The Parkerian Hexad

CSH6 Chapter 3

"Toward a New Framework for Information Security"

Donn B. Parker

Copyright © 2014 M. E. Kabay. All rights reserved.

Topics

- The Classic Triad
- Parkerian Hexad
  - Confidentiality
  - Possession
  - Integrity
  - Authenticity
  - Availability
  - Utility
- Functions of INFOSEC Personnel

CSH6 Ch 3

Copyright © 2014 M. E. Kabay. All rights reserved.

The Classic Triad

"I would say that Vulnerability would be a frequently involved given the context of the incidents. Most incidents take advantage of how certain systems are designed, implemented, and/or how a system may be configured."

C – I – A

Copyright © 2014 M. E. Kabay. All rights reserved.

The Parkerian Hexad

Protect the 6 atomic elements of INFOSEC:

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

Copyright © 2014 M. E. Kabay. All rights reserved.

Why "Parkerian?"

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

Copyright © 2014 M. E. Kabay. All rights reserved.

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

Copyright © 2014 M. E. Kabay. All rights reserved.

Confidentiality & Possession Losses

- Locating
- Disclosing
- Observing, monitoring, and acquiring
- Copying
- Taking or controlling
- Claiming ownership or custodianship
- Inferring
- Exposing to all of the other losses
- Endangering by exposing to any of the other losses
- Failure to engage in or to allow any of the other losses to occur when instructed to do so

Copyright © 2014 M. E. Kabay. All rights reserved.

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

Copyright © 2014 M. E. Kabay. All rights reserved.

Integrity: JIT Comment

I would think that Integrity is most frequently involved in a security incident. If your software is tampered with or if your server is hacked into it automatically loses integrity even if nothing was changed. Integrity is very fragile.

Copyright © 2014 M. E. Kabay. All rights reserved.

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

Copyright © 2014 M. E. Kabay. All rights reserved.

Integrity & Authenticity Losses

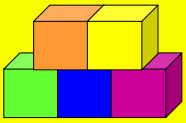
- Insertion, use, or production of false or unacceptable data
- Modification, replacement, removal, appending, aggregating, separating, or reordering
- Misrepresentation
- Repudiation (rejecting as untrue)
- Misuse or failure to use as required

Copyright © 2014 M. E. Kabay. All rights reserved.

Availability

Timely access to data

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



Copyright © 2014 M. E. Kabay. All rights reserved.

Availability: JIT Comment

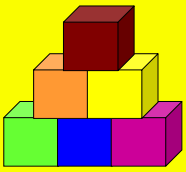
Availability seems to be the number one contender. A company many times are required to allow employees access into the company network and database so that they may be able to accomplish their everyday tasks. This is not for a lack of control by the company but out of production necessity. Therefore this scenario is most likely to be exploited due to availability.

Copyright © 2014 M. E. Kabay. All rights reserved.

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



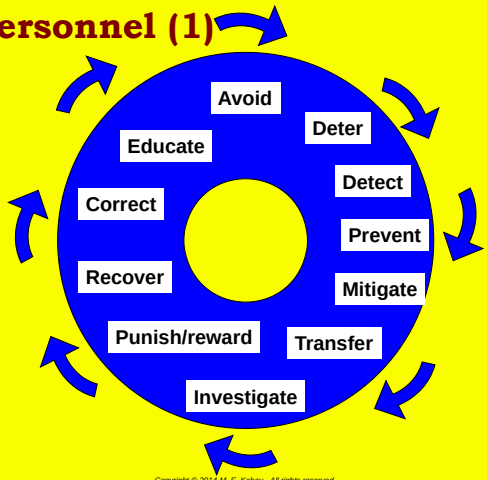
Copyright © 2014 M. E. Kabay. All rights reserved.

Availability & Utility Losses

- Destruction , damage, or contamination
- Denial, prolongation, acceleration, or delay in use or acquisition
- Movement or misplacement
- Conversion or obscuration

Copyright © 2014 M. E. Kabay. All rights reserved.

Functions of INFOSEC Personnel (1)



Copyright © 2014 M. E. Kabay. All rights reserved.

Functions of INFOSEC Personnel (2)

- Avoidance: e.g., prevent vulnerabilities and exposures
- Deterrence: make attack less likely
- Detection: quickly spot attack
- Prevention: prevent exploit
- Mitigation: reduce damage
- Transference: shift control for resolution

Copyright © 2014 M. E. Kabay. All rights reserved.

Functions of INFOSEC Personnel (3)

- Investigation: characterize incident
- Sanctions & rewards: punish guilty, encourage effective responders
- Recovery: immediate response, repair
- Correction: never again
- Education: advance knowledge and teach others

Copyright © 2014 M. E. Kabay. All rights reserved.

Now go and study

Copyright © 2014 M. E. Kabay. All rights reserved.