



William H. Miller, Governor
Tommy M. Thompson, Secretary
www.kdor.gov

FTA Computer Security Workshop

Secure Email

March 8, 2007

Stan Wiechert, KDOR IS Security Officer

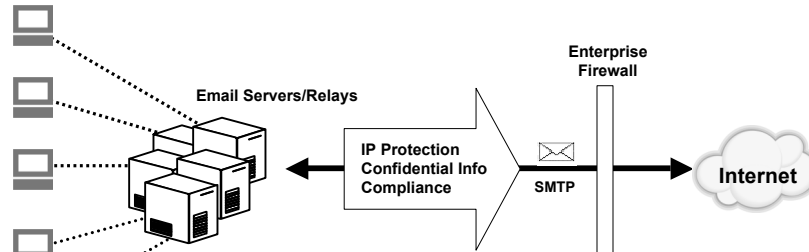


William H. Miller, Governor
Tommy M. Thompson, Secretary
www.kdor.gov

Outline of Presentation

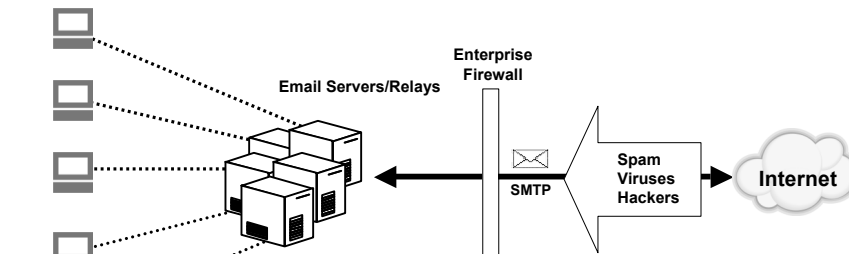
- The Risks associated with Email
- Business Constraints
- Secure Email Features
- Some Solution Components
- One Solution- Tumbleweed

Risks in the Outbound Environment



- Outbound Email Threats:**
- Confidential information leaks (FTI, PHI, PII)
 - Distribution of sensitive//illegal/offensive material to outsiders
 - Potential of legal liability
 - Violations of security and privacy regulations
 - HIPAA, GLBA, SOX, SEC, SB1386...
 - Exposure of internal network information
 - Lack of reliable delivery tracking/auditing

Risks in the Inbound Environment



- Inbound Email Threats:**
- Email fraud/phishing attacks
 - Viruses/worms/malicious code
 - Executable attachments
 - Spam, sexually inappropriate content
 - Denial of Service (DoS) attacks,
 - Directory Harvesting Attacks (DHA)
 - Relay hijacking



William H. Miller, Governor
Lisa M. Reynolds, Secretary
www.kansas.gov

Business Constraints

- Recipients all have different email environments and different degrees of willingness to change their behavior
- Enterprise support desks can't afford to handle calls from internal and external users who don't understand how to use the secure email application
- IT needs to meet varying security vs. ease-of-use requirements per the business units they support
- While the business community may need multiple secure messaging options, senders must not be asked to choose

5



William H. Miller, Governor
Lisa M. Reynolds, Secretary
www.kansas.gov

Secure Email Features

- *Privacy*: Only the intended recipient can read the message, even if someone intercepts it in transit. Privacy is important because sensitive documents get transmitted among employees, business partners and customers.
- *Data integrity*: The recipient can determine if anyone has tampered with the message. Data integrity proves that the message received is in fact what the sender had sent.
- *Authenticity*: The recipient knows who sent the message. Authenticity assures the recipient that the message came from the purported sender and is not a forgery.
- *Proof of receipt*: The sender knows that the message was delivered to the recipient. Certain business uses for secure e-mail require some form of delivery confirmation notifying the sender that the message has been received and providing an audit trail that can prove this fact.
- *Non-repudiation*: The recipient can prove to a third party, such as a court of law, that the purported sender sent the message. This is a crucial aspect of business-grade messaging: being able to hold the sender to business commitments made through e-mail.

6

Some Solution Components

- Trend is to integrated applications to provide:
 - access control, encryption, content filtering, anti-spam, and anti-virus services with central administration capabilities
- Need to determine:
 - When to send email securely
 - How email is securely delivered
 - How senders and recipients are authenticated
 - What users types are allowed
 - What user roles are allowed
- Other requirements:
 - How Email will be securely stored, logged, archived, reported, etc.

7

One Solution- Tumbleweed

- Disclaimer
 - By this presentation, neither the Kansas Department of Revenue nor any KDOR representatives endorse Tumbleweed as the only appropriate solution for your state environment.
 - The following slides are presented solely as an illustration of how Tumbleweed addresses some of the components of a secure email solution.

8



William H. Miller, Director
State Treasurer, Secretary
www.kansas.gov

Tumbleweed Secure Messenger™

- is an Internet email security solution
- provides browser-based secure message delivery options in conjunction with the protection modules of the Tumbleweed Email Firewall (EMF)
- provides access control, encryption, content filtering, anti-spam, and anti-virus services
- works for all email sent to and received from outside the enterprise over the Internet.
- uses policies to define resulting actions

9



William H. Miller, Director
State Treasurer, Secretary
www.kansas.gov

Determining when Email is sent securely

- Outbound email
 - End-users can decide to encrypt
 - Reserved text in email subject line or body (#secure)
 - Email administrator can enforce policies automatically without end-user involvement
 - The content and identity-filtering capabilities of the EMF Engine let admins encrypt outbound messages that contain customer-private information
 - Content Policy- The private information could be identified in any part of the email, including
 - Attachments, combinations of weighted keywords and phrases, patterns, attachment types, and other message characteristics can trigger a content-based encryption policy
 - Identity-based encryption policy could be applied to encrypt email
 - from or going to certain email addresses (legal department to an outside law firm)
 - A combination of content and identity-based policies can be used
 - all email from the finance department that contains a spreadsheet file attachment should be encrypted and delivered securely.

10



Determining when Email is sent securely

- Inbound email:
 - SMTP messages that should have been encrypted can trigger policies that alert the sender of the violation:
 - If email contained customer private information
 - Email came from a business partner who should always encrypt
 - Secure Messenger provides a web-based application to enable those users to submit future messages over an encrypted SSL browser session
 - These messages can be converted back to SMTP by Secure Messenger so they can be scanned for viruses and other threats before being passed back to the internal email Inbox of the Enterprise User.

11



How email is securely delivered

- Online Pull Delivery Using a Web Browser
 - Known as Email Notification, Secure Messenger first stores the email in encrypted form on the Secure Messenger server.
 - It sends an Email Notification to the recipient containing a unique Web link.
 - Recipients click on the link to access the message directly at the Secure Messenger server over an SSL-protected browser session.
 - Authentication using a login password can be required before the message content is viewed.
 - Recipients can receive, read, and reply to a secure message, and to save it, without the need for any plug-ins or client-side software in their email client or browser.
 - By bringing recipients to the enterprise Web site to access the message, they have a centralized archive for all secure email communication with the enterprise.
 - Message expiration settings can be set by the administrator to control data storage management.

12

How email is securely delivered

- **Offline Push Delivery Using A Web Browser**
 - Called Secure Envelope, sends a password-encrypted message directly to a recipient's email Inbox.
 - Uses standard SMTP email as the transport, but encapsulates the encrypted message content in an HTML attachment.
 - To decrypt a message, recipient opens the attachment using their offline browser and enters the correct password.
 - Since password entry and decryption functionality are embedded in the HTML attachment, the recipient's browser can manage the process without preinstalled software.
 - Allows recipients to manage their secure emails locally on their desktops without always having to connect to the Secure Messenger server.

13

How email is securely delivered

The Email Firewall (EMF) independently provides S/MIME functionality

- When a recipient's digital certificate is available for encryption and the recipient's email infrastructure supports the S/MIME standard, the EMF provides offline push delivery using both gateway-to-gateway and gateway-to-desktop S/MIME.
- If the receiving domain has an S/MIME-compatible email gateway, all email to that domain can be secured automatically. After a one-time exchange of a domain digital certificate, the EMF transparently secures all future email between users in the two domains using strong S/MIME encryption and digital signature technology.
- For external end-users who have S/MIME enabled email clients, the EMF supports gateway-to-desktop encryption. Dynamic public key lookup and validation of certificates from external directory servers is supported, in addition to local storage of recipient certificates. If the external user has previously sent a digitally signed message into the enterprise, the EMF will automatically harvest the correct certificate, store it locally, and use it to encrypt all future email for that user, using an EMF policy.
- End-user proxy certificate issuance to external users enables them to send encrypted messages to Enterprise Users while allowing the EMF to decrypt the messages and inspect the content for viruses or other inappropriate content.
- When S/MIME policies are applied in the EMF directory hierarchy, all email to and from designated users is encrypted, regardless of content.

14



William H. Miller, Governor
Katie Maguire, Secretary
www.kansas.gov

Authenticating Secure Messenger Users

Recipient Authentication

- Recipients of messages sent by one of the browser-based delivery options are typically authenticated using a password.
- Multiple password-based authentication mechanisms are supported
- Native support is provided for enterprise passwords managed through Microsoft Active Directory and other LDAP-enabled directory servers. Typically used for the enterprise's employees and those external users who also have their credentials managed by the enterprise directory.
- Administrators or users can define passwords that are managed internally in the Secure Messenger database. User passwords can be defined initially and communicated by email to recipients, or recipients can define an account password the first time they receive a secure delivery. Secure Messenger does not automatically send the password.
- Users who later on forget their passwords can have either a hint or the password itself emailed to them.
- Certificates, tokens, or other online external authentication systems can be supported for browser-based delivery methods using the Secure Messenger SDK. *Developer's Guide*. In addition, digital certificates can be used to authenticate recipients of an S/MIME message.

15



William H. Miller, Governor
Katie Maguire, Secretary
www.kansas.gov

Authenticating Secure Messenger Users

Sender Authentication

- Can be authenticated to recipients in one of two ways
 - Enterprise employees whose SMTP messages are routed to Secure Messenger for delivery will have had their email address checked against the enterprise LDAP directory. Sender's whose email address doesn't exist in the directory will typically not be allowed to send messages through the system.
 - External senders must authenticate using their account password before composing or replying to a message using the browser-based interface.
 - When senders (either enterprise or external) have personal digital certificates available to their email client, an S/MIME digital signature can be applied to provide authentication information to the message recipient. This method of sender authentication is not support directly by Secure Messenger, but instead by the Email Firewall.

16



User Types

Enterprise Users

- A pre-existing LDAP-compliant directory (i.e., Active Directory) manages the user's account and authentication credentials for those who need to send secure outbound messages. There can also be select external customers and partners who have accounts in the enterprise directory.

Registered Users

- The Secure Messenger server manages the user's account information and authentication credentials (password). These are the enterprise's external customers and partners that the Secure Messenger server enrolls during the first secure message delivery.

Unregistered Users

- Neither the Secure Messenger server nor the enterprise directory manages the user's account or authentication credentials. These are users for whom no authentication is required to receive a secure message and limitations are placed on their message reply capabilities.

When Secure Messenger is trying to map the email address in a message to the User Type, it searches through its own list of Registered Users first, then searches the configured Enterprise LDAP directories. If no match is found in either location, the user is assumed to be an Unregistered User.

The user type also determines how the user's role information will be retrieved and applied during message delivery.



User Roles

When messages are determined to be handled by Secure Messenger for delivery, users corresponding to the email address in the message (either From:, To:, CC:, or BCC:) are always assigned to a role.

A role is a collection of messaging capabilities for that user that include:

- How messages are received (Email Notification, Secure Envelope, or Standard Email)
- How long received messages remain on the server (expiration)
- How enrollment of unregistered users occurs
- What restrictions are placed on the sending of messages (number, size, and recipients)
- What type of notifications should be sent (HTML or text)
- What branding should be used for notifications and Web page user interfaces
- What constraints should be placed on the user's password, login attempts (account lockout), and account inactivity threshold.

