



TOC: You know a concept has gone mainstream when you find that related products are frequently out of stock at your local discount warehouse. For me, that epiphany was prompted by—as unlikely as it may seem—paper shredders.

E-Docs: Signed, Sealed, and Delivered

ROBERT J. BOERI

You know a concept has gone mainstream when related products are frequently out of stock at your local discount warehouse. For me, that epiphany was prompted by—as unlikely as it may seem—paper shredders, when I bought the next-to-last one on the shelf. Shredders are almost foolproof, but paper is usually only one rendition of an original electronic source file. To assure document security, (the concept behind the product) how do you protect all those electronic source files, be they Office, Acrobat, or rich media types, that can be compromised with the click of an email Send button? A tough problem. Let's begin with some recent history.

Almost since the beginning of electronic office and PDF documents, you could password-protect a single file. That was fine, provided only the intended document recipient knew the document's password, didn't divulge the password to others, and you had only a single document to protect. Such security was obviously flawed for single documents, and single-document security does not scale. I could simply tell you the security password for my document, email you the document, and you then could view it, change or remove the password, and distribute it to others. Scaling was a larger problem. Distributing easily-duplicated CDs full of sensitive documents securely requires unique keys for each user and one or more of the following: time-expiration; a fixed number of times the document can be opened; print-locks on the documents; and other controls. Early solutions simply provided a single key for all documents or—worse still—a single key for all CDs containing the document collections. Distributing those documents via the Web increased the problem, with hackers actively lurking to compromise both your site and its documents.

In the mid-90s, solutions included customized add-ons to PDF files extending protection to groups of files, permitting a fixed number of accesses, and time-use restrictions. Even these systems had at least one Achilles' heel, whether they could be short-circuited by resetting workstation calendars or allowed printing.

Have security solutions improved? Microsoft Office 11 will extend security of various sorts to individual documents, including file access controls (disallowing printing, for example) digital signa-

tures to prevent document tampering and encryption. Most early security vendors have gone out of business or have been acquired (with products sometimes dropped after the acquisition). Some players are still left standing and new ones have emerged. Authentica secures HTML, PDF content, and email. FileOpen provides PDF security. Adhaero Technologies secures Microsoft Office documents and email. I also found one innovative vendor, SealedMedia, which seems to have learned from the limitations of earlier security limitations and protects the widest variety of file types I've seen: MS Office, PDF, HTML, and many types of rich media files.

Nobody's security solution is perfect. As you approach perfect security, costs increase faster than additional benefits no matter whose solution you pick. That said, how well do today's solutions measure up for documents delivered via physical media like CD-ROMs and via the Web? According to SealedMedia's founder and CTO, Martin Lambert, SealedMedia uses a technique called *file sealing* that stores access rights separately from secured files themselves. This allows extending protection to document components, including rich media, so "Users can open them from CDs, emails, Web, intranets, and extranets. Users must download access rights initially, but offline access is straightforward."

What about divulged passwords? SealedMedia's solution isn't perfect (see earlier note about the relationship between perfection and cost), but the barrier to this is very high due to the caching of access rights separately from the sealed files. If someone gives their file and password to an unauthorized user, the authorized person can't access that file or any others to which that right applies while the unauthorized party is doing so. Lambert adds: "Detailed audit trails generated by the SealedMedia Unsealer and License Server make sharing easy to detect and pinpoint to individual computers. Finally," says Lambert, "if password sharing must be prevented at all cost, issued rights can be locked to specific devices." Concerned

Nobody's **security solution** is perfect.

about password or security overload? SealedMedia also enforces the kind of best-practice security policies and classifications recommended in ISO17799, geared for large numbers of users.

Microsoft's Office 11 also promises to allow saving documents as XML. XML files, by their very nature, are easily transformed into insecure renditions such as text or HTML. Neither Microsoft, SealedMedia, nor any other company I know of protects XML files at this time. XML security standards for key management, signatures, and encryption are emerging, but it will be at least a year before vendors build those standards into their products. Perfect security is unattainable, but SealedMedia seems to provide very broad and effective solutions today, providing hope for a concept whose time has come. ☐

ROBERT J. BOERI (rboeri@ieee.org) is a knowledge management analyst for a Boston-area biopharmaceutical firm.
Comments? Email letters to the editor to eclletters@infoday.com.