

security center *of excellence*

Forensics Challenges

Windows Encrypted Content

John Howie CISA CISM CISSP

Director, Security Community, Microsoft Corporation

Introduction

- Encrypted content is a challenge for investigators
 - Makes it difficult to obtain evidence
 - Cost of data recovery when encryption is involved very high
 - Often precludes use in non-investigative scenarios
- Understanding how Microsoft implements encryption can
 - Enable investigators to identify the owner of encrypted data
 - Can request access to protected content
 - Lead investigators to recovery keys
 - Can be used to access content without owner's permissions
- Contrary to belief there is no encryption backdoors
 - Even for Microsoft itself or for governments

Overview

- Overview of Windows Encryption
- The Encrypting File System
- Rights Management Services
- S/MIME and Exchange
- The Future: BitLocker
- Planning for Future Investigations

Overview of Windows Encryption

Windows Encryption

- Microsoft has built encryption into several products
 - Examples include:
 - Encrypting File System (EFS)
 - Rights Management Services (RMS)
 - S/MIME in Outlook
- Encryption is not centralized
 - Found in user DLLs, applications, and the kernel
 - Will be centralized in Vista and Longhorn Server
- Designed to be secure
 - Keys are strongly protected

Encryption Algorithms

- Most technologies use Cryptographic Service Providers
 - Algorithms and Key Lengths supported vary by CSP
 - Microsoft ships several CSPs
 - Third party CSPs are available
- While there are many algorithms, few used in products
 - Strong trend away from DES, 3DES, RC4, etc
 - Customers asking for stronger algorithms
 - High demand for pluggable-crypto
 - Customers want to control which algorithms are used, and when

Key Storage

- Keys are created by applications and the OS as needed
 - Keys are not kept in memory and are securely deleted
 - Difficult given compiler optimization
- Keys are usually stored in users' profiles
 - Profile is created when user first logs on
 - Keys protected by DPAPI

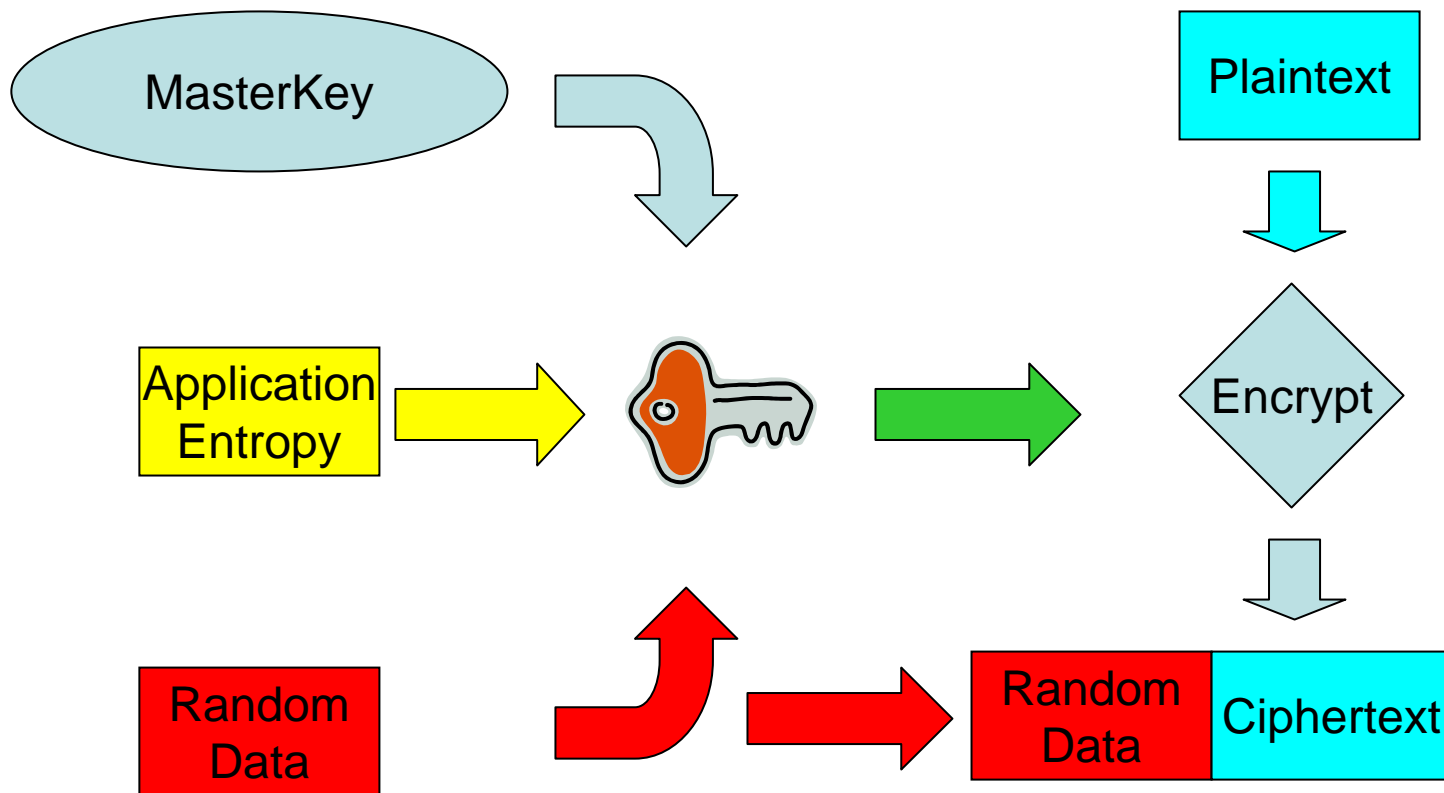
Key Storage and Roaming Users

- Users who logon to many systems have profiles on each
 - Required keys must be in profile before it can be used
 - May prevent user getting access to data or creating signatures if key is in profile on one system while user is logged on to another
- Two solutions for users who use multiple systems
 - Roaming profiles
 - Copy of profile stored on server and downloaded when user logs on and uploaded when user logs off
 - Available in Windows 2000 and later
 - DIMS
 - Keys are securely downloaded to client from server
 - Windows 2003 SP1 support only

Data Protection API (DPAPI)

- Introduced in Windows 2000
 - Part of the CryptoAPI
- DPAPI creates a **MasterKey**
- The MasterKey is not used to encrypt keys directly
 - MasterKey combined with random data
 - Additional entropy can be provided by applications
 - Random data stored with encrypted data

DPAPI in Action



The MasterKey

- Protected by user's password
 - PKCS #5 generates key from user's password
 - Triple-DES used to encrypt MasterKey
 - Encrypted MasterKey stored in user profile
- When the user password is changed
 - MasterKey decrypted with old password
 - MasterKey encrypted with new password
 - Old password recorded just in case...

The MasterKey (continued)

- Changes every three months
 - Old MasterKeys kept to access older content
- MasterKey is backed up automatically
 - DPAPI uses Domain Controller's public key
 - Encrypted key stored with password protected key
 - Can be sent to Domain Controller to be decrypted
- It is not safe to reset the user's password to access their encrypted content
 - Windows designed to defeat this style of administrator attack

The MasterKey in Workgroups

- Resetting a password locks out MasterKey
 - All protected data is lost, including keys
- Users can create a Password Reset Disk
 - Public-private key pair is created
 - Public key is used to encrypt user password
 - Encrypted password stored in SAM
 - Private key written to PRD
- Look for a Password Reset Disk during investigations!

The Encrypting File System (EFS)

Introduction to EFS

- Introduced in Windows 2000
 - Updated in Windows XP and Windows Server 2003
 - Uses a different, stronger algorithm and key length
- Implemented as a file system filter driver
 - Layered on top of NTFS
- Certificate-based technology
 - EFS can issue its own certificates
 - Leverages Enterprise Root CA if available

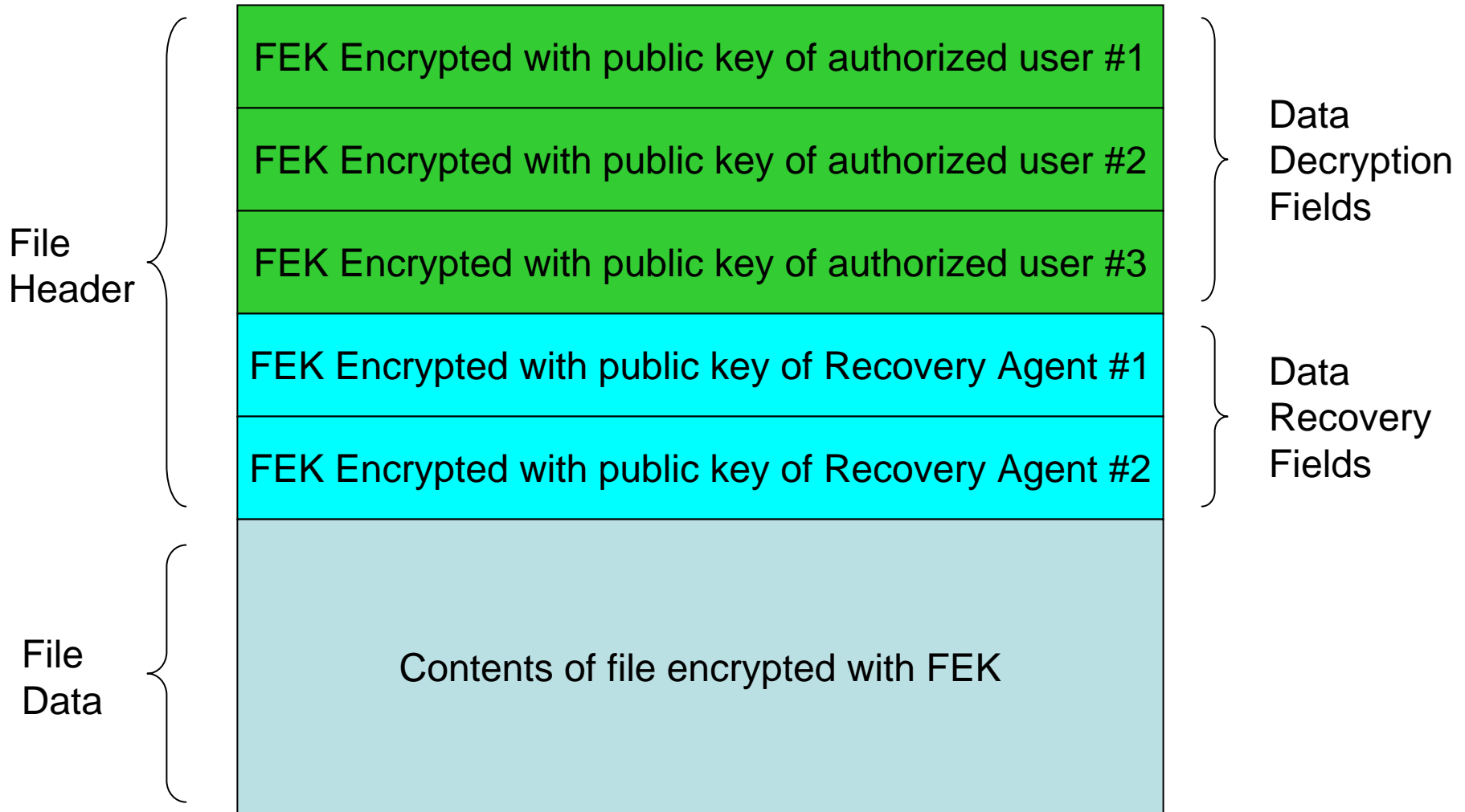
How EFS Works

1. Users obtain EFS Certificates
2. Random File Encryption Key (FEK) is generated
3. File contents are encrypted with FEK and stored in secure temporary file

How EFS Works (continued)

4. FEK is encrypted with public key from each authorized user's EFS Certificate
5. FEK is encrypted with public key from each EFS Recovery Agent Certificate
6. Encrypted FEKs and encrypted content is written to file

How EFS Works (continued)



Recovery Agents

- EFS provides for recovery if user loses private key
 - Designated user accounts become Recovery Agents
- Recovery Agents decrypt content on systems where their private key is stored
 - May be different system from that on which content was created

Recovery Agents (continued)

- Windows 2000
 - Administrator is a Recovery Agent:
 - In workgroup environments
 - Where no Enterprise Root CA exists
- Windows XP, 2003
 - No default Recovery Agent

Recovery Agents Certificates

- Where an Enterprise Root CA exists:
 - Recovery Agents request an EFS Recovery Agent certificate
 - EFS Recovery Agent certificates distributed to workstations by Group Policy
 - EFS automatically encrypts FEK with public key in EFS Recovery Agent Certificates

Accessing EFS Content

- Easiest option is to logon with user's account to access content
 - Must logon to system where private key is stored
 - Requires you to know user's password
 - PRD can be used for workgroup users
 - RAINBOW tables can be used if hash is known

Using Recovery Agents

- Recovery Agent account can be used
 - Content may need to be moved to system where Recovery Agent's private key is stored
 - NTBACKUP.EXE can be used
- Recovery Agents cannot be added retroactively
 - FEK is encrypted with new Recovery Agents when file is next opened

Rights Management Services (RMS)

Introduction to RMS

- Client-Server Technology
 - Based on XrML 1.2 Standard (www.xrml.org)
 - RMS Server runs on Windows 2003 Server
 - Clients can be Windows 98 SE and later
- Applications must be RMS-aware
 - The Microsoft Office System (Office 2003)
 - Rights Management Add-on (RMA) for IE
 - ISV-supplied applications

How RMS Works

- All users identified by Rights Management Account Certificates (RACs)
- Symmetric key created to encrypt content
- Publish License created with users and rights defined by author, and symmetric key encrypted by public key of License Server

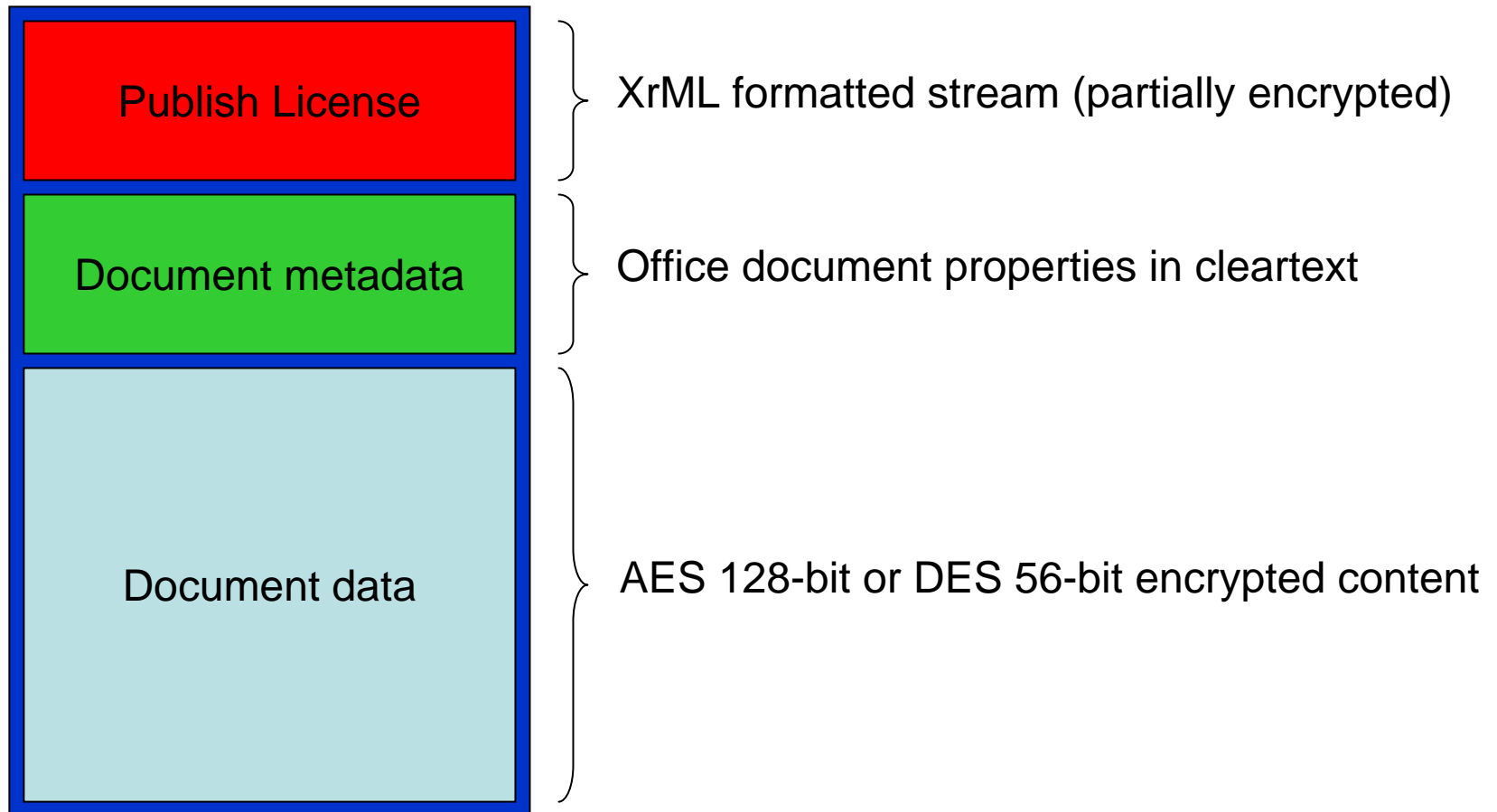
How RMS Works (continued)

- Recipient presents Publish License and RAC to License Server
 - URL of RMS License Server in license
- License Server decrypts key in Publish License with its private key

How RMS Works (continued)

- RMS Server binds symmetric key encrypted with user's public key and rights into Use License
- Application takes Use License, decrypts encrypted content with user's private key, and enforces rights
 - Only trusted applications may use RMS

Protected Office Document



Recovering RMS Content

- User account grants access to content
 - Opening content gets Use License
 - RAC obtained if not present on workstation
- Members of superusers group can access any content protected by License Server
 - Set group using RMS management interface
 - Manage group membership using AD tools

RMS Forensic Considerations

- Each application defines own file format
 - RMS data is in standardized format (XrML)
 - Need original content authoring application
- Office applications store Use Licenses in documents if user has write access
 - Has implications for chain of custody

S/MIME and Exchange

How S/MIME Works

- Sender creates email message
- Random symmetric key generated and message is encrypted
- Symmetric key encrypted with public key from recipient's X.509v3 certificate

How S/MIME Works (continued)

- Encrypted key and encrypted content sent to recipient
- Recipient decrypts encrypted symmetric key with their private key
- Message decrypted with symmetric key

X.509v3 Certificates

- Certificates can be issued by:
 - Microsoft Certificate Services
 - Enterprise CA integrated with domain
 - Standalone CA
 - Independent Certification Authority
- Certificate and private key required to access S/MIME protected email
 - Private key protected by DPAPI

Forensic Considerations

- Unlike EFS and RMS, application entropy often used to secure access to X.509v3 S/MIME certificate private key
 - Usually in the form of a PIN entered by user
 - Resetting password and using PRD won't help

Recovering S/MIME Email

- First try resetting user password
 - If domain user or PRD available
- Check for presence of key escrow system
 - Exchange 2000 with Key Management Service
 - Windows Server 2003 Enterprise Edition Certificate Services

The Future: BitLocker

BitLocker Volume Encryption

- Formerly called Full Volume Encryption (FVE)
 - Will be introduced in Vista
- Works by encrypting entire disk volumes
 - Not just folders and files like EFS
- BitLocker systems require at least two volumes
 - System volume (from which the OS boots) is not encrypted
 - Contains some of the OS start-up files that understand BitLocker
 - BitLocker-protected volumes

BitLocker Volume Encryption (continued)

- BitLocker encryption keys stored on System volume
 - Keys are encrypted
- When Vista boots BitLocker keys are decrypted using encryption key stored on
 - Trusted Platform Module (TPM) v1.2 security chip
 - USB key drive inserted into machine at boot time
- Recovery Agent functionality will be available for
 - Broken laptop where hard disk is inserted into new laptop
 - Lost USB key drive

Planning for Future Investigations

Workstations and Users

- Make each workstation and user a member of a domain
 - Allows DPAPI MasterKey recovery
- Restrict user access to a single workstation or use roaming profiles
 - Know where private keys are held
 - DIMS not viable yet

The Encrypting File System

- In a domain environment
 - Create EFS Recovery Agent accounts
 - Requires Enterprise CA
 - Backup the private keys
- In a workgroup environment
 - Create EFS Recovery Agent account for Windows XP systems
 - Backup the private keys

S/MIME

- If running Exchange 2000
 - Deploy Certificate Services and Exchange Key Management Service
- If running Windows Server 2003
 - Enable Certificate Services Enterprise Edition key archival and recovery functionality

Thank You!

For more information, and to contact me:

jhowie@microsoft.com

Questions and Answers