BITS

FINANCIAL SERVICES ROUNDTABLE

BITS EMAIL SECURITY TOOLKIT: PROTOCOLS AND RECOMMENDATIONS FOR REDUCING THE RISKS

A PUBLICATION OF THE
BITS SECURITY AND RISK ASSESSMENT WORKING GROUP

April 2007

BITS
The Financial Services Roundtable
1001 Pennsylvania Avenue NW
Suite 500 South
Washington D.C. 20004
(202) 289-4322
www.bitsinfo.org

BITS EMAIL SECURITY TOOLKIT: PROTOCOLS AND RECOMMENDATIONS FOR REDUCING THE RISKS

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Email is now a primary means of communication from financial institutions to their customers and from financial institutions to other financial institutions and service providers. However, email is insecure and therefore fraught with risks. The medium lacks confidentiality and integrity unless uniform and explicit controls are put into place. Fraudsters and scammers are leveraging the convenience and cost-effectiveness of email to compromise the security of customer accounts and to undermine the reputations of financial institutions. While there are no "silver bullet" solutions, some of these risks can be mitigated by implementing existing technologies and protocols.

This *BITS Email Security Toolkit: Protocols and Recommendations for Reducing the Risks* is the result of cooperative industry-led efforts initiated through BITS to identify the best available current technologies for improving email security. The result is a set of recommendations for implementation of three specific technologies and associated processes. These protocols may be used to mitigate some of the inherent insecurities in the current email infrastructure and its deployment. Through cooperation among financial institutions and with key stakeholders, including Internet Service Providers (ISPs), the financial services industry can lead the way to increase email security and restore customer confidence in email as a channel of communication with financial institutions. Beyond the scope of this *Toolkit*, additional work will need to be accomplished by the product vendors, ISPs and other industry partners to develop true end-to-end solutions that will drive customer confidence.

In 2006, members of the BITS Security and Risk Assessment Working Group embarked on a project to enhance the security and integrity of email communications. The goals of the BITS Email Security Project were to:

- Enhance the security and integrity of electronic mail communications;
- Reduce the amount of phishing and malicious code (e.g., spyware);
- Improve confidentiality and integrity of information exchange among financial institutions and between financial institutions and their customers and clients;
- Strengthen protection of customers and their accounts from identity theft and account fraud; and
- Restore greater reliability of the email delivery channel for financial institutions.

These goals may never be achieved absolutely, but financial institutions can improve on the current situation and make email a more secure and useful tool for the conduct of business.

The BITS Email Security Working Group recommends the adoption of three specific technologies to enhance email security:

- **Transport Layer Security** (TLS);
- **Sender Authentication**—Sender ID Framework (SIDF) or Sender Policy Framework (SPF)); and
- **DomainKeys Identified Mail** (DKIM).

Transport Layer Security (TLS) technology protects confidentiality and data integrity as it automatically authenticates servers and encrypts email messages between the servers. This encryption reduces risk of "man-in-the-middle" attacks by authenticating the servers and reducing the amount of traffic that is passed in clear text.

Sender Authentication (SIDF/SPF) provides a way for financial institutions, ISPs and others to identify the authorized mail servers for a particular domain and validate that mail originated from these authorized sources. Through implementation of Sender Validation checks by both financial institutions and Internet Service Providers, institutions will help reduce the fraudulent mail received by their customers. Customers will be less likely to be exposed to, and therefore less likely to respond to, phishing and other malicious email-based attacks. This, in turn, will reduce the amount of identity theft and account fraud activity initiated through fraudulent emails.

DomainKeys Identified Mail (DKIM) is a cryptographically based protocol that provides message header and body integrity verification mechanisms. It provides a mechanism for authenticating and determining the authorization of email from a domain. Its policy component is critical to providing protection against exact domain phishing and forgery.

Each of these technologies is gaining wider acceptance, is becoming more transparent to the end user, and is relatively inexpensive to implement and maintain. Each of these protocols addresses a particular problem. The protocols can be used in conjunction with each other as part of a layered approach to security.

This *Toolkit* includes specific recommendations for each of the protocols. In addition, there are several overall recommendations:

- **Implement each of the recommended technologies within 18 months.**
- **Promote awareness of email security** concerns among financial institutions, clients, consumers, Internet Service Providers and Mail Service Providers.
- **Engage and encourage service providers to implement the recommended technologies.**
- **Add email security requirements to contracts** with business partners and service providers.

The BITS Email Security Working Group has established a timeline for implementation of these technologies and urges all financial institutions to participate. In addition, the BITS Email Security Working Group will engage the leading ISPs and other stakeholders to urge them to cooperate in developing end-to-end solutions. The effectiveness of this Email Security Project is enhanced by industry-wide participation. In addition to urging implementation on a definite timeline, the BITS Email Security Working Group will, over the duration of the implementation schedule, survey BITS member companies to evaluate progress in improving and achieving email security.

For Additional Information, contact:
John Carlson, Executive Director, john@fsround.org
John Ingold, Director, johni@fsround.org
BITS, (202) 289-4322
www.bitsinfo.org

BITS EMAIL SECURITY PROJECT GOALS AND DESCRIPTION

When established in 2006, the goals of the BITS Email Security Project were to:

- Enhance the security and integrity of electronic mail communications;
- Reduce the amount of phishing and malicious code (e.g., spyware);
- Improve confidentiality and integrity of information exchange among financial institutions and between financial institutions and their customers and clients;
- Strengthen protection of customers and their accounts from identity theft and account fraud; and
- Restore greater reliability of the email delivery channel for financial institutions.

The key components of the BITS Email Security Project include:

- Outlining existing email security problems and the importance of this project to the financial services industry;
- Seeking agreement within the financial services industry for an implementation strategy for these protocols;
- Engaging key Internet Service Providers (ISPs) and other important stakeholders from the vendor community to solicit broader adoption of and support for these protocols; and
- Developing a strategy for communicating this effort with media, regulators, and policy officials.

THE PROBLEM AND ITS IMPORTANCE TO FINANCIAL INSTITUTIONS

BITS and its member financial institutions believe the adoption of email security controls and coordination between financial institutions, ISPs, and other stakeholders will both improve confidentiality and integrity of information exchange and will reduce phishing and other forms of malicious email that adversely affect customers and the availability of email services. The key reasons for engaging in this effort are to improve email security and to restore consumer confidence in the email delivery channel.

Spam is increasing at a rapid pace. BITS member financial services institutions have reported that spam activity increased over 400% between February and December 2006. One large institution recorded an increase in spam from 3 million messages per day to 13 million messages per day. Most institutions find that unwanted email represents over 85% of all mail received.

Phishing is swiftly becoming more common, more costly, and more sophisticated. In 2005, over 185,000 unique phishing reports were received. By the middle of 2006, at least 160,000 unique phishing schemes had already been reported. In 2004, losses in FBI cases totaled over sixty-eight million dollars.[1] In 2005, that number had jumped to over 183 million dollars.[2]

[1] IC3 2005 Internet Crime Report at 6. Available at http://www.ic3.gov/media/annualreport/2005_IC3Report.pdf

[2] Id.

Regulations require financial institutions to protect customer information from threats and hazards that could compromise information security and integrity and to protect it from unauthorized access or use that could be harmful to the customer. These regulations require financial institutions to implement reasonable and appropriate security measures to control identified risks. Proper controls should address risks to information in transit and in storage.

Many organizations are seeking ways to secure their communications with business partners, clients, and consumers. To achieve more secure communications, firms are looking at using proprietary alternatives such as portal-based email services on their web sites, engaging service providers that offer multiple encryption solutions to secure email, or implementing commercial software products. Each of these solutions offers more protection than unsecured email, but each suffers from serious drawbacks. These drawbacks include:

- Requiring recipients to have multiple accounts and passwords or to have decryption keys to access or decrypt email;
- Requiring recipients to go outside of their preferred email client to retrieve email;
- Incompatibility with tools some institutions have implemented to archive, search, and retrieve email for compliance purposes; and
- Inefficiency and scalability issues.

To address these concerns, the BITS Email Security Working Group recommends the adoption of three specific technologies to enhance email security:

- **Transport Layer Security** (TLS);
- **Sender Authentication**—Sender ID Framework (SIDF) or Sender Policy Framework (SPF)); and
- **DomainKeys Identified Mail** (DKIM).

Transport Layer Security (TLS) technology protects confidentiality and data integrity as it automatically authenticates servers and encrypts email messages between the servers. This encryption reduces risk of "man-in-the-middle" attacks by authenticating the servers and reducing the amount of traffic that is passed in clear text. TLS reduces risk through mutual authentication between two institutions and through protection of the information contained in the message from disclosure to unauthorized parties.

Sender Authentication (SIDF/SPF) provides a secure way for financial institutions, ISPs and others to identify the authorized mail servers for a particular domain and validate that mail originated from these authorized sources. Through implementation of Sender Validation checks by both financial institutions and Internet Service Providers, institutions will help reduce the fraudulent mail received by their customers. Customers will be less likely to be exposed to, and therefore less likely to respond to, phishing and other malicious email attacks. This, in turn, will reduce the amount of identity theft and account fraud activity initiated through fraudulent emails.

DomainKeys Identified Mail (DKIM) is a cryptographically based protocol that provides message header and body integrity verification mechanisms. It provides a mechanism for authenticating and determining the authorization of email from a domain. Its policy component is critical to providing protection against exact domain phishing and forgery.

DKIM serves a similar purpose as Sender Authentication, but utilizes different technology and is complementary to Sender Authentication.

Each of these technologies is gaining wider acceptance, is becoming more transparent to the end user, and is relatively inexpensive to implement and maintain. Each of these protocols addresses a particular problem. The protocols can be used in conjunction with each other as part of a layered approach to security.

These protocols are open standards and provide both a good return on investment and a high level of risk reduction around email-based threats. Specifically, the recommended protocols share a number of beneficial attributes; they are:

- Recognized standards that are currently or in the process of becoming widely accepted;
- Transparent to the end-user and not an inconvenience to users (for the most part);
- Relatively low-cost both in terms of implementation cost and total cost of ownership;
- Fairly easy to implement;
- Scalable across both small and large, multinational enterprises;
- Compatible with the solutions financial service companies have implemented for compliance with regulatory guidelines around communications; and
- Generally available in or soon to be available with common off-the-shelf products and services.

There is no single solution to the email security problem. Financial institutions must approach this as a process that will involve multiple generations of solutions. BITS Email Security Working Group members believe that a logical progression can begin with the deployment of Transport Layer Security (TLS) and progress through the deployment of Sender Authentication (SIDF/SPF) and ultimately DomainKeys Identified Mail (DKIM). By the time these solutions are in place, there may be additional tools available that merit consideration and will continue the push toward secure email.

Timing is important. As financial institutions go through their annual budget cycles, it is important that these financial institutions secure the funding to implement controls such as these recommended protocols.

ENGAGING KEY STAKEHOLDERS

To achieve the goals of this project, BITS and members of the BITS Email Security Working Group engaged experts from both financial services companies and Internet Service Providers (ISPs). In November, 2006, BITS convened a meeting with members, leading ISPs, and other key business partners to discuss benefits from the implementation of the protocols addressed in this paper and ways to cooperate in order to improve the reliability of, and restore consumer confidence in, the email delivery channel. Implementation of all three protocols should reduce the amount of successful phishing and malicious code, and, therefore, the amount of identity theft and account fraud. BITS and its member companies will continue to engage these key partners as the recommendations included in this *Toolkit* are implemented.

PROTOCOLS

Transport Layer Security (TLS)
(Secure SMTP over TLS)

Problem Statement
Sending unencrypted messages over insecure networks increases the risk that messages can be intercepted or altered. Financial services firms require a relatively easy way to ensure the confidentiality of email communication with third parties and clients to reduce the risk of unauthorized access to the contents of email messages and to comply with regulatory guidance on safeguarding customer and other confidential information. Proprietary solutions and commercial encryption products are not acceptable because they are not scalable over the long-term and place too much inconvenience on both the sender and the recipient. They also are not always compatible with regulatory compliance solutions already in place.

Solution
Secure SMTP over TLS provides a relatively easy way to provide encryption over the transport layer between two or more companies using email services. It is a standard protocol that is widely supported by technology infrastructure vendors based on their current releases of products. TLS security technology protects confidentiality and data integrity as it automatically authenticates servers and encrypts email messages between the servers. The value of TLS is risk reduction through mutual authentication between two institutions and, more importantly, protection of the information contained in the message from disclosure to unauthorized parties.

The SMTP (RFC 821) protocol was introduced by Jonathan Postel in 1982 for email communication. The current version of SMTP, RFC 2821, is heavily utilized for exchanging emails between two parties. SMTP is a clear text protocol. All exchange of data occurs in clear text. Secure SMTP over TLS (RFC 2487) was introduced by P. Hoffman in 1999 and later revised (TLS (RFC 3207)) by P. Hoffman in 2002. These RFCs described in detail the implementation of STARTTLS extension for Secure SMTP over TLS.

How Does It Work?
The TLS protocol is made up of two layers:

- The *TLS record protocol* ensures that the connection is private by using symmetric data encryption.
- The *TLS handshake protocol*, using asymmetric keys in the form of digital certificates, allows authentication between the server and client and the negotiation of an encryption algorithm and cryptographic keys before the application protocol transmits or receives any data.

TLS is used to open secure channels between email servers. Once two email servers start talking TLS to each other, they can then pass all their email traffic over that secure channel. Every message between those two companies is automatically encrypted and decrypted without any effort on the part of the end user. TLS support is built into most email gateway software products available today. There is usually no extra software cost to use TLS.

However, there may be small incremental costs associated with the performance impact to the gateways running TLS.

Most TLS encryption services for SMTP servers can be configured to support different classes of email service on an opportunistic or a per-domain basis. For example, policies can ensure that for a particular domain, the TLS-capable SMTP servers will:

- Always send and receive emails unencrypted;
- Use TLS encryption if available, otherwise revert to unencrypted;
- Always use TLS and, if not available, refuse mail;
- Always use TLS, and verify the certificate's Common Name matches the other party's fully-qualified domain name; otherwise, refuse mail; or
- Only accept certificates signed by a known, trusted Certificate Authority and that have not expired or been revoked.

Effectively, for TLS, organizations can configure for opportunistic mode or force TLS for all sessions. One BITS member firm has measured TLS traffic at about 40% of business-related email received from financial institutions, corporate clients, government agencies, and educational institutions.[3]

A 2005 survey of BITS members revealed that over 60% of BITS members had implemented or planned to implement TLS on their mail servers within 12 to 18 months. In mid-2006, one BITS member measured the TLS encryption rate among financial institutions to be 40% of mail traffic and growing. Financial institutions expect this rate of adoption to continue. However, not all customers and clients have the ability to enable TLS because they are using a third party to provision email services. In these cases, financial institutions must rely on the third party to implement TLS in order to complete the TLS "circle of trust" with consumers and small firms. Another BITS member measured in late 2006 an overall TLS encryption rate of 10% of all inbound mail.

Benefits

Financial service firms using TLS in either mode today are reducing the amount of email traffic that is passed in clear text and subject to "passive snooping," thereby improving the security of email and reducing the probability of unauthorized access to confidential information.

Email over TLS provides the following advantages compared to traditional (unencrypted) email:

[3] This figure was calculated by examining all email received over a two-week period in June, 2006, grouped by domain name and segmented by the count of messages received via TLS and not with TLS. First, the percentage of TLS to all traffic was calculated. Second, the count of messages was reduced by the number of messages received from particular domains that are known to not be financial institutions – for example, yahoo.com, aol.com, comcast.net, verizon.net, etc. In practice, a relatively small number of these domains accounted for a significant portion of total email. Once these domains were identified and eliminated from the total population, the percentage of TLS email was again compared to total email and the percentage obtained was just over 40%. Although the majority of this remaining mail was to financial institutions, there were many messages sent to other types of firms but these could not easily be separated from the mail to other financial institutions.

- Protection. Email servers can be configured to enforce TLS encryption between named parties and confidential information can be exchanged without fear of eavesdropping or interception over the secure session.
- Every email sent and received is encrypted. When TLS is enforced, no individual review or decision is required to determine whether or not to encrypt an email based on the email's content.
- Email encryption is transparent to both the sender and the receiver. Both parties send and read emails the same way as they do today.
- TLS is globally accepted and currently available on most, if not all, email servers.
- Industry standard. There is a growing trend among financial institutions and other companies to use TLS.
- Regulatory compliance. Regulators, such as the SEC, the Fed and FTC, may eventually mandate encryption, and could levy fines if encryption is not used and privacy is compromised as a result of a breach. TLS implementation is an initial step toward meeting potential encryption regulations.
- Reduced liability. The use of TLS can reduce exposure to lawsuits and/or risk to the brand reputation.
- Compatible with regulatory audit requirements. Because corporate gateways – rather than end-users – encrypt and decrypt messages, companies in regulated industries, such as broker/dealers, will find it easier to comply with applicable legislation and government regulations.

Impacts and Considerations

The implementation of TLS is relatively simple provided the email gateway infrastructure used by financial services firms is recent enough to provide for RFC 3207 compliance. All leading email infrastructure vendors offer different products that support this standard today. However, firms relying on more mature (legacy) technology may have to incur the cost of upgrading their email gateways to take advantage of the RFC 3207 protocol for TLS based email.

The operating cost of using TLS may be insignificant since there may be little impact on performance; however, there are specific settings when enforcing domain-specific controls that may require configuration changes to add or delete domains. In addition, administration costs can be high over time. This is particularly true for institutions that deploy TLS on a broad basis to hundreds of domains or that experience large changes in their inventory of managed Internet domains.

It should also be noted that SMTP over TLS secures *only* the link between the two email servers. However, it does not provide protection after the message has reached the destination server. Therefore, it is important to ensure the necessary agreements are in place to ensure confidential information is handled properly once it is received. TLS depends on the trust chain of certificates used to authenticate the endpoints and does not rely on the integrity of the information in DNS.

Another important consideration is that TLS is not immune from attack. In what is known as a "downgrade attack," TLS clients and servers can sometimes be made to fall back to a prior, less secure, cryptographic or hash algorithm; this can be mitigated by explicit control over the algorithms that are considered by the endpoint to be sufficiently secure.

Some institutions noted that it can take up to 18 months to fully implement TLS, including challenges in coordinating across business lines.

Should an institution be using a third party email service, then the digital certificate for TLS will have to be installed at the third party. Under these circumstances, the institution should carefully review the contract with the third party to ensure that the digital certificate and its private key are suitably protected.

Implementation

The BITS Email Security Working Group members view TLS as a standard protocol that should be endorsed and enforced for financial service firms. However, the technology adoption curve may constrain certain firms from using TLS if they have more mature (legacy) technology in place for their email gateway. These firms are forced to upgrade their technology to newer versions of products that offer TLS and may need time to research and evaluate products, determine the appropriate budget cycle for the purchase of the products and then implement the products. The consensus of the BITS Email Security Working Group is that BITS member institutions should be able to complete any required upgrades and fully implement TLS within eighteen months.

Endorsement of TLS and adoption in an opportunistic mode will provide immediate benefits to firms and continue to reduce risk as firms adopt TLS. Since many non-financial institution mail servers use self-signed certificates for TLS, opportunistic TLS provides the possibility of gaining the privacy benefits associated with TLS for a broad section of customer bound messages. The use of domain-specific lists for TLS is product dependent and offers firms an option of enforcement of TLS for specific partners and suppliers that may be helpful.

As noted previously, RFC-3207 provides for two different ways to implement TLS based on a company's preference:

- Opportunistic TLS—Email servers will attempt to negotiate a TLS connection with other servers and resort to unencrypted email if they are unable to negotiate a TLS connection.
- Enforced TLS—All email traffic will be sent using TLS and emails addressed to third party servers that do not provide a TLS "handshake" will not be sent.

There are other implementation options that are specific to the choice of the vendor email gateway servers chosen. For example, many vendor products have the ability to enforce TLS usage for a specific set of predetermined domain names and to set TLS to opportunistic mode for all other domains. This enables a financial services company to identify its partner domain names and enforce TLS for all email between the company and its partners. This option requires more administration of the domain name list by the financial service firm to implement since it will need to change as partners change. This option also assumes that the partners identified have email infrastructure that is TLS compatible. With this option, partners that do not have TLS, or if TLS fails as a result of an error, will not receive any email.

Recommendations

- Implement TLS in the enforced mode with business partners and service providers within 18 months.
- Implement TLS in the opportunistic mode immediately.
- Limit unencrypted email traffic with confidential information where feasible until TLS is fully implemented.
- Consider adding email security requirement language to contracts with business partners and service providers.
- Promote awareness of this issue among all financial institutions, clients, consumers, Internet Service Providers and Mail Service Providers.
- Develop programs and materials to encourage all financial institutions to implement TLS.
- Develop programs and materials to encourage ISPs and mail service providers to implement TLS in order to provide the benefits of TLS to their customers and enable secure communications with their financial institutions.
- Maintain opportunistic TLS for communication with other (including customer) mail servers.

Sender Authentication (SIDF/SPF)

Problem Statement

Spam and phishing are growing at a rapid pace. Customers of financial institutions lack the tools to validate email from a legitimate financial institution. Due to inherent weaknesses in email security, email is frequently used in "phishing" attacks on the customers of financial institutions. These phishing attempts are designed to trick individuals into providing personal data (e.g. ID, password, SSN, account numbers) which phishers subsequently use for fraudulent purposes. Increasingly, email also is used as a vehicle to surreptitiously install key logger, screen capture and remote control programs that enable unauthorized access to data onto customer computers. Additionally, the high volume of spam challenges the capacity of email infrastructures and support organizations servicing both external and internal customers.

Solution

Sender Authentication is a technical method to combat the forgery of emails. Sender Authentication provides a way for financial institutions and their customers to identify and validate the return address domain of an email and the mail gateways authorized to send mail on behalf of that domain. The sender first publishes the possible IP addresses or IP networking ranges from which it will send email messages, and once emails are received, the IP addresses or networks can then be validated by the recipient.

Currently there are several Internet standards available to verify the authenticity of a sending domain name. These include RFC 4406 Sender ID (SIDF) and RFC 4408 Sender Policy Framework (SPF). Both SIDF and SPF require publication of "SPF" records, although there are differences in the way the protocols are implemented. Specifically, the protocols apply authentication at different messaging layers. SIDF applies authentication in the message header and SPF in the message envelope. However, neither standard excludes the use of the other. Given the co-existence of email authentication standards, it is important for institutions to address implementation considerations that ensure both interoperability and the integrity of authentication processes. Institutions should refer to the relevant RFCs for Sender ID (RFC 4406) and SPF (RFC 4408). Microsoft's web site provides additional information on Sender ID and relevant information on SPF can be found at openspf.org.

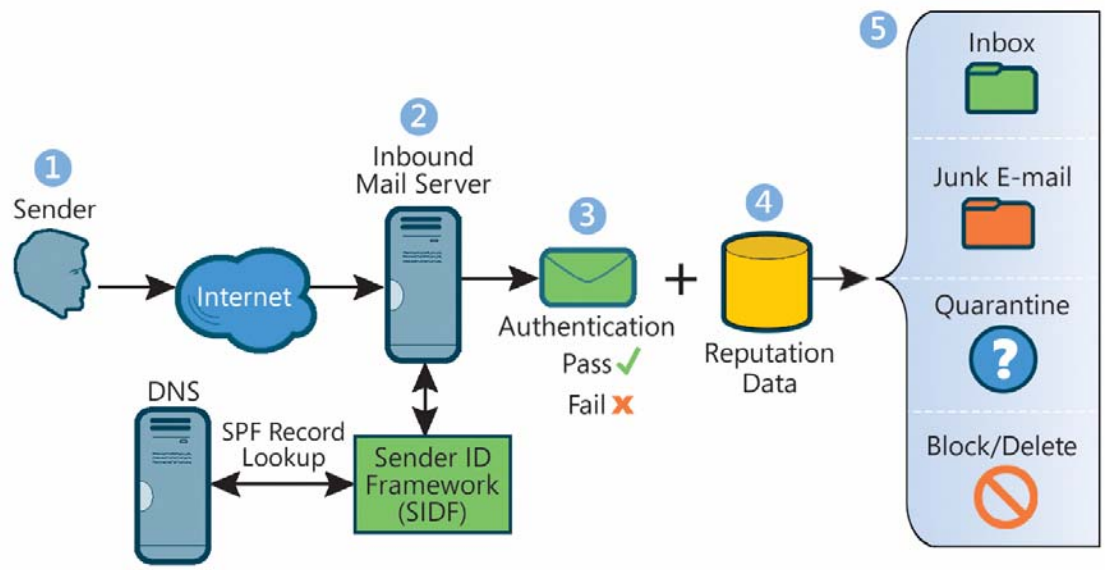
<u>Sender ID Framework (SIDF)</u>

Sender ID framework is the merger of two similar approaches including the original Sender Policy Framework and Microsoft Caller ID for Email. Together they provide a single record format for outbound mail authentication and provide alternatives for receiving networks to combat the forgery of emails. The Mail From check alternative provides a secure way for financial institutions and their customers to identify and validate the return address of an email from a particular domain. The financial institution first publishes the possible IP addresses from which it will send email messages, and once emails are received, the IP addresses can then be validated by the recipient.

Sender ID provides the option of utilizing the Purported Responsible Address (PRA), RFC 4407, as spearheaded by Microsoft and others, and was designed to counter the spoofing and social engineering exploits that are visible to the end user, not unlike the return address on an envelope. This Purported Responsible Address selects the header field with the email address “responsible” for sending the message for validation, recognizing that mails may be resent by forwarding agents, mail list servers or other software.

How Does It Work? (SIDF)

Domain administrators publish in the Domain Name System SPF records that identify authorized outbound email servers. Receiving email systems verify whether messages originate from properly authorized outbound email servers. The following diagram illustrates the verification process.



SIDF illustration provided by Microsoft.
© 2007 Microsoft, Inc. All rights reserved.

The Steps in the process are:

1. The sender transmits an email message to the receiver.
2. The receiver’s inbound mail server receives the email message.
3. The inbound mail server checks which domain claims to have sent the message and checks the DNS for the SPF records of that domain. The inbound server then determines if the sending email server’s IP address matches any of the IP addresses that are published in the SPF record. If the IP addresses match, the email is authenticated and delivered to the receiver. If the addresses do not match, the mail fails authentication and should not be delivered.
4. The Sender ID result can be combined with reputation data about the IP/domain holder.
5. When combined with the receiving network’s anti-spam and anti-phishing technologies, the email may be delivered to the Inbox, the Junk or Quarantine folders, or may be blocked and deleted.

Benefits (SIDF)

The following are benefits of SIDF:

- Prevents phishing attacks. Sender ID is better at preventing phishing attacks than SPF, because it checks the “from” address at the message header layer. Phishers can use a correct envelope return address and outbound email servers but dupe users with fake content and “from” addresses.

- Improves deliverability of messages.
- Protects credibility and reputation of brands and domains.
- Enhances user trust and confidence.
- Results in a reduction in the volume of non-delivery receipts received by the spoofed domain.
- Is easily deployed.

Sender Policy Framework (SPF)

The *SPF Project* was founded in 2003, and in December 2004, the *SPF Council* was established to steer the overall SPF standardization effort, promote the deployment of SPF on the global Internet, and develop and improve the project's public messaging and communications.

How Does It Work? (SPF)

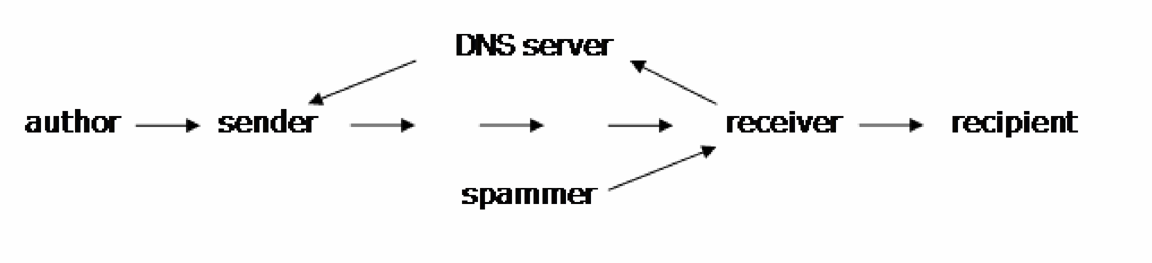
Emails come with two particular types of sender identity addresses, both of which can be forged. One is part of the letterhead and is referred to as the *header sender address* of the email message. It contains the *from* or s*ender* field that is displayed to the user by email programs (note that most email programs used by consumers do not display *sender*, only *from*). The other sender identity address is on the envelope that is wrapped around the email message as it traverses from the sending mail gateway to the receiving gateway. It is referred to as the *bounce address, envelope sender address, the mail from address,* or *return-path* field. It is usually not displayed to the user by email programs. SPF uses the message "envelope" to validate the sender of the email, so that validation is performed early during the SMTP transaction, before the bulk of the message (its header and body) is transmitted.

SPF authenticates both the envelope HELO and MAIL FROM identities by comparing the sending mail server's IP address to the list of authorized sending IP addresses published by the sender domain's owner in a "v=spf1" DNS record. SPF operates at the level of the SMTP transaction, and utilizes three pieces of information for validation:

- The MAIL FROM: parameter of the incoming mail
- The HELO or EHLO parameter of the sending SMTP server (used for Mailer-Deamon bounces which send a blank MAIL FROM)
- The IP address of the sending SMTP server

SPF validation requires both sides of the mail relaying technology to work together. First, the domain owner publishes the IP addresses or network range of their sending gateways in a record in the domain's DNS zone. Second, receiving gateways then perform a SPF lookup to determine that the message complies with the domain's stated published record.

SPF uses a "txt" type DNS Resource Record (RR) to declare which mail gateways are, and are not, authorized to use a particular domain name for the "HELO" and "MAIL FROM" email identities. The SPF record is a single string of text that can include a number of parameters in the form of modifiers, functions, arguments, and mechanisms, to meet the needs of a wide variety of environments.



Benefits (SPF)

The following are benefits of SPF:

- Reduces network traffic and need for computing resources. SPF validation was designed to take place early during the SMTP process "initial handshake" before the bulk of the message (header and body) is transmitted, therefore network traffic is reduced (rejected messages) as are computing resources for processing further email checks.
- Improves deliverability of messages.
- Protects credibility and reputation of brands and domains.
- Enhances user trust and confidence.
- Results in a reduction in the volume of non-delivery receipts received by the spoofed domain.
- Is easily deployed.

Impacts and Considerations

Implementation of the Sender Authentication (SIDF/SPF) can be a straightforward and inexpensive process. Publication of SPF records requires no extra software or services. However, the scope of SIDF/SPF implementation will vary from institution to institution and some institutions may realize costs.

Each institution should address multiple concerns before it proceeds with SIDF/SPF implementation to ensure success. Institutions should examine how SIDF/SPF should and will work in their particular environments, including potential unintended results of SIDF/SPF implementation. Specifically, before implementing SIDF/SPF, institutions should identify all mail domains in use, the associated outbound gateways, and the DNS hosts. It is also important to note that SIDF/SPF relies on the integrity of the information in DNS and on the integrity of the DNS system itself.

Institutions also should assess their current email and marketing practices and must identify mailings they outsource to third parties or marketing partners. It is important to identify external service providers that are sending these mailings on behalf of the institution as they may be "spoofing" the institution's internal corporate email domains. Further, modifications to their mailings may be required. If an institution's corporate email gateways are not configured to prevent spoofing, institutions should set priorities for the implementation of fundamental anti-spoofing controls.

SPF records can be published in a manner that helps protect those domains never intended to send email (e.g., domains purchased to protect intellectual property). For example, to protect against unauthorized use of company brands, and to help reduce risk of potential phishing attacks, a company can publish SPF records for domains that will never send email using the "-all" syntax (refer to RFC 4406 for SPF2.0 record syntax and RFC 4408 for v=spf1 syntax). Depending upon whether a financial institution chooses to validate incoming mail based upon SIDF (RFC 4406) and PRA (RFC 4407) or SPF (RFC 4408), interoperability considerations need to be addressed to ensure intended mail handling. Therefore, in addition to publishing v=spf1 records, you may want to also publish spf2.0 records.[4]

Institutions that have not implemented Sender Authentication (SIDF/SPF) may see that attackers will focus their malicious efforts on institutions that do not have Sender Authentication controls in place. SIDF/SPF will also result in a reduction in the volume of non-delivery receipts received by the spoofed domain.

Sender Authentication results can also be used as a part of reputation system scoring. Reputation system scoring is the process that identifies the worthiness of senders by determining, for example, whether the site is a zombie "hacked pc" and is being used to send unwanted or malicious mail. Such an approach can be implemented to help assess the reputation of sending domains, the validity of emails, and ultimately, the disposition of emails from a domain.

Finally, the impact of mail forwarders must be considered. Mail forwarders are used to route email from one hosting site to another. When mail is handled by mail forwarders, the forwarded email retains the header data while the originating source IP or network of the registered SPF record is replaced with the route information of the forwarding gateway. The receiver of this forwarded email would detect this as domain spoofing and potentially drop the email. Therefore, each institution should determine how it uses forwarders, and possibly limit or eliminate their use. Where forwarders do exist, institutions should determine their impact on Sender Authentication implementation.

Additional Considerations with SIDF/SPF

Email Security Controls/Best Practices

Fundamental email security controls have emerged as best practices that focus on "validating" emails, in order to help ensure the fundamental integrity of email processing (e.g., User Validation controls, Mail Relay controls, and DNS lookups). Therefore, these email best practices should be implemented by financial services institutions. Email validation controls are needed in addition to more traditional email controls (e.g., Anti-Spam, Anti-Virus, Blacklists, Attachment Filters).

User Validation Controls

[4] Refer to Microsoft's Sender ID homepage (http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx) for more information on SIDF and http://www.openspf.org/ for further guidance on SPF.

Perform user validation via a lookup to an authoritative source (e.g., Active Directory, Alias Table, LDAP) for email received at the perimeter of your network to ensure the intended recipient(s) are on your user directory. If the recipient is not on the institution's user directory, the email is rejected. User Validation look-ups will improve the performance of your messaging infrastructure as mails are dropped at the network perimeter, thereby avoiding further downstream processing through other more processing intensive filters.

Mail Relay Controls

Configure the institution's perimeter corporate mail gateways to ensure that messages can only be sent from authorized subnets or domains. If gateways are not properly configured and are effectively "Open Relays", it is highly likely that unauthorized use of the institution's corporate mail services will take place, increasing the risk of the institution's domain being blacklisted. In turn, blacklisting will affect the integrity and availability of email services.

DNS Lookups

Mail gateways perform a hostname lookup on the IP address of the connecting client. Next the IP addresses of that hostname are looked up. If the client IP address does not appear in that list, then it is highly likely the mail is forged.

Implementation

To implement Sender Authentication (SIDF/SPF), institutions must enable Sender Authentication validation on their email servers so that they can validate incoming mail and honor the SIDF/SPF directives of other institutions by performing SPF record lookups to validate incoming email before routing it. Institutions must also publish SPF records for the mail domains and gateways that it or its partners operate.

Once these guidelines have been instituted into the email validation system, the institution should actively manage updates to ensure accuracy of the validation system. In addition:

- Newly hosted mail and non-mail domains must have a published SPF record.
- Future mailings done by third parties must comply with the SPF requirements and recommended solution. This should be invoked via contract.
- Future network system modifications and technologies must be assessed to ensure they do not negate or impact the implemented solution.

Domain owners must decide how they want the receiving institution to handle mail from their domain based upon the lookup result, and must reflect that preference in the SPF record.

Also as part of the implementation process there are a few key consistent implementation attributes that must be employed to mitigate the level of variability and improve the benefit to be realized. These attributes include financial institutions publishing SPF records as "Hard Fail." Another important attribute is that receiving environments honor the records that are published as "Hard Fail," and not deliver mail to the recipient.

It is necessary, while assessing these Sender Authentication methods, to note that SIDF/SPF alone will not address all of the issues related to the myriad of fraudulent emails. However, SIDF/SPF are methods that can help alleviate part of this growing problem. By coupling

SIDF/SPF with the help of service providers, and by using these solutions in conjunction with TLS and DKIM, we will see an effective reduction in the scale and scope of problems associated with email.

Mail that is sent by third parties utilizing the domains to be published needs to be addressed. One solution is to migrate the mail that is being sent by a third party to utilize one of the third party's published domains. When this isn't feasible, due to perhaps a branding or legal requirement, a number of other options are available.

These other options include bringing mailings in-house or creating a business partner connection to the vendor site. A third option, and one that affords the most control, is for institutions to create and delegate a sub-domain that is hosted by the outside service provider. To implement this option it is important to consider branding and recognition as well as customer confidence in receiving mail from a domain with which they are not familiar. Another important consideration is potential cost associated with having the business and the third-party service provider retool the application and mailing procedures to use a new sub-domain.

There are several key steps to the beneficial use of delegated sub-domains by third-party service providers. First, the financial institution creates a DNS entry for the sub-domain associated with each third-party service provider's DNS server names. Second, the third-party service provider creates DNS entries for the delegated sub-domain: A, MX, PTR and TXT records, which include the SPF parameters. Third, financial institutions need to apply an approach that meets the business Reply To requirements for their mailings. Alternatives for handling replies include the third-party service provider's auto-forwarding "Reply To's" to the sending financial institution, or note on the email "Do Not Reply To Email" with instructions for replying to a specific sending institution email address rather than to the third-party service provider via the reply function of the consumer's mail client. Naturally, the financial institution should carefully review its contract and agreement with the third party to ensure that all liabilities and legal issues have been considered in the contract.

Recommendations

- Publish SPF records for both email and non-email domains enabling Sender Authentication within eighteen months from the release of this *Toolkit.*
- Enable SPF record validation on incoming email immediately.
- Publish SPF records as "Hard Fail"; "Soft Fail" should only be used for SPF testing purposes.
- Honor records in receiving environments that are published as "Hard Fail", and not deliver the mail to the recipient. It is recommended that the mail be rejected as it is originating from unauthorized sources. Receiving institutions may want to "quarantine" records temporarily for operational or investigative purposes.
- Utilize delegated sub-domains for third party external mailings, and publish SPF records for sub-domains.
- Promote awareness of this issue among all financial institutions, clients, consumers, Internet Service Providers and Mail Service Providers.
- Develop programs and materials to encourage all financial institutions to implement Sender Authentication.

- Develop programs and materials to encourage ISPs and mail service providers to implement Sender Authentication in order to provide the benefits of SPF record validation to their customers and enable communications with their financial institutions.

DomainKeys Identified Mail (DKIM)

Problem Statement
The proliferation of spam, including phishing, is undermining consumer and financial institution confidence in email. Furthermore, there is increasing concern over the alteration of the email message and the content of the information and data.

Solution
DKIM is a cryptographically-based protocol that provides for both message authentication and authorization and message integrity verification mechanisms without the classic overhead of a full blown Public Key Infrastructure system. It provides a means to digitally sign select headers as well as the email body itself to ensure that email information has come from the purported sender and that it has not been altered. DKIM can help reduce the proliferation of spam, including phishing, and also restore confidence in email content through the validation of the signed content and aggressive filtering by ISPs, spam filters and the like. It includes both a signing component and a policy component.

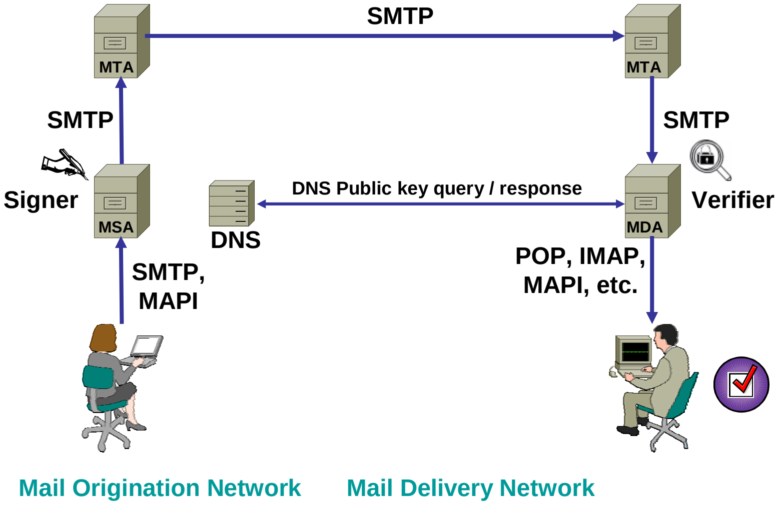
The discussion of the development of the DKIM protocol was coordinated by a confederation of service providers, enterprises, and providers of email products. It is derived from Yahoo's DomainKeys and Cisco's Identified Internet Mail. The DKIM protocol was submitted to the Internet Engineering Task Force (IETF) in 2005 by Cisco, PGP Corporation, Sendmail and Yahoo. Some key benefits are DKIM's ability to authenticate messages independent of the path they take to the recipient, and low usage costs relative to other approaches.

DKIM is not a complete solution, but it provides an effective means to significantly reduce spam or junk email through validation and aggressive filtering methods. It should be viewed as one step in a multi-step or multi-generational solution. It should be noted that although the DKIM standard for signing messages is stable, the Sender Signing Policy (SSP) may be fluid for some time to come.

How Does It Work?
The sending organization adds a digital signature to the message, associating it with a domain name of that organization using a private key for which the corresponding public key is published in the Domain Name Service (DNS). Typically, signing will be done by a service agent within the authority of the message originator's Administrative Management Domain (ADMD). Signing might be performed by any of the functional components, in that environment, including: Mail User Agent (MUA), Mail Submission Agent (MSA), or other Message Transfer Agents (MTA).

DKIM permits signing to be performed by authorized third parties. On the receiving side, an agent in the recipient's ADMD compares the signature against the header information using the published public key and is then able to validate that the signer is who they claim to be. The Sender Signing Policy provides guidance for handling unsigned, improperly signed or third-party signed mail. Policies could be put in place at the receiving organization that would permit the rejection, deletion, or tagging of unsigned or improperly signed messages when a valid signature is expected.

In the diagram below, the MTAs play the role of the authorized agent for both the sender and recipient of the email message.



DKIM illustration provided by Cisco Systems.
© 2006 Cisco Systems, Inc. All rights reserved.

Benefits

DKIM provides highly effective means for authentication and integrity of email messages when implemented correctly. By implementing DKIM, financial institutions and ISPs can reduce the impact of spam and phishing attempts through more aggressive filtering of messages from unknown sources. DKIM also reduces the threat of content alteration by digitally signing the email message and thereby validating the email content integrity. The combination provides greater confidence in the email environment. In conjunction with other protocols and controls, DKIM can provide a much stronger means for reducing unwanted or malicious email to customers. Additionally, DKIM provides capabilities for sender delegation which eases its use by third party suppliers. With the Sender Signing Policy, message policies can be easily put in place to deal with unsigned or improperly signed email as appropriate.

Message integrity and authenticity are the main benefits of DKIM. While these are important factors to email security, it does not address message confidentiality. Confidentiality issues must be taken into consideration when evaluating email security solutions. Additional tools, such as TLS, can help protect message contents from unauthorized access.

Acceptance of DKIM within the information technology industry is increasing as several ISPs and MTAs (e.g. Sendmail, Postfix, and several MTA appliances) have implemented it and as more financial institutions begin to deploy it.

Impacts and Considerations

The implementation of DKIM is only one step in a multi-generational application approach. If confidentiality is required, it is important to also incorporate other means of email security, including authentication through Sender Authentication and encryption using TLS.

DKIM relies on the integrity of the information in DNS and on the integrity of the DNS system itself. There are email security and authentication issues not addressed by DKIM. Financial institutions should apply a risk-based approach to identify and mitigate these residual risks by, for example, validating client certificates before sending email as a sending domain and by encouraging their business partners to do the same.

The use of DKIM validates sending domains, not individual email senders within the domain. Therefore, individual email integrity and accountability needs to be provided via augmentative technologies if required for business, legal or other purposes.

ISPs and other service providers can have a direct impact on the effectiveness of DKIM. ISPs and other providers must implement processes to leverage the capabilities that DKIM and other email authentication protocols use in order for them to be effective and to provide the desired results.

As in other email security methods, an important aspect of the deployment of DKIM is the underlying means of establishing and maintaining trust with the final recipient of an email message. Financial institutions should work in partnership to derive a series of end user interface recommendations for both agent and agent-less (e.g., web based) email platforms.

The implementation of these protocols requires involvement of ISPs. By partnering with ISPs, financial institutions can ensure consistent implementation which will assist in end user adoption. Financial institutions can take the lead by instituting DKIM as a means of authentication and then urging ISPs and other stake holders to work in collaboration.

DKIM in its basic form allows for the use of self-generated digital credentials. In the case of financial institutions, the use of credentials from trusted Certificate Authorities should be considered. These certified credentials will provide a greater level of competency for this protocol. However, because of the size of certificates, there may be some technical difficulties with this implementation. Institutions may need to consider extending DKIM to use Internet Key Exchange (IKE) or another key distribution protocol.

DKIM uses DNS as a means to publish public key material used in signing messages headers and bodies. Implementing procedure for trusted delivery of public key material is an integral part of this protocol. Therefore, procedures for trusted delivery of public key material should be explored to provide enhanced confidence provided by the DKIM signing process. The use of DNS Security (DNSSEC), when deployed, will considerably mitigate this issue.

Implementation

When implementing DKIM, consideration must be made for system resources, throughput requirements, operational support personnel, help desk and the like. Processes must also be put in place for managing third party keys so that the integrity of mail coming from third party suppliers on behalf of the institution is maintained or improved. It should be noted that the cost of DKIM may be approximately the same as the cost of TLS.

Throughout implementation, it is essential to have an understanding of the efficiency with which this protocol operates. Financial institutions should develop key metrics for their assessment. By developing a set of key metrics, financial institutions can assess the efficiency with which this protocol operates. The following are metrics that financial institutions may consider in their assessment:

- Volume of email
- Volume of signed email
- Average throughput of email through the system (performance metrics)
- Rejection rates related to unsigned email, improperly signed email
- Helpdesk calls sorted by type of call, frequency, etc. with feedback mechanisms to update processes, procedures as appropriate

Financial institutions should consider the overhead costs when implementing this protocol and the protocols previously recommended in this paper. The following are costs that financial institutions should consider:

- **Additional server capacity to meet the increased overhead.** While this will be small, large volumes of email will still have some impact on infrastructure performance. The increased overhead is directly proportional to the email traffic and applies to both the sending and receiving gateways.
- **Additional resources.** Consider those resources that will be required to manage keys, resolve problems, assist third party supplier key management and similar efforts.
- **Help desk support.** Implementation strategies should be put in place to minimize impacts to help desk volume; however, training procedures, escalation processes, problem resolution, and other solutions may be required and demand additional resources.

Institutions must also take care to not modify messages after they are signed. Particular attention should be given to forwarding situations since forwarding services often append text (e.g., indicating virus scanning has occurred). Such additions will break signatures in most circumstances. However, DKIM permits senders to sign only a portion of the message using the “l+” tag to specify the number of bytes that are signed. Using this functionality will prevent signatures from breaking, but it opens a window for attackers to add malicious unsigned data to the end of a message. HTML messages, for example, can sometimes be completely replaced when displayed.

Recommendations

- Publish domain keys and policy records in DNS for all email domains as soon as possible.

- Begin signing email messages using DKIM within 18 months. While the standards are not "official," they have not materially changed and are not expected to change prior to formal adoption. Most products available today already support DKIM. This will help members understand the impact on existing resources with minimal impact on delivering messages.
- Once the DKIM standards are official, work with your third party suppliers to begin signing email sent on your behalf.
- Engage key ISPs to encourage them to implement DKIM.
- Adopt a model to quarantine or reject improperly signed emails and not deliver to intended parties. Alternatively, encourage consider marking unsigned mail in such a way that the intended recipient has some indication that the email may not be trustworthy.
- Promote awareness of this issue among all financial institutions, clients, consumers, Internet Service Providers, and Mail Service Providers.
- Develop programs and materials to encourage all financial institutions to implement DKIM.
- Establish migration paths from older, and in some cases proprietary, tools to standards-based DKIM.
- Develop programs and materials to encourage ISPs and mail service providers to implement DKIM in order to provide the benefits of DKIM to their customers and to enable secure communication with financial institutions.
- Develop policies that govern disagreement between DKIM and Sender Authentication. Some institutions may wish to mark such messages to indicate concern about their authenticity.

CONCLUSION

Email is both inherently insecure and a necessary vehicle for communication with business partners, service providers, and customers. Technology does not exist to eliminate all of the email-related threats posed by fraudsters and scammers to the reputations and customers of financial institutions. However, technologies do exist which may begin to mitigate these threats. The BITS Email Security Working Group has identified three of these technologies, Transport Layer Security (TLS), Sender Authentication (SIDF/SPF), and Domain Key Identified Mail (DKIM), as important to the establishment of confidence in email communication. Each of these technologies becomes exponentially more effective toward achieving these goals as adoption increases among financial institutions, Internet Service Providers (ISPs), and other interested parties.

This *BITS Email Security Toolkit: Protocols and Recommendations for Reducing the Risks* is the first step in BITS' efforts to encourage broad adoption of these technologies by key parties. Through cooperation among financial institutions and with key stakeholders, including ISPs, the financial services industry can lead the way to mitigate the threat to email security and restore customer confidence in email as a channel of communication with financial institutions. Additional work will need to be accomplished by the product vendors, ISPs and other industry partners to develop true end-to-end solutions that will drive customer confidence.

This *Toolkit* includes specific recommendations for each of the protocols. In addition, there are several overall recommendations:

- **Implement each of the recommended technologies within 18 months.**
- **Promote awareness of email security** concerns among financial institutions, clients, consumers, Internet Service Providers and Mail Service Providers.
- **Engage and encourage service providers to implement the recommended technologies.**
- **Add email security requirements to contracts** with business partners and service providers.

The BITS Email Security Working Group has established a timeline for implementation of these technologies, and urges all financial institutions to participate. In addition, the BITS Email Security Working Group will continue to engage the leading ISPs and other stakeholders to urge them to collaborate in developing end-to-end solutions. The effectiveness of this project is enhanced by industry-wide participation. In addition to urging implementation on a definite timeline, the BITS Email Security Working Group will, over the duration of the implementation schedule, survey BITS member companies to evaluate progress toward improving and achieving email security.

Disclaimer

THIS DOCUMENT IS FOR INFORMATIONAL PURPOSES ONLY. Neither the individual members, nor the member institutions of BITS or The Financial Services Roundtable, make any warranty or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of the information contained in this document, or represent that this document's use would not infringe privately-owned rights. Reference to any special commercial products, processes, or services by trade name, trademark, service mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by BITS or The Financial Services Roundtable.

About BITS

BITS is a nonprofit industry consortium of 100 of the largest financial institutions in the U.S. BITS is the non-lobbying division of The Financial Services Roundtable. BITS' mission is to serve the financial services industry's needs at the interface between commerce, technology and financial services. BITS works as a strategic brain trust to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect. BITS focuses on key issues where industry cooperation serves the public good, such as critical infrastructure protection, fraud prevention, and the safety of financial services. BITS' activities are driven by the CEOs and their direct reports—CIOs, CTOs, Vice Chairmen and Executive Vice President-level executives of the businesses.

About the BITS Security and Risk Assessment Working Group

The mission of the BITS Security and Risk Assessment Working Group is to strengthen the security and resiliency of financial services by:

- Sharing and developing best practices to secure infrastructures, products and services;
- Maintaining continued public and private sector confidence; and
- Providing industry input to government agencies and regulators on policies and regulations.

The priorities of the SRA Working Group are determined by the SRA Steering Committee and reviewed by the BITS Advisory Board and BITS Committee. The focus of the SRA may vary from year to year but includes four major areas:

- Product and Service Security
- Legislation/Regulation/Supervision
- Operational Risk
- Emerging Issues

BITS
The Financial Services Roundtable
1001 Pennsylvania Avenue, NW
Suite 500 South
Washington DC 20004
(202) 289-4322
www.bitsinfo.org
www.fsround.org