Enhanced Mobile Security using Multi-Factor Biometric Authentication

An Le
Chief Technical Officer,
BluStor PMC, Inc.

BLUSTOR

©2013 BluStor PMC, Inc.

Contents

The Rise of Mobile Computing 3

Multi-Factor Biometric Authentication 5

The Platform 7

Comprehensive Security 9

Password Management and Role-Based Access Control 11

On-Device Biometrics 15

Conclusion 17

©2013 BluStor PMC, Inc.

The Rise of Mobile Computing

The world has gone mobile, and given rise to an urgent need for security solutions that can keep pace. BluStor is the first platform to protect the full stream of mobile security: devices, users, and data.

Thanks to innovators like Apple, Google, Samsung and others, in the span of a few short years we've seen the rise of an entire mobile computing ecosystem of billions of smartphones and tablets, and millions of apps that can be downloaded and run on them.

These platforms give us the power to create, store and access vast amounts of information wherever we roam. And the internet makes it possible to share this information instantly, with anyone, anywhere.

The proliferation of mobile devices and the internet has been a boon to productivity, but it's had unintended consequences, too.

Millions of internet users worldwide experienced a malware or hacker attack in 2012. Losses to fraud and identity theft are in the hundreds of billions of dollars, and set to grow exponentially as billions more mobile devices enter service in the next few years. That's because the security tools relied upon for decades -- PINs and passwords -- simply aren't up to the challenge.

Most providers of service (e.g., banks) require users to authenticate themselves via the use of a user ID and a password. Likewise, companies and enterprises use IDs and passwords for controlling access to company’s servers by employees. Users often choose trivial passwords to make it easy for them to remember. This, in turn, makes it easier for hackers to attack the users and services by guessing the passwords.

©2013 BluStor PMC, Inc.

More sophisticated users may choose to manage various user IDs and non-trivial passwords via a password file or vault protected by a master password or passphrase. Even for these sophisticated users, however, the master password can be vulnerable to malware that records the keystrokes. Regularly running anti virus scanners on computing devices is one of the key safe computing practices. But when a new virus or spyware appears, most anti-malware programs fail to detect it initially.

The goal is to protect data, whether it's user identity data, corporate data, health records, or anything valuable that you don't want made public. Too often, security strategies begin and end with the device. Protecting the device is necessary, but not sufficient.

Instead, we must focus on protecting identities and transactions. And that requires a more sophisticated approach to mobile security.

©2013 BluStor PMC, Inc.

Multi-Factor Biometric Authentication

An effective strategy must address the full stream of mobile security. That's 1) the device; 2) the user; and, 3) data. And, of course, it must do so in a way that's both secure and easy to use.

Finally there are tools available to achieve both convenience and security: Biometrics — those unique personal characteristics like fingerprints, voice, iris, and facial features — are the keys that prove a person's identity with a high degree of accuracy.

A security system that uses multiple types of biometrics meets that requirement. But to implement a sophisticated biometrics-based security system requires quick and secure access to a variety of detailed biometrics files. Where will those files be stored? How will they be accessed?

Of course, to be truly secure you must separate the keys to security from the device. What's known as multi-factor authentication.

Storing and accessing a user's biometric ID files from someplace secure—someplace other than the mobile device itself—satisfies two factors at once. Ideally, the storage device should be something the user can carry at all times. The BluStor card, with its large storage volume, can store templates for various forms of biometric authentication such as fingerprints, iris, facial, and voice.

Depending on the security requirements of an application, biometric authentication can be performed by the BluStor card itself, by a trusted central server, or by a combination of the BluStor card and a trusted central server. In either of these scenarios, the user's biometric features are captured by a reader, camera or a microphone built into or attached to the mobile computing device.

©2013 BluStor PMC, Inc.

As an example, consider the case where a high security application requires a cardholder's voice be authenticated by a trusted central server. While the BluStor card is capable of performing voice authentication itself, the owner/provider of this application desires the authentication to be performed by a powerful central server for performance reason. The BiometricAuth library will establish a secure communication session between the BluStor card and the trusted central server. Since the BluStor card does not have a direct connection to the central server, the communication between the two devices will be conducted through the mobile computing device. The secure communication session, which is protected via encryption by a temporary cryptographic key shared between the BluStor card and the central server, will ensure that critical data exchanged between the two devices cannot be modified by an eavesdropper or a rogue app running on the mobile computing device.

Once a user is successfully authenticated as the cardholder of the BluStor card, he is authorized to use the card in various consumer and enterprise applications.
It should be noticed that the BluStor card is not vulnerable to the attacks via Bluetooth that have been documented. This is because the card does not readily or blindly connect to any Bluetooth device. Depending on the security and operational requirements of an application, the BluStor card can be configured so that it will connect and exchange data with another counterpart Bluetooth device only if both of the following conditions are met:

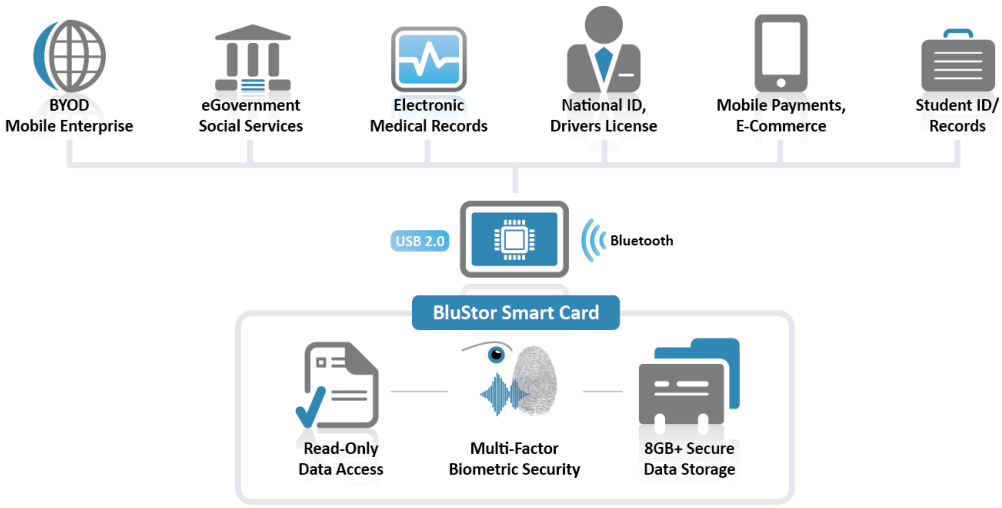
- The BluStor card has successfully verified the certificate of the counterpart Bluetooth device that the latter has been authorized to participate with the BluStor card in designated applications
- The cardholder has successfully authenticated himself to the BluStor card via multi-factor biometric authentication

©2013 BluStor PMC, Inc.

The Platform

Introducing the BluStor mobile security platform. BluStor helps eliminate fraud and identity theft in a mobile world, by using advanced biometric identity authentication to provide answers to two simple questions: “Are you who you say you are?” and “Are you authorized to do this activity?”

BluStor can provide this level of security for every mobile transaction because it has strong encryption capabilities and sufficient storage capacity to allow for match-on-card multi-factor biometric authentication.



BluStor meets all of the requirements for a mobile, secure card platform for high-end applications such as healthcare, eGovernment, and BYOD.

©2013 BluStor PMC, Inc.

Key Features

The BluStor platform contains the following key features:

ISO Compliant

The BluStor cards will conform to several ISO smart card standards, including credit card form factor, the ISO 7816 standards, and standards for biometric verification, cryptographic applications, and card management.

Secure Processor

The BluStor card will use a 32-bit high performance and energy efficient processor with built-in security features that aid greatly in meeting security requirements, including the European EAL 5+ and the US FIPS 140-2.

Wireless Interfaces: Bluetooth 4.0/LE and NFC

The BluStor card transmits data wirelessly via Bluetooth 4.0/Low Energy and NFC wireless protocols. To maximize the number of supported devices, the card can contain a Bluetooth module that operates in dual mode: BLE and EDR. The NFC interface helps maintain compatibility with existing applications and can help automate the pairing of Bluetooth devices.

Bluetooth 4.0/LE (for Low Energy) has become a de facto standard for low-energy wireless communication. Bluetooth 4.0 is now available on many popular mobile devices, including Apple's iPhone and iPad. It is expected Bluetooth 4.0 will be universally available on all new smart phone and tablets within a year or two.

Mass Flash Storage

The BluStor card offers flash storage capacity, configurable up to multiple gigabytes. This will enable users to store various kinds of data, such as biometrics files (e.g., facial, voice, fingerprint) for multi-factor biometric authentication, health records, government records, and other large data files such as music and video clips.

©2013 BluStor PMC, Inc.

Rechargeable Polymer Lithium Battery

The BluStor card contains an ultra-thin, rechargeable Polymer Lithium battery. For some applications that transmit data via the BLE interface, it is expected the battery will provide energy for up to one year in a single charge. With special "energy harvesting" circuitry, the battery life is expected to extend substantially.

USB Interface

The BluStor card provides the USB interface to support compatibility with existing applications where a USB smart card reader is required. This will also enable high-speed transfer of large amounts of data such as high-resolution medical images.

Comprehensive Security

The security architecture of the BluStor card provides flexibility to balance cost with the following security features, depending on the security requirements of an application.

Match-on-Card Biometrics

This feature enables the card to verify a cardholder's fingerprint, voice or iris template that has just been captured against a reference template that is stored securely on the BluStor card. If the verification is successful, the cardholder is authenticated and the card can proceed to carry out an intended function. A fingerprint can be captured by a fingerprint reader in the mobile device, an external fingerprint reader, or an optional fingerprint sensor on the BluStor card.

©2013 BluStor PMC, Inc.

Tamper Detection Circuitry

Tamper detection circuitry zeroizes crucial cryptographic keys whenever a tampering attempt on any element within the physical security boundary of the BluStor card is detected. These circuits include monitoring sensors to defend against probing attacks that attempt to vary operating temperatures or voltages.

Tamper-resistant Coating/Shield

Tamper-resistant coating/shield mitigates physical attacks on the security perimeter of the BluStor card.

Hardware-based Random Number Generator

Hardware-based random number generator (RNG) produces highly random numbers – a feature that is often required in many security applications.

Cryptographic Co-processors

Cryptographic co-processors accelerate symmetric encryption of bulk data and/or asymmetric cryptographic operations for supporting Public Key Infrastructure (PKI)-based applications.

Bluetooth 4.0/LE with Selective Pairing

The BluStor card is not vulnerable to the types of attacks via Bluetooth that have been documented. BluStor card does not connect blindly to another Bluetooth device. Depending on the security requirements of an application, the BluStor card can be configured so that it will connect and exchange data with another Bluetooth device only if both of the following conditions are met:

- The BluStor card has successfully verified the public key certificate of the counterpart Bluetooth device.
- The cardholder has successfully authenticated himself to the BluStor card via multi-factor biometric authentication

©2013 BluStor PMC, Inc.

Secure Code Download

The BluStor card will contain mechanisms for securely updating code and downloading new code. As an example, if a security weakness is discovered in an app implemented on the BluStor card, update code can be distributed via the Internet to BluStor cards in the field, without the need for recalling the cards. For security, an associated digital signature produced by a designated authority will accompany all update code. The BluStor card that receives the update code will accept it only after: 1) it has validated information associated with the code, such as (non-decreasing) version number or the device ID of the card intended for this code update; and 2) it has successfully verified the digital signature on the code and associated information. Besides code updating, this feature can also be used to install new applications on the BluStor card.

In the remainder of this paper, we discuss several possibilities where the BluStor card can be used to greatly enhance security in several enterprise applications.

©2013 BluStor PMC, Inc.

Password Management and Role-Based Access Control

One of the key features of the BluStor card is to eliminate the passwords in any interaction between a user and a mobile device. This is achieved by supporting multi-factor biometric authentication, to reliably and securely authenticate a user/cardholder to the card and the device.

Depending on the security requirements of an application, biometric authentication can be performed by the BluStor card itself, by a trusted central server, or by a combination of the BluStor card and a trusted central server. Regardless of the partition of functions, sensitive data traveling to and from the BluStor card, such as a live biometric template captured by a mobile device, or a success/failure result of a biometric authentication performed by a trusted server, is always encrypted under a temporary session key formed between the BluStor card and the counterpart device. The forming of this session key is the result of a challenge-response process between the BluStor card and the counterpart device and is based on public key cryptography, to ensure the two devices have mutually authenticated each other.

Password Management

Although passwords have been eliminated as a means for authenticating a cardholder to the BluStor card, users, whether enterprise employees or consumers, still need to use matching IDs and passwords to logon to existing accounts. The BluStor card's storage can be used as a secure vault to store user IDs and passwords for all accounts. An app can be developed for various mobile computing platforms to help users manage these passwords. For some platforms, we envision an app can be developed to retrieve the user ID and password from the secure vault of the BluStor card and fill in the appropriate login boxes for a user, thereby making the login process much more user-friendly and at the same time minimizing the potential security problems of password capturing by a key-logger planted by malware.

©2013 BluStor PMC, Inc.

One-Time Passwords

Strategically, the BluStor card is an ideal vehicle for providers of service and enterprises to deploy a One-Time Password (OTP) solution for secure logon. One security advantage the OTP approach offers is that an adversary gains nothing in intercepting a password, as it is used only once. Like the RSA SecurID Token and some other USB and smart card-based security tokens in the marketplace, the BluStor card can produce one-time passwords that users can use to logon to websites and remote servers. However, unlike many of the existing security tokens, the BluStor offers the following advantages:

The BluStor card authenticates a user via biometric authentication before it produces an OTP for the user. Therefore, a user authentication that involves an OTP produced by the BluStor card means it has the security strength of true multi-factor authentication.

The BluStor card has flexibility to provide both the above immediate solution (i.e., the password vault) and the strategic, long term OTP solution. To deploy either solution, a service provider merely needs to provide an appropriate Password Management app for the mobile computing device and a counterpart app for the BluStor card that users can download and install on these devices.

Role-Based Access Control

The BluStor card can also serve as an effective tool for role-based access control. We envision an IT administrator assigning certain roles for a user and granting access to data and applications based on those roles. This can be specified in a matrix that is included in a public key certificate assigned to the user. When a user accesses an application, he presents the certificate to the application for verification. If the user cheats by changing the role-based matrix, the digital signature that accompanies the credential will not be correctly verified and the application will reject the user.

©2013 BluStor PMC, Inc.

Deactivation of access can also be enforced via the BluStor card in a proactive and secure manner, via the digital signature mechanism. For example, in a sensitive project where a user's access rights to applications or documents are required to be validated daily or weekly, the BluStor card can check whether a user's current certificate that contains the access rights is valid or expired. If the certificate is expired, the BluStor card will demand a new certificate signed and issued by a designated IT manager. If no new certificate is presented, or if the digital signature associated with the new certificate is not valid, the BluStor card will issue an authentication failure status to the mobile device.

Remote Enterprise / BYOD

The BluStor card can help IT managers minimize security problems related to remote computing and BYOD. The use of BluStor card helps minimize the number of devices that the IT manager must manage. For example, a user may have a company-assigned laptop, and may bring his iPad to work on some day, and use his iPhone to access corporate data on some other days. In this case, the IT manager may have to manage 3 devices for this user. With the BluStor card, one card can be assigned to protect all those three devices, and the IT manager only need to manage one card for each user.

©2013 BluStor PMC, Inc.

On-Device Biometrics

In the iPhone 5S Apple has introduced a fingerprint technology that replaces the passcode as the means for controlling access to the device. This fingerprint technology, known as TouchID, has been lauded by various well-known technical evaluators. Naturally, this raises the question whether the BluStor Card is still needed or relevant.

These developments simply serve to validate and reinforce the need for biometrics, and the need for BluStor. The biometrics capture capabilities of an iPhone 5S serves to complement, and not compete with, BluStor.

The BluStor card supports multi-factor biometric authentications, including fingerprint, voice, and iris. Already, there has been a report of German hackers breaking the fingerprint reader on the iPhone. With the BluStor card, other biometric authentication methods such as voice and iris can be used in place of the TouchID.

Undoubtedly, Apple can provide a fix for the TouchID technology. Having support for multiple biometric authentication methods provides flexibility to handle situations such as user's fingerprints got dirtied or burned.

Having support for multi-factor biometric authentications will enable a security solution provider to support multi-level security applications. For example, the Apple TouchID technology is used to control access to the iPhone 5S, but once the user is granted access to his iPhone 5S, a secure enterprise email app may require the user to authenticate himself via voice recognition before he can access to his email.

Having multi-factor authentication capability significantly improves the level of security and reliability, bringing this to 6-sigma.

©2013 BluStor PMC, Inc.

Although the iPhone 5S TouchID controls access to the iPhone, it does not control user's unsafe computing practice in downloading apps that may contain malware. A malware may be able to capture a fingerprint of the user stored on the iPhone 5S and send it back to a server for ID theft purpose. [Need to verify this fact]. It is virtually impossible to steal biometric templates stored in the BluStor card, as the card never let this type of information leave its security boundary.

The TouchID technology currently provides only access control to the iPhone 5S. Apple allows this to be bypassed, or the required authentication period can be configured to the user's liking, e.g., 15 minutes, one hour, or 4 hours. During this interval, user's sensitive data stored on the smart phone can be vulnerable if the user is not attending to his device. With the BluStor card, user's sensitive data can be stored in the secure storage of the card, and not on the device. Regardless of the duration that a user configure for his TouchID, if the user does not tend to his mobile device within a predefined period (say, 15 miutes), or if the user walks away from his mobile phone, the BluStor card will disconnect itself.

Last but not least, a general purpose mobile device usually don't have built-in physical security (e.g., tamper-resistant circuitry) like a BluStor card. Thus, even if a mobile device has an effective biometric authentication method to control access, a skilled and well-funded criminal or crime organization may be able to probe the mass storage cells of a lost mobile device and read sensitive information.

There are hundreds of millions of existing smart phones, tablets, and laptops that do not have built-in fingerprint scanners. But they have a camera and a microphone capable of capturing a user's iris, face and voice. And with a Bluetooth communication interface, they can communicate with the BluStor card to create an effective multi-factor biometric authentication solution.

©2013 BluStor PMC, Inc.

Conclusion

At BluStor we started by asking a simple question: "What's possible?"

We realized effective mobile security requires a rethink of what it means to be secure, and our answer is ingeniously simple: a next-generation security platform that is unlike anything available today -- yet uses familiar, field-proven technologies and established security methods -- to provide comprehensive mobile security in a real-world environment.

With its Bluetooth interface, large storage capacity, and multi-factor biometric authentication support, the BluStor card provides a seamless and convenient way to protect the full stream of mobile security: device, user, and data.

©2013 BluStor PMC, Inc.