Enterprise Mobile Application Security

Mobility has added a new dimension of risk to enterprise data and systems. Mobile device management solutions have quickly evolved to address a number of risks ranging from poor device profiles to user behaviours. The mobile application layer has become more vulnerable to attacks due to below par device, data, and systems, and not surprisingly, attackers have shifted their focus to the mobile application layer. Frequent OS updates and the urgency to release new app features to meet business needs are forcing mobile app developers to adopt agile methodology. This agile methodology necessitates multiple-version releases of the app within a short duration.

This dynamic mobile world does not lend itself to the traditional web app security management model. Enterprises need to develop a mobile-specific security management program that eliminates risk to enterprise data and the network from mobile apps. This article talks about the need for enterprises to build a robust mobile application security program with a focus on how automated mobile security assessments can help an enterprise embed security into an agile software development life cycle (SDLC) of mobile apps.

Introduction

Most enterprises today use mobile apps to stay connected with customers and employees, and while adoption of mobility has increased productivity and resulted in higher levels of user delight, it has also created a new form of risk. Just as with the networked world of desktops, the first wave of threats is from the infrastructure. A new breed of tools such as mobile device management (MDM) then helped mitigate those risks. Now, as other layers of the mobile environment become impenetrable, malicious entities target the application level. A dynamic environment marked by frequent updates/releases by mobile device manufacturers and OS developers, and typically short development cycles with multiple releases make it difficult for enterprises to stay up-to-date as well as ensure safety.

The key to a successful and secure digital strategy therefore lies in implementing a scalable, automated, and robust mobile application security program that integrates into the short development cycles of mobile apps.

Mobile apps: The soft target for security exploits

Insecure mobile application layer. While mobile users, mobile apps, mobile OS, design firmware, OEM customizations, and networks are traditional targets for mobile attacks, new attack vectors such as rogue app stores and malware target user behaviour. Of these, the mobile app layer has proven to be the most targeted area as developers overlook mobile app security best practices. Insecure apps deployed in production systems open up attack surfaces for exploit impacting enterprise brand, customer confidential information, business continuity and intellectual property.

App integrity exploits. Despite enterprises implementing measures to ensure app security, mobile malware continues to be a threat to both corporate and home users. Critical financial apps used by large blocks of customers are often hacked, reverse engineered and misused across Android and iOS platforms. Hacked apps, especially on the Android platform, are commonly repackaged and distributed through third party app stores. The underground hacking community has also introduced variants of mobile rootkits that target the mobile OS, and is finding innovative ways to bypass the security barrier.

Jail-broken or rooted mobile devices. Mobile users who want to download new apps published in third party app stores try to circumvent the OS security controls by jail-breaking or rooting the mobile device. Jail-breaking or rooting a device exposes the mobile device and makes OS security features ineffective. This makes it easy for any hacker to break in and get privileged access to the resources on the device. An enterprise that uses a mobile channel to connect with end customers may not want to debar an end user from using their mobile apps just because the end user's mobile device is rooted. As a result, it becomes imperative for mobile app developers to build mobile apps with in-built security controls equipped with self-defence mechanisms.

It is thus evident that existing security controls are getting increasingly ineffective because of the advanced nature of attacks, and the solution to counter this problem lies in adopting a layered security model fortified up to the application layer.

Limitations of the traditional web app security model

Unlike traditional web apps where control lies on the server, mobile apps are installed on the device. Mobile apps are particularly susceptible to reverse-engineering attacks that expose the code and app logic, allowing malicious entities to identify and exploit vulnerabilities. These mobile apps leave a lot of sensitive information on the device, and it is therefore critical to build security controls into the app. For instance, the onus of handling the transport layer security lies on app developers in the absence of a browser to handle the Secure Sockets Layer (SSL) validation. The biggest fallacy is the belief that merely calling the SSL Application programming interface (API) is enough and it takes care of all validations.

Widespread adoption of mobility has diluted the amount of control enterprises have on mobile operating systems and hardware as mobile device manufacturers and platform developers introduce bug fixes, patches and updates with increasing frequency. These frequent changes requires the app security model to be more agile, which the traditional web app security models lack.

Global bodies such as the Open Web Application Security Project (OWASP) recommend security testing that is heavily inclined towards client-side testing to identify privacy issues, and counter attacks such as structured query language (SQL) injection. The traditional application testing products available in the market are typically web app security testing tools extended to mobile apps. As a result, these tools lack adequate device-side testing capabilities, and also fail to address new types of vulnerabilities that spring up in the mobile ecosystem. It is therefore essential to create a balanced program that can address all the risks without overdependence on a single tool that the enterprise is traditionally comfortable with.

Enterprise mobile app security program – need of the hour

Develop and institute secure mobile app development guidelines - An enterprise with a mature mobile environment should have clearly articulated platform-specific development guidelines to ensure security. The apps should be designed in such a way that they have minimal access to device features and interconnect points within the mobile eco system. By not granting unnecessary permissions to the app, you will minimize the risk of letting other apps on the device exploit the system vulnerabilities. The mobile OS platforms provide a lot of security features such as authentication and encryption support which should be leveraged by the app developers. More often than not, developers tend to believe in security through obscurity and create their own mode of steganography or inappropriately use software development kit (SDK) features. A well-designed developer training and enablement program is therefore critical. Once the mobile app is developed, it is advisable to protect the mobile app against reverse-engineering attacks by using techniques such as code obfuscation.

Establish secure mobile app vetting, approval and deployment processes - Enterprises should invest in non-enterprise apps (third party developed) with caution and assess the risk associated with the mobile app. It is also important to understand the target audience of the mobile app within the enterprise and accordingly manage the distribution of the app. For instance, a third party app that is continuously tracking the location of the device may not be allowed to run on devices carried by executive-level employees. Enterprises can adopt MDM and Mobile App Management (MAM) tools to manage mobile devices and apps.

Integrate mobile security assurance automation in agile development - Every mobile app that goes live in the production environment, should be subjected to detailed security assessment and made free of security issues. Enterprises are in a hurry to get their mobile apps out in the market to catch up with new trends in mobility. To achieve this, most mobile app development now follow Agile methodology, which shortens the app development cycle to a great extent. However, mobile apps, developed using agile methodology, typically have frequent releases and it is difficult to conduct the app security assessment for every release. In this scenario, an automated mobile app security testing product will help swiftly conduct app security assessments at every release. For major updates, mobile apps should undergo penetration testing as well.

Mobile security CoE - A trend that the industry is witnessing is that enterprises are now setting up Centres of Excellence (CoE) dedicated to mobile security with teams to handle all aspects of their mobile environment. Enterprises should adopt a mobile focused approach to address mobile app security risks and invest in setting up mobile security CoE equipped with automated mobile security testing tools and necessary security frameworks. .The CoE defines security governance by integrating people, processes and technology in an optimal organizational structure to deliver secure mobile software in an agile and cost effective way. Continuous improvements are achieved by keeping track of the latest threat vectors, and security breaches and formalizing the necessary changes backed with a metrics program that measures improvements over a period of time.

Conclusion

Given the limited control that enterprises have on the mobile OS platform, network and mobile device features, focus is rapidly shifting to securing the mobile application layer. In addition to MDM/MAM at the infrastructure level, secure SDLC is critical for mobile application development. Enterprises should introduce stringent app development guidelines and adopt robust mobile app security frameworks to conduct security assessment of all the mobile apps in their environment. They should ensure comprehensive security assessment, with emphasis on device-side testing, which is critical in the mobile context.

Using agile SDLC methodology could result in multiple releases because of the fast pace of mobile app developments and shorter development cycles. Performing comprehensive security assessment for every release of the app can thus become cumbersome unless an automated security testing product is deployed.

About the Authors

Col. Rajmohan

Col. Rajmohan currently heads the digital security practice within the Digital Enterprise Unit of TCS. He has 24 years of experience, and his areas of expertise includes application security, identity and access management, cryptography, and infrastructure security. He graduated with honours from NPS, California with a master's degrees in computer security and IT management. Besides having published a number of papers on security through his long career, he has also filed patents on 'Secure Mobile Computing'. Col. Rajmohan is a Certified Information Systems Security Professional governed by the International Information Systems Security Certification Consortium.

Satheesh Kumar

Satheesh currently works as a presales and solutions consultant with the digital security practice of TCS. He has close to eight years of IT industry experience, and his areas of expertise include mobile security, identity and access management and enterprise system monitoring. He holds a post graduate diploma in general management from XLRI Jamshedpur and a Bachelor's degree in computer science and engineering from Visvesvaraya Technological University, Karnataka.

TATA CONSULTANCY SERVICES
Experience certainty.

About Digital Enterprise Unit

The TCS Digital Enterprise unit applies the Digital Five Forces – Mobility and Pervasive Computing, Big Data and Analytics, Social Media, Cloud, and Artificial Intelligence & Robotics – to meet the unique needs and opportunities of each industry. We help clients reimagine their business models, products and services, customer segments, channels, business processes, and workplaces by leveraging a combination of the Digital Five Forces to gain sustained competitive advantage.

Our experienced global team includes business strategy consultants, business analysts, digital marketers, user experience designers, data scientists, and engineers who are passionate about today's digital technologies and their impact on businesses. Backed by our technology vendor partnerships, pre-built customizable products and reusable assets, and deep industry expertise, we offer everything an enterprise needs for complete Digital Reimagination™.

Contact

For more information about TCS' mobile security products and services, email **digital.enterprise@tcs.com**

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India's largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at **www.tcs.com**

IT Services
Business Solutions
Consulting

TCS Design Services | M | 06 | 14