International Journal of Advanced Smart Convergence Vol.13 No.3 13-17 (2024)
http://dx.doi.org/10.7236/IJASC.2024.13.3.13

IJASC 24-3-2

Research on the Necessity and Measures for Protecting Local Storage Data of Homecam Devices

Ga. Hyeon. LEE[1], Hoon. Jae. Lee[2]*

[1]Master(M.A), Digital Forensics, Dongseo University, Korea
[2]professor, Dept of information security, Dongseo University, Korea
*E-mail: *hjlee@gdsu.dongseo.ac.kr*

Abstract

The local storage method for home cameras, which relies on inserting an SD card into the device to store data, offers a convenient and cost-effective solution, as there are no recurring expenses after purchasing the SD card. However, we recognize that this method comes with significant security challenges. In particular, the ease with which third parties can access the SD card makes it vulnerable to both physical and software tampering. As the acceptance rate of home camera footage as evidence in courts has increased, we have become increasingly aware of the critical nature of these security issues. Digital data from home cameras, unlike other types of physical evidence, can be more easily tampered with and altered. To ensure that such data is recognized as valid legal evidence, we must prove its integrity and demonstrate that it has not been tampered with. In response to these challenges, we are committed to strengthening the security measures for both the home camera device and its local storage. By doing so, we aim to ensure the integrity and reliability of the data, thereby enhancing the overall security and trustworthiness of home camera systems.

Keywords: *HomeCamer, SDcard, Security CCTV*

1. INTRODUCTION

Current home camera devices have vulnerabilities that allow third parties to easily locate and physically damage them. This is mainly because home cameras are installed within homes in easily accessible locations, which lowers the level of physical security for these devices. Additionally, if local storage is used, the structure allows SD(Secure Digital) cards to be easily intercepted. The local storage method involves storing the data recorded by the home camera on an SD card, which is inserted inside the camera, making it easy for third parties to access and steal. Particularly, SD cards lack special security and encryption measures, so if an SD card is stolen, the data stored on it can be easily damaged or deleted, and sensitive personal information may be exposed [1]. These issues extend beyond simple security concerns and can significantly impact the use of such data as evidence in court.

Currently, many IoT devices are being adopted as legal evidence, so ensuring the integrity and reliability of

Manuscript Received: July. 3. 2024 / Revised: July. 10. 2024 / Accepted: July. 15. 2024
*Corresponding Author: hjlee@dongseo.ac.kr
Tel: *** - **** - ****
prfessor, Dept. of information security, Dongseo University, Korea

this digital data is crucial. For digital data to be recognized as legal evidence, it must be proven that the data has not been altered since its creation [2, 3]. Additionally, the data must be protected from unauthorized access or tampering. To address these security issues, additional security measures for home camera devices and local storage methods are necessary. Measures such as encrypting the data stored on the SD card or implementing security systems that control access rights can be considered to prevent unauthorized access by third parties. Even if the data is stolen, encryption can make it difficult to decipher, thereby maintaining the integrity of the data [1].

Moreover, it is important to install home cameras in more secure locations and add physical protection measures to prevent physical damage to the devices. Options include installing home cameras in higher places or using protective cases with locking mechanisms. These measures can reduce the risk of physical damage. To ensure the integrity and reliability of digital data, these various security measures must be implemented to protect the data safely and maintain its value as legal evidence. By doing so, home camera devices can be used more safely and reliably, and can serve as definitive evidence in the event of legal issues.

In conclusion, strengthening the security of home cameras is not only about protecting personal privacy but also plays a critical role in legal procedures. Users should enhance the security of their home cameras to protect their data and ensure it can be used as valid evidence in legal disputes. Therefore, both home camera manufacturers and users need to recognize these security issues and continuously improve security measures.

1-2. THE DIFFERENCE BETWEEN HOME CAMERAS AND CCTV

The primary difference between homecam devices and regular CCTV systems lies in their intended use. Homecam devices are primarily used indoors for observing specific areas or monitoring pets and people. They are designed to be easily installed and managed by general users. In contrast, CCTV systems are used both indoors and outdoors in public places, companies, parking lots, etc., for security, surveillance, and safety purposes. CCTV systems are typically installed and maintained by professionals [4].

Homecam devices are user-friendly and can be easily connected to smartphones via wireless connections for remote real-time monitoring. On the other hand, CCTV systems use high-resolution cameras, usually with wired connections, and are linked to Network Video Recorders (NVR) or Digital Video Recorders (DVR). CCTV systems are managed through central control systems.

Home camera devices provide unlimited access through the application, allowing users to monitor their homes anytime, anywhere, while CCTV systems provide advanced security features and are accessed by authorized users through a central management system [4, 5]. The main difference between these two systems is the biggest distinction between professional and unrestricted systems. The main differences between CCTV and home cameras are summarized in Table 1.

Table 1. Comparison between home cameras and CCTV

	Homecam Device	CCTV
Intended use	For observing specific places or organisms within the home	No restrictions on external and internal locations
Installation and Management	Installed and managed directly by the average user	Installation by experts and maintenance by experts
Usability	Easy to use, capable of real-time remote monitoring via wireless connection with	High-resolution camera. Typically wired connection, NVR, DVR

	smartphone integration	
Approach	Access is possible if the application has been connected once or more	Access through central control system
Security level	Provides basic security features	Provides advanced security features, accessible only to users with specific permissions

1-3. HOMECAM DEVICE SECURITY

Home cameras are generally more physically exposed to third parties and outsiders compared to CCTV systems, making them susceptible to local storage and SD card tampering. However, home cam devices often lack physical and software security, remaining consistently exposed [6].

Since home cameras record footage inside residences, stored data may contain sensitive information such as family members, daily routines, and private spaces, making it vulnerable to leaks. As depicted in Figure 1, Incidents of sensitive data leaks from home interiors via IoT devices have occurred [4]. Furthermore, recently, home cam data is used for monitoring and recording criminal activities like theft and intrusion; thus, if stored data is compromised or leaked, crucial evidence of crimes could be lost [7, 8].

Figure 1, shows Depicts an actual incident in which a living room intercom was hacked by infiltrating the server network of an apartment complex, leading to the unauthorized access and exposure of multiple home cameras. This incident highlights the vulnerability in security, showing that hacking a single server network can compromise multiple households. It serves as a reminder that homes, which were considered safe, may become less secure due to the convenience of IoT devices installed within them.

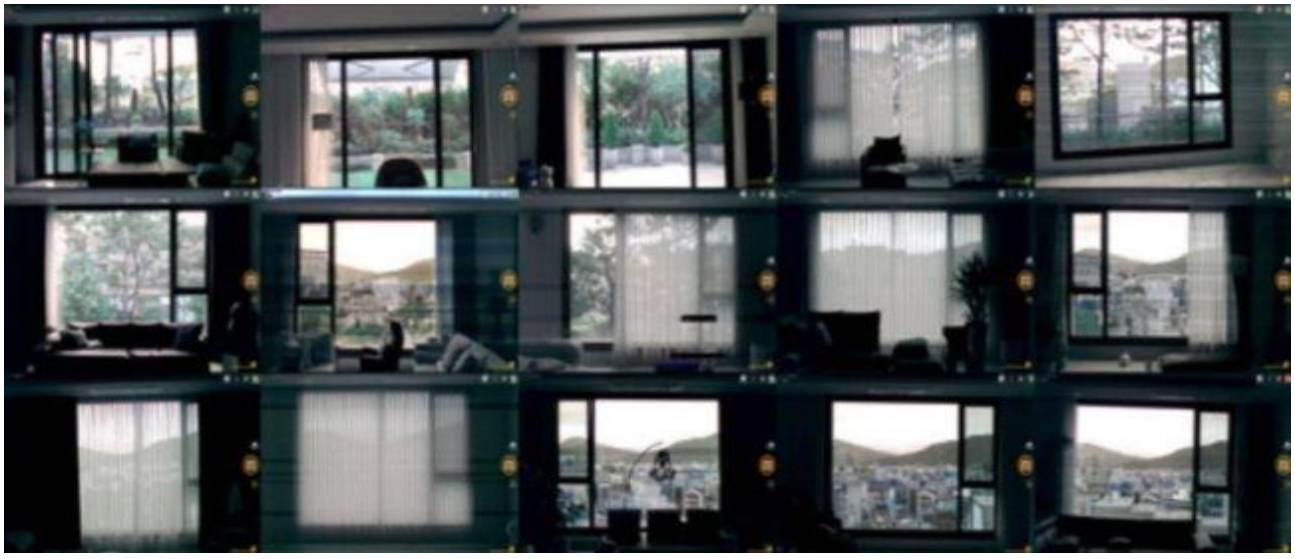

Figure1. Woolpad hacking incident

3. DISCUSSION

In order for stored video data to be admissible as evidence in court, security measures are necessary to prevent tampering or deletion. Maintaining data integrity is crucial for it to be considered reliable evidence [8, 9]. Data stored locally can be at risk of loss due to hardware failures, software errors, malicious attacks, and

strengthening security can mitigate the risk of data loss [10]. For these reasons, some countries or regions require enhanced security for CCTV and home cam data in accordance with privacy laws and data protection regulations.

4. RESULTS

4-1. Security Enhancement Measure is the Development of an SD card Data Access Restriction System.

This system aims to add features that protect data on the SD card even if it is stolen, using the company's home camera application.

- **Unique Identifier-Based Restriction.** Each SD card will have a unique identifier and be paired with a specific device. When the SD card is first inserted, the user is prompted to enter a password during the initial pairing process, which generates and applies a unique encryption key.

- **Password Authentication System**. To use the SD card, a password must be entered through the application. This applies to all access permissions, including read, write, and delete operations when the SD card is acce ssed via a computer. If the password is entered incorrectly, access is denied. This system includes a password attempt limit feature to prevent brute force attacks.

4-2. Measure is Data Encryption.

Encrypting the data stored on the SD card ensures that the data is protected even if the SD card is physically stolen.

- **Encryption Key Management.** The encryption keys are securely stored within the device. The key management system enhances security by periodically updating or rolling the keys. Additionally, the keys are stored and managed using hardware security modules like TPM (Trusted Platform Module).

4-3. Measure is the Implementation of a Physical Write Protection Switch.

The SD cards produced by the company will feature a physical write protection switch. When activated, this switch prevents any additional writing or deletion of data after the SD card is stolen and attempts are made to tamper with it externally.

- **Implementation of Physical Switch.** The SD card will be equipped with a physical write protection switch that the user can activate to enable write-protection mode. This switch operates at the hardware level, providing security against software-based attacks.

- **Security Logging Feature.** Whenever the write protection mode is activated, logs are recorded to provide transparency to the user regarding the SD card’s status. This allows users to check the protection status of the SD card at any time.

- **Damage Prevention Feature.** If the SD card is stolen and an attempt is made to physically damage it, the activated write protection switch will protect the data from being compromised. This plays a crucial role in maintaining the integrity of important data.

5. CONCLUSION

Enhancing the security of home security cameras is crucial for protecting the privacy of households and ensuring that important data is safely preserved. Measures such as the development of access-restricted SD cards, data encryption, and the implementation of physical write protection switches strengthen the security of local storage on home security cameras. These measures enable households using home cameras to protect their privacy more effectively during criminal situations and to obtain reliable evidence. Additionally, to safeguard users' information from remote hacking and data breaches, we need to develop an SD card data access restriction system, implement data encryption, and introduce a physical write protection switch system. Therefore, strengthening the security of home security cameras is essential. This allows users not only to protect their personal information but also to secure important evidence in a safe environment and respond quickly and effectively in the event of an incident.

Acknowledgement

This work was supported by Dongseo University."Dongseo Cluster Project (type 2)"Research Fund of 2024 (DSU-20240004)

References

[1] Minho Kim, Hyunuk Hwang, Kibom Kim, Taejoo Chang, Minsu Kim, and Bongnam Noh, "Vulnerability Analysis Method of Software-based Secure USB," Journal of the Korea Institute of Information Security & Cryptology, vol. 22, no. 6, pp. 1345-1354, 2012.
DOI: https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE02064362

[2] Park, Rak In. "A Study on Search and Seizure of Digital Evidence and its Admissibility." The Journal of Police Science, 15(3), 205-232. 2015.
DOI: https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE07019333

[3] Judicial Policy Research Institute, Ji-Young Son, and Joo-Seok Kim, "A Study on the Admissibility of Digital Evidence," JPRI Research Report, vol. 2015, no. 8, pp. 0-0, 2015.
DOI: https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE07153460

[4] Hyo-Name Kim and Jae-Kyung Park, "A Study on the Design of Security Mechanisms for CCTV Control," Proceedings of the Korean Society of Computer Information Conference , vol. 28, no. 2, pp. 445-446, 2020.
DOI: https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE09415070

[5] Jonghyeok Chae and Seunghoon Oh, "Research on application of CCTV video encryption technique - Using AI segmentation technique," Korean Institute of Electrical Engineers Conference, pp. 556-558, 2023.
DOI: https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE11701404

[6] Chosun Ilbo, Article, https://it.chosun.com/news/articleView.html?idxno=2021112401767 11.25.2021

[7] Lee Gyu-min, "A study on securing legality and integrity for CCTV video information gathering of investigation agency in terms of digital forensics," 2022.
DOI: https://www.dbpia.co.kr/journal/detail?nodeId=T16068567

[8] Hwang Kijin, "A Study on Object Tracking and Video Information Security in IoT Environment," 2017.
DOI: https://www.dbpia.co.kr/journal/detail?nodeId=T14373238

[9] Oh Hyeon-seo, "A Study on the Improvement of Digital Forensic Procedures for IoT Crimes," 2020.
DOI: https://www.dbpia.co.kr/journal/detail?nodeId=T15486763

[10] Lee Jeong Bong. "Evaluation of Scientific Evidence under the Evidence Rule." Korean Journal of Criminal Case Studies, 21, 563-616. 2013.
DOI: https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE10875942