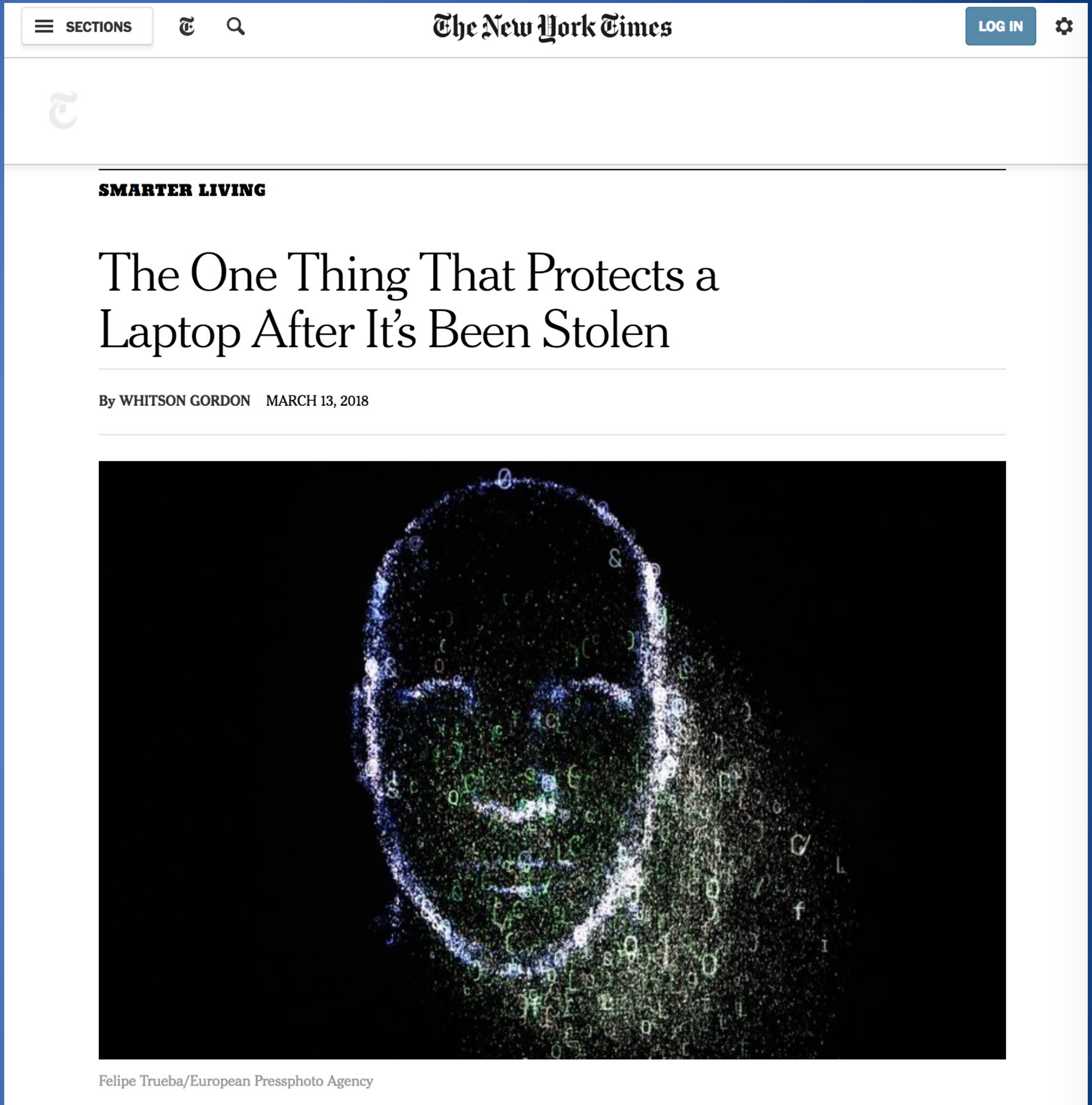
Storage Encryption

CS 1660: Introduction to Computer Systems Security

New York Times 3/13/2018

https://www.nytimes.com/2018/03/13/smarter-living/how-to-encrypt-your-computers-data.html



SMARTER LIVING

The One Thing That Protects a Laptop After It's Been Stolen

By WHITSON GORDON MARCH 13, 2018

Felipe Trueba/European Pressphoto Agency

Lost Laptops

- Laptops commonly lost and stolen
  - 12,000 laptops lost per week in US airports in 2008
  - A laptop is stolen every 53 seconds
- Impact of lost laptop for an organization
  - Brand damage
  - Customer turnover
  - Business interruption
  - Data breach notification and other regulatory actions
  - Remediation efforts
  - Forensic and legal analysis
- Hardware cost is negligible
- Source: Ponemon Institute, Gartner, Inc.

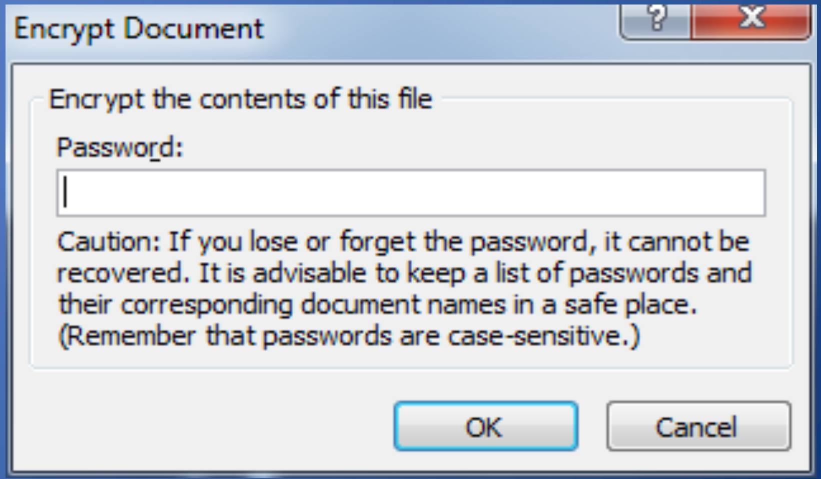
Other Data Breach Scenarios

- Loss of USB drives and smartphones
- Data-stealing malware
- Decommissioned and donated machines
- Equipment seizure by customs and law enforcement
- Recycled obsolete and faulty machines
- Off-site backups
- Cloud storage

File Encryption

Password-Based File Encryption

- File content encrypted
- File name and other metadata not encrypted
- User explicitly encrypts/decrypts files
- Encryption key derived from password
- Standalone feature or built into applications
- Microsoft Office 2007 and later versions
  - AES encryption with 128- or 256-bit keys
  - Secret key derived from password by repeatedly hashing salted password
  - Default for Office 2016 is AES256 with password and salt hashed 100,000 times
  - Maximum password length: 16 characters



Caution: If you lose or forget the password, it cannot be recovered. It is advisable to keep a list of passwords and their corresponding document names in a safe place. (Remember that passwords are case-sensitive.)

Password-Based File Encryption

- File remains encrypted when it is
  - Emailed as attachment
  - Uploaded to cloud storage or copied to USB drive
  - Exfiltrated by malware
- Challenges
  - Difficult for users to create strong passwords
  - Difficult for users to keep track of passwords
  - Cumbersome to enter password each time file is opened
  - Password may be captured by keylogger
  - Sharing requires transmitting password on separate channel
  - Operating system or application may store unencrypted version in temporary file or folder

Sharing Encrypted Files

- Solution A
  - Encrypt file with single symmetric key, K
  - Share K with authorized users
  - Users need to keep many keys, one per shared file
  - User revocation requires redistributing new key

- Solution B
  - Use, different symmetric keys, K_1, …, K_{n} , one per authorized user
  - Encrypt file multiple times with K_1, …, K_n
  - One copy of the file for each authorized user
  - Inefficient in terms of space and computing time

Efficient Sharing of Encrypted Files

- Encryption
  - Encrypt file with single symmetric key K
  - Encrypt key K multiple times with public keys of authorized users PK_1, …, PK_n
  - Share $E_{PK1}(K)$ with user 1, $E_{PK2}(K)$ with user 2, …, $E_{PKn}(K)$ with user n
- Decryption for user i
  - Obtain K by using secret key SK_i to decrypt $E_{PKi}(K)$
  - Decrypt file with K
- Advantages
  - Efficient space usage and computing time
- User revocation?

Beyond Single File Encryption

- Folder encryption
  - Encrypting File System (EFS) in Windows
- Container (volume) encryption
  - Encrypted Disk Image in OS X
  - Encrypted volume in VeraCrypt

- Drive (full disk) encryption
  - BitLocker in Windows
  - FileVault 2 in OS X
  - System encryption in VeraCrypt

Folder Encryption

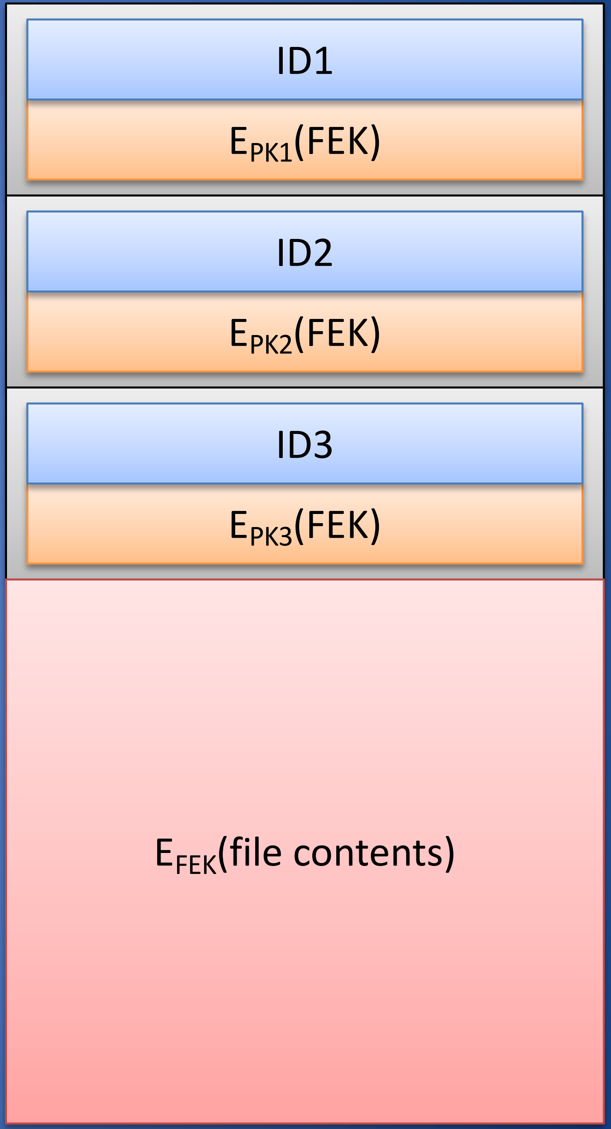
Windows Encrypting File System (EFS)

- Since Windows 2000
- Keys unlocked on successful user login
- Automatic encryption/ decryption of files in folder and subfolders
- Supports sharing of encrypted files (but not folders)
- Latest version uses RSA, SHA-256, and AES

- Protects file content but not file name and other metadata
- Protection local to file system
  - Files decrypted before copying to USB drive, uploading to cloud, or emailing as attachments
- Applications may leak content to unencrypted temp files
- Complex key management

EFS Keys

- Users have public-private key pairs
- Each file is encrypted with a different symmetric file encryption key (FEK)
- FEK is encrypted with public key of file owner and other authorized users
- Data decryption fields (DDF) stored in file header (metadata)
  - ID of authorized user
  - FEK encrypted with public key of user



ID1

E_{PK1}(FEK)

ID2

E_{PK2}(FEK)

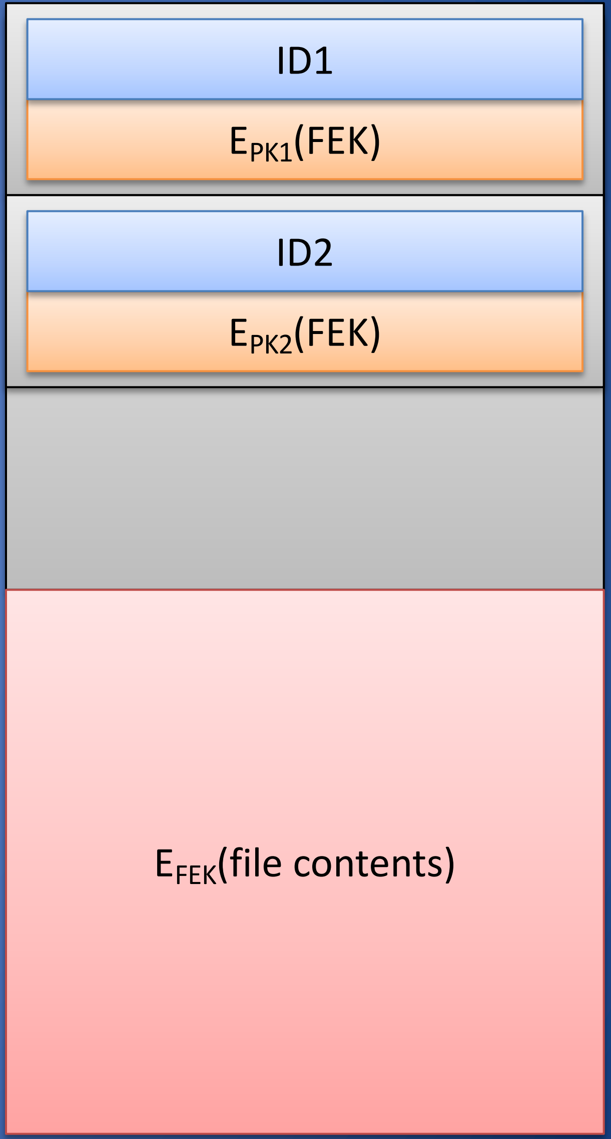
ID3

E_{PK3}(FEK)

E_{FEK}(file contents)

Working with EFS

- Initial encryption
  - File encrypted when created or EFS initialized
  - DDF of file owner created and added to file header
- Adding new authorized user
  - DDF of new user created and added to file header
  - Any authorized user can add other users
- Removing previously authorized user
  - DDF of revoked user removed from file header so they can no longer access file contents
  - File is not re-encrypted with a new FEK



Clicker Question (1)

What happens when an authorized user accesses a file that has been encrypted with EFS?

A. The user's personal FEK is used to decrypt the file header

B. The user's private key is used to decrypt the FEK, which is then used to decrypt the file contents

C. The user's public key is used to encrypt the FEK, which is then used to decrypt the file contents

D. The user's private key is used to decrypt the file contents

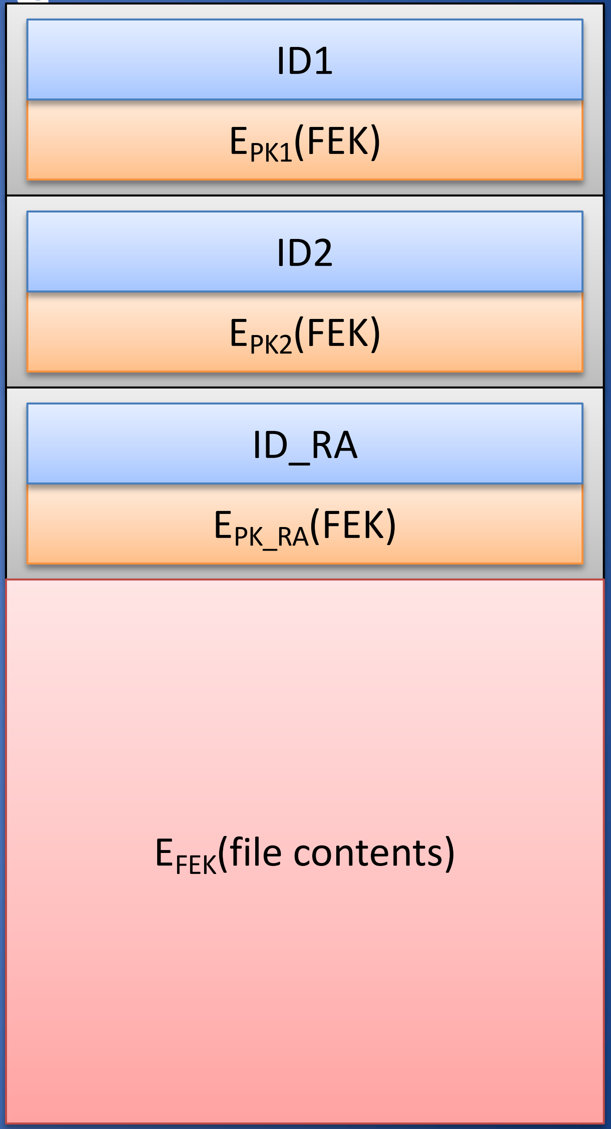
Clicker Question (1) - Answer

What happens when an authorized user opens a file that has been encrypted with EFS?

A. The user's personal FEK is used to decrypt the file header
B. The user's private key is used to decrypt the FEK, which is then used to decrypt the file contents
C. The user's public key is used to encrypt the FEK, which is then used to decrypt the file contents
D. The user's private key is used to decrypt the file contents

Recovery Agent

- Data recovery fields (DRFs) provide additional encrypted FEKs, associated with recovery agents
- Inside the file header there will be a DRF if there is a Data Recovery Agent present in the OS
- It is not possible to add a Data Recovery Agent if you do not have access to the plaintext version of the encrypted file



ID1

E_{PK1}(FEK)

ID2

E_{PK2}(FEK)

ID_RA

E_{PK_RA}(FEK)

E_{FEK}(file contents)

Container Encryption

Encrypted Container

- Included in macOS and Windows
- Alternatively, use open source software VeraCrypt (successor of TrueCrypt)
- Initial encryption
  - Store entire content of folder (and subfolders) into single encrypted image file (container)
  - Key randomly generated or derived from user password
- Decryption
  - Mount decrypted image file to virtual drive by providing key or password
- Reencryption
  - Unmount virtual drive (automatic on logoff/shutdown)

Containers and Virtual Drives

- Benefits
  - User enters password once when mounting image
  - Encryption protects an entire folder and subfolders
- Caution: file in virtual drive is decrypted when it is
  - Emailed as attachment
  - Uploaded to cloud storage or copied to USB drive
  - Exfiltrated by malware

- Challenges
  - Files within virtual drive are not individually encrypted
  - To email/upload encrypted file, must wrap file into container and transmit container
  - Difficult for users to create and keep track of strong passwords
  - Difficult for users to securely generate and store random keys/passwords

TrueCrypt/VeraCrypt

- TrueCrypt: Free open-source disk encryption software for Windows 8/7/Vista/XP, Mac OS X, and Linux
  - Discontinued on June 2014 and then a fork in VeraCrypt
  - Security report from Isec Partners: goo.gl/9TR2Rn
  - Creates virtual encrypted disk inside an ordinary file
- In Windows, when the user provides the correct password, the file becomes a with a drive letter—just like inserting a USB drive
- Files copied to/from this encrypted volume are encrypted/decrypted on the fly, automatically and transparently

A less common issue…

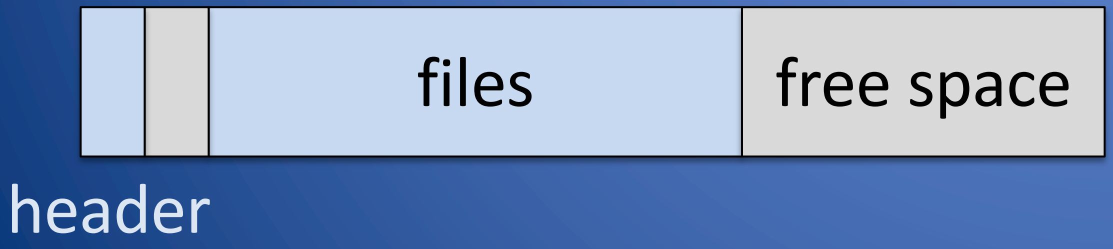
- Personal laptop or memory card, for “security” reason can sometimes be seized when you cross international borders, e.g.
    - Alice is a human-rights worker, and keeps sensitive information on her computer.
    - The data is encrypted, but she is concerned that the secret police will seize her computer and, noticing that part of the disk is encrypted, threaten her — or worse — for the key.
    - She needs to protect her data in such a way that it is ***deniable***: there must be nothing that would indicate to the secret police that there are hidden files on her computer

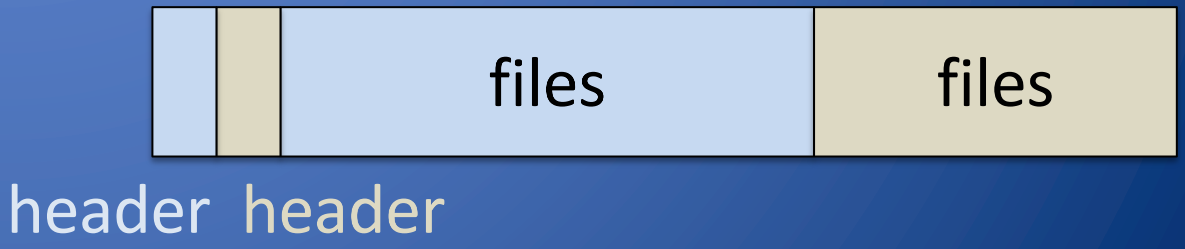
Defeating Encrypted and Deniable File Systems, Schneier et al. 2006

Hidden Container

- An encrypted container may store hidden encrypted files
  - Free space of container normally filled with random data
  - Encrypted files would be indistinguishable from free space

- Enables plausible deniability
- The VeraCrypt open source tool supports a hidden container (aka volume) within outer container
  - If password fails to open outer container, try hidden container





DEMO VERACRYPT

Plausible Deniability

- Political doctrine developed in the US around the 50's:
  - Applied to CIA operations. (i.e. the bay of pigs)
  - If illegal operations are discovered, it was possible to deny any connection or guilt of the principals.
- In general with Plausible Deniability means:
  - Any act that leaves little or no evidence of irregularities or abuse
  - In the computer world is the ability to deny the presence of data within a container

Plausible Deniability (2)

- Until decrypted, hidden container just looks like random data
- Cannot distinguish hidden encrypted data from random data
- Ethical considerations
  - Consider cases where a user is being tortured for their data
  - Attacker cannot know if user has revealed all their data; may continue torturing even after user has revealed everything

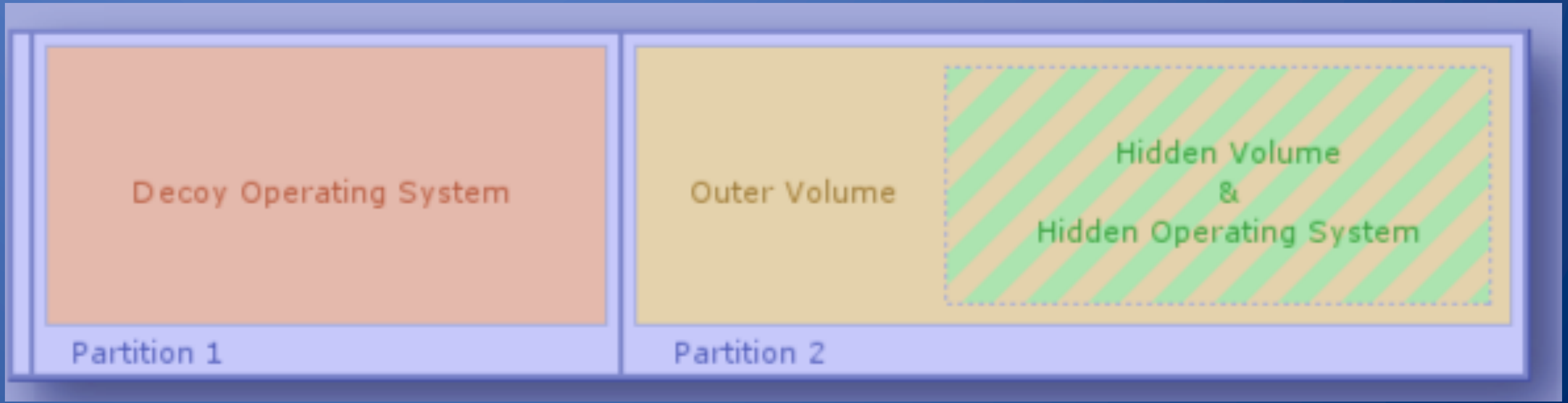
- Legal considerations
  - Prosecutors cannot prove existence of encrypted data
  - Does this + user's denial produce reasonable doubt about whether there is encrypted data?
- See VeraCrypt's documentation on plausible deniability

Deniable file systems leak!

- Recent files (e.g. Shortcuts)
- Auto recovery (e.g. World documents)
- Caching (e.g. Swap space)

To mitigate these problems Veracrypt allows a hidden operating systems

https://veracrypt.eu/en/VeraCrypt%20Hidden%20Operating%20System.html



Drive Encryption

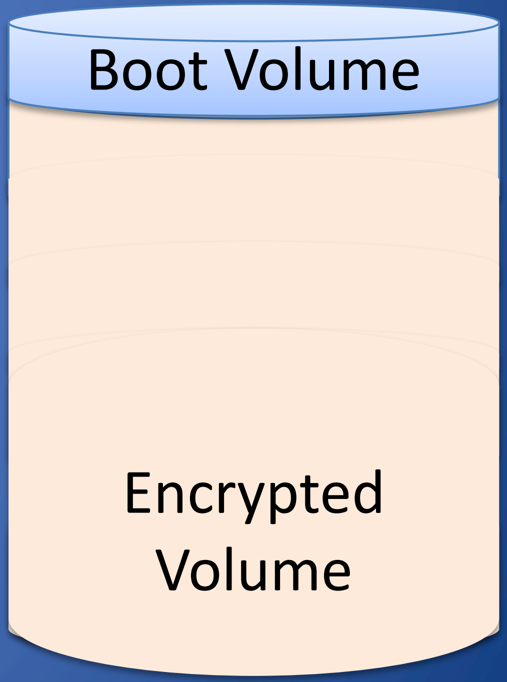
Drive Encryption

- Entire hard drive is encrypted
  - Symmetric encryption of each block
  - Master boot record not encrypted
- Key supplied at boot time and kept in memory
- Blocks always stored encrypted on the drive
  - decrypted on read
  - reencrypted on write

- Options for supplying key
  - Insert USB drive
  - Enter password
  - Use secure chip within computer
  - At least two of the above
- Tools
  - FileVault 2: built in Apple OS X
  - Bitlocker: built in Microsoft Windows
  - VeraCrypt: open source software

BitLocker Architecture

- Volumes
  - Small unencrypted boot volume
  - Large encrypted volume storing rest of OS and user files
- Volume Master Key (VMK)
  - Unlocked through authentication procedure
- Full Volume Encryption Key (FVEK)
  - Used to encrypt sectors of encrypted volume
  - Stored on boot volume encrypted with VMK
  - Kept in memory and never written unencrypted to disk

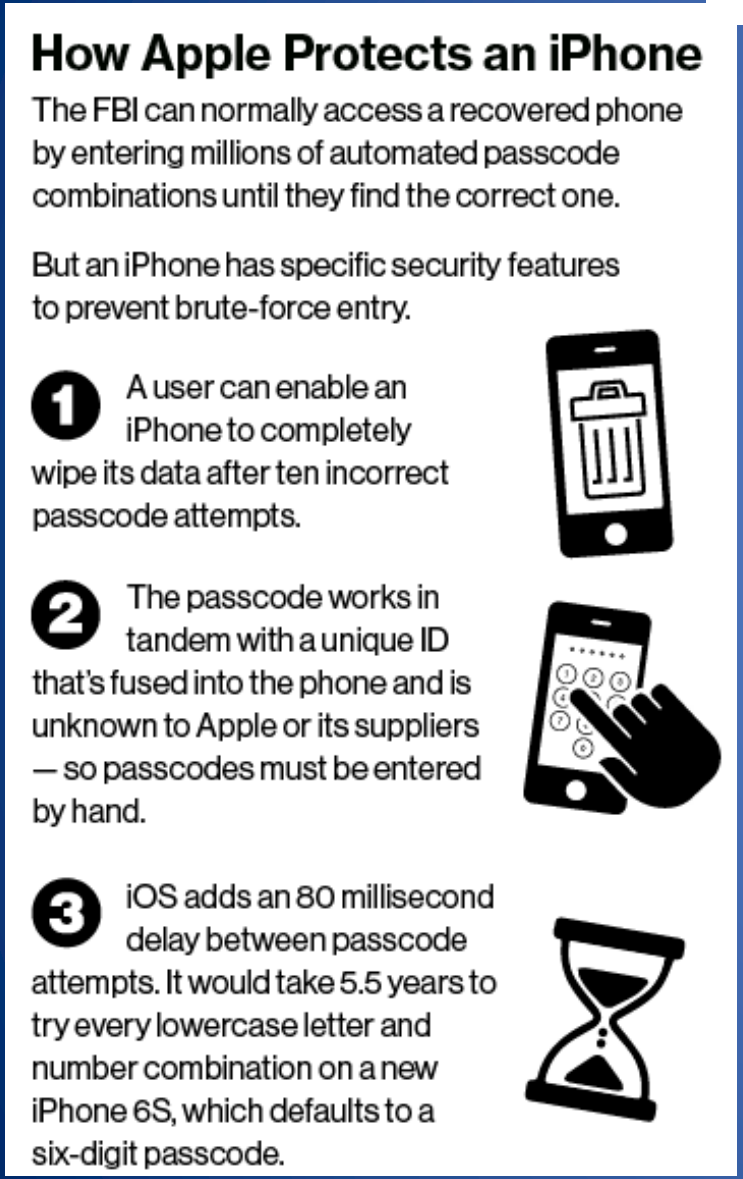


FileVault 2

- Apple equivalent of BitLocker
  - OS X Lion and later
  - compatible with HFS, Apple's proprietary filesystem
  - Fewer options than BitLocker for recovery
- Similar architecture to BitLocker
  - Non encrypted boot volume, and encrypted startup volume
- Encrypts disk with 256-bit AES key, 128-bit blocks

IOS Vs. FBI

Source: Bloomberg



How Apple Protects an iPhone

The FBI can normally access a recovered phone by entering millions of automated passcode combinations until they find the correct one.

But an iPhone has specific security features to prevent brute-force entry.

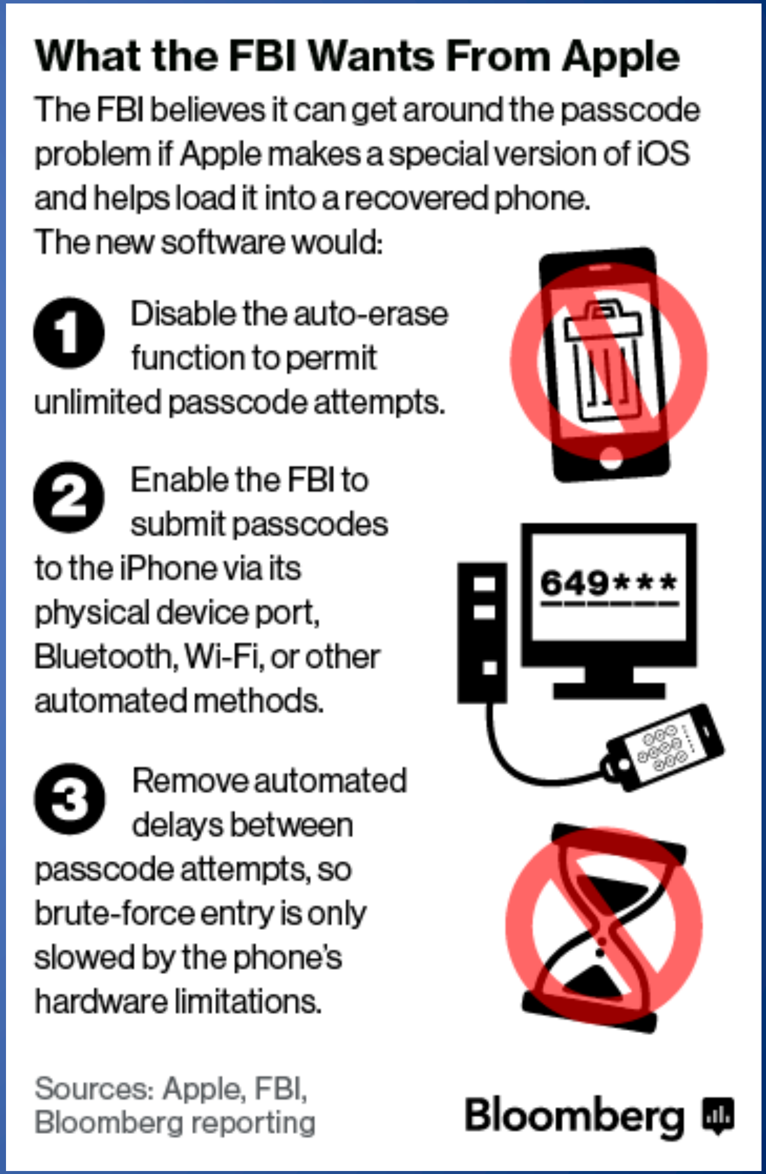
1 A user can enable an iPhone to completely wipe its data after ten incorrect passcode attempts.

2 The passcode works in tandem with a unique ID that's fused into the phone and is unknown to Apple or its suppliers — so passcodes must be entered by hand.

3 iOS adds an 80 millisecond delay between passcode attempts. It would take 5.5 years to try every lowercase letter and number combination on a new iPhone 6S, which defaults to a six-digit passcode.

Obstacles to avoid guessing passcode:

1. iOS may completely wipe the user's data after too many incorrect PINs entries
2. PINs must be entered by hand on the physical device, one at a time
3. iOS introduces a structured delay after every incorrect PIN entry



What the FBI Wants From Apple

The FBI believes it can get around the passcode problem if Apple makes a special version of iOS and helps load it into a recovered phone. The new software would:

1 Disable the auto-erase function to permit unlimited passcode attempts.

2 Enable the FBI to submit passcodes to the iPhone via its physical device port, Bluetooth, Wi-Fi, or other automated methods.

3 Remove automated delays between passcode attempts, so brute-force entry is only slowed by the phone's hardware limitations.

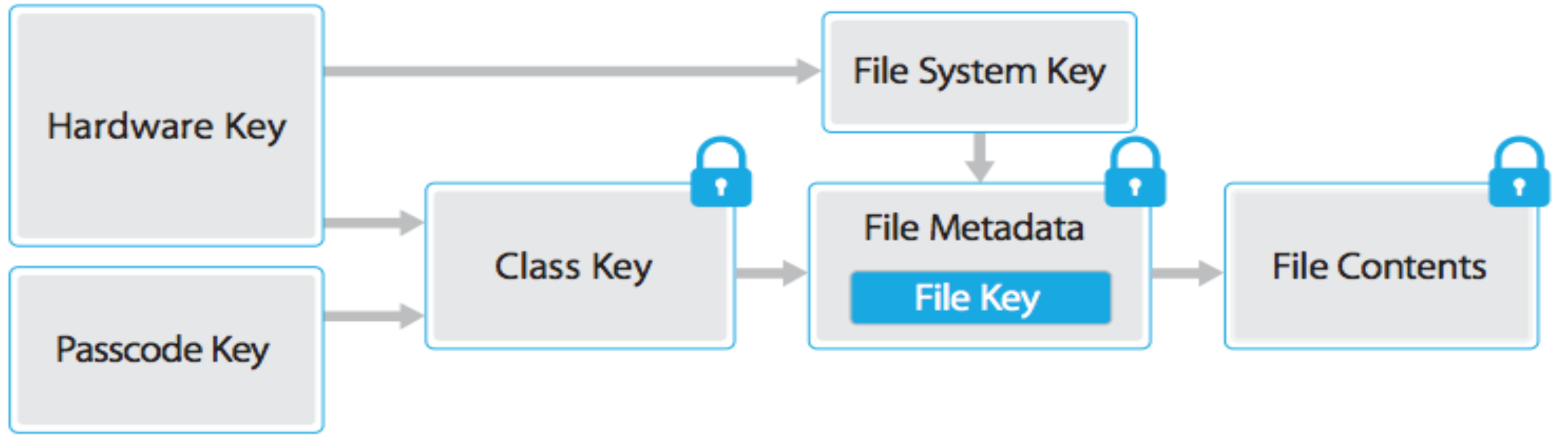
Sources: Apple, FBI, Bloomberg reporting

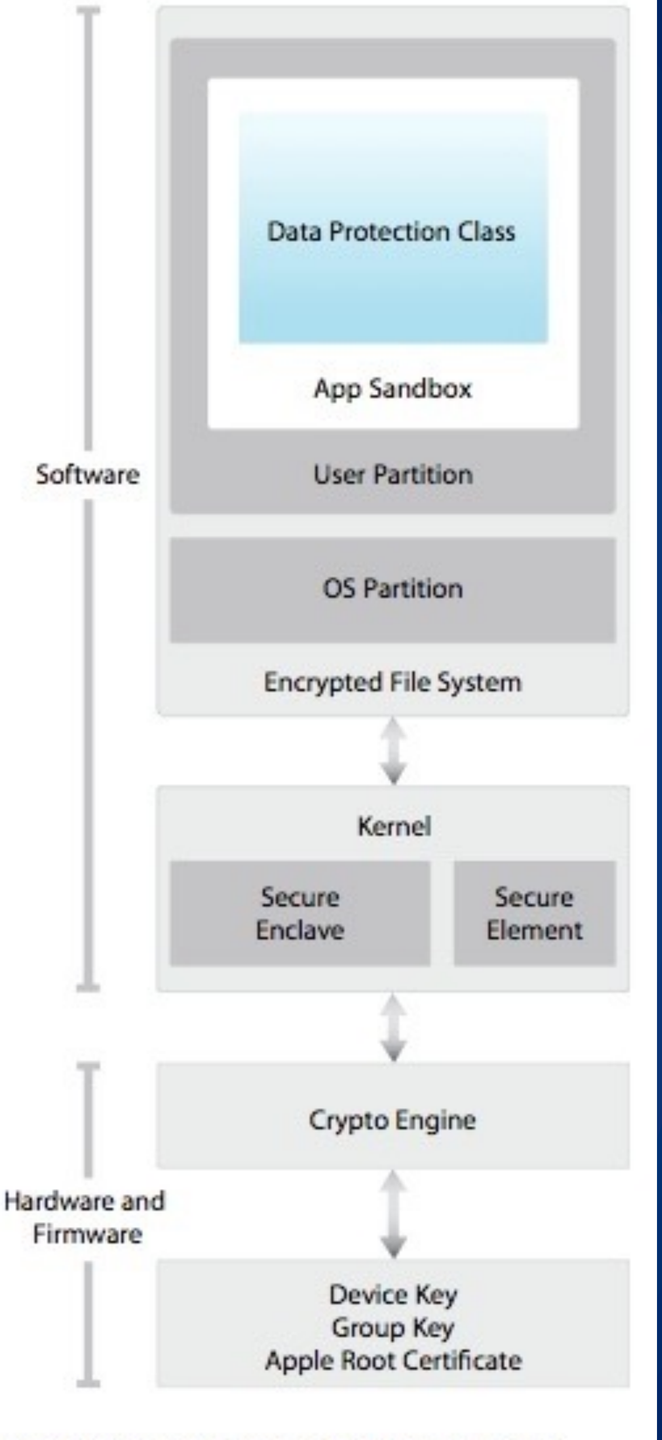
Bloomberg

IOS Vs. FBI

- Apple IOS 9.0 Security Guide: goo.gl/6BsBNR
- Secure Enclave is a coprocessor starting from Apple A7:
  - has its own secure boot and software update separate from the application processor
  - provides all cryptographic operations, uses encrypted memory and includes a hardware random number generator
  - is provisioned during fabrication with its own UID (Unique ID) not know by Apple

Source: developer.apple.com



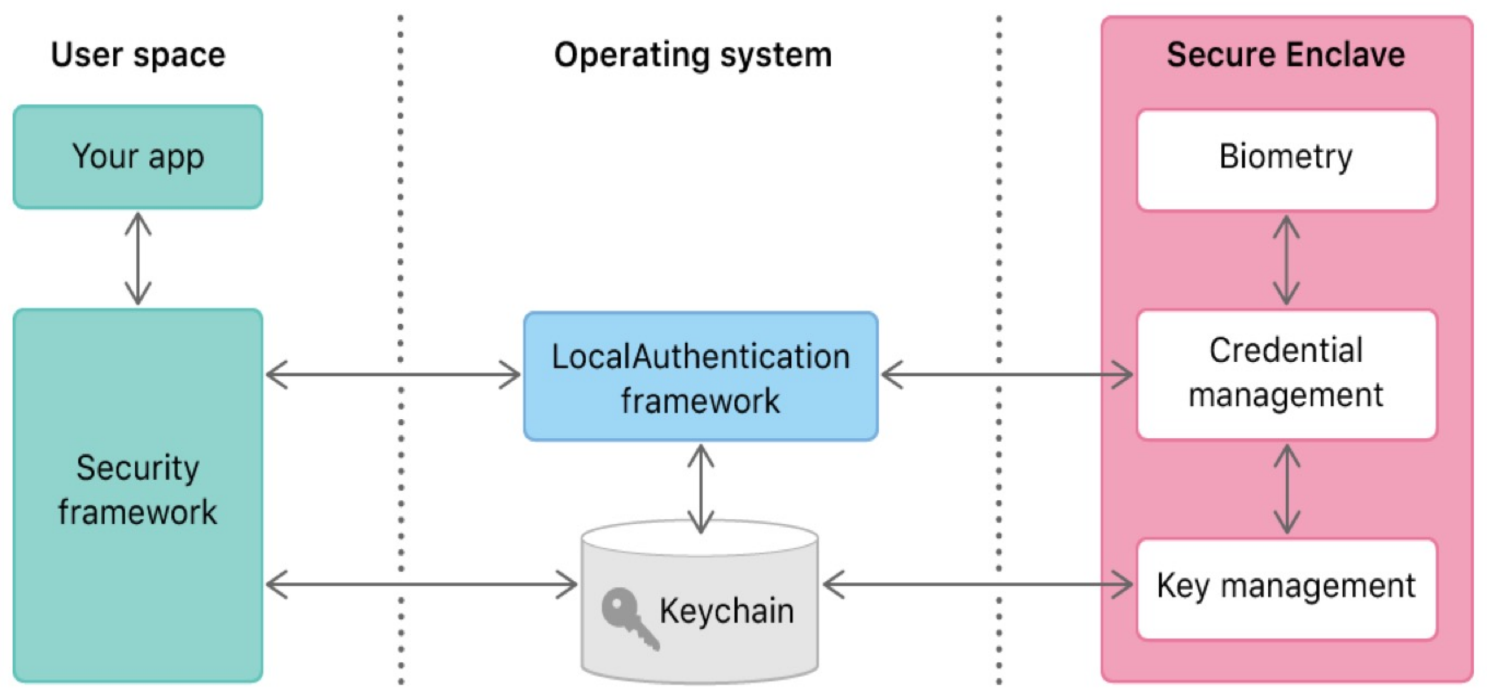


iOS Drive Encryption

Secure enclave: tamper-proof silicon hardware on device

- is a coprocessor starting from Apple A7 runs own microkernel, 4MB of storage
- stores 256-bit ECC private keys unique to device
- has its own secure boot and software update separate from the application processor
- provides all cryptographic operations, uses encrypted memory and includes a hardware random number generator

- Keys never synced to cloud or seen by OS
  - To decrypt data, OS makes request to secure enclave



Source: developer.apple.com

Trusted Platform Module (TPM)

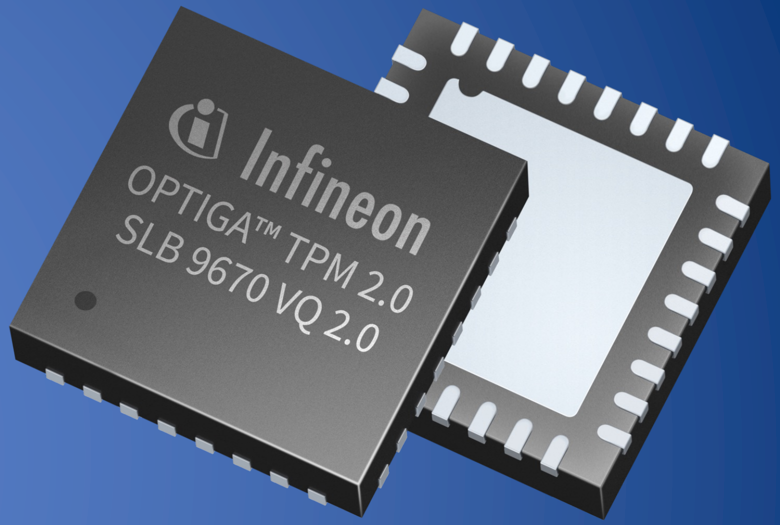
- The TPM crypto processor
  - Mounted on motherboard, tamper-resistant
  - Can be used with Bitlocker to stores the volume master key (VMK), or a share of it
  - Stores information that enables verifying the operating system has not been modified

Source: Infineon Technologies

- Bitlocker TPM authentication upon boot
  - Verify the integrity of the operating system (basic authentication)
  - Optionally asks user to enter a password
  - Releases the VMK, or the share it stores
  - Optionally asks user to supply remaining share of VMK via USB drive

Stealing the Key from the TPM

- Crypto processor
  - Mounted on motherboard, tamper-resistant
  - Releases the volume master key (VMK) after verification of OS integrity



Source: Infineon Technologies

- Attacks to steal the key from the TPM
  - Tamper resistance means simple attacks will damage the TPM and destroy the key stored inside it
  - Complex and expensive attacks are possible via chip deconstruction and microscopy [Tarnovsky, Black Hat DC 2010]

Cold Boot Attack

- Assumptions
  - Volume decryption key is (or can be made to be) stored in memory
  - Attacker has physical access to laptop
- Example
  - Laptop locked in sleep mode
- Attack steps
  - Cool RAM to retain content
  - Boot from USB
  - Dump memory content
  - Search for decryption key
- [Halderman et al., USENIX Security 2008]

To Learn More

- Cryptography and encryption in Office 2016
- The Encrypting File System
- Using Encrypting File System
- Microsoft Bitlocker
- Apple FileVault 2
- VeraCrypt
- C. Tarnovsky. Deconstructing a 'Secure' Processor. Black Hat, 2010
- A. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman, J. Appelbaum, E. W. Felten: Lest We Remember: Cold Boot Attacks on Encryption Keys. USENIX Security 2008
- B. Schneier. "Evil Maid" Attacks on Encrypted Hard Drives. Schneier on Security, 2009

What We Have Learned

- Password-based file encryption
- Sharing encrypted files
- Container encryption and hidden containers
- Drive encryption
- Cold boot attack