International Journal of Security and Its Applications
Vol.9, No.7 (2015), pp.347-356
http://dx.doi.org/10.14257/ijsia.2015.9.7.32

Security Threats Recognition and Countermeasures on Smart Battlefield Environment based on IoT

Jung ho Eom

Military Studies, Daejeon University, 62 Daehakro, Dong-Gu, Daejeon,
eomhun@gmail.com

Abstract

In this paper, we drew new security threats on IoT (Internet of Thing) based smart battlefield environment and proposed countermeasures against them. DoD (Department of Defense) is focusing its attention on the development of unmanned combat systems (UCS) to prepare for future war. The IoT technology provides networking service to connect each other unmanned combat system. But, IoT has the security vulnerabilities of each element of the technology itself because the technology integrates several components to configure a specific service. And new security vulnerabilities will be caused when they are interconnecting. If we fail to defend the security threat that may arise from IoT based smart battlefield environment, we can't obtain intelligence superiority and furthermore will not be able to assure the victory of the cyber war. In smart battlefield environment applied to IoT, we can draw four main security threats; illegal remote control, information leakage, false information insert, and signal disturbance. And we propose countermeasures in response to these security threats; authentication, access control, intrusion prevention, and cryptography technology.

Keywords: *IoT, Security Threat, Smart Battlefield, IoT Security*

1. Introduction

Smart battlefield will be the new IoT (Internet of Things) based battlefield environment that combines the information & communication technology applied to IoT and national defense science technology. A modern battlefield is a network-centric warfare (NCW). This constitutes an information grid that connects the elements of all combat soldiers, weapons, military equipment and so on by utilizing computers, sensors, wired/wireless network. And it is warfare concept that increases war power by intelligence superiority through information sharing and integration as connecting intelligence collection systems, command and control system, and strike system [1]. Each system is connected to network for faster information collection, analysis, and sharing in network-centric warfare. By doing so, it is to obtain intelligence superiority and improve the real-time resilience on the battlefield. And the unmanned combat systems development has accelerated on the NCW environment. The unmanned combat system is a complex system to complement the existing human-oriented combat system by reducing the manpower and increases the combat effectiveness by operating the unmanned equipment in the NCW environment [2]. In modern battlefield environment, unmanned combat systems are mostly operated by remote control and a programmed procedure in advance. There are limits to share information among unmanned combat systems and operate autonomously.

ISSN: 1738-9976 IJSIA

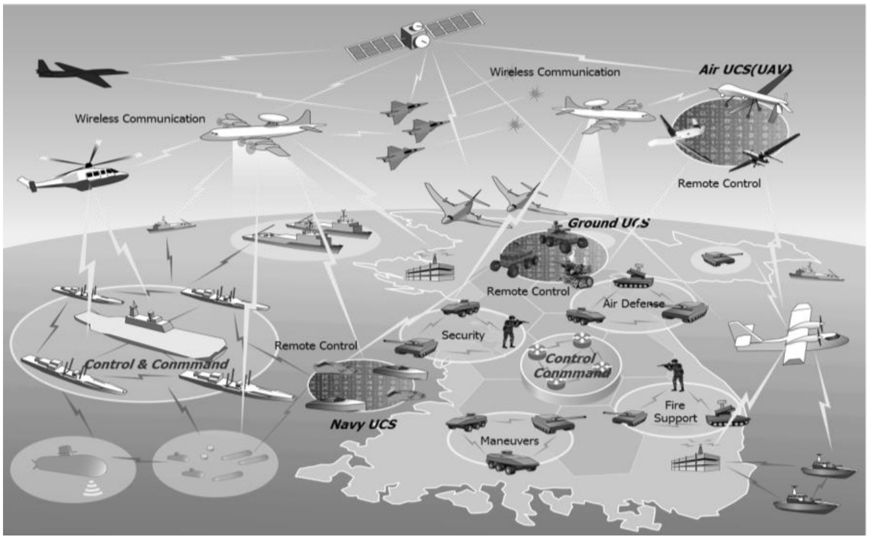

Figure 1. Smart Battlefield Environment

Ministry of Defense has planned to apply IoT to NCW environment. IoT is thing space network that form intelligent relationship such as sensing, networking, and information processing with mutual cooperation without human intervention on the distributed environment composed of human, thing, and service [3]. The most advantage of the IoT it to enable to communicate among the objects connected to the Internet. Ministry of Defense plans to build a smart battlefield environment beyond the NCW environment by utilizing these IoT advantages.

IoT has specific security vulnerabilities for each respective component because the physical and technology components are done seamless communication and information delivery from the end sensor to the user service. In addition, new security vulnerabilities which did not exist on each component could be existed by connecting each component [4]. If IoT applies to national defense information and communications systems, the similar security vulnerabilities will be happened. When communicating things and things in the IoT environment, the most primary security technique is a reliable mutual authentication. Consider that an authorization of some things takeovers to enemy due to hacking. All the information communicated to one another exposed to enemy, and military operations will be failed. So, it is important to identify these security vulnerabilities and necessary to establish countermeasures accordingly.

This paper organized as follows. We will describe IoT security threats in section 2 and security threats in the smart battlefield environment in section 3. We propose countermeasures on security threats in section 4, and conclude in the last section.

2. IoT Security Threats and Countermeasures

The Internet of Things (IoT) refers to technology for connecting things embedded with electronics, software and sensors on the internet. It also means connectivity to enable to achieve service by exchanging data with connected devices. Each thing has a unique IP to distinguish itself through its embedded computing system, and they are able to interoperate within the existing internet infrastructure. IoT is composed of three main factors such as human, objects, and service. IoT technology is to connect machine to machine, machine to man, and man to man. To connect to the factors, it is needed main component technologies such as sensing, communication and network, and service interface techniques. The sensing obtains information about the objects and the environment using a various sensors. The communication and network refers to all wired and wireless networks that can be connected to the human, objects, and service. The service interface is responsible for interlocking IoT factors and the application service to perform a specific function [3, 5-6].

In IoT techniques, new security vulnerabilities are possible to occur when interconnecting each component technologies. Of cause, it has the security vulnerabilities of each element of the technology itself because the technology integrates several components to configure a specific service. It is difficult to guarantee security in IoT environment because there are various subjects such as devices provider, communication & network provider, service developer, API developer, platform providers, and data owners, etc. According to Cisco [7], there are devices connected to each other more than 10 billion worldwide and is expected to be exceeded 50billion by 2020, and is expected to record 50% growth over the next three years. When this occurs, the security threats targeted on IoT is expected to increase as much. The following table shows IoT security vulnerabilities.

Table 1. IoT Security Vulnerabilities

Components	Security Vulnerabilities
Devices	Infrastructure paralysis by devices and equipment malfunctions, information leakage and forgery caused by device loss, theft and forgery, malware transition and threats between devices, difficulties of IP security technology application in lightweight and low power required equipment,
Networks	Information leakage and forgery in the interworking communication between heterogeneous IoT, network and gateway hacking, IoT DDoS by the large-scale things Bots, the signal data confidentiality and integrity violations
Platforms	Unauthorized access and attacks on platforms by malicious devices and users, platform collapsed threat by the encryption key hacking
Services	Invalid authentication by sniffing attacks, personal information leakage and privacy invasion in cloud and big data

It is likely to threaten human life by hacking vulnerabilities of cars, health care system and so on as well as invasion of privacy. In particular, a variety of security problems associated with the movement of a number of data has been a trending. Zombie home appliances are realized as detecting spam and phishing sending cases of 75 million using smart TV or refrigerator connected to the Internet like zombie PC. And it is demonstrated that hacker can manipulate to break into the wireless IP camera via a search engine 'Shodan' which find all the component things connected the server, webcam, printer, and router to the internet. In Black Hat 2013, researchers revealed how Toyota Prius and the Ford Escape, which are the most popular vehicles in the US, to hack cars that can be manipulated at will in the notebook. In Black Hat 2014, security researchers show off the things they create for hacking techniques that the drone would fly around sniffing out WiFi networks has hardware inside that allows it to spoof a cell phone tower [8]. There could be caused the reverse effects such as information disclosure, data modulation, service stop, an invasion of privacy and so on through such security threats. The following table shows the security threats on the IoT components. The following table shows examples of security threat.

Table 2. Examples of IoT Security Threat [9]

Security Vulnerabilities
Collect personal information regardless of time and place by Google Glass Possible to steal passwords and financial information from bank accounts by Google Glass
The private video was leaked by hacking a camera mounted on a smart TV in USA
The privacy and sensitive information saved at smartphone was leaked by UAV
Seized control of the flight-in UAV that use commercial GPS receivers by a spoofing attack
Possible to monitor in real-time with the camera mounted on the robot vacuum cleaner by hacking the vulnerability of the authentication method which needs for remote control of the robot cleaner and AP security settings of the application
Demonstrated remote control room temperature, TV on-off, blinds, etc. in China hotel with iPad2 by using KNX protocol based vulnerability
Can operate brake, orientation, and release alarm device by controlling access area network(CAN) installed in the engine to the computer system check

IoT security must be addressed throughout the network & communication, device, and service [10-12]. In the network & communication security, there are three primary security techniques; access control, lightweight encryption and security protocol. Access control technique manages access to various resources (data, application, services, hardware, etc.) as identifying users who has an access authorization, resources which user want to access. And it constrains to request by users who hasn’t a legitimate authorization to access resources in the system. Access control prevents unauthorized entities from obtaining access to system resources. It also ensures that legitimated entities can only access the resources they have authorization to access. Therefore, trusted access control policies must be established for secure communication in the IoT network. The lightweight encryption and security protocol are necessary to block the leakage of data transmitted over the network. The public key encryption technique is often useful to prevent changing or deleting transmitted data (Data Integrity).

In the device security, security expert proposes identification and authentication, access control, and security system. Identification is to uniquely identify objects and manage their identities before authenticating as legitimate objects while connecting IoT infrastructure. Authentication defines the access rights after an entity gains access to a system in the identification process and plays a major role before connecting a communication channel among various entities. In the IoT, authentication is very important to confirm mutual trust between different objects, users or systems by verifying their identities. Device authentication allows accessing a network or other devices by using a similar set of trust tables stored in a secure server. Firewall and intrusion prevention system (IPS) also need to block or inspect packet to control traffic that is destined to terminate or overload at the device. They need to filter the suspect data destined to terminate or overload at the device.

In the service security, authentication and resources management are needed. An authentication management is to isolate from operation system logically for protecting device operation system, hardware, etc. from data coming from outside through virtualization technology. It also must authenticate whether the received data is transmitted from authenticated sensors or devices, and guarantee the data integrity by encryption techniques. A resource management is to manage and distribute device and sensor resources efficiently, considering that IoT device and sensor’s lightweight resources is vulnerable to a DoS attack.

In the semantic white paper [13], they presented the minimum security techniques to protect the IoT environment as following table.

Table 3. Advice to Reduce the Risk in the IoT

Advice
Use strong passwords for device accounts and Wi-Fi networks
Change default passwords
Use a stronger encryption method when setting up Wi-Fi networks such as WPA2
Disable or protect remote access to IoT devices when not used
Use wired connections instead of wireless if possible
Necessarily check when buying used IoT devices, as they could have been tampered with
Apply the vendor's device security measures
Modify and strengthen the privacy and security policy settings of the device to your needs
Disable functions that are not being used
Always install updates when they become available
Use devices on separate home network if possible
Ensure that a power outage, for example due to disturbance or a network failure, does not result in a unsecure state of the installation
Verify if the smart features are really required or if a normal device would be sufficient before installing or using

3. Security Threats in the Smart Battlefield Environment

DoD said it would promote the transformation to operations readiness based on IoT that is intelligent technologies and service to communicate information between human and things, things and things which are connected information and communication technologies and all the things to internet. If such initiatives are realized, it possible to perform mission in condition that command post as well as various weapons systems and even each soldier linked to the internet and to share allies and enemies information in real-time.

IoT is applicable to the various field of national defense such as surveillance and reconnaissance systems, soldiers combat uniform, logistics supply, etc. In particular, IoT is very useful to collect, analyze, and share information. And intelligence refers as useful information which analyzes, filters, and remanufactures raw data (information) collected from intelligence, Surveillance, and Reconnaissance (ISR) system. In other words, intelligence defines as the product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information such as hostile or potentially hostile forces or elements, or areas of actual or potential operations. It is also a valuable data when it contributes to the commander's decision-making process by providing reasonable perception into future battle conditions or situations. If the IoT is applied to the information field, it is possible to shorten the data collection, analysis, and the sharing time. Data collected from each combat system performs a primary filter by using big data analysis technologies, in case of urgent intelligence, all combat systems can share intelligence directly [14-16].

IoT can be applied unmanned combat systems, combat soldiers, precise guided munitions, Army/Navy/Air Force combat platforms, surveillance and reconnaissance systems, and so on. In the modern battlefield, if IoT is applied to a process of information collection and analysis, target acquisition, weapons selection, and target attack, important security threats are remote control, information leakage, false information insert, and signal disturbance. The following figure is showing security threats in the Smart Battlefield Environment applied to IoT.

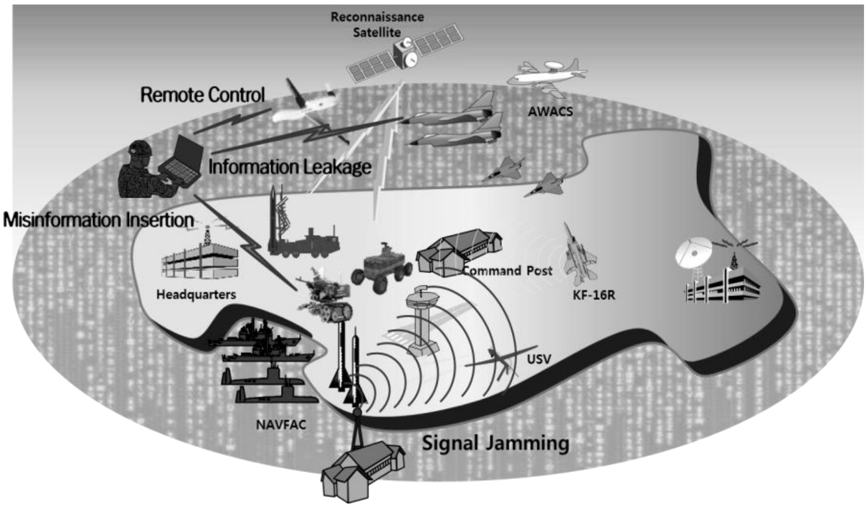

Figure 2. Security Threats in the Smart Battlefield Environment

Remote control is to seize control by acquiring access authorization of unmanned combat systems (UCS). Firstly, the attacker obtains access authorization of user as cracking the password or finding system vulnerabilities. And it seizes the super user privilege by using the user's access authorization. If the Window operating system is installed at UCS, the attacker can install a remote control program using Windows security vulnerability without the security system's detection. As mentioned earlier, in the Blackhat 2013, hacking competition participant demonstrated that it is possible to do the remote control a car which could be used a cellular service or Wi-Fi network by hacking. The control of the device can be easily lost to enemy in the IoT environment because the communication is connected between human and device or device and device without sufficient security techniques. The attacker can degrade the enemy's combat power as preventing attack by the unmanned combat systems and making to attack each other, using remote control of unmanned combat systems. If the remote control of UCS is handed over to enemy, the military operation control as well as intelligence superiority is same to hand over to enemy.

Information Leakage is to extract information that is propagated through the network, using sniffing or ARP spoofing attack techniques. IoT technology has a great advantage which can send and receive information between the objects without human intervention. However, most devices connected to IoT technology transmit the collected information to the cloud or a local network in the unencrypted state. It also uses a web interface which has security vulnerabilities, and does not use encryption when updating software. In other words, IoT technology is very vulnerable to encryption and access control so far. In Blackhat 2014, a security expert demonstrated that the Google Glass can collect personal information regardless of time and place. If enemy leaks operations plan or location in advance by hacking objects, war power could be not concentrated on the battlefield, the joint operations with ground, navy, and air force will fail. And it cannot guarantee victory in war.

False information insert is inserted into incorrect information on target or replaced transmitted information to fake information, using replay or session hijacking attack techniques. It is a data forgery/tampering attack technique that an attacker disguises as the legitimate communicator using the non-authorized communication terminal and deceives as the legitimate information after forgery or tampering information intercepted from network. According to security company IOActive Labs, they announced that a broad range of design and security flaws are found by investigation results from the road vehicle sensing technology. In particular, the attacker was possible to transmit a fake data to the traffic management system or control the major infrastructure such as traffic lights by masquerading as legitimate sensors. In Blackhat 2013, TVshing used the man-in-the-middle attack (MITM) has been released. TVshing (TV+Smishing) is a technique in which an attacker sends manipulated subtitles instead of the original broadcast subtitles by intercepting the communications of the TV and set-top boxes [9]. If false the target information is inserted in communication between unmanned combat systems, the exact strike isn't conducted and the military operations will be caused confusion.

Signal disturbance is to paralyze the communication as emitting a stronger output of frequency noise than radio wave frequency of the radar or communications equipment. In IoT environment, one of major required techniques is low power or power supply technology that can withstand as long as possible in as limited power. The communication radius, data transfer rate, and power consumption supported by the objects change according to the communication scheme of things. The power of the device consumes heavily because IoT service is consisted of a large number of devices and the end to end data transmission occur frequently. If the power of the device is weaken, a normal data flow will be hard, communication radius also reduces, and the communication strength will weaken. Since the unmanned combat systems must conduct combat missions on the battlefield for a long time, communication between the unmanned combat systems will occur frequently, they also will transfer a lot of data. If the power will be consumed much, it cannot communicate smoothly between unmanned combat systems, and enemy easily disturbs the frequency using a low frequency disturbance devices. Any communication or data transfer can't between the unmanned combat systems in the signal disturbance situation.

4. Countermeasure on Security Threats in the Smart Battlefield

As discussed earlier, the main security challenges for smart battlefield environment are from the large scale of objects connected to Internet. In this section, we will discuss these security issues with more details.

❍ Unmanned Combat System (UCS) Identification and Authentication

An identification is to uniquely identify the unmanned combat system and manage their identities from firstly access smart battlefield network to the combat ends [12, 17]. It is a method to identify UCS involved in the IoT, and the management of their identities is fundamental for keeping robust authentication. In particular, when UCS is firstly access to the IoT networks, it should identify itself before connecting or transmitting data. The easiest way to identify the UCS is to determine based on it has ever connected to the IoT network previously. For example, if the ID of UCS requesting access is included in the ID list of connectable UCS, it is recognized as a legitimate UCS. If not in the list, it is determined the access through the more sticky identification procedure. And if it has been denied access previously, it must be reported promptly to security administrator.

An authentication is to verify the permission to perform the task in identified UCS, and prevent forgery and unauthorized access to the smart battlefield network. In smart battlefield environment, an authentication should confirmed mutual reliable between UCSs, UCS and post by verifying their identities. In this section, we propose a more reliable two-way and factor authentication and biometric authentication mechanism. A two-way and factor authentication is used to UCSs, the biometric authentication is applied to human (users). A two-way authentication may block to connect by hacking through UCS mutual authentication. A two-factor authentication is to process a thorough authentication procedure with different authentication factors. Biometric authentication provides verification of the user's identity by matching the measured biometrics attributes with his biometric template stored in the database. It is essentially user characteristics recognition system that operates by extracting from physiological characteristics of a user into templates, and compares these templates set with the template set in the database. So, the controller tries to connect to UCS for doing remote control, it is possible to improve the reliability by using the biometric authentication in the authentication step.

❍ Access Control

Access control is necessary to block unauthorized UCSs and users from obtaining access to smart battlefield's resources, and to ensure that authorized UCS and user can only access the resources they are allowed to operate. In smart battlefield environment, a number of networks are built, there are many operating UCSs. In other words, each group or the allied forces operates networks and UCSs, and even, enemy operates their networks and UCSs. It should be restricted to use only the resources of the smart battlefield by only UCS and user that have legitimate authorization. The resource usage must be separated by each group and the allied forces, and also be separated by roles and missions. In this study, we propose a layered mission-based access control mechanism. This subsequently allowed to access the type of military, specific roles, conducting mission in the smart battlefield. For example, suppose unmanned aerial vehicle (UAV) which has a mission of imagery information collection transfer imagery information to air force information analysis center on ground and receive the following mission from commander post. Firstly, it will determine whether the UAV belongs to air forces, and whether its role is an information collection or not. Finally, it will determine the permission to access the air forces information analysis center, making sure whether its mission is an imagery information collection or not.

❍ Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)

It is hard to guarantee complete security in the smart battlefield which is consisted of different and heterogeneous wire or wireless networks such as information transmission system, command and control system, and remote control system, etc. [17]. Intrusion detection is to detect attacks in real-time, which try to access the battlefield network without authorization for leaking information and inserting false information or paralyzing smart battlefield network. In smart battlefield, even if the rate of false alarms is somewhat higher, we recommended anomaly based detection technique which inspects all suspected traffic incoming from outside. We also recommended a host-based intrusion detection technique to ensure the security of the UCS.

Intrusion prevention system (IPS) examines all traffic incoming from outside, when it is determined a suspicious packet, blocks all incoming traffic from the IP address or port. IPS is a proactive intrusion detection technology that inspects the packets to attack UCS in real-time and blocks the suspicious packets not going to intrude. IDS and IPS applied to the smart battlefield must detect intrusion in real-time and block it immediately, and analysis and report is progressed later. If they can't block the intrusions in rea-time, UCS control is passed to enemy or smart battlefield network is paralyzed, and the operational superiority couldn't guaranteed in the combat.

❍ Lightweight Encryption Techniques

The protection of data transferred between UCS is very important in the smart battlefield. In other words, it is necessary to keep the confidentiality and integrity of data. For example, when transmitting information about the attack target between UCS, if the information is leaked to enemy by hacking, military operation will be failed. There are encryption techniques to protect the information of the military operation. It is possible to block to know the content of the information if hacker has not a decryption key even though information is leaked to hacker. Because most UCS requires a small area, low power consumption, etc. for rapid maneuver and operational capability of a long time, the performance of the CPU and MCU which are the basis of the encryption system is relatively low. Therefore, we recommend a lightweight encryption for applying to the smart battlefield environment. A small hardware chips must be installed in UCS system, and the encryption computation speed should be fast. It also has the efficiency of the key generation, and needs to maintain a normal level of security by a small key size.

❍ Low Power Technology

As described above, when the UCS is conducting its mission, if the power is weakened, the efficiency of data transmission is lowered, and the communication between UCS doesn’t connect normally. If so do, the communication between UCS can be paralyzed by enemy’s simple signal disturbance. A solution is a low power technology that can withstand as long as possible in a limited supply terminal. For example of CPU, it could be saved power that task which is complex and has many data throughput is allocated to a high-performance core, and simple task is allocated to the low power core. Or it is also technology that the power assigns to frequent used component of the communication chip.

In addition, there are many security techniques such as firewall, secure booting, updates and security patches, etc.

5. Conclusion

Future battlefield will be transformed into a smart battlefield applied to IoT technology. If the IoT technology applies to the battlefield network environment, new security vulnerabilities will be occurred. So, in this paper, we drew new security threats on IoT (Internet of Thing) based smart battlefield network environment, and proposed countermeasures against them. DoD is focusing its attention on the development of unmanned combat systems (UCS) to prepare for future war. The infrastructure for UCS operation is more efficient to apply IoT technology to battlefield network. The IoT technology provides networking service to connect each other unmanned combat system. But, IoT has the security vulnerabilities of each element of the technology itself because the technology integrates several components to configure a specific service. And new security vulnerabilities will be caused when they are interconnecting. If we fail to defend the security threat that may arise from IoT based smart battlefield environment, we can’t obtain intelligence superiority and furthermore will not be able to assure the victory of the war.

In smart battlefield environment applied to IoT, we can draw four main security threats; illegal remote control, information leakage, false information insert, and signal disturbance. And we propose countermeasures in response to these security threats; authentication, access control, intrusion prevention, and cryptography technology. An authentication is to verify the permission to perform the task in identified UCS, and prevent forgery and unauthorized access to the smart battlefield network. Access control is necessary to block unauthorized UCSs and users from obtaining access to smart battlefield’s resources, and to ensure that authorized UCS and user can only access the resources they are allowed to operate. Intrusion detection is to detect attacks in real-time, which try to access the network without authorization for leaking information and inserting false information or paralyzing smart battlefield network. Intrusion prevention system is a proactive intrusion detection technology that inspects the packets to attack UCS in real-time and blocks the suspicious packets not going to intrude. The encryption technique is to protect the information of the military operation. In addition, there are many security techniques such as firewall, secure booting, updates and security patches, etc.

In future, we will research the technical details and the effectiveness of the proposed countermeasures by implementation of each countermeasure.

Acknowledgements

"This paper is a revised and expanded version of a paper entitled [Security Threats on National Defense ICT based on IoT] presented at [UCMA2015, Porto and 21~23 June]."

References

[1] J.-h. Eom, "An Introduction of cyber Warfare", hongpub, (**2012**).
[2] H.-B. Bang, "Role and Future of Unmanned Combat System", (**2011**).
[3] Ho.-w. Kim and D.-k. Kim, "IoT Technology and Security, Journal of Information Security", vol. 22, no. 1, (**2012**), pp. 7-13.
[4] H.-w. Kim, "Issues of Security/privacy in IoT Environment", TTA Journal, vol. 153, (**2014**), pp. 35-39.
[5] http://en.wikipedia.org/wiki/Internet_of_Things
[6] K. Zhao and L. Ge, "A Survey on the Internet of Things Security", Proceedings of Ninth International Conference on Computational Intelligence and Security (CIS2013), (**2013**), pp. 663-667.
[7] "Increasing Security Threats targeted on IoT", KISA Monthly Cyber Security Issue, (**2014**), pp. 7-8.
[8] J.-h. Eom, "New ICT Techniques' Security Threats and Countermeasure", 2014 National Defense Information Conference, (**2014**)
[9] "IoT Trend and hot issue", Institute for information & communication Technology Promotion (IITP), Insight 4 (**2014**).
[10] "SECURITY IN THE INTERNET OF THINGS", WIND River white paper, (**2015**).
[11] B.-I. Jang and C.-S. Kim, "A Study on the Security Technology for the Internet of Things", Journal of Security Engineering, vol. 11, no. 5, (**2014**), pp. 429-438.
[12] Z.-K. Zhang, "IoT Security: Ongoing Challenges and Research Opportunities", 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications (**2014**), 17-19 Nov., Matsue Japan.
[13] M. B. Barcena and C. Wueest, "Insecurity in the Internet of Things", the Symantec white paper (2015).
[14] [14] Jung ho Eom, "Roles and Responsibilities of Cyber Intelligence for Cyber Operations in Cyberspace", International Journal of Software Engineering and Its Applications, vol. 8, no. 9, (**2014**), pp. 137-146.
[15] M. E. Dempsey, Joint Intelligence, Joint Publication 2-0 (**2013**).
[16] W. E. Gortney, "department of Defense Dictionary of Military and Associated Terms", Joint Publication 1-02, (**2014**).
[17] I. Alqassem and D. Svetinovic, "A Taxonomy of Security and Privacy Requirements for the Internet of Things", 2014 IEEE International Conference on Industrial Engineering and Engineering Management (2014), 9-12 Dec., Bandar Sunway Malaysia.

Author

Jung ho Eom, he received his M.S. and Ph.D. degrees in Computer Engineering from Sungkyunkwan University, Suwon, Korea in 2003 and 2008, respectively. He is currently a professor of Military Studies at Daejeon University, Daejeon, Korea. He is now the director of cyber forces development and CPO forum. His research interests are information security, cyber warfare, network security.