Aalto special assignment topic proposals

Zero-effort authentication in an industrial control room

Background

Control rooms of industrial control systems are collaboration spaces where operators work together to monitor, troubleshoot and improve the process of an industrial plant. In the future, control rooms will take advantage of emerging user interface technologies such as augmented reality, speech and gesture control. Computers, phones, tablets and info screens can all be used to control the plant. An illustration of future control rooms can be seen in the video [1], which is a result from FIMECC research program User Experience & Usability in complex Systems (UXUS). UXUS created new interaction concepts and innovative practices in developing the user and customer experience.

As shown in the video, access control is an essential feature of a control system. Authorization checks must be performed on every operation, and all user actions are recorded in an audit trail. Because the work context is shared, sessions can be handed over between users for instance when the work shift changes or users simply changes places. However, authentication and unauthentication should be convenient, or even seamless for the end user.

Due to the nature of the automation systems, dependability and availability of the system is the most important security objective. Therefore, the availability and reliability of the authentication and unauthentication mechanism is very important.

Industrial plants employ multiple levels of defense, including perimeter security. Improper authentication and unauthentication by friendly, non-malicious users is likely to be a more relevant threat than malicious attacks. However, control systems can also be used in distributed environments with a lower level of physical security.

Goals

- Summary of known zero-effort authentication and unauthentication techniques and previous research
- Analysis of the applicability of these techniques in industrial control systems
- Comparison and discussion on alternative convenient (un)authentication techniques that require some user effort
- Threat models of the solutions that take into account the dependability requirements that are typical for industrial control systems

Requirements

- Knowledge of different authentication and unauthentication mechanisms and zero-effort (un)authentication

More information

More information is available from jouni.ruotsalainen@valmet.com and henry.haverinen@valmetpartners.com

References

[1] A day at a future plant, YouTube video https://www.youtube.com/watch?v=kgLiCR6jCf0