

DISTRIBUTED DATABASE SOLUTIONS ADDRESS SECURITY CONCERNS OF LAN/WAN CLIENT–SERVER DEPLOYMENTS

By:

STEVEN H. BLACKWELL
President & CEO
Management Counseling Services
Alexandria, Virginia

Partner Member
FileMaker Solutions Alliance



“This White Paper focuses on issues particular to security of deployed FileMaker Pro solutions in conjunction with FileMaker Server. It addresses how these issues are managed by the distributed synchronized environment, rather than by the client–server deployed one.”

FSA members are independent entities without authority to bind FileMaker, Inc. and FileMaker, Inc. is not responsible or liable for their actions. The views and recommendations expressed in this White Paper are solely those of the author, and may not necessarily reflect those of FileMaker, Inc. FileMaker Pro® and FileMaker® Server are registered trademarks of FileMaker, Inc. of Santa Clara, California.

January 2004

DISTRIBUTED DATABASE SOLUTIONS ADDRESS SECURITY CONCERNS OF LAN/WAN CLIENT–SERVER DEPLOYMENTS

“This White Paper focuses on issues particular to security of deployed FileMaker Pro solutions in conjunction with FileMaker Server. It addresses how these issues are managed by the distributed synchronized environment, rather than by the client–server deployed one.”

I. Executive Summary

Deployed FileMaker® Pro files hosted by FileMaker® Server for access by WAN based TCP connections or through web browser access using FileMaker Pro Unlimited experience significant threats to the confidentiality and the integrity of their data as well as threats to their proprietary intellectual property. These threats come from both inside and outside the organization in the form of hackers, disgruntled employees and former employees, and spies bent on committing corporate espionage.

Data can be lost or compromised, in the more insidious instances even without the legitimate owners being aware they have been victimized. Money can be lost; legal liability can be incurred; and corporate reputation and images can be damaged, often significantly.

FileMaker Pro files can be subject to security lapses because of architectural or environmental conditions or by a developer’s failure to follow recommended Best Practices. Developer lack of understanding of the security capabilities of the products contributes significantly to this problem.

Distribution of FileMaker Pro solutions to many nodes and the on–going process of synchronization of those files across those nodes can significantly and materially reduce these security threats. The same synchronization process can also provide business continuity features in the FileMaker Pro environment commonly found only in larger enterprise systems.

II. The Information Environment

The Internet and the services it offers are critical to businesses of every type and structure. Whether it's a university providing access to databases of scientific research data, a package delivery service providing tracking of shipments, a national trade association providing an on-line database of its members, or a manufacturing concern reporting to customers on order status—all these rely on rapidly accessible, constantly updated sources of information.

Bruce Schneier is perhaps the world's leading authority on Internet security. A founder of the renown Counterpane Internet Security company, Schneier talks about the risks inherent in the Internet environment:

...with that connection comes new threats: malicious hackers, criminals, industrial spies. These network predators regularly steal corporate assets and intellectual property, cause service breaks and system failures, sully brands, and frighten customers.

Despite decades of research, and hundreds of available security products, the Internet has steadily become more dangerous. The increased complexity of the Internet and its applications, the rush to put more services and people on the Internet, and the desire to interconnect everything all contribute to the increased insecurity of the digital world.¹

So the Information Highway and a lot of way stations along it really provide much less protection than what anyone might suspect, assume, or desire. Yet it need not necessarily be that way.

Bruce Schneier, again talking about the digital world and how we live in it delineates some of our expectations²:

The promise of the Internet is to be a mirror of society. Everything we do in the real world, we want to do on the Internet: conduct private conversations, keep personal papers, sign letters and contracts, speak anonymously, rely on integrity of information, gamble, vote, publish digital documents. All of these things require security. Computer security is a fundamentally enabling technology of the Internet; it's what transforms the Internet from an academic curiosity into a serious business tool. *The limits of security are the limits of the Internet.* And no business or person is without these security needs....

As risky as the Internet is, companies have no choice but to be there. The lures of new markets, new customers, new revenue sources, and new business models are just so great that companies will flock to the Internet regardless of the risks. There is no alternative. *This, more than anything else, is why computer security is so important.* [emphasis supplied]

¹ Schneier, Bruce. "Managed Security Monitoring: Network Security for the 21st Century. Counterpane Internet Security. 2001. <http://www.counterpane.com/msm.pdf>

See also Schneier. *Secrets & Lies Digital Security in a Networked World*. New York, NY. John Wiley & Sons. 2000.

²Schneier. "Managed Security Monitoring" *op.cit.* pp. 2-4.

Protect What?

Security then is important. But what are we trying to protect? What is vulnerable? Generally speaking, database security should address three specific issues:

- Protection of Intellectual Property
- Data Confidentiality
- Data Integrity

Developers of software products should have every reason to expect that their proprietary intellectual property will remain safe and secure. Companies should have every expectation that their proprietary data will remain secure and safe from unauthorized disclosure. And companies also should have every expectation that only authorized individuals can add, modify, or delete information in their systems.

All these expectations are reasonable; none, however, is a guarantee. And sometimes developers and corporations are their own worst enemies when it comes to security. Consider the case of Secure Socket Layers (SSL). This technology, familiar to most web users, can be used to provide encrypted connections from web browsers to secure servers, thus facilitating e-commerce solutions. Likewise, SSL can be used to provide Virtual Private Network (VPN) connections from remote users to corporate LAN's³.

Now, as part of an effort to thwart viruses and to filter content, some organizations have employed SSL filtering software. This software makes it possible to break SSL encryption and read the content of a supposedly secure message. As one commentator recently noted:

...imagine this technology being used by an ISP, or even worse, a repressive government⁴.

Some Threats

What are some general threats to information security in a digital world? Hackers come to mind almost immediately. But who are they and what are they really doing? Are they the prime source of danger to information security? Most malicious

³ Janowski, Davis D. and Sarrel, Matthew D. "Simpler, Safer Remote Access" *PC Magazine*, August 19, 2003. pp. 104-117.

⁴ Raposa, Jim. "SSL Filtering Won't Increase Security" *eWeek*, October 13, 2003. <http://www.eweek.com/article2/0.4149.1348593.00.asp>

damage—or most *reported* malicious damage—comes from the inside. These attacks are more frequent, and they are more costly.⁵

Threats to intellectual property as well as to data confidentiality can come from programs that crack passwords. Numerous such nefarious little utilities can be found all over the Internet; they can be run on files created in programs ranging from Microsoft Excel®, to Adobe Acrobat®, to FileMaker Pro.

Unsecured wireless access to corporate LAN's is one of the most significant and rapidly growing threats to information security⁶. Large percentages of networks, even in the heart of the Silicon Valley, have wireless access (802.11x) devices enabled without any authentication challenges at all. Through use of external antenna, including one made from a Pringles™ Potato Chip can⁷, eavesdroppers can lurk at great distance from the wireless base stations and still pick up signals and intercept traffic.

All these threats conspire to attack the privacy of personal and financial data. Such information can be used to steal assets. These data can also be used by terrorists and criminals to steal identities and to manufacture new, false ones. These threats present the real possibility for corporate espionage where proprietary organization secrets, business processes, and customer lists and buying histories can be sold to competitors.

Likewise security vulnerabilities present disgruntled outsiders who have an insider's knowledge of information assets opportunities to wreak havoc with these assets

⁵ According to a program broadcast on the History Channel on July 26, 2003, Symantec has ascertained that over 50 percent of the hacks with economic loss are caused by insiders and that an insider attack causes greater loss than an external one.

⁶ "Wireless Wardriving" *San Jose Mercury News*, 9/30/2002.
<http://www.siliconvalley.com/mld/siliconvalley/4181308.htm>

"Secret Service Exposing Unsecured Wireless Networks" 9/29/2002
<http://www.nandotimes.com/technology/story/555541p-4378549c.html>

Wearden, Graeme "Drive-by spam hits wireless LANs" 9/6/2002
<http://news.956911.htmlcom.com/2100-1033-956911.html>

Janowski, Davis D. and Chang, Stephanie "The lay of the wireless LAN" *PC Magazine* 5/21/2002

Harmon, Amy "Good (or Unwitting) Neighbors Make for Good Internet Access" *New York Times* 3/4/2002 <http://www.nytimes.com>

Edward, Mark T. and Andress, Mandy "Beware Wireless Security Woes" *E Business Advisor* March 2002

Vichr, Roman and Vivek, Malhotra. "Securing 802.11 transmission, Part 1" 4/15/2003
<http://www-106.ibm.com/developerworks/library/wi-80211security.html>

Krim, Jonathan "WiFi Is Open, Free, and Vulnerable to Hackers" *Washington Post* 7/27/2003

Musgrove, Mike "Keeping WiFi Private Proves Arduous Task" *Washington Post* 7/27/2003

Sherman, Erik "Walk-By hacking" *New York Times Magazine* 7/13/2003

⁷ <http://www.oreillynet.com/cs/weblog/view/wlg/448> and www.vnunet.com/News/1129904

and to engage in extortion and blackmail. Disgruntled insiders, perhaps the single largest source of security breaches, as we have seen, can exploit vulnerabilities to extort money, to seek revenge, or to commit mischief and mayhem.

Finally, a class of individuals I call the *idle curious* can exploit security weaknesses out of a sense of adventure, from a desire to impress co-workers, or just because they have discovered they can do so. And in many instances they cause damage of a significant and serious nature without even intending to do so.

The Damage

The damage from all these intrusions and attacks ranges from the inconvenient to the catastrophic. Loss of proprietary information, including customer lists and histories, loss of business process management data such as manufacturing instructions and plans, and destruction of years of research data can and have crippled organizations, driving them from the marketplace and into oblivion. Damage to organizational reputation, not the least of which is loss of confidence by clients or customers, can cripple future growth and dash expansion plans. Loss of financially valuable data such as membership lists, dues billing and payment histories, credit card transaction confirmations,⁸ and accounts receivable data can strike at the heart of an organization's financial strength, both current and prospective future.

And there are invisible losses as well. A particularly nefarious theft of corporate information, *e.g.* a list of seminar registrants for a training company, would be one that is completely covert. Someone steals the company's data; the company isn't even aware that the data are gone. The next thing that happens is that the registrants get solicited by a rival. Or, in an effort to create mischief or damage the original company's reputation, a competitor sends a bogus cancellation notice. When the original company finds out, they scramble to notify the registrants that the program really wasn't cancelled. However, in doing this, they raise questions about their internal security practices. It truly is a circle, and *vicious* doesn't do it justice as a description.

Combating Threats

To combat these threats and to introduce some security elements into deployed database systems, especially those requiring some sort of persistent WAN based remote access, IS/IT managers have traditionally relied on one or the other of two choices: remote access *via* Secure Socket Layers (SSL) or remote access *via* IP Security (IPSec). When multiple users need simultaneous access in real time or near real time to

⁸ An item often overlooked in the frenzy of discussion about protecting credit card *numbers*.

organizational data and when those users are widely dispersed, the issue of remote access security becomes a fundamental concern.

What are some of the differences in these two approaches? Principally, IPSec based Virtual Private Networks⁹ (VPN's) require installed software on the remote computers or network router with the attendant requisite IT responsibility for configuration, maintenance, and support. SSL users, in contrast, require only the use of a modern web browser for secure remote access¹⁰. In the FileMaker Pro world for example, the use of the CitrixMetaFrame NFuse client¹¹ running *inside a web browser* has delivered the FileMaker Pro desktop database experience to remote users. Such approaches, while effective in the right circumstances, entail expensive licensing and require significant setup as well as dedicated servers and support staff.

III. LAN—WAN Security Threats in the FileMaker Pro Environment

There are a number of specific threats to the security of deployed files hosted by FileMaker Server and accessed by FileMaker Pro. Some of these are architectural; others are environmental. Yet others result from not following recommended Best Practices.

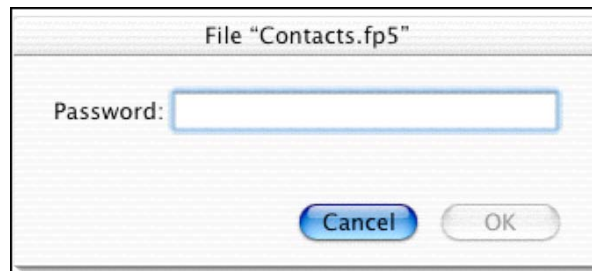
FileMaker Pro and FileMaker Server employ a trusted client model of authentication when a user attempts a connection to a hosted file from the LAN or from a WAN, including the public Internet¹². Essentially this means that passwords are challenged at the client workstation rather than at the server. When a user selects a password protected file name from the File→Open Remote dialog, he or she is presented with the password dialog box:

⁹ Either client to network VPN's or network to network VPN's.

¹⁰ Janowski and Sarrel, *op. cit.* for a fuller discussion of IPSec and SSL driven VPN's..

¹¹ Now referred to by Citrix as "Web Interface for Citrix MetaFrame Server

¹² See FileMaker, Inc. Tech Info Letter 108462, *Security Considerations When Sharing Hosted Databases*, <http://www.filemaker.com/ti/108462.html>



When the user enters a password and clicks the “OK” button, a weakly encoded list of all the passwords for the file is sent from the server to the workstation. If the user–entered password matches one of those in the list from the server, the user is allowed access to the file. If the user–entered password fails, the server repeats the process, sending the weakly encoded list across the LAN or WAN again. Such packets are susceptible to interception and cracking, revealing all the passwords in the file.

Except in certain specific instances, data between FileMaker Pro and FileMaker Server are sent in unencrypted bits representing clear text. A packet sniffer¹³ can easily read this traffic if a hacker gains unauthorized, often surreptitious, access to the network. In an effort to address this issue FileMaker Pro developers have turned to the use of two encryption plug–ins, the Troi Coding Plug–In¹⁴ and the Crypto Tool Box Plug–In¹⁵. Both of these plug–ins allow for the encryption of data in a FileMaker Pro field. Additionally, when FileMaker Server is used in conjunction with FileMaker® Pro 6 Unlimited and a separate web server such as Apache or Microsoft Internet Information Services (IIS), Secure Socket Layer (SSL) transactions can occur for the part of the data’s journey to and from the web server.

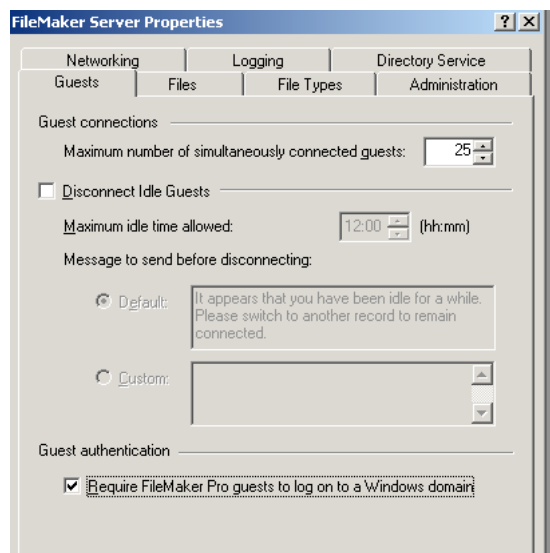
Improperly configured networks are another source of security lapses in the FileMaker Pro environment. FileMaker Server running on the Windows 2000 Server OS provides for user authentication to the domain before a guest is allowed to connect to a hosted file. This feature, introduced in FileMaker Pro 5.5, applies to both Windows and Macintosh guests. In many instances, however, IS/IT administrators have not invoked this option. The option is set by right–clicking on the root level icon of the FileMaker Server executable in the Server Console window to reveal the tabbed interface, and then selecting the “Guests” tab as shown:

¹³ Fuchs, Deborah A. *Watching FileMaker® Pro Network Packets*.

<http://www.apworks.com/downloads.html>

¹⁴ Troi Automatisering <http://www.troi.com>

¹⁵ Protolight Software <http://www.geocities.com/SiliconValley/Network/9327>



In other instances, firewalls are not properly configured, or there are no firewalls employed on a particular LAN.¹⁶ Additionally, in many instances, IS/IT managers or developers enable OS level file sharing on the CPU running FileMaker Server in the *mistaken belief* that file sharing is required for FileMaker Server to operate properly. In fact, it is not. File sharing is both a security risk and a genuine threat to the physical integrity of the file structure of the database. Despite extensive documentation from FileMaker, Inc.¹⁷ and from authoritative third parties¹⁸ cautioning against the use of file sharing, the practice persists. Still another issue, as noted earlier in this paper, is unsecured and unencrypted 802.11x wireless access to LAN's.

The physical security of many FileMaker Pro files is not well maintained. Uncontrolled access to servers by removable media, unlocked server facilities, file sharing, and unsecured “backup” copies of database files all offer ample opportunity for compromising data confidentiality.

¹⁶ The correct port to open for FileMaker Server is Port 5003 for TCP.

¹⁷ *FileMaker Server Best Practices White Paper*, http://www.filemaker.com/downloads/pdf/fms_best_practices.pdf

¹⁸ Blackwell, Steven H. and Miller, Tony. “Optimize FileMaker Server 5.5” *FileMaker Advisor*, July 2002, pp. 28–39.

Article updated, March 2003: http://www.fmp-power.com/Optimal_Server.pdf

Many FileMaker Pro databases are also shared *via* FileMaker Pro Unlimited for access by web browsers. These files are vulnerable to the extraction of their metadata¹⁹ using XML results from CGI calls, including:

- dbnames
- findany
- scriptnames
- layoutnames

While FileMaker Pro 6 addressed the related, but different, issue of purloining of CDML format files by the introduction of the `cdml_format_files` folder, many organizations do not utilize this protective feature.

Another commonly found security lapse for hosted files made accessible for Web Companion sharing is that such files are left set to multi-user. This practice enables them to be accessed directly by FileMaker Pro as a TCP connected guest, exposing data and processes not available from the web browser. FileMaker Pro files do not need to be set to multi-user to be web accessible.

Finally, FileMaker Pro has the capability to import data from an XML source to a local FileMaker Pro file by passing a CGI as part of the specified http request. This process can bring the entire contents of a remote FileMaker Pro hosted file to the local desktop, even creating a new file on the fly as it does so. Thus in many instances, data are exposed to access in unintentionally authorized and unexpected fashions.

IV. The SyncDeK® Model

But there is another way to address the requirement for multiple users in multiple locations to have near real time access to the same data. It is a method that does not require that the database servers be exposed to access from outside a trusted and protected Local Area Network. This method is called *synchronization*, and it offers significant information security benefits and advantages. In the FileMaker Pro environment, this process is accomplished by use of the SyncDeK® system pioneered by WorldSync²⁰, Inc. of Berkeley, California. This White Paper focuses on issues particular

¹⁹ See the FileMaker, Inc. White Paper *FileMaker Pro Web Publishing Security Guidelines*, Version 2, December 2002. <http://www.filemaker.com/downloads/pdf/websecurity122002.pdf> and a related updated Tech Info Letter 108377 <http://www.filemaker.com/ti/108377.html>

²⁰ <http://www.SyncDeK.com>

to security of deployed FileMaker Pro solutions in conjunction with FileMaker® Server. It addresses how these issues are managed by the distributed synchronized environment, rather than by the client–server deployed one.

Because they are exposed to outside connections, WAN accessed FileMaker Pro databases are vulnerable as we have seen. The TCP based protocols allowing data access and transfer are subject to many vagaries and are subject to session hijacking and to data interception. Many organizations take no further precautions to protect networks such as VPN's, dial-in authentications such as PAP or CHAP,²¹ or SSL based connections. However in the distributed model, there is no need for the database to be exposed to the outside public or even to the Local Area Network for that matter. The SyncDeK model is a patent–pending FileMaker Pro database synchronization program that provides for the distribution of FileMaker Pro solutions to multiple nodes as standalone and LAN served modules instead of WAN based or web browser accessed systems. Manufactured by WorldSync of Berkeley, California,²² SyncDeK is a JAVA based background service with an accompanying plug-in to allow control directly from within FileMaker Pro.

At a conceptual level the *synchronization* model has three major components. First, each node has its *own* copy of the database. Second, as changes are made, the various copies are *synchronized* according to various business process rules so that each node has in near real time the same set of information. Third, only those *changes are transmitted* among the various nodes; and, the changes are encrypted before they are transmitted, decrypted, synchronized, and encrypted again.

At an operational level, the synchronization process seeks to answer the core question of *what has changed in a record* since the last synchronization occurred. A user defined timestamp field tracks the last modification to the record. The SyncDeK product then internally determines what fields, if any, have changed in the record. The changed data in all modified records together with all data in new records are then tagged for synchronization with all other users' copies of the database. Deleted records require special handling. Here the challenge is not the deletion in the local copy of the file, but the management of the deletes in the remote files. Deletes must be scripted and maintained in a separate deletes table, a functionality that has multiple, additional beneficial uses²³ as I will discuss subsequently.

²¹ Password Access Protocol and Challenge Handshake Authentication Protocol {sometimes called Challenge Handshake Access Protocol}, both remote access verification and authentication protocols.

²² <http://www.SyncDeK.com>

²³ Not the very least of which is a deletion history of the solution.

Looking further into the SyncDeK process reveals several key attributes of the system:

1. There is no requirement for WAN based or Web based outside access to FileMaker Pro files. Indeed, this restriction can be extended to the Local Area Network as well, when the situation warrants.
2. Only the changes to the files are being sent to all the nodes. This greatly reduces the amount of traffic as well as protecting the bulk of information from exposure.
3. These changes are sent in an encrypted fashion.
4. The local synchronization files remain encrypted after their use at each node.

Adherence to well-known and tested industry standards for encryption is an important part of the security schema of any system. Rather than relying on proprietary systems that have not been subjected to rigorous testing and—yes, hacking attempts—the use of industry standards provides some assurance that an encryption algorithm has had some trial by fire and that its vulnerabilities and strengths are known. It does little good to remove outside access to the database files and then send only the changes to the nodes, if the files containing those changes are susceptible to interception or tampering. Hence a strong encryption algorithm is needed to assure the *confidentiality* and the *integrity* of the synchronization data files.

SyncDeK utilizes the Java Cryptography Extension (JCE) as the basis for its encryption process. Sun Microsystems has developed the JCE²⁴ as a set of “...packages that provide a framework and implementations for encryption, key generation and key agreement, and Message Authentication Code (MAC) algorithms. This includes “...symmetric, asymmetric, block, and stream ciphers.

The JCE is specifically designed to permit addition of qualified cryptography libraries as well as management of jurisdiction questions related to the export of strong but limited versions of the files to countries where the United States Government has placed restrictions on the export of such software.

²⁴ <http://java.sun.com/products/jce>

Specifically, the JCE supports the following algorithms, and SyncDeK users can choose the most appropriate ones for their use:

DES	PBEWithMD5AndTripleDES
DESede	Diffie–Hellman key agreement among multiple parties
Blowfish	HmacMD5
PBEWithMD5AndDES	HmacSHA1
	AES (certain Java SDK’s only)

V. How the SyncDeK Model Addresses Enterprise Security Issues

Business Continuity.

The SyncDeK Java based service has considerable more design rigor than is normally present in an *ad hoc* FileMaker Pro solution. Because of this rigor, in addition to providing synchronization, SyncDeK creates with the FileMaker Pro environment a suite of capabilities normally found only in much more complex, enterprise wide database systems:

- Roll Forward
- Deletion Logging and Roll Back
- Audit trails
- Global Unique Ids
- Database version tracking and automated update

Consider some of the implications the presence of this suite raises. Some of these items fall under the distinction of data integrity: namely that only authorized users are permitted to take actions and that management can rely on the database’s security schema to enforce business process rules. But beyond that lies another area: that of *system survivability* and redundancy and *business continuity*. *A database system needs to be able to survive multiple points of failure.* SyncDeK’s capabilities aid system survivability to a large degree and assist in assuring business continuity.

FileMaker Pro developers as well as IS/IT professionals need to view database security in the larger context of business continuity. An underlying purpose of security activities is to assure that that business critical data are available on an on-going basis so that essential business processes can continue. Therefore we need to plan these activities within the broader construct of business continuity.

What is *business continuity*? What are its parts? Simply stated, business continuity is the prearranged and predetermined set of plans and processes an organization implements to assure that it can continue to operate at least at a core level in the event of any number of attacks or disasters.

What will you do if your business site loses electrical power for 48 hours or longer? How will you communicate if your Internet access is interrupted for 72 hours? How will you continue to provide services if a hacker takes down your database server and that server can not be resurrected? Or as we all sadly saw on September 11, 2001, how will you continue to function if your business site or that of your ISP is destroyed in a terrorist attack?

Roll Back and *Roll Forward* are added features of the SyncDeK model. Each time a synchronization occurs an encrypted shuttle file is sent to each node. This file contains instructions along with data. These shuttles are archived after each synchronization. If an anomaly occurs, *e.g.* accidental deletion of records, these deletes can be rolled back into the database using a function available in SyncDeK's deletion log. Conversely, if a crash occurs, reprocessing all shuttles created after the time of the last stable backup will roll the database forward to its state just before the crash occurred. If data in any one of the distributed files is lost, the system may simply be replaced along with the updates that have occurred in the interim.

The *Audit Trail* is an added SyncDeK feature that can be toggled on or off. When activated, it creates a field level change log that indicates the history of that field as well as the identities of the actors on the field. It is a simple text file, but it can be imported into a FileMaker Pro database for further analysis.

Data Confidentiality Protection.

In the SyncDeK induced and controlled synchronization process, data do not travel unencrypted over a WAN based connection as they do in a client-server model. If intercepted these data are protected by a strong encryption algorithm, *e.g.* TripleDES. Additionally, only the *changes* are sent, not the entire file along with its metadata as is the case in the client-server model. Moreover, there is no WAN-based access to files hosted by FileMaker Server. Such files can be vulnerable²⁵ to external access and attempts to extract data. Because of the trusted client model (as described in Section III

²⁵ Absent additional protect such as a VPN.

of this White Paper), password data could possibly be intercepted and decoded, giving unauthorized users access to the files.

Additionally, in many instances as also noted previously, FileMaker Pro developers have not employed various Best Practices; indeed they have frequently introduced items such as ersatz log-on files that diminish actual security and that further jeopardize the security of their files. These files are especially vulnerable to attack on an open WAN connection. The distributed database model envisioned by SyncDeK can dramatically reduce these exposures.

VI. Security Issues Raised by the Distributed Solution Model

One issue the distributed model raises is that multiple copies of the database are dispersed to a wide variety of locations. Physical security of these files is important; this is particularly true for data stored on laptop computers used by mobile workers. Strict management policies for such computers significantly lessen the likelihood of compromised data. At the very least log-on passwords and password controlled screen savers can add a minimal level of security. Other circumstances and business conditions may require stronger measures.

The SyncDeK shuttle files travel in a strongly encrypted state, and once used in the synchronization process, return to their encrypted state for archiving. They thus pose little risk for threats to data confidentiality.

VII. Comparative Judgments and Best Practice Recommendations

Based on a review of the options available for both distributed systems and for deployed client-server systems, I can offer three comparative judgments and Best Practice recommendations:

1. Removing FileMaker Pro files from Internet access by Web browsers significantly reduces a major security threat to the data in such files. Replacing them with a distributed, synchronized system is a much better option. For files that still require browser based access, stringent architectural protections and internal LAN security protections should be invoked to preserve their integrity and confidentiality.

2. Removing access to FileMaker Pro files hosted by FileMaker Server from the public Internet serving as a WAN significantly reduces another major series of threats to their integrity, confidentiality, and proprietary intellectual property. Significant precautions in both network architecture and WAN gateway configuration need to be taken on behalf of files that still require WAN based access *via* the Internet or *via* a closed WAN for that matter.
3. The use of a synchronized, distributed system can achieve the benefits of closing WAN based access without having to resort to dramatic steps as port forwarding, encryption plug-ins, or VPN tunneling, including the use of L2TP,²⁶ IPSec, CHAP²⁷, *etc.*

#####

²⁶ Layer Two Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by an Internet service provider (ISP) to enable the operation of a virtual private network (VPN) over the Internet. L2TP merges the best features of two other tunneling protocols: PPTP from Microsoft and L2F from Cisco Systems. For more information see http://searchNetworking.techtarget.com/sDefinition/0,,sid7_gci493383,00.html

²⁷ Challenge Handshake Authentication Protocol {sometimes called Challenge Handshake Access Protocol}, a verification and authentication system used in some remote connectivity schemes, including analog or ISDN dial-up.

STEVEN H. BLACKWELL



Steven H. Blackwell is an independent FileMaker Pro consulting developer and a long-time Partner Member of the FileMaker Solutions Alliance. He has twice been recognized by FileMaker, Inc. with its highest award: the FILEMAKER EXCELLENCE AWARD, both in 1998 (the first ever awarded) and again in 2003. He has also been the recipient of the FileMaker, Inc. “Mad Dog” award for promoting positive media coverage of FileMaker Pro. He is a frequent speaker at FileMaker DEVCON’s and MacWorld FileMaker Power Tools programs. He is Senior Contributing Editor of *FileMaker Advisor* magazine. He maintains the FileMaker Power web site at <http://www.FMP-Power.com>. He is co-author of the *FileMaker Server Best Practices White Paper* available on the FileMaker, Inc. website at <http://www.filemaker.com>. He is considered the leading authority in the developer community on the subject of FileMaker Pro security and is the author of the forthcoming book on FileMaker Pro and FileMaker Server security, *Inside the Security Veil*, to be released in 2004.

