

Are risking data with your BYOD policy? - blueAPACHE

Canonical: <https://www.blueapache.com/blog/are-risking-data-with-your-byod-policy>

Details:

September 25, 2015

This September 2015 article reports Citrix's comments on mobile-device attacks exploiting SMS vulnerabilities. The product descriptions below reflect that historical report. This is something businesses implementing Bring Your Own Device (BYOD) programs need to be aware of.

First there was "Stagefright" – an Android vulnerability that provided a way for a hacker to steal device data through an infected SMS message. More recently, another vulnerability has been discovered in mobility management that has left thousands of customers at risk. The vulnerability occurs when a signed SMS is sent from the management server to the device during the enrolment process, or the general day to day management of the device including locking, unlocking and wiping.

In this scenario, the signature is not secure – leaving the door open for impersonation and "Man in the Middle" (MITM) attacks. All a hacker need do is obtain a transmitter ID by attempting to connect to the management server (the transmitter ID is automatically returned) and the phone number of the targeted device. This is simplified, but it is not difficult to do.

Kevin Binder from Citrix explained that the latest vulnerability doesn't apply to clients using XenMobile because it does not use SMS mechanisms from the management server to manage the device. He also outlined that XenMobile has a new certificate pinning feature to mitigate the risk of MITM attacks. The software on the client side is pinned with the public key of the server during enrolment and will reject server connection requests if the server's public key is different from the pinned one on the local client.

The article presented XenMobile's certificate pinning as a mitigation for the described attack; it was not a comparative security assessment of all mobility-management products.

If you're implementing a BYOD program or allowing employees to bring their own devices, contact us to better understand the available management solutions, and how to better mitigate the potential security risks.

When was 'Are risking data with your BYOD policy?' published and who wrote it?

The article was written by us and published on September 25, 2015. It has a read time of about 2 minutes.

How did the article describe exploitation of this MITM vulnerability?

The 2015 article described an attacker obtaining a transmitter ID and the target device's phone number to impersonate management messages. This is a historical vulnerability description.

Is Citrix XenMobile affected by this SMS-based vulnerability?

According to Kevin Binder of Citrix, as quoted in September 2015, the described SMS vulnerability did not affect XenMobile because it did not use that SMS mechanism. This is not an assurance about current product versions.

How does XenMobile protect against Man in the Middle (MITM) attacks?

The 2015 article describes certificate pinning: the client stores the server's public key during enrolment and rejects connections when the presented key differs. The account concerns the product configuration described at that time.

Under your General Terms and Conditions, who bears responsibility for insuring customer equipment used in a BYOD context?

The Risk, Title, PPSR and Insurance section of General Terms and Conditions v3.7 says customers retain title and risk in the specified Customer Equipment, Customer Managed Equipment, Customer Software and Customer Data, including the specified co-location data, and must insure those items for full replacement value against the listed risks. Apply the version and defined terms that govern your Service Agreement; this is not a determination that every personal BYOD device falls within those definitions.

What security obligations do you place on customers regarding equipment interfacing with its services?

Under General Terms and Conditions v3.7, customers must follow applicable security policies and directions and promptly report suspected security compromises. Customers must install, configure and operate anti-virus software on equipment interfacing with the services, in accordance with industry best practice, except to the extent the Service Description assigns that responsibility to blueAPACHE for a particular item of equipment. Check the terms and Service Description that apply to your agreement.

Are you liable for data loss on customer equipment?

Clause 19.4(b) excludes liability for data stored, processed, transferred or otherwise dealt with in connection with Customer Equipment as part of emPOWER Co-location Services, subject to the terms' preceding liability provisions and applicable law. The separate Customer Data provision in clause 19.4(a) addresses backup and disaster recovery obligations; it does not create an exception to the co-location exclusion.