Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India
सत्यमेव जयते

CERT-In Advisory CIAD-2016-0071

Mobile and Cloud Data Security

Original Issue Date: December 07, 2016

Description

The fast pace of modern life, accelerated business processes and decision making, have all created the need for fast and reliable access to data and information. Mobile devices, which have become ubiquitous, offer easy connections to the world of information. Now we have data moving across a multiplicity of devices, including tablets, smart phones and even wearable devices as people use their smart watches to notify them of company phone calls, SMSs and so forth.

This means much more data flowing from devices to servers, servers to devices, sensors to devices and devices to devices. A good deal of that data will be business-generated information and that needs to be kept confidential or have restricted access. Mobile devices generally connect over wireless networks rather than wired Ethernet, which presents additional security vulnerability and exposure. Mobile applications are highly connected to web services and this broadens the possible vectors for data exfiltration. And above all this, there's cloud.

More and more companies, however, are moving their data as well as their applications to cloud services providers (CSP), in which case you may not know exactly what security measures are being implemented to protect that data and you most likely will have no idea what the physical location of the data is. From security point of view, it makes sense for the CSP to keep that information under wraps, but it also makes us feel as if we're no longer in control. Making the move to the cloud requires placing our data in the hands of the CSP, which means it involves trusting that the CSP will protect it.

Protecting Mobile and Cloud Data

In many ways, protecting data that has "gone mobile" or is stored in the cloud is the same as protecting data in an on-premises data centre.

Authentication: The first step in protecting data is to verify the identity of the person who is attempting to access it. With sensitive mobile data, traditional username and password authentication isn't enough. Multi-factor authentication provides stronger protection and today's mobile devices support many forms of authentication; including fingerprint scanners, pattern recognition etc.

Authorization and access controls: Once identity has been established, the system must be able to determine which data files that user is allowed to open and what level of access he/she can have (read only, modify, delete, etc.). This is done by setting permissions, privileges and user rights.

Encryption: Encrypting the data adds another level of protection and is the best way to protect data. Mobile data needs to be protected while at rest on the device and while in transit across the Internet. Web-based data traffic is usually encrypted using Transport Layer Security (TLS), which is the newer iteration of Secure Sockets Layer (SSL). Non-web data can be encrypted using VPN protocols such as IPsec or SSH tunneling. Email can be encrypted using S/MIME or PGP.

Containerized applications: Containerization is a big trend these days and goes hand-in-hand with cloud computing. Containerized applications can create a private corporate workspace on a user's personally owned device so they get access to the corporate data and apps with enterprise-grade security.

Virtual private networks: VPN protocols such as SSL or IPsec encrypt the transmission of data between the remote user and the corporate network, and most companies support VPN connections.

Mobile Device Management (MDM) and Mobile Application Management (MAM): An MDM system allows you to create and apply policy-based security to all of the mobile devices that access your company network, manage certificates and keys, monitoring device health and security status, track usage and access, control access to data, and even lock or remote wiping a device if it's lost or stolen. MAM helps you keep mobile apps updated and configured correctly for best security, which makes the data they generate and store more secure.

User education: Ensure that mobile users are aware of your best security practices and understood how to apply them. One of the most important aspects of training is encouraging them to not jailbreak devices. Jail breaking lets users override devices application protections to download non-approved, non-supported apps, which can make devices more vulnerable to malware and attacks.

Educate yourself: When selecting a cloud services provider, be sure to read the user agreement regarding the storage of your data and ask questions of you have concerns or don't understand something. Ensure that your CSP encrypts stored data.

Data classification: Such classification allows you to evaluate whether some of your data may not be appropriate for cloud storage because of its sensitivity or because of regulatory requirements.

Back it up: Ensure that data can be restored after a device is damaged, wiped or lost, by taking advantage of data backup capabilities supported by each mobile OS. Best practices include passcode-protecting access to backup files and cloud storage, encrypting those backups wherever possible and preventing business data from being backed up to personal storage areas.

References

http://www.gartner.com/smarterwithgartner/how-to-move-mobile-data-without-leaking/
https://www.sans.org/reading-room/whitepapers/cloud/security-accountability-cloud-data-center-survey-37327
http://www.cio.com/article/2380182/cloud-security/5-tips-to-keep-your-data-secure-on-the-cloud.html
http://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2016-0069

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-24368572

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India