International Journal of Advanced Science and Technology
Vol.111 (2018), pp.97-106
http://dx.doi.org/10.14257/ijast.2018.111.09

Designing and Implementation a Secure Electronic Attendance System with in Reliability Assurance through an Analysis of Security Threats of Electronic Attendance Systems

Hyunjoo Kim[1] and Seongjong Kim[2]

[1]Dept. Of Electronic & Electrical Engineering Dan-kook University, Korea
[2]Dept. Of Aviation and IT Convergence, Far East University, Korea
[1]chopinkhj@gmail.com

Abstract

As electronic attendance systems are increasingly used, security threats are also increasing. With the recent introduction of an electronic attendance absence recording system at universities to emphasize the reliability and accuracy of attendance management, illustrations of the system's practical use in the academic administration business are increasing. The existing electronic attendance systems were mainly operated for large-scale lectures with a large number of students. The systems, which were initially intended to resolve the inconvenience of handling many students' attendance within a certain time period, are currently being used in various ways. The currently used electronic attendance–absence recording system is classified into the following technologies: smartcard-based, location-based beacon, smartphone-related phone-to-phone-based, and quick-response-code-based electronic attendance–absence recording systems. But, most of these attendance management applications have many security threat elements as security inquiry has not been conducted properly. In particular, the commonly used beacon-based electronic attendance–absence system uses mobile phones, beacons, and Bluetooth, and therefore is at a risk of many elements whose security safety has not been properly examined. The current study aims to support a safer electronic attendance–absence recording system by performing the security check of operation cases of such systems managed by universities and systematically analyzing the trend of security threat in these systems.

***Keywords**: Electronic Attendance Absence*

1. Introduction

With the increase in the use of electronic attendance systems, security threats are also increasing. There has been an increase in the number of universities introducing the electronic attendance–absence recording system to emphasize the exactness and accuracy of attendance management and utilizing the system for academic administration business. The existing electronic attendance systems were mainly operated for large-scale lectures with a large number of students. The systems, which were initially intended to resolve the inconvenience of handling many students' attendance within a certain time period, are currently being used in various ways. In an electronic attendance system, attendance is confirmed by using an electronic mechanical device. Most universities in Korea are operating electronic attendance systems to ensure accurate attendance and to prevent manipulation of the existing manual operation in large-scale lectures. Presently, all universities in Korea manage the electronic attendance–absence recording system to check the accuracy of attendance and prevent attendance manipulation. The currently used electronic

Received (October 8, 2017), Review Result (December 19, 2017), Accepted (January 25, 2018)

attendance–absence recording systems are classified into the following five types of technologies: smartcard-based, location-based beacon, phone-to-phone-based, quick response (QR)-code-based, and authentication-number-transmission-based electronic attendance absence recording systems. All these technologies, except for the smart card based system, use smartphones. Therefore, the early electronic attendance–absence recording systems started as optimal systems that performed a quick and accurate attendance–absence process by using student IDs to solve this issue. However, universities did not prefer this smartcard-based electronic attendance–absence recording system because it required tagging, which was only to be performed using a card for checking attendance–absence and the initial purchase cost of such electronic attendance–absence devices was expensive. Nevertheless, most universities have recently begun to focus on the electronic attendance–absence recording systems because according to the national policy, the strictness of classroom management has been emphasized as a part of evaluation indexes of local universities. The most widely used electronic attendance–absence method authenticates individuals by using their smartphones and confirms their attendance. Most universities use the location-based beacon electronic attendance–absence recording system; however, this system uses mobile phones, beacons, and Bluetooth, and therefore is at a risk of many elements whose security safety has not been properly examined.

This study performed security checks of operation cases of the electronic attendance–absent recording system managed by universities. In particular, we checked the trend of security threat of the most commonly used electronic attendance–absence technologies and analyzed the security threat. Currently, three of the most popular electronic attendance systems at universities are selected and analyzed to determine whether they meet the OWASP standards, to analyze mobile security vulnerabilities and design and implement a secure electronic attendance system.

The system proposed in this paper was designed as an electronic attendance system that guarantees security and reliability by addressing the security threats of the existing ones.

2. Related Work

2.1. The Definition of Electronic Attendance-Absence

Electronic attendance–absence refers to an electronic machine that checks the attendance–absence for a class [1]. Early electronic attendance–absence systems began with the intention of processing the attendance–absence quickly and accurately by using a smartcard or a student ID card equipped with radio frequency identification (RFID) for classes with many attendees. The electronic attendance–absence recording system refers to a system in which an application program is incorporated into an attendance–absence machine that checks the attendance–absence by using an electronic machine.

2.2. The Characteristic of Electronic Attendance-Absence

The major characteristic of an electronic attendance–absence system is that it can manage various analyses in real time by using lecture time setting, attendance status check with respect to subject and student, electronic attendance record, attendance record inquiry, and attendance statistics. In addition, an accurate electronic attendance–absence helps increase students’ participation in classes and minimizes student complaints by preventing proxy attendance. Primarily, the improvement of class productivity can be achieved through personnel reduction owing to the attendance–absence management of large-scale lectures [2].

2.3. Electronic Attendance-Absence Application Case Situation

As described earlier, the technology applied in electronic attendance–absence systems are classified into the following types: smartcard-based, location-based beacon electronic, smart phone-related phone-to-phone-based, QR-code-based, and authentication-number-transmission-based electronic attendance–absence recording systems. The early electronic attendance–absence systems were mainly based on smartcards and performed the attendance–absence process quickly and accurately by using student ID cards to reduce the time required for the process for large lectures with many attendees. The method of tagging information for identifying attendance by sending personal information of an individual from a smartcard to a central server was most commonly used. However, the smartcard-based electronic attendance-absence system requires tagging, which could be done only by using a card for checking attendance–absence and the cost of this system was high; thus, this was not a preferred model for small-sized universities.

Currently, the most widely used technology is the beacon-based electronic attendance–absence system using Bluetooth. This system installs a beacon in a classroom. A user smartphone app finds the location of the beacon and communicates with the main center server to check electronic attendance–absence of the user. Alternatively, students communicate with a server by connecting to Bluetooth of a professor’s smartphone and checking the attendance–absence. In yet another method, the attendance–absence is checked by a professor transmitting an authentication number to the students. By using a QR code, the attendance–absence can be checked in a specified time by a server transmitting a one-time password (OTP) QR code to students. The electronic attendance system using QR codes had a short development period; it was the cheapest method in terms of operating cost. However, electronic attendance using QR codes is mainly used as a secondary means of attendance-checking in the universities that use smartcards as the electronic attendance method.

2.4. OWASP Mobile Security Project

The mobile security project of the OWASP foundation describes 10 weak points frequently encountered in mobile devices. [Figure 1] illustrate the top 10 mobile risks of the OWASP Mobile Security Project, describing 10 mobile security weak points by using a table. In this study, a security vulnerability analysis is conducted in terms of the OWASP Mobile Security Project. The vulnerabilities M1 through M10 are described as follows:

- M1: Improper Platform Usage indicates unintentional behaviors that occur on the Web because of problems caused by unreliable input values, misuse of platform functionality, or the lack of security controls.
- M2: Insecure Data Storage is a vulnerability that occurs due to sensitive information being stored in an unsecure location or unintended data leakage.
- M3: Insecure Communication is a vulnerability that occurs when data is not encrypted during communication with the server for data transmission; or due to an incomplete connection such as an SSL connection error.
- M4: Insecure Authentication means a vulnerability due to a user authentication error caused by incorrect session management.
- M5: Insufficient Cryptography indicates a vulnerability due to an incorrect cryptography attempt.

- M6: Insecure Authorization indicates a vulnerability due to failure of authorization decisions on the client side and authorization errors caused by user authentication.
- M7: User Code Quality refers to buffer overflows and format string vulnerabilities that occur during the operation of a mobile device.
- M8: Code Tampering covers binary patches, local resource modification, method hooking, method swizzling, and dynamic memory modification issues. An attacker can either modify code, alter memory, or alter the system APIs that an application uses, thereby providing the attacker with the means to convert the usage of a software for monetary benefits.
- M9: Reverse Engineering is a vulnerability that exploits revealing information about back end servers, cryptographic constants and ciphers, and intellectual property rights in applications by analyzing source code, libraries, algorithms, and final core binaries.
- M10: Extraneous Functionality describes a hidden backdoor functionality, internal development security controls that are not intended to be released in a production environment, or disabling two-factor authentication during an application testing [3-5].

OWASP Mobile Top 10 Risks
M1- Improper Platform Usage
M2- Insecure Data Storage
M3- Insecure Communication
M4- Insecure Authentication
M5- Insufficient Cryptography
M6- Insecure Authorization
M7- Client Code Quality
M8- Code Tampering
M9- Reverse Engineering
M10- Extraneous Functionality

Figure 1. Top 10 Mobile Risks [5]

3. Security Threat Analysis for Electronic Attendance-Absence Recording System

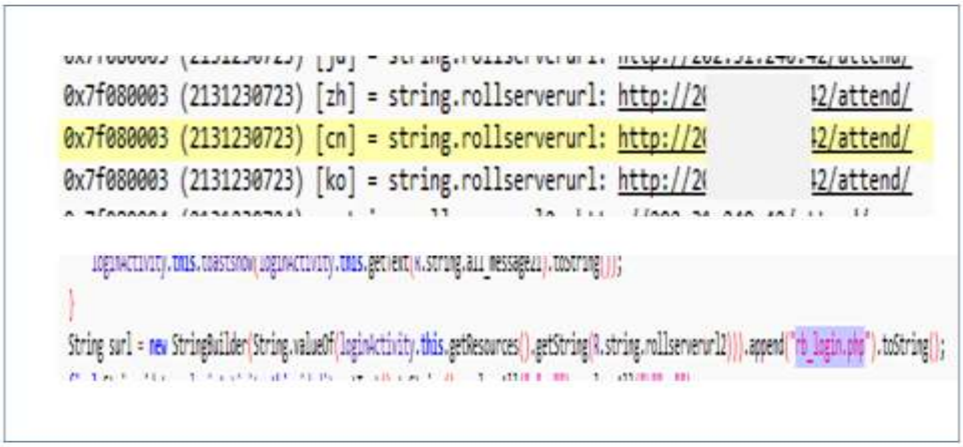
3.1. Overview of the Security Threats Analysis

The Most of the recently used electronic attendance–absence recording systems are implemented using applications in mobile devices. Therefore, we analyzed the security weak points of the system in universities based on the 10 mobile security weak points categorized by the OWASP Foundation's Mobile Security Project [4-5].

3.2. Analysis of Security Weak Points of the Electronic Attendance-Absence Recording System by University

This study conducted security checks for main operation cases of the electronic attendance–absence most commonly operated in universities. We selected three universities, say A, B, and C, for security check and analyzed the trend of security threats of the electronic attendance–absence recording system. The results of the analysis based on the top 10 mobile risks of the Mobile OWASP Mobile Security Project showed the following common security threats: M2, Insecure Data Storage; M3, Insufficient Transport Layer Protection; M5, Poor Authorization and Authentication; and M9, Improper Session Handling.

In the case of university A, the beacon information was stored as a plain text. We found the system vulnerable to security threats as the electronic attendance–absence app used a weak encryption algorithm with an easy mechanism for the beacon and user information. An attacker could fool his/her location by exploiting this, and there was a possibility for a malicious shell to be sent to the server. In addition, we could confirm the absence of obfuscation of the app and memory-related security technique; thus, an attacker could use a dynamic-based app analysis technique to tamper with the app. The analysis results showed that the server address was exposed as it was. The json object was created and converted into a String, and then the method of transmitting data by Post method was exposed. This is an insecure data storage vulnerability of M2, which requires encryption to be applied when storing data. In addition, the system was identified as the most vulnerable electronic attendance–absence recording system exposed to vulnerabilities such as weak communication, weak authentication and authorization, code tampering, and reverse engineering.

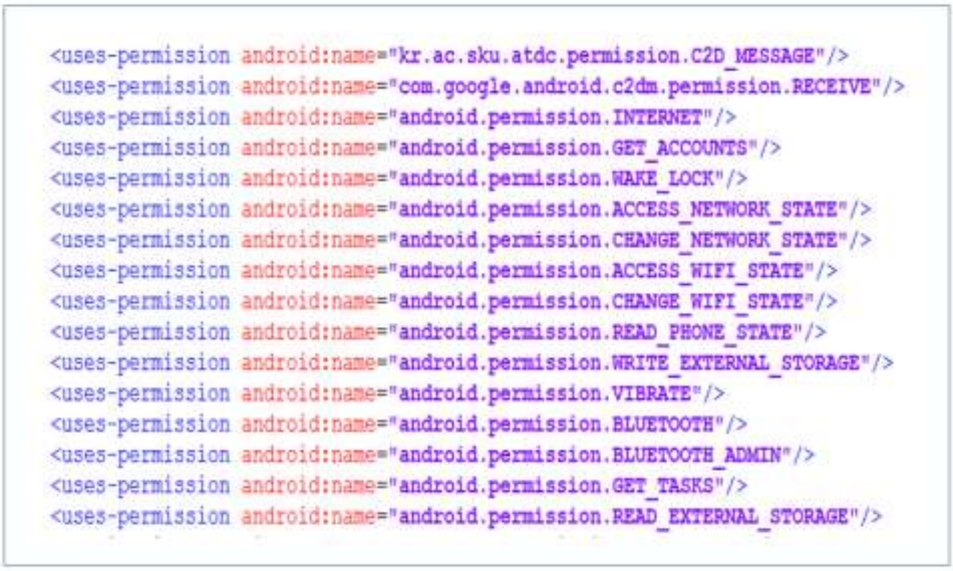


```
0x7f080003 (2131230723) [zh] = string.rollserverurl: http://2[redacted]42/attend/
0x7f080003 (2131230723) [cn] = string.rollserverurl: http://2[redacted]42/attend/
0x7f080003 (2131230723) [ko] = string.rollserverurl: http://2[redacted]42/attend/
```

```
    loginActivity.this.toastShow(loginActivity.this.getText(R.string.all_message21).toString());
}
String surl = new StringBuilder(String.valueOf(loginActivity.this.getResources().getString(R.string.rollserverurl2))).append("rb_login.php").toString();
```

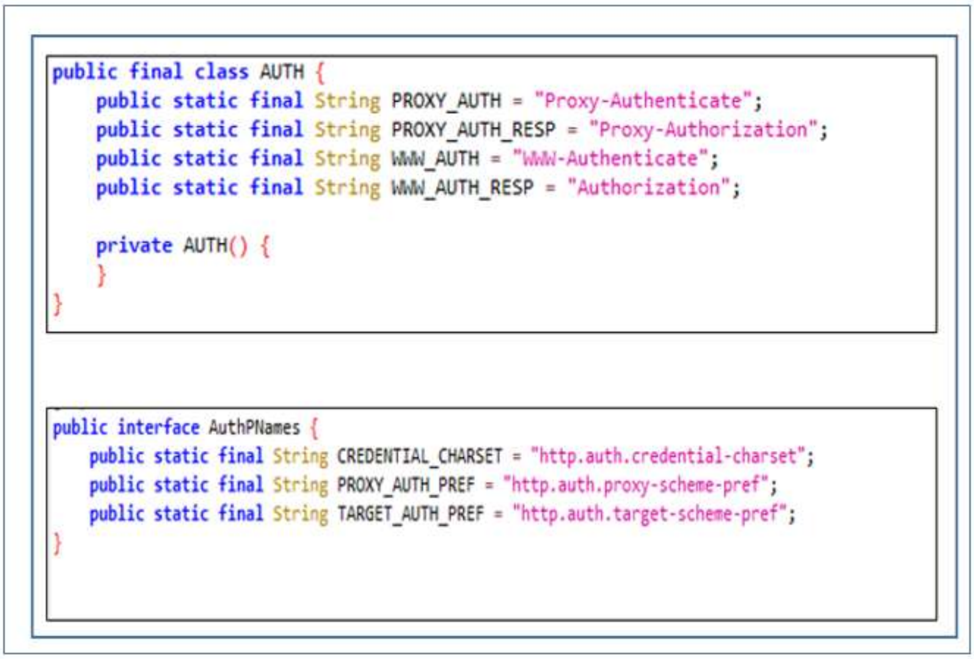
Figure 2. A University Server Information Exposure (Example)

In case of University B, unsafe data storage was found. B University was developed using the open source AltBeacon, and the config file was saved in json format and used from AltBeacon. Moreover, the authentication parameters of the httpclient communication process were exposed as they were. We could confirm that the login address of the server was stored as resource type and plain text. As this information is important for system operation, it should be securely encrypted and stored. In addition, the ID and password were encrypted and sent at login attempts, yet the encryption key value was stored as a form of plain text in the app. This is an M3 security risk. The didRangBeaconsInRegion() and didEnterRegion() functions calculate beacon information and distance. A vulnerability has also been found in which an attacker can change and transmit data at a desired location through M8 code modulation.



```
<uses-permission android:name="kr.ac.sku.atdc.permission.C2D_MESSAGE"/>
<uses-permission android:name="com.google.android.c2dm.permission.RECEIVE"/>
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="android.permission.GET_ACCOUNTS"/>
<uses-permission android:name="android.permission.WAKE_LOCK"/>
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
<uses-permission android:name="android.permission.CHANGE_NETWORK_STATE"/>
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
<uses-permission android:name="android.permission.READ_PHONE_STATE"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.VIBRATE"/>
<uses-permission android:name="android.permission.BLUETOOTH"/>
<uses-permission android:name="android.permission.BLUETOOTH_ADMIN"/>
<uses-permission android:name="android.permission.GET_TASKS"/>
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
```

Figure 3. B Transitional Authority of University (Example)



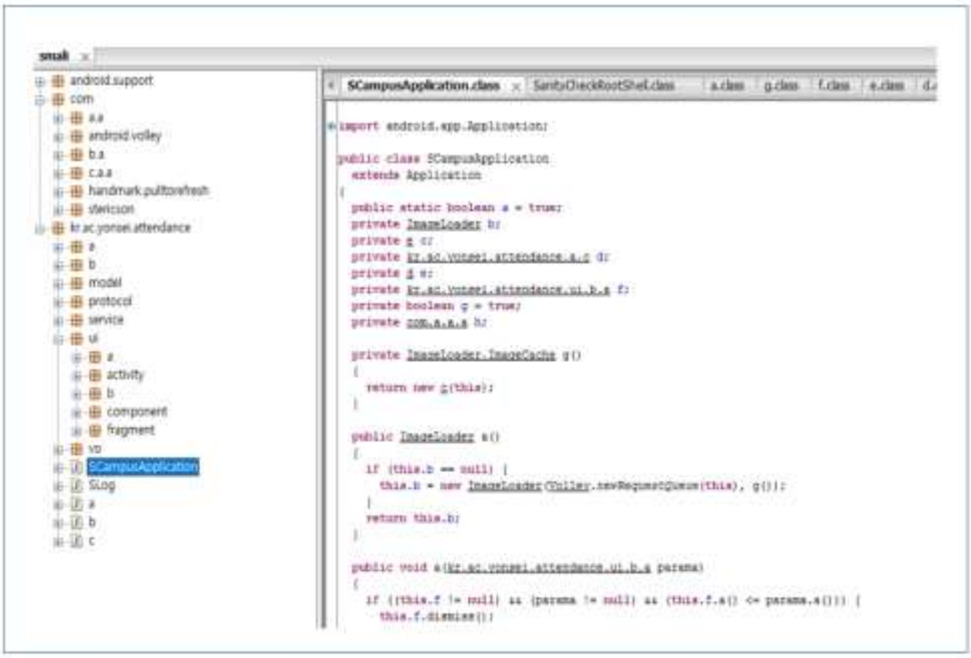
```
public final class AUTH {
    public static final String PROXY_AUTH = "Proxy-Authenticate";
    public static final String PROXY_AUTH_RESP = "Proxy-Authorization";
    public static final String WWW_AUTH = "WWW-Authenticate";
    public static final String WWW_AUTH_RESP = "Authorization";

    private AUTH() {
    }
}
```

```
public interface AuthPNames {
    public static final String CREDENTIAL_CHARSET = "http.auth.credential-charset";
    public static final String PROXY_AUTH_PREF = "http.auth.proxy-scheme-pref";
    public static final String TARGET_AUTH_PREF = "http.auth.target-scheme-pref";
}
```

Figure 4. B University's M4 Unsafe Authentication (Example)

We could confirm that University C was more secure than Universities A and B. The apps in University C had several features to defend against M8 (code tampering) and M9 (reverse engineering). However, we could confirm that they were using Stericson.RootShell open source for routing detection to prevent code tampering. This open source checks the known routing apps, SU binaries, and build.prop values for routing detection. This is a simple routing detection technique and techniques for bypassing this open source are currently well known; thus, we consider that it is inappropriate to use this method for electronic attendance–absence process. In addition, University C uses obfuscation to prevent reverse engineering. The system used iBeacon which was more secure than the existing beacon. The tendency to be prepared for security vulnerability made it difficult to conduct an analysis by applying methods and string obfuscation, and by using Java Reflection.



```
import android.app.Application;

public class SCampusApplication
  extends Application
{
  public static boolean a = true;
  private ImageLoader b;
  private g c;
  private kr.ac.yonsei.attendance.a.c d;
  private d e;
  private kr.ac.yonsei.attendance.ui.b.a f;
  private boolean g = true;
  private com.a.a.a h;

  private ImageLoader.ImageCache g()
  {
    return new g(this);
  }

  public ImageLoader a()
  {
    if (this.b == null) {
      this.b = new ImageLoader(Volley.newRequestQueue(this), g());
    }
    return this.b;
  }

  public void a(kr.ac.yonsei.attendance.ui.b.a parama)
  {
    if ((this.f != null) && (parama != null) && (this.f.a() <= parama.a())) {
      this.f.dismiss();
```

Figure 5. C University's Use Reverse Engineering (Example)

4. Design and Implementation of Secure Electronic Attendance System Reliability

This study conducted security audits focusing on the most commonly operated electronic attendance systems in universities and examined the security vulnerabilities based on the 10 vulnerabilities in the OWASP Foundation's Mobile Security Project. Based on this, this study sought to design an electronic attendance system that guarantees safety and reliability by addressing the vulnerabilities of existing systems. The re-designed flow of the implementation and the improved design of the secure electronic attendance system that guarantees reliability in terms of the Mobile Security Project are described as follows:

- M1 Improper Platform Usage: It is reaffirmed that validation and authorization, especially that of unauthenticated functionality, are provided to the application to prevent unusual behaviors on the Web.
- M2 Insecure Data Storage: To prevent user data from being misused, user data is designed to be automatically deleted at the time of logout. When it is required to be stored, the iOS and Android devices are designed to be managed separately.
- M3 Insecure Communication: Instruct to connect via HTTPS and to manage sessions with a time limit.
- M4 Insecure Authentication and M5 Insufficient Cryptography: The login password is designed to be encrypted by applying a strong encryption procedure and the 3DES encryption algorithm according to the national security guidelines. For example, a password should consist of eight or more characters that include a mix of upper case, lower case, numeric, and special characters. If the number of login attempts exceeds the threshold, the connection will be automatically blocked and a user notification will be issued.

- M6 Insecure Authorization: The access speed is designed to be improved by reducing excessive privileges based on user classification; a device registration and a user are connected to only one session with one device. It is also designed to automatically logout after a certain time if no user intervention is made.
- M8 Code Tampering: It is designed to adopt a session mode because injection attacks can occur on the server or database when the data value is altered due to a binary patch, local resource modification, memory modification, attacker's code modification, or application user system API modification.
- M9 Reverse Engineering: De-compiling or reversing makes it impossible to determine the structure of an application, and it detects the Android device rooting or iOS device jailbreaking to examine if debuggers are running. In addition, it is designed to dynamically generate and apply a data encryption key when the client connects to the server.
- M10 Extraneous Functionality: Through documentation of the hidden backdoor functionality that may occur during the development process, or the internal development security functionality that is developed unintentionally during system testing, it is reconfirmed that the source is deleted or disabled after completing the operation.

As described above, OWASP's Mobile Security Project improves the vulnerability of M1 to M10 and applies it to the proposed system to implement a secure electronic paging system.

5. Conclusions

The use of electronic attendance–absence recording systems enables operators to check in real-time attendance status according to the subject, student attendance status, electronic attendance record, attendance record inquiry, and attendance statistics. In addition, it aims to support efficient educational management systems by improving students’ participation in class through accurate attendance–absence management and minimizing their complaints by preventing proxy attendance.

This study conducted security checks for the currently used electronic attendance–absence recording systems at local universities. This study sought to design a secure electronic attendance system by addressing the security vulnerabilities of the existing systems used in domestic universities. We checked security threats by selecting three types of electronic attendance-absence recording systems most widely used in universities. We found most of the security vulnerabilities defined in top 10 mobile risks of OWASP Mobile Security Project for the electronic attendance–absence recording systems. From among those security threats, we determined the following security threats commonly shown in the three electronic attendance–absence recording systems: M2, Insecure Data Storage; M3, Insufficient Transport Layer Protection; M5, Poor Authorization and Authentication; and M9, Improper Session Handling. This indicates that the attacker can use these threats to tamper with the data. In other words, this is an example of the fact that most of the commercially available electronic attendance–absence recording systems are poorly developed from a security perspective. In addition, this analysis showed cases in which some individuals took advantage of the system by tampering with its data.

In order to overcome those vulnerabilities, a secure electronic attendance system was designed and implemented based on the top 10 mobile risks of the OWASP Mobile Security Project. The proposed system improved the login information, data encryption, data storage, and the history of communication with the server so that the users could be provided a secure and reliable electronic attendance system. We applied the vulnerability of 10 items of OWASP to the proposed system to implement a secure electronic check - in system in response to security threats.

The proposed system improved the login information, data encryption, data storage, and the history of communication with the server so that the users could be provided a secure and reliable electronic attendance system.

In addition, based on this research, we will open-sourced the secure electronic attendance system technology to cope with the security threat of the electronic attendance system, and will freely use this technology in the university where it is needed.

Acknowledgment

This work was supported by the 2018 Far East University Research Grant (FEU 2018).

References

[1] D. Ryu, "Development of BLE Sensor Module based on Open Source for IoT Applications", J. of the Korea Institute of Electronic Communication Sciences, vol. 10, no. 3, **(2015)**, pp. 419-424.

[2] J. Kim, "A Smart Home Prototype Implementation Using Raspberry Pi", J. of The Korea Institute of Electronic Communication Sciences, vol. 10, no. 10, **(2015)**, pp. 1139-1144.

[3] E.-S. Kim, S.-C. Park and S.-C. Kim, "Trends of Application Technology and Service Based on Beacon", Korea Society For Internet Information, vol. 17, no. 1**, (2016)**, pp. 335-346.

[4] https://www.owasp.org/index.php/OWASP_mobile_Security_Project.

[5] J.S. Cho, H.J. Choi, S.Y. Kim and H.S. Kim, "Researching Security Threats and Countermeasures for Mobile PinTexh Application", Communications of the Korean Institute of Information Scientists and Engineers, ISSN 1229-6821, vol34, no. 4, **(2016)**, pp. 34-41.

[6] H. Soo-A, S.-C. Park and J.-H. Kim, "Design and Implementation of Smart Acess System Using Bluetooth Beacon in IoT Enviroment", Korea Society For Internet Information, **(2015)**, pp. 265-266.

Authors

Hyun-Joo Kim, she is a Team Leader of the Computerized Information Office, Hyupsung University, Hwaseong-Si Kyeonggi-Do, Korea. Her received his Ph.D. degree in Electronic & Computer Engineering at Dankook University, Her recent interests are in big data, mobile payment, java card, ubiquitous, smart information system, internet of thing, security in general and cloud computing. She can be reached chopinkhj@gmail.com. ***first authorr*

Seong Jong Kim, he received the bachelor's degree in the Department of Electronics from the DanKook University in 1987. He received the M.S. degree and the Ph.D. degree in the Department of Electronics from DanKook University in 1989 and 1998, respectively. He was a professor in the Department of Ubiquitous IT at FarEast University since 1998. His current research interests include IoT, EoT, Security of IT and embedded system. He is a member of the KKITS. **corresponding author*