International Journal of Security and Its Applications
Vol. 10, No. 8 (2016), pp.13-22
http://dx.doi.org/10.14257/ijsia.2016.10.8.02

An Empirical Study of the Military IoT Security Priorities

Seung-hoon Jung[1], Jae-choon An[2], Jin-young Park[3], Yong-tae Shin[4] and Jong-bae Kim[5*]

[1]156-743 Department of IT Policy and Management, Soongsil Univ., Seoul, Korea
[2]156-743 Department of IT Policy and Management, Soongsil Univ., Seoul, Korea
[3]156-743 Graduate School of Software, Soongsil Univ. Seoul, Korea
[4]156-743 Department of IT Policy and Management, Soongsil Univ., Seoul, Korea
[5]156-743 Graduate School of Software, Soongsil Univ., Seoul, Korea*
[1]hoonyjung9999@gmail.com, [2]anjaechoon46@naver.com,
[3]jin0902666@naver.com, [4]shin@ssu.ac.kr, [5]kjb123@ssu.ac.kr*

Abstract

Recently, in many countries, military has adopted Cloud, Big Data, IoT, etc. in order to win the war. Therefore, a favorable environment for future battles based on the soldiers with a variety of IoT technologies that will foster and build elite combat forces in the center can be expected. Similar to the conventional Internet environment, IoT is not only the type of security threat for a variety of networks, data, and personal information for each of the features has also identified protocol management. Therefore, to enhance the security of the environment in the future IoT based on full-length, it is necessary to study the security priority. A recent survey of military IT professionals shows communications / network security is the most important sector. In addition, the survey can distinguish between the security field will be considered fragile. To the study of future IoT-based battlefield, see the results of this study are reflected in the professional military security structure, we should effectively against threats expected in a given amount of the budget.

***Keywords**: Military IoT, security priority, Military IT, Internet of things*

1. Introduction

Since 2003, Future Combat Systems (FCS), which started in the U.S. Army, has shown many implications. FCS is equipped with various sensors for detecting the type of equipment and weapon system, provided that each soldier uses it [1].

Since recently, the South Korean military has committed to effectively perform the mission of synchronizing the cloud, big data, and Internet of things (IoT) with reference to a case such as FCS.

Further, a significant reduction of the population is expected in the future; thus, it can be assumed that there will also be a reduction in the number of military personnel. Therefore, it is absolutely necessary to take advantage of IoT, *etc*. in helping a handful of soldiers become elite combat forces of the center. To realize this, various IT technologies are expected to be equipped with a variety of systems that will enable each soldier to use the IoT technology in the battlefield, and that will thus configure the battlefield of the future based on IoT.

In this way, the military environment will become more complex, consisting of a simple sensor and equipment with IoT suitable for the structured synthesis conditions. Also, cyber threats due to the changes in this environment can be expected to occur more frequently. IoT has the same Internet security threats as in the existing environment.

[5*] Corresponding author. Tel. : +82-10-9027-3148.
Email address: kjb123@ssu.ac.kr(Jong-Bae Kim).

ISSN: 1738-9976 IJSIA

It has faced various security threats designed for its characteristics, such as the IoT environment as well as additional protocol, network, and data, and is equipped with a privacy threat identification management system [2].

Therefore, to enhance the security of the future IoT battlefield environment, measures must be taken to anticipate and respond in advance to the expected security threats.

2. Related Works

2.1. Features of the Future Battlefield Environment

According to development of military and civilian technologies, changes in the warring concepts and the recent case of war. Battlefield environment of the future is changing in aspect to achieve the goal by securing geographical objectives as before, or to exercise physical force identified the enemy important core nodes and hit the center rather than to choose a way to end the war in advance [3].

This is in accordance with recent changes in the major industrialized countries 'Command, Control, Communication, Computer & Intelligence (C4I)', 'Intelligence, Surveillance & Reconnaissance (ISR)' and 'Precision Guided Munitions (PGMs)' including the United States , with interconnected systems such as complex precision strike systems (C4ISR + PGMs) are making an effort to take advantage of the various unmanned combat systems [4].

Our military have concept that future Joint Operations basic idea as 'Aggressive integrated operations'. The concept is integrate effort, capability, activity, time and space in the ground, sea, air, universe and cyberspace under network centric warfare to maximize the synergies and to attack the enemy's center has a notion of victory in the war [5].

To this end, the United States established a modernization strategy, the so-called 'The Army Modernization Plan 2012 (ModPlan12)' around the Army in 2012 and are going to develop through continuous modification supplement, the more detail in conjunction with the US army's Brigade Combat Team (BCT) Modernization Plan established its modernization strategy of Army equipment it is under [6-8].

2.2. IoT Security Vulnerabilities and Attack Types

IoT is a composite of a variety of techniques, such as protocols, IoT sensors/devices, gateways, middleware platforms, and IoT services. It is organically combined with the interaction. IoT has physical configurations, including various technical elements, such as a communication/network and data mining technologies, a service mash-up technology, a technical service API, and a user interface technology. Therefore, it may have a variety of security vulnerabilities or flaws, and there may be specialized component parts connected to each of the components [9, 10].

A summary of the security vulnerabilities of IoT is shown in Table 1.

Table 1. IoT Security Vulnerabilities

IoT target areas	Security vulnerability
Communication/ networks	Worm, virus, DoS/DDoS, inappropriate firewall, protocol vulnerabilities, confidentiality/integrity attack
Device	Worm, virus, unauthorized access, OS vulnerability attack, clone attack, unauthorized I/O, setting mistake & error, confidentiality/integrity attack, unsafe firmware attack, fake signal attack, discharge battery attack

Gateway	Worm, virus, unauthorized access, OS vulnerability attack, clone attack, unauthorized I/O, setting mistake & error, confidentiality/integrity attack, unsafe firmware attack
Platform	Worm, virus, unauthorized access, OS vulnerability attack, improper use of anti-virus software, unauthorized I/O, inappropriate recording in the system log, setting mistake & error, confidentiality/integrity attack, privacy invasion
Application services	Worm, virus, unauthorized access, OS vulnerability attack, improper use of anti-virus software, unauthorized service, unauthorized user, unauthorized I/O, inappropriate recording in the system log, setting mistake & error, unsafe-password attack, confidentiality/integrity attack, privacy invasion

The possible attacks on IoT can be divided into five categories: acquisition, imitation, blocking, privacy attacks, and hindrance. The acquisition attack includes skimming, tampering, eavesdropping, and traffic analysis attack. The imitation attack includes spoofing, cloning, and replay. The blocking attack includes service denial, service disturbance, and spreading of malicious codes. The privacy attack can be used to gain commercial advantage through the use of stolen information about each user's location, appetite, behavior (individual and group), *etc.*, or for a possible second attack. Finally, the hindrance attack may be an attack signal, such as for modulation or regarding battery consumption.

According to the transmitted and received order message or information to respond to such an attack, the policies and technology for performing decryption through the encryption module and the authentication of the legitimate device and the transmission and receipt of the information pertaining to the authenticated and authorized device are mandatory. The device may be authenticated through the user's stored and managed ID and by communicating with the authentication center of the service provider, the information collected about these devices, or the ID of the device user, can be mimicked. As it is exposed to the environment, it may be vulnerable to attacks on the service block [11, 12].

The possible IoT attacks in the environment and the types of measures that can be taken to prevent such attacks are shown in Table 2.

Table 2. Types of IoT Attacks and Countermeasures

Category	Types of attacks	Types of countermeasures
Acquisition	Skimming	Encryption, encrypted messages
	Tampering	Hash functions, message authentication
	Eavesdropping	Encryption, ID-based authentication
	Traffic analysis	Network forensics
Imitation	Spoofing	ID-based authentication, key distribution
	Cloning	Physically impossible to replicate the function
	Replay	Time stamps, time synchronization
Blocking	DoS/DDoS	Firewall, router control
	Spreading of malicious code	Vaccine
Privacy	Personal	Aggregate proving, advanced digital signature

Hindrance	Group	Selective disclosure, data distortion
	Signal modulation	Defensive interference
	Battery consumption	Battery control

3. Security Vulnerability Priorities in the Military IoT

Recently, in connection with the IoT research, the understanding of the situation of IoT was sought by a different group of IT professionals in the military. Their comprehensively conducted research on the relationships among the variables related to the IoT target population groups in terms of the error situation, however, has yet to be completed.

Therefore, in this study, areas thought to be vulnerable to the center of the IoT target area were selected, and opinions on the degree of risk for each of the vulnerabilities of each target sector were gathered to prioritize and synthesize the study results. The research model is shown in Figure 1.

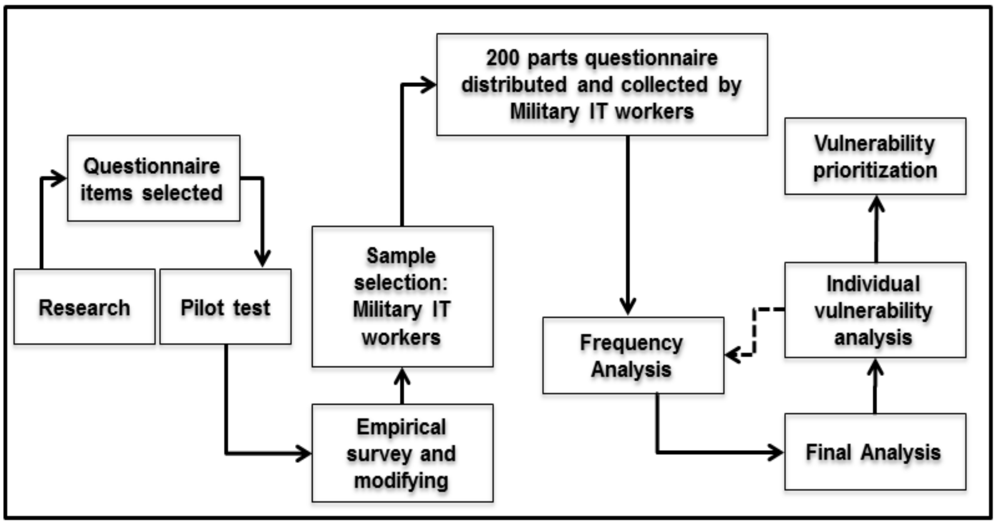
200 parts questionnaire distributed and collected by Military IT workers
Questionnaire items selected
Vulnerability prioritization
Sample selection: Military IT workers
Research
Pilot test
Individual vulnerability analysis
Frequency Analysis
Empirical survey and modifying
Final Analysis

Figure 1. Security Vulnerability Priorities Analysis Model in the Military.

This study was focused on how to find the relative influence of each of the elements shown, and how to analyze the effects of the cause of each variable used in the conventional survey analysis methods. The validity of each factor analysis problem is limited by the complexity of the IT sector, and the mutual AMOS structural equation has very diverse applications. Therefore, in this study, statistical processing using SPSS ver. 23, and frequency analysis, were carried out for rank selection. A questionnaire on the IoT security vulnerabilities identified in [9] and [10] was developed for measuring such vulnerabilities, based on a 7-point Likert scale.

While conducting research for comparison purposes, variables such as gender, age, number of years worked, education, and class included in the demographic questionnaire were excluded from the study analysis, and there is a need for a separate study including such variables. A total of 181 accomplished questionnaires were recovered from among the 200 that were distributed in February 2016 (90.5% recovery rate). To determine the reliability of the answers, analysis of 174 recovered questionnaires (minus the seven questionnaires with unanswered items) was conducted.

The results of the reliability analysis of the questionnaires are shown in Table 3. Cronbach’s α showed very good values (0.801-0.935).

Table 3. IoT Security Vulnerabilities

IoT target areas	No. of questions	Cronbach's α
IoT security vulnerabilities in the military environment	6	.809
Communication/networks	6	.835
Device	11	.853
Gateway	9	.877
Platform	10	.801
Application services	13	.935
Total	55	.966

With regard to the correlations between the IoT target areas shown in Table 4, one predicted unexpected vulnerability was chosen by many respondents. Communication/networks showed a normal correlation between gateway and platform. Platform had the strongest correlations with gateway, device, and application services. It can be seen, as a result, that the people recognize that IoT networking is formed around the platform.

Table 4. Correlation Vulnerabilities of the IoT Target Areas

		1	2	3	4	5	6
1. Communication /Networks	Pearson correlation sig. (2-tailed)	1					
2. Gateway	Pearson correlation sig. (2-tailed)	.491** .000	1				
3. Device	Pearson correlation sig. (2-tailed)	.268** .000	.368** .000	1			
4. Platform	Pearson correlation sig. (2-tailed)	.448** .000	.738** .000	.840** .000	1		
5. Application Services	Pearson correlation sig. (2-tailed)	.347** .000	.260** .000	.886** .000	.789** .000	1	
6. Unexpected vulnerabilities	Pearson correlation sig. (2-tailed)	-.075 .326	-.308** .000	.394** .000	.247** .001	.491** .000	1

** The correlation is significant at the 0.01 level (2-tailed), N=174.

In the analysis of each item's mean, standard deviation, minimum, maximum, and median values, the security vulnerability that was believed to be important was sought. Clean-up was deemed a priority for any vulnerability that is more dangerous than the average, and such vulnerability was corrected when the priority value to be represented by considering the median value was not deemed important. For example, the average score of a particular vulnerability is "1>2" than if the median is higher than "2>1. Therefore, when considering these ranking points, the "2>1" order was organized.

Table 5. Military IoT Security Vulnerability Analysis

IoT target areas	Average	Standard deviation	Minimum	Maximum	Median
Communication/networks	6.26	.967	4	7	7
Gateway	5.12	1.008	4	7	5
Device	5.50	.758	4	7	6
Platform	5.21	.830	4	7	5
Application services	5.60	1.059	3	7	6
Unexpected vulnerabilities	6.44	.667	5	7	7

For the vulnerability of the battlefield environment, IoT as applied to the group, as shown in Table 5, was analyzed. When considering the median, among all the vulnerabilities, the vulnerability of the communication/network is thought to be more important. There were no vulnerabilities in unexpected parts in addition to the known vulnerabilities.

Considering the mean and median ranks, the security vulnerabilities of the communication/network, application services, device, platform, and gateway were considered most important, in descending order.

For the military environment, the IoT communication/network security vulnerabilities results are shown in [13]. Considering the average and median values, the security vulnerabilities were ranked as follows (in descending order): DoS/DDoS> protocol vulnerabilities> inappropriate firewall> confidentiality/integrity> worm/virus.

Table 6. Military IoT Device Vulnerability Analysis

IoT device vulnerability	Average	Standard deviation	Minimum	Maximum	Median
Worm/virus	5.40	.973	4	7	5
Unauthorized access	5.33	1.213	3	7	6
OS vulnerability attack	5.39	.978	4	7	5
Clone attack	5.21	.825	4	7	5
Unauthorized I/O	5.23	1.194	3	7	6
Setting mistake & error	5.51	1.157	3	7	6
Confidentiality/integrity attack	5.22	1.027	3	7	5
Unsafe firmware attack	5.68	.737	5	7	6
Fake signal attack	6.07	.790	4	7	6
Discharge battery attack	6.16	.566	5	7	6
Unexpected vulnerabilities	6.35	.781	5	7	7

Military security vulnerability results were obtained for the military IoT devices, as shown in Table 6.

Considering the median values of the vulnerability to unauthorized access attacks, the unauthorized I/O access attack involving vulnerability to configuration errors and mistakes, unprotected firmware attack vulnerability, battery consumption attack vulnerability, and sensor signal modulation attack vulnerability are considered the most important security vulnerabilities. It can be seen, in addition to the well-known weaknesses, that there were certain vulnerabilities that were unexpectedly vulnerable. The vulnerability importance ranks considering the average and median values are as follows: fake signal attack> battery discharge attack> unsafe firmware attack> setting errors and mistakes> unauthorized access attack> unauthorized I/O> worm/virus, OS vulnerability attack> confidentiality/integrity attack> clone attack.

Table 7. Military IoT Gateway Vulnerability Analysis

IoT gateway vulnerability	Average	Standard deviation	Minimum	Maximum	Median
Worm/virus	4.66	1.166	2	7	5
Unauthorized access	5.04	.958	3	7	5
OS vulnerability attack	4.74	.978	4	7	4
Clone attack	5.03	.964	4	7	5
Unauthorized I/O	4.66	1.089	3	7	4
Setting mistake & error	5.22	1.128	4	7	5
Confidentiality/integrity attack	4.75	.875	4	7	5
Unsafe firmware attack	5.12	.792	4	7	5
Unexpected vulnerabilities	5.79	.933	4	7	6

The military IoT gateway security vulnerability results are shown in Table 7.

The median values show that the military IoT gateway security vulnerability attack is perceived as somewhat less important compared to the prior-confirmed communication/network and device vulnerabilities.

In addition to the well-known vulnerabilities, it was thought that it would be an additional and unexpected vulnerability. Considering the average and median values, the vulnerability importance ranks are as follows: setting errors and mistakes> unsafe firmware attack> unauthorized access attack> clone attack> confidentiality/integrity attack> worm/virus attack> OS vulnerability attack> unauthorized I/O attack. The military IoT platform security vulnerability results are given in [13]. The importance ranks considering the average and median values are as follows: OS vulnerability attack> setting mistake & error> unauthorized access attack> worm/virus attack> privacy invasion> inappropriate recording in the system log> confidentiality/integrity attack> improper use of anti-virus software> unauthorized I/O attack. The military IoT application service security vulnerabilities results are given in [13]. The ranks considering the average and median values are as follows: unsafe password attack> setting mistakes & errors> worm/virus attack> OS vulnerability attack> unauthorized access attack> privacy invasion> improper use of anti-virus software> unauthorized user access> confidentiality/integrity attack> unauthorized access to services> inappropriate recording in the system log> unauthorized I/O attack.

Table 8. Comparison of the Group Values and the Average Value

IoT target areas	Group values			Average value		
	Average	Median	Rank	Average	Median	Rank
Communication/networks	6.2644	7	1	5.6954	5.8	1
Gateway	5.1149	5	5	5.0026	4.9	5
Device	5.5000	6	3	5.5961	5.4	3
Platform	5.2126	5	4	5.2839	5.2	4
Application services	5.5977	6	2	5.4058	5.5	2

The questionnaire was configured to consider the broad categories into which the IoT target areas could be divided. The subsequent details were considered to represent the vulnerability of each type. The comparison of the organized values was expected to enable a more precise selection of the priorities. The averages of the different areas were gathered and compared. For the results, the IoT target areas vs. the priority ranking of the general average value of each type were determined to be the same.

As shown in Table 8, the average value of the detailed vulnerability elements for the regions generally considered susceptible to security vulnerabilities had the same pattern. This result can be regarded as a very important finding in this experiment because each of the elements may influence the perception of the large area with the same content.

A summary of the security vulnerability priorities and of those that require clean-up every 1-3 days is shown in Table 9.

Table 9. Military IoT Security Vulnerability Priorities

Priorities	First	Second	Third
1st: Communication/ networks	DoS/DDoS	Protocol vulnerability	Inappropriate firewall
2nd: Application services	Unsafe password attack	Setting mistake & error	Worm/virus
3rd: Device	Fake signal attack	Battery discharge attack	Unsafe firmware attack
4th: Platform	OS vulnerability attack	Setting mistake & error	Unauthorized access
5th: Gateway	Setting mistake & error	Unsafe firmware attack	Unauthorized access

In the above table, the security vulnerability priorities can be seen. On the other hand, the vulnerability of setting errors and mistakes may have to be checked three times, and unauthorized access attack was mentioned twice, required the thorough checking of such vulnerabilities. The table also shows that in addition to the recognized or existing vulnerabilities, other vulnerabilities that did not appear in the list of priorities may surface. Finally, there is a need for continued research on the newly identified important vulnerabilities.

4. Conclusion

In this study, a survey was conducted among soldiers to identify the anticipated security threats to the military Internet of things (IoT). The priority rankings of such military IoT security threats and vulnerabilities were determined based on statistical evidence. Thereafter, the need to clean up the important priority "setting error and mistake," which was seen as an important vulnerability in many areas, was determined. Unauthorized access attack was also recognized as an important vulnerability. Through this, it can be seen that there is a need to promote a high specific gravity with the corresponding administrative system.

The protection of military information on existing policies and large budgets tends to be reflected on various projects that are in progress, and the introduction of a physical system with a corresponding spindle information protection system equipment is required. As shown in this study, however, there is a threat management system.

To address these points, including those that are still only in the introduction stage but can effectively respond to security vulnerabilities in the IoT battlefield. The survey results are actually accurate only when the application of military IoT is enabled; otherwise, the importance of the vulnerability is not easy to judge. Also, the next actual data value is expected to be a more accurate assessment through the complementary element.

References

[1] A. Feickert, "The Army's future combat system (FCS): Background and issues for congress", LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE, **(2006)**.

[2] R. Roman, N. Pablo and L. Javier, "Securing the internet of things", Computer 44.9, **(2011)**, pp. 51-58.

[3] M. O'Hanlon, "Technological change and the future of warfare", Brookings Institution, Washington, DC, **(2000)**.

[4] S. D. Richard, "Battlespace Technologies: Network-Enabled Information Dominance", Artech House Intelligence and Information Operations 1st Edition, Artech House, **(2010)**.

[5] R.O.K Joint Chiefs of Staff, "About Weapons", **(2016)** http://www.jcs.mil.kr/mbshome/mbs/jcs2/ebook/jcsbook/index.html.

[6] A. Feickert, "The Army's Ground Combat Vehicle (GCV) Program: Background and Issues for Congress", LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE, **(2013)**.

[7] U.S. Army, "Army Modernization Plan 2012", U.S. Army, **(2011)**.

[8] U.S. Army, "Army Equipment Modernization Strategy - Equipping the Total Force to Win in a Complex World", U.S. Army, **(2015)**.

[9] C. M. Medaglia and A. Serbanati, "An overview of privacy and security issues in the internet of things", The Internet of Things, Springer, New York, **(2010)**, pp. 389-395.

[10] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu and D. Qiu, "Security of the internet of things: Perspectives and challenges", Wireless Networks, Springer, New York, vol. 20, no. 8, **(2014)**, pp. 2481-2501.

[11] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions", Future Generation Computer Systems, vol. 29, no. 7, **(2013)**, pp. 1645-1660.

[12] L. Li, "Study on security architecture in the Internet of Things", Measurement, Information and Control (MIC), 2012 International Conference on, IEEE , vol. 1, **(2012)**, pp. 374-377.

[13] S. H. Jung, J. C. An, J. Y. Park, D. K. Kim and J. B. Kim, "An Empirical Study on the Security Priorities in the Future Battlefield Environment in Internet of things", Advanced Science and Technology Letters, vol. 129 (Mechanical Engineering 2016), **(2016)**, pp. 75-78.

Authors

Seung-Hoon Jung, He received his bachelor's degree of Computer Science & Engineering in Korea National Defense University, Seoul (2015). He is studying his master's degree of IT policy and management in Soongsil University, Seoul. His current research interests include IT policy and Computer Security.

Jae-Choon An, He received his bachelor's degree of Computer Science & Engineering in Korea National Defense University, Seoul (1996). He is studying his master's degree of IT policy and management in Soongsil University, Seoul. His current research interests include IT policy and Satellite engineering.

Jin-Young Park, She received her bachelor's degree of Business Administration in Soongsil University, Seoul (2016). She is studying her master's degree of software engineering in Graduated Soongsil University, Seoul. Her current research interests include Software engineering and Open source software.

Yongtae Shin, He is a Ph.D. professor in the School of Computer Science and Engineering at Soongsil University in Seoul, Korea. His research interests focus on Multicast, IoT, Information Security, Content Security, Mobile Internet and Next Generation Internet.

Jong-Bae Kim, He received his bachelor's degree of Business Administration in University of Seoul, Seoul(1995), his master's degree(2002) from the same university and doctor’s degree of Computer Science in Soongsil University, Seoul(2006). Now he is a professor in the Graduate School of Software at Soongsil University in Seoul, Korea. His research interests focus on Software Engineering, and Open Source Software.