Cyber Physical Security for Industrial Control Systems and IoT

Kazukuni KOBARA\(^{a)}\), Member

SUMMARY
cyber-attacks and cybersecurity used to be the issues for those who use Internet and computers. The issues, however, are expanding to anyone who does not even use them directly. The society is gradually and heavily depending on networks and computers. They are not closed within a cyberspace anymore and having interaction with our real world with sensors and actuators. Such systems are known as CPS (Cyber Physical Systems), IoT/E (Internet of Things/Everything), Industry 4.0, Industrial Internet, M2M, etc. No matter what they are called, exploitation of any of these systems may cause a serious influence to our real life and appropriate countermeasures must be taken to mitigate the risks. In this paper, cybersecurity in ICS (Industrial Control Systems) is reviewed as a leading example of cyber physical security for critical infrastructures. Then as a future aspect of it, IoT security for consumers is explained.

**key words:** security, Cyber Physical System, Industrial Control System, IoT, M2M

1. Introduction

Future society will heavily depend on computers and networks in any aspect. This has already been or is becoming true in most of social infrastructures based on ICS (Industrial Control Systems), which include critical manufacturing, chemical industry (dealing hazardous materials), smart systems for power grid, energy-networks, cities, home, agriculture, healthcare, automotive and so on. In a broad sense, they are also known as CPS (Cyber Physical Systems), IoT/E (Internet of Things/Everything), Industry 4.0, Industrial Internet, M2M and so on, and have a common feature that they consist of sensors and actuators, and have interfaces and interactions with our physical world. The consequences of cyberattacks on such systems will not be confined within a cyberspace but flood into our real life.

Taking this situation into account, this paper reviews the cybersecurity in ICS as a leading example of such cyber physical security, and then considers the future of them. In Sect. 2, the situation of ICS is explained. In Sect. 3, their security threats and their countermeasures are summarized. Then, cyber physical security in future, especially of IoT for consumers, is considered in Sect. 4, and finally concluded in Sect. 5.

2. Industrial Control System

In this section, we explain the situation and features of ICS in terms of security by introducing an example of a typical ICS configuration.

2.1 Example of ICS Configuration

Even though ICS configurations are rich in variety in practice, an example is shown in Fig. 1 to grab a rough image of ICS. In this figure, actuators and sensors are connected to the field/sensor networks (or data buses), which are usually proprietary and industry specific. The sensors and actuators are controlled and managed by controllers such as PLC (Programmable Logic Controller) and DCS (Distributed Control System). These controllers are also connected to a control system network, which is used to manage the sensors, actuators and their controllers, e.g. to change the set point by way of HMI (Human Machine Interface), to update their logic or programs by way of EWS (Engineering Work Station), to collect logs by Historian, and to supervise them by SCADA (Supervisory Control And Data Acquisition) systems and so on.

Control system networks usually consist of Industrial Ethernet that is compatible with standard Ethernet protocols but their hardware is designed for real time processing and...
harsh environments. To manage the production or operation, some information is usually exchanged between corporate networks and control system networks, and some of the maintenances might be performed remotely, which are called remote maintenance.

2.2 Features of ICS in Terms of Security

One of the most significant features of ICS is that they have interfaces with the real world and due to this they might cause a serious problem to our real life after exploitation by attackers and crackers. Other features include:

1) Availability is usually higher priority than confidentiality and integrity.
2) Life cycle is longer than usual ICT (Information and Communication Technologies).
3) Loosely isolated from the Internet.
4) Proprietary and/or specific purpose protocols and operating systems are used.

Due to 1) and 2), conventional ICT countermeasures are not necessarily applicable as they are. E.g. rapid and frequent patching to bugs is not suitable for some sensitive ICS since patching may deteriorate the compatibility with minor device drivers or the performance the system must satisfy, though patching is a must and a fundamental countermeasure in ICT.

Due to 3) and 4), ICS did not used to be a major target of cyberattacks. The situation, however, has been changing. Proprietary and/or specific purpose protocols and operating systems are gradually replaced with general purpose ones with which adversaries are familiar. Isolated environments are gradually getting connected to other networks. As shown in Fig. 2 and Fig. 3, the major OS in ICS was Windows followed by Unix, Linux and RTOS (Real Time OS), and then more than one third of them were connected to a network as of 2008 [1]. This trend will be inherited to smart manufacturing, Industry 4.0, Industrial Internet and so on where more ICT technologies are introduced.

On the other hand, trend of cyberattacks is also changing. Their purposes are shifting from fun and curiosity to moneymaking, terrorism, cyberware and so on to impose adversaries’ demands. Their methodologies are becoming persistent rather than casual while changing their targets from general public to intended organizations such as critical infrastructures and their related organizations. Their system targets are covering even isolated environments, proprietary and industry specific protocols, software and operating systems.

In fact, the number of incidents and vulnerabilities reported to ICS-CERT [2] is increasing as shown in Fig. 4 after the epoch-making incident Stuxnet [3], which targeted industry specific software and closed network and then ruined centrifuges for nuclear material in Iran in 2010. Similar trend can also be observed in the repository of industrial security incidents [4].

3. Cybersecurity Threats and Countermeasures in ICS

In this section, major cybersecurity threats and their countermeasures for ICS are summarized in Sect. 3.2 to 3.4 while introducing a visualization method for their relationship in Sect. 3.1.

Publicly available major tools are introduced in Sect. 3.2 to 3.4. While these tools might be abused for attacks and some of the readers might think that these information should be hidden, this is not a recommended strategy. These tools are fundamental for adversaries and they use more powerful and tailored ones. Protection side should recognize this, and confirm that the potential targets can resist against at least these fundamental tools.
3.1 Relationship between Security Risks and Countermeasures

One of the most difficult parts of managing potential security risks is to identify an optimal set of effective countermeasures against security threats taking their costs, performance deterioration, interoperability with current and future systems and management styles and so on. Inappropriate or few countermeasures may cause security problems and the cost of expensive over-spec countermeasures may exceed the expected damage by the security threats. In order to look for an optimal set of countermeasures, it is important to grasp the relationship between security threats and their countermeasures, and this can be intuitively depicted by visualization.

One approach to express security risks visually is to create an attack tree, which shows a problem as the root and its sources as the leaves. Weaknesses of attack trees, however, are that they do not express which paths are most risky and which are not, which countermeasures are effective to which paths. To overcome these weaknesses, we propose to improve the attack tree by adding the following expressions (we call it extended attack tree):

1) The severity level of each stage (node).
2) The transferability from one stage to another.
3) Countermeasures and their effects.

In the examples Fig. 5 and Fig. 6, the red part represents an attack tree and then the above expressions are added as follows. The severity is expressed as the darkness of the color of the stages. The transferability is expressed as the thickness of the line between stages. While the severity and the transferability in Fig. 5 are divided into four and three levels, respectively, their precision should be customized depending on the application. Countermeasures are divided into prior and posterior. In Fig. 5, they are colored in green and purple, respectively, with arrows or lines they are related to. In the case of monochrome, their texture should be changed instead of the colors. Gray boxes are used for notes, and in Fig. 6 the notes show the related subsections in this paper with the dotted black lines as the separators.

The risks are expressed as the combination of the severity level and the transferability to reach at the severity level. Once risks are identified, one can take the actions: 1) Reduce, 2) Accept, 3) Transfer and 4) Avoid, to them. Reduction of risks is achieved by application of prior and posterior countermeasures. If the residual risks are small, they may
be acceptable by preparing risk finances for them. If they are not acceptable even after the reduction, they should be transferred to insurance or outsourcing. If even transfer is not possible, one should consider avoiding the services or projects causing the unacceptable residual risks.

Figure 6 is an example to image this concept, and precise relationship among security threats and their countermeasures should be created in each industry or application area with collaboration among its stakeholders. The created one should, then, be used in the area or industry as a common reference. Optimal sets of countermeasures, however, vary in each organization or product depending on the management policy so on. It is not necessarily recommended to apply all the available countermeasures without taking the cost, performance deterioration, compatibility with current and future systems and management styles and so on into account, especially in a constraint environment like ICS.

The check box in the upper left corner in each countermeasure is to show which countermeasures are not taken and instead which ones are taken to look for an optimal set of countermeasures. While conventional security check lists assume that all the terms should be satisfied and it is not clear what will happen and what to do when some of the terms are not satisfied, the check boxes here in the extended attack tree are to support risk control by looking for alternatives, or deciding whether its residual risks are acceptable or not when some countermeasures are hard to satisfy.

In the following subsections, security risks and their countermeasures are explained more concretely.

### 3.2 Risks and Countermeasures around Remote Access

This subsection corresponds with the upper right area in Fig. 6. Some of the ICS open communication ports that are accessible from the Internet for remote maintenance and these will be the target to analyze.

In most cases, the first step of cyberattacks is reconnaissance of targets [5], which remotely scouts the targets’ profile and configurations including not only networks and systems but also internal information such as operators and their operational roles. In the case of APT (Advanced Persistent Threats), this phase is performed elaborately and persistently.

While port and vulnerability scanners such as Nmap [6] and Nessus [7]/OpenVAS [8], have been popular for looking for open ports, services and their vulnerabilities from Internet, another approach utilizing dedicated search engines such as SHODAN [9] and ERIPP [10], has been becoming serious since they can easily list up vulnerable targets right after a vulnerable is discovered in a service. They create a database of IP addresses, port numbers and their contents displayed after connection such as banner, HTML title tags, etc. Then IP addresses and port numbers can be searched from a key word related to the service. ERIPP currently covers only port 80, and SHODAN is covering more ports including the port numbers used in ICS. To enhance the usability of these search results, some projects map the rough location of identified vulnerable services and devices [11–13].

If the targets do not have publicly known vulnerabilities, further vulnerabilities are examined. Some of the modern ICS devices or services provide Web interfaces, which might be vulnerable to SQL/OS command injections or cross site exploits including cross site scripting, cross site request forgery and so on. They may also equip inappropriate remote access control such as default IDs and passwords, bypassing mechanism to their authentication and access control schemes. ICS and embedded devices tend to be used with their default IDs and passwords, which are publicly available at various sites including [14]. Bypassing mechanisms may be prepared to deal with password loss, and these information may be either written in a manual, or discussed in the Internet [15], [16].

Needless to say, a must countermeasure against reconnaissance from Internet is to place devices and servers behind a firewall or a security gateway. While this is basic, a considerably high number of them are still accessible from Internet as shown by SHODAN etc.

To grasp the reconnaissance activities on them, ICS/SCADA honeypots are useful. They mimic the behavior of common industrial control protocols and then monitor the activities on them. Such honeypots can be constructed using CONPOT [17], etc. For telnet-based devices, which are common in certain types of IoT devices, IoTPOT is available [18].

Against Web exploitation, Web applications should be created ideally to avoid the above vulnerabilities. If they have already been created, their vulnerabilities should be examined with Web application penetration tools including OWASP ZAP [19] that can work with external tools such as Nikto [20], Burp Suite [21], sqlmap [22], ssllscan [23], etc.

For remote access for remote maintenance, user authentication and access control should be reviewed and strengthened. Default IDs and passwords must be changed and bypassing mechanisms that are available from remote must be disabled, though these are fundamental as well.

For ICS embedded devices and services, there are certification programs called Functional Security Assessment for Embedded Device Component (FSA-E) and System (FSA-S), respectively. They are parts of ISASecure’s Embedded Device Security Assurance (EDSA) [24] and System Security Assurance (SSA) [25] certifications, respectively. They are being or has standardized as IEC 62443 (Industrial communication networks) in Part 4-2 (Technical security requirements for IACS components) and Part 3-3 (System security requirements and security levels), respectively.

### 3.3 Risks and Countermeasures around Software

This subsection corresponds with the left area in Fig. 6. Discovery of new vulnerabilities by adversaries is a serious issue since they are used for zero-day attacks. For software,
fuzzing (or fuzz testing) and reverse engineering are used for this purpose. Fuzzing gives data in unusual format to the target and then checks its behavior. If it gets stuck or acts strangely, it may have some mal memory handling that leads to a buffer overflow to hijack the target. Comprehensive list of fuzzing tools (fuzzers) is available at [26] and some of them support ICS specific communication protocols. ICS and embedded systems tend to rely on legacy software and it has such vulnerabilities with non-negligible probability.

In the case of ICS and embedded systems, the target of reverse engineering includes firmware whose images may be downloadable from Web sites or extracted from on-chip debug interfaces using hardware tools such as JTAGulator [27]. The obtained firmware is then analyzed, vulnerabilities and hardcoded passwords may be revealed and then mal functions might be inserted to it if no countermeasure is taken. Structure analyses of firmware and then extraction of executable files are performed by using firmware tools such as binwalk [28]. Once executable files are extracted, they are analyzed further by using usual disassembler, debugger, etc. For this purpose, IDA [29], which is a disassembler and a debugger, supports various processors including those used for ICS. These analyses may eventually identify new vulnerabilities used in zero-day attacks.

Against vulnerabilities caused in software development, there exist ISASecure’s certification programs called Software Development Security Assessment (SDSA), Security Development Lifecycle Assurance (SDLA) [31] and Communication Robustness Testing (CRT). CRT certification program is available in Japan too since April of 2014 [30] and CRT and SDSA are parts of EDSA certification program. CRT, SDSA and SDLA are also under standardization as IEC 62443 Part 4-1 (Product development requirements) as of July 2015.

Against reverse engineering of firmware and software, obfuscation or encryption should be applied to them. Against modification of them, alteration detection should be added to them. Alteration detection can be realized using either a digital signature such as RSA signature and ECDSA, or a Message Authentication Code (MAC) such as HMAC and CMAC. These cryptographic approaches, however, require the devices to hold cryptographic keys securely. While public keys (for signature verification and encryption of symmetric keys) and root certificates to verify them do not need to be protected against reveal, their processing speed is around 100 to 1000 times slower than that using a symmetric key. Therefore algorithms using a public key might not be suited to low-end embedded devices without crypto accelerators. On the other hand, while the algorithms using a symmetric key such as AES (Advanced Encryption Standard) are faster than that using a public key, symmetric keys must be protected against not only modification but also reveal. Protection of keys is usually provided by a tamper resistant module, whose validation or certification is provided as EAL (Evaluation Assurance Level) of CC (Common Criteria) that is in accordance with ISO/IEC 15408, or by CMVP (Cryptographic Module Validation Program) or JCMVP (Japan CMVP) [32] that are in accordance with FIPS 140 [33].

3.4 Risks and Countermeasures in LAN

This subsection corresponds with the lower and middle right area in Fig. 6. In Fig. 1, corporate networks, control system networks and field/sensor networks correspond with Local Area Networks (LAN). They are usually placed behind a firewall or a security gateway, and their levels of countermeasures tend to be lower than those accessible from Internet. Therefore, an adversary or malware, which succeeds in intrusion there, may proceed to next attack stages relatively easily if no countermeasures are taken. Intrusion into LAN is plotted by way of various channels including an attached file, a Web link in an e-mail, a shared folder, a brought PC, removal media such as USB memory, or even by a malicious insider. In case of ICS, engineering PCs or removal media may be brought in LAN to set-up or maintenance the systems and so on.

Activities after intrusion include communication with C&C (Command and Control) servers, investigation of the LAN while downloading and utilizing tools and/or modules necessary for further activities, escalating privilege, setting up backdoors, deleting logs, migrating to another network and so on. If an adversary or a malware reaches at a target, they try to collect secrets from it, modify its behavior or destroy it to reduce it to a critical situation or out of operation. In factories, secrets to protect include recipes for production. Mal-operations are attempted by way of HMI or by modifying control logics and set points for automatic control.

Basically, countermeasures in LAN should be taken by assuming that adversaries may exist there. One fundamental countermeasure is to divide both LAN and physical space into small zones to restrict or block unnecessary access to critical systems in a zone from other zones. To do this, one has to start with grasping the current network topology and configurations correctly. This may be completed instantly while running the systems with active scan using Nmap. It would, however, disturb or disrupt sensitive ICS. ANTFARM (Advanced Network Toolkit for Assessments and Remote Mapping) [35] is one of the tools for this purpose, which can parse and analyze multiple sources of network information including network device configuration files, traffic logs and so on, and then create a visual depiction of the network without disturbing or disrupting sensitive systems in ICS networks.

While zoning may restrict or block unnecessary access to critical systems from other zones, it cannot restrict accesses from privileged or legitimate combinations of a terminal and an account for operation. For example, HMI and EWS in one zone need to have access to controllers in

\[^{†}\text{FIPS 140-3 is under development[34] as of August 2015, which corresponds with ISO/IEC 19790 (Security requirements for cryptographic modules).}\]
to determine allowed purpose computers that are used in various ways and hard blocks unpermitted actions.

There are two directions to deal with this. One is to enhance detection and prevention ability against terminal hijacking by monitoring the symptoms and anomaly with IDS/IPS (Intrusion Detection/Prevention System) or more holistically UTM (Unified Threat Management) or SIEM (Security Information and Event Management). The other is to enhance the authorization mechanism against system modifications by using multiple terminal authorization and safety installment.

As the former approach to detect and exclude hijacked terminals, we have studied monitoring and prevention in deeper system layers, which are device I/O, hypervisor and kernel as shown in Fig. 7. The approach in kernel [36], [37] checks the parent-child relationship of created processes to detect maliciously created or inserted processes by adversaries, in addition to the integrity check of binaries to detect their modification and replacement. It can also control the access to computing resources such as files, directories, devices, IP addresses and port numbers. The approach using lightweight pass-through type hypervisor [38], [39] provides monitoring function for system calls invoked in the guest OS, and hiding function for unnecessary peripheral devices to the guest OS to prevent data leakage and/or malware infection via removal media or peripheral devices brought from outside. The approach using a device I/O board [40] monitors I/O of HDD/SSD, USB and Ethernet, and then blocks unpermitted actions.

These approaches might not be suitable for general purpose computers that are used in various ways and hard to determine allowed/disallowed actions in advance. They, however, are applicable to computers dedicated to a specific purpose where most operation rules are fixed in advance. They also have an advantage that they can be applied to pre-installed and pre-configured OSes later on without changing their configurations whereas the approach using non pass-through type hypervisors require to reinstall device drivers or even abandon minor devices they do not support.

Depending on the system layer to be used, there exist pros and cons. While the deeper layer is better to prevent intruders from disabling the monitoring and prevention functions, available data become more raw and primitive and harder to analyze.

Even if the above approaches fail to detect hijacked terminals, mal-operations can still be rejected if multiple terminal authorization is used, which is realized by letting an operator input a command or order by one terminal and then confirm that with the other independent terminals. The requirements for the independent terminals are given as follows [41]:

1) [Separation:] To avoid simultaneous hijacking of all the multiple terminals, they must be placed in different zones (or built as different systems).

2) [Independent Authentication:] Credentials to authenticate the terminals must be unique to each terminal to prevent impersonation using the stolen credentials.

Needless to say, independent authentication cannot be realized with only the same credential, i.e. the same password and the same private key among the terminals for the multiple terminal authorization since an adversary who has hijacked one terminal may send both requests and their confirmations by using the same credential. While independent authentication can be realized using unique secret to each terminal or distinguishing terminals with physical ports of routers or hubs the terminals are connected, these cannot distinguish and trace the operators who committed malicious operations. In addition, when authentication servers are used, it is important to protect their databases as well since they hold verification data for all the terminals and users. LR-AKE (Leakage-Resilient Authenticated Key Establishment) [42] not only satisfies independent authentication but also provides operator authentication and resiliency against leakage of stored secrets from any side of servers (or their databases) and terminals without relying on expensive tamper resistant modules.

If either multiple terminal authorization or zoning is not employed or compromised, safety instrumented systems will be the last resort to maintain a safe state against mal-operations. Safety instrumented systems including failsafe, limit, interlock, foolproof and so on used to be designed mainly against accidental non-intended errors. They should furthermore take intentional mal-operations by adversaries into account. Study in [43] constructed a miniature process control system with safety mechanisms and zoning, analyzed consequences of modification of its set points and alarms, and then investigated how they can be detected and prevented.

4. Cyber Physical Security in Future

Needless to say, one of the most significant features of cyber physical systems is that they have interfaces with real world, and these interfaces might be abused from cyberspace to
attack on the real world. This threat is not only specific to ICS or more widely Industry 4.0 and Industrial Internet, but also becoming common even in consumer areas with IoT (Internet of Things). They have the following additional features:

1) **[Physical Access:]** While sensors, actuators and controllers in factories and critical infrastructures are placed mainly in physically protected areas, those for IoT especially for consumers or small enterprises will be placed or distributed through outside of the physically protected areas. Adversaries may have physical access to them, and some of them might be cracked, and then form which they may intrude or input malicious data or programs into a network while impersonating the cracked devices.

2) **[Privacy:]** While sensors for ICS are mainly used for measuring equipment and materials, those for IoT, especially for healthcare, wearable and so on, will be used to collect privacy related or personal data around users.

3) **[Intelligence:]** Systems will be more intelligent with the help of Cloud, Big Data Analyses, Machine Learning, AI (Artificial Intelligent) and so on. While users will be more dependent on the intelligence, the intelligence might be abused or maliciously controlled by adversaries.

To preserve privacy while collecting necessary data for the intelligence, the privacy preserving methods will play more important roles than ever. They include:

1) **[ID Anonymization:]** Either removing or replacing Personally Identifiable Information (PII) from a data set, or collecting data not identifying individuals but verifying that they belong to a certain group with certain attributes. The latter can be realized using anonymous authentications [44], [45] or group signatures over an anonymous channel [46], [47].

2) **[Data Anonymization:]** Modification of data sets by adding noise, rounding, suppressing and generalizing their attributes to satisfy a certain level of privacy metrics such as k-anonymity [48], l-diversity [49], t-closeness [50] and differential privacy [51], or to resist against de-anonymization attacks [52] while maintaining their statistical characteristics. To brush up these skills, anonymization and de-anonymization contest was held in Japan [53].

3) **[Encrypted Data Processing:]** Processing secrets or encrypted data without revealing or decrypting them until the final result is obtained. This can be performed using homomorphic encryptions, PPDM (Privacy-Preserving Data Mining) [54], [55], SMC (Secure Multiparty Computation) [56]–[59] and so on.

The above cryptographic solutions require devices to hold keys, which must be protected against steal of the devices by adversaries who will then analyze them both invasively and non-invasively. Keys in a stolen device can be protected, e.g. by using a tamper resistant module or LR-AKE Credential Service [60]. An advantage of the latter is that it does not rely on an expensive tamper resistant module. Another way of protection is to generate keys using PUF (Physically Unclonable Functions) [61], [62] instead of storing them on a nonvolatile memory, which can be read and copied easily. The generated keys can be used to encrypt or deliver other keys used in applications. Advantages of using PUF for key generation include: 1) the generated keys are not stored in the module when the power is off, 2) it is difficult to copy a PUF so that the copied PUF can generate the same keys for new challenges due to the physical unclonable properties of PUF, and 3) revealed keys can be replaced with fresh ones by changing the challenges to them or by using uncontrollable noises intrinsically caused in PUFs [63] and by correcting the noises at the other party (whereas delivering a new key after encrypting it with the revealed old key compromises the freshness of the new key).

Frequent and uncontrollable change of keys can mitigate the risk of keys to be extracted from the modules using side-channel information such as power consumption, electro-magnetic leakage, etc. If a PUF is deployed in a device, it can also be used to distinguish the genuine module from its counterfeits to enhance the traceability in supply chains when a hardware Trojan is discovered.

5. Conclusion

In this paper, the security in ICS is reviewed as a leading example of cyber physical security especially for infrastructures where identification of optimal sets of countermeasures is significant taking their restrictions and constraints into account. The necessity of cyber physical security in future will expand not only to various infrastructures, but also to consumer area with IoT where preserving privacy and physical protection of devices will play more important roles especially when adversaries can have physical access to them.

I hope this paper helps the readers who are not necessarily familiar with this area understand the situation of cyber physical security especially of ICS and IoT for consumers.

Acknowledgments

The author would like to thank the reviewers for their useful comments and suggestions. This research was partly supported by JST, Infrastructure Development for Promoting International S&T Cooperation.

References


Kazukuni Kobara received his Ph.D. degree in engineering from the University of Tokyo in 2003. He joined the Institute of Industrial Science of the University of Tokyo in 1994, and then moved to the National Institute of Advanced Industrial Science and Technology (AIST) in 2006. His research interests include cryptography, cryptographic protocols, cybersecurity, security risk assessment, etc. He received the SCIS Paper Award and the Vigennaire Award from IEICE in 1996 and 2003, respectively. He also received the Best Paper Award of WISA, the ISITA Paper Award for Young Researchers, the IEICE Best Paper Award and Inose Award, the JSSM Best Paper Award and RISONA Industry-Academia-Government Coordination Award in 2001, 2002, 2003, 2006 and 2013, respectively. He served as a member of ETC (Electronic Toll Collection System) security committees from 1999 to 2015, CRYPTREC (Cryptography Research and Evaluation Committees) from 2000 to 2008, the vice chairperson of MIC WLAN security committee in 2003, the chief investigator of INSTAC identity management committee from 2007 to 2010, ISO/IEC JTC1 SC27 WG2 expert from 2012 to present and IEC ACSEC (Advisory Committee on Information Security and Data Privacy) member and JP NC chair from 2015 to present.