Poster: Toward a Secure Controller Framework for Flight in 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

At 2015, after locking the plane's pilot out of the cockpit, the co-pilot A. Lubitz flew Germanwings Flight 4U 9525 into a mountain committing murder-suicide [1]. At 2014, Malaysia Airlines flight MH370, a more mysterious incident, disappeared carrying more than 200 passengers and crew members. Explanations to sudden disappearance range from mis-operations of suicidal pilots to cyber-attacks [3]. In fact, electronic control systems maybe vulnerable to malicious controllers, inside or outside: military robots may rebel their human masters [2] and hackers can manipulate modern automobiles or unmanned military aerial drones from a variety of attack surfaces [4]. The problem we endeavor to solve is that, when malicious controllers are trying to take it over, can we present a secure control framework to protect the control system e.g. aircraft with higher level of security?

Motivation: Traditionally, control systems such as aircrafts are handled by onsite human operators. Gradually, electronic automation control systems can partially participate in the control and then so does remote access control systems which forward control commands through cyber communication channels. This paradigm shift offers customers more options, incredible productivities and significant convenience but meanwhile the security concerns remain: it is possible that the control system falls to the wrong hand: the human operator can act maliciously, the automation control system can be infected or may be born with vulnerabilities, and the remote access control system through cyber channels can be compromised. A recent evident growth in misbehavior activities covering all possible aspects of Physical, Human and Cyber (Phc) [2], [4], serves a major motivation for this paper: adversaries could potentially launch attacks from all channels and we should mitigate the risks by well-designed access control mechanism as well as identifying and preventing the malicious controllers.

Contributions: To answer these questions, our new ideas are to (a) Propose the Physical, Human and Cyber Triad (b) Generate an access control mechanism that can grant a controller access right to a control action (c) Ensure that a control action cannot be executed without at least t out of n controllers' approval via secret sharing scheme. (d) Establish a quantitative framework that aims to develop a set of metrics which are used to assess the evilness of each controller. Flight is treated as a case study to verify it.

Related works: To evaluate the malicious activities and to prevent the cyber-attacks, the reputation of hosts has been widely studied which can detect, filter and block the misbehavior activities such as spams, unauthorized access control, etc. [7]. A cyber-physical-social based security architecture (namely, IPM) studied three critical security perspectives: information, physical, and management [6]. The cyber–physical system security for aeronautical communications is analyzed [8]. But, as the best of our knowledge, less attention is paid to study critical topics, (1) Phc triad over flight control system, (2) specific access control mechanism for flight, and (3) identify misbehavior controllers as well as withdraw their access rights.

II. Theoretical Background

Secret Sharing Scheme: In order to grant the access right over the control system, we will leverage the Shamir's (t, n) threshold scheme [9], based on which any set of t (or more) out of n controllers can execute a control action whose level requires at least t controllers. But any set with less than t controllers cannot.

Supervisory Control Theory: our research tries to isolate the malicious Phc controllers of flight from the control system via employing the supervisory control theory in which, the discrete state spaces and event-driven dynamics are widely used. From the viewpoint of discrete event systems, the control system under protection can be modelled as a plant, to which the supervisory controllers send control actions.

Blacklist for Cyber Misbehavior: The reputation of a host [7] has been treated as a vital metric which measures the security condition of a host. Based on the reputation value, some systems construct a blacklist with purpose to block / filter the inbound or outbound traffics sent from / forwarded to hosts in the list.

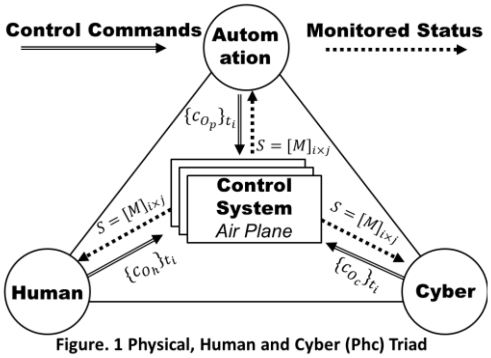
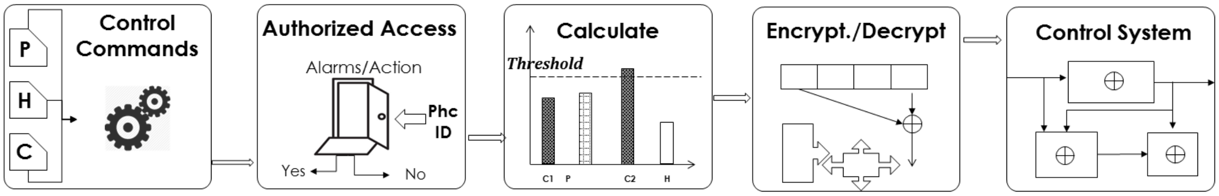


Figure. 1 Physical, Human and Cyber (Phc) Triad

III. Our System Overview

Physical-Human-Cyber (Phc) triad: As depicted in Fig. 1, our paper proposes a new Physical-Human-Cyber (Phc) triad system which is comprised of three components (sketched as circles), each denoting one type of controllers.



(1) Capture Commands (2) Filter Bad Commands (3) Calculate Badness (4) Encrypt Control Comm. (5) Control System

Figure 3: Overview of the Data Flow

The system under protection is represented by the "control system" blocks (sketched as rectangles) e.g. aircrafts. The solid, directional links connecting controller elements and the control system blocks denote the capability of the control privilege and the dashed links represents functions of collecting statuses from control systems.

Access Control Mechanism includes 2 components. First, let $F\left(C, c_j\right) = \{0,1\}$ denote a map where C is one controller and c_j is a control action. If the output is 1, it means that C can execute c_j. Second, any c_j is associated with 3-tuple $\{p, h, c\}$ where p, h, c are numbers of physical, human and cyber controllers, respectively. It denotes, to execute c_j, how many controllers of physical, pilot, cyber remote are required. For example, if the 3-tuple is {0, 2, 1}, it requires at least two pilots' and one cyber controller's endorsement and each of them has access right to c_j.

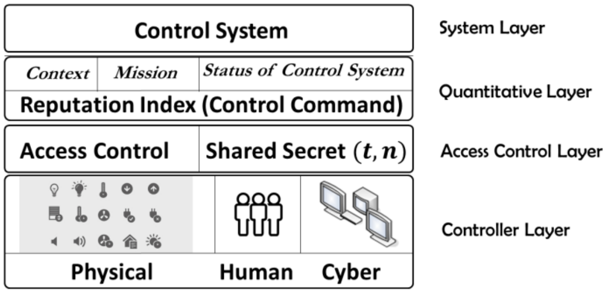


Figure 2. Architecture of our System

IV. Our System

We outline our system here but the detailed implementation will be our future tasks. As depicted in Fig. 2, our architecture includes four layers. In the *controller layer*, control actions are issued by physical (automation control system), human and cyber remote access operators. In the *access control layer*, we complete, (1) verify that whether a controller C has been granted the access right to a specific control action c_j via checking if $F\left(C, c_j\right) = 1$ and (2) count the number of controllers who approve the control command c_j and compare the result with 3-tuple $\{p, h, c\}$ which is associated with each control action c_j. In the *quantitative layer*, a set of metric is established for each controller in Phc triad. In the *system layer*, t controllers (note, $t = (p + h + c)$ and each of them has access right to c_j) provide their shares and collaborate with each other to recover the key K. The control action c_j is encrypted by K and the ciphertext is forwarded to control system which in turn, decrypts it to then execute control action c_j. Refer to Fig. 3 for detailed data flow.

Capture Control Commands and Monitor Statuses: control commands issued by Phc controllers and a finite sequence of statuses of control systems are collected. Those raw data will be de-noised, stored, classified, filtered and evaluated through a set of pre-processing operations or algorithms: we first map a sequence of observable events $E = \{e_1, e_2 \ldots, e_n\}$ to a set of control actions $\{c_1, c_2 \ldots, c_n\}$. Function $T\colon E \times \{c_1, c_2 \ldots, c_n\} = \{e_i\} \times \{c_j\}$. Our intrusion detection system is defined as I (a fault-diagnosis function). The control loop $A \rightarrow T$ (where A: a finite-state automation) is named as a potential attack if the action c_j is misbehaviour and if the e_i is one of the faulty states: wrong operations can unsafely impact the control systems, which are showed as different kinds of symptoms. Combining the active fault-diagnosis theory and the finite-state automation method, the intrusion detection I could abstract the control system as discrete-state event-driven dynamic and identify the misbehaviour or attacks as an active fault event.

We will analyze the malicious activities through the data collection and measurement method. Its result reflects reputations of each controller, which constructs blacklist.

Misbehavior Abstraction, Profiling and Modeling: while analyzing control commands, we aim to identify, profile, model and filter attacks based on a formal method. The macilious/bad command c_i will be put on the *BlackList*.

Record Misbehavior: for each c_i on the BlackList, c_i's owner, the controller, C will be impacted by its reputation.

References

[1] Germanwings: Crash leaves many unanswered questions, Online, URL, http://www.bbc.com/news/world-europe-32084956

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

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

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

[5] D. Li, Z. Aung, J. R. Williams, and A. Sanchez. "Efficient and fault diagnosable authentication architecture for AMI in smart grid." *Security and Communication Networks (SCN),* 2014.

[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. Pathak, *et al*. "Botnet spam campaigns can be long lasting: evidence, implications, and analysis." ACM SIGMETRICS Performance Evaluation Review. Vol. 37(1). Pp. 13-24, 2009.

[8] K. Sampigethaya, and R. Poovendran. "Aviation Cyber–Physical Systems: Foundations for Future Aircraft and Air Transport." Proceedings of the IEEE, Vol. 101(8), pp: 1834-1855, August 2013.

[9] A. Shamir, "How to Share a Secret", *Communication of ACM,* vol . 22(11), pp. 612-613, 1979.