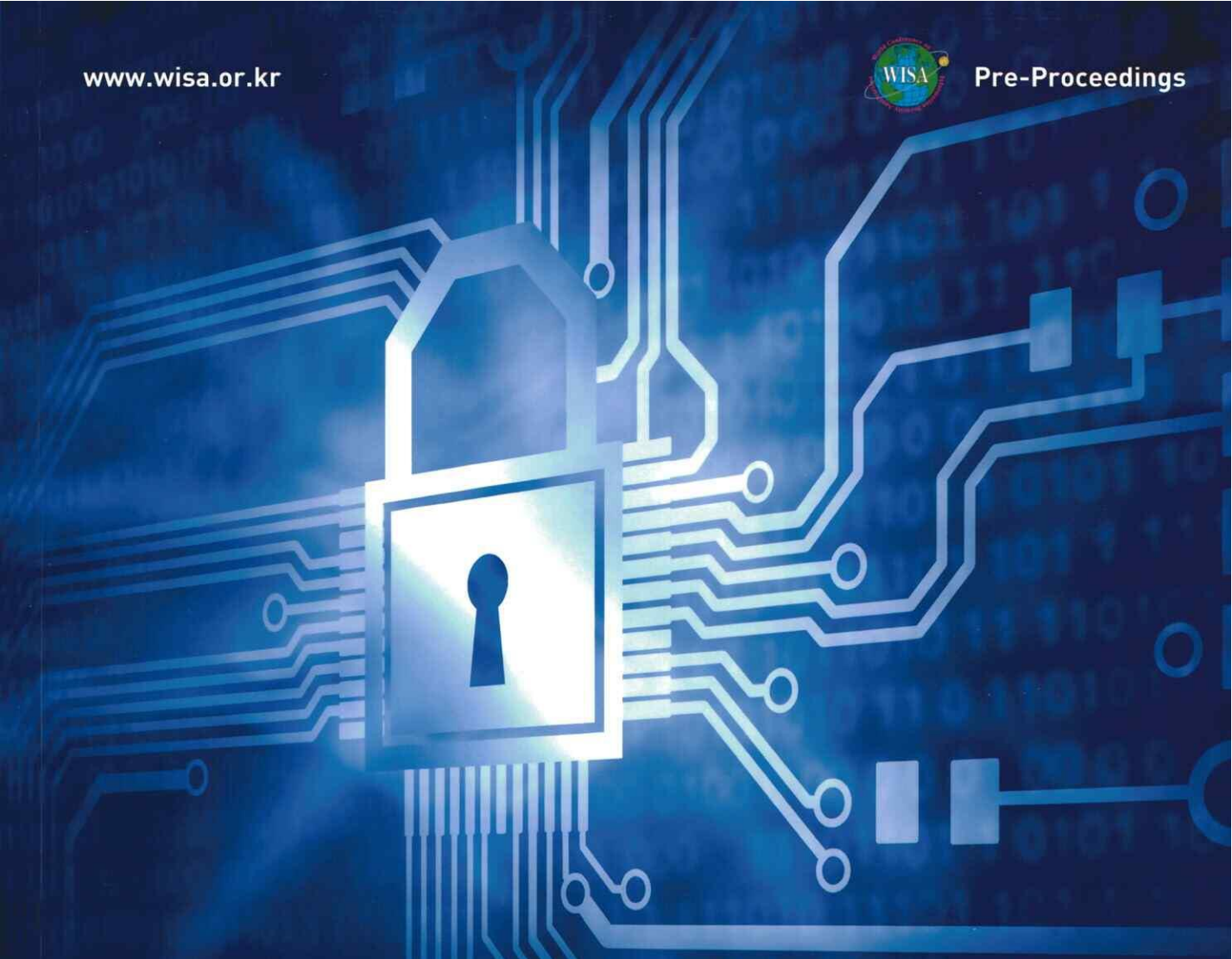
www.wisa.or.kr

Pre-Proceedings



The 21ST World Conference on Information Security Applications

WISA 2020

August 26-28, 2020

MAISON GLAD, Jeju Island, Korea

Hosted by: Korea Institute of Information Security & Cryptology

Sponsored by: Ministry of Science and ICT, NIS

Co-Sponsored by: KISA 한국인터넷진흥원, NSR, ETRI, KONA I, WINS

Poster: Self-Destructible Electronic Bracelets for Privacy in Quarantine Monitoring System

Sung-Kyu Ahn, HyeLim Jung, Sung-Kyung Kim, Ki-Woong Park*
Department of Information Security, Sejong University, Seoul, Korea
*Corresponding author

Introduction

To control disease transmission, monitoring the quarantine status of patients during pandemic situations caused by diseases such as COVID-19 should be given utmost importance [8, 5, 6, 3]. The Internet of Things (IoT) technology is used for efficient quarantine monitoring to control highly infectious diseases in many countries. For example, Bulgaria is the latest to join the list of countries that have tested a wristband that can track people during the COVID-19 pandemic. Additionally, South Korea and Hong Kong have been using electronic trackers to help enforce quarantine. Various IoT technologies are used to prevent people from leaving quarantine for the national health safety, of which electronic bracelet-type devices are used as a method [Figure 1] [1, 4]. This type of devices can report the user information in real-time to a control station, such as the Center for Disease Control(CDC), allowing the detection of regulatory violations, such as forced removal of the monitoring device and unauthorized departure from an isolated area.

However, these technologies pose problems such as leakage of personal information because various personal information, including location information, is collected[8, 2]. To overcome such problems, this research proposes a method for constructing a monitoring system that can ensure the safety of personal information by using physically separated memory and real-time streaming technology [4]. Consequently, a measure capable of ensuring the safety of the personal information of users is presented by operating the personal information of the user and the general driving information of the system separately.

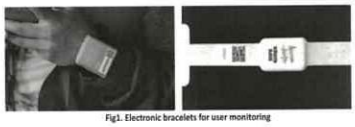
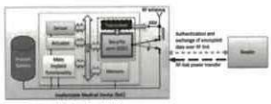
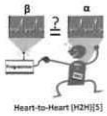


Fig1. Electronic bracelets for user monitoring

Related Work



Christos Strydis[7]



Heart-to-Heart (H2H)[5]

Christos Strydis[7] studied methods to prevent malicious external access in implantable medical device (IMD) environments. In this study, a new implant system architecture is proposed, wherein the security and the main implant functionality are completely decoupled by running the tasks on two separate cores. Wireless communication passes through a custom security application-specific instruction set processor, known as Smart-Implant Security Core, which runs an energy-efficient security protocol. The secure core is powered by the energy harvested from RF until external reader authentication is performed. This ensures safety against malicious access attacks, such as battery denial-of-service attacks.

Heart-to-Heart (H2H)[5] is a technology that uses biometric information for certification of medical devices. H2H uses ECG (heartbeat data) as an authentication mechanism, ensuring access only by a medical instrument in physical contact with an IMD-bearing patient. In addition, this study proposed an encryption device pairing protocol that prevents access through simple ECG comparison by extracting random data from ECG signals.

Threat Model and Assumptions

Several conditions must be satisfied to realize *S-DEB*. First, this system must support network communication for the transmission and updating of information. The data for normal operation of the *S-DEB* remain in non-volatile memory, even when the power is off. Therefore, the size of non-volatile memory must be minimized so that sensitive data do not remain in the memory. The size of the volatile memory must be minimal to minimize user damage in the event of data leakage and abuse. Next, we define the capabilities of an attacker. Threats to this system are characterized by the leakage or abuse of data, including personal information. We do not consider hardware attacks, such as bus probing and memory tampering. However, threats still exist, and we believe the risk of personal information leakage is serious. The software installed on the device still has vulnerabilities that could be exploited during sensitive data collection and system monitoring operation.

Approach and Challenges

The self-destructible electronic bracelets (*S-DEB*) presented in this study aims to protect the user information measured in real time and rapidly distinguish users who violate the regulations specified by the state and appropriate agencies in environments where tracking real-time locations and routes is a top priority, such as in regions affected by COVID-19. *S-DEB* attempts to minimize the leakage of personal information by utilizing Random Access Memory(RAM) wherein the stored data are volatilized and deleted when the power is cut off. The best technique to operate the embedded devices designed for monitoring users to prevent violations of regulations, such as out-of-quarantine and unauthorized access to specific zones, is to impose sanctions only if violations of regulations occur without providing personal information. Further, users whose monitoring has been terminated without regulatory violations would not have provided their personal information in any way to any target, including the control agency. However, for the safety of a country and its people, tracking user-specific information and distinguishing users who violate regulations are essential. Therefore, this study suggests a method to prevent the leakage and abuse of personal information through real-time streaming updates and by storing and using information in physically separable volatile memory.

C1.Separation of personal information and identification information: Implementing a secure monitoring system, such as *S-DEB*, should not involve personally identifiable information that can identify individuals through leaked or monitored information.

C2.Destruction of personal information: A secure monitoring system such as *S-DEB* shall be able to completely destroy the collected information.

C3.Prevention of personal information leakage: A secure monitoring system such as *S-DEB* should be able to remotely delete the data in the event of an information leakage and prevent recovery of the data through reverse engineering.

S-DEB

Basic Design

An *S-DEB* is a system for monitoring information such as the current position and movement paths of a user. All *S-DEBs* present in the platform can continuously update their identities from the control station. An ID is a key that is designed to distinguish users and is essential to transmit sensor values.

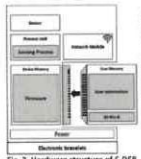


Fig. 2. Hardware structure of *S-DEB*

Hardware Structure The hardware structure of the *S-DEB* is shown in Figure 2. A battery provides the power supply that can run the *S-DEB* for a specified monitoring time. The "Process Unit" measures the *S-DEB* sensor values and determines the system and user abnormalities. Users must mount a 'User Memory' to utilize the *S-DEB* system to use the system and devices. The User Memory stores the unique ID of a user in the control station, when the user receives the device and saves the sensing values measured by the Process Unit during device operation. The *S-DEB* operates normally only when a User Memory is installed. If the User Memory is uninstalled abnormally or the user violates the policy, the *S-DEB* sends the information stored in the User Memory to the Control Station.

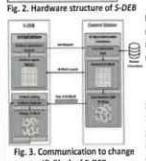


Fig. 3. Communication to change ID-Block of *S-DEB*

User Memory User Memory consists of volatile memory. After the monitoring period is complete, the user can manually unmount the User Memory from the *S-DEB* and delete the data by turning the power off. If the User Memory is removed arbitrarily during the monitoring period, the *S-DEB* reports the status of the user to the Control Station.

Real-time Software Streaming The Control Station updates the ID stored in the User Memory of *S-DEB* through network streaming. Leakage of personal information can be prevented because the ID is updated in real-time. The user can delete the ID and sensing information by dismounting the User Memory or on receiving an information removal command from the Control Station.

Solving the Challenges

Three major challenges were presented in section 3: (a) separation of personal information and identification information, (b) destruction of personal information, and (c) prevention of personal information leakage. In this subsection, we describe the technique by which the *S-DEB* addresses these challenges.

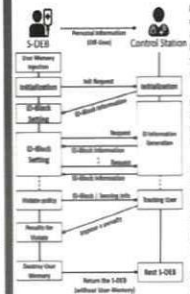


Fig. 4. Operation sequence of *S-DEB* and Control Station

Initialization As described in the previous section, the *S-DEB* has an internal device memory. When a user mounts the User Memory on the *S-DEB*, the SDEB sends an *InitRequest()* to the Control Station, following which the Control Station generates an Identification Block (ID-Block) based on the registered user's information and sends it to the *S-DEB*. The *S-DEB* performs the writing process of the ID-Block received in the internal user memory.

Identification Block Streaming It continuously sends some of the segmented ID-Block operation values to the *S-DEB*. The *S-DEB* applies the received IDBlock values to the ID-Block in the User Memory to maintain the other IDBlock . Figure 3 shows the initialization and ID-Block Streaming processes of the Control Station and the *S-DEB*.

Request/Response The *S-DEB* requests an ID-Block update from the Control Station at regular intervals and receives and updates the new ID-Block information. If the ID-Block information is not received within a certain time after an ID-Block Request, the *S-DEB* performs a Reset operation and attempts Initialization again. Furthermore, if there is no ID-Block update request from the *S-DEB* within a specified period, the Control Station determines this to be abnormal behavior and sends a *Reset()* command

Reporting of Sensing Data If a user violates the policy specified by the Control Station (scenarios such as a user leaving the isolation zone, or if the User Memory is unmounted), the *S-DEB* transmits the user's recently measured sensing data and ID-block to the Control Station. Figure 4 illustrates the process implemented if a user violates the specified policy.

End of Monitoring If the monitoring period is complete, or monitoring is no further required, a user can unmount the User Memory from the *S-DEB* by oneself. If the User Memory is unmounted, the sensing information and the ID are deleted at the same time. If a user could not unmount the User Memory, the power to the *S-DEB* can be cut off by receiving a *Finish()* command from the Control Station to delete the internal data of the User Memory

Leakage of Data When the *S-DEB* is physically removed from the user, the power is automatically cut off, and the data in the Device Memory and the User Memory located inside are deleted. Moreover, if abnormal behavior is detected in the *S-DEB* (such as high network load rate and timeout of Request/Response), data leakage can be prevented by an Emergency *Stop()* command from the Control Station

Conclusion

An *S-DEB* was presented to address the problem of personal information leakage and the abuse of the embedded systems used to monitor users in scenarios such as quarantine monitoring in pandemic situations including COVID-19. By using the real-time binary block streaming technology and hardware-isolated memory, the *S-DEB* can prevent personal information leakage and abuse. Although this study has not been implemented, we expect additional research will help prevent the leakage and abuse of personal information in pandemic situations such as COVID-19. Furthermore, we will study data protection using the volatile features of hardware memory proposed in this study in the future.

Reference

1. Processing privacy while addressing covid-19. https://blogs.microsoft.com/on-the-issues/2020/04/20/privacy-covid-19-data-collection/ (Apr 20, 2020)
2. A 'travelling' of the times in south korea: Mapping the movements of coronavirus carriers. https://www.washingtonpost.com/ (March 14, 2020)
3. Cho, H., Ippolito, D., Yu, Y.W.: Contact tracing mobile apps for covid-19: Privacy considerations and related trade-offs. arXiv preprint arXiv:2003.11511 (2020)
4. Marzal, U., Yaghagh, A., Pai, S.: Plar: Towards a pluggable software architecture for securing iot devices. In: Proceedings of the 2nd International ACM Workshop on Security and Privacy for the Internet-of-Things. pp. 50–57 (2019)
5. Kotsias, M., Juels, A., Kosafidis, F.: Heart-to-heart (h2h) authentication for implanted medical devices. In: Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. pp. 1099–1112 (2013)
6. Singh, R.P., Javaid, M., Haleem, A., Suman, R.: Internet of things (iot) applications to fight against covid-19 pandemic. Diabetes & Metabolic Syndrome: Clinical Research & Reviews (2020)
7. Strydis, C., Seepers, R.M., Peris-Lopez, P., Sklavos, D., Sourdis, I.: A system architecture, processor, and communication protocol for secure implants. ACM Transactions on Architecture and Code Optimization (TACO) 13(4), 1–25 (2016)
8. Zhang, Z.K., Cho, M.C.Y., Wang, C.W., Hsu, C.W., Chen, C.K., Shieh, S.: Iot security: ongoing challenges and research opportunities. In: 2014 IEEE 7th international conference on service-oriented computing and applications. pp. 230–234. IEEE (2014)