BYOD, Mobile apps and Information Security Trend

The dawn of BYOD and Mobile application Security Threat

Keywords

Security trends in network security, it security trends, mobile data protection, Security Response, encryption, Internet of Things (IoT), Misleading mobile apps

Overview

Today consumers want to use more than ever mobile applications for everything from banking to travelling to shopping. In this context of ever growing cyber-attacks and increasingly connected mobile, social media and cloud services, enterprises IT security must evolve security programs to adapt to these new forces.

If not you, Who? If not If not now, When? If not here, Where?
These devices and applications know where we are, who we were there with, and when we are doing what! We also use them to make phone calls, take pictures, and even video conferencing. To hackers, access to this information can be very valuable.

Now Trending in Digital Technology organization's planning radar

Mobile, social, big data and cloud — are disrupting businesses everywhere by revolutionizing the role technology plays in our everyday lives

Mission Targets

In this article publication, we present a brief insight about mobile business/computing trend and the related critical security requirements and challenges. We also present LONGMAI's security approach that's based on secure element/chip technology to deliver comprehensive, multi-level data protection flowing through applications and underlying platforms.

Definitions:

- **BYOD (aka BYOT), bring your own phone (BYOP | BYOPC**)—refers to the policy of permitting employees to bring personally owned mobile devices (laptops, tablets, and smart phones) to their workplace, and to use those devices to access privileged company information and applications is a popular topic this year as more companies are adopting mobile devices (or deciding against it for security and data control)
- **mToken** is the brand used for all LONGMAI digital security token solutions for both public and private organizations – represents strength and protection of identities, data and network infrastructure.
- **Mobile device management (MDM)** is an industry term for the administration of mobile devices, such as smartphones, tablet computers, laptops and desktop computers. MDM is usually implemented with the use of a third party product that has management features for particular vendors of mobile devices.

Industry Figures: apps & mobile devices

Today, employees want access to all their apps from any mobile device, including their own personal devices. Modern mobile apps have expanded beyond conventional tools and use cases such as mobile email, calendar and contact management.

Gartner, Inc predicts/suggests:

- Through 2015, more than 75% of mobile applications will fail basic security tests.
- By 2017, the focus of endpoint breaches will shift to tablets and smartphones.
- Through 2018, a variety of devices, user contexts, and interaction paradigms will make "everything everywhere" strategies unachievable.

The following insights are extracted from "Internet of Things Study 2015, Volume I by Evans Data Corporation":

- 79% of IoT app developers spend at least 25% of their time with analytics or databases, and 42% work on Big Data or advanced analytics projects.
- 55% of IoT developers primarily connect devices through the Cloud, with 32% connecting through a hub or middle tier.

Mobile Security: a key challenge in Information Security

More employees than ever are demanding access to applications and data that help them achieve maximum productivity outside the office; moreover mobile devices like smartphones and tablets offer new mobility and flexibility for people and IT. But the escalating reliance upon mobile computing has introduced many new security risks hence satisfying mobility requirements is becoming more challenging. For example, allowing users to access all their apps and data from untrusted devices and unpredictable locations can raise significant security concerns and also pose new challenges for information security and privacy.

In most case, to do significant damage in the mobile world, malware would need to act on devices that have been altered at an administrative level for example user deliberately 'jailbreaking' or 'rooting' iOS and Android devices respectively. The 'Rooted' or 'jailbroken' mobile devices also become prone to brute force attacks on passcodes.

Apps trend: Security and the evolving business risks

Mobile applications are changing the way business is done today, offering instant access to services for end-users. As enterprise employees download from app stores and use mobile applications that can access enterprise assets or perform business functions, IT security must evolve security programs to adapt to new forces like cloud, mobile communications and social media. This is because these applications are exposed to attacks and violations of enterprise security policies.

Mobile platforms: Defending against possible attacks

Enterprises that embrace mobile computing and bring your own device (BYOD) strategies are vulnerable to security breaches unless they adopt methods and technologies for mobile application security testing and risk assurance.

Most enterprises are inexperienced in mobile application security, even when application security testing is undertaken; it is often done casually by developers who are mostly concerned with the functionality of applications, not their security. Attackers are taking advantage of this and the many complexities created by the mobile ecosystem to exploit vulnerabilities, resulting in sophisticated fraud schemes and theft of sensitive data.

In this article we argue that the best defense mechanism for mobile security is to keep mobile devices fixed in a safe configuration and follow a mobile device management (MDM) policy or an enterprise mobility management baseline for all mobile devices. Meanwhile, IT security leaders also need to use network access control methods to deny enterprise connections for devices that exhibit potentially suspicious activity and deploy strong identity authentication mechanisms to prevent possible attacks on the core network infrastructure.

LONGMAI Mobile Security Approach

Overview

Today, a majority of companies are concerned about loss of and unauthorized access to corporate data; therefore use of encryption is mandatory as risk control measure for mobile devices. LONGMAI leverages its deep understanding of authentication and mobile technology to deliver trusted and proven solutions while addressing customers' need for mobility.

LONGMAI mToken ecosystem of cryptographic modules support PKI certificate storage used for mobile-based identity and data management (incl. signing/encrypting of email, PDF documents, MS office files, and software applications, as well as VPN and web-based SSL).

The portfolio consists of cryptographic modules meeting industry compliance requirements to ensure secure network authentication, communication encryption and protect sensitive information both on the network and in wireless terminals.

Explorer our solutions:

Mobile: mToken Smart Card microSD

LONGMAI Smart Card microSD is a driverless mass storage PKI carrier with in-built high performance smart-card chip based on SD/TF card interfaces and the SD/IO protocol to communicate with the host device - mainly focused on mobile terminal PKI application to deliver flexible secure storage functionality based on technology.

This portable and easy-to-use solution ensures security by encryption of documents and application data, independent of any operating system or device.

Wireless: Bluetooth LE Wireless Token

LONGMAI mToken Bluetooth LE Wireless Token solution for mobile balances the need for stronger mobile security with user demands for convenience. It natively integrates Bluetooth LE communication and 2FA with electronic signing into mobile applications using standard high level encryption algorithms.

Through our robust library of APIs, developers can extend and strengthen security for all standard and custom applications to deliver unprecedented convenience to end-users. The mToken BLE ecosystem product portfolio offers the highest level of security for multiple form factor certificate-based authentication for mobile users, ensuring security at every level and bringing an innovative inter-connected levels of security to desktop and mobile applications thus reducing threats, combating fraud and also improving the mobile user experience (UX).

In addition, mToken BLE ecosystem can secure logical access control services hosted on any system by USB connection or Bluetooth communication thus making it ideal for use on Windows, Linux, Android, iOS and all mobile terminal supporting Bluetooth standard.

Top-5 Benefits of LONGMAI Mobile Security

1) Innovative and secure exchange and storage of sensitive data with strong 2FA/MFA solutions adopting 32-bit smart card chip technology,
2) Offers high usability and scalability with diverse portfolio of authentication devices that can leverage existing infrastructure,
3) Cost-effective,
4) Support for multiple mobile terminals and desktop OS platforms, thus convenient in situations that require secure authentication even when smart card readers are not available,
5) Highly customizable to enable re-marketing.

Conclusion

As industry departments deploy mobile ecosystem services, there's great potential for expanding business and increase productivity, but also great potential for threats – to organization as well as to employees/customers/end-users; and when it comes to mobile applications, improving security across all areas of an application is critical. Vulnerabilities or weaknesses in any area of a mobile application can open an organization up to risks and may result in serious consequences, including data loss, fraud, loss of revenue, and even damage to brand reputation.

Get Started:

If you are interested in knowing more about deploying secure and convenient technologies or need more information about related pki multi-factor solutions, click download to access the full White Paper.

You can speak to Longmai sales representatives about becoming our **registered partner** (*contact with us to know about the benefits of becoming* Longmai partner) or inquire about our products and solutions and services such as:

- E-Government & Enterprise digital signature solutions
- Software License Protection
- Electronic Document Leakage Prevention(DLP)
- Wireless PKI and Mobile data security
- E-Banking & E-Commerce security
- Network Identity Authentication security
- Product customization and OEM Service
- **White Paper:** *Bluetooth Low Energy in Wireless PKI deployments*

About CENTURY LONGMAI

Established in 2003, Century LONGMAI Technology Co., Ltd is one of the most leading digital security device vendors in China with extended experience in developing latest generation of digital security solutions and products for secure information access and transmission across multiple media. LONGMAI solutions and products are dedicated to help customers and their end-users build safe, efficient and sustainable networks and are widely used by mobile network operators, financial institutions, Governments, Retailers, Transport authorities, software developers and system integrators.

For more information visit, http://lm-infosec.com, or follow us on *@LongmaiInfoSec* on Twitter and *+Lm-infosec* on Google+

3F, GongKong Building, No.1 WangZhuang Rd, Haidian District, Beijing, P.R China
Phone: (86) 10-62323636 Fax: (86) 10-62313636 Email: info@lm-infosec.com