

# **XECRET: REMOTE DELETION CRITICAL OF FILE ON STOLEN MOBILE VIA SMS**

**Ahmad Kamil Kamaruddin Malik, Shamsul Kamal Ahmad Khalid**  
*Faculty Computer Science & Information Technology, University Tun Hussein*  
*Onn Malaysia,*  
*Johor, Malaysia*  
kamil.kamaruddin@outlook.com, shamsulk@uthm.edu.my

**Abstract.** Nowadays, many people lost their phone at public area. This may lead to data disclosure when someone find into the phone information and expose to public. However, there are many remote wiping tools have been developed. But there is issue on connection and wiping methods. In this project, remote wiping is developed to delete file from stolen phone called Xecret application. This project creates an alternative way to remote wiping. Xecret application use Single-Pass Write Zero to make sure the data cannot be retrieved and using SMS (Short Message Service) to connect to stolen phone.

## **1 Introduction**

Nowadays, mobile phone is a necessity for everyone regardless of ages. Mobile phone usage has been increasing with the widespread use of social media and online shopping. Some people even have more than one mobile phones, to be used for work and for entertainment. Mobile phone helps people in their daily activities such as making communication and storing of information easier. Furthermore, it allows users to keep pictures and personal information in one place. In short, mobile phone can ease users from bringing book, album and important documents.

Number of mobile devices grow from year to year. Loss of devices is one of the problems faced nowadays. When a mobile device is lost, user will try to locate it by calling the device's phone number. However, it only works if it is within a close distance to the user. A bad person who steals or finds the mobile device may use the information stored in the device for illegal purposes. Lost mobile phones may lead to data privacy disclosure that can affect the owner's reputation.

Due to the data privacy disclosure, mobile phone users need to be aware about the importance of mobile phone security. User needs to know that mobile phones are vulnerable to be lost or stolen. Due to this, some precaution needs to be taken for instance by installing remote wipe application in the phone. The application can be used to send remote wipe instruction to erase important information in the phone.

There are already some existing applications on the market providing features to solve stolen or lost phone issues. One example of existing application available in the market is 'Find My Device' which has been developed by Google on August

2017. Nevertheless, the application requires connection to server via internet connection to operate.

Thus, an application called XECRET application is proposed. XECRET only uses SMS (no server required) via 4G network or internet connection to send remote wiping instruction. It does not require a server like the implementation of 'Find My Device'. XECRET focuses on secure remote deletion of folder selected by user during installation via proposed SMS instruction. XECRET agent will be installed in a Slave phone (the phone that need to be monitored if stolen) and Master phone (the phone that issue the wiping command).

## 2 Related Works

In this project, a remote data wiping operation will be developed when the private information in a device can be deleted remotely using a SMS command. The user needs to install the Xecret agent in the mobile phone and adjusts the settings in the application. Once the phone receives the right command through the SMS from the device's owner, the agent will run the data wiping process in the current mobile phone.

### 2.1 Comparison of Existing Operating System

Table 2.1: Comparison of various operating system platform

OS Info	Android	iOS	Windows	KaiOS
Worldwide Smartphone Market Share Source: GS. StateCounter (October 2018)	74.69%	22.34%	0.36%	0.93%
Smartphone Company	Samsung, Huawei, Xiaomi, Sony, LG	Apple	HTC, Dell, Nokia	JioPhone, Alcatel, Nokia, Maxcom
Operating System Source	Open	Closed	Closed	Open (Linux)
Application Market	Google Playstore	Apple App Store	Windows Phone Store	KaiStore

Table 2.1 shows four different platforms for mobile phones were compared to determine which platform is best suited for the proposed application. Android platform dominated the mobile market with a share of 74.69 percent, followed by iOS (22.34 percent), Windows (0.36 percent) and KaiOS (0.93 percent). In conclusion, the Android operating system platform was chosen by most of the users.

## 2.2 Data Wiping

Data wiping means erasing the files content after overwriting the files content with some characters like null character or randomized character. After wiping process, it becomes impossible to recover the previous existing data because it deletes the links to memory blocks and replace the files content with some new character value (Olvecky & Gabriska, 2018).

### 2.3.1 Technique of Data Wiping

Data wiping is one way to delete a file in computer securely. Perfect process of wiping data can make retrieve of data become impossible. There are two type of data wiping techniques that already available on the internet can be shown in table 2.1 below: -

Table 2.1: Description of Data Wiping Techniques

Data Wiping Technique	Description
Degaussing	Deletion of data by using magnetic field on hard disk to corrupt the entire disk.
Overwritten	Overwrite the existing data on hard disk using existing method with multiple round to make sure the data are irretrievable.

## 3 System Methodology

In this chapter, the methodology for development of Xecret application is discussed. Methodology refers to the application development method, rules, standards and techniques. The methodology allows people to examine whether the project meet their requirements or not (Yeh & Tanik, 1989).

Prototype software development method is chosen in developing the Xecret application. Prototype is the first product example that needs to be developed. So that, people can test it while it's still in developing process.

The prototype software development methodology is a system development method (SDM) in which a prototype is built, tested and modified as necessary until an acceptable prototype is finally reached from which the entire application now be developed. This model works best in situations where not everything works (Jones et al., 1992). Prototype software development can be separated into few types, which are throwaway prototyping, evolutionary prototyping and incremental prototyping. Evolutionary prototyping methodology were used in development of Xcret Application

### 3.1 Comparison of Prototyping Methodology

Table 3.1: Comparison Between Prototype Method

Prototype Method Characteristic	Throwaway	Evolutionary	Incremental
Period	Very Short Period	Short Period	Long Period
Testing	Not Used for Testing	Used for Testing & Training	Used for Testing & Training
User Understanding	Hardest (Prototype produce to validate requirement)	Easy (Stages prototype to become final system)	Easiest (Prototype is produced by parts)

Based on Table 3.1, Evolutionary Prototyping Methodology is used because its support short period development time and can be used for testing functionality. Furthermore, the prototype application can be extended for developing the actual application. Refer to this comparison, the proposed project will be implemented using Evolutionary Prototype Methodology.

### **3.2 Evolutionary Prototype Methodology Phases**

Evolutionary prototype methodology phase consists of 5 phases namely planning phase, analysis phase, design phase, prototype phase and testing phase.

#### **3.2.1 Planning Phase**

During planning phase, objective of developing the application has been defined. All the problem statements already stated, and the project is acceptable to be developed. In the planning phase for Xecret applications, all mobile operating systems are examined to select the most appropriate operating system to be developed the application. The Android operating system was chosen because of it allow developer to build their own application and the most widely used operating system in the world.

#### **3.2.2 Analysis Phase**

Analysis phase is conducted, at this phase all important information and jargon words are reviewed to determine which technique and software are suitable while developing this project. Furthermore, Techniques of data wiping have been analyzed and Single-Pass Write Zero technique were chosen in wiping data process. Then, the Java language was used to develop the Xecret application because it is Object-Oriented Programming (OOP). This programming language makes it easy for the developer to create classes and inherited information from another class.

#### **3.3.3 Design Phase**

Design phase is carried out to design the interface of the application for user. Proper design should be user friendly to ensure that user can understand and manage to use the application without any problems. All buttons, font types and colors used in the interface design must be suitable to avoid burdens on the user while using the application.

Xecret application was develop native application-based. Native application is a software program developed use on device. Native application can quickly access multiple services on a device such as microphone and camera. Xecret application interface was build using Android Studio using XML language.

### 3.2.4 Prototype Phase

Prototype phase is process of development application will be conducted. The application will have many versions during the development of the prototype due to errors and errors. Every bug and error that the developer solves will create a new prototype version to distinguish between old and new applications. The Xecret application prototype will be tested on the mobile phone to determine the functionality and interface design.

### 3.3.5 Testing Phase

Finally, testing phase will be conducted before delivered the final version of application to end user. Xecret application will be tested all their functionality to ensure there is no bug and error occur before handed to end user. User feedback also will be determined by using questionnaire, user will test the application based on their interface design and functionality.

## 3.4 System Architecture

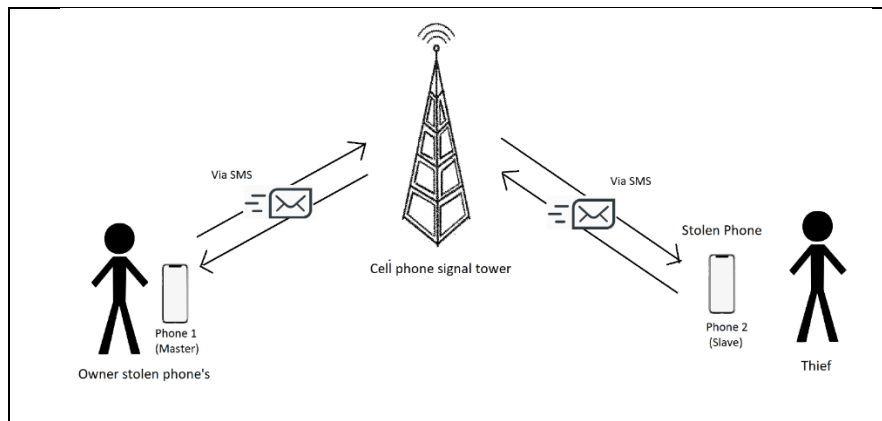


Figure 3.4: System Architecture Diagram

Figure 3.4 shows the diagram of the Xecret Application Architecture. During the wiping process, two mobile phones are needed, the stolen phone acts as a Slave and the remote phone acts as a Master. All the wiping command requests and successful notification is received are via SMS.

### 3.5 Xecret Application Framework

Table 3.4: Xecret Application Framework

Phone 1 (Slave)	Phone 2 (Master)
Before the phone was stolen or lost	
Stage 1: Installation Process	
Step 1: Download & install Xecret application into the Slave mobile phone.	
Step 2: Complete all the configurations in the application. e.g.: Password setting, enter emergency contact and select important files into designated folder.	
After the phone have been stolen or lost	
Stage 2: Wiping Process	
	Step 3: Owner sends wiping command with password via SMS.
Step 4: Agent read all incoming SMS and compare with the configured wiping command in Step 2. If match is found, wiping process will be triggered in the background.	
Step 5: Secure deletion based on SMS command received from Master using (a) single-pass overwrite or (b) default factory reset.	
Stage 3: Notification Process	
Step 6: Agent will send an acknowledgement to Master phone after successful wiping (Only for secure deletion).	
	Step 7: Master phone receives wiping acknowledgement succeed from the Slave.

There are 3 stages in Xecret secure wiping application as shown in Table 3.2, which comprises of two steps in stage 1 (Installation Process), followed by three steps in stage 2 (Wiping Process) and finally 2 steps in stage 3 (Notification Process)

## 4 Analysis and Design

The analysis and design process for the development of the Xecret application is discussed in detail in this chapter. The application components and structure are discussed to produce better illustration on how the application works with the user. Unified Modeling Language (UML) is used to create illustrations between

users and the application and to explain the application workflow using case diagram, sequence diagram and flowchart. The flowchart is used to show the process user in the application step by step.

In addition, database design was also included in this chapter to show how the data stored in the application is managed. The design of the database is important for the proper management of the data without redundancy occur. Lastly, interface design for each page has been created to show the application environment to the user.

## 4.2.2 Application Requirement Analysis

The purpose of the analysis of application requirements is to obtain a detailed understanding of the application function. Application requirement analysis consists with two components which are functional requirement and non-functional requirement. These analyses intended to collect information about the task and action will be taken in the application.

### 4.1.1 Non-Functional Requirement Analysis

Table 4.1 shows the functional requirement of Xecret application. Functional requirement defined what was done by identifying the tasks or actions to be carried out.

Table 4.1: Functional Requirements of Xecret Application.

Page	Functionalities
Login	✓ Application allow user to login using passcode
Register	✓ Application allow new user to setup passcode
Setting	✓ Application allow user to configure all the information needed such as emergency contact, change passcode and choose whether user want to turn on or off features provided.

### 4.1.2 Non-Functional Requirement Analysis

Non-functional requirements describe how the application behavior in term of efficiency and performance. Non-functional requirement analysis is described in Table 4.3, the main requirements for non-functional requirement are performance, operational and security.



Table 4.2: Non-Functional Requirements of Xecret Application.

Requirements	Descriptions
Performance	<ul style="list-style-type: none"> <li>✓ The application should be able to be used at anytime</li> <li>✓ Use less storage and memory to minimize the battery consumption</li> </ul>
Operational	<ul style="list-style-type: none"> <li>✓ The application features can fully functional without any error and bug.</li> <li>✓ The application will be running at the background.</li> </ul>
Security	<ul style="list-style-type: none"> <li>✓ The application locked using passcode.</li> </ul>

## 4.2 Use Case Diagram

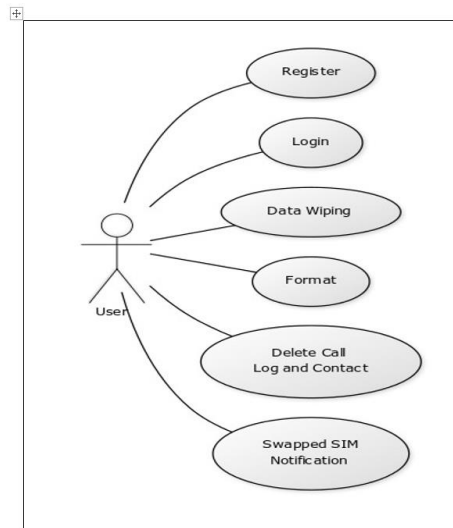


Figure 4.1: Use Case Diagram

Figure 4.1 displays the application case diagram for Xecret. First, users must register by entering passcode before the application can be used by the user. After register, user can login using passcode that user have entered during the registration. If the passcode is true, users can access the application's menu interface and used all the features provided.

#### 4.2.1 User Registration Sequence Diagram

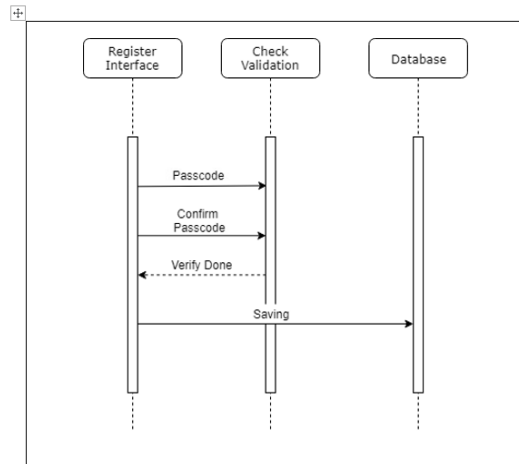


Figure 4.2: User Registration Sequence Diagram

Figure 4.2 shows the user registration sequence diagram. User needs to enter passcode twice in their first login information into the registration form. Then, the data will be collected and saved in database. After registration, user not require registering anymore because it only for one-time action.

#### 4.2.2 User Login Sequence Diagram

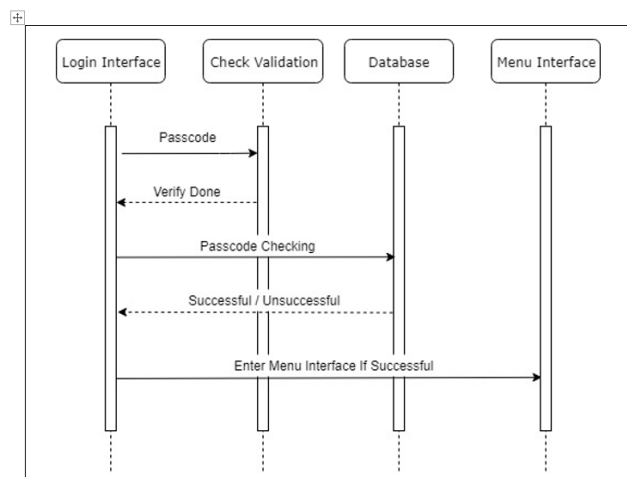


Figure 4.3: User Login Sequence Diagram

Figure 4.3 shows the user login sequence diagram. User require to enter passcode to login into the application. The passcode will be verified with the registered passcode that contain in database. If the passcode is true, then user will go to the menu interface where it will display all the function on the application.

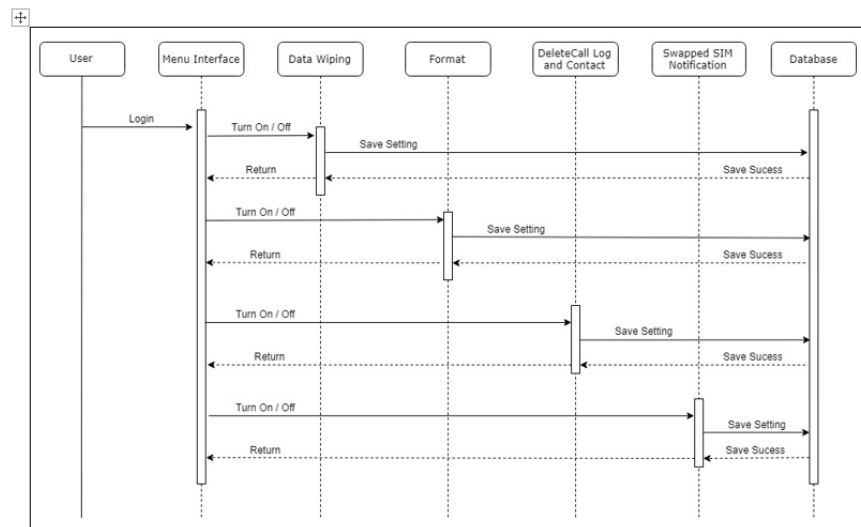


Figure 4.4: Features Sequence Diagram

Figure 4.5 shows the features sequence diagram. User can decide the four main functions which are data wiping, format, delete call log & contact and swapped SIM notification. User can choose whether to turn on or off the features provided. After finish choose the features, user need to save all the configuration by pressing the save button at the bottom of the screen. Then, all the configuration of setting will be stored in the database.

### 4.3 Database Design

Table 4.3: User Information Table

No	Attribute	Data Type	Description	Key
1	User_ID	Integer	Unique ID	PK
2	Passcode	Integer	Passcode for user login to the application	
3	User_number	Integer	Current phone number based on SIM card attached	

Table 4.3 shows the user information table that contain information about the user, the attribute for user information table are User\_ID, Passcode and User\_number. All the attributes are using integer data type and User\_ID act as primary key in this table.

Table 4.4: Setting Configuration Table

No	Attribute	Data Type	Description	Key
1	User_ID	Integer	Foreign key	FK
2	Xecret_wiping	Boolean	Configuration in setting whether turn on or off	
3	Xecret_format	Boolean	Configuration in setting whether turn on or off	
4	Xecret_call	Boolean	Configuration in setting whether turn on or off	
5	Xecret_swapsim	Boolean	Configuration in setting whether turn on or off	

Table 4.4 shows the setting configuration table that contain data of configuration in setting, the attribute for setting configuration table are User\_ID, Xecret\_wiping, Xecret\_format, Xecret\_call, and Xecret\_swapsim. All the attributes are using Boolean except User\_ID using integer data type and User\_ID act as primary key in this table.

Table 4.5: Emergency Contact Table

No	Attribute	Data Type	Description	Key
1	Row_ID	Integer	Unique ID	PK
2	Xecret_contact	Integer	Emergency contact for acknowledgement	

Table 4.4 shows the emergency contact table that contain information about the emergency contact lists, the attribute for emergency contact table are

Row\_ID, Passcode and Xecret\_contact. All the attributes are using integer data type and Row\_ID act as primary key in this table.

#### 4.4 SMS Command Structure

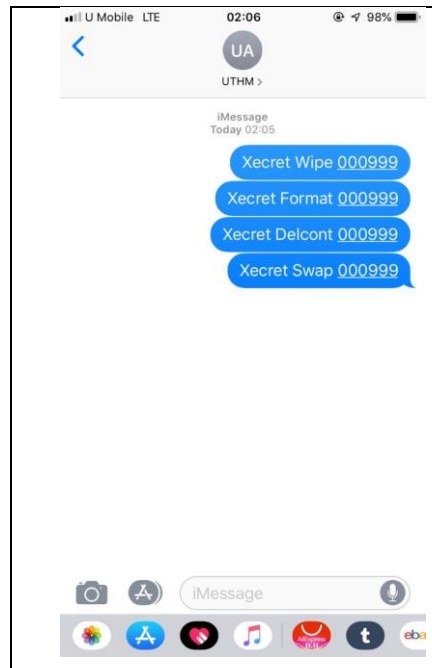


Figure 4.5: Default Command Via SMS

Figure 4.5 shows the sample default command that send by Initiator Phone via SMS. There are four default command which are for wiping, format, delete call log and swapped SIM notification. The structure of the command below: -

Xecret <space> “Action-Type” <space> passcode
---

Figure 4.6: Default Command Structure

Figure 4.6 shows the default command structure. The first word is “Xecret”, it indicates the Xecret application command format and followed by action-type. Action-type comprises of “Wipe” (Data Wiping), “Format” (Reset Factory), “DelCont” (Delete Call Log) and “Swap” (Swapped SIM Notification).

## References

- Yeh, R. T., & Tanik, M. M. (1989). "Rapid Prototyping in Software Development" in *Computer*, 1989, vol. 22, pp. 9-11.
- Jones, M., Li, Z., & Merrill, M. (1992). *Rapid prototyping in automated instructional design*. *Educational Technology*, 30(8), 42-47
- Pressman, R. (2010). *Software Engineering: A Practitioner's Approach*. Boston: McGraw Hill. pp. 41–42.
- Burd, B. (2015). *Android Application Development All-in-One For Dummies*. 2nd ed. New York, NY: John Wiley & Sons.
- Manson, D., Carlin, A., Ramos, S., Gyger, A., Kaufman, M., & Treichelt, J. (2007). Is the Open Way a Better Way? *Digital Forensics Using Open Source Tools*. Waikoloa: IEEE. pp 266b-266b.
- Olvecky, M., & Gabriska, D. (2018). Wiping Techniques and Anti-Forensics Methods. 2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY).