Authentication Technologies

The aim of this session is to provide a further exploration of the issues surrounding the effective use of authentication technologies.

Task 1: Evaluating Website Password Meters

An increasing number of websites are now incorporating password meters in order to assist users in selecting good passwords. Your task in this session is to explore and evaluate the use of these meters, and to determine how effective they are in practical terms.

1. Identify 4 websites that use password meters as part of their user registration process.

2. Examine how the password meters actually work by trying them out with a series of test passwords (e.g. how many levels are there, and what are the criteria for the different strengths of score).

3. Consider how well the meters have been realised. For example:

    - Do the ratings that they give align with your understanding of good password practice (e.g. in terms of password length, composition etc).
    - Are the meters explained on the site and/or are users provided with suitable tips and advice that they could follow in order to select a password that would be rated strongly. Is it clear what is actually being rated?
    - Do the password meters give good ratings to obviously poor choices (e.g. the word 'password', passwords that include the user's name).

4. Draw up a comparison of the sites based upon a comparison of your findings. Share the results on Menti.

Task 2: Developing your own criteria

What would be your approach if your were implementing a password meter of your own? Can you specify the criteria that you would use in order to award different levels) of rating?

Task 3: Weaknesses of Token-Based Technologies

Token-based technologies have a variety of applications in physical and logical access systems including:

- PC-based login (e.g. YubiKey, RSA SecurID)
- Physical door access (e.g. Yale Keyless)
- Remote Central Locking of Cars (e.g. Land Rover, Mercedes)

- Transport (e.g. Oyster Card)
- Finance (e.g. Debit/Credit Cards)

Perform a quick examination looking at published vulnerabilities of these systems? Share your findings within on Menti

Task 4: Exploring trade-offs in biometric modalities

Biometric technologies offer the opportunity of achieving both security and usability. However, in practice, they introduce a wider range of variables that need to be considered in order for the technology to be viable.

As highlighted, key considerations include:

- Uniqueness
- Universal
- Permanence
- Collectable
- Acceptable
- Circumventable

With respect to the following applications, please recommend, with a supporting rationale, which biometric modality would be most suitable?

1. Construction Industry – access to a site
2. Border control – for use in airports to enter a country
3. Mobile Phone – for access to the device and services
4. Work computer – for continued access to organizational resources
5. Surveillance – use of CCTV in scenarios such as airports and concerts

Use Menti to share your recommendations.

Task 5: Ideal solution to authentication?

Having understood the pro's and con's of differing approaches, please share your thoughts on:

- One technique that you would be most happy to use
- One technique that you would least want to use