Lesson 4 – Risk analysis

Authentication review

- Authentication is the process by which the information system assures that you are who you say you are; how you prove your identity is authentic.
- Methods of performing authentication are:
  - user ID and passwords. The system compares the given password with a stored password. If the two passwords match then the user is authentic.
  - Swipe card, which has a magnetic strip embedded, which would already contain your details, so that no physical data entry takes place or just a PIN is entered.
  - digital certificate, an encrypted piece of data which contains information about its owner, creator, generation and expiration dates, and other data to uniquely identify a user.
  - key fob, small electronic devices which generate a new random password synchronized to the main computer
  - Biometrics - retinal scanners and fingerprint readers. Parts of the body are considered unique enough to allow authentication to computer systems based one their properties.
- For a very secure environment, it is also possible to combine several of these options, such as by having fingerprint identification along with user ID and key fob.

Types of authentication

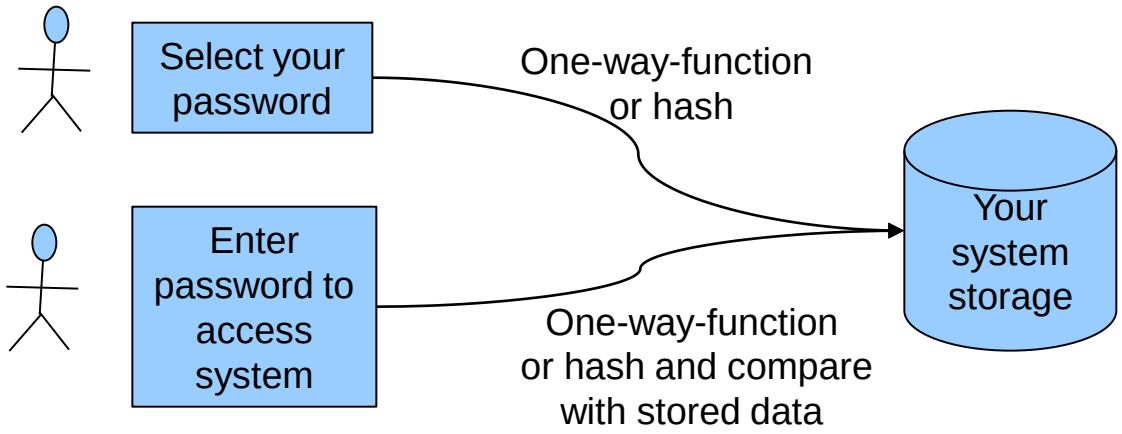
- Based on something the user **knows**
  - Password, passphrase, key
  - Personal Identification Number (PIN)
- Based on something the user **possesses**
  - Debit card, token
  - Car-door key
- Based on something the use **is (Biometrics)**
  - Voice, hand writing
  - Finger print

Passwords or passphrase versus keys

- Cryptographic algorithms use keys not passwords or passphrases
- Key may be derived from a passwords or passphrases
- Keys are normally 2^nbits length (64, 128, 256)
  - A 64bits length key has 2^{64} possible keys
- Never use a password or passphrase as a key
  - Bad idea, because makes the key easy to figure out
  - A 64bit key has same length as 8 ASCII chars
    - The most common ASCII chars are letters, numbers, and some special chars. Which can be encoded in around 4 bits. Therefore, your key became 32bit long (which is half of the original 64bits)

Designing password based systems

- Never store the passwords in your system
- Use one-way-functions or hashes and store the result
- Never give information on authentication failures
  - For example: “password error”, instead say “authentication error”
- Make your users change password frequently



- The quality of passwords and keys is very important in a cryptosystem
  - Weak keys undermine strong algorithms

Risk analysis

Risk management process

1. Define the Scope and Boundary and Methodology
2. Identify and Value Assets,
3. Identify Threats and Determine Likelihood,
4. Measure Risk,
5. Select Appropriate Safeguards,
6. Implement and Test Safeguards,
7. Accept Residual Risk.

Risk impact matrix

- Risk impact matrixes are easy to understand
- Columns represent severity of a security incident
- Rows represent the affected area

Domain	1 Insignificant	2 Minor	3 Moderate	4 Major	5 Catastrophic
Customer					
Reputation					
Financial					
Legal					
Data					
Technology					

Risk impact matrix example

	1	2	3	4	5
Descriptor	**Insignificant**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Objectives/Projects	Insignificant cost increase/schedule slippage. Barely noticeable reduction in scope or quality	<5% over budget/ schedule slippage. Minor reduction in quality/scope	5-10% over budget/schedule slippage. Reduction in scope or quality.	10-25% over budget/schedule slippage. Failure to meet secondary objectives.	>25% over budget/ schedule slippage. Doesn't meet primary objectives.
Injury (Physical/Psychological)	No apparent injury or minor injury not requiring first aid.	Minor injury or illness requiring first aid treatment.	RIDDOR/NPSA reportable	Major injury, or long term incapacity/ disability (loss of limb)	Death or major permanent incapacity
Patient Experience/Outcome	Unsatisfactory patient experience not directly related to patient care	Unsatisfactory patient experience – readily resolved	Mismanagement of patient care, short term effects (less than a week)	Serious mismanagement of patient care, long term effects (more than a week)	Totally unsatisfactory patient outcome or experience
Complaints/Claims	Locally resolved complaint	Justified complaint peripheral to clinical care	Below excess claim. Justified complaint involving lack of appropriate care.	Claim above excess level. Justified multiple complaints.	Multiple claims or single major claim

Likelihood Score

- Likelihood Scores indicates how often an incident is expected
- Should be based on probability or frequency

Likelihood Score	Description
1 - Rare	The event may never occur. The event is not expected for years.
2 - Unlikely	The event is not expected, but it may happen. Expected at least yearly.
3 - Possible	The event will occasionally happen. Expected at least every semester.
4 - Likely	The event will probably happen. Expected at least monthly.
5 - Almost certain	The event will certainly happen. Expected at least weekly.

5x5 Risk scoring matrix

- Columns correspond to risk-impact scores
- Rows correspond to likelihood scores
- The risk score is calculated by multiplying the column impact score with the row likelihood score

	1 - Rare	2 - Unlikely	3 - Possible	4 - Likely	5 - Almost certain
1 - Insignificant	1	2	3	4	5
2 - Minor	2	4	6	8	10
3 - Moderate	3	6	9	12	15
4 - Major	4	8	12	16	20
5 - Catastrophic	5	10	15	20	25

5x5 Risk scoring matrix example

	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

Mitigation/Action matrix

- Describes what to do when a security incident occurs
- Scores come from the 5x5 risk scoring matrix
- Risk is a categorization of the scores

Score	Risk	Mitigation and action
1 - 3	Low	
4 - 6	Moderate	
8 - 12	High	
15 - 25	Extreme	.

Mitigation/Action matrix example

Score	Risk	Actions	Reporting Requirements
1-3	Low	Where appropriate carry out local investigation for low risk incidents. Local managers would be expected to monitor trends associated with this grade of incident and identify where causal factors are generic to the service/area and take appropriate action to address any local systems failures. Any identified low level risks should be managed through existing control measures and assessments kept under review.	Report to manager/supervisor of the area in which the accident/incident occurred or where the risk has been identified.
4-6	Moderate	Investigate to determine underlying causes. Where appropriate review any existing risk assessment and consider the effectiveness of the controls. Implement any further treatment plans as required.	Report to manager/supervisor of the area in which the accident/incident occurred or where the risk has been identified.
8-12	High	**Make safe the situation**. Carry out a full RCA. Action plans to be developed, implemented and monitored. Where a high level risk is identified review effectiveness of existing controls. If adequate control cannot be implemented immediately, an action plan must be developed to indicate how the risk will be reduced, who will be responsible for implementation and the time-scale involved.	**Report immediately** to the appropriate Director/Senior Manager. (See Incident Reporting Policy) Enter onto Corporate Risk Register
15-25	Extreme	**STOP activity and make safe the situation.** Immediate action must be taken to either eliminate or adequately control the risk before any further activity is undertaken. Carry out a full RCA and where appropriate develop, implement and monitor further action plans.	**Report immediately** to the appropriate Director/Senior Manager. (See Incident Reporting Policy) Report to Trust Board. Enter onto Corporate Risk Register

Assignment 4

- Read Weller chapter 2 (The Internet Bookstore - a case study)
- Using the attached word template,
  - develop an action mitigation plan for the Internet Bookstore, by creating the risk impact matrix, likelihood score matrix, 5x5 Risk scoring matrix, and finally the mitigation action matrix
  - Be sure to
    - replace with your own text all the notes enclosed in <>
    - Fill all the cells in the matrixes
  - Feel free to modify the document as you see fit
- In the risk impact matrix, be sure to include the customer, the bookstore, the bank, and the courier as affected areas (domains)
- Note: There were no Assignment 3

The End