ENTERPRISES HAVE SMARTPHONE BIOMETRIC OPTIONS

Facial recognition, fingerprint identification are available, but BYOD complicates the matter.

By David Jacobs

BIOMETRIC AUTHENTICATION TECHNOLOGIES are available to protect critical data residing on smartphones and tablet devices and while the options are increasing, enterprise security professionals will find that choosing a single technology could be a complicated process.

The trend toward Bring Your Own Device (BYOD) muddles the selection process because not all authentication methods are available on all phones. Facial and voice recognition methods are either available or can be developed on most phones since virtually all have a microphone and camera. Fingerprint readers are available on only a few phones. When choosing a solution, security
professionals will need to analyze security requirements and the selection of phones in use across the enterprise.

In some cases, custom software development may be required to integrate authentication with applications. Some solutions are provided through phone-resident software while others require interaction with Web or hosted applications.

**Making the Case for Smartphone Biometrics**

Authenticating users of smartphones and mobile device users has become imperative in today’s world. Laptops have long required user authentication since they can typically be used to access a broad swath of confidential data and email. Now smartphones are used in the same way and often receive the same broad network and data access as notebooks, thus they require the same level of security and authentication.

Usernames and passwords/tokens have been effective mobile device authentication methods in the past, but recent malware attacks have demonstrated that additional steps must be taken to prevent unauthorized access to highly sensitive data via smartphones.

For example, the Zitmo variant of the Zeus Trojan has infected thousands of Android-based phones. Anti-virus companies report that new variants have been observed and that the virus is now targeting Blackberry. So far, hackers have focused on bank login credentials, but coupling the same malware technology with spear phishing could enable an attacker to gain access to an enterprise. For situations like this, biometric authentication can add an additional level of security.

**Comparison of Biometric Authentication Methods**

Biometric authentication methods and technologies are based on a physical characteristic of the user, and are therefore difficult for an attacker to copy. Available types of biometric authentication include:

- Fingerprint authentication
- Voice recognition
- Facial recognition and retinal scanning
Fingerprint Authentication

Fingerprint authentication is a highly secure form of authentication since each individual’s fingerprints are unique. The choice of phones with a built-in fingerprint reader is currently limited. The Motorola Inc. ATRIX 4G Android phone includes an integrated fingerprint reader. The Fujitsu REGZA and more recent ARROWS models include a fingerprint reader, but neither phone is available in the US.

Both the Motorola and Fujitsu products rely on hardware and software from AuthenTec, Inc., but the future is unclear for these products. Microsoft in July offered to buy AuthenTec. In September the press reported that AuthenTec had informed its non-Apple customers that it will not offer its products to them in 2013. The sale was completed in early October.

Other vendors offer fingerprint technology. Innovatrics offers software for Android, iPhone and Windows, but the products were originally developed for PCs and must be integrated with an external fingerprint reader. Neurotechnology also sells a product developed for PCs and also requires an external reader. Aware Inc. offers fingerprint authentication software and engineering services for Android, BlackBerry, iOS, and Windows.

Apple iPhones do not include a fingerprint reader but Precise Biometrics has developed Tactivo, an iPhone case with an integrated fingerprint reader. The case slides over the phone, connects to the phone via the standard 30-pin connector, and includes a slot on the back that accepts a smartcard. Precise Biometrics provides an iOS toolkit that can be used to create and integrate authentication solutions using the fingerprint, the smartcard or both. Tactivo currently supports only the iPhone 4 and 4s.

Voice Recognition

Voice recognition performs authentication by matching the smartphone user’s voice against a pre-recorded sample. No specialized hardware is required since all phones include a microphone. Voice recognition is not appropriate for phone users who need to access their phones to check email during meetings, presentations or other events when speaking into the phone is not acceptable behavior.

PerSay Ltd., recently acquired by Nuance Communications, has developed a product that requires a caller to authenticate by repeating a passphrase. Another
**MOBILE AUTHENTICATION**

PerSay product requires no passphrase, but monitors the caller’s speech for several seconds to determine whether the caller’s voice matches a pre-recorded sample. All software executes on a server at the customer site.

PhoneFactor Inc. and Rapidsoft Systems Inc. both offer host-based voice authentication software that works with any phone. Users access a website and speak a passphrase. Software on the host verifies the user against a pre-recorded voice sample. A Software Development Kit (SDK) is provided so partners can integrate the products with other server-based applications. Rapidsoft also offers professional services to aid in this integration.

### Facial Recognition, Iris Scanning, Retinal Scanning

Facial recognition performs authentication by matching the picture taken by the phone’s camera to a previously taken picture of the authorized user. Nearly all phones now include a camera, making facial recognition a readily available biometric option for a wide variety of customers. The recently released Samsung Galaxy S III comes equipped with apps that implement both facial and voice login.

Multiple vendors provide SDKs and engineering services for integrating facial recognition for each phone technology. Animetrics Inc., Solidpass and Visidon Ltd. product offerings include SDKs that security staff or integrators

<table>
<thead>
<tr>
<th>BIOMETRIC METHOD</th>
<th>ADVANTAGES</th>
<th>DISADVANTAGES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprint authentication</td>
<td>Fingerprints are unique to individuals.</td>
<td>Currently available on only three released phones; requires integration with network access software</td>
</tr>
<tr>
<td>Voice recognition</td>
<td>No extra hardware required.</td>
<td>Not viable in settings where user must remain quiet</td>
</tr>
<tr>
<td>Facial recognition and retinal scanning</td>
<td>Extra hardware not usually required; many available applications.</td>
<td>Does not work well in low light. Reports that it’s possible to defeat authentication with a picture of the phone owner</td>
</tr>
</tbody>
</table>
can use to integrate with network access software.

Iris or retinal scanning technology has not yet been made widely available, but Bi2 Technologies’ Mobile Offender Recognition and Identification System (MORIS) product is currently in use by police forces.

In choosing a solution, be aware that what is sometimes described as a ready-to-deploy solution for voice or facial authentication may control access to remote resources only. Access to data resident on the phone is not protected. These solutions are sufficient where all that is required is user authentication before creating a VPN link. Where critical data is stored on the phone itself, it may be necessary to modify or create phone-resident code to protect access to that data.

Before recommending an authentication method, consider unique user requirements. Factor in the environment where the phone will be used, the types of information that employees will access or download to their phones, and how valuable information would be to an attacker. For some employees, passwords may be sufficient, while the CFO and financial staff may require a highly secure solution.

As in the case with all aspects of security, no solution is static. It’s essential that security professionals constantly monitor emerging threats as well as newly available authentication products.

David B. Jacobs of The Jacobs Group has more than 20 years of networking industry experience. He has managed leading-edge software development projects and consulted to Fortune 500 companies as well as software start-ups.