



Technology Insights...

October 25, 2006

J.Gold Associates, 6 Valentine Road, Northborough, MA 01532
www.jgoldassociates.com jack.gold@jgoldassociates.com 508-393-5294

Research, Analysis, Strategic Consulting

**A PUBLICATION FOR
CLIENTS OF J.GOLD
ASSOCIATES**

Microsoft's Direct Push Insecurity

The epidemic of recent data losses on mobile devices, primarily laptops, has heightened awareness within most companies of the need to protect portable data and defend it from compromise. Many enterprises are now coming to the realization that mobile security is an imperative, and protection for smart phone devices is becoming as important as securing a notebook. The vast majority of smart phone devices are still only used for email and some limited web surfing, although increasingly corporate back office systems are being extended to users of these devices. We see this trend accelerating in the next 2-3 years as more capable devices at lower cost come to market, and as increasingly available and affordable broadband wireless connectivity options enable more complex and/or robust functions in handheld computing packages for the mobile workforce.

Most enterprise level wireless email systems take data security very seriously. BlackBerry has developed probably the most secure environment, as it provides (and protects) the entire data-chain from server to device. But Good's GoodLink, and Sybase's OneBridge solutions, also do an excellent job of making sure any data transferred from the email server (typically Microsoft Exchange or Lotus Notes) is fully protected. All data is encrypted before it is transferred and also stored as encrypted data on the device, often with full FIPS-level security models. Several third party mobile security products (i.e., Credant, Pointsec, Afaría), provide a protection mechanism for any general data transfers to devices similar to the safe and secure methods incorporated within wireless email platforms, as do the data transfer capabilities within the wireless email packages. All of these products encrypt the data (whether email or application data) at the server, transfer it over their own syncing mechanism, and store the data in encrypted form on the device until it is used and decrypted by the end user.

"...we have recently been made aware of a potentially significant security flaw in Microsoft's Direct Push Technology wireless email that many enterprises should evaluate, and avoid if possible....."

However, we have recently been made aware of a potentially significant security flaw in Microsoft's Direct Push Technology

wireless email, available for the latest versions of Exchange Server 2003 (SP2) and Windows Mobile devices (WM 5.0 with MSFP). This flaw causes security concerns that many enterprises should evaluate, and avoid if possible. The problem arises in the way Direct Push transfers data to the devices.

Direct Push utilizes AirSync, a derivative of ActiveSync, which adds specific over-the-air (OTA) synching protocols (e.g., keep alive signals between device and server, SSL data transmission encryption). ActiveSync (or AirSync for OTA wireless devices) is used for synching data with all of Microsoft's Windows Mobile devices and provides a way for a data store on the device to be synchronized with a data store on a server (or PC if desired). This one-to-one synching is how Pocket PCs and Windows Mobile devices are updated, and how Pocket Outlook synchs with desktop Outlook and/or Exchange Server.

However, the current version of ActiveSync (and AirSync) can only do a file synch of specially formatted datasets that meet certain Microsoft data specifications. That means that any transfer of data, from Exchange Server to Pocket Outlook, for example, must be done in an unencrypted file-state as file encryption would not allow ActiveSync to perform properly. This further means that Direct Push, which utilizes AirSync as its synching method, must transfer unencrypted data files between server and device (although the transmission itself is secured using SSL encryption). This is contrary to how the major wireless email third party applications currently perform, where all data transferred to the device is in an encrypted file format in addition to encrypting the transmissions. In the Direct Push scenario, although the transmission of data files across a network is secure, the storage of data files on the device is not.

ActiveSync (and AirSync) is also problematic for third party providers of security SW, as they are not able to "modify" its operation to heighten security. There is no easy way (via APIs) to hook-in a third party encryption tool to encrypt the Pocket Outlook data stores so synching can be done in an automated fashion while encrypted. While it is possible to encrypt the data stores through add-on SW, it is then not possible to use Direct Push as there is no way for AirSync to synchronize that data with Exchange Server. And there is no way for ActiveSync/AirSync to send an alert to third party SW to say, "I am about to synch, decrypt the data store so I can synch with Exchange, and now that I am done, encrypt the data store". This means no automated encrypt/decrypt process can currently be utilized with Direct Push technology. Third parties who wish to use an encrypted process throughout must therefore build their own synching mechanism and forego the Direct Push solution, or build their own client instead of utilizing Pocket Outlook.

"We believe companies considering the use of Microsoft Exchange Direct Push technology should be very cautious.... explore alternatives to Microsoft Direct Push wireless email until Microsoft has fixed the inherent security problems....."



J. Gold Associates

6 Valentine Road
Northborough, MA 01532

Phone:
508-393-5294

Web:
www.jgoldassociates.com

E-mail:
Jack.gold@jgoldassociates.com

**Research, Analysis,
Strategic Consulting**

Although most data streams over wireless carriers are highly secure, and therefore not subject to interception, companies must nevertheless be concerned about the devices themselves and whether or not the resident data can be easily compromised. The rate of loss and/or theft of smart devices is on the rise. Storing sensitive data in open format is certainly not a “best practice” for any company whose users often have highly sensitive data, including within email. And encrypting only select portions of the device data stores (i.e., everything but email) is only a partial solution at best and allows substantial exposure and risk

Bottom Line: We believe companies considering the use of Microsoft Exchange Direct Push technology should be very cautious. Most end users have sensitive data within their emails. And although devices can be protected with passwords, this is generally not a high enough level of protection for sensitive data. Companies with substantial information security needs (e.g., financial services, health care, life sciences, government) would do well to explore alternatives to Microsoft Direct Push wireless email until Microsoft has fixed the inherent security problems within the application and brought it up to par with the other wireless email solutions available on the market.

