



WHY DO USB FLASH DRIVES KEEP GETTING HACKED?

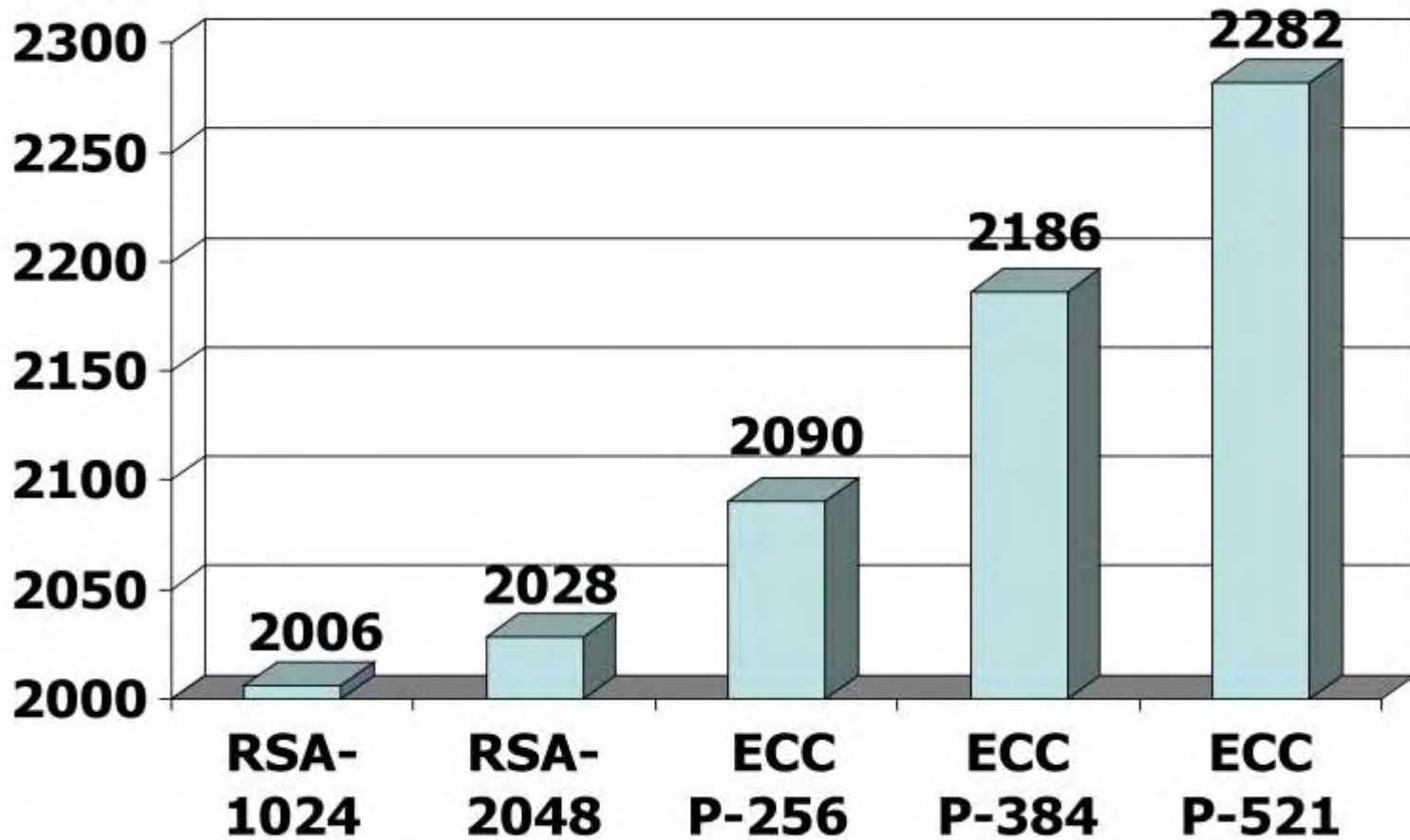
Ron LaPedis, CISSP-ISSAP, ISSMP

Director, Product Management & Marketing

SPYRUS, Inc

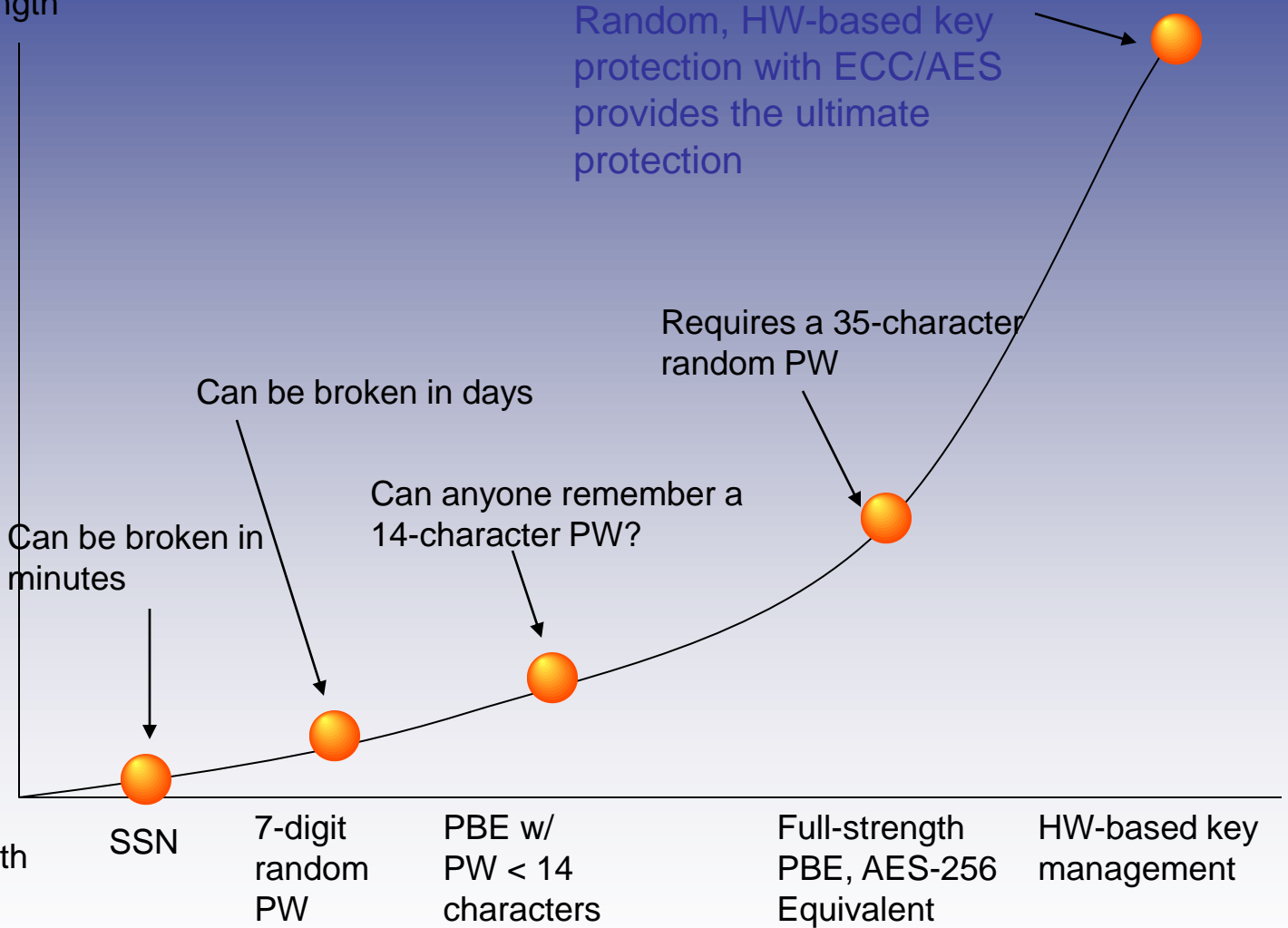
- Software
 - Password
 - Unlocking mechanism
 - Encryption keys
 - Key encryption key
 - Archive
- Hardware
 - USB interface
 - PC board
 - Memory or crypto components

Crypto Strength: Useful life of keys.



Password Based Encryption: Beware!

Highest strength



Low strength

SSN

7-digit
random
PW

PBE w/
PW < 14
characters

Full-strength
PBE, AES-256
Equivalent

HW-based key
management



Why Hardware-based Encryption?

- Keys stored in software are vulnerable to viruses and malware
- Personal computers with dual-core CPUs are vulnerable to attacks that can compromise an AES key in seconds
- Weaker random number generators used by SW = weaker encryption
- HW key protection protects against password-guessing attacks, side-channel attacks, and software substitution attacks.
- **Only hardware-based key management can prevent password-guessing attacks**

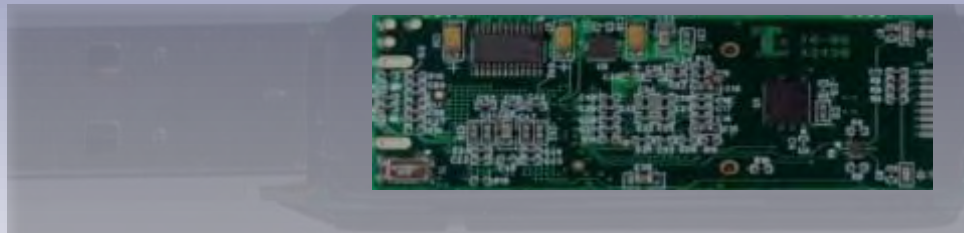


FIPS 140-2 Is Not The Entire Solution

- What is the security boundary and why is it important?
- What does FIPS validation mean?
- Where does processing take place?



FIPS Boundary





FIPS Boundary



FIPS Boundary



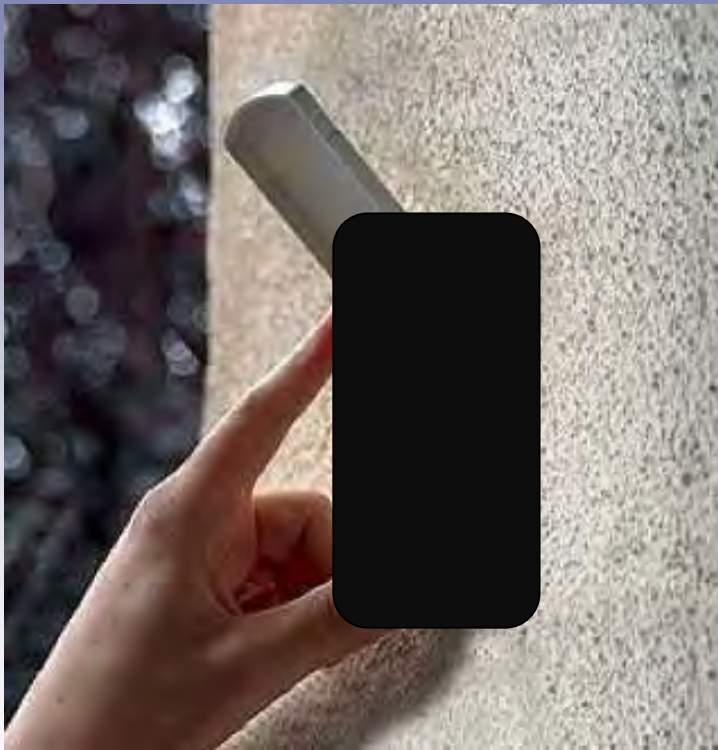
FIPS Boundary



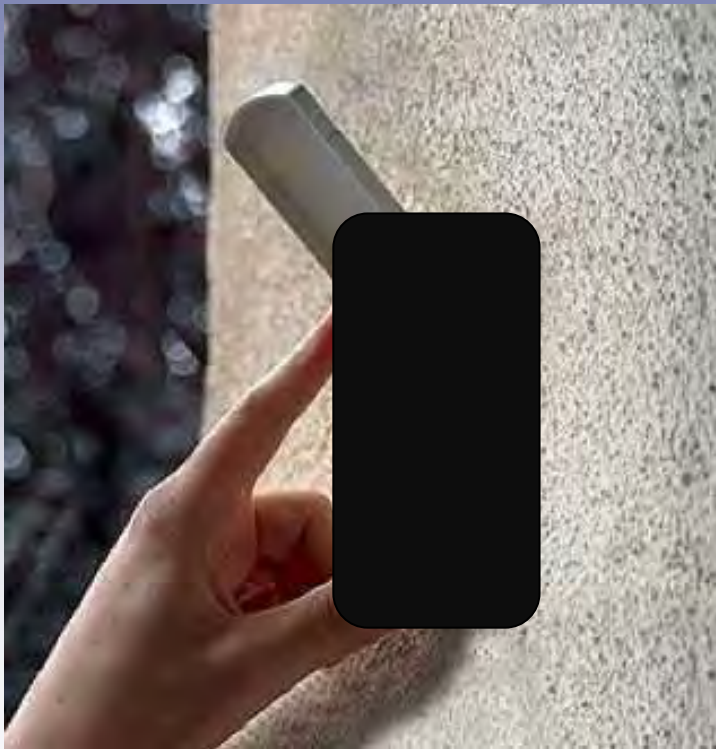
FIPS Boundary



FIPS Boundary



FIPS Boundary – SySS Hack



- "From our initial analysis, it appears that the software authorizing decryption, rather than the cryptographic module certified by NIST, is the source of this vulnerability"



Basic Encrypting Drive

- Drive is unlocked after authentication
- Files are protected only when the drive is locked or powered down
- Files moved off the drive are unprotected

CDROM Partition

Device Access Software

Encrypted Partition

File	File	File	File
File	File	File	File
File	File	File	File





Password Archive





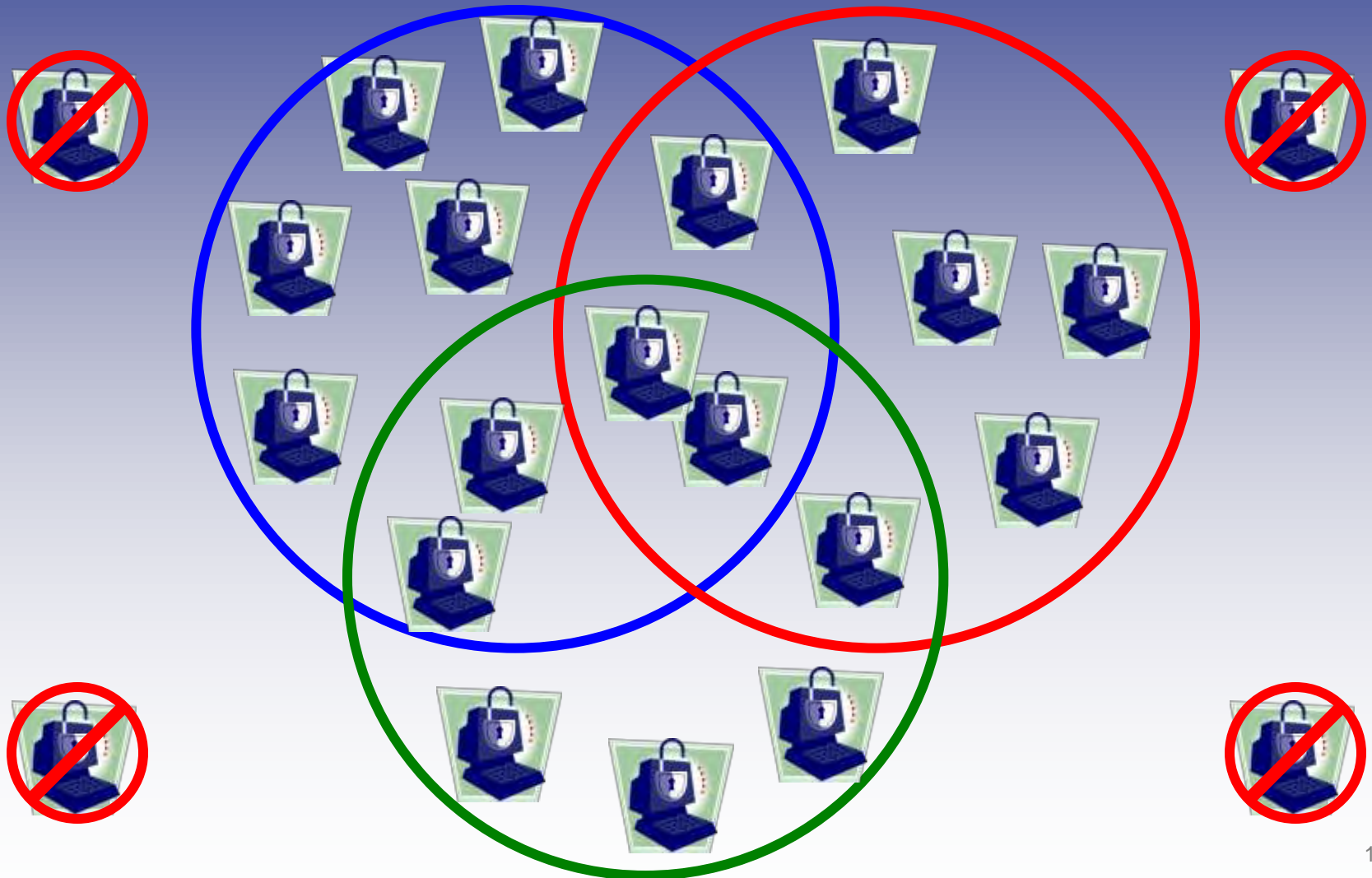
Some Solutions

Some Solutions

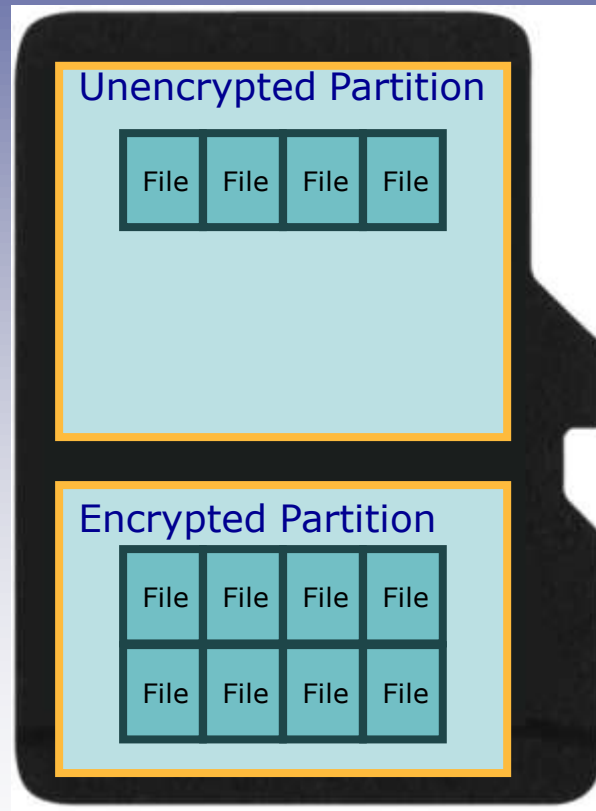
- All security happens within the FIPS boundary
- Quorum Technology—Device cannot be decrypted without several pieces of information coming together



Quorum Technology

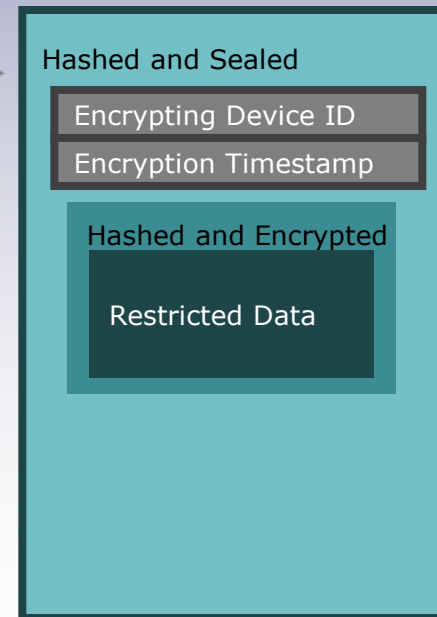
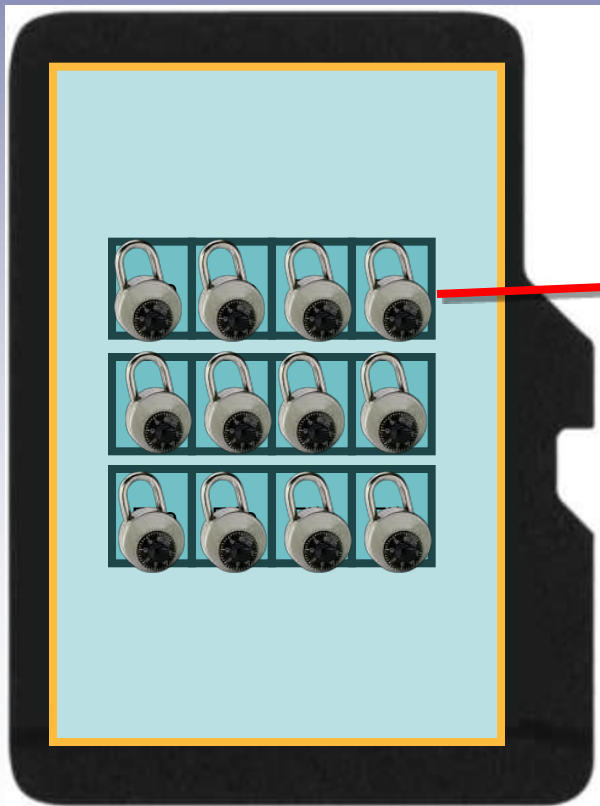


Partition Drive For Separation



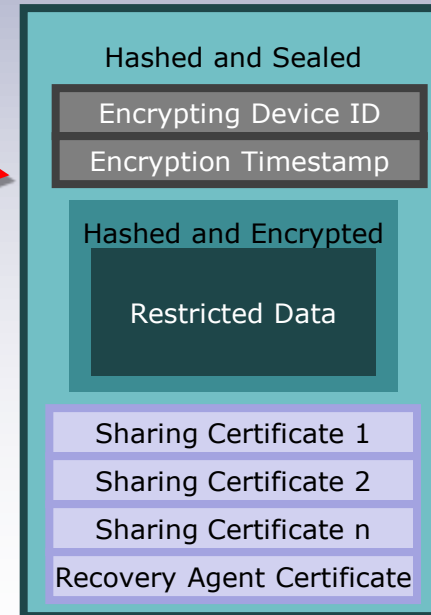
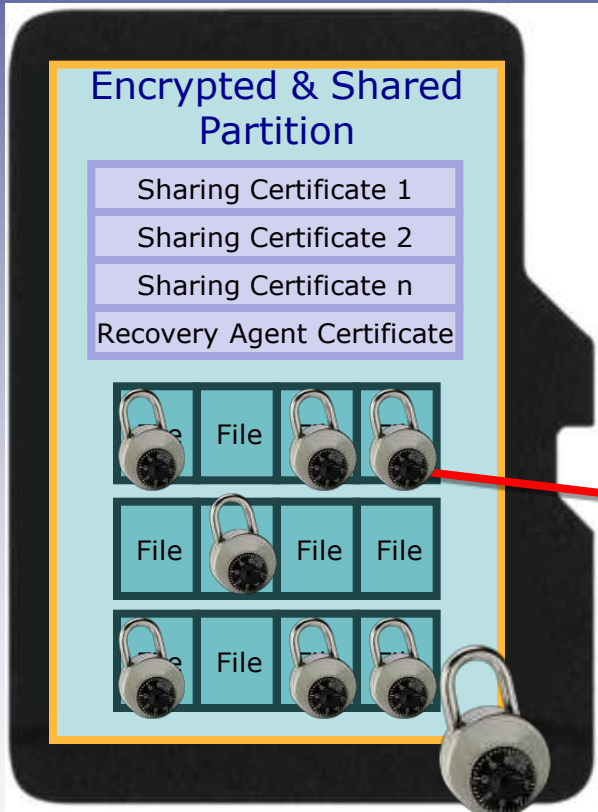
File-Based Encryption


- Each file encrypted under a unique key.
- Encrypted files can be safely stored anywhere.



Use certificates for secure sharing

(similar to S/MIME used for email)





Do you
know where your secure
USB flash drive comes from?

“Assembled in USA” does not
mean trusted parts. Check to
see that your drive is designed,
developed, and manufactured
in the USA.



www.spyrus.com
(408) 392-9131

Ron LaPedis, CISSP-ISSAP, ISSMP, MBCP, MBCI
Director, Product Management and Marketing

SPYRUS, Inc.

T: +1 408 392-4354

rlapedis@spyrus.com