**Security Threats to Mobile Multimedia Applications: Camera-Based Attacks on Mobile Phones**

**ABSTRACT:**

Today’s mobile smartphones are very power ful, and many smartphone applications use wireless multimedia communications. Mobile phone security has become an important aspect of security issues in wireless multimedia communications. As the most popular mobile operating system, Android security has been extensively studied by researchers. However, few works have studied mobile phone multimedia security. In this article, we focus on security issues related to mobile phone cameras. Specifically, we discover several new attacks that are based on the use of phone cameras. We implement the attacks on real phones, and demonstrate the feasibility and effectiveness of the attacks. Furthermore, we propose a lightweight defense scheme that can effectively detect these attacks.

**EXISTING SYSTEM:**

Several video-based attacks targeted at keystrokes have been proposed. The attacks can obtain user input on touch screen smartphones. Maggi et al. [4] implement an automatic shoulder surfing attack against modern touch-enabled smartphones. The attacker deploys a video camera that can record the target screen while the victim is entering text. Then user input can be reconstructed solely based on the keystroke feedback displayed on the screen. However, this attack requires an additional camera device, and issues like how to place the camera near the victim without catching an alert must be considered carefully.

**DISADVANTAGES OF EXISTING SYSTEM:**

Moreover, it works only when visual feedback such as magnified keys are available.

**PROPOSED SYSTEM:**

In this article, we first conduct a survey on the threats and benefits of spy cameras. Then we present the basic attack model and two camera-based attacks: the remote-controlled real-time monitoring attack and the passcode inference attack. We run these attacks along with popular antivirus software to test their stealthiness, and conduct experiments to evaluate both types of attacks. The results demonstrate the feasibility and effectiveness of these attacks. Finally, we propose a lightweight defense scheme.In this work, we are able to hide the whole camera app in Android. Moreover, we implement advanced forms of attacks such as remote-controlled and real-time monitoring attacks. We also utilize computer vision techniques to analyze recorded videos and infer passcodes from users’ eye movements.

**ADVANTAGES OF PROPOSED SYSTEM:**

The main challenge is to make the attacks run stealthily and silently so that they do not cause a user alert.

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System : Pentium IV 2.4 GHz.
* Hard Disk : 40 GB.
* Floppy Drive : 1.44 Mb.
* Monitor : 15 VGA Colour.
* Mouse : Logitech.
* Ram : 512 Mb.
* MOBILE : ANDROID

**SOFTWARE REQUIREMENTS:**

* Operating system : Windows XP/7.
* Coding Language : Java 1.7
* Tool Kit : Android 2.3 ABOVE
* IDE : Eclipse

**REFERENCE:**

Longfei Wu and Xiaojiang Du, Temple University Xinwen Fu, University of Massachusetts Lowell, “Security Threats to Mobile Multimedia Applications: Camera-Based Attacks on Mobile Phones**,**” **IEEE Communications Magazine, March 2014**