fst
Financial Services Technology
www.usfst.com • Vol 2 Issue 2

THE CUSTOMER EXPERIENCE CHALLENGE
MARK BUBAR, CA TECHNOLOGIES: WHERE THE INDUSTRY NEEDS TO GO

CORPORATE VISION
GARY GREENWALD, CITI: DIGITAL SIGNATURES

STAMPING OUT FRAUD
PAYPAL'S MICHAEL BARRETT ON HOW TO BEAT THE PHISHERS

MOBILE BANKING
ILIEVIA AGEENKO TALKS WACHOVIA'S NEW MOBILE SERVICE

THE ONLINE INNOVATORS

GREG FRAMKE ON HOW E*TRADE IS MASHING UP THE WEB

A layered approach to trusted messaging

By **Arvel Hathcock**

Remember when your business first leveraged the power of e-mail communication and utilized the ability to instantly communicate important aspects of your business? How the world has changed in a few short years. You still want to communicate with your customers for legitimate business reasons but your customers won't even open your messages. Industry surveys reflect that nearly 80 percent of banking customers are less likely to respond to your communications and 19 percent will not enroll in online banking or bill payment because of the fear of identity theft. Statistics like these make you wonder if trust in e-mail can ever be restored again between you and your customer. Fortunately, many companies and industry associations are working to restore the effectiveness that e-mail communication first offered your business.

"You still want to communicate with your customers for legitimate business reasons but your customers won't even open your messages"

To help rebuild this trust, a layered approach to messaging is progressively making inroads. Authentication protocols used by e-mail platforms, like Alt-N's MDaemon e-mail server, use Domain Keys Identified Mail (DKIM) and Sender ID to provide important steps to confirm a message's authenticity. According to the Authentication and Online Trust Alliance (AOTA), an industry association focused on facilitating best practices and deployment of authentication and reputation standards, nearly 7 million domains and 43 percent of e-mail traffic contain some form of authentication. But authentication is just one of the many layers of protection needed to restore the confidence e-mail users need.

Another area to work on is the practice of e-mail certification and reputation services. While there are some forms of proprietary certification available today, an open standards approach will help to move this technology into the mainstream. Efforts by the Domain Assurance Council (www.domain-assurance.org) are tackling this issue and have introduced a technology known as 'vouch by reference' (VBR). In essence, VBR describes a mechanism through which certification data can be obtained. Certification is a process whereby a source that you trust vouches for the good behavior of some third party. If you trust the judgment of the certifier you could, for example, skip expensive spam filtering on messages. The result is the creation of a trusted community of e-mail users who employ this technology.

In the meantime, what can you do if you are a small or medium-sized community bank or local financial institution without full-time IT resources to manage your messaging platform? Does this mean that implementing a safe and reliable e-mail solution can only be found in a platform designed for the enterprise and retrofitted for your size of business? Absolutely not. There are some security defenses that you should consider when reviewing the performance capabilities of your e-mail server.

Outbreak protection. Outbreak protection analyzes millions of e-mail patterns over the internet in real-time to detect threats of spam, viruses and other malicious outbreaks.

Content analysis. The e-mail server should implement various layers of threat detection technologies such as Bayesian classification, heuristic learning, sender address verification, keyword matching, virus signature detection and attachment removal of potentially risky messages.

Authentication and access restrictions. The e-mail server should require authentication for sending messages, using strong passwords and restricting the addresses for incoming an outgoing e-mail. Some servers can automatically restrict access through the real-time analysis and response to security-risk behavior patterns exhibited by specified senders.

Verification, reputation and behavior assessment. Spammers and other online predators exhibit common behavior patterns when sending e-mail. These detectable characteristics include using unrestricted open-relay servers, falsifying or spoofing sender identities, tampering with e-mail in transit and sending millions of messages each day. To identify these issues, e-mail servers should use technologies such as DNS black lists, DomainKeys Identified Mail, Sender ID, reverse lookups, greylisting and tarpitting.

Encryption. Industry-standard secure sockets layer (SSL) and transport layer security (TLS) encryption security technologies should be part of any e-mail solution. These technologies use authentication certificates and data encryption to protect against eavesdropping, tampering and forgery.

Alt-N Technologies has deployed over 70,000 e-mail servers around the world to help combat the threats to e-mail security in an effort to restore trust in e-mail communications for small and medium businesses. It also received the AOTA's 2007 Online Safety Leadership award for deploying technologies that are helping to restore online safety, trust and confidence.

While challenges remain toward returning higher levels of trust in e-mail communications between customers and their financial institutions, solutions such as the MDaemon e-mail server are helping to fight the battle. ■

Arvel Hathcock is Founder and CEO of Alt-N Technologies.