RAMA UNIVERSITY

www.ramauniversity.ac.in

FACULTY OF EGINEERING & TECHNOLOGY

MOBILE SECURITY

LECTURE -3

Umesh Kumar Gera
Assistant Professor
Computer Science & Engineering

OUTLINE

- Mitigating Mobile Security Risks
- Mobile Payment Trends
- Real-time Mobile Security Risks
- Common Mistakes in Source Code
- MCQ
- References

MITIGATING MOBILE SECURITY RISKS

Mitigating Mobile Security Risks

The total number of detected security incidents is growing at a rate of 48 percent, says a global information security survey report from PricewaterhouseCoopers. It says many organizations are unaware of attacks, and the rise in incidents is in part due to increasing use of mobile applications and payment devices.

Majorly risk categorized in three aspects

1. Real-time mobile security risks
2. Avoiding common mistakes in source code
3. Ways to secure mobile payment infrastructure

MITIGATING MOBILE SECURITY RISKS

Mobile Payment Trends

Trend of mobile payments and payment devices usage has boosted security risks for consumers. What kind of attack vectors are emerging that challenge security teams?

❑Real-time Mobile Security Risks

❑**Mobile Device Risks:** caused due to direct interface and wireless with the use of malware, third-party applications or automatically generated malicious applications, Android and iPhone.

❑**Mobile Application Risks:** insecure data storage, as the data is not stored encrypted by the application, reliance on OS security controls, unauthorized access to PII and insecure payload, reverse engineering involving sensitive data disclosure and patch the application.

❑**Payment Device Risk:** caused due to unrestricted access to setting and through communication channels as Bluetooth device is integrated on the payment device. Add-on Devices Risks: caused due to fingerprint scanners and printers.

MITIGATING MOBILE SECURITY RISKS

Common Mistakes in Source Code

1. Hardcoded sensitive data;
2. Cryptography usage;
3. Exception & Error Handling;
4. Logging l
5. Improper Code Signing;
6. Permissions;
7. Configuration Files;
8. Session Management

MCQ

11. Activate _____________ when you’re required it to use, otherwise turn it off for security purpose.

a) Flash Light

b) App updates

c) Bluetooth

d) Rotation

12. Try not to keep ________________ passwords, especially fingerprint for your smart-phone, because it can lead to physical hacking if you’re not aware or asleep.

a) Biometric

b) PIN-based

c) Alphanumeric

d) Short

13. Which of the following tool is used for Blackjacking?

a) BBAttacker

b) BBProxy

c) Blackburried

d) BBJacking

14. BBProxy tool is used in which mobile OS?

a) Android

b) Symbian

c) Raspberry

d) Blackberry

15. Which of the following is not a security issue for PDAs?

a) Password theft

b) Data theft

c) Reverse engineering

d) Wireless vulnerability

REFERENCES

- https://www.bankinfosecurity.asia/mitigating-mobile-security-risks-a-8481
- https://www.sanfoundry.com/cyber-security-questions-answers-mobile-phone-security/