FMK FileMaker Konferenz

Security and Database Encryption

Jon Thatcher
FileMaker, Inc.

Who is Jon Thatcher?

- Lead Software Engineer on Database Server
- 25 years at FileMaker (and Claris)
  - Directed development of Draco engine, FileMaker Pro and Server 7
  - Helped Clay Maeckel ship the first FileMaker Server in 1994
  - Worked on FileMaker Pro starting in 1993
  - Previous experience at Intel, Convergent Technologies, and Esvel (database startup)

What’s in this session

- Security: the Threat Landscape and FileMaker
  - Or “Why you need FileMaker 13 Database Encryption”
- Database Encryption – Under the Hood
  - Why, What and How

Security: the Threat Landscape and FileMaker

- Adapted from Rosemary Tietge’s presentation
  - But I made **lots** of changes, so don’t blame her!
- Rosemary: a Consulting Engineer at FileMaker
  - 25 years of experience with FileMaker
  - Advises customers of all sizes, all over the USA
  - Started work in Washington, DC with customers in the US government, many highly concerned about security

Security: the Threat Landscape - Agenda

- The scary numbers
- How – Attack vectors
- What – Incident Patterns
  - Who is vulnerable
  - What can we do?
  - Related compliance areas
  - Resources

Some Scary Numbers

- **63437** confirmed incidents in 2013*
- **1367** confirmed data breaches in 2013*
  - *Verizon Data Breach Investigations Report 2014: http://www.verizonenterprise.com/DBIR/2014/
- **40 million** credit and debit cards stolen from Target between Nov. 27 and Dec. 15, 2013**
  - **Krebs on Security, The Target Breach by the Numbers: http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/

More Scary Numbers

- **8** breaches each exposed >10 million identities
- Median number of identities exposed: **6777**
- In total over **552 million** identities were breached in 2013
    - From Symantec Internet Security Threat Report 2014: http://www.symantec.com/security_response/publications/threatreport.jsp

Scariest Numbers

- 30% of breaches were targeted at small to medium businesses (SMBs, <1000 employees)
- 60% of SMBs close within 6 months of a breach
- 72% of SMBs shut down within 24 months of a data breach
  - From Symantec Internet Security Threat Report 2013

A truly world-wide problem

- Personal information stolen on 2 million out of 32 million Vodaphone Germany customers
  - http://www.vodafone.de/privat/hilfe-support/kundeninformation.html?icmp=Privatkunden%3A217142%3A%3A3
- European customer information stolen from French Internet provider OVH
  - http://status.ovh.net/?do=details&id=5070

Attack vectors

- Targeted attacks
- Zero-day vulnerabilities
- Viruses and malware
- Attacking the Internet of Things

Targeted attacks

- Spear phishing
  - Targeted at a specific user or group
  - Uses previously gathered data to appear more legitimate
  - Fools user into giving data or compromising device
- Watering hole
  - Legitimate website compromised to host malware
  - Uses zero-day vulnerability to install on visitor machines

Zero-day vulnerabilities

- A zero-day (or zero-hour) vulnerability is…
  - An attack that exploits a previously unknown vulnerability in a computer application—one that developers have not had time to address and patch
  - There are zero days between the time the vulnerability is discovered (and made public), and the first attack
- Often occur in Java or Flash, but lots of others, like “Heartbleed" bug in OpenSSL

Viruses and malware

- Viruses
  - Computer viruses spread themselves by using built-in tools like email and contacts to spread through a group
- Malware
  - Often downloaded via spear phishing or watering hole
  - May log keystrokes to get bank accounts and passwords
  - “Ransomware” encrypts hard drive and demands ransom
  - May target mobile devices or be embedded in rogue apps

Attacking the Internet of Things

- Attacking security flaws in…
  - Home security cameras – to watch your keyboard
  - Home network routers – to capture your data
  - Baby monitors(!) – to listen to your phone calls
- More devices include small web servers
  - May be vulnerable to Heartbleed or similar attacks
  - Often have weak default passwords

Verizon data breach report

- Nine patterns of incidents identified
  - Covers 95% of reported security incidents
- For each pattern:
  - Attack methods
  - Industries targeted
  - How to mitigate risks

Nine Incident Patterns

People and Things

1. Insider and Privilege Misuse
2. Physical Loss and Theft
3. Miscellaneous Errors

High Value Information

4. Point of Sale Intrusions
5. Web App Attacks
6. Card Skimmers

Other Crime

7. Crimeware
8. Cyber Espionage
9. Denial of Service Attacks

Graphic: Verizon Data Breach Investigations Report 2014

Secure the People and the Things

1. Insider and Privilege Misuse
2. Physical Loss and Theft
3. Miscellaneous Errors

- Easiest to address and with quick benefits
- Applies to all industries

1. Insider and Privilege Misuse

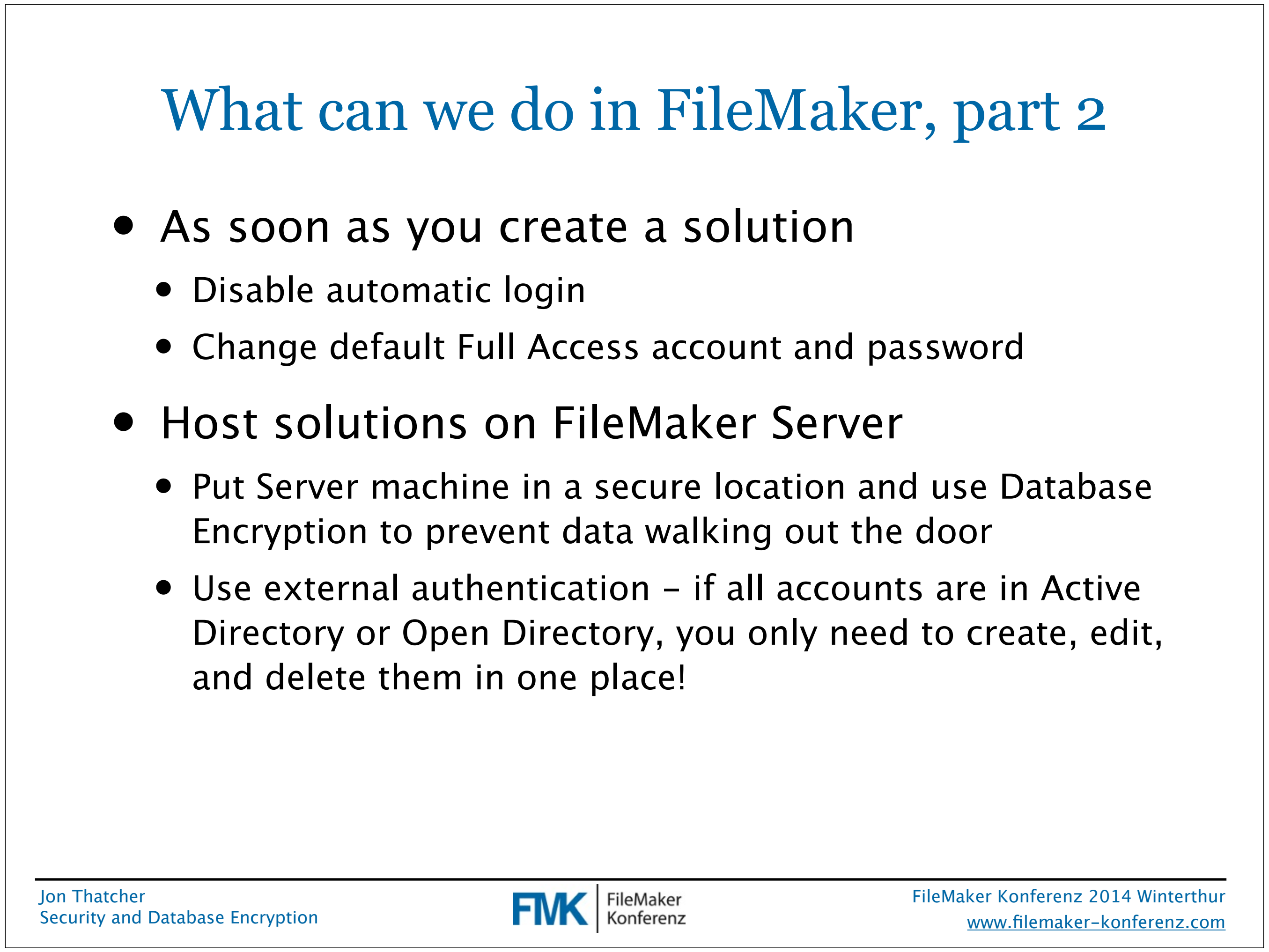
- 11698 incidents
  - 112 with confirmed data disclosure
  - Privilege abuse in 88% of cases
- Authorized or known people sometimes do bad things
- Most extreme case: Edward Snowden

Insider and Privilege Misuse: A story

“A customer of mine fired his secretary and before leaving she printed a list of all customers. Then she found a new job with a competitor and started calling them. My customer knew about this because one of his customers called him giving a heads up. Since then, in our users module, you can specify who can print and who can export data. My suggestion to all my customers is that if they plan to fire someone, first block all access privileges on the system before talking with the employee.”

What can we do in FileMaker?

- Know your data and who has access to it
  - Principle of least privilege: grant only the access a user needs to do their job and nothing more
- Use FileMaker's security, don't roll your own
- Don't rely on "security through obscurity"
  - Simply hiding fields from users doesn't secure them
  - Users with no access to a field won't even see it in field lists in Table View or the Export dialog



What can we do in FileMaker, part 2

- As soon as you create a solution
  - Disable automatic login
  - Change default Full Access account and password
- Host solutions on FileMaker Server
  - Put Server machine in a secure location and use Database Encryption to prevent data walking out the door
  - Use external authentication – if all accounts are in Active Directory or Open Directory, you only need to create, edit, and delete them in one place!

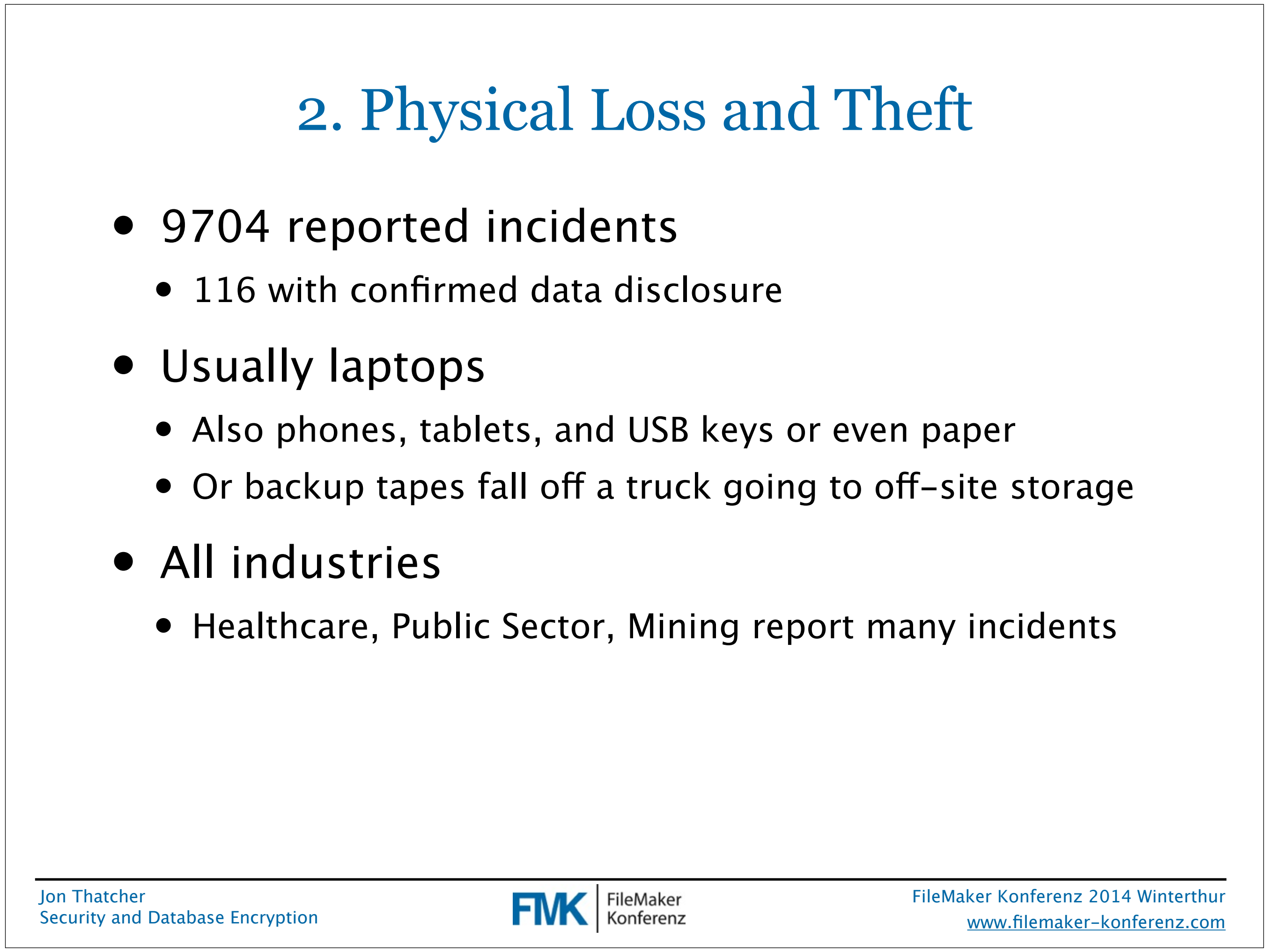
NOTE: Database Encryption is also known as Encryption At Rest (EAR)

What can we do in FileMaker, part 3

- Enable File Access Protection
  - Prevent users from connecting to your solution via a new or unauthorized FileMaker file
- Review user accounts / privileges regularly
  - Disable accounts as soon as an employee leaves
- Read the FileMaker Security Guide:
  - http://help.filemaker.com/app/answers/detail/a_id/13291

Tip: Audit access and publish results

- Publishing anonymized results of access audits is a strong deterrent to bad behavior
- Audit logs can have other benefits
  - Troubleshoot performance problems
  - Resolve disputes of who did or didn’t perform an action
  - Quickly identify access issues and problems with the solution or work process



2. Physical Loss and Theft

- 9704 reported incidents
  - 116 with confirmed data disclosure
- Usually laptops
  - Also phones, tablets, and USB keys or even paper
  - Or backup tapes fall off a truck going to off-site storage
- All industries
  - Healthcare, Public Sector, Mining report many incidents

TD Bank data breach affects 267,000 customers, including 73,000 in Massachusetts (reported in Oct. 2012)
http://www.boston.com/businessupdates/2012/10/12/bank-data-breach-affects-maine/1aVgFQdpoRkXmqxT6Q25AM/story.html
“The bank told customers that two tapes disappeared in transit while being shipped to one of its location in March. The company has not been able to find the tapes. The tapes were unencrypted and contained extensive customer information, including Social Security numbers and bank account numbers…”

What can we do?

- Minimize risk of data exposure when someone loses that laptop or device — it will happen
- Encrypt all data on computers, iOS devices, etc
  - Passcode or TouchID will encrypt the entire iOS device
- Automate and encrypt backups
- Keep portable devices with you
- Lock down or secure equipment / documents

3. Miscellaneous Errors

- 16554 reported incidents
  - 412 with confirmed data disclosure
- Usually documents
- Top industries
  - Public Sector, Administration, Education, Healthcare

Some Miscellaneous Errors

- "Off by one" errors in a mass mailing
  - Customer A gets customer B's documents
- Posting private data to a public location
- Mis-disposal
  - Paper that should have been shredded is not
  - Computers or other information media are disposed of without being erased

What Can We Do?

- Include IT when disposing of electronics
- Shred everything (including hard drives!)
- Spot check mass mailings
- Double check all publications
- Educate users

Secure the High Value Information

4. Point of Sale Intrusions
5. Web App Attacks
6. Card Skimmers

- Cost of data breach is high (US$188 per record)
- Median 6777 records * $188 = over $1 million

4. Point of Sale Intrusions

- 198 incidents
  - All with confirmed data disclosure
- Top industries
  - Retail, Accommodation and Food Service
- Most breaches and loss from small businesses
  - May not have robust security measures of larger business

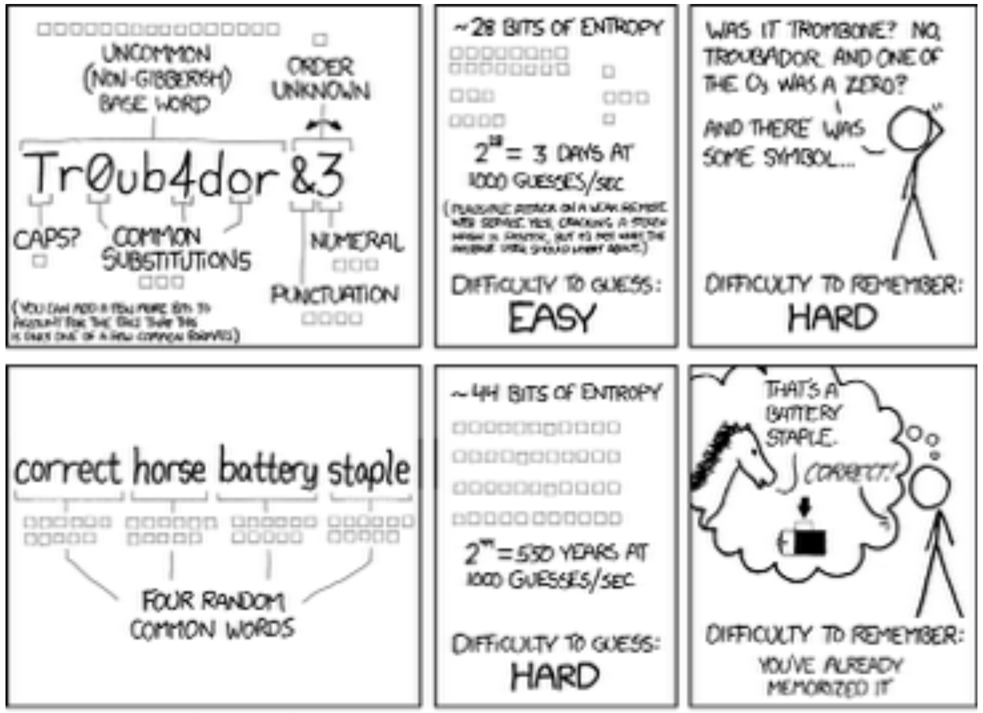
Point of Sale breach

- Hackers use a spear-phishing or watering hole attack to obtain network credentials
- Use credentials to attack internal server
- From server, traverse network, and install malware on POS terminals, collect data on compromised servers and exfiltrate it
  - http://krebsonsecurity.com/wp-content/uploads/2014/01/Inside-a-Targeted-Point-of-Sale-Data-Breach.pdf

What Can We Do?

- Restrict Remote Access to POS systems
  - https://www.us-cert.gov/sites/default/files/publications/BackoffPointOfSaleMalware.pdf
- Enforce strong, non-default passwords
- Isolate POS systems
  - Only POS activities on these systems: no email, no Web
- Deploy Anti-Virus

Password strength: http://xkcd.com/936/


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
~28 BITS OF ENTROPY
2^{28} = 3 DAYS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^{44} = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Follow PCI-DSS

- Payment Card Industry Data Security Standards
- Applies to all entities that store, process or transmit cardholder data
- Standard has 12 specific requirements with many sub-requirements
    - https://www.pcisecuritystandards.org

PCI-DSS Penalties

- Strictness of standards and size of penalties depends on number of transactions processed by the entity as a whole
  - Not just transactions done by your department
- Payment brand fines bank => fines merchant
  - $5,000 to $500,000 per incident
  - $50 to $90 fine per cardholder data compromised
- Plus indirect costs (audits, mailing, staff time)

PCI DSS in Practice

- Use tokenization
  - Avoid storing card data directly
- Use FileMaker 13 Database Encryption
  - Securely store the high value data
- Path to compliance
  - Learn: Getting Started with PCI DSS Compliance
  - Build solutions that meet requirements
  - Deploy in an environment that meets requirements

PCI DSS Resources

- Talk to bank or manager of merchant accounts
  - Review their materials and follow their guidelines
- https://www.pcicomplianceguide.org/
- http://solutions.filemaker.com/made-for-filemaker/search.jsp?search=credit+card

5. Web App Attacks

- 3937 total incidents
  - 490 with confirmed data disclosure
- Ideological and financial motives
  - 2/3 ideological: deface site or compromise to attack users
  - 1/3 financial: similar to attacks on POS systems
- Top industries
  - Information, Utilities, Manufacturing, Retail

The Web Is an Attack Vector

- Symantec Internet Security Threat scan:
  - 78% of legitimate websites have at least one vulnerability
  - 16% of legitimate websites have a Critical vulnerability
- Critical vulnerability could allow attackers to
  - Access sensitive data
  - Alter the website’s content
  - Compromise visitors’ computers

What Can We Do?

- Secure your web applications
  - Use multi-factor authentication or use authentication API
- Validate inputs
  - Reduce risk of SQL injection or “Shellshock” attacks
- Patch content management systems
- Monitor outbound connections
  - How much data is going out and where to?

6. Payment Card Skimmers

- 130 reported incidents, always disclosed data
- Top industries: Finance, Retail
- Chip and PIN cards in Europe help, but…
  - Skimmers can include camera to capture the PIN
  - http://krebsonsecurity.com/category/all-about-skimmers/

Prevent Other Crime

7. Crimeware

8. Cyber Espionage

9. Denial of Service Attacks

7. Crimeware

- 12535 incidents
  - 50 with confirmed data disclosure
- Malware to gain control of systems
  - Also targets Android and Blackberry
- Top industries
  - Public Sector, Information, Utilities, Manufacturing

Types of Crimeware

- In most incidents, malware infects computers to put them into a “bot” network aka bot-net
  - Used to steal credentials (banking)
  - Take over computer for DDoS or spamming attacks
  - Hijack a browser to boost ad revenue
- Ransomware up 500% in 2013
  - One tool got $27 million in ransom in 2 months

What Can We Do?

- Keep browsers up to date
- Disable Java in the browser
- Use two-factor authentication
- Check links before clicking
  - Don’t trust shortened links
- Maintain a strong user education campaign

8. Cyber Espionage

- 511 incidents
  - 306 with confirmed data disclosure
- Top Industries
  - Public Sector, Professional Services, Manufacturing
- Targets: trade secrets, intellectual property, etc
  - http://www.businessweek.com/articles/2014-07-17/how-russian-hackers-stole-the-nasdaq

What Can We Do?

- Patch all the things (servers, browsers, plugins)
- Use anti-virus and keep it up to date
- Train users
  - Not a lost cause!
  - Breaches are detected by users more often than technology
- Keep good logs
  - Greatly beneficial during incident response

9. Denial of Service Attacks

- 1187 incidents
- Top industries
  - Finance, Retail, Professional Services
  - Information, Public Sector
- Attackers shifting from bots on home computers to cloud servers
  - Makes your servers a more tempting target to take over

What Can We Do?

- Patch servers and disable unnecessary services
- Segregate key servers
  - Use second IP address range so attack on main Web server doesn't take down the rest of your operation
- Have a plan
  - If you have an anti-DDoS service, test it
  - Know what to do in the event of an attack

Nine Incident Patterns - Covered!

People and Things

1. Insider and Privilege Misuse
2. Physical Loss and Theft
3. Miscellaneous Errors

High Value Information

4. Point of Sale Intrusions
5. Web App Attacks
6. Card Skimmers

Other Crime

7. Crimeware
8. Cyber Espionage
9. Denial of Service Attacks

Security Policy and Training Resources

http://www.stopthinkconnect.org

http://www.staysafeonline.org/business-safe-online/

http://www.sans.org/security-resources/policies/

http://www.csoonline.com/article/2123889/identity-access/security-tools-templates-policies.html

http://www.securingthehuman.org/enduser/

One more risk...

- XP and other out of date operating systems
  - About 24% of computers are still running Windows XP
    - http://www.netmarketshare.com/
  - Microsoft no longer patching XP or Office 2003
  - Vendors no longer patching their XP software
  - Hackers can try exploits revealed by Windows 7 and 8 patches against XP
- XP came out in 2001, it's past time to upgrade!

What’s in this session

- Security: the Threat Landscape and FileMaker
  - Or “Why you need FileMaker 13 Database Encryption”
- Database Encryption – Under the Hood
  - Why, What and How

Database Encryption

- Why do we need it?
- What does it do?
- How does it work (under the hood)?
- How does it perform?

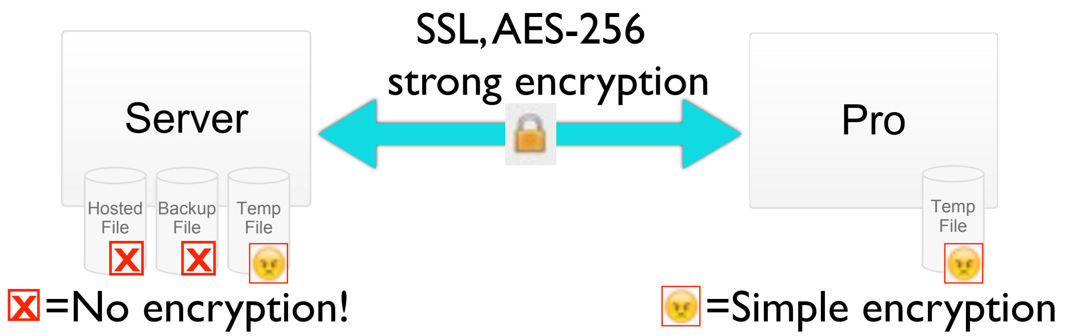
Before FM 13 Database Encryption

- FM Server has done encryption “over the wire” for years
  - Uses SSL to encrypt network traffic between Server and client
- For highest security, Server needs a “custom” certificate from a trusted Certificate Authority
  - Matching Server name to custom certificate prevents Man In The Middle attacks

Before FM 13 Database Encryption

- SSL only protects the data while in transit over the network
  - Hosted database file is unencrypted
  - Any backups made by Server are unencrypted
  - Temporary file uses simple encryption, relatively insecure

Without Database Encryption



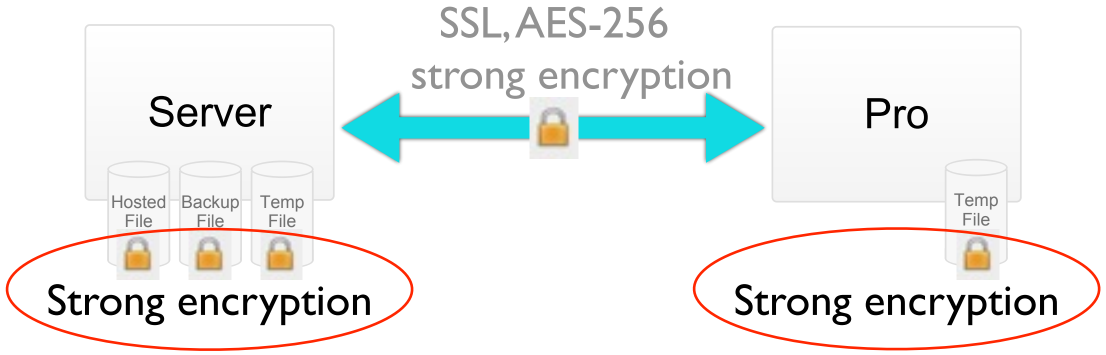
Database Encryption - What does it do?

- Encrypting the database rewrites the entire file using AES-256
  - Every 4KB block is encrypted using AES-256 (aka Rijndael) for very strong security
  - FYI: also known as Encryption at Rest
- Opening the database requires entering the encryption password
  - Once file open, each 4KB block is decrypted only when read from disk into FileMaker RAM cache

Database Encryption - What does it do?

- Also encrypts:
  - All Server backups of encrypted database
  - Temporary files for encrypted database on both client and Server
- NOTE: always secure network communications with SSL when using Database Encryption!

With Database Encryption



SSL, AES-256
strong encryption

Server

Hosted File
Backup File
Temp File

Strong encryption

Pro

Temp File

Strong encryption

I didn’t highlight SSL here, because it is separate from Database Encryption
BUT… if you encrypt your databases, you should ABSOLUTELY enable SSL too!

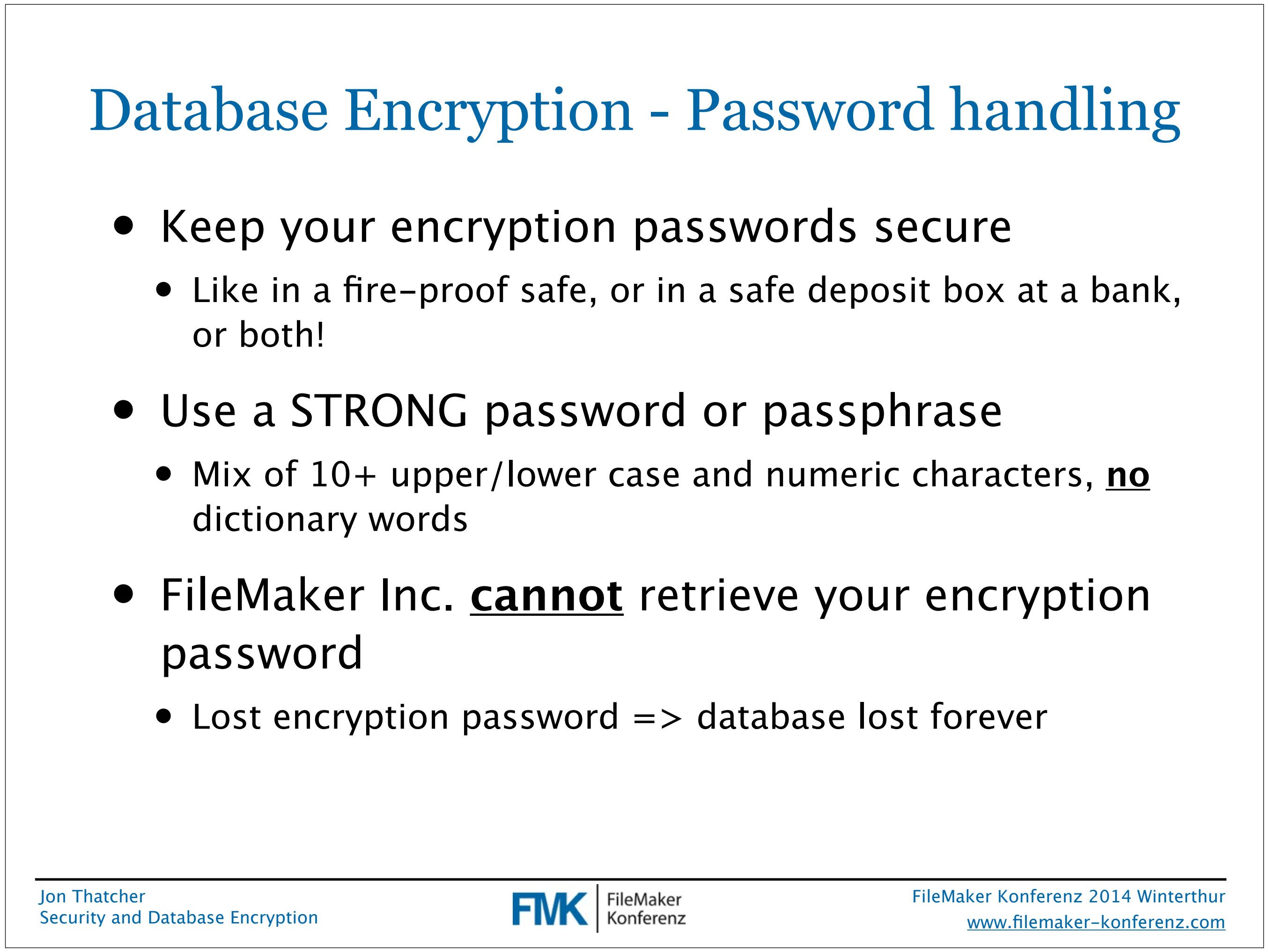
Database Encryption - How it Works

- Password handling
- Algorithm use
- Everything else you need to know

Database Encryption - Password handling

- Encryption password is **NOT** stored in the database file
    - Only the hint and the Shared ID are stored
- Encryption password must be given to open the database locally or as host, **not** as client
- Server has optional secure keystore for encryption passwords

NOTE: Encryption password is NOT needed to open database over the network as a client; the host has already done the open that requires encryption/decryption



Database Encryption - Password handling

- Keep your encryption passwords secure
  - Like in a fire-proof safe, or in a safe deposit box at a bank, or both!
- Use a STRONG password or passphrase
  - Mix of 10+ upper/lower case and numeric characters, **no** dictionary words
- FileMaker Inc. **cannot** retrieve your encryption password
  - Lost encryption password => database lost forever

Though you could ask the NSA if they have saved your password ;-)

Database Encryption - Server keystore

- Keystore can’t be used or decrypted elsewhere
  - Encrypted with machine/user-specific data by FM Server
- Server Admin decides whether to store password per database
  - Can only be stored at open, when password specified
  - Server Admin can clear one or all stored passwords from keystore at any time

Database Encryption - Keystore, part 2

- Keystore only read when Server opens encrypted database
- Totally optional: simply avoids the Admin having to enter the encryption password on every open of the database

Database Encryption - Algorithm use

- Each 4K block is encrypted with AES-256
  - Decrypted by Draco engine when read from disk into RAM
  - Re-encrypted by Draco when written from RAM to disk
- Each block includes some extra random data
  - Encryption starts with different random data **every** time a block is written
  - Result: no way to tell what is actual encrypted data versus random junk

Encryption - without random data

```
Highly confidential data
Name Bill Epling
Salary 40 peanuts
000000000000000000000000
```

▶

```
rGgHn8hRp8xQ5Iqnh6yF8/
WtyNrXDFZFEv41VTF7zmzUCJBctW+Vl/
Z5RyOmb5D4Mi6KIxSxOsCF3BscCrkaLomOHHKie
tkdvzogaN5TblAyuSQlOgW2TTbn0p966Q6H
```

```
Highly confidential data
Name Bill Epling
Salary 42 peanuts
000000000000000000000000
```

▶

```
rGgHn8hRp8xQ5Iqnh6yF8/
WtyNrXDFZFEv41VTF7zmxCfKb/
NYtq50TyLBwRchYAIETSPcCeWsEI1610f4imDPP
NZw3y+EVBHtIkbfmNE12NIO82Kpoi9EkgH/
165LBY
```

Database Encryption - with random data

```
Highly confidential data
Name Bill Epling
Salary 40 peanuts
000000000000000000000000
```

▶

utaFh8+P2m34enxErjY947Se6t3eg3zyMOlHQJ0e/
YhBD5XKsRlsZTTNFpGHlZALDbcAgOfWeocXaq12SS
X+de8MySgxRvoj6Oq+NedNQ/LCDHaBYLLaSuM5A2X
+aVS/h7DlLilFbLFJrCYPX/Dcq9kCsnv4zeFY

```
Highly confidential data
Name Bill Epling
Salary 42 peanuts
000000000000000000000000
```

▶

xAnIsN3zrBlnUCxsE2flIz8aJzY9d9zjH5p8SN9/
D2aOni+gs82D669XD+WdFaLeP4X7En32mukh2T
+jxfUWRhmgCmtXD9aYqHXYz/aZiXgam
+X21eFDRCEid
+9JXFzPzqDAOegeUk5TZnwphDCPpP2rd53BQiOq

Database Encryption - Algorithm “salt”

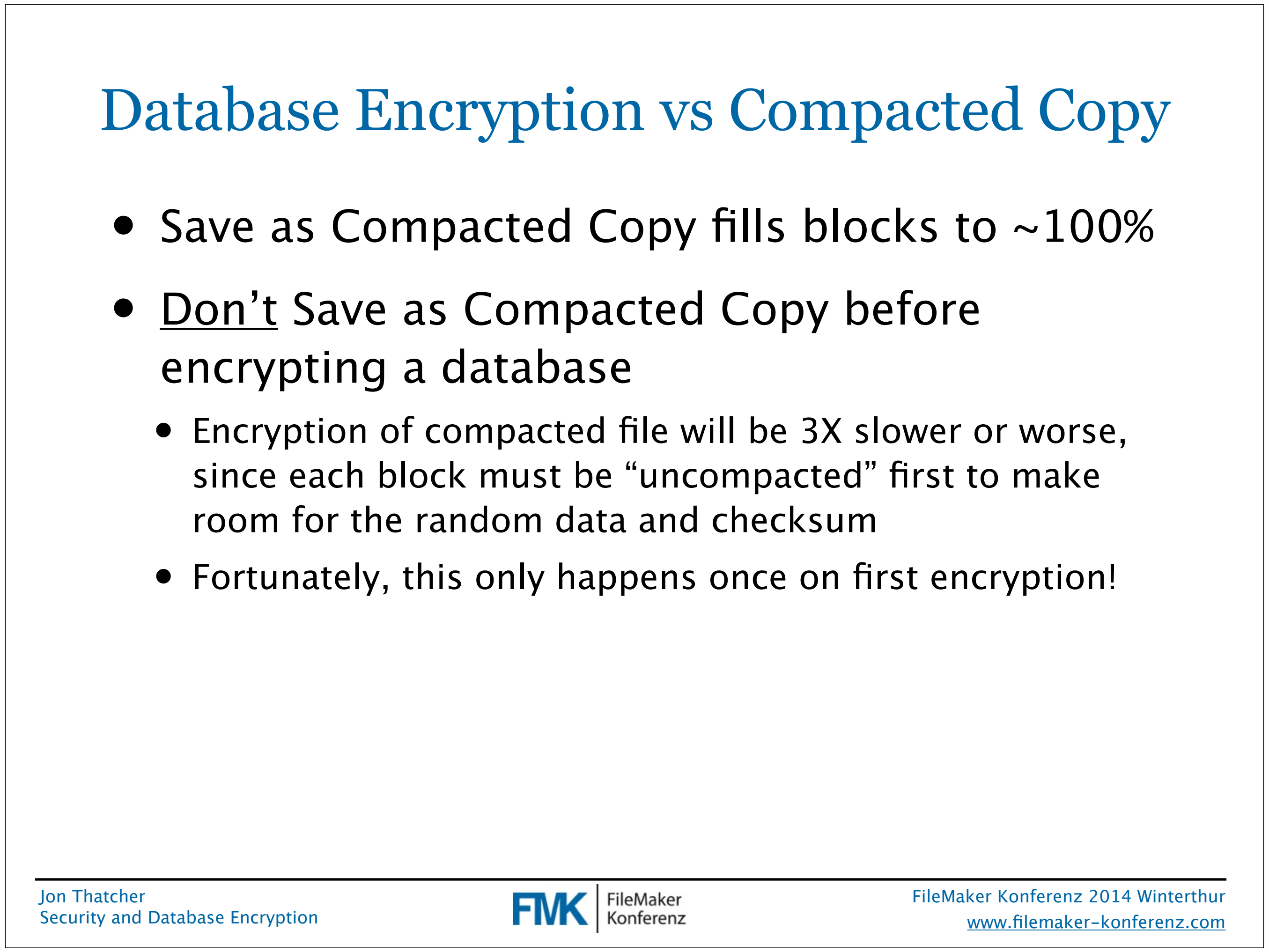
- Every database has a different “salt”
  - Prevents an attacker’s use of rainbow tables (precomputed hashes) to guess password
  - Result: blocks from database A can’t be inserted into database B, since salt is unique
- Password and salt are hashed into encryption key, which takes a lot of computation
  - Result: brute force attack impossible, because every password guess is expensive and long

Database Encryption - Block checksum

- Every block has an encrypted checksum for authenticating data
  - Checksum verified when block is decrypted; mismatch means File Damaged
  - Result: Prevents any change of data within a block from being accepted by FileMaker

Database Encryption - Space needed?

- Where does the space come from to store random data and checksum in each block?
  - Draco engine tries to keep each 4KB block 50-75% full
  - Normally there is free space to add random data and checksum to each block during encryption
- What about Save as Compacted Copy?

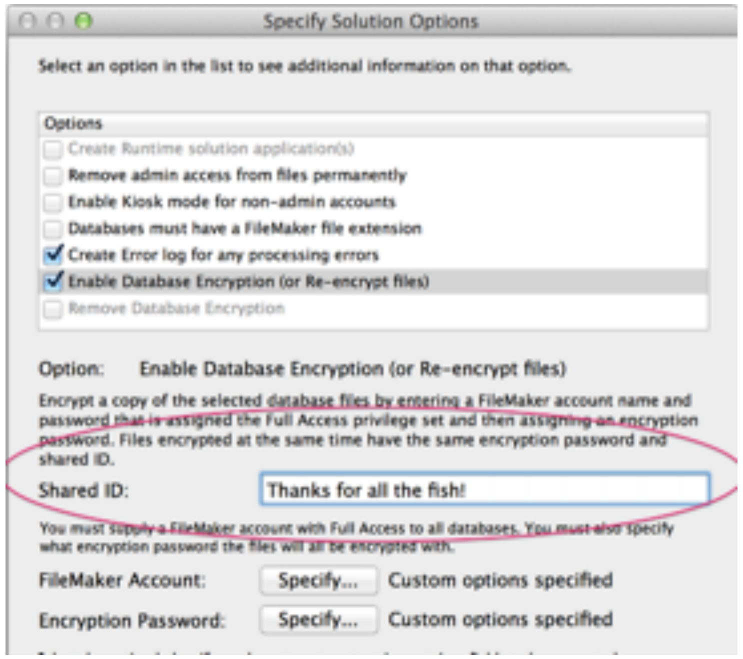


Database Encryption vs Compacted Copy

- Save as Compacted Copy fills blocks to ~100%
- Don’t Save as Compacted Copy before encrypting a database
  - Encryption of compacted file will be 3X slower or worse, since each block must be “uncompacted” first to make room for the random data and checksum
  - Fortunately, this only happens once on first encryption!

This only slows down the initial encryption of database using Developer Tools

Shared ID...



Specify Solution Options

Select an option in the list to see additional information on that option.

Options

- □ Create Runtime solution application(s)
- □ Remove admin access from files permanently
- □ Enable Kiosk mode for non-admin accounts
- □ Databases must have a FileMaker file extension
- ☑ Create Error log for any processing errors
- ☑ Enable Database Encryption (or Re-encrypt files)
- □ Remove Database Encryption

Option: Enable Database Encryption (or Re-encrypt files)

Encrypt a copy of the selected database files by entering a FileMaker account name and password that is assigned the Full Access privilege set and then assigning an encryption password. Files encrypted at the same time have the same encryption password and shared ID.

Shared ID: Thanks for all the fish!

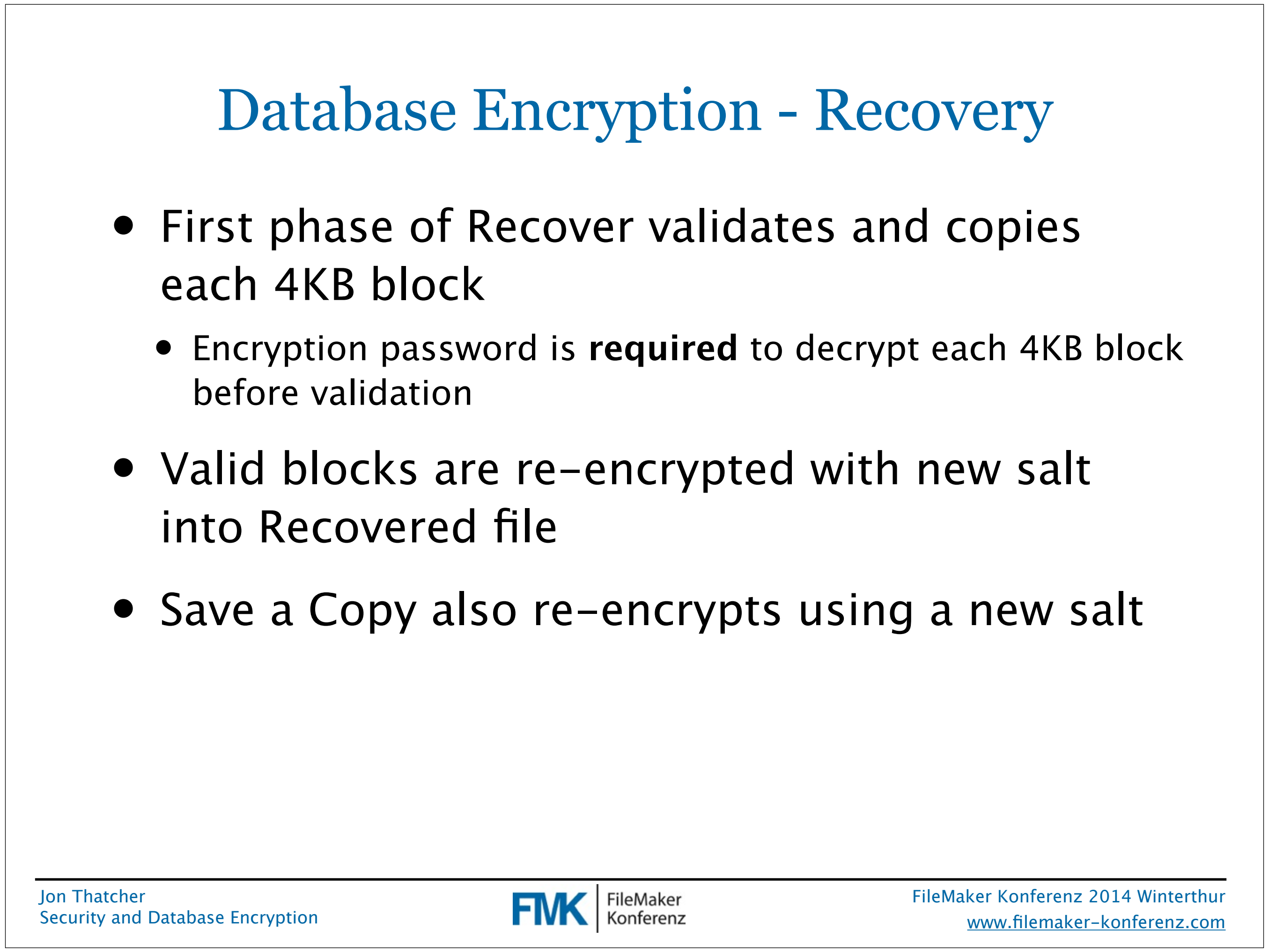
You must supply a FileMaker account with Full Access to all databases. You must also specify what encryption password the files will all be encrypted with.

FileMaker Account: Specify... Custom options specified

Encryption Password: Specify... Custom options specified

Database Encryption - Shared ID, etc.

- Shared ID logically groups files with same encryption password
  - Allows just one encryption password to be entered when opening first file of a multi-file solution
  - Remember the Shared ID so you can re-use it when adding a new file to a solution
  - Does NOT require that files use the same password, just tells FileMaker to try parent file encryption password first
- Note: encrypted databases openable in FileMaker 13 and later only



Database Encryption - Recovery

- First phase of Recover validates and copies each 4KB block
  - Encryption password is **required** to decrypt each 4KB block before validation
- Valid blocks are re-encrypted with new salt into Recovered file
- Save a Copy also re-encrypts using a new salt

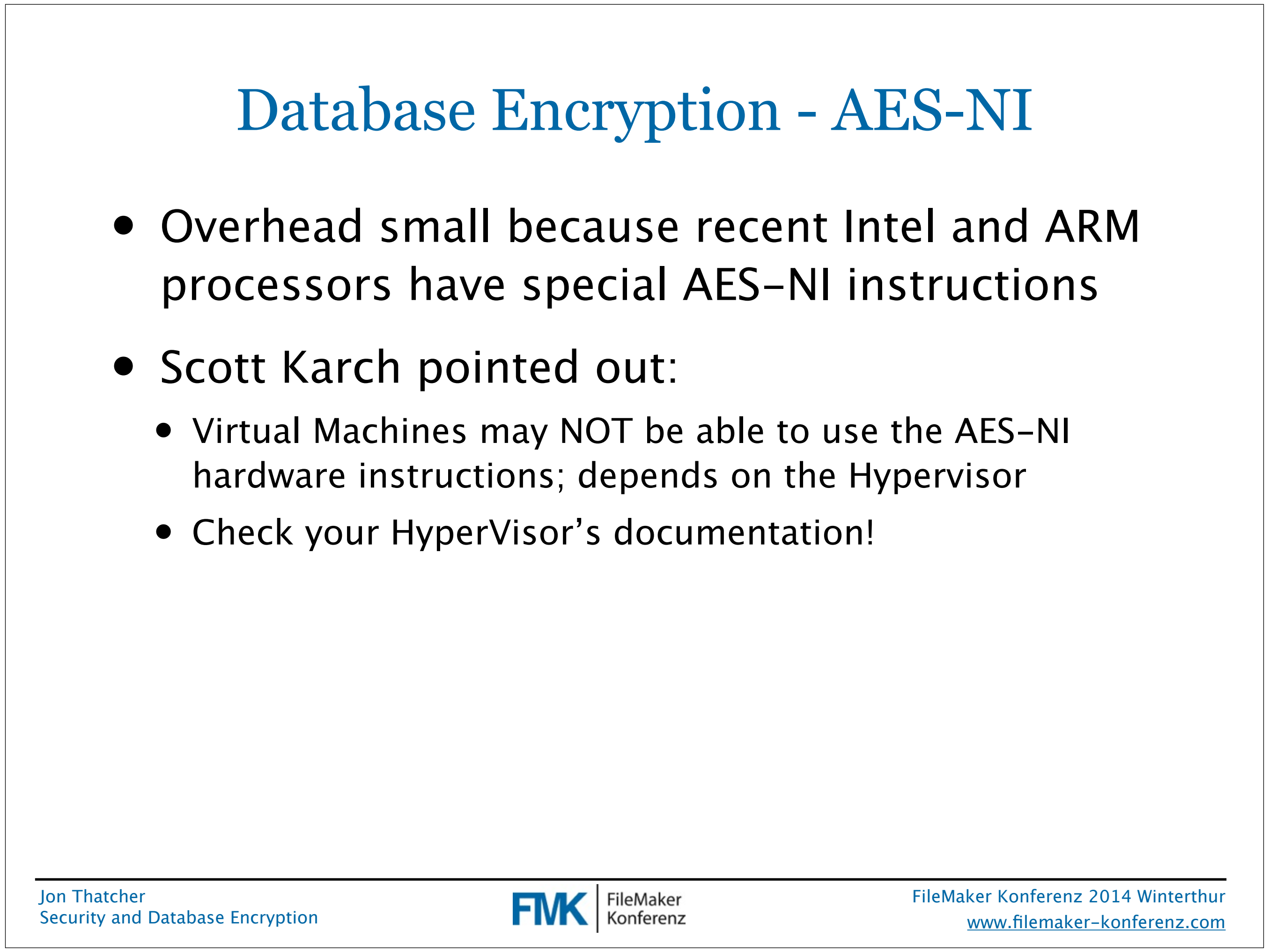
So Save a Copy is a “logical” copy of the file
But: Server Backup is a block-for-block copy of the original file

Database Encryption - Backups

- No AES overhead for scheduled or command line backups
    - These backups make an exact block-for-block copy of file
    - So no decryption/encryption needed
- Progressive backup does have extra overhead for encrypted DB
    - “Redo” log must contain full 4KB encrypted block for each change
    - Versus 100-2000 bytes per change in unencrypted DB

Database Encryption - Performance

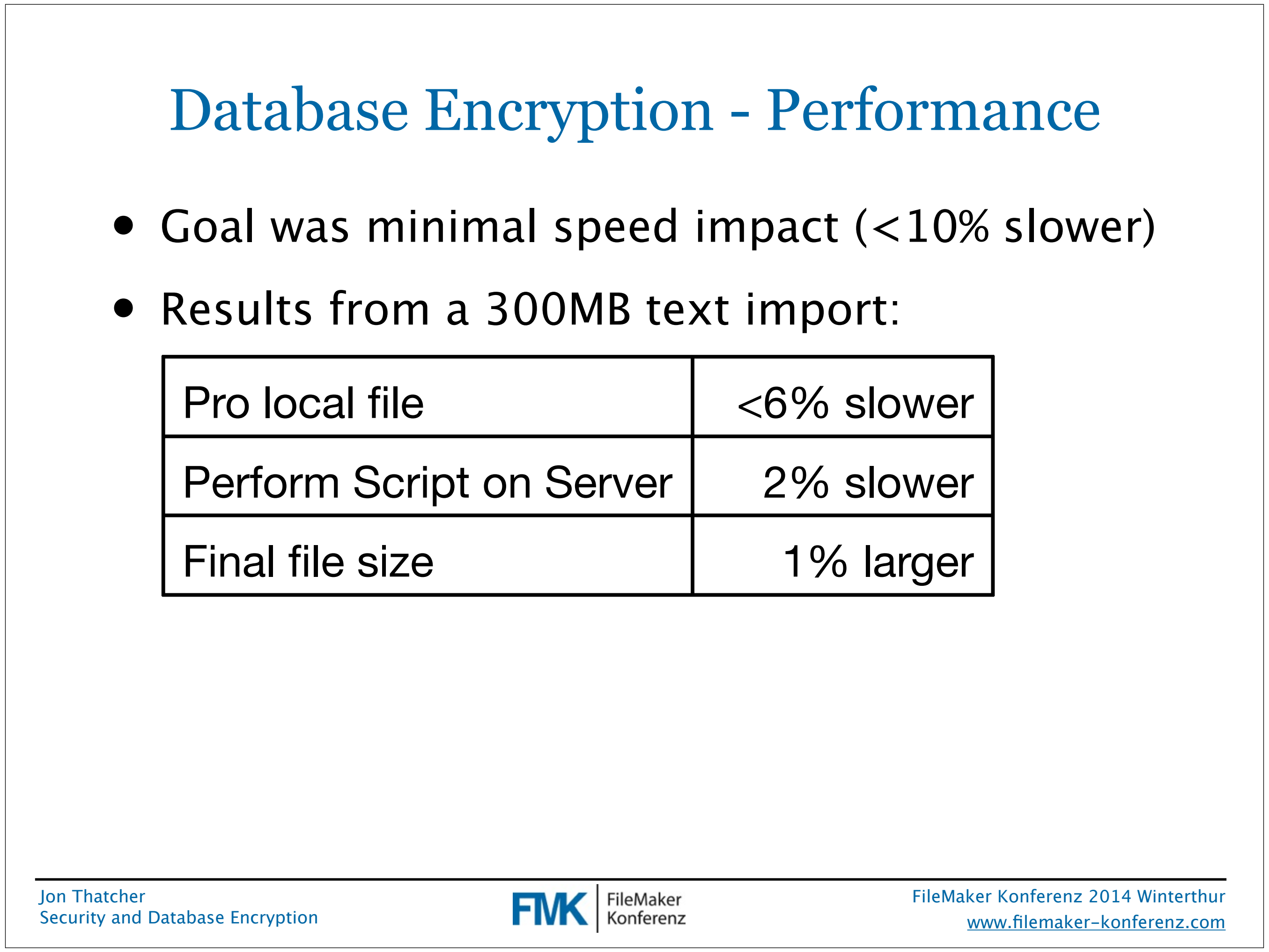
- Overhead from AES on every disk read / write
  - Write 4K block: Database RAM cache > Encryption > File
  - Read 4K block: File > Decryption > Database RAM cache
- SSL encryption between Server and client has small overhead (<5%)
  - Every packet must be encrypted by sender and decrypted by receiver



Database Encryption - AES-NI

- Overhead small because recent Intel and ARM processors have special AES-NI instructions
- Scott Karch pointed out:
  - Virtual Machines may NOT be able to use the AES-NI hardware instructions; depends on the Hypervisor
  - Check your HyperVisor’s documentation!

NOTE: Scott Karch, virtualization expert, pointed out to me after the session that Virtual Machines may NOT be able to use the AES-NI hardware instructions; that depends on the Hypervisor being used, so check your HyperVisor’s documentation!



Database Encryption - Performance

- Goal was minimal speed impact (<10% slower)
- Results from a 300MB text import:

Pro local file	<6% slower
Perform Script on Server	2% slower
Final file size	1% larger

Pro local case was about 5 and 1/2 % slower

Database Encryption - Standards, Review

- Using National Institute of Standards and Technology (NIST) standards
  - For decryption/encryption
  - Key generation
  - Hashing
- Reviewed by Apple Information Security team
  - Improvements made in randomization and checksum generation / checking

What’s in this session

- Security: the Threat Landscape and FileMaker
  - Or “Why you need FileMaker 13 Database Encryption”
- Database Encryption – Under the Hood
  - Why, What and How
- Forbes.com: How To Talk To Your Employees About Cybersecurity (Without Putting Them To Sleep)

Summing it all up

- Inform yourself and your users on security best practices and implement them!
- Use the tools that FileMaker 13 provides you
  - FileMaker security model
  - External authentication
  - Secure network connections
  - Database encryption

Q & A

Vielen Dank unseren Sponsoren

Danke für das Bewerten dieses Vortrages!