Is Your Phone Leaking Data?

Introduction

Today our mobile devices are used for more than just phone calls. With a powerful handheld computer in many of our pockets, we have access to so much information, which in turn, means others may be trying to access our information. Could your phone be leaking data that you are not aware of?

What is mobile data leakage?

Data leaks happen when an organization or an individual loses control of their information. Control of the data may be lost due to unauthorized or unwarranted transmission of data to an external source. Mobile data leaks can also occur when mobile device privacy settings or applications are misconfigured.

How do mobile leaks occur?

NIST Special Publication (SP) 1800-4 *Mobile Device Security Cloud and Hybrid Builds, Volume B,* discusses how mobile data leaks occur, including:

- Lack of mobile access control (e.g., loss of the mobile device, or lock screen protections were not enabled)
- Lack of confidentiality protection of information (e.g., encryption of data in transit) due to operating on unsafe or untrusted networks (e.g., public Wi-Fi)
- Unpatched firmware or operating systems
- Application software bypassing the operating system security architecture (e.g., rooted/jailbroken device)
- Users running malicious mobile applications
- Device interaction with cloud services outside corporate control
- Misuse or misconfiguration of location services, such as a global positioning system
- Acceptance of fake mobility management profiles, providing malicious actors with a high degree of device control
- Social engineering via voice, short message service/multimedia messaging service, third-party text communication, or email communication

What happens when a mobile phone leaks data?

Data leaks containing personally identifiable information (PII) could involve information like financial and health data. But it also includes less obvious types of privacy-related data, such as video and audio files, information about the way an individual uses the Internet, and location tracking data.

The list below shows examples of the types of *privacy related data* stored on mobile devices and describes what could happen if that data is leaked:

- **Financial data** leakage could result in account hacking and misappropriation of finances.
- **Health-related data** leakage could result in improper health treatments, health related information becoming publicly available, or violation of health privacy laws.
- **Location data** leakage could result in tracking of persons.
- **Camera or microphone data** leakage could result in conversations or events being publicly disclosed.
- **Internet browsing data** leakage could result in the release of your internet habits and targeted solicitations.
- **Password** leakage could result in unauthorized access to personal or organizational information.
- **Text messages and email** leakage could result in disclosure of individual or organizational data that could lead to reputational damage.
- **Contact lists or call log** leakage could result in device owner spoofing or impersonation, spear phishing, and social engineering risks.

How to protect against data leakage

In addition to the lists below, NIST SP 1800-22 *Mobile Device Security: Bring Your Own Device* provides guidance to help organizations and individuals improve their mobile device security and privacy. Organizations and individuals can help protect their mobile devices from data leakage with the following recommendations:

For Organizations:

- **Manage mobile device settings** by including Mobile Device Management (MDM) solutions when planning an organization's IT architecture. MDMs may help with creating mobile device policies and configurations to prevent data leaks by using multifactor authentication, password management, application security, device lock screen, and remote wipe policies.
- **Preserve confidentiality** by employing data in transit protection like Transport Layer Security or IPsec Virtual Private Networks to protect your data against an eavesdropping adversary.

- **Protect organizational data** by keeping mobile operating system and applications up to date and by applying zero trust principles to ensure data access is verified and given only to required resources.
- **Separate work from personal information** by deploying a Bring Your Own Device (BYOD) solution like Apple User Enrollment or Android Enterprise. BYOD solutions can provide logical data separation between enterprise and personal user data, preventing leakage between the two separate workspaces.
- **Improve your organization's application security and privacy profile** by deploying App vetting to identify security and privacy risks.
- **Help maintain mobile device security posture** by using a Mobile Threat Defense solution that monitors for device-, app-, and network-based attacks.

For Individuals:

- **Avoid phishing attempts** by not clicking on suspicious links and promotions that come in an email or a text message from unknown numbers or accounts.
- **Protect your device** by only installing apps from trusted sources.
- **Protect private information** by reviewing permissions that applications request (e.g., requests for microphone or camera access).
- **Obtain the latest security features** by installing regular updates on your phone.
- **Prevent unauthorized access** by enabling a lock screen and prevent notifications from displaying their content on the lock screen.
- **Protect your accounts** by using multi-factor authentication when possible.

For more information, visit us at www.nccoe.nist.gov/mobile-device-security. To get in contact with our team, email us at mobile-nccoe@nist.gov.