Two Factor Authentication on the IBM i:
Security Beyond Usernames and Passwords

IN THE WAKE OF WIDELY PUBLICIZED DATA HACKS, ACCOUNT TAKEOVERS, AND THE LOOMING THREATS OF IDENTITY THEFT, many enterprises are reevaluating their strategies for authenticating end users with methods that are stronger than traditional passwords.

Today's organizations must take a defensive strategy against the constant threat of network breaches. Recent password leaks from high-profile sites suggest that their sensitive data may not be as secure as once thought. Companies and web properties have to do a better job protecting security credentials.
Executive Summary

Of the myriad threats that face companies, account compromise stands out as one of the most easily addressed with available and mature security technologies. Nonetheless, compromised email, social media, online gaming, eCommerce, financial services and other types of cracked accounts continue to threaten both personal and corporate well-being.

Historically, companies used physical tokens to provide authentication on the IBM i beyond username and password. Even if someone hacked a user’s password, they still could not login without the physical token. However, tokens are not foolproof as the recent attack on RSA proved.

Tokens represent another layer of protection, called two-factor authentication, which is a step in the right direction. Unfortunately, tokens increasingly do not make fiscal sense for enterprise IT departments who have to deploy, manage, and troubleshoot these tokens. How do organizations quickly and cost-effectively rollout two-factor authentication to a large and sometimes global user base?

Innovative solutions that leverage the phone as a reliable means of out-of-band authentication have emerged. For example, instead of tokens, businesses can simply send an SMS or voice message that contains a one-time authentication code to the IBM i user’s phone. This means cyber criminals cannot log into the IBM i without physical control of the actual phone.

This white paper examines the nature and the extent of this security threat on the IBM i, and presents two factor authentication as a viable solution for meeting compliance regulations and safeguarding the vast amount of data and numbers of users with access to sensitive information on the IBM i.

INDUSTRIES

While all industry segments have an interest in securing company digital assets and the data of their customers, professionals from the following industries will benefit most from reading this document.

Education: Protecting the provisioning of internet access, email, research resources, grades, enrollment, financial aid, and endowment information for faculty, IT staff, students, and alumni

Financial Services: Safeguarding access to banking, trading, and other types of high-value services by authenticating login, transactions, and account management activities

Health Care: Ensuring privacy of patient and provider information for online insurance claims, Rx requests, provider correspondence, etc. in conformance with HIPAA and other regulatory regimes

Retail: Safeguarding online transactions, consumer accounts, and sales channel management
The IBM i May Not Be As Secure As You Think

The IBM i platform has a well-earned reputation for security. But IBM i security is only as strong as the weakest point in the enterprise network. User PCs, internal and external web servers, and network applications represent points of attack. These systems are not secure from:

• Memory scraping
• Keyboard logging
• Stolen vendor credentials
• Stolen user passwords from external web services

The Need for Verification

The media, enterprise IT, corporate management and interested end users spend increasing time, energy, and funds on securing digital and physical assets with technology of growing complexity. Strong encryption, multifactor biometrics, intrusion detection, anti-malware software, and other advanced security measures provide necessary protection against a range of threats, but a simple truth remains: verifying computer-systems users provides the greatest return on security investment. Verification before a transaction (or a security breach) occurs is always cheaper and more effective than attempting to remedy the consequences of failing to do so.

Verification is not merely a piece of larger security regimes. Verification lets users, employers, and vendors build and leverage online reputation for applications that include:

• Protecting account access
• Preventing bulk account registrations
• Securing eCommerce transactions
• Enabling trusted password reset
• Verifying businesses

In short, verification is key to securing IBM i activities where knowing who is attempting to access digital assets is as important as what that person is doing.

Verification Helps Mitigate Corporate Risks

Popular literature and media hype of Internet security may highlight personal risk from attacks on private assets, but businesses have even more to lose from compromised security:

IDENTITY, ASSETS AND REPUTATION AT RISK

End User Risk

• Loss of account access and use
• Unauthorized change of mailing address and related information
• Compromised address books including information on friends and associates
• Destruction of historical data (email messages, gaming archives, etc.)
• Hijacked account for spam and DDoS
• Impersonation for purposes of fraud
• Exposure of personal data, especially financial or health-related information
• Unauthorized purchases and other financial transactions
• Degradation of credit rating and other online reputation factors
• Comprehensive identity theft - national identity numbers, credit card accounts, etc.

Corporate Risk

• Loss of customer trust
• Loss of customer and trade
• Site or service blacklisting as source of spam
• Degradation of user experience and failure to meet terms of SLAs
• Damage to brand and reputation
• Exposure of trade secrets and other proprietary information
• Indemnification and recovery costs
• System-wide remediation costs
• Regulatory compliance failure
• Legal liability from leakage of customer data and resulting damages
• Individual and class-action lawsuits
Critical Data and Operations
The average business keeps a range of records and runs a plethora of activities online. These assets and applications range from the mundane to business-critical, and in some cases, to life-critical (as with medical or national security concerns): accounting/finance, sales and customer relations, business intelligence, legal, engineering, manufacturing and production, human resources, and more all rely on online applications and stored data. And these data and apps are vulnerable to the scourge of cybercrime, from vandalism of corporate sites to industrial espionage to wholesale data theft and exposure of proprietary company, customer, and employee information.

Reputation
The costs to patch a vulnerability, to upgrade software, to repair vandalized resources and otherwise recover from failed security measures can be high but not usually debilitating. Companies are more hard-pressed to recover from loss of reputation and public trust. Years of effort and millions of dollars of investment in quality assurance and branding can vanish in the hours and days following a publicized attack.

Verification and FFIEC Compliance
Threats to online accounts are not a recent phenomenon. In 2001, in response to threat levels of the day, the Federal Financial Institutions Examinations Council (FFIEC) issued guidelines for Authentication in an Internet Banking Environment, providing minimum expectations for authentication of “high-risk” online transactions involving customer access to critical information and/or movement of assets.

While security by government fiat may not itself be viable, the FFIEC guidelines do a good job at laying out the scope of threats to banks and other online institutions.

Key Points from FFIEC Guidance
- Account fraud and identity theft are frequently the result of single-factor authentication exploitation (e.g., ID/password)
- Single-factor authentication, as the only control mechanism, is inadequate for high-risk transactions involving access to customer information or the movement of funds
- Authentication techniques employed by financial institutions should be appropriate to the risks associated with those products and services
- Doing business with unauthorized or incorrectly identified persons in an Internet banking environment can result in financial loss and reputation damage through fraud, disclosure of customer information, corruption of data, or unenforceable agreements
- The success of authentication methods depends not just on technology but also on appropriate policies, procedures, and controls
- Effective authentication methods should have customer acceptance, reliable performance, scalability to accommodate growth, and interoperability with existing systems and future plans

These guidelines were very ambitious at the time of their creation, and still remain daunting to many financial institutions tasked with implementation.

Verification and PCI DSS Compliance
IBM i customers who process credit card information must meet the PCI Data Security Standards requirement for verifying remote users. Remote users are defined as those who are connecting to the IBM i platform from outside the Cardholder Data Environment (CDE). This requirement would apply to most internal users who access the IBM i server from within the processing facility if the connection originates or connects to non-CDE networks. Two-factor authentication would then help meet PCI DSS requirements.

PCI DSS Requirement 8.3
8.3 Incorporate two-factor authentication for remote network access originating from outside the network by personnel (including users and administrators) and all third parties, (including vendor access for support or maintenance).

Key Points from PCI DSS Guidance
- Two-factor authentication requires two different forms of authentication for higher-risk accesses such as those originating from outside the Cardholder Data Environment (CDE).
- This requirement is intended to apply to all personnel—including general users, administrators,
and vendors (for support or maintenance) with remote access to the network—where that remote access could lead to access to the cardholder data environment. If remote access is to an entity’s network that has appropriate segmentation, such that remote users cannot access or impact the cardholder data environment, two-factor authentication for remote access to that network would not be required. **Note that many IBM i customers provide access to the CDE network from internal non-CDE networks. In this case it is prudent to require two factor authentication even though the user is not remote in a geographical sense.**

- However, two factor authentication is required for any remote access to networks with access to the cardholder data environment, and is recommended for all remote access to the entity’s networks.
- PCI also states it is recommended for all remote access, regardless of if it hits CHD environments, which is an absolute requirement for remote access to a CHD environment.

### Using the Phone to Enhance Security

Mobile phones are today the most ubiquitous devices on earth. In fact, mobile phones are so pervasive that Silicon India recently reported that the number of active cell phones is expected to reach 7.3 billion by 2014. Complement that number with 1.2 billion landlines and a growing number of Internet (VoIP) phones and the total number of phone exceeds today’s global population of nearly 7 billion people.

Mobile phones and landlines present key advantages for verification and authentication regimes:

- They possess unique identifiers – phone numbers, electronic identifiers and account numbers
- They remain in the possession of users or near at hand most of the time
- They are difficult to spoof
- If stolen or otherwise misappropriated, they are easy to disable
- Their association with actual individuals is verifiable through the operators that provide phone service

While none of these attributes by itself is sufficient, together they provide a compelling basis for verification and authentication.

### Two Factor Authentication on the IBM i

Alliance Two Factor Authentication brings mobile SMS and voice two factor authentication to the IBM i platform. IBM i customers can significantly improve the security of their IBM i systems through implementation of proven two factor authentication.

Alliance Two Factor Authentication lets your users select to receive authentication messages as SMS text messages to their mobile phone or as voice calls to their mobile or standard phone. You can define up to five phone numbers to receive messages, and the user can select which phone number to use each time they perform an authentication. Because some IBM i users have poor mobile cell phone coverage when away from work, you can easily define a home phone number or alternative number for authentication. Alliance Two Factor Authentication will remember your preferred phone number and method of delivery.

### IBM i Logon Two Factor Authentication

The primary way that users authenticate to the IBM i platform is through the 5250 terminal logon panel. A user types a user profile name (account) and a password or passphrase. You can easily change the user profile to use the initial program provided in the Alliance Two Factor Authentication solution.

Alliance Two Factor Authentication makes it easy for a security administrator to implement two factor authentication for a user. A list of users is displayed with their current security level (high, medium, low) and the current setting for their initial program. Typing a single option next to the user profile will install the Alliance Two Factor Authentication initial program on the user profile. The next time the user logs on, the two factor authentication will be in effect.
For IBM i customers who have created their own Initial Programs for user profiles, you can easily call the Townsend Security logon initial program from your own application to implement two factor authentication logon security.

Security administrators can choose one of two options for two factor authentication failures:
1. Immediately log the user off
2. Disable the user profile and log the user off

When activating two factor authentication security, security administrators have the option of using a “Preview” mode. When in preview mode a user will be prompted for two factor authentication, but a two factor authentication failure will not prevent them from continuing to their normal application. They will have the ability to contact the security administrator and resolve any problems. Once in normal two factor authentication activation mode, two factor authentication failures will not allow use of the system.

### IBM i Application Program Interfaces (APIs) for Two Factor Authentication

IBM i customers want to implement Two Factor Authentication for critical or sensitive application functions. You might want to use two factor authentication when financial transactions are above a certain amount. Or you might want to use two factor authentication when critical system restore functions are initiated. For any sensitive application requirement you can call the Alliance Two Factor Authentication API to force a two factor authentication sequence. Your application will receive notification of the success or failure of the two factor authentication operation and can take appropriate action.

### Web Applications and Two Factor Authentication

IBM i web applications can also perform Two Factor Authentication by using the Alliance Two Factor Authentication application program interfaces. Java, RPG, and other web application languages can easily call the application program interfaces to retrieve the valid phone numbers for a user, then perform authentication. If authentication fails, the web application can take the appropriate steps to prevent access.

### Verification with TeleSign

Two Factor Authentication based on voice call and SMS technologies is only as good as the service that delivers the authentication information. TeleSign is an experienced and mature global provider of two factor authentication services to large and small organizations. With the ability to deliver voice and mobile messages to every country, even large IBM i customers can rest assured that their two factor authentication needs will be met regardless of the location of their international sites.

Townsend Security has partnered with TeleSign to deliver the Alliance Two Factor Authentication solution. When you license and install the Townsend Security two factor authentication solution, you will also be provided with a TeleSign account and authentication information.

### Conclusion

Passwords are no longer good enough. Security professionals understand this, and the on-going flood of data breach news just confirms this on a daily basis. We aren’t going to stop using passwords on our IBM i platform, and we aren’t going to stem the flood of attacks any time soon. We can take a giant security step forward by implementing two-factor authentication to dramatically reduce the risk of a security breach. Major web sites like Google, Yahoo and others have already taken the leap, and IBM i users now have an affordable solution for their platform.

### Learn More About Alliance Two Factor Authentication on the IBM i

Alliance Two Factor Authentication brings mobile SMS and voice two factor authentication to the IBM i platform. By requiring an additional piece of information delivered to authorized users via SMS text or voice message, organizations can improve security of their core business applications. IBM i customers
can significantly improve the security of their systems without the added expense of security tokens or appliances.

---

**About TeleSign**

Every second, of every day, TeleSign protects the world’s largest Internet and Cloud properties by establishing and verifying Mobile Identity. Digital businesses use TeleSign’s Mobile Identity platform to preserve their ecosystem by detecting a suspicious user before account creation, and to better protect their existing user base from account compromise.

TeleSign is trusted by the world’s largest companies and protects 2.5 billion accounts in more than 200 countries and in 87 languages.

---

**Townsend Security**

Townsend Security creates data privacy solutions that help organizations meet evolving compliance requirements and mitigate the risk of data breaches and cyber-attacks. Over 3,000 companies worldwide trust Townsend Security’s NIST-validated and FIPS 140-2 compliant solutions to meet the encryption and key management requirements in PCI DSS, HIPAA/HITECH, FISMA, GLBA/FFIEC, DIACAP, SOX, and other regulatory compliance requirements. Learn more at [www.townsendsecurity.com](http://www.townsendsecurity.com).

**Web:** [www.townsendsecurity.com](http://www.townsendsecurity.com)

**Phone:** (800) 357-1019 or (360) 359-4400

**International:** +1 360 359 4400

**Email:** info@townsendsecurity.com

---

**Additional Resources**

**Product:** [Alliance Two Factor Authentication](http://example.com)

**Evaluation:** [Alliance Two Factor Authentication](http://example.com)

**Webinar:** [Two Factor Authentication and the IBM i](http://example.com)

**Podcast:** [Two Factor Authentication on the IBM i](http://example.com)