

TAG's Security Subgroup Cooperative Security Practices

Tim Blevins
FTA Technology Conference
August 14, 2006

What is the TAG Security Subgroup?

- Formed November 2005 by request of FTA-IRS Tactical Advisory Group
- IRS representatives from Wage & Investment, Small Business/Self Employed, Mission Assurance Security Services and Electronic Tax Administration with other resources as needed
- Six states invited by FTA
 - Dennis Gilleran Massachusetts
 - Partick Dooley Wisconsin
 - Patrick McGuire California
 - Stan Wiechert Kansas
 - James Norton Connecticut

Who's on it?

- Key IRS representatives by function
- State members to represent all states
 - Balance of size, geography
 - FTA facilitates communications
- State members serve 2-year terms
- A portion of the State members rotate off every year
 - Liaison with TIGERS for technology security related implementations

How did the TAG Security Subgroup Come About

- Participation in IRS Security Summit
- Review of high-level policy
- TAG Determined need for Security Subgroup
 - State information security officers
 - Executive level IRS support
 - Six states plus TIGERS
 - Monthly conference calls

What do they work on? Data Security Issues

- Update of Publication 1075
- Review of system-specific settings (“SCSEMs”) and self-audit tools
- Security of IRS data in state data warehouses
- Pilot strong authentication for MeF
- Foreign nationals/background checks
- Data at Rest Products
- Automated Software Checking Tools
- Remote Connectivity

Common Security Controls

- Derived from NIST SP 800-53 *Recommended Security Controls for Federal Information Systems*
- Management Controls:
 - Risk Assessment -identify and document all vulnerabilities
 - Planning- includes a Security plan, policies and procedures
 - System and Service Acquisition- adequate security in place for contractors
 - Certification, Accreditation, and Security Assessments- NIST 800-53 detailed requirements

Common Security Controls (cont)

■ Operational Controls

- Personnel Security-Background checks, access authorized
- Physical Security And Environmental Protection
- Contingency Planning- backup, restoration of data, off-site protections, testing of DR plans
- Configuration Management -maintain inventory of hardware and software components, change control system in place
- Maintenance- Periodic, ongoing, tools used, etc
- System and Information Integrity- Correct flaws, protection mechanisms(anti-virus, spam, attacks, etc) accuracy, completeness, validity and authenticity.

Common Security Controls (cont)

■ Operational Controls continued

- Media Protection-in storage, and when disposed
- Incident Response- Plan and staff to deal with anomalies
- Awareness and Training- Communicate security requirements

■ Technical Controls

- Identification and Authorization
- Access Control- need to know, least permissions
- Audit and Accountability- Reports, Monitoring
- System and Communication Protection -boundary controls, application separation, transmission controls, encryption, web environment controls, etc

Any Project Must Follow Controls

- Controls apply to Data Warehouse or Tax Processing of FTI
- Apply to all environments- Development, Test, and Production
- Apply to onsite and offsite deployments
- In addition Data warehouses have some extra requirements- Exhibit 7 of Pub 1075

Data Warehouse Unique Controls

- Risk assessments of the DW environment
- Planning, detailed policies and procedures of the functions of DW, how legacy data will be brought into the DW and cleansed, not subject to disclosure to the public
- Have adequate security controls to block FTI data to contractors not authorized to access
- For Contingency planning, assure DW resources are synchronized and capable of being restored
- DW audit log must capture information on queries submitted
 - actual query being performed
 - Originator of the query
 - relevant time/stamp information

Secure e-mail Features

- The features of secure e-mail solutions include:
 - *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.
 - *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.
 - *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.

Secure E-Mail Product Vendors

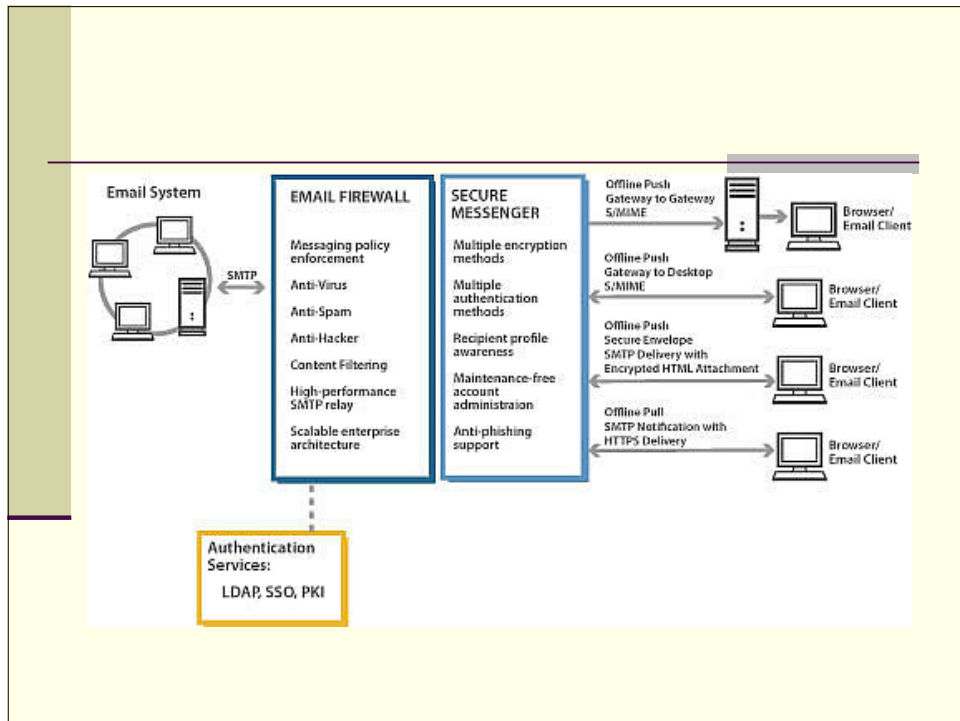
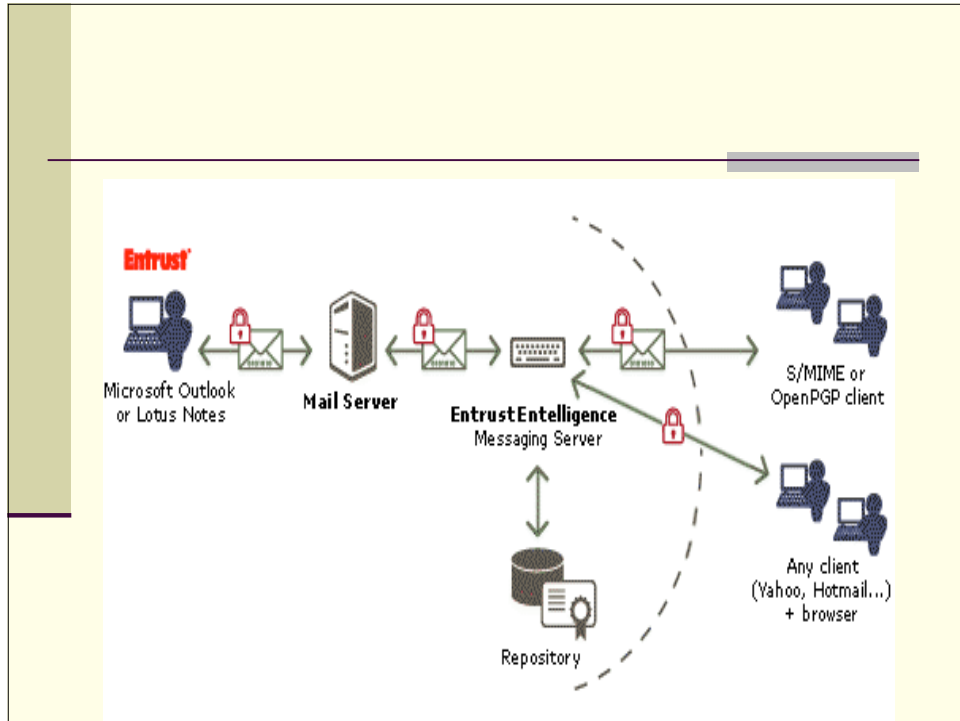
- **Tumbleweed** pioneered what Giga refers to as a *Web courier* method whereby messages are transferred in a three-step process: The sender uploads a message to the courier service via a browser, the service sends an unsecured e-mail notification to the recipient along with a URL link and the recipient downloads the message via a browser by clicking on the URL. Once the message is retrieved it is deleted from the server. The security is achieved through SSL browser sessions, passwords established out-of-bands and audit trails of the activity.
- **Hypersend.com, CertifiedMail.com**
- The *e-mail courier* model works much like the Web courier approach, but instead of going to a browser, the messages are sent between the users and service through the e-mail client. Messages are still sent via HTTP/SSL and so this method requires that users install a plugin. It also only works when both users are members of the same service - unless the service has a "fallback" to Web based delivery for non-member recipients.
- **PrivateExpress, Zixt, Wellance and MailedSafe**
- Secure e-mail gateways reside on the corporate network between the sender and the Internet. Either in the SMTP stream or embedded into an e-mail server such as Microsoft Exchange or Lotus Domino. Secure e-mail gateways intercept outbound, unsecured messages and convert them to secure e-mail. Similarly, these gateways intercept inbound secure messages and convert them to standard, unsecured messages for delivery to the internal recipient.

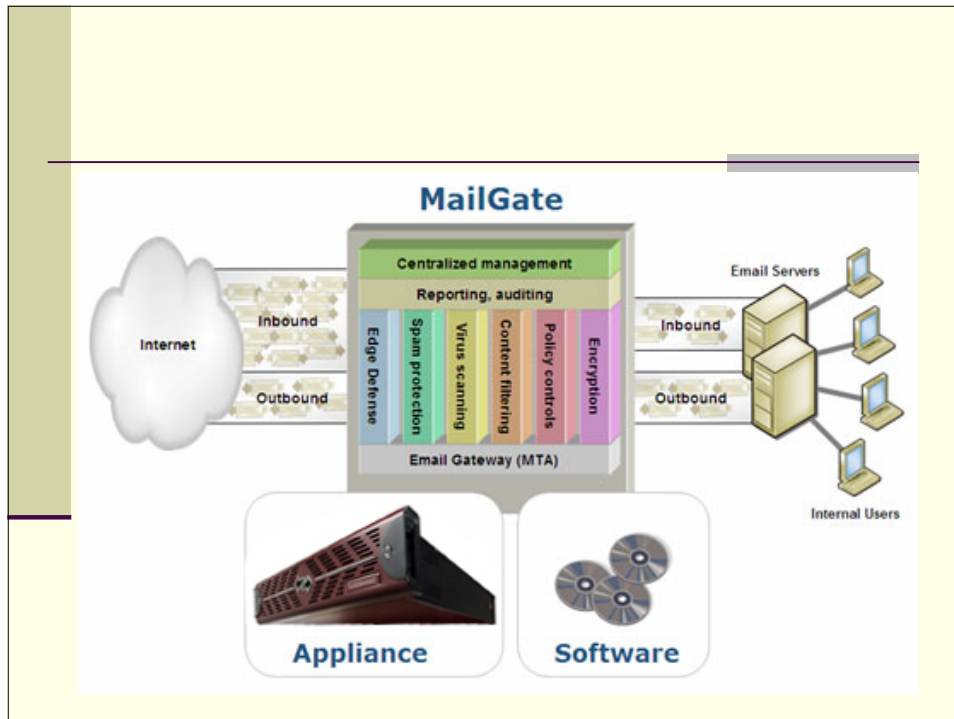
Secure Email Industry Trends

- **HIPAA compliance is driving interest and adoption.**
- **Secure email is merging into broader email content security.**
- **Gateway encryption still remains the way to go, but that might change soon.**
- **Validating the sending server.** Sender validation identifies that the transmitting server is authorized to send on behalf of the sending person's domain. It is performed during the transmission of email from a sending server, called a Message Transfer Agent (MTA), to a receiving server. It prevents spoofing by ensuring that only servers designated by *domain.com* can in fact send mail on behalf of parties with *@domain.com* email address. The two leading candidates for sender validation are SPF and Caller ID.
- **Validating the message.** Message validation techniques bind the sender's identification within the context of a particular message and carry this identification within the message payload. Message validation prevents spoofing by using digital signatures (cryptographic hashes) to ensure that only the purported sender could have created the message. This way, anyone can send, or even relay, a message as long as the payload was signed with a key corresponding to the sender's domain. Yahoo!'s DomainKeys approach appends this signature to the message header, using a unique signing key for each sending server. Receiving servers then look up the public key and validate the signature.

Evolution of email Security

Iteration	Key Features	Ease of Use	Best Use	Solution examples
1 st	Out of band exchange of keys. Manual authentication.	Administratively intense	One-to-one communications with known trading partner	Zip, Acrobat, Word, Omtool
2 nd	In or out of band exchange of keys. Asynchronous. Manual Authentication.	No significant improvement over 1 st iteration	One-to-one communications with known trading partner	PGP
3 rd	Website storage of message. Use of SSL to secure connections to view messages.	Significant improvement in ease of use for message senders and recipients. Message recipient views message on a website in some cases.	One to many or many to one communications. Use of a website to minimize email delivery and email client issues.	Zix, Tumbleweed, Certified Mail, Kryptiq
4 th	Secure "push", encryption and authentication separated to allow use of multiple standards and deliver message to any email client.	Use all existing sender and recipient email boxes. Significant ease of use for all users. Can re-use existing authentication methods.	One to many, many to one, pushing documents and messages to recipient's inbox of choice.	Sigaba, Siemens, ClearSwift





Kansas Dept. of Revenue Security Awareness Training Curriculum

- **Policies**
 - IRC 7213, 7213A, and 7431- Unauthorized Disclosure of Information
 - Confidentiality Provisions and Oath
 - Acceptable Use Policy and Employee Consent Form
 - ID Verification Form
 - Annual Evaluation Reminder Checklist
- **Physical Security**
 - Keycard Badges
 - Building Security- Capitol Police
 - Taxpayer Assistance Center
 - Tailgating
 - Remote Users
- **System Security**
 - Firewalls
 - Internet Usage Reports
 - Antiviral Software
 - Do/Don'ts re email, links, downloading software

Kansas Dept. of Revenue Security Awareness Training Curriculum

- **Application Security**
- Security Management Database
- Confidential Information Safeguards (IRS, KBI, AAMVA)
- Installing Software-PC Support
- Property Rights
- Warning Banners
- Logging
- Conflict of Interest

Kansas Dept. of Revenue Security Applications Security

- Tax Operations:
 - Review Adjustments to Income Tax Records
 - Weekly Report of Abatements of Late Payment Penalties
 - Review of Moved items report
 - Random analysis of transactions by an individual associate
- Motor Vehicles:
 - Review of document deletions
 - Review of Re-instatement of Licenses
 - Review of Issuance of Driver's Licenses

Kansas Dept. of Revenue Security Awareness Training Curriculum

- **Data Security**
- Storage, transmission, backup, and disposal
- Encryption
- Passwords
- Internet access
- Email allowed
- Voice mail
- Fax machines
- PDAs, USB Data Storage, emerging technology
- Reporting Incidents
- Locking PCs
- White boards
- Confidential data
- Shredding
- Clear desk
- Social Engineering

QUESTIONS?

Tim Blevins, Kansas DOR

trb@kdor.state.ks.us

(785)296-5041

Helping to assure the security of KDOR
employees, facilities, and information
systems