Prevent Malicious Controller in a Physical, Human and Cyber Triad

Depeng Li
Department of Information and Computer Science,
University of Hawaii at Manoa, Honolulu, Hawaii, USA
depengli@hawaii.edu

I. Introduction and Related Works

Gone are those simple days when cyber-attacks are not introduced to our physical world, the malfunction of a control system is treated as pure device failures, and the control system rarely threats customers' safety in an active way. Malaysia Airlines flight MH370, for example, disappeared carrying more than 200 persons on March 8, 2014. Explanations do not reach an agreement ranging from mishandling of a suicidal pilot to cyber-attacks [1].

As a matter of fact, current control systems are vulnerable to potential attacks: military robots may rebel their human masters [2], hackers can manipulate modern automobiles or unmanned military aerial drones from a variety of attack surfaces [3], [4], and India blackout 2012 is partially resulted from misoperations of the protection system of electric grid [5]. The recent evidences in misbehavior activities covers all possible aspects of Physical, Human and Cyber (Phc) [2], [3], [4], [5].

Objective and Contributions: The *problem* we endeavor to solve is that, when malicious controllers are trying to take it over, can we train electronic control systems to choose the right from wrong? The *goal* of this paper is the development of an innovative framework for protecting control systems against malicious operations. Our objective is not to completely eliminate the attack, but rather to mitigate the risk resulted from misbehaviors.

Related works: In [6], a cyber-physical-social based security architecture (namely, IPM) is proposed but how to prevent the malicious activities in Phc triad over the control system and how to withdraw the access right from misbehavior controllers have not been studied.

II. Proposed Solution

Physical, Human and Cyber (Phc) triad: It is possible that the control system falls to the wrong hand [1]: human operators can act maliciously, automation control systems can be infected or may be born with vulnerabilities, and remote access through cyber channels can be compromised. Here, we propose a new *Physical-Human-Cyber* (Phc) triad system (Fig. 1) which is comprised of three types of controllers (*sketched as circles*) and a control system (*sketched as rectangles*). Instances of the latter can be aircrafts, modern vehicles, drones, unmanned robots, etc.

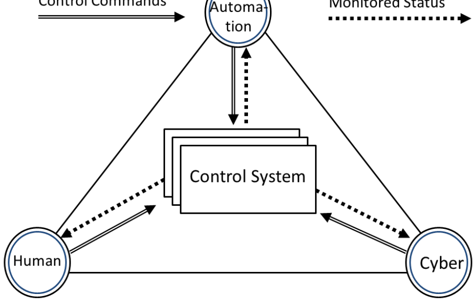

Figure. 1 Physical, Human and Cyber (Phc) Triad

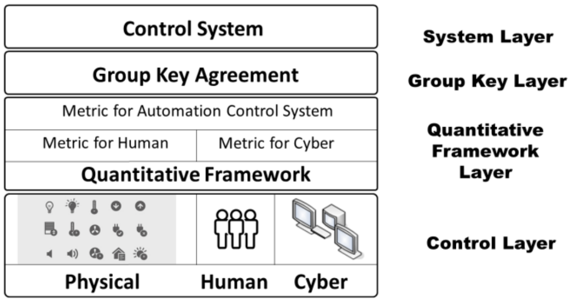

Figure 2. Architecture of our System

Architecture: our architecture (Fig. 2) includes four layers: in the controller layer, control commands are issued by physical, human and cyber remote access controllers. In the quantitative framework layer, a set of metric is established to evaluate the data captured in the controller layer for each controller in Phc triad, including *human operator guide* [6], *reputation of hosts* [7], and *Cyber-Physical Systems* [8]. Each controller instance's metric indicator decides whether the controller instance is malicious or not. In the group key layer, the malicious controller instance will be expelled from the group key agreement [9] in such a way that a new group key is generated and the expelled group member has no chance to access the new group key and therefore cannot send its control commands to the control system. In the control system layer, the control system decrypts the ciphertext command by using the new group key and then executes the command.

References

[1] Missing Malaysia Airlines flight: 13 conspiracy theories surrounding the disappearance of MH370, *Online, URL*: http://www.mirror.co.uk.

[2] How To Prevent A Robot Rebellion. *Online*, URL: http://www.createthefuturecontest.com/

[3] S. Checkoway, *et al*. "Comprehensive Experimental Analyses of Automotive Attack Surfaces." In *USENIX Security Symposium*. 2011.

[4] US military begins research into moral, ethical robots, to stave off Skynet-like apocalypse. URL: http://www.extremetech.com/, 2014.

[5] Report on Grid Disturbance On 30th & 31st July 2012, 2012 India blackouts, *Online URL*: http://www.cercind.gov.in/2012/

[6] H. Ning, and H. Liu. "Cyber-physical-social based security architecture for future internet of things." *Advances in Internet of Things,* vol. 2, pp. 1-7, 2012.

[7] A. Ramachandran, F. Nick, and V. Santosh. "Filtering spam with behavioral blacklisting." In *the 14th ACM* CCS'07, pp. 342-351.

[8] S. Munir, J. A. Stankovic, C.-J. Mike Liang, and S. Lin. "Cyber Physical System Challenges for Human-in-the-Loop Control." In *the 8th International Workshop on Feedback Computing*. USENIX 2014.

[9] D. Li and S. Sampalli. "An efficient group key establishment in location-aided mobile ad hoc networks." *ACM PEWAUN*, pp. 57-64., 2005.