International Journal of Security and Its Applications
Vol.9, No.2 (2015), pp.159-168
http://dx.doi.org/10.14257/ijsia.2015.9.2.15

Security Protection Technology of Cyber-Physical Systems

Hong Ye

School of Information Science and Technology, Dalian Maritime University
Dalian, Liaoning, China, 116026
yehong@dlmu.edu.cn

Abstract

Based on computation and network technology, Cyber-Physical Systems (CPS) has achieved rapid growth but it is faced with increasingly serious security problems and needs targeted security protection technologies. Considering the characteristics of the typical architecture of CPS, this paper integrates the analytical method of information flow based on the noninterference theory and proposes the security protection design of CPS through formal methods and provides a kind of safety system based on this design framework.

Keywords: *Cyber-Physical Systems (CPS), Security Protection, Security Model, Noninterference*

1. Introduction

Cyber-Physical Systems (CPS) unifies computation process and physical process and becomes a next-generation intelligent system integrated with computation, communication, and control. CPS realizes interaction with physical process through human-machine interface and controls a physical entity through networked space in a remote, reliable, real-time, safe, and cooperative way [1].

CPS includes mobile terminals, intelligent robots, industrial SCADA, distributed control system etc. The Visual Network Index report of Cisco has estimated that by 2017 more than 10 billion mobile devices will be connected, including over 1.7 billion machine-to-machine connections and the ever-increasing network connections make it possible to take advantage of large amounts of network security holes so protecting system security becomes the important direction of current research of CPS.

CPS security model provides accurate definition of security demands and goals expressed by security policy and uses process algebra and logical reasoning to abstract system into process, action, state, and output through formal methods. The design of security model is the premise of achieving high-security CPS.

This paper first introduces the typical architecture of CPS and the analytical method of information flow based on the noninterference theory. Based on this, it then puts forward CPS security protection design through formal methods and provides a kind of safety system based on this design framework. Finally, it provides conclusion and proposes the future research direction.

2. The Analysis of CPS Architecture and its Current Security Situation

CPS has unique characteristics including heterogeneous integration, collaborative autonomy and open interconnection that raise a number of issues for system security. Developing new security models, key technologies and approaches is critical in the development of CPS.

2.1. Definition and Architecture of CPS

CPS is a next-generation network connected collection of loosely coupled distributed cyber systems and physical systems monitored/controlled by user defined semantic laws. CPS is a multi-dimensional complex system integrated with computation, network, and physical environment and can realize real-time perception, dynamic control, and information service of large-scale project systems through 3C technologies, namely, computation, communication, and control. CPS overlaps with Internet of Things, software system, and embedded system but is also different from them. It can be seen as the intersection of those three kinds of systems, as presented in Figure 1, while the differences are mainly reflected in the following aspects.

1) Apart from the interconnection between things put forward by Internet of Things, CPS also puts emphasis on the real-time and dynamic information control and information service of things. Academician He Jifeng contends that the significance of CPS is that it can make physical devices connected, especially connected to the Internet, which enables physical devices to have five functions, namely: computation, communication, accurate control, remote coordination, and self-management [2].
2) Compared with software system, CPS attaches greater importance to functionality. Software system is a sequence of state transition and aims at realizing data transformation while the ultimate goal of CPS is to coordinate physical process or to achieve information processing and physical control and CPS emphasizes instantaneity, reliability, security, privacy, and adaptability etc.
3) CPS is the development direction and research focus of embedded system. Embedded system lays particular emphasis on the operation on processors. It is an optimization technique in a limited resource environment. As a combination of computation and physical elements, CPS embeds computation and communication capabilities into traditional physical system, which leads to the changes in computation objects. It turns computation objects from digital into simulative, from discrete into continuous, and from static into dynamic.

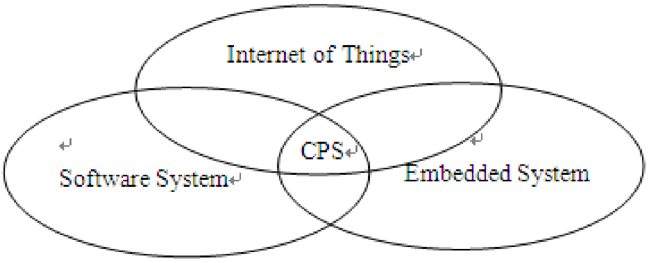


Figure 1. Function Orientation of CPS

Globally speaking, countries with more advanced information technology, such as the United States, European countries, and Japan, all place considerable emphasis on CPS and make great efforts to develop CPS. They have invested a large quantity of capital, manpower and material resources.

Early in 2006, American government took CPS as an important research project in American Competitiveness Initiative; in 2007, President's Council of Advisors on Science and Technology (PCAST) gave first priority to CPS among eight key information technologies in Leadership Under Challenge: Information Technology R&D in a Competitive World report; and in 2008, the United Sates set up CPS steering group and applied CPS to many areas, including transportation, national defense, medical treatment, agriculture, and large-scale construction and facilities and so on.

From 2007 to 2013, European Union has invested more than $7 billion on CPS project ARTMEIS in the hope that it would become the world leader of intelligent electronic system in 2016. Both the large-scale scientific funding scheme of the Seventh Framework of Europe and German government's aid program SEIS have invested a large amount of capital on CPS researches.

In China, most of the current research object is the elementary form of CPS—Internet of Things. Shanghai has carried out the pilot project in intelligent transportation field and achieved real-time monitoring and collection of the information of all components of automotive electronics through vehicle information terminals and connected this to background information service system through wireless communication to establish a networked automobile remote information service system so as to achieve real-time monitoring of vehicle condition, operating state control, real-time traffic status dynamic navigation, and online diagnose, remote maintenance and control of vehicle malfunction etc.

As the base of CPS research, architecture is very important, but currently, there were no unified frameworks or general architectures can be used in most applications. CPS has close relationships with embedded systems, sensors and wireless network, but has its own characteristics. In [3], Hyun Jung La *et al.* proposed a 3-Tiers architecture of CPS. The architecture is in Figure 2.

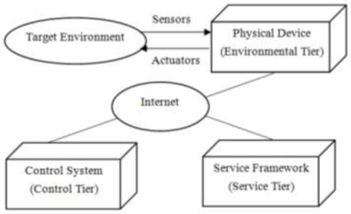


Figure 2. The Three Tiers of CPS Architecture

2.2. The Current Security Situation of CPS

After Iran's Bushire nuclear power plant was attacked by Stuxnet in 2010, Advanced Persistent Threat (APT) targeted at CPS has been increasing, as illustrated in The most common attack methods in the appliance of CPS include: amount amendment in RFID data reading and writing, data leakage in two-dimension code applications, attacking background system terminals and their operation, business logic bugs of CPS, customers' privacy disclosure caused by remote reading data, Trojan virus of hand-held terminals, backdoor and BUG of embedded system development, data hijacking of CPS bearer networks, forging identity to deceive authentication server in the interaction process, and attacking data center and "dragging" to cause customers' privacy disclosure and so forth.

The current security arrangement based on virus killing cannot effectively protect current CPS and therefore emerge many new safety precautions. ARM's "TrustZone" virtualization technology sets safety zones different from the common OS operation zone in a processor core to prevent network attacks [4].

Table **1**. The following part will perform analysis from areas of industrial control system, civil use, and security protection.

In the field of industrial control system, according to ICS-CERT, 198 security incidents related to industrial control system were reported in 2011, which increased greatly compared with that in 2009 and 2010. Most of the security incidents took place in areas of energy resources, water conservancy, chemical industry, governmental agencies, and nuclear facilities and so on, among which 52 security incidents have taken place in energy industry during the three years, accounting for 21% of the total security incidents.

In the civil use field, 2013 American Black Hat and 2014 Singapore Black Hat displayed car attacks targeted at Ford Explorer, Toyota Prius, and Tesla and attacks aimed at cardiac pacemaker and smart television respectively.

In security protection field, seven international renowned security institutions, fireeye, Fortinet, Lancope, Neohapsis, Symantec, Websense, and Zscaler, all mentioned attacks targeted at CPS in 2014.

The most common attack methods in the appliance of CPS include: amount amendment in RFID data reading and writing, data leakage in two-dimension code applications, attacking background system terminals and their operation, business logic bugs of CPS, customers' privacy disclosure caused by remote reading data, Trojan virus of hand-held terminals, backdoor and BUG of embedded system development, data hijacking of CPS bearer networks, forging identity to deceive authentication server in the interaction process, and attacking data center and "dragging" to cause customers' privacy disclosure and so forth.

The current security arrangement based on virus killing cannot effectively protect current CPS and therefore emerge many new safety precautions. ARM's "TrustZone" virtualization technology sets safety zones different from the common OS operation zone in a processor core to prevent network attacks [4].

Table 1. Typical CPS Security Incidents

CPS fields	Typical security incidents
Energy management	Stuxnet Attacks targeted at nuclear power plant
Automobile cars	Attacks targeted at Ford Explorer, Toyota Prius, and Tesla
Environment monitoring	Attacks targeted at pollution treatment equipment in water works
Medical industry	Attacks targeted at cardiac pacemaker
Key infrastructure	Attacks targeted at smart television among key infrastructure
Military equipment	Attacks targeted at crystalline silicon
State power plant	Attacks targeted at power plant and intelligent electric meters

The protection of CPS industrial control system usually adopts security isolation design and partitions three isolated sub-domains, namely engineer station, controller, and APC Server and employs firewall, intrusion detection, and traffic monitoring and so on to implement isolation. Meanwhile, it examines, tracks, and protects OPC technology. Every time the OPC application program creates a connection, it only opens needed TCP port [5] between OPC Client which creates the OPC connection and OPC Server dynamically and completeness check is carried out on the information of illegal format and abnormal behavior communication.

3. Noninterference Theory of Information Flow

Since the most important and most easily attacked part of CPS is software system, the analysis of CPS security can adopt software system's analytical method, namely information flow. The formal expression of noninterference of information flow is a scientific security policy description and the security policy based on the noninterference has the form of logical theory. Any realization in accordance with models can be proved to be secure.

Goguen and Meseguer first put forward the noninterference idea of information flow [6]. After that, many kinds of noninterference security models have been established, including Bevier's noninterference model based on state [7], McLean's noninterference model of broad sense [8], McCullough's noninterference model of noncomposability

[9], Focardi's noninterference model based on nondeterministic system[10], Mantel's probability noninterference model [11], and Rushby's noninterference model based on state machine [12] etc. Among them, Rushby's noninterference model is the most suitable one to describe security policy, and the following part is the brief description of the noninterference model given by Rushby.

Definition 1: The definition of System M is as follows:

- W's set S of states, with an initial state s_0, $s_0 \in S$;
- W's set A of actions;
- W's set O of outputs;
- State function after W executes a single step action: $step: S \times A \to S$;
- State function after W executes a series of actions: $run: S \times A^* \to S$, $run(s,\Lambda)=s$, $run(s,a\circ\alpha)=run(step(s,a),\alpha)$, where Λ denotes the empty sequence, a denotes single action, and α denotes an action sequence;
- Output function after W executes actions: $output: S \times A \to O$;
- W's set D of security domains, domain action function $dom: A \to D$ which shows the execution domain of each action of system;

Definition 2: D's information flow security policy $u\square>v$ is defined as that information can flow from u to v:

- If $u\square>v$, $v\square>w$, then $u\square>w$.

Definition 3: For given domain v and action sequence α, function $purge(\alpha,v)$ shows the remaining actions after deleting all actions in the domain which is not inter-interfered with v from action sequence α:

$$purge(\Lambda,v)=\Lambda$$

$$purge(a\circ\alpha,v)=\begin{cases} a\circ purge(\alpha,v) & if\ dom(a)\square>v \\ purge(\alpha,v) & otherwise \end{cases}$$

Definition 4: System W is secure for policy $\sim>$:

$$output(run(s_0,\alpha),a)=output(run(s_0,purge(\alpha,dom(a))),a)$$

4. Noninterference Model Design of Safe CPS

For CPS, the definition of its security includes confidentiality, integrity, usability, and controllability and so forth and covers components including physical layer, media access control layer, network layer and application layer. Thus, the noninterference model proposed by this paper consists of an abstract security protection model which contains a set of orders including license agreement, authorization, and password management and so forth and crosses several aforementioned system layers. It provides safe access approaches for application layer and guarantees safety of communication.

4.1. Noninterference Model of Safe CPS

Noninterference model of safe CPS expands traditional intransitive noninterference security model, namely to define a transitive connected domain of CPS. When this domain accords with intransitive noninterference security model, then secure access service can be provided, which means that the transitive connected domain of CPS can satisfy Reference Monitor hypothesis:

Hypothesis1. Output-consistency

For $\forall u \in D$, a is an action from domain u, and the transitive connected domain of CPS can satisfy:

$$s \overset{u}{\sim} t \rightarrow output(s,a) = output(t,a)$$

Hypothesis2. View dependency

a is an action from domain u, then:

The influence of an action from CPS transitive connected domain on the system state is only dependent on the system view of the last state of the domain from which the action comes.

Hypothesis3. Object writability

In the CPS transitive connected domain, if particular action changes the value of object, then the domain from which the action comes can definitely access this object, namely

$$cont(step(s,a),m) \neq cont(s,m) \rightarrow m \in alter(dom(a),s)$$

Theorem 1: If CPS can satisfy the aforementioned hypothesis 1, 2, and 3, then CPS transitive connected domain can satisfy the security policy of intransitive noninterference access control ~>.

Proof:

1) Output-consistence

It is proved by RM hypothesis1.

2) Weak step consistency

$s \overset{u}{\sim} t \wedge s \overset{dom(a)}{\sim} t \rightarrow step(s,a) \overset{u}{\sim} step(t,a)$ can be rewritten as for $\forall n \in domview(u,s)$,

then $s \overset{u}{\sim} t \wedge s \overset{dom(a)}{\sim} t \rightarrow cont(step(s,a),m) = cont(step(t,a),m)$.

In it m can respectively satisfy:

If $cont(step(s,a),m) \neq cont(s,m)$, then the fact that M satisfies RM hypothesis 2 provides $cont(step(s,a),m) = cont(step(t,a),m)$

If $cont(step(t,a),m) \neq cont(t,m)$, then the fact that M satisfies RM hypothesis 2 provides $cont(step(s,a),m) = cont(step(t,a),m)$

If it is not the above two cases, then it must have

$$cont(step(s,a),m) = cont(s,m) \wedge cont(step(t,a),m) = cont(t,m)$$

And $cont(step(t,a),m) \neq cont(t,m)$ provides

$cont(step(s,a),m) = cont(step(t,a),m)$, thereby weak step consistency proved.

3) Local correlation

From we have provides

$$cont(step(s,a),m) \neq cont(s,m) \rightarrow m \in alter(dom(a),s)$$

and $m \in domview(u,s)$, then $dom(a) \sim> u$ .Therefore it is proved.

Thus CPS transitive connected domain complies with intransitive noninterference access control policy model.

4.2. ZigBee Platform Safety Design

From bottom to top, ZigBee system can be divided into radio frequency transceiver, physical layer, media access control layer, and application layer, among which the application layer can also be divided into application support sub-layer, application object, and ZDO and so on. ZigBee security platform bases its design on the noninterference model and carries security service across every layer of ZigBee system. ZigBee security platform consists of security service platform and security application system. Security service platform performs managements, configuration, and audit of all terminals in the system, as illustrated in Figure 3 and employs the main security protection technologies, including policy service of each layer, system layer monitoring, access control, identity authentication mechanism, file verification technology, and audit service and so forth.

Policy service provides executive program measurement, prevents the execution of executive programs which are unauthorized or do not meet expectation, achieves active defense against known or unknown malicious code, and reduces the risk of damage to

CPS operation system integrity and usability. From the management perspective, it provides program installation interface and only permits the complete installation of system security software through program installation interface. Meanwhile it can generate acquisition module and realize batch installation upon the authorization and approval of the administrator so as to prevent the installation of software and plug-in from unknown resources and ensure the secure execution of the system.

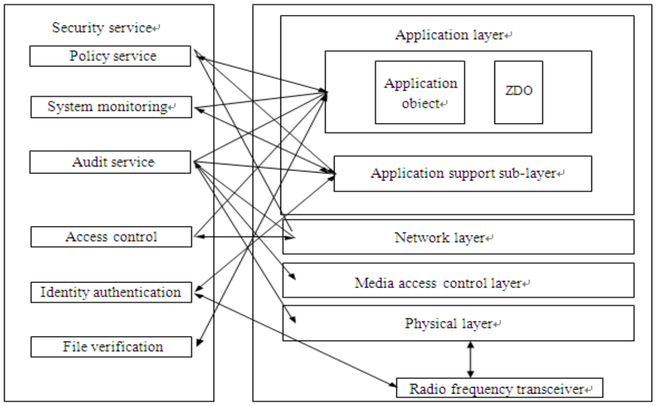


Figure 3. ZigBee Security Platform

When communication between different terminals of ZigBee platform is connected, connection policy is established to enhance network access control capabilities of terminal platforms. Terminals should identify the identity of access terminals in accordance with security policy and effectively control the access to authorized node by unauthorized node and realize effective control of access.

5. Conclusion

The main trend of CPS is to employ Ethernet and TCP/IP as the most important communication protocol and means to achieve networked, standard, and open development. The information security issues of CPS have become extremely urgent. This paper combines the analytical method of information flow based on noninterference theory, targets at characteristics of the typical framework and puts forward CPS security protection design through formal methods and provides the safety system of ZigBee platform frame.

Acknowledgements

This work is supported in part by National Natural Science Foundation of China under Grant No.61173034 and the Fundamental Research Funds for the Central Universities under Grant No.3132013040 and 3132014093.

References

[1] E. A. Lee, "Cyber physical systems: Design challenges", in International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing (ISORC), May 2008, invited Paper.

[2] J. He, "Cyber-physical Systems [J]", China Computer Federation, vol. 6, no. 1, (**2010**), pp. 25-29

[3] H. J. La and S. D. Kim, "A Service-based Approach to Designing Cyber Physical Systems", in 2010 IEEE/ACIS 9th International Conference on Computer and Information Science, Yamagata, (**2010**), pp. 895-900.

[4] T. Benzel, B. Braden, D. Kim, C. N. A. Joseph and K. S. R. Ostrenga and S. Schwab, "Experience with DETER: A Testbed for Security Research. Second IEEE Conference on testbeds and Research Infrastructures for the Development of Networks and Communities", (**2006**) March, Barcelona.

[5] A. Viswanathan and C. Neuman, "A Survey of Isolation Techniques Information Sciences Institute", University of Southern California, (**2009)** February.

[6] J. A. Goguen and J. Meseguer, "Security policies and security models", Proc. of the 1982 IEEE Symposium on Security and Privacy, IEEE Computer Society Press, 11-20, (**1982**) April.

[7] W. R. Bevier and W. D. Young, "A state-based approach to noninterference", in Proceedings of the Computer Security Formulations Workshop VII.IEEE Computer Society, (**1994**).

[8] J. McLean, "Security models and information flow", In: Proc. of 1990 IEEE Symposium on Research in Security and Privacy[C]. IEEE Press, (**1990**), pp. 177-186.

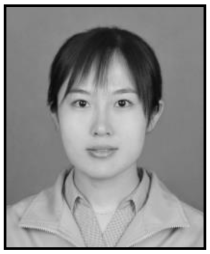
[9] D. McCullough, "Noninterference and the Composability of security properties", In Proceedings of the 1988 Symposium on Security and Privacy. IEEE, (**1988**) April.

[10] R. Focardi and R. Gorrieri, "Classification of security properties (Part I: Information Flow). In: Foundations of Security Analysis and Design", LNCS, vol. 2171, Springer-Verlag, (**2001**).

[11] H. Mantel, "Possibilistic Definitions of Security-An Assembly Kit", in Proceedings of l3th Computer Security Foundations Workshop (CSFW'00), July 2000, Cambridge, England.

[12] J. Rushby, "Noninterference, transitivity, and channel-control security policies", Technical Report, CSL-92-02, Menlo Park: Stanford Research Institute, (**1992**).

Author



Hong Ye, She received her master's degrees from Dalian University of Technology, China in 2003. Now she is full lecturer school of Information Technology, Dalian Maritime University, China. Since 2009, she has been pursuing the Ph.D. Degree at the Department of Computer Sciences, Dalian Maritime University. Her current research interests include different aspects of Distributed Systems.