context

Context Mobile Applications
The growing mobile risk

Mobile computing has transformed the way we do business and allowed organisations to increase productivity and flexibility with anytime, anywhere access to applications and data. But the increasing use of mobile devices and applications to provide portability and convenience comes at a price.

Mobile devices are an extension to your network perimeter, but unlike a server or desktop, they are far easier to lose or steal. And the opportunity to gain access to sensitive personal, proprietary and financial information makes mobile phones, tablets, laptops or even smart watches, prime targets for attack from malicious threat actors.

The risk of a lost, stolen or compromised device is not just about the data stored locally, mobile devices can also provide a direct route into the heart of your organisation through VPNs and workspace browsers. If compromised these could provide a means to reach further into a company's internal network and databases.

Don't leave things to chance

Whatever your industry or size of your organisation, you simply can't afford to ignore the mobile threat and potential financial and reputational damage caused by a serious breach. At Context we can help you to ensure that your users, sensitive data, IT systems and reputation are secure and protected by identifying weaknesses in your mobile applications and the configuration of mobile devices, before they are exploited in the wild. We will also ensure that you are fully-compliant with industry regulatory requirements. We will help you to:

— Protect the confidentiality of potentially very sensitive information at rest, on the device and in transit to mobile APIs.

— Secure information so it cannot be modified by unauthorised individuals.

— Ensure that authentication to and authorisation within a mobile application is handled securely to prevent unauthorised actions taking place.

— Meet industry standards such as PCI, GDPR and Cyber Essentials +.

No stone unturned

At Context, we are nothing if not thorough and our comprehensive mobile security testing will identify vulnerabilities affecting the use of mobile technologies through detailed and audited processes including:

— Manual penetration testing of iOS and Android mobile applications for phones, tablets, laptops and other mobile devices. Our methodology covers industry standard checks such as those defined by OWASP as well as our own checks identified through years of experience. We can also perform testing of iOS applications without needing a jailbreak.

— Code review of mobile applications. This white-box approach goes in-depth into the code of the application, identifying vulnerabilities that may be hard or impossible to expose via a black-box perspective.

E info@contextis.com
T +44 (0)207 537 7515

context

Context Mobile Applications
The growing mobile risk

Code reviews are often performed in parallel with manual testing of mobile applications.

— Policy reviews of enterprise mobility management (EMM) solutions. Our methodology reviews the settings enforced on devices by EMM solutions and checks that they are applied as expected. We can also help you assess any scenarios you may be concerned about. For example, can users install apps outside of the company curated Appstore or is it possible for a user to exfiltrate corporate data from workspace apps to non-workspace apps?

Our mobile security testing can also be run in parallel with our web application testing services. Often the web and mobile APIs are shared and your mobile applications may be an extension of the web app. We can also ensure your MDM (Mobile Device Management) policies are secure, investigate the external infrastructure of API endpoints, perform audits of any cloud-hosted components and check that the builds of your supporting web servers and databases are secure.

What is important is that mobile testing should be treated as a key part of the secure development lifecycle and ongoing security posture of your organisation.

Proof Case – Mobile Testing

Our client came to us looking to have their document sharing application penetration tested. Used by high value individuals in the company, it was imperative that data was secured at rest and in transit. The test was conducted against the iOS and Android versions of the application, including the shared API that handled network communications between the apps and the back-end servers. The client also provided source code of the applications, to assist in the identification of findings.

The first challenge was that the iOS application would only run on a version of iOS that did not have a current jailbreak. Jailbreaking is important as it allows the tester to fully assess the application and how it interacts with the host OS and other applications. But it was possible to use our custom tooling and experience to perform a test of the application without needing a jailbreak. This ensured coverage for the client in the event a jailbreak is discovered in the future for the iOS version supported.

By following our methodology, the Context team was able to identify weaknesses that could allow an attacker, with access to a stolen device, to retrieve authentication details and then use these to gain access to the API and retrieve arbitrary documents. Furthermore, documents that were already downloaded were found to be stored insecurely and from the code review it was identified that an attacker could also escalate their privileges within the application and gain access to administrative functionality.

Following the delivery of the report, the client requested a follow-up retest of the fixes implemented and commissioned mobile application testing training for their developers.

E info@contextis.com
T +44 (0)207 537 7515

context

Context Mobile Applications
The growing mobile risk

Proof Case – Mobile Device Policy

An international corporation was moving from using a bring-your-own-device (BYOD) model to using iOS devices in a corporately-owned, personally enabled (COPE) policy model, which also involved switching its MDM provider in the process. An assessment was performed to ensure the new policies were secure and applied as expected. The impact of a corporate device being lost or stolen whilst the phone is unlocked was assessed, as well as whether employees could remove the protections offered by the MDM policy.

The first stage was to sit down with the client and review the policies being applied to the device via the MDM console. Although largely secure, a number of device operations were allowed, which could result in the disclosure of sensitive company information. Following this, a test device was assessed to see if the policies were applied as expected. Due to several conflicting policy items, some restrictions were not enforced, which put the security of the device at risk.

Finally, time was spent reviewing the configuration of the device against defined scenarios. It was identified that if a device was stolen whilst the phone was unlocked, it could result in client data being compromised as the workspace session timeout was excessive, allowing a user access to the corporate email without the need for re-authentication and only a weak PIN. The MDM compliance policy mandated that if a user removed the policy from the device, a full factory reset was enforced, securing any client data from compromise.

Why Context?

At Context we have been helping businesses to manage their cyber security risk and detect and respond to sophisticated **cyber attacks** for over 20 years. Our specialist services range from penetration testing, red teaming and cyber incident response to product and application security testing.

Technical excellence and trust underpin everything we do. Context is accredited by the NCSC's Cyber Incident Response (CIR) scheme and CREST, the not-for-profit body that sets the bar for penetration testing, incident response and threat intelligence. At Context, our staff are hand-picked from a variety of technical and commercial backgrounds.

The skills, knowledge and experience of our consultants is second to none and many have the highest levels of CREST individual certification. We have also helped to shape the development of the Bank of England's CBEST scheme and accredited to deliver Cyber Essentials and Cyber Essentials +.

So, if you are looking to put your trust in a company that can protect your organisation's assets and good reputation, do not hesitate to contact us.

E info@contextis.com
T +44 (0)207 537 7515

contextis.com
E info@contextis.com
T +44 (0)207 537 7515