-Fi

A mobile device is only as secure as the network through which it transmits data. Companies need to educate employees about the dangers of using public Wi-Fi networks, which are vulnerable to attacks from hackers who can easily breach a device, access the network, and steal data. The best defense is to encourage smart user behavior and prohibit the use of open Wi-Fi networks, no matter the convenience.

5. Beware of apps

Malicious apps are some of the fastest growing threats to mobile devices. When an employee unknowingly downloads one, either for work or personal reasons, it provides unauthorized access to the company's network and data. To combat this rising threat, companies have two options: instruct employees about the dangers of downloading unapproved apps, or ban employees from downloading certain apps on their phones altogether.

6. Mobile device encryption

Most mobile devices are bundled with a built-in encryption feature. Users need to locate this feature on their device and enter a password to encrypt their device. With this method, data is converted into a code that can only be accessed by authorized users. This is important in case of theft, and it prevents unauthorized access.

MCQ

6. The full form of EDR is _____

a) Endpoint Detection and recovery

b) Early detection and response

c) Endpoint Detection and response

d) Endless Detection and Recovery

7. _____ technology is used for analyzing and monitoring traffic in network and information flow.

a) Cloud access security brokers (CASBs)

b) Managed detection and response (MDR)

c) Network Security Firewall

d) Network traffic analysis (NTA)

8. Compromising confidential information comes under _____

a) Bug

b) Threat

c) Vulnerability

d) Attack

9. Lack of access control policy is a _____

a) Bug

b) Threat

c) Vulnerability

d) Attack

10. Possible threat to any information cannot be _____

a) reduced

b) transferred

c) protected

d) ignored

REFERENCES

- https://resources.infosecinstitute.com/category/computerforensics/introduction/mobile-forensics/the-mobile-forensics-process-steps-types/#gref