A

Authentication for Cyber-Physical Systems

Chuadhry Mujeeb Ahmed[1] and Jianying Zhou[2]
[1]University of Strathclyde, Glasgow, UK
[2]SUTD, Singapore, Singapore

Synonyms

Authorization; Fingerprinting; ICS; Identification; IIoT; Verification

Definitions

In the following two key terms in the entry are defined.

Cyber Physical Systems: "Cyber-Physical Systems (CPS) comprise interacting digital, analog, physical, and human components engineered for function through integrated physics and logic. These systems will provide the foundation of our critical infrastructure, form the basis of emerging and future smart services, and improve our quality of life in many areas." (NIST 2014)

Authentication: "Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system." (NIST 2004). Authentication in general means to establish validity of objects (e.g., a person, a machine, a process, or data) so that an untrusted object can be stopped. Level of trust is always an issue when dealing with cross-domain interactions.

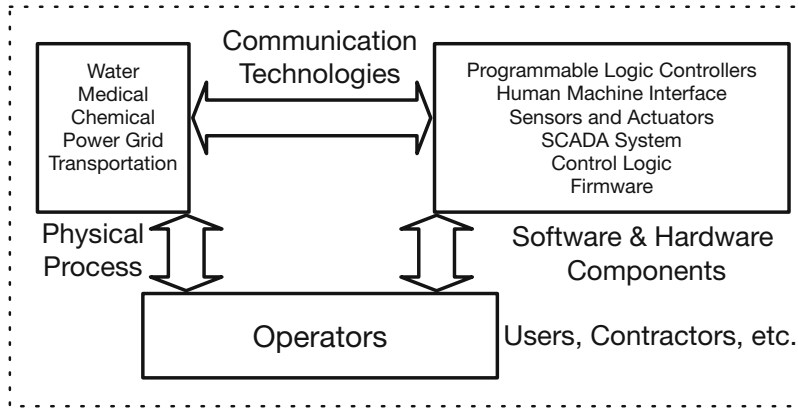
Authenticating entities in CPS is an important aspect to ensure secure control and brings challenges that merit a detailed discussion. Cyber-Physical Systems by design are multi-domain systems. Ensuring authentication in such complex systems is crucial. In this work, the challenges and potential solutions regarding the authentication for CPS devices are highlighted.

Background

The integration of cyber technologies (computing and communication) with the physical world gives rise to complex systems referred as Cyber Physical Systems (CPS). CPS has changed the methods that humans used to interact with the physical world. Some examples of CPS are manufacturing, transportation, smart grid, water treatment, medical devices, and the Industrial Internet of Things (IIoT) (Sutton 2018). Many of those systems are part of the critical infrastructure and need to perform safely, reliably, and securely in real time.

Major components of a typical CPS are shown in Fig. 1. A CPS consists of Programmable Logic Controllers (PLC), sensors, actuators, Supervisory Control, and Data Acquisition (SCADA) workstation and Human Machine Interface (HMI) that are interconnected via a communications network. The PLCs control a physical process based on the sensor

S. Jajodia et al. (eds.), *Encyclopedia of Cryptography, Security and Privacy*,
https://doi.org/10.1007/978-3-642-27739-9_1721-2



Authentication for Cyber-Physical Systems, Fig. 1 Components of a Cyber Physical System

measurements. The advances in communication technologies help to better monitor and operate CPS, but this connectivity also exposes physical processes to malicious entities on the cyber and physical domains. Recent incidents of sabotage on these systems (Lee et al. 2016; Slay and Miller 2008; Falliere et al. 2011) have raised concerns on the security of CPS (Ahmed et al. 2020a).

Challenges in CPS security are different as compared with the conventional IT systems, especially in terms of consequences in case of a security lapse. Attacks on CPS might result in damage to the physical property, as a result of an explosion (CNN 2007; Wired 2015), or severely affect people who depend on critical infrastructure as was the case of recent power cutoff in Ukraine (Lee et al. 2016). Data integrity is an important security requirement for CPS (Gollmann and Krotofil 2016), and hence the integrity of sensor data should be ensured. Sensor data can either be spoofed in cyber (digital) domain (Urbina et al. 2016) or in physical (analog) domain (Shoukry et al. 2015; Son et al. 2015). Sensors are a bridge between the physical and cyber domains in a CPS. From Fig. 1 it is seen that at a high level the major entities are physical process, communication technologies, hardware devices, software, and users. In a typical IT system, for example, a user logging into an online banking system has to prove his identity by providing unique credentials setup for that particular user. In a CPS all major entities need to authenticate each other as most systems work autonomously; it is not enough to authenticate a human operator as was the case in a typical IT system. Sensors are transmitting data to controllers as well as to human operators; it is important to authenticate that data before any use. Similarly, a Programmable Logic Controller needs to authenticate to other devices so that fake information cannot be sent on behalf of the legitimate PLC. Moreover, the process needs to authenticate itself, but there are hard computational constraints on most of the processes and devices in a CPS. These problems do not exist in pure IT systems.

In this entry, we highlight the authentication techniques employed in CPS based on the unique device and process fingerprints. Moreover, the introduced techniques can also be used to detect an anomaly since the authentication is a function of either a process or device characteristics.

Application

We consider a particular type of CPS called Industrial Control Systems (ICS) as an application. In particular, we use a water treatment testbed to elaborate authentication for CPS. The testbed is a six-stage water purification system with main components on each stage being sensors, actuators, PLCs, as well as water tanks and piping (Mathur and Tippenhauer 2016; Ahmed

et al. 2017). In the following, we explore three examples of authentication in a CPS.

Sensor Authentication

Fingerprinting of various physical and logical devices has been proposed for uniquely identifying and authenticating objects in mainstream IT systems such as PCs, laptops, and smart phones. However, the application of such techniques in ICS is less explored for reasons such as lack of direct access to such systems and the cost of faithfully reproducing realistic threat scenarios. The feasibility of using fingerprinting techniques in the context of realistic ICS related to water treatment and distribution systems is recently presented (Ahmed et al. 2020b). Using extensive experimentation with sensors, it is shown that noise patterns due to microscopic imperfections in hardware manufacturing can uniquely identify sensors with high accuracy. The proposed technique can be used to detect physical attacks, such as the replacement of legitimate sensors with faulty or manipulated sensors. For NoisePrint (Ahmed et al. 2018), a combined fingerprint for sensor and process noise is created. Sensor measurement noise based sensor authentication is a particular example in a broader field of device fingerprinting. In summary, the idea of authenticating users based on their fingerprints is extended to sensors based on randomness in the sensor measurements.

Actuator Authentication

The idea of fingerprinting has been extended toward actuator authentication based on unique hardware fingerprints. Among the earliest works (Formby et al. 2016) proposed a fingerprinting approach that uses the control aspects of ICS environments to generate signatures from the physical operations being taken by the physical devices on the network. Even though two relays or valves from different vendors may have similar ratings, there will always be physical variations in their construction resulting in fundamental differences in their operation times. These differences are then used to identify device types or spoofed command responses, which we call physical fingerprinting.

In another recent proposal (Gu et al. 2020), audio channel information is leveraged as side channel information of an operating CPS to study the feasibility of authenticating actuators based on acoustic fingerprinting. More specifically, the types of devices, their operation status, and their locations in space are inferred from the audio recorded using microphones. Convolutional neural network (CNN) is employed to learn and predict these parameters based on the transformed audio data. The result demonstrates that with only a small amount of training data, CNN can correctly predict the operation status of individual devices in a realistic water treatment testbed with approximately 100% accuracy.

Process Authentication

A recent technique called *Process Skew* uses the small deviations in the ICS process (herein called as a process fingerprint) for process state authentication (Ahmed et al. 2020c). The process fingerprint appears as noise in sensor measurements due to the process fluctuations. Such a fingerprint is unique to a process due to the intrinsic operational constraints of the physical process. The proposed technique is validated using the data from a real-world water treatment testbed. The results show that one can effectively authenticate a process based on its fingerprint and detect process anomaly with a very low false-positive rate.

PLC Authentication

There are some recent efforts on authenticating PLCs in a non-cryptographic manner. The iFinger (Yang et al. 2020) utilizes register states to generate ICS fingerprints to detect malicious attacks on industrial networks. Specifically, the Boolean logic represents every register state sequence of the ICS controller, and the deterministic finite automaton (DFA) generates a device fingerprint to authenticate a PLC and logic. Another proposal uses the scan cycle timing channel to authenticate PLCs. Scan cycle is the cyclic behavior of the PLCs to execute inputs, outputs, and control logic (Ahmed et al. 2021). The idea is to measure the scan cycle time on the network to authenticate a PLC and detect

network-based intrusions. To summarize, these research outputs point toward hardware- and software-based PLC authentication, a practical design for the resource-constrained controllers.

Control Logic Authentication

There have been several efforts to authenticate the control logic being executed by a PLC. Zeus (Han et al. 2017) monitors for control flow integrity of the PLC program execution. Zeus monitors the communications between the human machine interface and the PLC and captures the control logic binary uploads to the PLC. Zeus exercises its feasible execution paths and fingerprints their emissions using an external electromagnetic sensor. Zeus trains a neural network for legitimate PLC executions and uses it at runtime to identify the control flow based on PLC's electromagnetic emissions.

There have been other efforts based on radio frequency emission by the PLC to validate the control logic (Wright 2014). A recent study proposed a power based profile for PLC logic execution (Aguayo Gonzalez and Hinton 2014; Xiao et al. 2017). Chen et al. (2018) and Ghaeini et al. (2019) uses the models of the physical process along with the control logic program to authenticate the control logic.

Open Problems and Future Directions

Due to the unique features of CPS, the physics-based authentication techniques employed in CPS are very different from the cryptography-based authentication techniques in traditional IT systems. However, those techniques are not mature enough at the current stage. Further research is needed to improve:

- Accuracy: It is really important to achieve authentication with ultra-low false rate in the context of industrial systems. Considering the process is a long continuing sequence of events unlike a webpage logging in event a higher number of false alarms spread over a day will make any authentication technique meaningless.
- Efficiency: It is also important that the authentication process shall be fast to meet real-time requirements of the critical systems.
- Stability: CPS are usually deployed in harsh environments; therefore, it is important that the authentication is not affected due to device aging and other environmental variables.

References

Aguayo Gonzalez C, Hinton A (2014) Detecting malicious software execution in programmable logic controllers using power fingerprinting. In: Critical infrastructure protection VIII. Springer, Berlin/Heidelberg

Ahmed CM, Palleti VR, Mathur AP (2017) Wadi: a water distribution testbed for research in the design of secure cyber physical systems. In: Proceedings of the 3rd international workshop on cyber-physical systems for smart water networks. CySWATER'17. ACM, New York, pp 25–28. https://doi.org/10.1145/3055366.3055375

Ahmed CM, Ochoa M, Zhou J, Mathur A, Qadeer R, Murguia C, Ruths J (2018) Noiseprint: attack detection using sensor and process noise fingerprint in cyber physical systems. In: Proceedings of the 2018 ACM on Asia conference on computer and communications security, CCS'18. ACM. https://doi.org/10.1145/3196494.3196532

Ahmed CM, Gauthama Raman MR, Mathur AP (2020a) Challenges in machine learning based approaches for real-time anomaly detection in industrial control systems. In: Proceedings of the 6th ACM on cyber-physical system security workshop, CPSS'20. Association for Computing Machinery, New York, pp 23–29. https://doi.org/10.1145/3384941.3409588

Ahmed CM, Mathur AP, Ochoa M (2020b) Noisense print: detecting data integrity attacks on sensor measurements using hardware-based fingerprints. ACM Trans Priv Secur 24(1). https://doi.org/10.1145/3410447

Ahmed CM, Prakash J, Qadeer R, Agrawal A, Zhou J (2020c) Process skew: fingerprinting the process for anomaly detection in industrial control systems, WiSec 2020. ACM, New York, pp 219–230. https://doi.org/10.1145/3395351.3399364

Ahmed CM, Ochoa M, Zhou J, Mathur A (2021) Scanning the cycle: timing-based authentication on PLCs, ACM asiaccs 2021. 2102.08985

Chen Y, Poskitt CM, Sun J (2018) Learning from mutants: using code mutation to learn and monitor invariants of a cyber-physical system. In: 2018 IEEE symposium on security and privacy (SP). IEEE, pp 648–660

CNN (2007) Staged cyber attack reveals vulnerability in power grid. http://edition.cnn.com/2007/US/09/26/power.at.risk/index.html

Falliere N, Murchu L, Chien E (2011) W32 stuxnet dossier. symantec, version 1.4. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Formby D, Srinivasan P, Leonard A, Rogers J, Beyah R (2016) Who's in control of your control system? Device fingerprinting for cyber-physical systems. In: NDSS

Ghaeini HR, Chan M, Bahmani R, Brasser F, Garcia L, Zhou J, Sadeghi AR, Tippenhauer NO, Zonouz S (2019) Patt: physics-based attestation of control systems. In: 22nd international symposium on research in attacks, intrusions and defenses (RAID 2019). USENIX Association, Chaoyang District, Beijing, pp 165–180. https://www.usenix.org/conference/raid2019/presentation/ghaeini

Gollmann D, Krotofil M (2016) Cyber-physical systems security. Springer, Berlin/Heidelberg, pp 195–204. https://doi.org/10.1007/978-3-662-49301-4_14

Gu Q, Beyah R, Ahmed CM (2020) Identifying process structure and parameters using side-channel information. https://ics2020.sched.com/event/eh1h/identifying-process-structure-and-parameters-using-side-channel-information

Han Y, Etigowni S, Liu H, Zonouz S, Petropulu A (2017) Watch me, but don't touch me! Contactless control flow monitoring via electromagnetic emanations. In: Proceedings of the 2017 ACM SIGSAC conference on computer and communications security, CCS'17. Association for Computing Machinery, New York, pp 1095–1108. https://doi.org/10.1145/3133956.3134081

Lee RM, Assante MJ, Conway T (2016) Analysis of the cyber attack on the ukrainian power grid. SANS Report

Mathur AP, Tippenhauer NO (2016) Swat: a water treatment testbed for research and training on ics security. In: 2016 international workshop on cyber-physical systems for smart water networks (CySWater), pp 31–36. https://doi.org/10.1109/CySWater.2016.7469060

NIST (2004) Authentication. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-27ra.pdf

NIST (2014) Cyber-physical systems. https://www.nist.gov/el/cyber-physical-systems

Shoukry Y, Martin P, Yona Y, Diggavi S, Srivastava M (2015) Pycra: physical challenge-response authentication for active sensors under spoofing attacks. In: Proceedings of the 22Nd ACM SIGSAC conference on computer and communications security, CCS'15. ACM, New York, pp 1004–1015. https://doi.org/10.1145/2810103.2813679

Slay J, Miller M (2008) Lessons learned from the maroochy water breach. Springer, Boston, pp 73–82

Son Y, Shin H, Kim D, Park Y, Noh J, Choi K, Choi J, Kim Y (2015) Rocking drones with intentional sound noise on gyroscopic sensors. In: Proceedings of the 24th USENIX conference on security symposium, SEC'15. USENIX Association, Berkeley, pp 881–896. http://dl.acm.org/citation.cfm?id=2831143.2831199

Sutton F (2018) An efficient platform and communication architecture for event-triggered cyber-physical systems. PhD thesis, ETH Zurich, https://doi.org/10.3929/ethz-b-000260384

Urbina DI, Giraldo JA, Cardenas AA, Tippenhauer NO, Valente J, Faisal M, Ruths J, Candell R, Sandberg H (2016) Limiting the impact of stealthy attacks on industrial control systems. In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. ACM, pp 1092–1105

Wired (2015) A cyberattack has caused confirmed physical damage for the second time ever. https://www.wired.com/2015/01/german-steel-mill-hack-destruction/

Wright BC (2014) Plc hardware discrimination using rf-dna fingerprinting. PhD thesis, Air Force Institute of Technology. https://apps.dtic.mil/dtic/tr/fulltext/u2/a602984.pdf

Xiao Yj, Xu Wy, Jia Zh, Ma Zr, Qi Dl (2017) Nipad: a non-invasive power-based anomaly detection scheme for programmable logic controllers. Frontiers of Inf Technol Electron Eng 18(4):519–534. https://doi.org/10.1631/FITEE.1601540

Yang K, Li Q, Lin X, Chen X, Sun L (2020) ifinger: Intrusion detection in industrial control systems via register-based fingerprinting. IEEE J Sel Areas Commun 38(5):955–967. https://doi.org/10.1109/JSAC.2020.2980921