**Summary**

“Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices” is a survey paper that seeks to provide an overview of the current state of mobile security from the back end telecommunications networks to the user level mobile applications such as the web browser. The authors see mobile security as an integral part of the IT security as the transition from dumb phones to smart phones takes place.

The definition of a mobile service and mobile phone have changed within the past 10 years. Mobile security is now a discipline of itself which originally branched off from computer security. Mobile devices have four general attack vector classes and models: hardware, device independent services, software centric, and use layer. The hardware layer involves the ability to eavesdrop on the user such as interception communications as well as attacking the device from a forensic aspect which requires physical possession at some point in time. Device independent security focuses on the communication between a mobile phone and a cellular base station and involves protocols such as GSM vs UTMS and SMS vs. MMS. One major concern is base station impersonation using IMSI catcher devices. The software centric security aspect involves financially motivated attacks that revolve around identify theft. Unknown bad actors may attempt to collect information on a user in order to use such information for unlawful purposes later on. A bad actor may also attempt to record phone conversations without the permission of the lawful user through abuse of privilege levels. The user remains a viable attack vector because the system has to balance security with usability. User attack vectors are not necessarily limited to the average user, but user attack vectors also include targets such as system administrators. Their access level could cause irreparable harm to a system.

This survey paper does a comprehensive job of outlining possible areas for mobile security improvement. The authors highlight security concerns from multiple levels and demonstrate while mobile security may be in its infancy, we are beginning an era in which attacks against smart phones will become more prominent.

This survey paper could be improved by providing equal focus on the motivations of attacks as well as attack vectors. For example, financially motivated attacks may be interested in certain attack models whereas non-financially motivated attacks may be interested in another set of attack models and targets. Being able to group types and motivations of attacks could help define who must collaborate for a mutual interest in improving mobile security.

**Suggestions**

Improvements could be made by grouping the attack vectors more similarly. For example, this survey paper is broken up by four attack vector classes: hardware, device independent services, software centric, and use layer. The eavesdropping attack model appears in at least three of the four above. The overall deficiency is that by separating out security into attack vector classes, one is answering the question, “What should we protect?” rather than “How should we protect against a malicious objective?” If we approached mobile security from the motivations and objectives of our attackers instead of the multi layered approach of our infrastructure, devices, and applications, we’ll be able to build a more targeted and multi-layered defense against eavesdropping. We’ll also be able to predict the level and extent of collaboration among mobile carriers, phone manufacturers, operating system/ecosystem developers, and application developers.

**Future Research**

Future research should go into researching malware designed to eavesdrop on someone’s SMS/MMS communications. There are a plethora of applications, especially on the Android platform, designed relay SMS/MMS to a web interface such as MightyText. There are even applications at the carrier level such as Verizon Messages+ that allow a user to send an SMS via a web interface to an external phone number without even using a mobile phone as a relay as in MightyText. This area of cell phone security is important because many online services that contain Privately Identifiable Information now use multi factor authentication where you are sent a code via SMS for secondary authentication.

I expect constant and consistent research into mobile network communication protocols such as GMS, UMTS, CDMA, and LTE (various versions) to occur primarily at the carrier and academic level. Improvements should be made to base tower authentication and encryption to prevent non-financially motivated actors such as state actors from eavesdropping on wireless communications.

I would like to see additional research and collaboration among government agencies, particularly law enforcement, and operating system developers to determine the best way to protect the privacy of United States citizens while adhering to the legal process in which an authorized agency can be granted access on a subject’s mobile device.