Securing Data at Rest

CSH6 Chapter 36

"Securing Stored Data"

David J. Johnson, Nicholas Takacs, & Jennifer Hadley

1

Topics

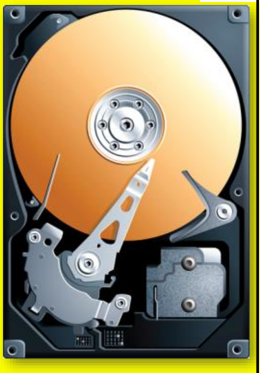
- ➢Introduction to Securing Stored Data
- ➢Fiber Channel Weakness & Exploits
- ➢NFS Weakness & Exploits
- ➢CIFS Exploits
- ➢Encryption & Data Storage
- ➢Data Disposal

CSH6 Chapter 36 covers nonvolatile media: magnetic disks, CDs, DVDs, flash drives. Does not include RAM (or ROM, PROM, EPROM).

2

Introduction to Securing Stored Data

- ➢Security Basics for Storage Administrators
- ➢Best Practices
- ➢DAS, NAS & SAN
- ➢Out-of-Band & In-Band Storage Management
- ➢File System Access Controls
- ➢Backup & Restore Controls
- ➢Protecting Management Interfaces



3

Security Basics for Storage Administrators

- ➢ Data storage security often ignored by security planners
  - ❑Relegated to infrastructure design
  - ❑Particularly strong conflicts between availability and other aspects of Parkerian Hexad
- ➢ Should be considered with other central elements of overall security planning
- ➢ Differentiated security appropriate
  - ❑Data classification helpful (see *CSH6* Chapter 67, "Developing Classification Policies for Data")
- ➢ Backup copies particularly important to protect (see *CSH6* Chapter 57, "Data Backups & Archives")

4

Best Practices (1)

- ➢ Audit & risk assessment on storage infrastructure
- ➢ Authentication across storage network
- ➢ RBAC (role-based access controls) & need-to-know assignment of rights
- ➢ Data encryption & data classification
- ➢ Strong security features & practices from storage vendors
- ➢ Securing SAN (storage area network) at switch (or fabric) level
- ➢ Policies for safely discarding media, devices
- ➢ Evaluating retention policies

5

Best Practices (2)

- ➢ Making retention policies comply with functional, legal & regulatory requirements
- ➢ Isolating storage management NW from organization-wide functional NW
- ➢ Access-log monitoring
- ➢ Employee & contractor background checks
- ➢ Physical controls to restrict access to data centers, lock cabinets & racks, lock servers, protect building/site perimeter (see *CSH6* Chapters 22 & 23 on information infrastructure)
- ➢ Secure backup-medium handling, tracking

6

DAS, NAS & SANs

3 main methods for storing data

- Direct attached storage (DAS)
  - ❑Part of or directly connected to computer
  - ❑Peripheral Component Interconnect (PCI), Small Computer System Interface (SCSI) or other standard
- Network attached storage (NAS)
  - ❑Specialized systems with DAS, dedicated processors & pared-down operating systems
  - ❑Generally connected to TCP/IP NWs
    - ✓Network File System (NFS) for Unix
    - ✓Server Message Block (SMB) or Common Internet File System (CIFS) for Windows
- Storage area networks (SANs) – *see next slide*

7

SANs

RAID: Some people define acronym using "Inexpensive" or "Drives"

- Storage Area Networks: centralized disks accessible to many servers
- Can add disks easily
- Facilitate centralized backups
- Often integrate RAID
  - ❑Redundant Arrays of Independent Disks
  - ❑Different levels from RAID 0 to RAID 6
  - ❑Allows for data duplication, performance improvements
- Connections
  - ❑TCP/IP
  - ❑Fiber Channels (see later in these notes)

8

Out-of-Band & In-Band Storage Management

- In-band management
  - ❑Same NW as data transfers
  - ❑Cleartext signaling
  - ❑DoS attacks on management interfaces
  - ❑Access to excessive information about devices & controllers
  - ❑Set/Reset commands available for abuse
- Out-of-band management
  - ❑Separate NW for control functions
  - ❑Must ensure restricted access – only administrators
  - ❑Ideally, use secure channels

9

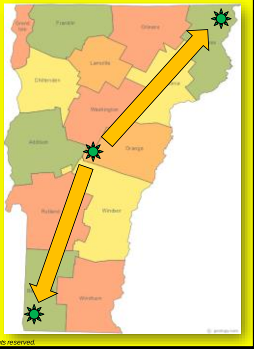
File System Access Controls

- Operating systems include file systems
- File systems generally provide for access controls
  - ❑Data ownership
  - ❑Access control lists (ACLs)
- But security through file system assumes proper user I&A
- For more information on these topics, see *CSH6* Chapters
  - ❑24 – Operating System Security
  - ❑25 – Local Area Networks
  - ❑28 – Identification & Authentication
  - ❑67 – Developing Classification Policies for Data

10

Backup & Restore Controls (1)

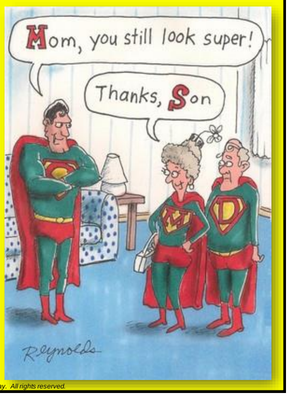
- Backup/restore systems critical for BC & DR
- Typically written to tertiary storage
  - ❑Tape, cassettes, optical media
  - ❑Offsite storage (often run by supplier)
  - ❑Electronic transfer
    - ✓Recovery site
    - ✓Electronic storage service
- Offsite storage needs
  - ❑Secure: authorized personnel only
  - ❑Geographically distant (not subject to same disaster)
  - ❑Audit security, hiring policies



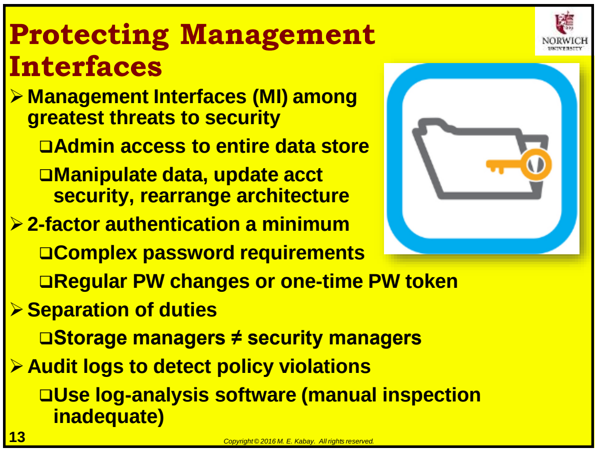
11

Backup & Restore Controls (2)

- Media longevity
  - ❑Verify longevity > archival requirements
- Interpolation of spoofed BU system
  - ❑Writes would be to unauthorized drive
- Insertion of spoofed data storage system
  - ❑Could request RESTORE to unauthorized system
- Authentication of systems essential
  - ❑Manual: login to authenticate BU request
  - ❑Auto: certificate exchange
- Data encryption valuable
- See *CSH6* Chapter 57 "Data Backups & Archives" for more information on these topics



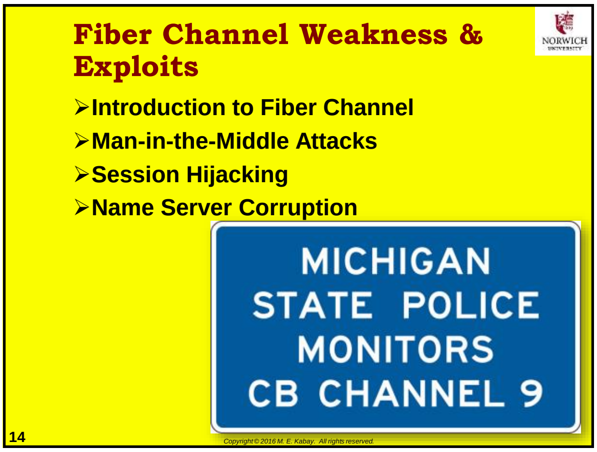
12



Protecting Management Interfaces

- Management Interfaces (MI) among greatest threats to security
  - ❑Admin access to entire data store
  - ❑Manipulate data, update acct security, rearrange architecture
- 2-factor authentication a minimum
  - ❑Complex password requirements
  - ❑Regular PW changes or one-time PW token
- Separation of duties
  - ❑Storage managers ≠ security managers
- Audit logs to detect policy violations
  - ❑Use log-analysis software (manual inspection inadequate)

13

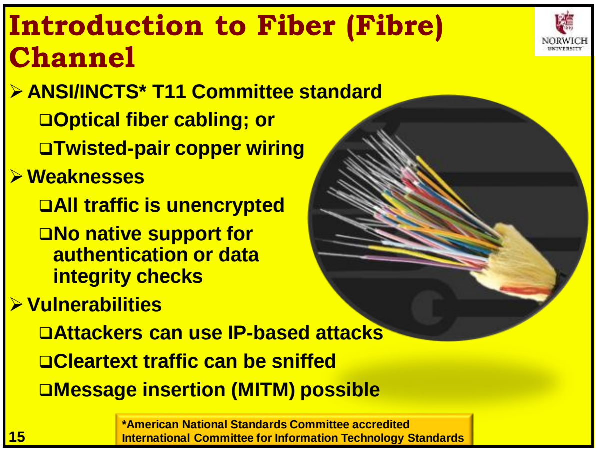


Fiber Channel Weakness & Exploits

- Introduction to Fiber Channel
- Man-in-the-Middle Attacks
- Session Hijacking
- Name Server Corruption

MICHIGAN
STATE POLICE
MONITORS
CB CHANNEL 9

14

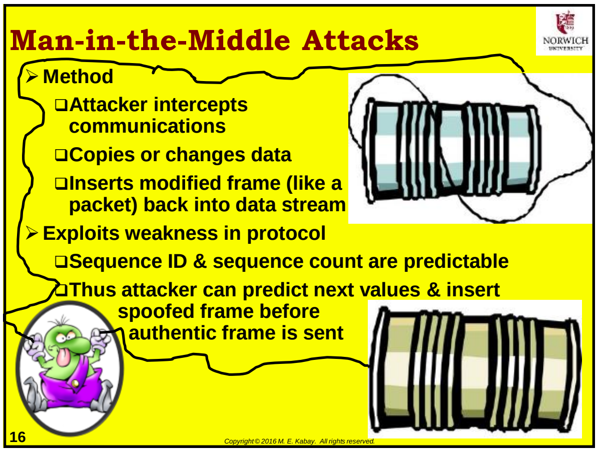


Introduction to Fiber (Fibre) Channel

- ANSI/INCTS* T11 Committee standard
  - ❑Optical fiber cabling; or
  - ❑Twisted-pair copper wiring
- Weaknesses
  - ❑All traffic is unencrypted
  - ❑No native support for authentication or data integrity checks
- Vulnerabilities
  - ❑Attackers can use IP-based attacks
  - ❑Cleartext traffic can be sniffed
  - ❑Message insertion (MITM) possible

*American National Standards Committee accredited International Committee for Information Technology Standards

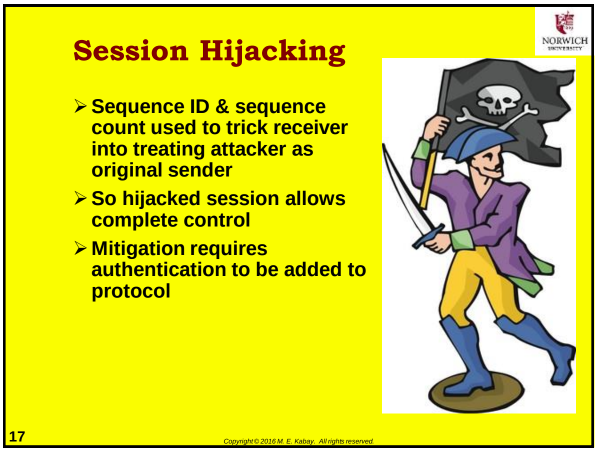
15



Man-in-the-Middle Attacks

- Method
  - ❑Attacker intercepts communications
  - ❑Copies or changes data
  - ❑Inserts modified frame (like a packet) back into data stream
- Exploits weakness in protocol
  - ❑Sequence ID & sequence count are predictable
  - ❑Thus attacker can predict next values & insert spoofed frame before authentic frame is sent

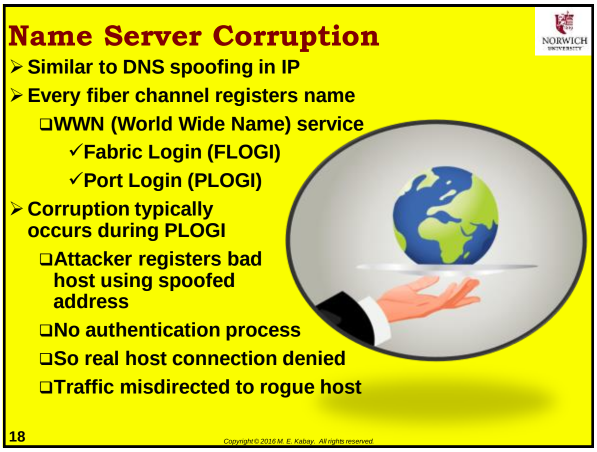
16



Session Hijacking

- Sequence ID & sequence count used to trick receiver into treating attacker as original sender
- So hijacked session allows complete control
- Mitigation requires authentication to be added to protocol

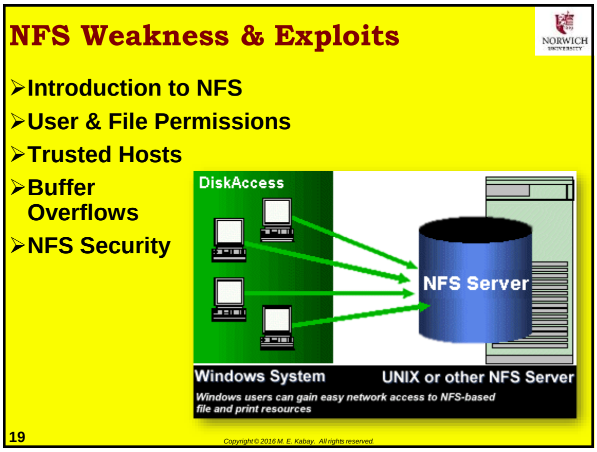
17



Name Server Corruption

- Similar to DNS spoofing in IP
- Every fiber channel registers name
  - ❑WWN (World Wide Name) service
    - ✓Fabric Login (FLOGI)
    - ✓Port Login (PLOGI)
- Corruption typically occurs during PLOGI
  - ❑Attacker registers bad host using spoofed address
  - ❑No authentication process
  - ❑So real host connection denied
  - ❑Traffic misdirected to rogue host

18

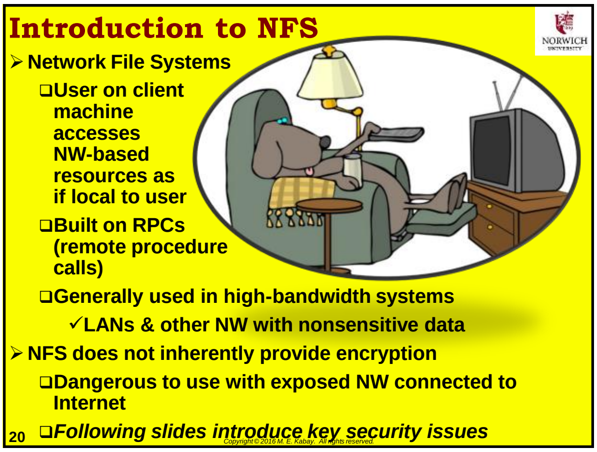


NFS Weakness & Exploits

- ➢Introduction to NFS
- ➢User & File Permissions
- ➢Trusted Hosts
- ➢Buffer Overflows
- ➢NFS Security

Windows users can gain easy network access to NFS-based file and print resources

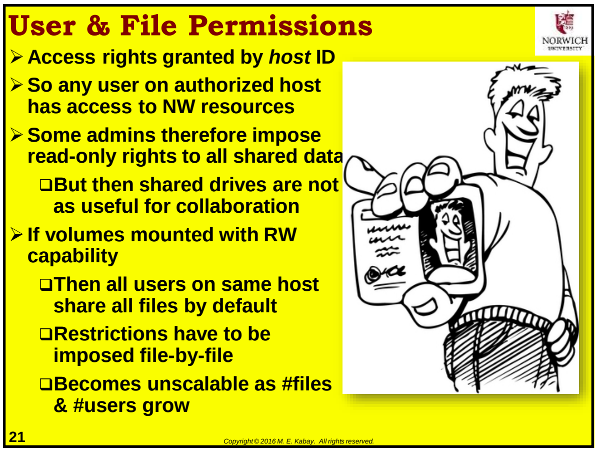
19



Introduction to NFS

- ➢ Network File Systems
  - ❑User on client machine accesses NW-based resources as if local to user
  - ❑Built on RPCs (remote procedure calls)
  - ❑Generally used in high-bandwidth systems
    - ✓LANs & other NW with nonsensitive data
- ➢ NFS does not inherently provide encryption
  - ❑Dangerous to use with exposed NW connected to Internet
  - ❑*Following slides introduce key security issues*

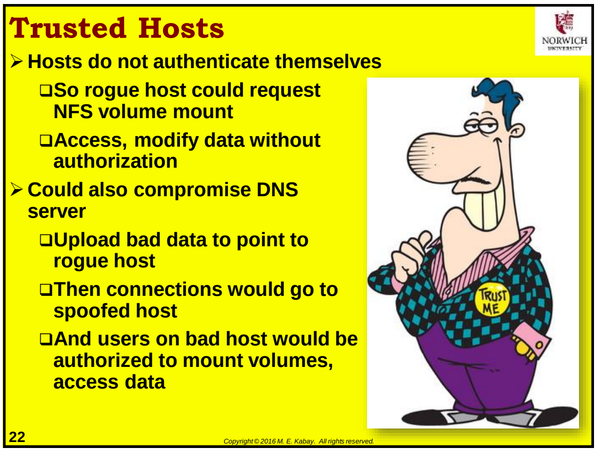
20



User & File Permissions

- ➢ Access rights granted by *host* ID
- ➢ So any user on authorized host has access to NW resources
- ➢ Some admins therefore impose read-only rights to all shared data
  - ❑But then shared drives are not as useful for collaboration
- ➢ If volumes mounted with RW capability
  - ❑Then all users on same host share all files by default
  - ❑Restrictions have to be imposed file-by-file
  - ❑Becomes unscalable as #files & #users grow

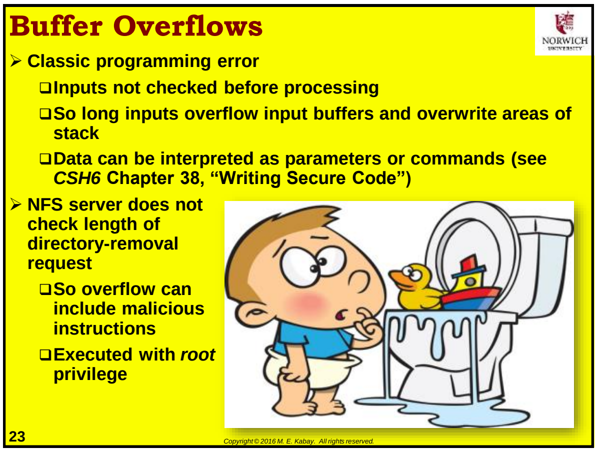
21



Trusted Hosts

- ➢ Hosts do not authenticate themselves
  - ❑So rogue host could request NFS volume mount
  - ❑Access, modify data without authorization
- ➢ Could also compromise DNS server
  - ❑Upload bad data to point to rogue host
  - ❑Then connections would go to spoofed host
  - ❑And users on bad host would be authorized to mount volumes, access data

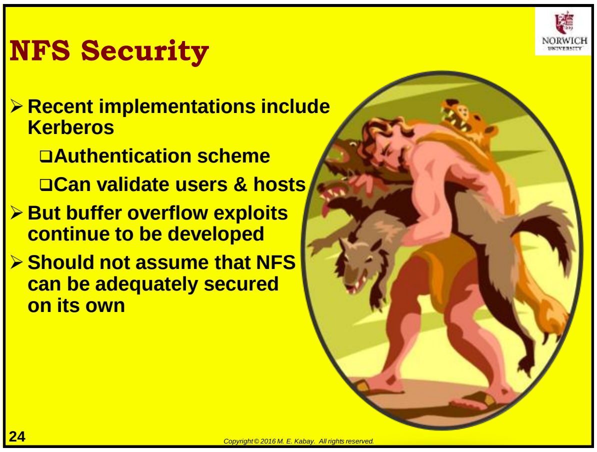
22



Buffer Overflows

- ➢ Classic programming error
  - ❑Inputs not checked before processing
  - ❑So long inputs overflow input buffers and overwrite areas of stack
  - ❑Data can be interpreted as parameters or commands (see *CSH6* Chapter 38, “Writing Secure Code”)
- ➢ NFS server does not check length of directory-removal request
  - ❑So overflow can include malicious instructions
  - ❑Executed with *root* privilege

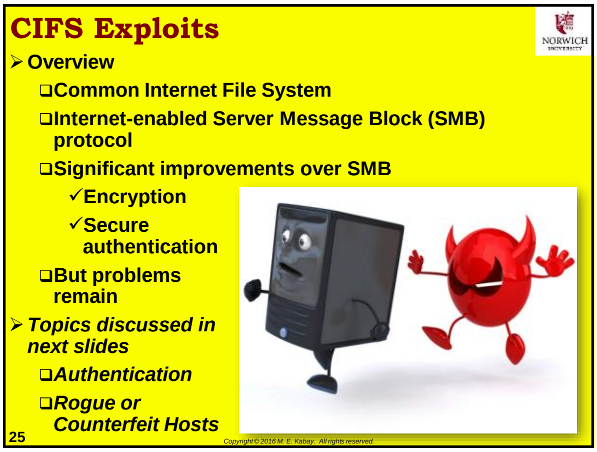
23



NFS Security

- ➢ Recent implementations include Kerberos
  - ❑Authentication scheme
  - ❑Can validate users & hosts
- ➢ But buffer overflow exploits continue to be developed
- ➢ Should not assume that NFS can be adequately secured on its own

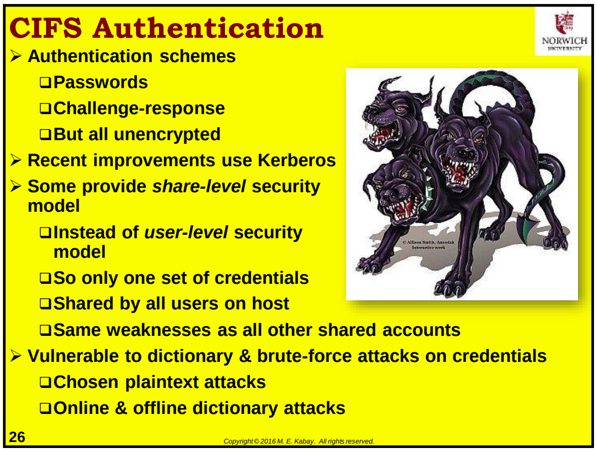
24



CIFS Exploits

- Overview
  - ❑Common Internet File System
  - ❑Internet-enabled Server Message Block (SMB) protocol
  - ❑Significant improvements over SMB
    - ✓Encryption
    - ✓Secure authentication
  - ❑But problems remain
- *Topics discussed in next slides*
  - ❑*Authentication*
  - ❑*Rogue or Counterfeit Hosts*

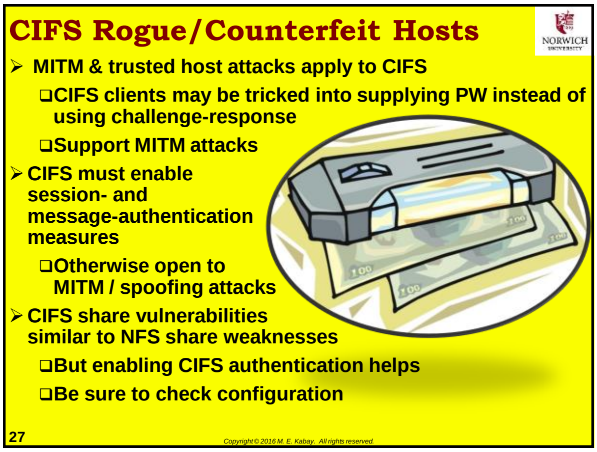
25



CIFS Authentication

- Authentication schemes
  - ❑Passwords
  - ❑Challenge-response
  - ❑But all unencrypted
- Recent improvements use Kerberos
- Some provide *share-level* security model
  - ❑Instead of *user-level* security model
  - ❑So only one set of credentials
  - ❑Shared by all users on host
  - ❑Same weaknesses as all other shared accounts
- Vulnerable to dictionary & brute-force attacks on credentials
  - ❑Chosen plaintext attacks
  - ❑Online & offline dictionary attacks

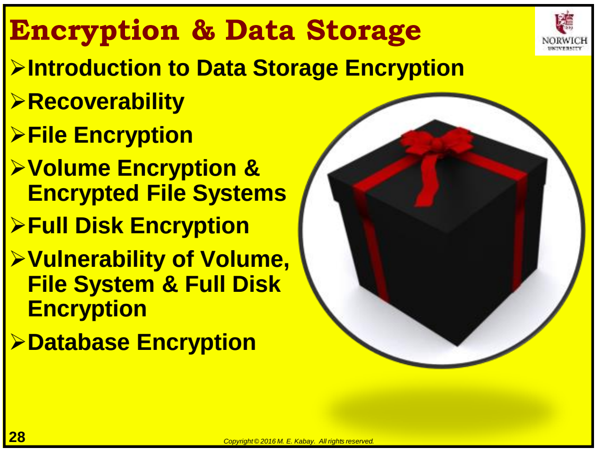
26



CIFS Rogue/Counterfeit Hosts

- MITM & trusted host attacks apply to CIFS
  - ❑CIFS clients may be tricked into supplying PW instead of using challenge-response
  - ❑Support MITM attacks
- CIFS must enable session- and message-authentication measures
  - ❑Otherwise open to MITM / spoofing attacks
- CIFS share vulnerabilities similar to NFS share weaknesses
  - ❑But enabling CIFS authentication helps
  - ❑Be sure to check configuration

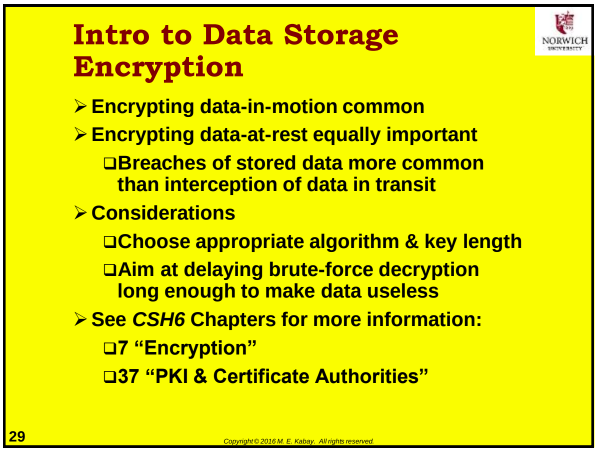
27



Encryption & Data Storage

- Introduction to Data Storage Encryption
- Recoverability
- File Encryption
- Volume Encryption & Encrypted File Systems
- Full Disk Encryption
- Vulnerability of Volume, File System & Full Disk Encryption
- Database Encryption

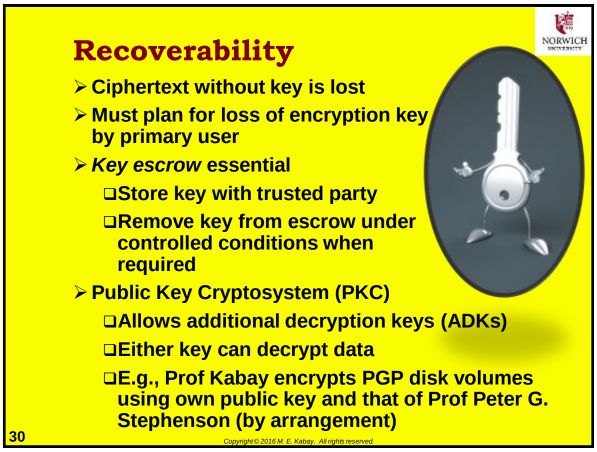
28



Intro to Data Storage Encryption

- Encrypting data-in-motion common
- Encrypting data-at-rest equally important
  - ❑Breaches of stored data more common than interception of data in transit
- Considerations
  - ❑Choose appropriate algorithm & key length
  - ❑Aim at delaying brute-force decryption long enough to make data useless
- See *CSH6* Chapters for more information:
  - ❑7 “Encryption”
  - ❑37 “PKI & Certificate Authorities”

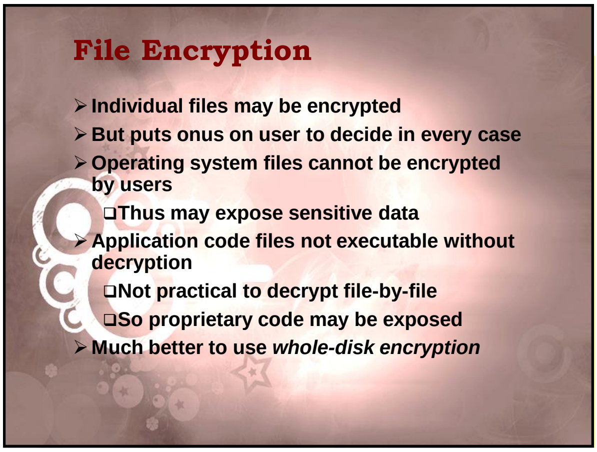
29



Recoverability

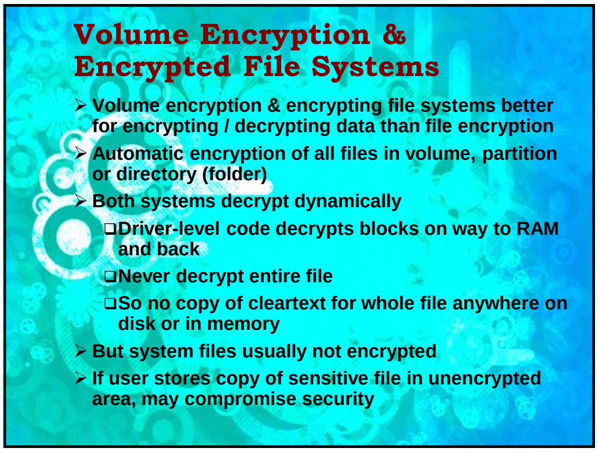
- Ciphertext without key is lost
- Must plan for loss of encryption key by primary user
- *Key escrow* essential
  - ❑Store key with trusted party
  - ❑Remove key from escrow under controlled conditions when required
- Public Key Cryptosystem (PKC)
  - ❑Allows additional decryption keys (ADKs)
  - ❑Either key can decrypt data
  - ❑E.g., Prof Kabay encrypts PGP disk volumes using own public key and that of Prof Peter G. Stephenson (by arrangement)

30



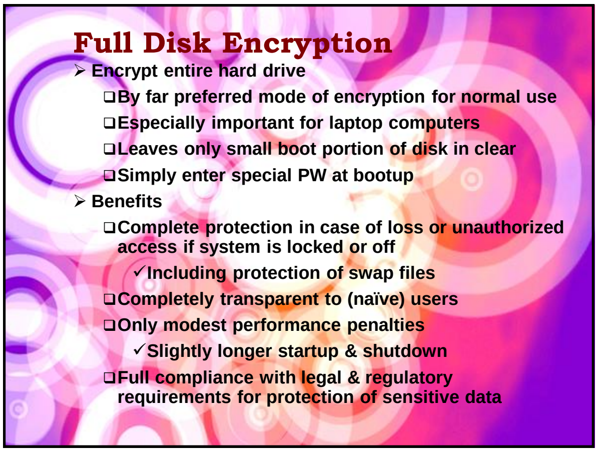
File Encryption

- ➢ Individual files may be encrypted
- ➢ But puts onus on user to decide in every case
- ➢ Operating system files cannot be encrypted by users
  - ❑ Thus may expose sensitive data
- ➢ Application code files not executable without decryption
  - ❑ Not practical to decrypt file-by-file
  - ❑ So proprietary code may be exposed
- ➢ Much better to use *whole-disk encryption*



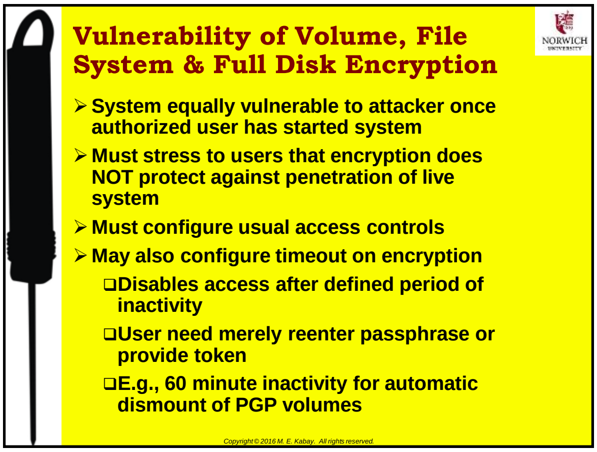
Volume Encryption & Encrypted File Systems

- ➢ Volume encryption & encrypting file systems better for encrypting / decrypting data than file encryption
- ➢ Automatic encryption of all files in volume, partition or directory (folder)
- ➢ Both systems decrypt dynamically
  - ❑ Driver-level code decrypts blocks on way to RAM and back
  - ❑ Never decrypt entire file
  - ❑ So no copy of cleartext for whole file anywhere on disk or in memory
- ➢ But system files usually not encrypted
- ➢ If user stores copy of sensitive file in unencrypted area, may compromise security



Full Disk Encryption

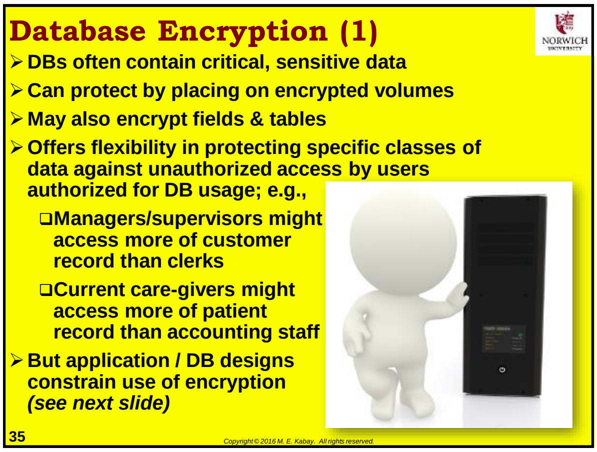
- ➢ Encrypt entire hard drive
  - ❑ By far preferred mode of encryption for normal use
  - ❑ Especially important for laptop computers
  - ❑ Leaves only small boot portion of disk in clear
  - ❑ Simply enter special PW at bootup
- ➢ Benefits
  - ❑ Complete protection in case of loss or unauthorized access if system is locked or off
    - ✓ Including protection of swap files
  - ❑ Completely transparent to (naïve) users
  - ❑ Only modest performance penalties
    - ✓ Slightly longer startup & shutdown
  - ❑ Full compliance with legal & regulatory requirements for protection of sensitive data



Vulnerability of Volume, File System & Full Disk Encryption

- ➢ System equally vulnerable to attacker once authorized user has started system
- ➢ Must stress to users that encryption does NOT protect against penetration of live system
- ➢ Must configure usual access controls
- ➢ May also configure timeout on encryption
  - ❑ Disables access after defined period of inactivity
  - ❑ User need merely reenter passphrase or provide token
  - ❑ E.g., 60 minute inactivity for automatic dismount of PGP volumes

Copyright © 2016 M. E. Kabay. All rights reserved.

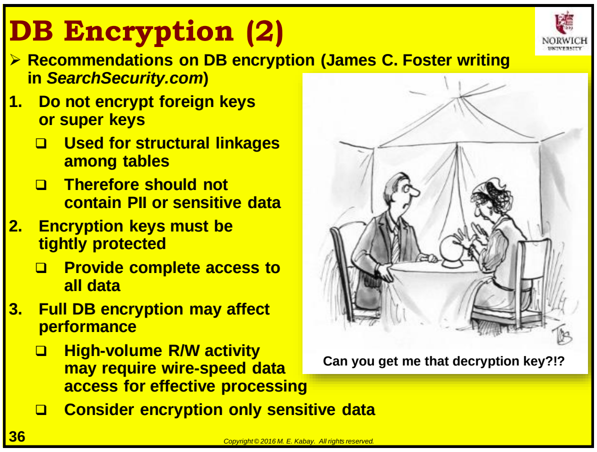


Database Encryption (1)

- ➢ DBs often contain critical, sensitive data
- ➢ Can protect by placing on encrypted volumes
- ➢ May also encrypt fields & tables
- ➢ Offers flexibility in protecting specific classes of data against unauthorized access by users authorized for DB usage; e.g.,
  - ❑ Managers/supervisors might access more of customer record than clerks
  - ❑ Current care-givers might access more of patient record than accounting staff
- ➢ But application / DB designs constrain use of encryption *(see next slide)*

35

Copyright © 2016 M. E. Kabay. All rights reserved.



DB Encryption (2)

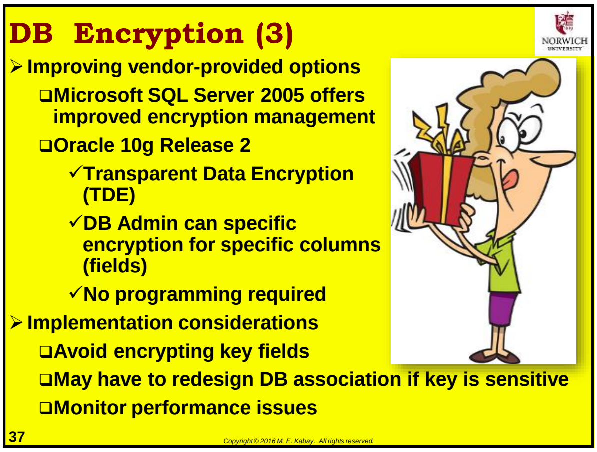
- ➢ Recommendations on DB encryption (James C. Foster writing in *SearchSecurity.com*)

1. Do not encrypt foreign keys or super keys
   - ❑ Used for structural linkages among tables
   - ❑ Therefore should not contain PII or sensitive data
2. Encryption keys must be tightly protected
   - ❑ Provide complete access to all data
3. Full DB encryption may affect performance
   - ❑ High-volume R/W activity may require wire-speed data access for effective processing
   - ❑ Consider encryption only sensitive data

Can you get me that decryption key?!?

36

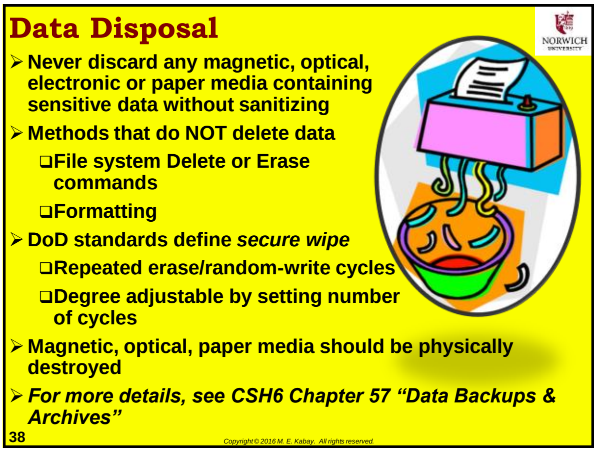
Copyright © 2016 M. E. Kabay. All rights reserved.



DB Encryption (3)

- ➢ Improving vendor-provided options
  - ❑Microsoft SQL Server 2005 offers improved encryption management
  - ❑Oracle 10g Release 2
    - ✓Transparent Data Encryption (TDE)
    - ✓DB Admin can specific encryption for specific columns (fields)
    - ✓No programming required
- ➢ Implementation considerations
  - ❑Avoid encrypting key fields
  - ❑May have to redesign DB association if key is sensitive
  - ❑Monitor performance issues

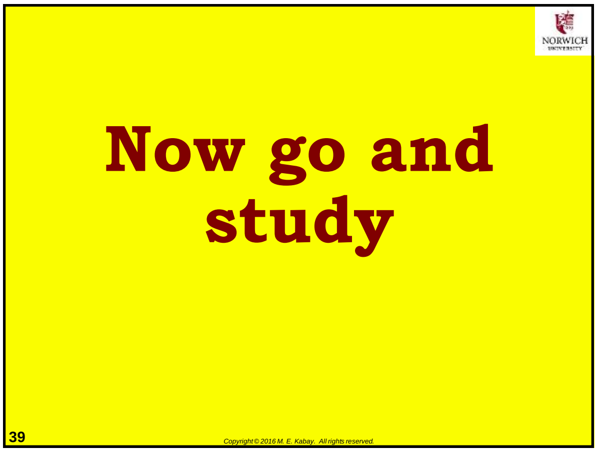
37



Data Disposal

- ➢ Never discard any magnetic, optical, electronic or paper media containing sensitive data without sanitizing
- ➢ Methods that do NOT delete data
  - ❑File system Delete or Erase commands
  - ❑Formatting
- ➢ DoD standards define *secure wipe*
  - ❑Repeated erase/random-write cycles
  - ❑Degree adjustable by setting number of cycles
- ➢ Magnetic, optical, paper media should be physically destroyed
- ➢ *For more details, see CSH6 Chapter 57 "Data Backups & Archives"*

38



Now go and study

39