ICIC Express Letters
Volume **14**, Number **8**, August **2020**

ICIC International ©2020 ISSN 1881-803X
pp. 829–836

ADVANCED TESTING METHODS ABOUT SECURITY FUNCTIONS BASED ON DIGITAL PRINTER

Wukjae Cha[1], Dongho Won[1] and HyukJun Kwon[2]

[1]Department of Electrical and Computer Engineering
Sungkyunkwan University
2066, Seobu-ro, Jangan-gu, Suwon-si, Gyeonggi-do 16419, Korea
{ wjcha; dhwon }@security.re.kr

[2]Department of IT-Finance Management
Soonchunhyang University
22, Soonchunhyang-ro, Shinchang-myun, Asan-si, Chungcheongnam-do 31538, Korea
gloryever@sch.ac.kr

Received February 2020; accepted May 2020

Abstract. *Digital printers used in public institutions and companies are complex devices that include numerous features in addition to the basic function of printing, such as copying, scanning, and faxing. The Common Criteria (CC) recently went through revisions regarding standard documents that are basis for revising standards related to the CCRA. Hence, this paper has added ATE_MTK, ATE_MTT, ATE_COMP and ATE_LCD categories to the existing test method for digital printers and added categories that verify the suitability and accuracy of evaluation methods for security products. Categories that can verify vulnerabilities in categories that were defined in the existing test method were added to propose an advanced test method with improved security. MTK is an abbreviation of TOE Modular Testing Knowledge, which is an item that can confirm the accuracy of the test. MTT is an abbreviation of TOE modular tracking possibility of test's functional requirements, and is an item that the test performs through the script. COMP is an abbreviation of compound functioning and is an item that confirms that the function is tested to meet the requirements. LCD is testing life-cycle model for test case. We believe that it can contribute to the appropriateness of the tests conducted through the fourth items.*

Keywords: Common Criteria, Digital printer security, Security sustainability, ISO15408

1. **Introduction.** Digital printers used by public institutions and companies are complex devices that include numerous features, in addition to the basic features of printing, such as copying, scanning, and faxing. It is a reality that the latest security threats are not prevented by evaluating them on old standards. Therefore, this paper suggests a more secure test method by adding ATE_MTK, ATE_MTT, ATE_COMP, and ATE_LCD categories to the existing digital printer test method and adding a category to verify the suitability and accuracy of the security product evaluation method [16-18].

Recently, hacking has been frequent with printers, and even though it reflects the latest security features of the printer, it has leaked a lot of confidential information. Therefore, it can be confirmed that it contributed to the development of technology test method and evaluation element technology based on security function of digital print.

In this paper, theoretical background is discussed in Section 2. We analyze to prepare test for security functions and digital printer security functions in Chapter 3, and make test method each security function in Chapter 4. Chapter 5 concludes paper.

DOI: 10.24507/icicel.14.08.829

2. **Theoretical Background.** Common Criteria describe testing methods coverage (ATE_COV), depth (ATE_DPT), independent testing (ATE_IND), functional tests (ATE_FUN) [17]. The general testing and analysis method involves five stages, namely prepare to test, test plan, build test environment, functional specification test, and test result analysis. As shown in Table 1, each test is executed according to the same format and the process and results must be clearly recorded [19].

Table 1. Filling out the test form

List	Content
Test objective	Purpose of the test
Test environment	Environment where the test is performed
Dependency	Test(s) that must be performed before or after the main test
Test procedure	Detailed process of conducting the test
Anticipated results	Results that are expected from the test
Actual results	Actual results of the test

ISO15048 discusses about tests list. The point is adequacy. CCRA added ATE_MTK, ATE_MTT, ATE_COMP to check more adequacy [3]. We proposed ATE_LCD to check adequacy and latest vulnerability.

Table 2. Comparison of ISO15408, CC standard and proposed

Item	CC standard	ISO15408	Proposed
Coverage	ATE_COV	ATE_COV	ATE_COV
Depth	ATE_DPT	ATE_DPT	ATE_DPT
Functional tests	ATE_FUN	ATE_FUN	ATE_FUN
Independent testing	ATE_IND	ATE_IND	ATE_IND
Vulnerability analysis	AVA_VAN	AVA_VAN	AVA_VAN
TOE modular testing knowledge		ATE_MTK	ATE_MTK
TOE modular traceability of functional requirements in tests		ATE_MTT	ATE_MTT
Composite functional testing		ATE_COMP	ATE_COMP
Testing life-cycle definition			ATE_LCD

3. **Proposed for Testing Method.** This chapter deduces items for testing/evaluating digital printer security functions that were analyzed in the previous chapters based on the Common Criteria. For this purpose, the test class (ATE) and vulnerability class (AVA) of the Common Criteria were referenced. The test class of the Common Criteria focuses on verifying whether or not the target product's security functions work according to the design. The vulnerability class addresses vulnerabilities that can potentially be misused during the product's development or operation [19].

As shown in Table 3 of Common Criteria v3.1, the test class and vulnerability class include the following families: ATE_COV, ATE_DPT, and ATE_FUN are families related to documents that were written and tests that were performed by the developer, and ATE_IND and AVA_VAN are families where the evaluator and test/vulnerability are linked. ATE_FUN is a family that is related to the legitimacy of the test conducted by the developer and is verified through the developer's document. AVA_VAN is related to the test regarding potential vulnerabilities. ATE_LCD is a family that is verified testing life-cycle model for test case. Tests are performed through the vulnerabilities reported in CIAC-2304 and IEEE P2600 for all security functions and major vulnerability analysis sites such as National Vulnerability Database (NIST) (http://nvd.nist.gov/),

Table 3. ATE class description

Class	Family	Description
ATE	COV	Verifies whether or not a security function was tested according to the statement of functions
	DPT	Addresses the level of detail of the security function test (directly tests internal interface)
	FUN	Guarantees that the test item on the test document was accurately performed and documented
	IND	The evaluator verifies the above tests and performs additional tests
	LCD	Verifies testing cycle
AVA	VAN	Tests potential vulnerabilities (function neutralization and evasion test)

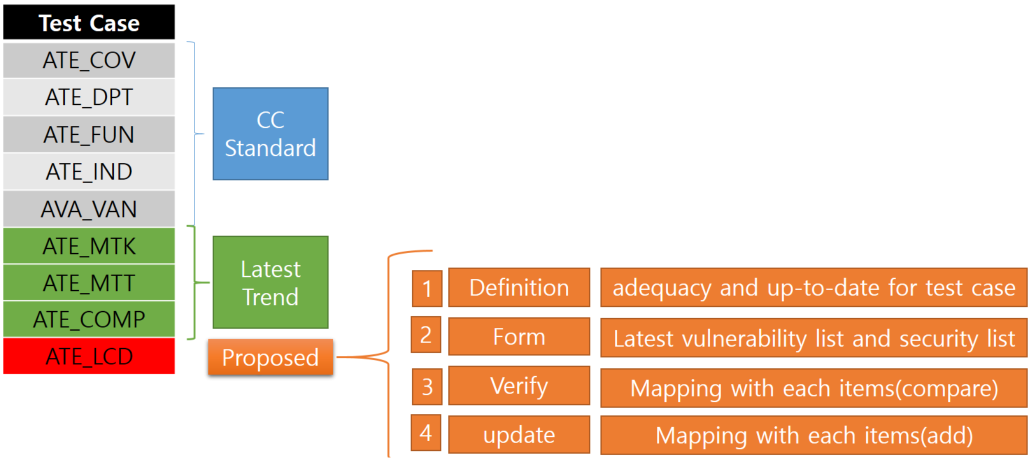

Test Case
ATE_COV
ATE_DPT
ATE_FUN
ATE_IND
AVA_VAN
ATE_MTK
ATE_MTT
ATE_COMP
ATE_LCD
CC Standard
Latest Trend
Proposed
1
Definition
adequacy and up-to-date for test case
2
Form
Latest vulnerability list and security list
3
Verify
Mapping with each items(compare)
4
update
Mapping with each items(add)

Figure 1. Proposed testing method

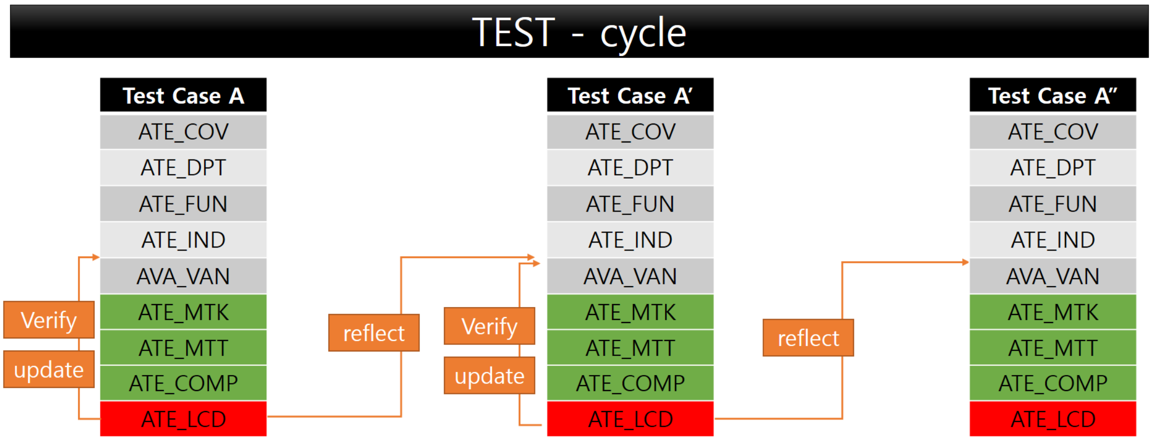


Figure 2. Proposed test cycle

SecurityFocus bugTraq (http://www.securityfocus.com/vulnerabilities), Secunia (https://secuniaresearch.flexerasoftware.com/community/research/), CVE (Common Vulnerability and Exposures) (http://cve.mitre.org/), and Black hat (http://www.blackhat.com) [5,8-10,12].

The purpose of MTK (TOE Modular Testing Knowledge) is to verify that the evaluator is capable of determining the accuracy of test results because the developer conducts tests on new modules and information on test records is managed with accuracy. For the MTT (TOE Modular Traceability of Functional Requirements in Tests), the developer provides information and the security function requirements mentioned in the target security statement are tested (scripted) through the test script test. Lastly, COMP (Composite Functional Testing) is performed on the properties required by the product to satisfy the functional requirements of the overall target security statement [6,11]. LCD (Life-Cycle Model) is checking for testing's life-cycle for test case.

Definition describes more detail to check test case's adequacy and up-to-date. Form lists latest vulnerability and security. Verify is mapping with each test case item to compare with old and new. Update is mapping with each test case item to add new. For example, "AVA_VAN" could include latest vulnerability. "ATE_COV" could reflect related "CVE-2019-6337".

4. Analysis Test Items for Each Security Function Using Digital Printer.

4.1. Residual information protection technology.

This technique prevents the recovery of residual data. It repeats the process of rewriting used data regions to keep used data from being restored [1,2,4]. Test items related to permanent deletion in accordance with the Common Criteria are shown in Table 4.

Table 4. Residual information protection technology that corresponds to test/vulnerability classes

Class	Family	Description
ATE	COV	Verifies whether or not a security function was tested according to the statement of functions
	DPT	Addresses the level of detail of the security function test (directly tests internal interface)
	FUN	Guarantees that the test item on the test document was accurately performed and documented
	IND	The evaluator verifies the above tests and performs additional tests
AVA	VAN	Tests potential vulnerabilities (function neutralization and evasion test)
ATE	MTK	Verifies that the residual information protection technology test was performed accurately
	MTT	Checks that the test was conducted in accordance with the test script's test
	COMP	Checks the properties required by products to satisfy functional requirements from the overall target security statement
	LCD	Checks the testing's life-cycle model for test case Latest Vulnerability list: CVE-2019-6337, CVE-2019-6327, CVE-2019-6326, CVE-2019-6325 Verify: ATE_COV, ATE_DPT, ATE_FUN, ATE_IND, ATE_VAN Reflex: update complete

4.2. Secure printing technology.

Test items on secure printing technology can be deduced based on two objectives [16]. First, a test is performed to verify that the function fully reflects the security requirements and that the test is conducted to check that the function works accurately, and is consistent with the statement, and that there are no faults or defects. Table 5 shows test items related to secure printing technology.

4.3. Forgery/reproduction prevention technology.

Two factors must be identified in order to test forgery and reproduction prevention functions. The first is to identify whether the purpose of the forgery and reproduction function is to completely prevent an original document from being copied, printed, or scanned or merely to specify if a

Table 5. Secure printing technology that corresponds to test/vulnerability classes

Class	Family	Description
ATE	COV	Verifies whether or not a security function was tested according to the statement of functions
	DPT	Addresses the level of detail of the security function test (directly tests internal interface)
	FUN	Guarantees that the test item on the test document was accurately performed and documented
	IND	The evaluator verifies the above tests and performs additional tests
AVA	VAN	Tests potential vulnerabilities (function neutralization and evasion test)
ATE	MTK	Verifies that the secure printing technology test was performed accurately
	MTT	Checks that the functional requirements in the target security statement were tested according to the test script's test
	COMP	Checks the properties required by the product to satisfy functional requirements from the overall target security statement
	LCD	Checks the testing's life-cycle model for test case Latest Vulnerability list: CVE-2019-xxxx Verify: ATE_COV, ATE_DPT, ATE_FUN, ATE_IND, ATE_VAN Reflex: update complete

document is a copy. In the case of the former, all of the detailed test items are relevant, but only some of the detailed test items pertain to the latter. The second factor is to identify the environment where the forgery and reproduction prevention technology is used to identify where this function is used from the digital printer's basic functions (copying, scanning, printing, fax transmission). After the environment is clearly specified, judgment is made on whether or not the forgery and reproduction prevention function works properly. Table 6 shows the test items related to the forgery/reproduction prevention technology in accordance with the Common Criteria.

4.4. **Print access and control technology.** Print access and control technology uses identity data to protect printed materials from other users. Therefore, user authentication is the key to print access and control technology. To evaluate the safety of print access and control technology, the authentication procedure and mechanism configured in the digital printer should be evaluated to ensure that they are appropriate along with the countermeasures in place when the authentication fails and the safety of the authentication server. This proves that the print access and control technology is safe against attackers. Table 7 shows the test items regarding the print access and control technology that uses user authentication in accordance with the Common Criteria.

5. **Discussion and Conclusion.** We have the appropriateness of testing through the ATE_MTT, ATE_MTK, ATE_COMP and ATE_LCD presented in this paper, and MTK has made it possible to verify the accuracy of the test. MTT ensured that the test was performed through the script to ensure appropriateness. COMP ensured that the function was tested to meet the requirements. LCD verifies testing life-cycle model for test case.

The appropriateness of the test has helped improve security and has been improved to provide the latest patches for test methods, not the latest patches on the product. Proper patches of testing methods for the technology applied to the product can significantly improve product quality.

TABLE 6. Forgery/reproduction prevention technology that corresponds to the test/vulnerability

Class	Family	Description
ATE	COV	Verifies whether or not a security function was tested according to the statement of functions
	DPT	Addresses the level of detail of the security function test (directly tests internal interface)
	FUN	Guarantees that the test item on the test document was accurately performed and documented
	IND	The evaluator verifies the above tests and performs additional tests
AVA	VAN	Tests potential vulnerabilities (function neutralization and evasion test)
ATE	MTK	Verifies that the forgery/reproduction prevention technology test was performed accurately
	MTT	Checks that the functional requirements in the target security statement were tested according to the test script's test
	COMP	Checks the properties required by products to satisfy functional requirements from the overall target security statement
	LCD	Checks the testing's life-cycle model for test case Latest Vulnerability list: CVE-2019-xxxx Verify: ATE_COV, ATE_DPT, ATE_FUN, ATE_IND, ATE_VAN Reflex: update complete

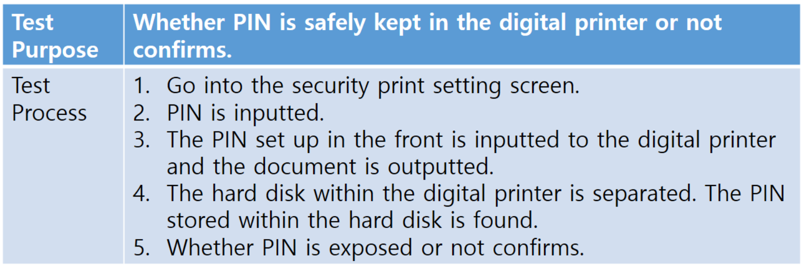
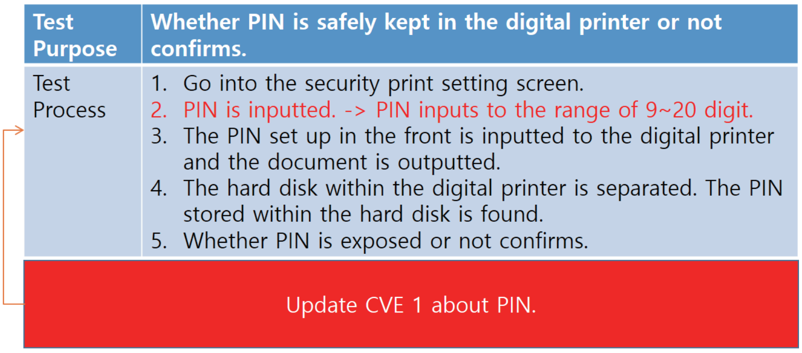
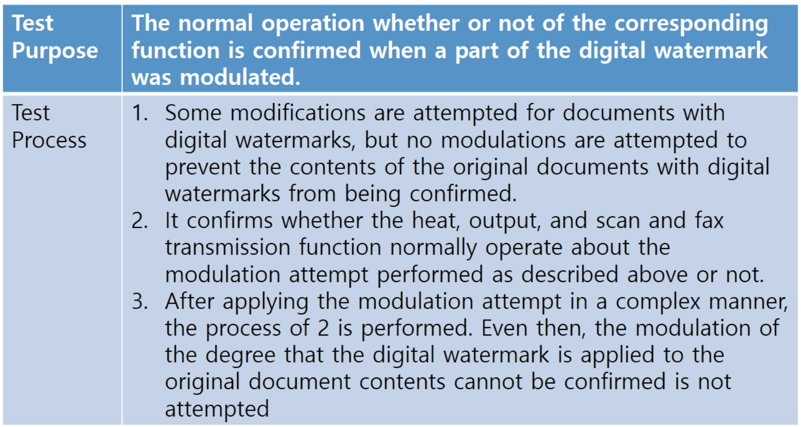
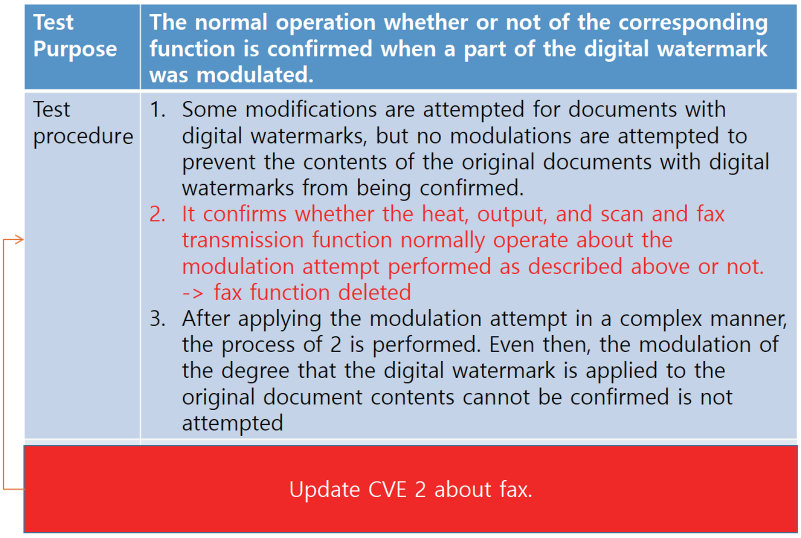
TABLE 7. Print access and control technology that corresponds to the test/vulnerability

Class	Family	Description
ATE	COV	Verifies whether or not a security function was tested according to the statement of functions
	DPT	Addresses the level of detail of the security function test (directly tests internal interface)
	FUN	Guarantees that the test item on the test document was accurately performed and documented
	IND	The evaluator verifies the above tests and performs additional tests
AVA	VAN	Tests potential vulnerabilities (function neutralization and evasion test)
ATE	MTK	Verifies that the print access and control technology test was performed accurately
	MTT	Checks that the functional requirements in the target security statement were tested according to the test script's test
	COMP	Checks the properties required by the product to satisfy functional requirements from the overall target security statement
	LCD	Checks the testing's life-cycle model for test case Latest Vulnerability list: CVE-2019-xxxx Verify: ATE_COV, ATE_DPT, ATE_FUN, ATE_IND, ATE_VAN Reflex: update complete

Using this methodology, we will also improve the testing methods for other products, contributing to the field of practical testing in the security industry.

Acknowledgment. This research was supported by the Soonchunhyang University Research Fund (Grant Number: 20190014).

Table 8. Reflect LCD test cycle example

Original test case A	 **Test Purpose** — **Whether PIN is safely kept in the digital printer or not confirms.** Test Process 1. Go into the security print setting screen. 2. PIN is inputted. 3. The PIN set up in the front is inputted to the digital printer and the document is outputted. 4. The hard disk within the digital printer is separated. The PIN stored within the hard disk is found. 5. Whether PIN is exposed or not confirms.
TEST Cycle A’	 **Test Purpose** — **Whether PIN is safely kept in the digital printer or not confirms.** Test Process 1. Go into the security print setting screen. 2. PIN is inputted. -> PIN inputs to the range of 9~20 digit. 3. The PIN set up in the front is inputted to the digital printer and the document is outputted. 4. The hard disk within the digital printer is separated. The PIN stored within the hard disk is found. 5. Whether PIN is exposed or not confirms. Update CVE 1 about PIN.
Original test case B	 **Test Purpose** — **The normal operation whether or not of the corresponding function is confirmed when a part of the digital watermark was modulated.** Test Process 1. Some modifications are attempted for documents with digital watermarks, but no modulations are attempted to prevent the contents of the original documents with digital watermarks from being confirmed. 2. It confirms whether the heat, output, and scan and fax transmission function normally operate about the modulation attempt performed as described above or not. 3. After applying the modulation attempt in a complex manner, the process of 2 is performed. Even then, the modulation of the degree that the digital watermark is applied to the original document contents cannot be confirmed is not attempted
TEST Cycle B’	 **Test Purpose** — **The normal operation whether or not of the corresponding function is confirmed when a part of the digital watermark was modulated.** Test procedure 1. Some modifications are attempted for documents with digital watermarks, but no modulations are attempted to prevent the contents of the original documents with digital watermarks from being confirmed. 2. It confirms whether the heat, output, and scan and fax transmission function normally operate about the modulation attempt performed as described above or not. -> fax function deleted 3. After applying the modulation attempt in a complex manner, the process of 2 is performed. Even then, the modulation of the degree that the digital watermark is applied to the original document contents cannot be confirmed is not attempted Update CVE 2 about fax.

REFERENCES

[1] Korea Institute of Patent Information, *Developmental Status of the Digital Watermarking Technology and Corporate Analysis*, 2003.

[2] J. Lotspiech, The advanced access content system's use of digital watermarking, *Proc. of the 4th ACM International Workshop on Contents Protection and Security (MCPS'06)*, 2006.

[3] *ISO*, http://www.iso.org, N1469_ISO-IEC_15408-3_WD2_20171215_with_change_marks.pdf.

[4] E.-S. Kim, J.-H. Park and Y.-K. Son, Notes on evaluation of digital watermarking, *Journal of Korea Multimeida Society*, 2001.

[5] *NIST*, http://www.sos.cs.ru.nl/applications/courses/security2008/nistiadraft.pdf.

[6] C. Wang, H. Zhang and X. Zhou, Review on self-embedding fragile watermarking for image authentication and self-recovery, *Journal of Information Processing Systems*, 2018.

[7] G. Kasana, K. Singh and S. S. Bhatia, Data hiding algorithm for images using discrete wavelet transform and Arnold transform, *Journal of Information Processing Systems*, 2017.

[8] R. M. Savola, A security metrics taxonomization model for software-intensive systems, *Journal of Information Processing Systems*, 2009.

[9] W. Zhu and C. Lee, A security protection framework for cloud computing, *Journal of Information Processing Systems*, 2016.

[10] J.-J. Kim and S.-P. Hong, A method of risk assessment for multi-factor authentication, *Journal of Information Processing Systems*, 2017.

[11] *ISO/IEC 15408-3:2013 Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 3: Security Assurance Requirements*, https://standards.incits.org/apps/group_public/project/details.php?project_id=685, Accessed on 12 June 2020.

[12] A. Grover and H. Berghel, A survey of RFID deployment and security issues, *Journal of Information Processing Systems*, 2011.

[13] P.-J. Chiang, N. Khanna, A. K. Mikkilineni, M. V. O. Segovia, J. P. Allebach, G. T. C. Chiu and E. J. Delp, Printer and scanner forensics: Models and methods, *Intelligent Multimedia Analysis for Security Applications*, pp.145-187, 2010.

[14] M. Yampolskiy, W. King, G. Pope, S. Belikovetsky and Y. Elovici, Evaluation of additive and subtractive manufacturing from the security perspective, in *Critical Infrastructure Protection XI. ICCIP 2017. IFIP Advances in Information and Communication Technology*, M. Rice and S. Shenoi (eds), Cham, Springer, 2017.

[15] S. N. Maximovsky, V. N. Ivanova, A. Y. Stavtsev, Nanowhiskerography – A new method of security printing using scanning laser radiation, *Bull. Lebedev Phys. Inst.*, vol.45, pp.341-345, 2018.

[16] A. Hecht, A. Sagi and Y. Elovici, PIDS: A behavioral framework for analysis and detection of network printer attacks, *The 13th International Conference on Malicious and Unwanted Software (MALWARE)*, 2018.

[17] CCMB, *Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components*, 2012.

[18] Threatpost, *DEF CON 2019: 35 Bugs in Office Printers Offer Hackers an Open Door*, 2019.

[19] Y.-J. Cho, K.-W. Lee, S.-K. Cho, H.-S. Park, H.-S. Lee, H.-S. Lee, S.-Y. Kim, W.-J. Cha, W.-R. Jeon, D.-H. Won and S.-J. Kim, Development testing/evaluating methods about security functions based on digital printer, *The KIPS Transactions: Part C*, vol.16, no.4, pp.461-476, 2009.