White Paper

FileMaker 7 Security

Purpose & Audience

This whitepaper compares the major features of the FileMaker, products against the security requirements of work-groups and departmental-level organizations. It provides technical details so security experts, IT staff, and application developers can determine how the FileMaker 7 products could met their security requirements and work together with their existing infrastructure for security services like authentication and auditing.

Product Line Overview

The FileMaker 7 product line includes four main products. FileMaker Pro 7 provides a platform for developing and executing database applications that can be accessed by local users, remote users via a web interface, peer-to-peer connections to other systems running FileMaker Pro 7, or client-server connections to FileMaker Server 7. The FileMaker Server 7 product provides large-scale capabilities for sharing database applications including extensive web publishing features. The FileMaker Developer 7 product provides additional tools for the creation and understanding of applications that run on the other two products. The FileMaker Mobile 7 product provides an easy way to build applications that run on handheld computers and synchronize with the other products.

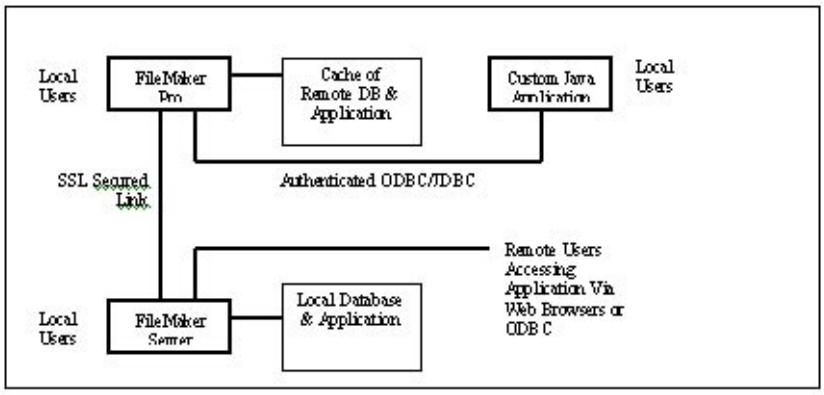

Figure 1. FileMaker Pro 7 systems support local users and a client-server links for remote database access. An application can allow GUI access via web browsers, or programmatic access via ODBC/JDBC and other methods.

The FileMaker products can be configured in numerous ways to meet the needs of different environments. The next two figures illustrate some ways that the products can be connected.

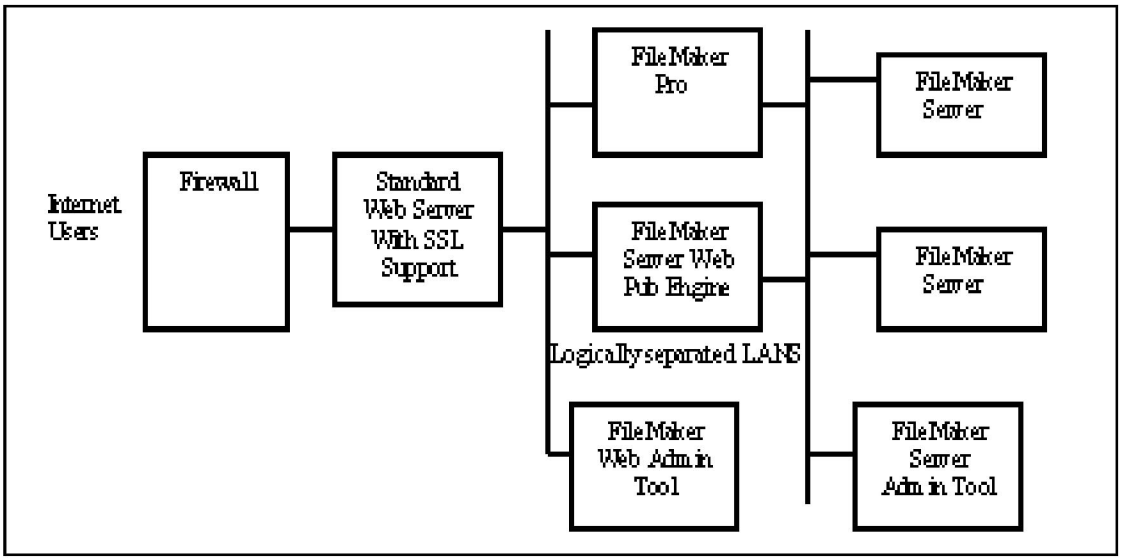

Figure 2. The FileMaker Server product supports more FileMaker Pro clients, enables additional web publishing capabilities and use of ODBC/JDBC for local and remote client applications. Developers can increase security over the Internet with an Apache or IIS web server providing an SSL front end for the web publishing components. FileMaker Server can be remotely administered via an SSL secured channel.

Security Philosophy & Goals

A distinguishing feature of the FileMaker 7 products is that they make good security relatively easy to set up. Many products have elaborate security systems that are very hard to setup or modify, so organizations simply turn off all the security. FileMaker has chosen security features that are easy to understand that interact with each other in straightforward ways and that are simple to setup and maintain. The product reference document explain security considerations for sensitive commands (e.g., granting privileges to accounts, or creating relationships between tables), and a separate security guide helps application developers and administrators understand security issues so they can choose appropriate mechanisms to meet their requirements.

The security features are designed to benefit three categories of FileMaker customers.

1. **Application Developers** need ways to protect the integrity of their applications to reduce support costs and increase revenues, and yet to allow end-users to perform expected changes like adding users and making minor enhancements. The fine-grain access control mechanisms for data, script execution, meta-data and the scriptable security features help in this area.

2. **System Administrators** want new technologies to leverage existing infrastructure for authenticating users and protecting network resources (e.g., firewalls). The FileMaker Server can use existing authentication

servers (Windows Domain or Apple Open Directory via proper OSX configuration), and use standard communication protocols for network access (HTTP for web clients, and CORBA and optionally over SSL/TLS for client-server). The FileMaker Server audit trails are simple text files that easily integrate with third party reporting tools. FileMaker Server includes secure remote management features including time-based scripting to automate tasks like database backups.

3. **End Users** want security to be as transparent as possible and they insist that applications always provide consistent information whenever that information is required. Users will be particularly happy with FileMaker applications that use existing authentication servers; for example, with a single account name and password users gain the benefits of "single sign-on" and thus can skip the pop-up for a account name-password dialog. Data consistency and availability has long been a fundamental feature of FileMaker products. In FileMaker 7, there are improved controls over access methods such as ODBC/JDBC*, Apple Events, Windows OLE and web publishing. The end users will benefit from high application availability and reliability due to a backup mechanism that more quickly produces a consistent database snapshot.

On the other hand, the security system is designed to thwart the attackers listed below in order of increasing capability.

1. Remote outsiders that may have some internal knowledge (e.g., ex-employees).
2. Local insiders with network access.
3. Local insiders with admin access to computers hosting FileMaker applications.
4. System crackers with reverse-engineering skills and insider network access.

The FileMaker 7 products are designed to be securable against the first two types of attackers, and by working with other security products (e.g., disk encryption and firewalls), the products can defend against the more powerful attackers.

The following table summarizes the product features that help address the major security requirements of work-groups and departmental-level organizations.

Table 1. Security requirements and features.

Requirement	Features
Security Documentation	Documentation explains security considerations for each command to simplify the work of building securable applications.
	Separate guide explains security issues and trade-offs.
File Security	Multiple tables, application layouts and scripts fit in a single file for uniform security treatment.
	Folder/Directory organization separates databases, backup datasets and other sensitive information for secure integration with web server folder structures.
	Proprietary compression thwarts text-editor attacks.
	Local record cache file (for peer-to-peer and client-server connections) is encrypted with fast proprietary algorithm.
	Integrates easily with third party disk, folder, and file encryption tools.

Requirement	Features
Backup & Recovery (FileMaker Server)	Backup folder can be separate from data and application folder.
	Remote administration can be authenticated via passwords over SSL secured channel.
Middleware & Application Security	FileMaker programs protected by standard OS security mechanisms and run with ordinary user privileges.
	FileMaker plugins protected in dedicated folder. Plugins can be centrally updated to ensure consistency.
	Applications built on FileMaker products are stored in the database files and thus protected by the same OS file access controls.
Communication Security	All peer-to-peer and client-server communication performed with CORBA formats. Server connections can be sent over SSL secured channels using server and/or client X.509 certificates. This thwarts eavesdropping and session hijacking.
	Certificates are automatically generated during installation. They are effectively self-signed, so the trust comes from the integrity of the hostname lookup system (DNS). Man-in-the-middle attacks are possible for insiders.
	Certificates are stored in standard formats (PEM). This enables third party enhancements to trust model.
	Web Publishing from FileMaker Pro or Server can restrict access to specific IP addresses to reduce potential attack sites.
	Internet client access can be secured using SSL through a standard web server like Apache or IIS.
Authentication	Allow individually assigned usernames and passwords.
	Can require username and password to authenticate all access methods include ODBC, JDBC, meta-data lookup, etc.
	Enforce minimum password length. Application developers can write scripts to enforce complex password quality rules.
	Either product dialogs or application scripts can manage accounts and passwords including deactivating accounts, resetting passwords, forcing a password change, etc.
	Passwords verified on FM Pro host or FM Server, so authentication information never leaves the well-protected environment.
	Passwords stored in database files as salted one-way hash values using well respected algorithm (PKCS #5 PBKDF2) to thwart dictionary attacks even if attackers has copy of the database file.
	Passwords sent to server are always obscured by a proprietary modification to a standard cryptographic algorithm.
	The FM Server can require that all passwords and other data exchanged with the server be carried over an SSL protected channel to prevent eavesdropping and tampering.
	The FM Server can work with an external authentication service like Windows Domain or Apple Open Directory to authenticate users who are already known to the OS and network environment. This allows the leveraging of existing security infrastructure and provides single sign-on to end-users.
	Access to Web Publisher applications can be restricted by source IP address or hostname.

Requirement	Features
Data-Level Access Controls	Good default security for newly created databases. The default includes read-only guest account, and an account with application designed privileges. The remote access methods (e.g., Web or ODBC) are turned off.
	Simple and uniform way to group together table, record and field level access controls into Privilege Sets (PS), and then each username is assigned to exactly one PS. This is basically role-based access control, which is ideal for database applications. Note that individual accountability is maintained.
	Coarse grain controls provide quick solutions to simple requirements for the major access modes of "read-only", "read-write", and "design application."
	Fine grain controls can restrict the set of accessible records based on real-time calculations that can involve user attributes (e.g., username or department), external calculations (e.g., time of day, source IP address), and fields in the record being accessed.
	Fine grain controls can hide specific fields from specific users or privilege sets.
Meta-Data Access Controls	The list of available database on an FM Server can be reduced to just show the databases to which a user has access.
	Several features can be turned on to make the list of tables, layouts, scripts, and fields hard to determine for external users even if the web publishing services are being used.
	SSL communication encryption with FM Server hides meta-data (e.g., table and layout names) as well as data values.
Application Access Controls	The fine grain controls can restrict the privilege sets that are allowed to access or modify scripts, layouts, value lists, and other aspects of the application.
	The ability to allow an individual script to run with "full privileges", so it can perform actions on behalf of a user who otherwise has restricted privileges. For example, there is no need to give the user explicit and general privileges to delete records in a table; a script can programmatically validate the circumstances under which a record can be deleted, and then using Full Privileges, delete the record on behalf of the user.
	Scriptable operations for user and password administration allow a developer to handle all user management with custom scripts.
	Plugin modules used by custom application to access resources outside of the FileMaker products are protected using standard OS mechanisms.
	Web publishing Custom Web Publishing with XSLT – developer can pre-define URL parameters such as database names and query strings to hide them from web browsers and override user-provided variations.
Auditing (FileMaker Server)	Valid and invalid login attempts are audited for all access methods including ODBC and JDBC.
	Audit files are in a simple text format that can be parsed by third party audit management tools.
	The web-publishing module can create detailed logs of each login and record access.
Remote Administration (FileMaker Server)	The FileMaker Server Administration Tool can monitor and modify different FileMaker Server systems via an SSL secured channel authenticated by a username and password.
	The Web-publishing modules support secure remote administration.
	Administrative change to privilege sets become effective at next login. There is no need to stop and restart the server.

The preceding table shows that the FileMaker 7 suite of products are designed to meet the primary security requirements in areas that are important to application developers, IT administrators and end-users. Additional information about the security features is presented in the following section, which are organized into the major security areas: authentication, access control, auditing, file security and communication security.

Authentication

The password management in FileMaker 7 is flexible and relatively easy to use. It is familiar to users and will give them a sense of individual accountability, since they cannot be wrongly blamed for actions taken by the use of a password that "everybody" knows. This enables one to have more responsibility and control. For example, the product includes self-management for passwords, so users can delegate their authority when they go on vacation by 1) changing the password, 2) telling their replacement the new password, and 3) restoring the old password when they get back. This is a common and valuable capability.

The administrators of the applications will appreciate that actions of the application can be tied to specific individuals. Such accountability tends to discourage irresponsible behaviors and allows administrators to identify the users who need additional training. If an attack does happen, the individual account identification may provide clues for an investigation.

FileMaker supports basic password quality checks (e.g., minimum length) and password management (e.g., expiration and reset) features. All these features can be automated in scripts, so the application developer can enforce complex rules for password quality and for account usage constraints (e.g., Tom is the acting branch manager from May 1 though May 15).

The external authentication feature in FileMaker 7 allows an application administrator to leverage the organization's existing infrastructure for authenticating users, and thus saves time for the administrators. An administrator can configure FileMaker application access by making existing user accounts be members of various named groups. FileMaker 7 translates the group names into specific privileges for the applications.

FileMaker 7 has a simple yet flexible system to perform external authentication checks. When a FileMaker 7 application is designed to use external authentication, there are likely to be only a small number of usernames defined, and these usernames will correspond to roles or classes of users, rather than to individual users. The FileMaker account names appear in an ordered list, and each account name may have a single external authentication server group name associated with it. This account names are marked as "external server" for authentication. FileMaker examines the account names in order to check whether the current user (who is already externally authenticated) belongs to the group name associated with that FileMaker username. If so, then FileMaker stops and assigns the user the username and privilege set associated with that FileMaker username. This solution is flexible enough to meet the needs of typical applications (e.g., where there are less than two dozen different roles or classes of users for an application) and is simple enough to explain quickly, which also means that it is simple enough to help avoid mistakes that could compromise the application's security.

Access Controls

The access control model for this release consists of associating access constraints to a named Privilege Set (PS) and then assigning the PS to one or more account names. Each account has exactly one PS. This design is simpler than many operating system security models. However, complex grouping (accounts belonging to multiple PS

groups) is not necessary for FileMaker. The current design is easy-to-understand and powerful enough to meet the needs of FileMaker applications. The primary reason that operating systems allow an account to belong to multiple groups is that each group corresponds to a new application that the user will participate in. For FileMaker applications, there will be a different database file for each application, so there is little need to have an account to have multiple Privilege Sets. There are great simplifications possible by restricting each account to a single Privilege Set (e.g., no need to define how conflicting access rights get resolved). Basically, Privilege Sets correspond to job roles in an application, and this is a model that is easier for people to understand.

The FileMaker application developers, who are often independent third-party software vendors, will appreciate several fine-grain control features in FileMaker 7. The major improvement is the ability to create applications that do not grant "full access" to any customer account, and yet can perform all the account management operations such as adding users and resetting passwords. In earlier releases, the software vendor needed to provide the end customer with an account that was powerful enough to add a new account, and this power also granted the customer the ability to view and modify all scripts and layouts and XSLT information. This in turn led to technical support problems when customers incorrectly modified the applications, and led to lost revenue for vendors who expected to be paid to enhance the application as the needs of the customer changed.

FileMaker 7 allows limited powers to be implemented by creating scripts that can be run by the customer under the "full access" privileges without granting the customer those privileges directly. There is a new feature that allows scripts to run with privileges that are not directly available to the end-user. Thus the scripts can perform all the required management operations without granting those powers to any end-user account.

The access control system for FileMaker 7 is uniform and easier to understand, which makes the developer's job easier than with earlier releases. The product includes fine-grain controls on meta-data such as the ability to modify layouts, scripts, value lists, and inter-table relationships. Thus an application developer can grant a customer the ability to make limited enhancements to an application and yet retain enough control to help avoid support problems and lost revenue.

Auditing

The FileMaker Server product and the Web Publishing feature of FileMaker Pro both produce audit trails that are stored as ASCII text files. This format can easily be parsed by third party tools for audit trail management and reporting.

As required by most organizations, all valid and invalid password attempts are audited. This allows an organization to detect password-guessing attacks. The auditing can cover all access methods including the authentication used to access meta-data (e.g., determine the list of databases accessible to a user), and programmatic interfaces such as JDBC.

The web publishing modules can provide detailed audit records about the source and nature of each request to the application. These records are important because the web modules are exposed to the widest class of attackers.

Audit trail information can also be used for non-attack problems. The information can help locate mistakes made by authorized used and to identify users who should receive additional training. Applications built with the FileMaker tools can easily include application-level audit tables that record information that is beyond the scope of what the core product can record.

File Security

The database file is not encrypted, but the data is obscured via a proprietary Unicode compression algorithm. This will help prevent casual attackers from extracting data from copies of the application files using a text-editor. When one FileMaker product is accessing peer-to-peer or client-server data, the local cache file no longer contains the list of all passwords, because authentication is performed remotely. The compressed data in the cache file is further obscured to protect the data and metadata with a fast proprietary encryption algorithm. Customers who require better file-level security can use file and folder encryption features built into the operating system (e.g., WinNT and WinXP Pro) or with third party tools. They can also use the file and folder access control mechanisms of the underlying OS to restrict access from local users. High security applications can use the FileMaker Server product running on a computer that is protected from ordinary users.

Communication Security

The communication between the FileMaker products such as Pro and Server is performed using CORBA formats and connections to FileMaker Server can be secured by an SSL session. The SSL session helps prevent an insider with access to the LAN from reading or modifying any of the data or control commands (including login requests) sent between the products. The SSL encryption is performed with the Triple-DES cipher and HMAC-SHA1 for integrity checking. These secure connections can cover client-server connections including the remote administration features for servers and web publishing modules.

In keeping with an ease-of-use philosophy, each FileMaker Server instance has a simple on/off switch that requires SSL protection for all or none of the connections. When it is turned on, both the client and server ends of the SSL connection use certificates to mutually authenticate each other. This applies to FileMaker Pro clients and FileMaker Server Web Publishing Engines, but not to ODBC/JDBC or web browsing connections. These certificates are generated when the product is installed and stored in a standard format file (PEM format). The X.509 certificates are effectively self-signed, so the trust between the ends of the SSL connection really comes from the hostname address resolution system (DNS) rather than the certificate. However, this approach does provide good privacy and integrity, and it prevents the hijacking of authenticated database sessions, which is possible for normal TCP connections. Third party products could change the contents of the PEM files to establish stronger trust relationship.

Summary

The security features in the FileMaker 7 family of products are intended to meet the security requirements of work-groups and departmental-level organizations for authentication, access control, auditing, file security and communication security. The security features in FileMaker 7 are more comprehensive and yet are generally easy to understand, setup and maintain.

Glossary

Apple Open Directory. The Apple operating systems support a centralized authentication service called the Apple Open Directory. This service supports several features other than authentication.

CORBA. This is a standard format and protocol for exchanging data and commands between computers that is based on an object oriented model.

ODBC, JDBC. This is standard a format and protocol for exchanging data and commands with database systems. The Java interface to this protocol is called JDBC.

Peer-To-Peer, Client-Server. Two FileMaker Pro systems can communicate directly with each other via a Peer-To-Peer link. When a FileMaker Pro or FileMaker Server system communicates with a FileMaker Server system, it is called a client-server link. The client-server links can be secured by an SSL channel.

SSL, TLS. The Secure Socket Layer protocol, and its successor, the Transport Layer Security protocol are the standard means to protect sensitive communication over the Internet. For example, most merchant sites turn on SSL or TLS security (as indicated by the lock icon) when a customer is entering a credit card number. FileMaker Server uses the more modern TLS protocol, but for historical reasons, this is often called an SSL secured channel.

Windows Domain. The Microsoft operating system supports a centralized authentication service called the Windows Domain Controller, which can be hosted on WinNT or WinXP. This service supports several features other than authentication.

X.509 Digital Certificate. The SSL and TLS protocols use these digitally signed identification credentials to ensure that the secure channel is established with a trusted entity (e.g., a merchant).

About the Author

Dr. Robert W. Baldwin has been building and breaking security systems for twenty-five years. He earned a Ph.D. at MIT for pioneering the field of expert system analysis of computer security. He has contributed to network security (IPSec, SSL, S/MIME), OS security (Orange Book, Common Criteria), Database Security (SQL authorization model), and cryptography (Crypto-C, SET). Plus Five Consulting was founded in 1999 by Dr. Robert W. Baldwin who was a Technical Director at RSA Security, and Ms. Anne C. Wilson was a Director of Engineering at RSA. Together they bring over 50 years of experience in software and security to help clients quickly produce profitable solutions to their problems.

(Footnotes)

*The FileMaker 7 product line can not act as an ODBC source on Mac OS X.