

**PROTECTING
DATA AT REST**

ISSA Hartford, CT
2007-10-16

M. E. Kabay, PhD, CISSP-ISSMP
CTO & MSIA Program Director
School of Graduate Studies, Norwich University
mailto:mkabay@norwich.edu V: 802.479.7937

1

Copyright © 2007 M. E. Kabay. All rights reserved.

Topics

- The Fundamental Attributes of Information
- What are Data at Rest?
- Why is Encryption Essential?
- Loss of Control over Unencrypted Data
- Full-Disk Encryption
- Management Challenges
 - Operational requirements
 - Key Management and Recovery
 - Managing Encrypted Backups

With thanks to Dan Lohrmann, CISO of the State of Michigan Distinguished Guest Lecturer, MSIA Program, Norwich

WHAT, NO SPECIFIC PRODUCTS?!? ☹

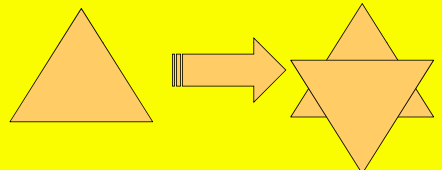
- Detailed product comparisons not appropriate in this presentation
 - MK lacks personal, practical experience of multiple products – cannot legitimately make recommendations!
 - Benefits/costs are context-dependent
 - ✓ Same feature may be + or – for different users
 - ✓ ROI highly dependent on details of implementation
- And we have only 45 minutes!

3

Copyright © 2007 M. E. Kabay. All rights reserved.

The Fundamental Attributes of Information

- Classic Triad
- Parkerian Hexad



4

Copyright © 2007 M. E. Kabay. All rights reserved.

The Classic Triad

C – I – A

5

Copyright © 2007 M. E. Kabay. All rights reserved.

The Parkerian Hexad

Protect the 6 atomic elements of INFOSEC:

- Confidentiality
- Possession or control
- Integrity
- Authenticity
- Availability
- Utility

6

Copyright © 2007 M. E. Kabay. All rights reserved.

Protecting Data at Rest

Why "Parkerian?"




7




Confidentiality

- Restricting access to data
 - Protecting against unauthorized disclosure of *existence* of data
 - E.g., allowing industrial spy to deduce nature of clientele by looking at directory names
 - Protecting against unauthorized disclosure of *details* of data
 - E.g., allowing 13-yr old girl to examine HIV+ records in Florida clinic




8




Possession

Control over information

- Preventing physical contact with data
 - E.g., case of thief who recorded ATM PINs by radio (but never looked at them)
- Preventing copying or unauthorized use of intellectual property
 - E.g., violations by software pirates



9



Integrity

Internal consistency, validity, fitness for use

- Avoiding physical corruption
 - E.g., database pointers trashed or data garbled
- Avoiding logical corruption
 - E.g., inconsistencies between order header total sale & sum of costs of details



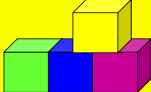
10




Authenticity

Correspondence to intended meaning

- Avoiding nonsense
 - E.g., part number field actually contains cost
- Avoiding fraud
 - E.g., sender's name on e-mail is changed to someone else's



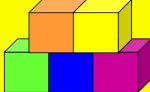
11




Availability

Timely access to data

- Avoid delays
 - E.g., prevent system crashes & arrange for recovery plans
- Avoid inconvenience
 - E.g., prevent mislabeling of files



12

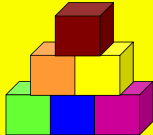


Protecting Data at Rest

Utility

Usefulness for specific purposes

- Avoid conversion to less useful form
 - E.g., replacing dollar amounts by foreign currency equivalent
- Prevent impenetrable coding
 - E.g., employee encrypts source code and "forgets" decryption key



13

Copyright © 2007 M. E. Kabay. All rights reserved.

What are Data at Rest?

- They are:
 - ✓ Data on a locally attached server hard drive
 - ✓ Data on a PC hard drive
 - ✓ Data on a laptop hard drive
 - ✓ Data on a portable storage mechanism (e.g., USB flash drive, USB/Firewire disk, CD, DVD)
 - ✓ Backups
- They are not:
 - ✓ Data being transmitted via e-mail
 - ✓ Data being transmitted over the network (internal or external)

14

With thanks to Dan Lohrmann, CISO of the State of Michigan Distinguished Guest Lecturer, MSIA Program, Norwich University for his kind permission to use some of his slides.

Why is Encryption Essential?

- Organizations responsible for the protection of stakeholder privacy and identity
- Changes in many states regarding breach notification
 - Some states do not require notification if lost data are encrypted
- To build stakeholder trust
- Avoid negative public relations and political distaste after loss of control over data
- Avoid legal liability
- Avoid threats to national security

15

With thanks to Dan Lohrmann, CISO of the State of Michigan Distinguished Guest Lecturer, MSIA Program, Norwich University for his kind permission to use some of his slides.

Encryption Protects

- Confidentiality
- Control
- Integrity
- Authenticity

16

Copyright © 2007 M. E. Kabay. All rights reserved.

Loss of Control over Unencrypted Data

- Data Storage Devices Lost & Stolen
- USA Today Today
- The Veterans Affairs Debacle

17

Copyright © 2007 M. E. Kabay. All rights reserved.

Data Storage Devices Lost & Stolen

- See INFOSEC Year in Review database <http://www2.norwich.edu/mkabay/iyr>
- Currently (Oct 2007) >10,000 abstracts
- 1997 onward
- Categories of interest:
 - 18.1 Stolen equipment or media
 - 18.2 Lost or missing equipment or media
- 122 cases in DB since 1997
 - Fraction (% unknown) of reported cases

18

Copyright © 2007 M. E. Kabay. All rights reserved.

Protecting Data at Rest

USA Today Today: Tuesday, 16 October 2007



- **Headline: TSA laptops with personal data missing**
- 2 laptop computers considered stolen
- Detailed PII about commercial drivers who transport hazardous materials
- 3930 people affected
- TSA contractor Biometric Technology
- Data had been deleted
 - ❑ But was not encrypted in first place
 - ❑ And was not securely wiped
- "TSA spokesman... said none of the data... has been misused." *Oh really?*

19

Copyright © 2007 M. E. Kabay. All rights reserved.

Veterans Administration



- Network World Security Strategies
 - ❑ <http://www.networkworld.com/newsletters/sec/>
 - ❑ Series published June-July 2007
- PIIsed Off Yet?
- VAgaries of Wandering Data
- VAgue Promises of Improvement
- VANishing Confidence
- VAleat Quantum VALere Potest

20

Copyright © 2007 M. E. Kabay. All rights reserved.

PIIsed Off Yet?



- Wife Dr D.N. Black is neuropsychiatrist at Vermont State Hospital
- In May 2007, received letter from VA office in Austin, TX
- Portable disk drive stolen from VA Hospital in Birmingham, AL
- Unencrypted data included personally-identifiable information (PII)
 - ❑ Unique Physician Identification Numbers
 - ❑ Birth dates
 - ❑ State medical license numbers
 - ❑ Business addresses
 - ❑ Social Security Numbers

21

Copyright © 2007 M. E. Kabay. All rights reserved.

The Bottom Line



- "We at VA take information security and privacy very seriously. We apologize for any inconvenience or concern this situation may cause, but we believe it is important for you to be fully informed of any potential risk to you."

22

Copyright © 2007 M. E. Kabay. All rights reserved.

VAgaries of Wandering Data



- May 3, 2006: VA employee took computer disks with PII home
- 26.5M veterans affected
- Late May: VA announced incident
 - ❑ Set up Website & 800-number for info
- May 26, 2006: VA Secretary James Nicholson issued directive
 - ❑ Managers & supervisors must adhere to VA policies
 - ❑ Know about all availability and use of all sensitive and confidential data
- June: VA disclosed inclusion of additional loss of control over PII
 - ❑ 1.1M active-duty military personnel
 - ❑ 645,000 reserves

23

Copyright © 2007 M. E. Kabay. All rights reserved.

VAgue Promises of Improvement



- June 14, 2006: Testimony before Congress
 - ❑ Committee on Veterans' Affairs, HR
 - ❑ Linda D. Koontz & Gregory C. Wilshusen, Government Accountability Office (GAO)
 - ❑ Reported years of significant concerns about lack of IA programs at VA
 - ❑ Still did not have incident response plan

24

Copyright © 2007 M. E. Kabay. All rights reserved.

Report by the VA IG



- July 11, 2006: George Opfer reports to Congress
 - Inspector General of the VA
- Severe criticism of senior managers for lackadaisical response to original theft of PII
- Inadequate security policies *still* not corrected
- VA Secretary Nicholson issued assurances that VA had "embarked on a course of action to wholly improve its cyber and information security programs."

25

Copyright © 2007 M. E. Kabay. All rights reserved.

VA nishing Confidence



- August 7, 2006: VA reports another loss
 - Desktop computer stolen
 - Unencrypted PII on up to 38,000 veterans
- August 14, 2006: VA announces new security plans
 - Spend \$3.7M on encryption software
 - Encrypt data on all VA computers and external storage media & devices
 - Installation to begin Aug 18.

26

Copyright © 2007 M. E. Kabay. All rights reserved.

Laptop Computer in Manhattan VA Hospital



- September 8, 2006: public disclosure
- Locked to cart
- Locked room
- Locked corridor
- Data unencrypted (against new policy) because "a decision had been made not to encrypt data being used for medical purposes."
- Mid-September: stolen desktop computer recovered

27

Copyright © 2007 M. E. Kabay. All rights reserved.

US Government Agencies



- October 2006: Congressional Committee on Oversight and Government Reform publishes report on data losses
 - US government agencies
 - Since January 1, 2003
 - Total of 788 incidents in 19 agencies + "hundreds" at VA

28

Copyright © 2007 M. E. Kabay. All rights reserved.

VA Admits Disks Lost 6 Months Prior



- October 31, 2006: reports data disks lost
- PII for 1,400 veterans
- Unencrypted data disks lost in May, June & July 2006
- Delay due to wait for administrative approval of press release

29

Copyright © 2007 M. E. Kabay. All rights reserved.

VAleat Quantum VALere Potest*



- February 2, 2007: VA Secretary Nichols reports another missing hard drive
 - Since 22 January
 - Used for backup
 - Unencrypted
 - PII on 48,000 veterans – oh no, wait: 535,000 veterans + 1.3M doctors (oops)

"Let it stand for what it is worth."

30

Copyright © 2007 M. E. Kabay. All rights reserved.

GAO Slams VA Managers

- February 28, 2007: Director of Information Security Issues Gregory C. Wilshusen
 - ❑ Report: "Veterans Affairs Needs to Address Long-Standing Weaknesses."
 - ❑ Consistent failure to develop & implement IA policies
 - ❑ Recurring weaknesses in protecting PII

31 Copyright © 2007 M. E. Kabay. All rights reserved.

Prompt and Decisive Action

- March 2007: VA CIO Robert Howard restricts portable devices
 - ❑ Only flash drives < 2 GB issues by VA itself
 - ❑ Encryption to be used throughout (ho hum)
- May 2007: all government agencies to stop storing SSNs and other PII wherever possible

32 Copyright © 2007 M. E. Kabay. All rights reserved.

Management of Disk Encryption

- Functional Requirements
 - ❑ Full-disk Encryption
 - ❑ Pre-boot Authentication
 - ❑ FIPS 140-2 Certified
- Operational Requirements
 - ❑ Key Recoverability
 - ❑ Auditability
 - ❑ Port Control
- Infrastructure Requirements
- Encrypted Backups

33 Copyright © 2007 M. E. Kabay. All rights reserved.

Functional Requirements

- Encryption Requirements
 - Full disk encryption (FDE)
 - Pre-boot authentication
 - FIPS 140-2 certified
- Operational Requirements
 - Key recoverability
 - Auditability
 - Port control
- Infrastructure Requirements
 - Ability to load users from Active Directory, E-Directory, and manually
 - Central key management (console)

34 With thanks to Dan Lohrmann, CISO of the State of Michigan Distinguished Guest Lecturer, MSIA Program, Norwich University for his kind permission to use some of his slides.

Encryption Requirements: Full Disk Encryption

- Without *full disk* encryption users cannot be sure that their data are encrypted
 - ❑ Many sections unprotected
 - ✓ E.g., user files in "Program Files"
 - ❑ Forget that some sections aren't safe
- Normal file deletion leaves residual data on the hard drive
- Applications and browsers leave data in unpredictable areas on the hard drive
- Users often do not realize they have sensitive data on their devices
- Google Desktop Index & Microsoft Outlook 2007 Index files *must* be encrypted

35 With thanks to Dan Lohrmann, CISO of the State of Michigan Distinguished Guest Lecturer, MSIA Program, Norwich University for his kind permission to use some of his slides.

Encryption Requirements: File-level Encryption Not Recommended

36 With thanks to Dan Lohrmann, CISO of the State of Michigan Distinguished Guest Lecturer, MSIA Program, Norwich University for his kind permission to use some of his slides.

Encryption Requirements: Full-Disk Encryption Recommended

The diagram illustrates a disk layout for Full Disk Encryption. It shows a horizontal bar representing the disk, divided into several sections. From left to right: a small green box labeled 'Master boot record', a larger green box labeled 'MBR', a green box labeled 'My sensitive files', a green box labeled 'Reserved Space', and a large green box labeled 'Drive C:'. Brackets indicate that the 'Master boot record' and 'MBR' are 'Not used', while the 'Reserved Space' and 'Drive C:' are 'Used'. A legend on the left identifies 'Encrypted Space' (green), 'Sensitive Data' (red), and 'File' (pink).

Note that FDE encrypts the entire disk including the unused space before the C partition and after it. (Encrypting only the C drive may leave attacker code in these spaces.)

With thanks to Dan Lohrmann, CISO of the State of Michigan Distinguished Guest Lecturer, MSIA Program, Norwich University for his kind permission to use some of his slides.

Encryption Requirements: Pre-Boot Authentication

- User must be identified prior to accessing the operating system
- Can be implemented in single signon mode thereby requiring only 1 username and 1 password to login to Windows (transparent to user)
- Compatible with existing SecurID tokens, Smart Cards, Biometrics and many other multi-factor authentication devices

With thanks to Dan Lohrmann, CISO of the State of Michigan Distinguished Guest Lecturer, MSIA Program, Norwich University for his kind permission to use some of his slides.

Encryption Requirements: FIPS 140-2 Certified

- Federal Information Processing Standard (FIPS) Publication 140-2
 - ❑ U.S. government computer security standard
 - ❑ Used to accredit cryptographic modules
- Industry best practice dictates that successful implementations of encryption products meet the FIPS 140-2 certification.

With thanks to Dan Lohrmann, CISO of the State of Michigan Distinguished Guest Lecturer, MSIA Program, Norwich University for his kind permission to use some of his slides.

Operational Requirements: Key Recoverability (Key Escrow)

- User forgets login – product must have an interface for Client Service Center to restore access
- Master login (backdoor)
 - ❑ Must not exist for *signing* keys
 - ❑ May exist for *encryption* keys
- Operations and security must have access to keys for acceptable-use policy investigations and others

Copyright © 2007 M. E. Kabay. All rights reserved.

Operational Requirements: Auditability

- Product must be able to validate that encryption has taken place for each device that is encrypted
- Audit logs will be used to fulfill notification requirement changes within law
- Port control audit logs can be used to enforce sensitive data control policies

With thanks to Dan Lohrmann, CISO of the State of Michigan Distinguished Guest Lecturer, MSIA Program, Norwich University for his kind permission to use some of his slides.

Operational Requirements: Port Control

- STAPLES now selling new external drive
 - ❑ 1 TB USB/Firewire I/F
 - ❑ Size & shape of a book – will fool guards
 - ❑ \$349(!)
- Need ability to restrict writing to USB ports for agencies that request it
- Selective device control (e.g., USB made by Company A but USB device made by Company B)
- Automatic encryption of data when sent to the USB port if allowed

With thanks to Dan Lohrmann, CISO of the State of Michigan Distinguished Guest Lecturer, MSIA Program, Norwich University for his kind permission to use some of his slides.

Infrastructure Requirements



- Central console to manage encryption enterprise-wide
- Centralized policy enforcement for users and groups of users
- Web-based interface for password recovery situations
- Ability to interface with different LDAP directories
 - ❑ Lightweight Directory Access Protocol
 - ❑ E.g., Novell E-Directory, Microsoft Active Directory
- Manual entry for users that don't exist in an LDAP

43

With thanks to Dan Lohrmann, CISO of the State of Michigan Distinguished Guest Lecturer, MSIA Program, Norwich University for his kind permission to use some of his slides.

Managing Encrypted Backups



- All backups must take change into account
 - ❑ Degradation of *storage media*
 - ✓ Copies on schedule
 - ❑ Changes in *software-defined* formats
 - ✓ Conversions as required
 - ❑ Changes in *hardware-defined* formats
 - ✓ Conversions as required
 - ❑ Changes in *encryption keys*
 - ✓ Decrypt, re-encrypt and write new as required
 - ✓ Requires confidence in *key management*
 - Which key at which time for which backups?

44

Copyright © 2007 M. E. Kabay. All rights reserved.

DISCUSSION



45

Copyright © 2007 M. E. Kabay. All rights reserved.