Practical 10 – Continuous Authentication

Ole André Hauge

April 11, 2021

CA System

1. We discussed how a CA system is designed.

   (a) 2 points Give pros and cons of an enrollment phase of 1 day?

   Answer: As I understand the question, we are looking at the pros and cons of using one day for enrollment of a user, which means that we will be able to, fairly quickly, collect and create a template reference consisting of the person's behavior. This reference template can then be used for CA and the user will be able to use the system knowing that imposters will be detected with a high probability. However, by only spending one day to enroll the user we risk restricting the user's behavior, hence creating a reference template (can be multiple, but for the simplicity of the explanation I will stay with one) that does not represent the behaviors of that users well enough. This is because the user that is being enrolled might not use all the applications or actions like copying text and printing documents, thus not being given enough time to provide sufficient variety of data.

   The result of this might be that the genuine user is locked out more often and/or that an impostor is believed to be a genuine user more often, than what would be the case if the enrollment phase is well thought through. In conclusion, there is an obvious balance between too long and too short of time spent during enrollment, and this balance needs to be kept in mind by the system administrator.

   (b) 2 points What are the 2 decision stages in a CA system?

   Answer: Here I assume that the question referrers to the two steps of the decision model as it was discussed in the presentation, which means that we are looking at what is done in the system after the score calculation where the probe is checked against reference template:

   The first stage is where the trust level of the system is adjusted based on the resulting score of the previous phase. This is done to add a better nuance of the decisions so that a genuine user's genuine mistakes or erroneous behavior does not result in him being locked out. It is implemented in such a way that the trust level will decrease over time depending on the number of errors/deviations from the reference template, thus an impostor will cause the score to drop faster than a genuine user as he is prone to deviate from the genuine user's behavior.

   The second stage uses the adjusted trust level to decide on whether the user can continue to work or if he is going to be locked out. This means that an impostor's low trust level will be detected and result in him being locked out more often than a genuine user would by committing errors.

Performance Analysis

2. Performance for a CA system is given in ANIA and ANGA.

   (a) 1 point What does ANIA mean?

   Answer: ANIA is an abbreviation for the *average number of impostor actions*, which is a measurement that shows the average number of actions an impostor can do compared to the reference of a genuine user. Or in simpler terms: imposters are identified based on how often their behavior deviates from a genuine user reference. The score should be as low as possible for a CA system, but as will be discussed in the next question, a relationship between ANIA and ANGA exists.

   (b) 2 points If I increase the (global) lockout threshold, what would that do to ANIA and to ANGA?

   Answer: If we increase the lockout threshold, we will get a lower ANIA value, meaning that imposters will be locked out more often, but this also means that the value of ANGA will increase so the number of genuine users that are locked out will also increase.

   We can only improve either ANIA or ANGA, not both, by adjusting the threshold.

Continuous Identification

3. CI is a way to identify an impostor after he/she is detected by a a CA system.

   (a) 3 points Describe why CA and CI work against each other?

   Answer: CI is used after an impostor has been detected to identify the impostor, and its performance depends on the amount of data the system has on that user. As CA aims to detect and lockout impostors (session highjacker) as quickly as possible, this creates an inherent conflict between the two. If CA locks out the impostor too fast CI will not have enough data to identify him. We, therefore, have to figure out if we want to lock out the user as quickly as possible or be more lenient to collect more data of the impostor before locking him out e.g. we need to find a balance between the security provided by locking out the impostor vs. data collection to be able to identify the impostor. This is something the system administrator has to be aware of.