

Biometric authentication for user access security

Solution Brief

Enterprise customers need a way to insure that only authorized users have access to their information assets. The right security solution has to correctly identify users, log every access event, and notify the security team of an attempted security breach. The Townsend biometric solutions provide the strong authentication needed to secure systems, data, and business applications.

User authentication – the security challenge

Security professionals know that passwords are a poor way to secure access to any IT system. Good passwords are hard to remember, and users often store them on paper or in unsecured documents where they can be easily compromised. Users have an unfortunate tendency to share their user IDs and passwords with others. They have demanding business objectives to meet, and it is easy to bypass the corporate security policy to get work done.

Even more worrying is the advance in software and computing power that makes breaking passwords much easier. It might not be possible to break strong encryption, but it is easy to break the passwords that control it. How can a company be sure that users of their information assets are actually who they say they are, and how can you know when violations of policy occur?

This is where biometric access controls, specifically fingerprint authentication, can fill the security gap. As law enforcement has known for years, a fingerprint is a very good method of identification. This paper discusses how the Townsend solution for fingerprint biometric access control helps you meet your companies' security needs.

Biometric technology overview

The technology for fingerprint scanning has improved dramatically over the years and is now in regular use to secure access to buildings and facilities. Now biometric readers can be used to secure information assets. At about one fourth the size of a PC mouse, modern biometric readers are far more reliable than the typical laptop fingerprint reader, and are easy to use with a PC or laptop. With the appropriate software you can now protect information assets on your application servers, including your IBM Enterprise servers, without impacting productivity.

The software that accompanies biometric solutions falls into four categories:

- User and system administration
- Application integration
- Audit reporting
- Access monitoring and alerting

A security administrator enrolls users through an initial fingerprint scan and associates the user with a computer account. The administration software can be distributed, as well as the systems that are being protected. The application integration software is used to control the actual logon to a computer system, database, or application. This is the component that actually reads the fingerprint and allows or denies access to the user. The audit reporting modules provide the compliance reports you need for the compliance team. The final software component includes real time monitoring of security failures and the sending of alerts to security staff to help you identify potential threats.

Shared user accounts and passwords

All security administrators know that users are often careless with their passwords. In spite of company policies prohibiting password sharing, it is a common practice and hard to control. Because strong passwords are hard to remember, users often write them down or store them in un-secure documents. These practices defeat the attempt to insure that systems are safe. Biometric controls are an excellent method of “defense in depth” for your IT systems. You can greatly reduce the risk of password sharing and password loss using fingerprint scanning technology.

Sometimes it is necessary for more than one person to know an account password. For example, the root or security password is generally known by two or more trusted individuals. When password sharing is required, how can you know who actually signed on at any point in time? Data security regulations require that you track this information, but it can be hard to do. Biometric controls provide the answer. Even if you share a privileged account among two or more users, biometric access logs will always provide you with an audit of who used the account because the audit trail is maintained by fingerprint, not account name.

Eliminating the threat of weak passwords

In one demonstration of how easy it is to break password controls, a security expert used freely available software on the Internet to discover a password to an encrypted Zip archive file. The user assumed that the password was secure because it was eight characters long, contained upper and lower case characters, numbers, and special characters. But it only took a few minutes to break the password using a brute force attack. The data was secured with strong 256-bit AES encryption, but the password was easy to break resulting in the exposure of the data.

In most cases, Enterprise servers and databases are secured with the same type of password control. Biometric controls strengthen password security to eliminate this type of loss. When combined with proper system monitoring and logging you can eliminate the inherent weaknesses in the use of passwords.

Securing data with biometric controls

In addition to securing user access to your systems, you can also implement biometric access controls on your IBM System i databases. You may have sensitive payroll or credit card information on your server and want to restrict access to specific individuals. You can implement biometric control at the database level to meet this challenge. Through the use of standard database triggers and biometric integration APIs, you can enforce biometric authentication before a user is allowed access to data. In addition to controlling access to data, you also create a permanent audit log of authorized access to the data.

Securing applications with biometric controls

In the same way that you can secure your data using biometric authentication, you can secure your business applications. For example, if you have a Human Resources application that allows a user to view and change salaries and benefits, you can secure this application directly with biometric access controls. The same permanent audit trail and monitoring functions help you meet regulatory requirements.

Adding biometric authentication to encryption

Strong encryption is used to protect credit card numbers, social security numbers, and other sensitive data. You can now add biometric access control to encryption or decryption requests when you combine the Townsend Alliance AES encryption solution with Townsend biometric access controls. Special encryption and decryption APIs enforce biometric authentication before allowing a user to decrypt and view data. The same principal of "defense in depth" can be applied to your encryption solution that you apply to user access to your systems.

Compliance

Many compliance regulations require that you collect information about user access to your systems, and review this information on a regular basis. These regulations include the Payment Card Industry (PCI) Data Security Standard, the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley (SOX) Act, and the Gramm-Leach-Bliley Act (GLBA). The biometric access controls implemented by Townsend provide full system logging of biometric security events as well as a permanent audit trail of user access. You can use the built-in reports to meet your compliance requirements.

Monitoring and alerting on biometric access failures

Biometric access controls give you the additional security you need for your sensitive data assets, but you also need pro-active monitoring and alerting when biometric access controls block user access. Townsend biometric access controls also include system logging to the IBM System i audit journal QAUDJRN for a permanent security record of the event. When combined with the Alliance LogAgent for System i product, you can fully integrate security events with your system logging consolidation solution and Security Information Management (SIM) product. Biometric security events can be monitored and alerted by any standard SIM product.

Alliance biometric solutions from Patrick Townsend & Associates

Townsend security solutions span a broad array of applications and platforms. On the IBM System i platform you can deploy biometric access controls to protect your

legacy applications, for user access control, and with strong data encryption using the Townsend AES encryption solution. You can also secure data transfer with the Townsend FTP, XML, HTTP, WebDAV, and AS2 transfer security solutions.

Supported platforms

The biometric authentication solutions from Patrick Townsend & Associates let you implement protection on a variety of platforms including:

- IBM System i
- IBM System z
- Microsoft Windows
- Linux (Red Hat, SUSE, etc.)
- IBM AIX
- Sun Solaris
- HP-UX

Biometric administration is performed at a standard PC using Microsoft Windows. The Biometric server runs on an IBM server appliance.

Implementation and development services

If you need assistance installing, configuring and enabling your systems for biometric access, Townsend can help you with your project. Contract services are available to implement biometric software controls and train your users and system administrators. Please contact your account representative for more information.

System security assessments

Many security administrators conduct a full system security audit when they start a new access control project. We can help you with your IBM System i security audit through our security services assessment team. We will bring seasoned System i security professionals to your assessment project to help you identify potential problems and how to correct them. In addition to identifying potential security weaknesses the assessment will help you define a roadmap for strengthening your system.

Patrick Townsend & Associates

Patrick Townsend & Associates provides security compliance solutions to Enterprise customers. Solutions include NIST certified AES encryption, encryption key management, system logging, assessment, and access security controls. The company can be reached on the web at www.patowndsend.com, by phone at (360) 357-8971 (International calls to +1 360 357 971).