CISSP® 2015

Domain 2: Asset Security

V1

Domain 2: Asset Security

- As rapid expansion of collection and storage -> increase importance of privacy considerations -> protecting controls
- Including
  - Information Classification,
  - Defining owner,
  - Protect Privacy,
  - Retention,
  - Data Security Control (at rest, in transit),
  - Handling (Markings, Labels, Storage, Destruction)

A. Classify information & supporting assets

- **Information Classification**
  - **Why**: assign different classification → assign different amount of funds and resources to protect.
  - **How**: define sensitivity scheme, identification, classification, controls (handling & procedure), audit,
  - Cost effective analysis
- **Table of example classification**
  - not too long list (suggest “Public”, “Internal”, Confidential” & “Strictly Confidential”)
  - Setup criteria parameter (eg. Usefulness, value, age, damage, legal…
  - including data, application, system,
  - including different format of data, eg. Disk, paper, video, fax, voice…..
- **Classification Controls**
  - procedure for proper classification program

Data Handling Requirements

	LEVEL I Low Sensitivity (Public Data)	LEVEL II Moderate Sensitivity (Non-Public/Internal Data)	LEVEL III High Sensitivity (Confidential/Restricted Data)
Mailing & Labels on Printed Reports	None	May be sent via Campus Mail; No labels required	Must be sent via Confidential envelope; Reports must be marked "Confidential"
Electronic Access	No controls	Role-based authorization	Individually authorized, with a confidentiality agreement
Physical Data/Media Storage	No special controls	Access Controlled area	Access controlled and monitored area
Electronic Communication	No special controls	Encryption recommended for external transmission	Encryption required for external transmission
Data Disposal	No controls	Recycle reports; Wipe/erase media	Shred reports; DOD-Level Wipe or destruction of electronic media

B. Determine & maintain ownership

- **Data Owner** (or information owner): usually in charge of a business unit and is responsible for the protection and use of specific subset of information.
  - Have to do data classification
  - ensuring necessary security controls are in place
  - approve of access, disclosure, backup requirement,
  - is not technical role, but business role
  - can delegates responsibility of day-to-day maintenance of the data protection mechanisms to **data custodian (usually IT or Security Dept.)**
- If more than one departments would like to own the information, have to set a criterion, say # of users, who contribute most? Who use?
- DO NOT assign multiple owners
- Similar concept apply to **System/Application owners**
- **Business/mission owners** are more on business side, say owning the operation, process, also access right and other protection.

Who is Custodian?

- **Data Custodian** (or information custodian):
  - Usually by IT or security department
  - Responsible for maintaining and protecting the data.
  - Including performing regular backup, periodically validating integrity, restore, retaining records of activity, follow security policy, standard….

Questions

Who has the primary responsibility of determining the classification level for information?

A. The functional manager

B. Senior management

C. The owner

D. The user

What should management consider the most when classifying data?

A. The type of employees, contractors, and customers who will be accessing the data

B. Availability, integrity, and confidentiality

C. Assessing the risk level and disabling countermeasures

D. The access controls that will be protecting the data

C. Protect Privacy (of Assets, Information)

- Worldwide issue, but in common:
  - Obtained fairly and **lawfully**
  - Used only for the original specified **purpose** (Example, not to give HR data to Credit Center)
  - Adequate, relevant and not excessive to **purpose**
  - Accurate and up to date
  - Accessible to the subject
  - Kept **secure**
  - **Destroyed** after its purpose is completed (say keep personal data for 3 months for the employment application if not employed)

C. Protect Privacy (of Assets, Information)

- Use layer defense approach, Layers are:
  1. **Data owners**: who should define protection requirement, at least complying the law (such as disclosure, access control, backup, BCP etc.), ensure these are in place…
  2. **Data processers**: including system, program, procedure which should provide various types of protections on data privacy (such as segregation of environment)
  3. **Collection limitation**: limits to the collection of personal data etc. which should be obtained by lawful and fair means and, with the knowledge or consent of the data subject.

Protect Privacy (of Assets, Information)

4. **Data remanence**: the residual physical representation of information
   - Including media repair & disposal, working paper, printout, temporary file, memory dump etc.
   - Controls:
     - Zeroization: overwriting with a pattern
     - Degaussing: magnetic scrambling
     - Destruction (shredding, crushing, burning)
     - Delete: only remove pointers

D. Ensure appropriate retention

- **General Steps:** involving Media, Hardware and Personnel
  1. Evaluate **Legal** requirement
  2. **Classify** types of records
  3. Determine **retention** period and **destruction** practices
  4. Draft and justify record retention **policy**
  5. **Train** staff
  6. **Audit** retention and destruction practices
  7. Periodically review & **update** policy
  8. Document policy, implementation, training and audits
- **Should not keep more than the retention requirement**

E. Determine Data Security controls

- Consider both data at rest, and data in transit
- **Data at rest**
  - **Examples:** data storage, Backup tapes, off-site storage, password files etc.
  - **Control**: Encryption, password complexity etc.
- **Data in Transit**
  - **Risk:** unauthorized intercept or monitor plaintext data across an unencrypted network
  - **Control:** Encryption but consider every part of network, client to server, server to server and server to client.
  - **Examples** of insecure network protocols and their secure alternatives

Action	*Instead of this ...*	*Use these ...*
Web Access	HTTP	HTTPS
File Transfer	FTP, RCP	FTPS, SFTP, SCP
Remote Shell	telnet	SSH3
Remote Desktop	VNC	radmin, RDP

Link Encryption vs. End-to-End Encryption

- **Link encryption:** Encrypts **all the data** along a specific communication path such as T1 etc. not only user information, but header, trailer address, routing data. Usually provided by service provider
- **End-to-End Encryption**: Encrypt **user information**, but not headers, address, routing and trailer, Usually initiated by user, more flexible, eg. Email encryption.

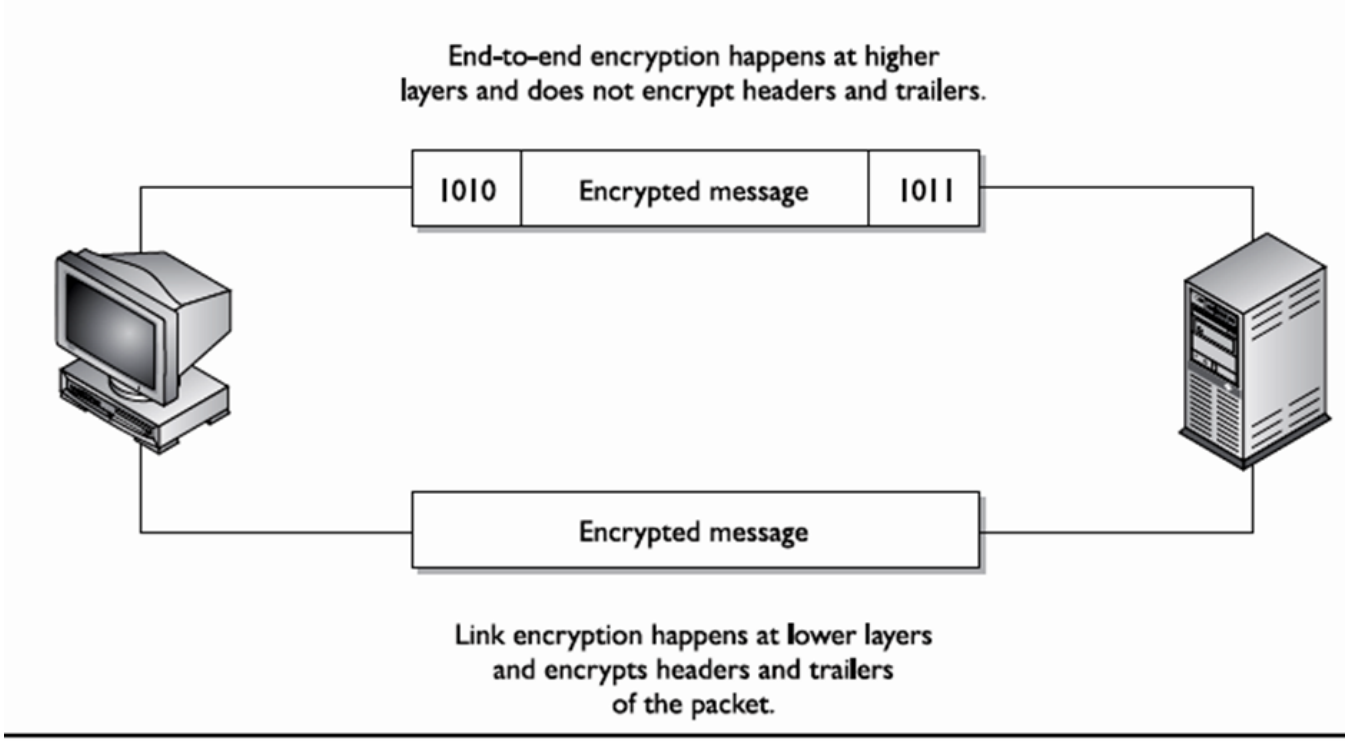

Figure 8-24 Link and end-to-end encryption happen at different OSI layers.

E. Determine Data Security controls

- **Baselines**:
  - Define a set of minimum security requirement, (say, backup requirement, encryption etc.)
  - Open question: can the whole organization use one baseline? Say same password length for all systems.
- **Scoping and tailoring**:
  - Use well-developed standard (or baseline) to avoid unnecessary and costly duplication of effort. However, scoping and tailoring are required.
  - **Scoping**: specific terms and conditions on applicability and implementation
  - **Tailoring**: to more closely match the characteristics of the information system & environment of operation.

E. Determine Data Security controls

- **Standards selection**:
  - CISSP needs to be familiar with a wide range of standards and the organizations. Here are a list standards.
    - **NIST Special Report 800-53** (National Institute of Standards and technology)
    - **FIPS 199** (Federal Information Processing Standard)
    - **Federal Information Security Management Act**
    - **ISO 27002** (International Organization for Standardization)