Design and Implementation of Improved Authentication System for Android Smartphone Users

—Anshita Agrawal

Contents

Introduction

- The devices used for IT services are changing from PCs and laptops to smartphones and tablets.
- Smartphones are characterized by low efficiency and low power .
- They need to be small for increased portability.
- They do not support the security software which require continuous monitoring to detect threats.
- As these devices start to contain increasing amounts of important personal information, better security is required.
- Security systems are rapidly being developed, however, even with these, major problems could result after a device is lost.
- Thus, strong authentication mechanisms are required to protect important personal information, even after the device is lost.

Security requirements

- Openness
  - A variety of external interfaces provides malicious code propagation paths and the code secreted by the developer to facilitate the creation of mobile applications leaves the internal interface vulnerable to malicious code.
- Portability
  - If you lose your smartphone, there can be outflows of personal and business information, such as internet banking information, internet search information, schedules, and business documents.
- Low Efficiency
  - Smartphones are characterized by low efficiency and low power . Thus, they do not support the security software which require continuous monitoring to detect and respond to security threats and malicious code.

Authentication schemes

- Slide Lock
- Glass Lock
- Keypad Lock
- Pattern Lock

Figure 1. Slide Lock

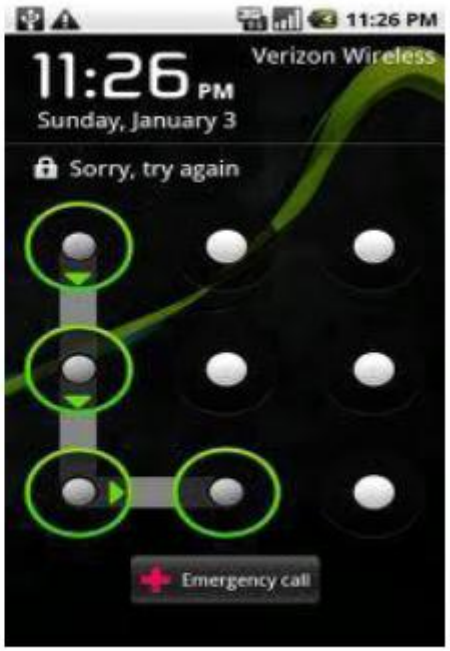


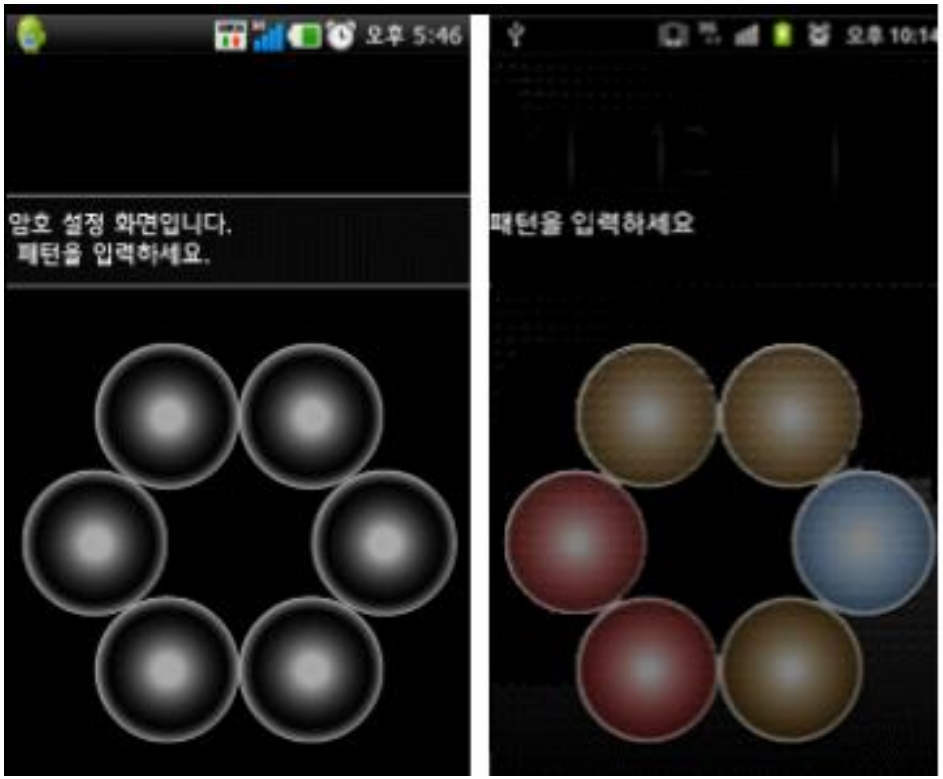
Figure 2. Pattern Lock

Improved Authentication System

- Current Lock Screens based on touch consist of “simple password-unlock” systems.
- We can input touch sensors, gravity sensors, and approach sensors, as in a “multiple password-unlock” system to restrict the phone’s function.
- Mode is divided into two parts
  - User mode
    - The User mode can be entered by entering the password. In this mode we can do everything with our mobile phone.
  - Guest mode
    - The Guest mode can be entered by using the acceleration sensor (shaking). In this mode we can only do the operations that are authorized by the User.

Lock Screen

- The upgraded Lock Screen system is shown here



Improved Authentication System (Contd.)

- Redundancy input (re-touching the circle) is allowed.
- When the circle is touched more than once, it changes colour (maximum of seven times) so that the user can identify the correct input.
- This Lock Screen system has about ten million (6^9 = 10077696) key spaces. It can also be made larger by increasing the number of repetitive touches.
- The security power depends upon the size of the key space; the bigger the key space, the more difficult is a brute force attack.
- To control the usage, besides entering the password, the acceleration sensor (shaking the mobile phone) can be used. Touching is not required.

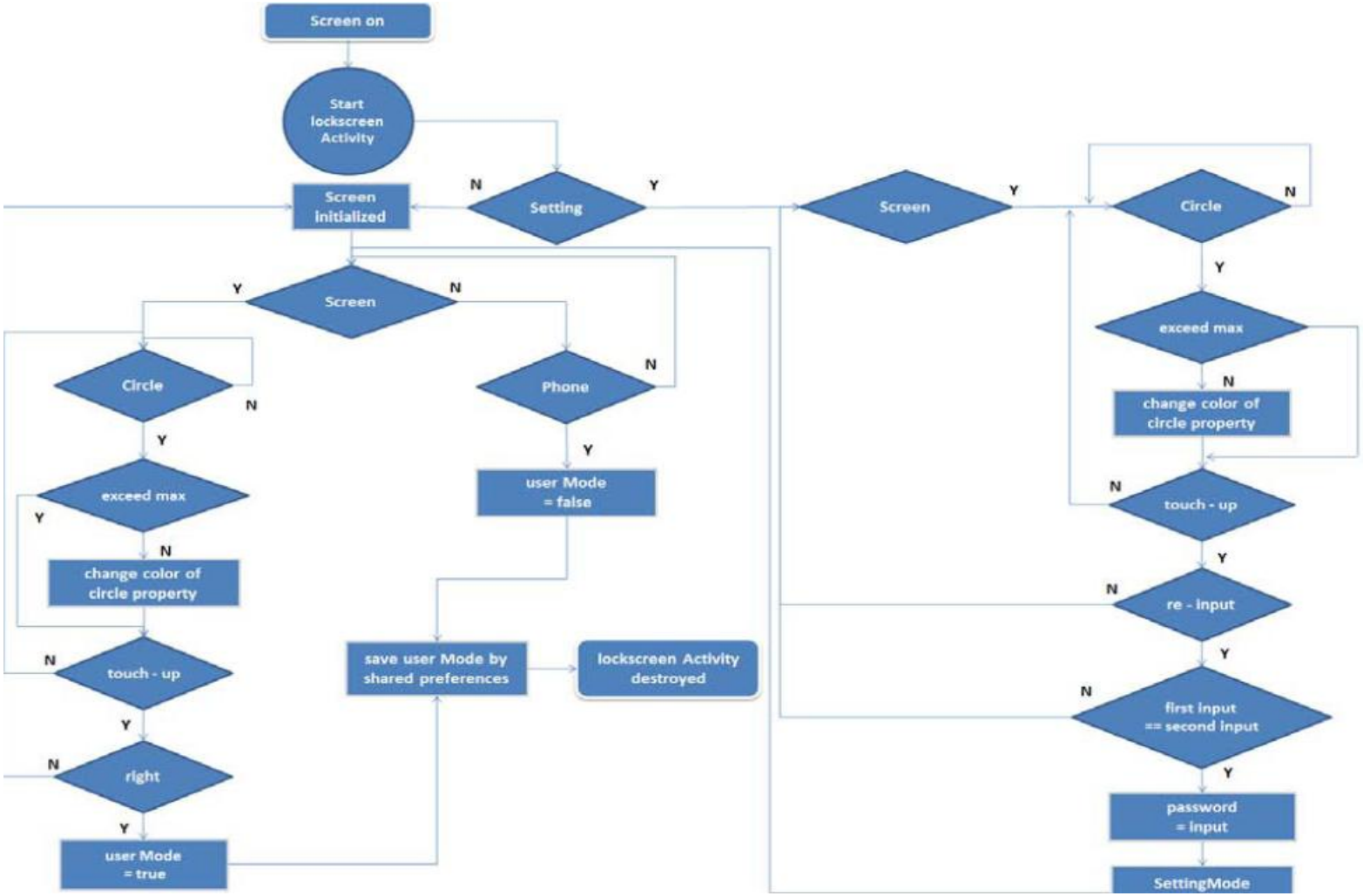
How it works

- The Lock Screen consists of activities, so it is included in the Home Launcher application package.
- The Screen receives the “On/Off Broadcast Receiver” so it is processed with Intent from Screen-On, activating the Lock Screen Activity.
- The Lock Screen Activity consists of Password settings and, to unlock the screen, a password must first be entered.
- After setting the password, two options are available: a user can either enter the password or shake the mobile phone.

How it works (Contd.)

- Binding the Home key is different in Guest mode than it is in User mode.
- If the Home key button is entered in the Lock Screen, the Guest mode is automatically entered and the user can only use a few allowable applications.
- The user can make widgets, icons, folders, and setting slides through various kinds of touches (touch, long-click, drag, home button, and menu button).
- If there are any changes or User/Guest processes, Home Launcher re-organizes the view.

How it works (Contd.)



Comparison with other systems

- Slide Lock: No security.
- Glass Lock: No security.
- Keypad Lock: Requires a four-digit password, so it provides key space of about 10,000 (0 to 9999). Brute force attack is easy.
- Pattern Lock: There are nine dots on the screen, each of which can be touched and dragged one dot at a time to make a password. It provides approximately one million (= 9P4 + 9P5 + 9P6 + 9P7 + 9P8 + 9!) of key space. Better than Keypad Lock but not very secure.
- Lock Screen: It has about ten million (6^9 = 10077696) key spaces with 9 inputs. It can also be made larger by increasing the number of repetitive touches. The bigger the key space, the more difficult is a brute force attack.

Conclusion

- Android is being installed in tablets and many other IT devices that require good security systems.
- By dividing the mode of entry, user's convenience and security have been improved.
- The use of this improved authentication system ensures protection of personal information.
- But this is not the ultimate solution. This can be improved further.

References

- Kwang Il Shin, J. S. (2012). Design and Implementation of Improved Authentication System for Android Smartphone Users. *26th International Conference on Advanced Information Networking and Applications Workshops.*

Thank You