J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

Enhancing the Cybersecurity Checklist for Mobile Applications in DTx based on MITRE ATT&CK for Ensuring Privacy☆

윤 지 희[1] 김 경 진[2*]
Gee-hee Yun Kyoung-jin Kim

ABSTRACT

Digital therapeutics (DTx) are utilized to replace or supplement drug therapy to treat patients. DTx are developed as a mobile application for portability and convenience. The government requires security verification to be performed on digital medical devices that manage sensitive information during the transmission and storage of patient data. Although safety verification is included in the approval process for DTx, the cybersecurity checklist used as a reference does not reflect the characteristics of mobile applications. This poses the risk of potentially overlooking vulnerabilities during security verification. This study aims to address this issue by comparing and analyzing existing items based on the mobile tactics, techniques, and procedures of MITRE ATT&CK, which manages globally known and occurring vulnerabilities through regular updates. We identify 16 items that require improvement and expand the checklist to 29 items to propose improvement measures. The findings of this study may contribute to the safe development and advancement of DTx for managing sensitive patient information.

☞ keyword : DTx (Digital Therapeutics), MITRE ATT&CK Mobile, Mobile App Security, Privacy

1. Introduction

Medical systems have been operated in a closed manner because data and medical information pertaining to patients are not intended to be shared. Medical systems are evolving into smart healthcare systems that utilize data. Furthermore, the paradigm is shifting from a conventional system that involves patients visiting hospitals for diagnosis and treatment to a prevention- and patient-centric model, which involve patients managing their own health in their daily lives[1]. Owing to these dynamic changes, the medical industry has investigated significantly in remote and digital therapies. According to Research and Markets[2], the global digital therapeutics (DTx) market is expected to expand at an average annual rate of 26.7% and reach $6.9 billion by 2025. In Korea, the official term for DTx is digital therapeutic device. In February 2023, Somzz, a cognitive therapy software for improving insomnia, became the first digital therapeutic device to receive regulatory approval[3].

DTx are software medical devices (SaMDs) that are designed to not only diagnose, monitor patients, and provide decision support, but also to prevent, manage, or treat disabilities or diseases. Specifically, they refer to platforms that use digital technology for therapeutic interventions[4].

1 Dept. of Convergence Technology Engineering, Sungshin Women's University Seoul, 02844, South Korea.
2 Dept. of Convergence Security Engineering, Sungshin Women's University, Seoul, 02844, Korea.
* Corresponding author (kyongjin@sungshin.ac.kr)
[Received 10 April 2023, Reviewed 11 April 2023(R2 04 July 2023), Accepted 11 July 2023]
☆ This work is partly supported by the National Research Foundation of Korea (NRF) grant funded by the Ministry of Science and ICT (MSIT) (No. 2022R1F1A1074038), the Korea Institute for Advancement of Technology (KIAT) grant funded by the Korean Government (MOTIE) (P0008703, The Competency Development Program for Industry Specialist), and the MSIT under the ICAN (ICT Challenge and Advanced Network of HRD) program (No. IITP-2022-RS-2022-00156310) supervised by the Institute of Information & Communication Technology Planning & Evaluation (IITP) and Korea Foundation for Women In Science, Engineering and Technology (WISET) grant funded by the Ministry of Science and ICT(MSIT) under the team research program for female engineering students (WISET-2023-140).
☆ A preliminary version of this paper was presented at ICONI 2022.

According to the authors of[5], in the context of domestic DTx, the classification of device usage based on type indicates that mobile device-based DTx are approximately three times more common than desktop device-based DTx. This is due to their development on widely popular mobile devices that offer portability and convenience.

In Korea, products used for the prevention or treatment of human or animal diseases are classified as pharmaceuticals or medical devices based on their physical form, as a separate category of therapeutic agents does not exist[6]. Despite its software-based nature, DTx are referred to as a digital therapeutic device. Furthermore, DTx undergo the same cybersecurity verification process as the safety review stage for medical device approval. However, software applications operating on mobile devices may exhibit different cybersecurity vulnerabilities than the typical hardware therapeutic devices. This paper addresses and proposes solutions to these issues.

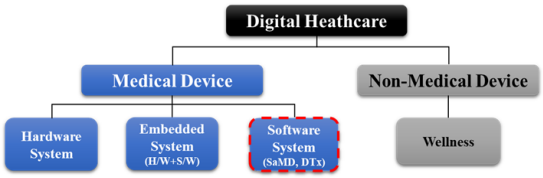
2. Background Information

2.1 Importance of DTx Security and Differentiation from Digital Devices

When a doctor prescribes a digital therapeutic device, the patient is eligible for its use. When a therapeutic device is used to treat a patient, the patient information is acquired by verifying the prescription issued by the doctor and inputting it into a digital therapeutic device. Biological changes are recorded and stored during the use of the device. Accurate treatment records must be maintained such that doctors can assess the patient's condition and prescribe additional treatment accordingly. Hence, developers obtain the medical records of patients via the application, which serves as an intermediary for transferring the acquired medical records to doctors [6].

The official definition of DTx is "SaMDs that provide evidence-based therapeutic interventions to prevent, manage, or treat medical disorders or diseases in patients"[7]. This definition clearly distinguishes DTx from existing smart medical devices[4].

SaMDs refer to independent software-based medical devices that perform functions to fulfill the purpose of medical devices without relying on hardware[7]. Additionally, being evidence based implies the necessity for medical evidence that aligns with the therapeutic goals. Clinical trial results should be published in professional journals or subjected to regulatory reviews; additionally, evidence and device performance data from actual clinical settings should be obtained and analyzed[8]. Furthermore, the therapeutic interventions provided by DTx should serve as a treatment alternative or concurrent therapy instead of a substitute for medications, thus distinguishing them from general health management applications[4]. Figure 1 illustrates the classification of DTx based on the delivery form.



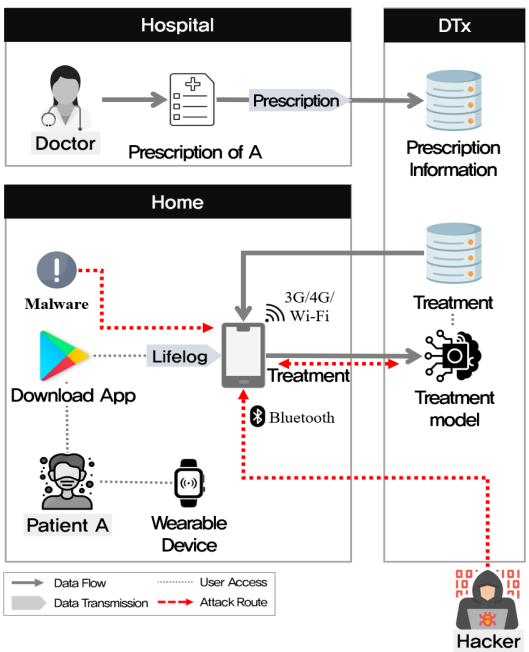
(Figure 1) Distinction between DTx and other medical devices(9)

Hardware and embedded systems are subjected to verifications to ensure the safety of their physical devices and the incorporated software. By contrast, DTx products, which are solely composed of software (particularly mobile applications), are known for their portability and accessibility, which increase the probability of exposure to diverse communication environments and expands the range of potential attack vectors.

2.2 Mobile App Cyber Threat

A mobile environment allows users to install various applications freely. However, this implies that malicious software can be unintentionally installed. In the case of DTx, which primarily appear in the form of mobile applications, unauthorized access to information or functional assets can occur through the exploitation of interapplication communication functions or vulnerabilities in applications by malicious software. Additionally, attacks from malicious attackers in physical proximity can occur via various near-field communication mechanisms such as NFC,

Bluetooth, and Wi-Fi. A malicious individual can steal a smartphone, which results in the risk of data leakage or loss of critical information. The threat scenarios are illustrated in Figure 2. For DTx products comprising only software, the cybersecurity verification process must be changed accordingly.

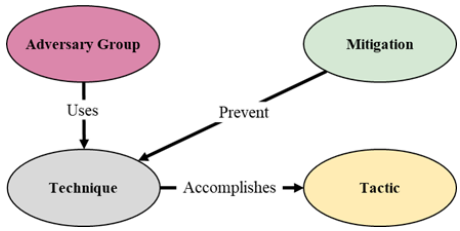


(Figure 2) Mobile App attack scenario

2.3 MITRE ATT&CK Framework

MITRE ATT&CK focuses on the process by which external adversaries compromise and operate within computer information networks. It serves as a curated knowledge base and model for cyber-adversary behavior, as well as reflect the various phases of an adversary's attack lifecycle and the targeted platforms. This framework comprises the key components illustrated in Figure 3.

In this study, MITRE ATT&CK was used to consider possible attacks on mobile devices. This framework provides tactics, techniques, and procedures (TTPs) for various domains, including enterprises, mobile devices, and ICS, with specific mechanisms for each element. This study aims to supplement and enhance existing checklists based on mobile TTPs and the mitigation measures defined in the framework[11].



(Figure 3) MITRE ATT&CK Mechanism

This framework is used to monitor known adversaries identified by public and private organizations, which are then reported in threat intelligence reports. These adversaries are monitored within ATT&CK using a group object, which assigns unique IDs to groups, provides group information, and offers details regarding similar groups, technologies, and subtechnologies used in the attacks.

The techniques and subtechniques within ATT&CK represent the details of an adversary's attack strategy, where the actions performed to achieve their objectives are described. These techniques are based on software used by hackers worldwide. Subtechniques further classify the behaviors described by the techniques into more specific descriptions of the manner by which the behavior is used to achieve an objective. In this study, a higher risk is recorded when the frequency of technology use in the attack group increases.

Tactics within ATT&CK describe an adversary's tactical objectives or the reasons for performing a specific action. Fourteen tactics were used, ranging from pre-attack tactics, which corresponded to the information-acquisition stage for attack attempts, to tactics that performed the actual attacks.

Mitigations in ATT&CK and CK represent security concepts and classes of technologies that can be used to prevent a technique or subtechnique from being successfully executed by an attacker. These mitigations can be used to improve an organization's overall security posture and reduce the likelihood of successful attacks. MITRE ATT&CK provides a comprehensive depiction of attack behaviors, which spans the entire lifecycle of attack execution and objective attainment. Based on this process,

suggestions for checklist improvements are proposed.

3. Comparative Analysis using MITRE ATT&CK

3.1 Cybersecurity Checklist for Stability Review

According to Article 22 of the Act on Nurturing Medical Devices Industry and Supporting Innovative Medical Devices, manufacturers are obligated to submit examination materials in four stages for medical device approval. During Stage 2, which focuses on the stability and performance assessment, the manufacturer is required to present the results of safety verification based on the medical device cybersecurity checklist (as shown in Table 1).

(Table 1) Medical Device Cybersecurity Checklist

Category	No	Requirement
Secure communication	1.1	Consideration of wired/wireless communication methods
	1.2	Validation of validity for internal/ external inputs
	1.3	Consideration of safe data transmission methods
Data protection	2.1	Use of secure encryption algorithms for data transmission and storage
	2.2	Secure encryption key management
Device integrity	3.1	Prevention of data repudiation
	3.2	Consideration of device integrity risks
	3.3	Consideration of control measures such as anti-malware programs
User authentication	4.1	Establishment of user authentication access control measures
Software maintenance	5.1	Establishment of firmware update procedures at regular intervals
	5.2	Consideration of operating system updates and controls
	5.3	Establishment of EoS and EoL response plans
	5.4	New security vulnerability response measures
	5.5	Ensuring integrity when updating firmware(e.g., code signing)
Physical access	6.1	Control measures for physical access by unauthorized personnel
Reliability & availability	7.1	Design of countermeasures for cyber security attacks

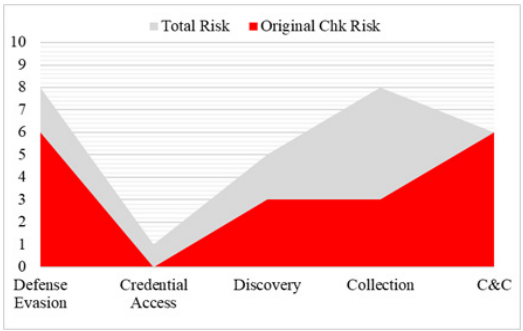
This entails providing supporting materials such as device applicability, suitability, and test reports that align with the checklist items. In addition, the manufacturer must address the cybersecurity aspects of the device, including the communication technology, usage environment, and utilization of public networks. The checklist specifies 16 requirements across 7 items.

However, the specified requirements have a broad scope. The Medical Device Cybersecurity Permit and Examination Guidelines[8] offer detailed criteria that enable manufacturers to exclude or add the necessary requirements based on a product's characteristics. Moreover, using the same cybersecurity checklist designed for physical medical devices for DTx, which are software applications, is risky, as crucial security elements specific to mobile applications may be overlooked.

Based on the attack scenario of the Windshift attack group provided by MITRE ATT&CK, the mitigation measures listed in Table 1 were applied. Among the 28 risk points, 10 were successfully mitigated, which resulted in a coverage of 35.7%, thus indicating that most attack chains cannot be effectively disrupted. This is illustrated in Figure 4. The analysis process is summarized in Table 2.

(Table 2) Procedure for analyzing attack technique coverage

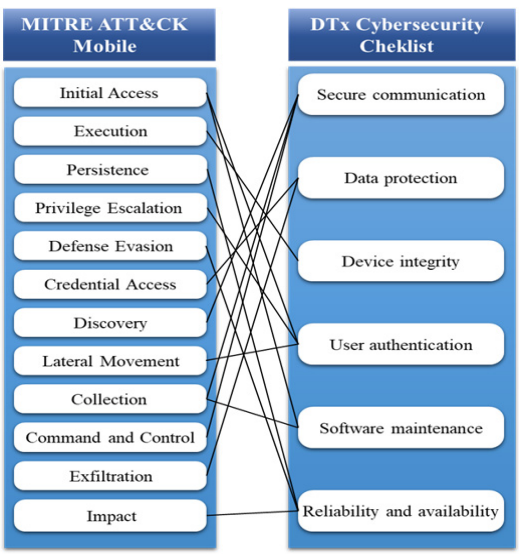
No	Contents
1	Technical analysis of attack group's attack phases using MITRE Navigator.
2	Assignment of risk levels to techniques: - 1 point : if both detection methods and defensive measures are specified. - 2 points : if either detection methods or defensive measures are specified. - 3 points: if neither the detection methods nor defensive measures are specified.
3	Matching mitigation measures with the existing checklist in a stepwise manner.
4	Matching mitigation measures for each phase with the existing checklist to assess the coverage.



(Figure 4) Residual risk level for the Windshift scenario

3.2 Comparison with MITRE ATT&CK

We matched the MITRE ATT&CK Mobile tactics to the checklist items presented in Figure 5. Based on analysis, we identify the vulnerabilities and suggest the corresponding mitigation measures.



(Figure 5) Mapping between MITRE ATT&CK and Cybersecurity Checklist

Among the original seven checklist items, "physical access" was excluded from the comparison because it applies only to hardware-based medical devices. To disrupt the step-by-step attack chain presented by MITRE ATT&CK, additional defensive measures were introduced at each defense stage.

3.3 Secure communication

Secure data transmission methods belong to the security-communication category. Table 3 presents the vulnerabilities that may occur due to the characteristics of mobile applications. In some cases where the abovementioned methods were used during security communication, the validity of SSL/TLS certificates were not verified adequately, thus allowing future MIMT attacks to occur. In this case, important data can be hacked through the theft of administrator accounts. When the mobile application detects an invalid certificate, it alerts the user through the UI. Furthermore, sensitive data can be encrypted using a separate encryption layer as an additional defense mechanism before they are transmitted through an SSL channel[12].

(Table 3) Vulnerabilities that can arise in Security Communication

Tactic	Vulnerability
Discovery	Adversaries discover and utilize the desired data for attacks through functional elements of systems or software, such as location tracking, network service scanning, and process and system information discovery.
Collection	Deploying oneself as an attacker between two or more network devices to manipulate transmitted data or perform subsequent actions such as endpoint DoS.
	Acquiring notification data sent from operating systems or applications, as well as essential data from well-known applications used in daily life.
	Acquiring video files using a camera and monitoring the physical location of devices.
	Searching for important files and data of interest through searching local system sources.
Command &Control	Change the standard port of a protocol and generate network traffic to bypass network data filtering or analysis.
	Adversaries may make, forward, or block phone calls without user authorization for various goals

3.4 Data protection

Data protection is defined as the protection of data during transmission and storage using secure encryption algorithms and secure management of encryption keys. Table 4 lists the potential vulnerabilities that may arise from mobile device applications. To address these vulnerabilities, security verification must be conducted from a security coding perspective. To prevent API attacks, the use of vulnerable library functions such as get, sprintf, strcat, strcpy, and vsprintf must be avoided[13]. In addition, source code obfuscation should be performed to prevent the theft of source codes and important information through tampering.

(Table 4) Vulnerabilities that can arise in Data protection

Tactic	Vulnerability
Credential Access	Capture user input such as passwords pasted by password management programs by exploiting clipboard manager APIs.
	Intercept important data from notifications (e.g., one-time authentication codes) sent through media such as email and SNS or disable notifications.
	Search for password storage locations and acquire credentials.
	Resource access through access token theft.
Exfiltration	Exfiltrate or steal data through existing command and control channels' protocols or other protocols.

3.5 Device integrity

Device integrity is defined as a method of preventing data repudiation, designing against device integrity risks, and establishing control measures using malware programs. Table 5 illustrates the vulnerabilities that may arise from the characteristics of mobile applications. To address these vulnerabilities, one must verify whether the permissions used in the mobile application are consistent with those granted in the application's source code and then modify them such that only the necessary permissions are used. Unnecessarily granted permissions may be exploited by malicious applications or viruses[13].

(Table 5) Vulnerabilities that can arise in Device integrity

Tactic	Vulnerability
Execution	Executing scripts using built-in interpreters such as Unix Shell
	Repetitive execution of malware using task scheduling APIs and libraries

3.6 User authentication

User authentication is an access control measure and prohibits credential sharing. Table 6 lists the vulnerabilities that may occur due to the characteristics of mobile applications. As a countermeasure, biometric authentication can be used instead of login methods. If the threshold is exceeded during user authentication, then additional identity verification is required to access the application[13].

(Table 6) Vulnerabilities that can arise in User authentication

Tactic	Vulnerability
Initial access	Access through compromised websites.
	Physical access (unlocking, supply chain theft, USB attacks).
Privilege Escalation	Bypassing permission escalation mechanisms
	Exploiting software vulnerabilities (applications, services, operating systems, kernels, etc.) for privilege escalation
	Executing arbitrary code in the context of other processes by executing code in a separate live process address space; and gaining access to the process's memory, system/network resources, and escalated privileges
Lateral Movement	Exploiting programming errors in the software or the kernel, or operating the system to execute attacker- controlled code.
	Using malicious programs or copying them onto a device connected via USB.

3.7 Software maintenance

The software maintenance item specifies measures to ensure the integrity of the system, such as updating the operating system, establishing an end-of-support (EoS) and end-of-life (EoL) response plan, developing new security vulnerability response measures, and ensuring integrity

during firmware updates. Table 7 lists the potential vulnerabilities that may arise from mobile device applications. Most attacks are based on vulnerabilities in the OS and firmware. To mitigate these problems, improved versions of applications must be distributed in response to newly discovered vulnerabilities, and users must update their applications to the latest version[13]. In addition, measures should be implemented to ensure that users can access the application after updating the OS in case of OS defects on mobile devices. Furthermore, the appropriate measures should be executed to prevent malicious manipulation of the application on rooted or jail-breaking devices. As this paper is intended to be submitted to an academic conference, non-English characters should be translated to English.

(Table 7) Vulnerabilities that can arise in Software maintenance

Tactic	Vulnerability
Initial access	Access through compromised websites
	Physical access (unlocking, supply chain theft, USB attacks).
Collection	Deploying oneself as an attacker between two or more network devices to manipulate transmitted data or perform subsequent actions such as Endpoint DoS.
	Acquiring notification data sent from operating systems or applications, as well as essential data from well-known applications used in daily life.
Collection	Acquiring video files using a camera and monitoring the physical location of devices.
	Searching for important files and data of interest from local system sources.

3.8 Reliability and availability

In reliability and availability requirements, a design that allows for the detection of, resistance against, response toward, and recovery from cybersecurity attacks is specified. Table 8 presents the potential vulnerabilities that may arise from the characteristics of mobile applications. Coding errors may result in resource depletion, thus ensuring the reliability and availability of an application. For example, one must verify whether the application exceeds the threshold for battery consumption owing to repetitive tasks, excessive traffic from synchronization, or abnormal resource usage while being used[13].

(Table 8) Vulnerabilities that can arise in Reliability and availability

Tactic	Vulnerability
Persistence	Using auto-execution scripts of the basic operating system or modifying installed applications to establish persistence.
	Setting persistence using system mechanisms that trigger execution based on specific events.
Defense Evasion	Bypassing privilege escalation control mechanisms.
	Exploiting software vulnerabilities (applications, services, operating system, kernel, etc.) to escalate privileges.
	Executing arbitrary code from a separate live process's address space, thereby accessing the process's memory, system/network resources, and escalated privileges by executing the code via another process.
Impact	Preventing legitimate access to user accounts to disrupt network resource availability, or deleting and locking accounts to remove access.
	Rendering access difficult through file encryption on mobile devices.
	Manipulating data and performing DoS attacks.
Impact	Generating outbound traffic for billing fraud
	Abusing Android's Accessibility API to inject input into the user interface, imitating user interaction.
	Deleting, changing, or sending SMS messages or manipulating phone calls without user authorization.

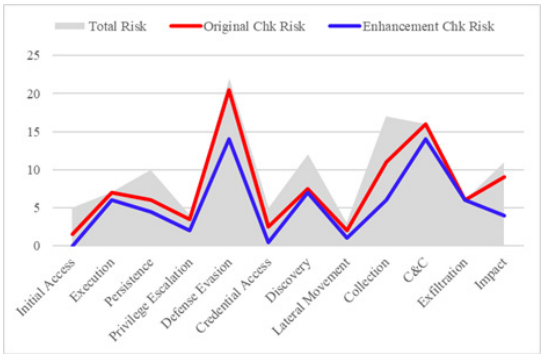
4. Checklist Improvement

Based on comparison and analysis, we discovered that the existing security checklist items for medical devices were insufficient to address the vulnerabilities that may arise in mobile devices. Based on the comparison results, we propose improvement measures that include the following additional items (see Table 9).

(Table 9) Additional checklist suggestion

Category	No	Improvement
Secure communication	1.4	Alert users through the UI if the mobile application detects an invalid certificate.
	1.5	Sensitive data should be encrypted with a separate layer of encryption as a secondary defense before being transmitted over the SSL channel.
Data protection	2.3	Avoid using vulnerable library functions such as gets, sprintf, strcat, strcpy, and vsprintf.
	2.4	Apply source code obfuscation to prevent reverse engineering and potential exploitation through source code tampering, which can result in the theft of sensitive information.
Device integrity	3.4	Verify if the permissions used in the mobile application match the permissions granted in the application's source code, and remove any unnecessary permissions.
	3.5	To prevent unauthorized manipulation of the application on rooted or jail-broken devices for malicious purposes, measures should be implemented to prevent it from being executed.
User authentication	4.2	Use biometric authentication as an alternative to IDs and passwords for application login.
	4.3	Implement access control to immediately block application access when login threshold is exceeded and require additional identity verification for access.
Software maintenance	5.6	Regularly distribute firmware updates for software application updates and implement access restriction for devices that are not updated.
	5.7	Implement application access for devices using the latest mobile operating system.
Reliability and availability	7.2	Identify coding errors that may cause resource depletion that exceeds battery consumption limits, such as excessive traffic caused by repetitive tasks or synchronization, or the use of abnormal resources, to ensure the reliability and availability of the application.
Guide	8.1	Provide guidelines and education pertaining to the prevention of security vulnerabilities to application developers.
	8.2	Provide all instructions or education to users to prevent certain configuration settings or potentially dangerous actions.

When applying the existing checklist based on the risk levels of the 12 techniques of MITRE ATT&CK, coverage of 21.6% was achieved. This coverage indicated a lack of resilience to attacks. However, using the checklist proposed in this study, the coverage could be improved to 44.9%, as shown in Figure 6. The increases in coverage for each phase are listed in Table 10.



(Figure 6) Comparison of Risk Reduction Levels between the Original Checklist and the Proposed Checklist based on the Total Risk Score for each MITRE ATT&CK Stage

In conclusion, the proposed approach enhanced the coverage from 12% to 45% across the MITRE ATT&CK framework, except for the Discovery and Exfiltration phases, which currently lack appropriate detection and mitigation measures.

(Table 10) Improvement in Risk Levels

Category	Original Risk	Fixed Risk	Mitigation Rate
Initial Access	1.5	0	30.0%
Execution	7	6	14.3%
Persistence	6	4.5	15.0%
Privilege Escalation	3.5	2	37.5%
Defense Evasion	20.5	14	29.5%
Credential Access	2.5	0.5	40.0%
Discovery	7.5	7	4.2%
Lateral Movement	2	1	33.3%
Collection	11	6	29.4%
Command and Control	16	14	12.5%
Exfiltration	6	6	0.0%
Impact	9	4	45.5%

5. Conclusion

DTx have been used to replace or supplement conventional treatments and typically involves the transmission and storage of disease-related patient data using devices. Although safety verification is included in the approval process for DTx, the cybersecurity checklist used for this purpose does not adequately reflect the unique characteristics of mobile applications. This implies that vulnerabilities in mobile applications may remain undetected during verification. Hence, we compared and analyzed the existing checklist items with globally known and frequently occurring vulnerabilities based on mobile TTPs. We identified areas for improvement in 16 items and expanded the checklist to include 29 items.

Consequently, when conducting inspections based on the checklist proposed herein, an attacker's progression can be interrupted or delayed through the stages of the attack chain. The findings of this may contribute to the safe development and advancement of DTx for managing sensitive patient information.

Reference

[1] Won Tae Lee, "Medical Device Security Testing Explanation Document", Korea Internet & Security Agency(KISA), 2022. https://www.mfds.go.kr/brd/m_218/view.do?seq=33479&srchFr=&srchTo=&srchWord=&srchTp=&itm_seq_1=0&itm_seq_2=0&multi_itm_seq=0&compan

[2] Ahn-seon Park, Seung-min Lee, "Current Status Analysis and Future Development Directions of Digital Therapeutics", ETRI Insight, 2020. https://doi.org/10.22648/ETRI.2020.B.000020

[3] Se-Dong Min "Evolution of healthcare solutions according to environmental changes", The Korean Institute of Electrical Engineers, 72(3),16-21, 2023. https://www.kiee.or.kr/board/?_0000_method=view&ncode=a004&num=2264&page=1

[4] Doug Hyun Han, "Results of Digital Therapeutics (DTx) Research Survey", Korea Internet Corporations Association, 2021. https://wowtale.net/wp-content/uploads/2021/03/wowtale.net-kinternet-dtx.pdf

[5] Young Seung Lee, Yoon Sang Kim, "A Study on Digital Therapeutics: cases analysis and suggestion", Journal of Digital Contents Society, 24(2), 303-312, 2023. https://doi.org/10.9728/dcs.2023.24.2.303

[6] Oh tak Kwon, "Legal consideration of information management system for digital therapeutics", Legislation and Policy Syudies, 14(1), 309-334, 2022. https://doi.org/10.22809/nars.2022.14.1.011

[7] National Institute of Food and Drug Safety Evaluation, "Digital Therapeutics Approval Review Guidelines", 2020. https://www.kbiohealth.kr/boardDownload.es?bid=0037&list_no=9605&seq=1

[8] National Institute of Food and Drug Safety Evaluation, "The Medical Device Cybersecurity Permit and Examination Guidelines", 2022. https://www.khidi.or.kr/board/view?pageNum=1&rowCnt=20&no1=960&linkId=48869156&menuId=MENU01516&maxIndex=00488698529998&minIndex=004882408499 98&schType=0&schText=&schStartDate=&schEndDate=&boardStyle=&categoryId=&continent=&country=

[9] Young-deok Gu, "Digital Therapeutics", ASTI Market Insight, ASTI Market Insight 2022-95, 2022. https://www.kisti.re.kr/post/asti-insight/5707?searchType=default&searchTxt=%ec%b9%98%eb%a3%8c%ec%a0%9c&t=1690170904645#

[10] Japan Smartphone Security Association (JSSEC), Android Application Secure Design/Secure Coding Guidebook, 2022. https://www.jssec.org/dl/android_securecoding_en_20220117/index.html

[11] Blake E. Storm at al., "MITRE ATT&CK: Design and Philosophy", The MITRE Corporation, 2020. https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

[12] OWASP, "OWASP Mobile Top 10", https://owasp.org/www-project-mobile-top-10/

[13] Ministry of Public Administration and Security, Korea Internet & Security Agency, "Mobile Public Service Security Vulnerability Assessment Guide",

2021.
https://www.kisa.or.kr/2060204/form?postSeq=4&lang_
type=KO&page=

◐ Authors ◑

Gee-hee Yun
2019 B.S. in Convergence security, Sungshin Women's University, Korea.
2018~2022 : employed as a Senior Consultant at F1Security
2022～Present : currently pursuing a Master's degree in Future Convergence Technology Engineering at Sungshin Women's University. korea
Research Interest : Privacy-enhancing technologies, Security compliance, Access control
E-mail : geehee_yun@naver.com

Kyoung-jin Kim
2007 B.S. in Computer Science, Sungshin Women's University, Korea.
2009 M.S. in Computer Science, Sungshin Women's University, Korea.
2013 Ph.D. in Computer Science, Sungshin Women's University, Korea.
2017～present : Professor, Dept. of Convergence Security Engineering, Sungshin Women's University, Korea
Research Interest : Privacy protection, Security framework, Access control, Blockchain
E-mail : kyongjin@sungshin.ac.kr