Usable security for control systems

Jun Ho Huh
Honeywell ACS Labs, research scientist
junho.huh@honeywell.com

Honeywell

What is usable security?

- Building security solutions that are *intuitive* and *easy to use*
  - Many security architects do not consider usability tradeoffs and implications
  - Do not know how to measure and balance the security and usability tradeoffs
- Improving usability of existing security solutions without compromising too much security
- Designing security based on understanding of users' mental models, perceptions, capabilities, and technological gaps
- The usable security community is actively investigating topics like usable authentication, privacy, security perceptions/experiences in different countries, security for minority groups, and so on.

What is the current status of usable security for control systems?

Security mechanisms for control systems are often designed without much consideration of usability implications

Security architects often don't understand operators' security awareness levels, expectations, preferences, and capabilities in using security mechanisms

The usable security community isn't really looking into this space…

Result: Control systems are often equipped with tedious security mechanisms that are hard to use

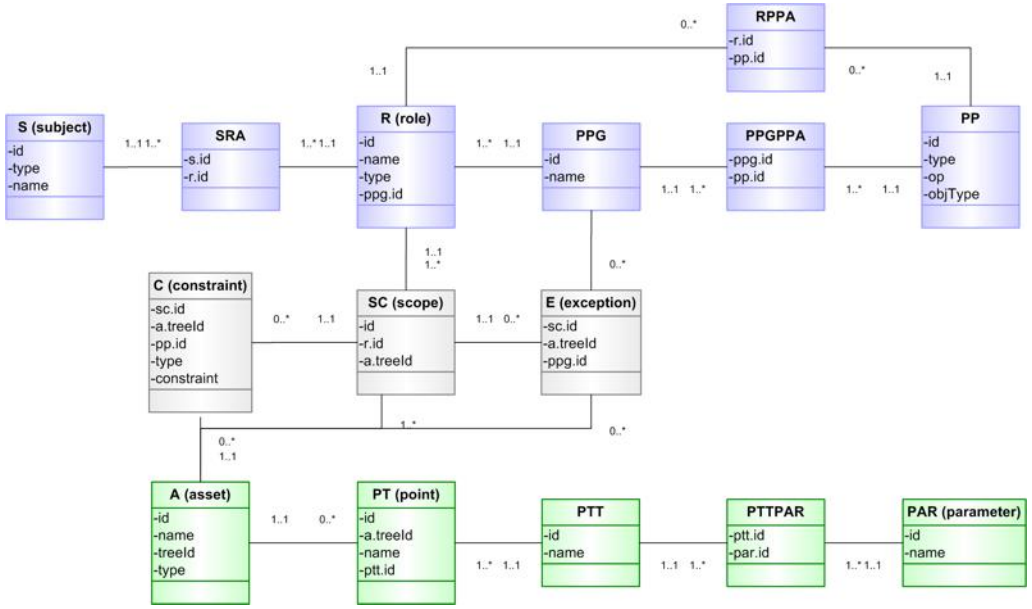
Having received numerous user experience complaints from customers, management folks have tendency to pushback security mechanisms that may significantly hinder daily operations of operators

RBAC project experiences

- In 2011, Honeywell worked with UIUC on a DOE-funded project to design an role-based access control (RBAC) system for distributed control systems (DCS)

- Designed an RBAC model fully tailored to DCS requirements
  - capable of capturing complex RBAC policies
  - e.g., temporal constraints, environmental attributes, role templates

- Designed an UI for managing complex RBAC policies



Strong pushback to deploy the new RBAC model because it was too complicated for DCS admins and operators to understand and use

Issue 1: Authentication for controllers

- Field operators often manage tens or sometimes hundreds of controllers across multiple building sites
  - A separate user account needs to be created for each controller
  - *Operators end up managing tens or hundreds of passwords*
  - Often use the same password across all controllers
  - Sometimes share the password with other operators
- Periodically changing a lot of passwords is cumbersome
- For admins, managing user accounts is difficult
  - e.g., deleting user accounts, assigning permissions to users, proper auditing is infeasible when operators share accounts, etc.
- Possible directions: Single sign-on (SSO), one-time passwords (OTP), and biometric authentication

Issue 2: Cybersecurity dashboards

- Existing research on intrusion detection for control systems primarily focus on advancing intrusion/anomaly detection engines
  - Designing new detection algorithms
  - Improving detection performance

- *How do we present the information about the detected events?*
  - Operators are non-experts
  - Existing warning systems are often *not intuitive* and *hard to use*
  - Not enough research is being done in this area

- Intuitive dashboards need to be designed to help operators easily understand detected cyber events, and quickly take desirable actions
  - Design based on the understanding of operators' security awareness levels, expectations, preferences, and capabilities
  - Conduct user studies to evaluate intuitiveness and ease of use