Evaluating compromising emanations in touchscreens

_Utvärdering av röjande signaler från touchskärmar_

Joakim Lidstedt

Supervisor: Niklas Johansson
Examiner: Jan-Åke Larsson

External supervisor: Jonathan Jogenfors
Upphovsrätt


Copyright

The publishers will keep this document online on the Internet – or its possible replacement – for a period of 25 years starting from the date of publication barring exceptional circumstances. The online availability of the document implies permanent permission for anyone to read, to download, or to print out single copies for his/hers own use and to use it unchanged for non-commercial research and educational purpose. Subsequent transfers of copyright cannot revoke this permission. All other uses of the document are conditional upon the consent of the copyright owner. The publisher has taken technical and administrative measures to assure authenticity, security and accessibility. According to intellectual property law the author has the right to be mentioned when his/her work is accessed as described above and to be protected against infringement. For additional information about the Linköping University Electronic Press and its procedures for publication and for assurance of document integrity, please refer to its www home page: http://www.ep.liu.se/.

© Joakim Lidstedt
Abstract

In a short time touchscreens has become one of the most used methods for input to smartphones and other machines such as cash registers, card terminals and ATMs. While the technology change was quick it introduces the possibility of new security holes. Compromising emanations is a possible security hole in almost all electronic equipment. These emanations can be used in a side-channel attack if they leak information that compromise the security of the device. This thesis studies a single-board computer (SBC) with a touchscreen and a smartphone in order to evaluate if any usable information leaks regarding what is done on the touchscreen i.e. where on the screen a user touches. It is shown that the location of a touch can be read out from information leaking through the power cable and wirelessly from the single-board computer. It is also shown that basic information can be read out wirelessly from the smartphone but further testing is required to evaluate the possibility to extract usable information from the device.
Acknowledgments

First, I would like to thank all the people at Sectra for their support and making this thesis a possibility by providing all the equipment needed. I would also like to give a special thanks to Mattias Fransson and Jonathan Jogenfors for both their technical support and feedback on the report.

Secondly, a big thanks to my examiner Jan-Åke Larsson and my supervisor Niklas Johansson for their feedback and advice when writing the report.

Finally, I would like to thank my family for pushing me forward when I got stuck and supporting me throughout the entire project.
# Contents

Abstract iii
Acknowledgments iv
Contents v
List of Figures vii
List of Tables ix

1 Introduction 1
   1.1 Motivation .................................................. 1
   1.2 Sectra AB ................................................... 1
   1.3 Purpose ..................................................... 2
   1.4 Research Questions ............................................ 2
   1.5 Delimitations ................................................ 2

2 Theory 3
   2.1 Compromising emanations ....................................... 3
      2.1.1 The physics behind compromising emanations .......... 3
      2.1.2 Conducted emanations .................................. 4
      2.1.3 Radiated emanations .................................. 4
      2.1.4 Shielded equipment ..................................... 4
   2.2 Touchscreen technology ........................................ 4
      2.2.1 Capacitive touchscreens ................................ 4
   2.3 Inter-Integrated Circuit ........................................ 5
   2.4 Signal processing ............................................ 5
      2.4.1 Cross-correlation ....................................... 5
      2.4.2 Normalized cross-correlation ............................. 6
      2.4.3 Cross-covariance ....................................... 6
      2.4.4 Normalized cross-covariance ............................. 6
      2.4.5 Application to compromising emanations ................. 6

3 Method 8
   3.1 Environment Setup ........................................... 8
      3.1.1 Oscilloscope ............................................. 9
      3.1.2 Spectrum analyzer ....................................... 9
      3.1.3 Linear amplifier ........................................ 9
      3.1.4 Absorbing clamp ........................................ 9
      3.1.5 Near-field probe ......................................... 9
      3.1.6 AUTO-ROS Software ...................................... 9
   3.2 Simulating touch ............................................ 10
   3.3 Targets .................................................... 11
List of Figures

3.1 Environment setup used to measure compromising emanations. The tools in the picture are (from left to right) A spectrum analyzer, an oscilloscope, a linear amplifier and a power supply. The gray box in the front left is an absorbing clamp and the small box in the front right is an optical receiver. .......................... 8

3.2 AUTO-ROS graphical user interface. ...................................................... 10

3.3 Paperclip attached to screen used to simulate touch. The cable is connected on the back of the device to ground it. ................................................................. 11

3.4 Connection between the single-board computer, touchscreen and oscilloscope. ... 12

4.1 Normalised cross-covariance measuring between the I²C reference signal and an average based on several conducted emanations emitted by the power supply cable in the SCB. Each color represents one kind of compromising emanations. The white graph contains three points of interest, depicted as the three white spikes all with a value higher than 0.4. By manually inspecting each point it was concluded that the highest spike with a value of 0.52 found at 138.9 MHz contained the clearest compromising emanations. ...................................................... 17

4.2 Graph depicting the single-board computers I²C reference signal in yellow and an average based on several conducted emanations at 138.09 MHz in green. Studying the signals a relation marked 1 can be seen as a wide block in the reference signal and three green spikes in the measured signal. A similar relation can be seen marked 4 and a weaker relation can be seen between the thin blocks and the spikes marked 2 and 3 ................................................................. 18

4.3 Normalised cross-covariance measuring between the I²C reference signal and an average of several radiated emanations emitted by the SCB. The graph contains two points of interest, depicted as the two white spikes. By manually inspecting each point it was concluded that the highest spike with a value of 0.68 found at 225.0 MHz contained the clearest compromising emanations. .......................... 19

4.4 Graph depicting the single-board computers I²C reference signal in yellow and an average of several radiated emanations at 225.0 MHz in green. Studying the signals a inverted relation, marked 1, can be seen as a wide block in the reference signal and a gap in the measured signal. A similar inverted relation can be seen marked 3 and a weaker inverted relation can be seen between the thin blocks and the gaps marked 2. ................................................................. 20

4.5 Normalised cross-covariance measuring between the I²C reference signal and an average of several radiated emanations emitted by the smartphone. The white graph contains several points of interest, all with a value higher than 0.4. By manually inspecting each point it was concluded that the highest spike with a value of 0.47 found at 211.7 MHz contained the clearest compromising emanations. 20
Graph depicting the smartphones I²C reference signal in yellow and an average of several radiated emanations at 211.7 MHz in green. Studying the signals a clear inverted relation can be seen at 25 $\mu$s between the two blocks in the reference signal at and the gaps in the measured signal. A similar inverted relation can be seen with the repeated thin gaps in the measured signal and the corresponding thin blocks in the reference signal, these thin blocks in the reference signal correspond to the ACK bits used by I²C.
List of Tables

4.1 Second read packet between the single-board computer and touchscreen containing the coordinate data for one touchpoint. ........................................... 15
4.2 Min and max values achieved by tracing the edge of the touchscreen connected to the SCB. ................................................................. 15
4.3 Second read packet between the smartphone and touchscreen containing the data describing number of touchpoints active on the touchscreen. ......................... 16
4.4 Third read packet between the smartphone and touchscreen containing the coordinate data for all active touchpoints. .............................. 16
4.5 Min and max values achieved by tracing the edge of the touchscreen of the smartphone. .............................................................. 16
Chapter 1
Introduction

This introductory chapter aims to motivate and explain why the research questions defined are necessary and relevant. It also explains the overall goal of the research questions and defines delimitations for what is not a part of this thesis.

1.1 Motivation

Since the beginning of personal computing the combination of keyboard and mouse have been the dominating way of using a computer. But, while they remain dominant for desktop computers, the desktop computer is losing ground to smartphones when it comes to actual usage.

With the shift from desktop computers to smartphones comes a shift from the traditional keyboard and mouse to touchscreens for input. A similar shift to touchscreens can be seen in other machines such as cash registers, card terminals and ATMs which all previously used mechanical keyboards.

The way input is provided on a touchscreen is often done by a virtual keyboard and dropdown menus very similar to those used with a traditional keyboard and mouse. For the end user this change is rather indiscernible but from a technological standpoint the change is huge. This technology change introduces the possibility of new security holes. One possible security hole existing in almost all electronic equipment is compromising emanations. Compromising emanations is the unintended leakage of information through emanations of many different kinds, such as optical, thermal, acoustic and radio waves [1].

When techniques incorporating these emanations are used to attack equipment they are often referred to as side-channel attacks. On equipment such as keyboards these attacks are well documented [2, 3], but when it comes to touchscreens the research is scarce. This lack of research poses a security risk for touchscreen usage.

The purpose of an attack using compromising emanations is to obtain information. Depending on the system targeted the information can differ in many ways. For example, Kuhn [4] extract the image of LCD TV sets while Vuagnoux et al. [2] obtain the keystrokes from keyboards. A touchscreen acts as both a visual output and a virtual keyboard input meaning the possible risks are twofold.

Today smartphones are used for everything from emailing to banking. If an attack using compromising emanations was implemented that made it possible to obtain the information describing where on the screen a user touches the possible danger could be enormous. For example it could enable an attacker to obtain information such as your pin code, passwords, bank details and anything else you would enter in to your phone by using the touchscreen.

1.2 Sectra AB

Sectra is an international company with subsidiaries in 15 countries. It was founded in the late 1970s when it carried out its first assignment, developing a security solution for the
banking industry. Today Sectra focus their development on three areas: medical systems, secure communication and critical infrastructure.

In secure communication products are held to a very high standard to ensure all requirements are met. This is done by researching components and thorough testing during development, including measuring compromising emanations. As a part of this research, this thesis aims to provide an initial evaluation of compromising emanations from touchscreens.

1.3 Purpose

The purpose of this thesis is to evaluate the security of touchscreens in regard to compromising emanations. In this thesis two touchscreen devices, a single-board computer (SBC) and a smartphone, are evaluated. The evaluation is done by measuring conducted and radiated emanations emitted from the devices.

1.4 Research Questions

- Can conducted compromising emanations from a capacitive touchscreen be detected?
- Can radiated compromising emanations from a capacitive touchscreen be detected?

1.5 Delimitations

The thesis only covers capacitive touchscreens, specifically a touchscreen designed to be used as an addon for single-board computers and a smartphone. Other touchscreen technologies such as resistive, infrared, and optical are not covered.

By request of the vendor the make and model of the smartphone used has been masked. Therefore, throughout the thesis the devices tested will be referred to as the single-board computer (SCB) and the smartphone.

When performing measurements the calculations are based on the average of several samples. As a security precaution the amount of samples used for averaging is kept secret.

There are several signals and calculations between touching the screen and the information reaching its final destination in the central processor. Each one of these steps may have the potential to leak information but this thesis only covers compromising emanations from the signal sent between the touchscreen microcontroller and the central processor.
Chapter 2
Theory

This chapter aims to provide a basic technical understanding of the devices targeted in this thesis, including the relevant parts inside them and the communication protocol used between the different parts.

2.1 Compromising emanations

All electronic equipment emit stray electromagnetic signals while they are turned on. This leakage of electromagnetic signals is amplified by the ever increasing clock frequencies seen in processors. A lot of the times this signal only contains random noise but it is possible for the signal to pick up and transport information from the device, when this happens the signal is referred to as a compromising emanation [1].

The signal leaking information can produce two kinds of compromising emanations. The first version carries the signal in full. The second version only contains information of when the signal value changes from high to low or vice versa, this is known as flank emanations. Flank emanations can be further divided based on if the signal goes from low to high, positive flank, or high to low, negative flank [5].

Regardless of the information contained, the emanations can then be divided into two categories: conducted and radiated.

2.1.1 The physics behind compromising emanations

One of the most fundamental concepts in electromagnetism is that “magnetic fields are produced both by conduction currents and by time-varying electric fields.” [6] In practice this means that all electronic systems generates a magnetic field while they are turned on.

As the state of an electronic system is based on the flow and control of the electrons within it, the magnetic field changes depending on the state of the electronic system. This means that the magnetic field can be observed in order to obtain information about the system. As information is obtainable in an unintended way the magnetic field can be seen as a basic form of compromising emanations.

Another fundamental concept in electromagnetism is that “whenever a charged particle accelerates, it radiates energy.” [6] In practice this means that all wires carrying currents that change with time generate electromagnetic radiation.

Similar to the magnetic field, the electromagnetic radiation depends on changes between different states in the electronic system. As these changes happen the information they carry can be obtained through the radiation. Unless the radiation is wanted the information it leaks out is a radiated compromising emanation.

A system designed to radiate electromagnetic signals most often use an antenna specifically designed to amplify the wanted signal. In its most basic form an antenna can be viewed as a wire with a length and shape selected for optimal performance within a specific frequency.

When it comes to compromising emanations it is possible for a wire or circuit in the electronic system to unwillingly act as antenna for the current it carries. This is caused by an
unplanned match between the frequency of the current and the length of a wire or circuit in the system. For example, the cable between a keyboard and computer or the ground plane on a circuit board may become an antenna as it carries a current. These unplanned antennas amplify the signal which increases the risk of compromising emanations being strong enough to leak out far enough for them to be detected outside the system.

2.1.2 Conducted emanations

Conducted emanations, as the name implies, require a conductor to carry it. A common place for these to occur is in power supply cables but it is also possible for signal cables to leak information other than the intended signal [1].

A good example of leakage through the signal cable is the British espionage on the French Embassy in London, by tapping into the cable carrying the encrypted signal from the embassy they found traces of another signal. This second signal contained the plaintext version of the encrypted signal [1].

2.1.3 Radiated emanations

If the leaked signal is modulated with a frequency that resonate with the cable length or other components in the equipment then the signal may radiate. If powerful enough, the radiated emanations can then be picked up wirelessly by an antenna [1].

It has been shown, several times, that displays often have this weakness [4, 8]. However, the problem is not exclusive to displays, other equipment such as keyboards [2], cables [9] and voting machines [10] may also be vulnerable to information leakage via radiated emanations.

2.1.4 Shielded equipment

Shielded equipment specifically designed to prevent compromising emanations exist, Van Eck [8] gives a few examples of techniques that can be used to prevent emanations such as constructing a metal shield around the equipment etc.

The price for approved shielded equipment is often a lot higher than off-the-shelf solutions, making it unfeasible for general usage [1].

2.2 Touchscreen technology

There are several different kinds of touchscreens each using different physical properties such as electric (resistive and capacitive), optical and acoustic to register touch events. The way of registering a touch may be different between the technologies but the overall purpose of a touchscreen is the same; to provide location based input to a system in a fashion similar to that of a mouse. The different technologies each have their own pros and cons.

2.2.1 Capacitive touchscreens

Among the different technologies the most common (at least for smaller screens such as smartphones and tablets) is capacitive touchscreens. Capacitive touchscreens work by detecting changes in capacitance on the screen. This is done by touching the screen with a electrical conductor capable of holding a big enough charge for the screen to detect, such as the human body.

In its most basic form capacitive touchscreens are built using a design called surface capacitance. A surface capacitance screen works by having one side of an insulator coated with a conductive material. By touching the uncoated side of the insulator with an electrical conductor, such as a finger or stylus, a capacitor is created. By measuring the capacitance in each corner of the screen the position of the touch can be calculated.
Another technique used in capacitive touchscreens is projected capacitance. Unlike surface capacitance the projected technique using mutual capacitance enables multi-touch, allowing the user to use several fingers or styluses at the same time which in turn enables smart gestures such as pinching for zoom etc.

Projected capacitance come in two versions, mutual- and self-capacitance. Both versions use a grid of conductive material layered on a sheet of glass.

For mutual capacitance this grid of rows and columns then act as a capacitor in each intersecting point. By touching the screen the electrostatic field is manipulated and this change is measured in each intersection allowing an algorithm to accurately pinpoint where the touch occurred.

The self-capacitance version of projected capacitance use the same grid of rows and columns but instead of measuring in each intersecting point the measurement is done on each row and column individually. This technique however does not allow multi-touch as the design has no way of grouping the rows and columns together when a touch occurs at two points at the same time.

### 2.3 Inter-Integrated Circuit

Inter-Integrated Circuit (I\textsuperscript{2}C) is a serial data bus for communication between integrated circuits. It is commonly used to connect microcontrollers and processors, two good examples are the single-board computer and smartphone used in this thesis as both use I\textsuperscript{2}C for communication between the processor and the touchscreen microcontroller.

The I\textsuperscript{2}C data bus use two roles to differentiate between the nodes on the bus: master and slave. It also supports multiple masters on the same bus using arbitration to ensure only one master controls the bus at a time. Communication is always initiated by a master node by generating the clock signal and sending a START signal followed by the address of the slave it wants to communicate with. The initial start and address are accompanied by a single bit used to indicate read/write. After this initial byte and every following byte the receiver responds with an ACK bit to acknowledge that it has received the byte. Communication is then terminated by the master sending a STOP signal [11].

### 2.4 Signal processing

Signal processing is the area of mathematics dedicated to analysis and modification of signals. Signals meaning everything between analog sound to digital data generated by a computer. This section only covers basics related to compromising emanations.

#### 2.4.1 Cross-correlation

Calculating the correlation between two signals measures their similarity. By stepwise shifting one of the signals it is possible to calculate the cross-correlation of the signals. Given two discrete-time signals \( x[n] \), \( y[n] \) and a shifting parameter \( l \), the cross-correlation [12] of \( x[n] \) and \( y[n] \) is calculated by:

\[
r_{xy}(l) = \sum_{n=-\infty}^{\infty} x(n) y(n-l) \quad l = 0, \pm 1, \pm 2, \ldots
\]

Inserting the special case \( y[n] = x[n] \) in equation 2.1 gives the autocorrelation of \( x[n] \). From the autocorrelation several important properties can be noted. In particular, \( r_{xx}(0) = E_x \) which is the energy of \( x[n] \) [12].
2.4. Signal processing

2.4.2 Normalized cross-correlation

When plotting cross-correlation the scale of the resulting graph is based on the amplitude of the ingoing signals. However, changing the scale of the cross-correlation does not alter its shape. Therefore, it is wise to normalize [12] the cross-correlation to the range -1 to 1 using the following equation:

\[
\rho_{xy}(l) = \frac{r_{xy}(l)}{\sqrt{r_{xx}(0)r_{yy}(0)}}
\] (2.2)

Using normalized cross-correlation makes it easier to understand the values as a value of 1 means perfect correlation between \(x\) and \(y\) and a value of -1 means perfect anti-correlation between \(x\) and \(y\) [5].

2.4.3 Cross-covariance

Calculating the covariance between two signals measures their joint variability. Similar to correlation, covariance is a way of measuring the association between two signals [13].

Calculating the covariance between two signals with a stepwise shift is known as the cross-covariance of the signals. This is done using the following equation, where \(\bar{x}\) and \(\bar{y}\) are the mean values of \(x[n]\) and \(y[n]\) respectively:

\[
c_{xy}(l) = \sum_{n=-\infty}^{\infty} (x(n) - \bar{x})(y(n-l) - \bar{y}) \quad l = 0, \pm 1, \pm 2, \ldots
\] (2.3)

The special case \(y[n] = x[n]\) in equation 2.3 is called auto-covariance. Similar to autocorrelation, calculating autocovariance with zero shift gives \(c_{xx}(0) = \sigma_x^2\) where \(\sigma_x^2\) is the variance of \(x\) [12].

2.4.4 Normalized cross-covariance

Without normalisation the values calculated by cross-covariance are not directly relatable to anything other than their relative size. By normalising the cross-covariance to the range -1 to 1 it is possible to give meaning to the values, similar to cross-correlation, a value of 1 indicates a completely linear relation between \(x\) and \(y\) while a value of -1 indicates a inverted completely linear relation between \(x\) and \(y\). Calculating normalized cross-covariance is done using the following equation:

\[
\gamma_{xy}(l) = \frac{c_{xy}(l)}{\sqrt{c_{xx}(0)c_{yy}(0)}}
\] (2.4)

Equation 2.2 and 2.4 are very similar and both provide a way of calculating the similarity of two signals. Using these equations it is possible to evaluate compromising emanations in a system [5].

2.4.5 Application to compromising emanations

By using either cross-correlation or cross-covariance it is possible to compare a signal with known information, called the reference signal, and a signal suspected to contain compromising emanations, called the measured signal. While the value calculated does not prove the existence of compromising emanations, a high absolute value indicates a higher probability that compromising emanations exist. Using normalised values it is possible to compare several measurements in order to establish a limit where all results above the limit are more likely to contain compromising emanations. However, the value does not give a direct mapping to the probability that compromising emanations exist i.e. a value of \(X\) does not guarantee that compromising emanations exist with probability \(P\) [5].
As the reference signal and measured signal are captured over a finite time span they need to be extended before calculating the cross-correlation or cross-covariance. One common way of extending a signal is with zero-padding, meaning the signal is assumed to have a value of 0 outside the recorded time span. Using this form of padding when calculating the cross-correlation of the signals creates a triangular shaped graph as the most nonzero multiplications occur when the shifting parameter \( l = 0 \). One way of avoiding the triangular shape is using another form of padding such as symmetric- or periodic-padding but this introduces issues with discontinuities at the point of repetition. However, when calculating cross-covariance the triangular shape is removed through the subtraction of the mean values \( \bar{x} \) and \( \bar{y} \).

The AUTO-RÖS software described in subsection 3.1.6 was developed as a part of the research done by Ekman [5]. It is a tool using normalised cross-covariance to scan for compromising emanations across a span of frequencies automatically. By storing the largest value for each frequency a graph is created, showing the probability of compromising emanations for each given frequency.
Chapter 3
Method

The practical part of this thesis have been divided into separate parts based on the device being tested. The devices being tested consist of a single-board computer with a 7 inch capacitive touchscreen display and a smartphone. The overall environment setup is the same regardless of device but some connections are modified in order to accommodate the difference between the devices.

3.1 Environment Setup

The environment used for measuring consist of an oscilloscope, a spectrum analyzer, an amplifier, a PC and either an absorbing clamp for conducted emanations or a near-field probe for radiated emanations. A picture of all the equipment aside from the computer can be seen in figure 3.1. The measurements are run from the computer using a software called AUTO-RÖS.

The hardware setup along with AUTO-RÖS was available at Sectra prior to the testing required for this thesis. Therefore, no deeper evaluation of the viability of the setup was done. As such, no alternative equipment was tested as a part of this thesis.

Figure 3.1: Environment setup used to measure compromising emanations. The tools in the picture are (from left to right) A spectrum analyzer, an oscilloscope, a linear amplifier and a power supply. The gray box in the front left is an absorbing clamp and the small box in the front right is an optical reciever.
3.1. Environment Setup

3.1.1 Oscilloscope

The oscilloscope used is a DSO-X3024A from Agilent Technologies. It has a sample rate of 4 GSa/s and support for analysis of serial protocols such as I²C etc.

In this study the oscilloscope was used for two tasks, mapping out the packet format used by the devices and using its trigger function to provide a reference signal to the AUTO-RÖS software. The trigger signal is also fed through to the spectrum analyzer allowing both devices to capture the same timeframe.

3.1.2 Spectrum analyzer

The spectrum analyzer used is a FSV from Rohde & Schwarz and supports frequencies between 10 Hz and 13.6 GHz. It is provided with an external trigger signal from the oscilloscope and is remotely controlled by the computer running AUTO-RÖS. The spectrum analyzer is used to measure the compromising emanations using either the absorbing clamp or the near-field probe.

3.1.3 Linear amplifier

Between the spectrum analyzer and the absorbing clamp/near-field probe a AM-1431 linear amplifier from Miteq is connected. It has a gain of 41 dB for signal frequencies between 1 kHz and 1 GHz and is used to amplify the signal before passing it to the spectrum analyzer.

3.1.4 Absorbing clamp

In order to measure conducted emanations an absorbing clamp is placed around the power supply cable for the system. The clamp is an MDS 21 from Schwarzbeck based on the original design by Stadelhofen [14]. The clamp consists of a row of ferrite rings, each ring is split in half allowing the clamp to be opened and the cable inserted. The row of ferrite rings absorb interference from the cable and the first rings in the row works as an RF-current transformer connected to the spectrum analyzer.

3.1.5 Near-field probe

The near-field probe is used for measuring radiated emanations from the device. The probe is in the shape of a loop antenna designed to pick up emitted magnetic fields.

3.1.6 AUTO-RÖS Software

AUTO-RÖS is a Swedish abbreviation for automatic compromising emanations which also describes the softwares general purpose. The AUTO-RÖS software running on the computer is connected to both the oscilloscope and the spectrum analyzer. The software enables remote control of both tools using a simple graphical interface shown in figure 3.2.

The leftmost column in figure 3.2 provides settings for the spectrum analyzer. The settings available are:

- **Frequency span (Hz)** - The min and max center frequencies for the measurements.
- **Resolution bandwidth (Hz)** - The bandwidth used for each measurement.
- **Stepsize (Hz)** - The distance between each measurement.

The software can be set up for measuring several different bandwidths with different stepsizes at the same time, it will then run the measurements for each bandwidth in sequence.

The second left column in figure 3.2 is used for fine tuning the settings for the oscilloscope. The trigger point used need to be set up on the oscilloscope manually, the software settings available are:
3.2 Simulating touch

The time it takes to run a measurement with the AUTO-RÖS software depends heavily on the frequency span and stepsize used. An average measurement takes around ten minutes but for very large and detailed measurements the time quickly grows to several hours sometimes requiring the measurement to be run overnight. Regardless of the timespan it is very important that the device being tested is not altered in any way during the measurement. In order to ensure the touchpoint on the screen is completely static human input could not be used.

Instead of using a person required to stay completely still, touch was simulated using the electrical properties of the screen explained in 2.2.1. As mentioned, the screen requires an electrical conductor capable of holding a charge in order to indicate touch. By placing a metal
object on the screen and connecting it to ground it is capable of drawing away enough charge for the screen to indicate a touch at the metal objects position. The metal object can then be firmly attached to the screen using tape in order to ensure it will stay completely still during the measurement. For the measurements performed in this thesis a paperclip made of copper was attached to the screen as shown in figure 3.3. The paperclip wire was then connected to ground on the back of the device.

3.3 Targets

Two devices were selected and used for the tests and measurements in this thesis. The reason for choosing these two are simple. The single-board computer is a very open and cheap system with easy access to pinouts for the different signals. This made it simple to connect it to the oscilloscope for testing.

The smartphone was selected as a representative for smartphones in general based on being a few generations old flagship model from a well known producer. A smartphone in general was also chosen as it is among the most common applications for touchscreens.

3.3.1 Single-board computer (SCB)

The single-board computer was attached to a 7 inch capacitive touchscreen using a ribbon cable, visible on the right in figure 3.4. The ribbon cable carried the signal containing both the visual display data and the touchpoint data. However, the I²C data bus was also accessible from a separate pinout on the controller card attached to the touchscreen. This pinout was used to attach the oscilloscope to the SCB allowing for easy monitoring of the I²C data without any major modification needed.

The reference signal between oscilloscope and SCB was transmitted using an optical connection. The transmitting diode was soldered on to the SCB shown in the bottom of figure 3.4. Using an optical connection for the reference signal is done to avoid the risk of creating a source for compromising emanations.

3.3.2 Smartphone

The smartphone is a very closed system compared to the SCB. In order to access the relevant signals the phone had to be disassembled and the screen removed. With the screen removed the ribbon cable was accessible, using trial and error the pins carrying the I²C signal was
found. The transmitting diodes was soldered to the signal pins using very thin cables, this allowed the screen to be reattached to the phone while still accessing the signals.

3.4 Packet format

In order to understand the data being transported on the I²C data bus between the touchscreen microcontroller and the processor all packets had to be mapped. The mapping was done using the oscilloscope described in 3.1.1, with its built-in support for decoding I²C the signal was automatically converted to bytes and start/stop-signals. By manually touching the screen with varying position, size, and number of touchpoints each packet sent over the bus was mapped.

3.5 Performing a measurement

The following section describes all steps required to perform a measurement and the order in which they were done.

For each performed measurement reported in the result section several steps are needed. Before any measuring could take place both targets where selected and modified as described in section 3.3 to allow access when measuring.

Once the pins transmitting the signal was accessible the packet format was mapped out as described in section 3.4.

The target was then setup as described in section 3.2 in order to continuously have an active touch event transmitting a signal. This signal is what was used as reference signal for the measurements.

The target was then connected to the equipment described in section 3.1. Mainly the oscilloscope was attached to the signal pins on the target and the absorbing clamp or near-field probe, depending on what kind of emanation was being measured, was mounted to the measurement point of the target.
3.5. Performing a measurement

3.5.1 Running AUTO-RÖS

After the target and equipment was setup the AUTO-RÖS software was run. After running AUTO-RÖS a live graph and its corresponding table is presented. This graph depicts the normalised cross-covariance value for each frequency measured as described in subsection 3.1.6.

As mentioned in section 2.4.5 the cross-covariance value does not guarantee the existence of compromising emanations. Instead, the graph is used to quickly filter out points of interest that have a higher likelihood of containing compromising emanations. For this thesis a cutoff value of 0.4 was chosen, meaning only results with a cross-covariance of 0.4 or higher was selected for further study.

By clicking the graph it is possible to study the signal at each measured frequency and based on the visual inspection come to a conclusion whether the signal contains compromising emanations or not. This is repeated for all points of interest as mentioned above.

The AUTO-RÖS steps described above were performed repeatedly with varying settings and several different positions used when simulating touch. After it was established that the results obtained from measuring were consistent, a final measurement covering the area with the strongest indications of compromising emanations was performed. The results of this measurement is depicted in the result section.
Chapter 4
Results

The results have been separated into two parts. The first part describes the packet format used by the single-board computer and the smartphone, this information was collected manually using an oscilloscope as described in section 3.4.

The second part of the results contain a selection of the measurements performed using the AUTO-RÖS software. Throughout the thesis a large amount of measurements where performed, the ones presented here were selected as representative of the general trend noticed in these measurements. The second part have then been separated into three categories based on the device tested and the method used to capture the compromising emanations.

4.1 Packet format

The results of the packet format mapping have been divided into two subsections, one for each device.

4.1.1 Single-board computer

Studying the signal reveals a recurring array of packets every 17.5 ms. It also revealed that all packets are sent in pairs with a write from master (the processor) to slave (the touchscreen microcontroller) followed by a read from master to slave. Since there is no other node connected to the bus and the master/slave roles never change, the address remains constant for all packets with a hex value of 38. The SCB uses two types of packet pairs and transmits up to 11 packet pairs within one 17.5 ms timeslot.

The first pair of packets exchanged contains the number of touchpoints currently active on the touchscreen. The first write packet always carries a single byte with a hex value of 02 and is used to trigger the touchscreen microcontroller to respond with how many active touchpoints are on the screen.

After the write packet is finished the processor retrieves the first read packet from the microcontroller. The first read packet contains a single hex value between 00 and 0A, this hex value corresponds to the 0-10 active touchpoints on the screen. Depending on the number of active touchpoints two different things happen. While there are no active touchpoints no other packets are sent between the processor and microcontroller. The first pair of packets is then repeated every 17.5 ms until a touch occurs.

If there is one or more touchpoints a second pair of packets is repeated once for each touchpoint. The write packet of the second pair contains a single byte with a hex value between 03 and 39. The value written in the second write packet decides what touchpoint data will be returned in the following read packet. If there is only one touchpoint there will only be a single write packet containing the value 03 followed by a read packet giving the position for that touchpoint. When there are more than one touchpoint the write value is incremented by six each time, i.e for two touchpoints there would be two write packets, the first with hex value 03 and the second with hex value 09.
4.1. Packet format

Table 4.1: Second read packet between the single-board computer and touchscreen containing the coordinate data for one touchpoint.

<table>
<thead>
<tr>
<th>Value</th>
<th>Write/Read</th>
<th>Data 1</th>
<th>Data 2</th>
<th>Data 3</th>
<th>Data 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note</td>
<td>Read</td>
<td>80-83</td>
<td>00-FF</td>
<td>00-01</td>
<td>00-FF</td>
</tr>
<tr>
<td>X-coord (MSB)</td>
<td>X-coord (LSB)</td>
<td>Y-coord (MSB)</td>
<td>Y-coord (LSB)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The second read packet, as described by table 4.1, contains 4 bytes of data used to define the X and Y coordinate of a touchpoint. In the first byte (Data 1), the first bit is constantly set regardless of touchposition and number of active touchpoints. Besides the first bit, the first two bytes (Data 1 and 2) constitutes the X coordinate of the touchpoint. The following two bytes (Data 3 and 4) constitutes the Y coordinate of the touchpoint. The touchscreen has been found to use a big-endian format meaning the first byte for each coordinate (Data 1 and 3) is the most significant byte (MSB).

By tracing the edge of the screen and observing the change in values the min and max for each axle was determined. Origo (0,0) is represented as the lower right corner of the screen. The decimal min and max values given in table 4.2 matches the specified screen resolution of 800x480, this creates a one-to-one mapping between drawn pixels and possible touchpoints.

Table 4.2: Min and max values achieved by tracing the edge of the touchscreen connected to the SCB.

<table>
<thead>
<tr>
<th>Hexadecimal</th>
<th>Decimal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min</td>
<td>Max</td>
</tr>
<tr>
<td>X</td>
<td>000</td>
</tr>
<tr>
<td>Y</td>
<td>000</td>
</tr>
</tbody>
</table>

4.1.2 Smartphone

The signal between the processor and touchscreen microcontroller in the smartphone is not repeated with a fixed timing, the array of packets used to make up a whole transmission is repeated every 10 ms on average. Studying the signal also showed that while there was no active touchpoint on the screen, no signal was transmitted on the bus. A whole transmission consist of eight write packets and six read packets.

Similar to the bus used by the SCB, the master/slave roles never change and the address remains constant for all packets with a hex value of 20. All packets are sent in pairs with each write being directly followed by a read, except for the fourth and eighth packet which have no read counterpart directly following them.

As mentioned, a whole transmission consists of 14 packets, of these packets 10 show no signs of correlation with touchposition or number of touchpoints. It is unlikely that the data contained in those packets is random but no clear pattern was found when measuring. As no information could be drawn from these 10 packets they have been omitted in the results.

The second pair of packets is the first to carry information related to the touchpoints on the screen. The second write packet always carries a single byte with a hex value of 07. This packet triggers the touchscreen to respond with the number of active touchpoints on the screen.

The second read packet, as described by table 4.3, contains two bytes and follows directly after the second write packet. Contrary to the single-board computer, the smartphone use a little-endian format meaning the first byte in all multibyte data is the least significant byte (LSB). In the second read packet each active touchpoint is indicated by a bit set to one.
e.g. a hex value of 1F = 00011111₂ indicates five active touchpoints. The second byte (Data 2) increases the same as the first byte above eight touchpoints.

No packets are being sent when there are no active touchpoints but it is possible to receive a value of zero i.e. no touchpoints. This happens among the very last packets that are sent after letting go of the touchscreen.

Table 4.3: Second read packet between the smartphone and touchscreen containing the data describing number of touchpoints active on the touchscreen.

<table>
<thead>
<tr>
<th>Write/Read</th>
<th>Data 1</th>
<th>Data 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>Read</td>
<td>00-FF</td>
</tr>
<tr>
<td>Note</td>
<td></td>
<td>00-03</td>
</tr>
</tbody>
</table>

The third pair of packets contain information about all active touchpoints. The value in the third write packet is a constant hex value of 06 regardless of the number of touchpoints, it is only used to trigger the touchscreen for a response.

The third read packet contain seven bytes of data, the first byte (Data 1) has a constant hex value of 01 through all packets except among the last packets that are sent after releasing the touchscreen where it instead has the hex value 00. The following six bytes (Data 2-7) are used to describe a touchpoint. Each coordinate is stored using two bytes as shown in table 4.4.

The last two bytes (Data 6 and 7) correlate with the area of the object used when touching the touchscreen. During a normal touch, using the index finger, both bytes stay at a fairly constant hex value of 06. By increasing the touch area, using several fingers or the side of the hand, the value increase.

Contrary to the SCB, the smartphone does not send multiple packets to handle multiple touchpoints. Instead the same read packet is extended with seven bytes for each additional touchpoint. These bytes follow the same pattern as the first (Data 1-7), each describing another touchpoint.

Table 4.4: Third read packet between the smartphone and touchscreen containing the coordinate data for all active touchpoints.

<table>
<thead>
<tr>
<th>Write/Read</th>
<th>Data 1</th>
<th>Data 2</th>
<th>Data 3</th>
<th>Data 4</th>
<th>Data 5</th>
<th>Data 6</th>
<th>Data 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>Read</td>
<td>00-01</td>
<td>00-FF</td>
<td>00-04</td>
<td>00-FF</td>
<td>00-07</td>
<td>04-19</td>
</tr>
<tr>
<td>Note</td>
<td>X (LSB)</td>
<td>X (MSB)</td>
<td>Y (LSB)</td>
<td>Y (MSB)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The smartphone has a specified screen resolution of 1080x1920, comparing this to the range shown in table 4.5 gives a near one-to-one mapping between drawn pixels and possible touchpoints. While finding Origo (0,0) was not achievable by tracing the edge of the screen the lowest value of X and Y was found in the top left corner of the screen.

Table 4.5: Min and max values achieved by tracing the edge of the touchscreen of the smartphone.

<table>
<thead>
<tr>
<th>Hexadecimal</th>
<th>Decimal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min</td>
<td>Max</td>
</tr>
<tr>
<td>X</td>
<td>010</td>
</tr>
<tr>
<td>Y</td>
<td>011</td>
</tr>
</tbody>
</table>
4.2 Compromising emanations

The results of the measurements from the AUTO-RÖS software have been divided into three sections. As mentioned earlier, the measurements presented were selected from a larger selection as they are representative of the overall results noticed throughout the thesis.

4.2.1 Conducted emanations from the single-board computer

The conducted emanations from the single-board computer was measured using an absorbing clamp. The clamp was placed around the power supply cable connected to the SCB. Figure 4.1 shows the normalised cross-covariance between the I²C reference signal and an average based on several conducted emanations measured by the power supply cable in the SCB. Each color represents one kind of compromising emanations. The white graph contains three points of interest, depicted as the three white spikes all with a value higher than 0.4. By manually inspecting each point it was concluded that the highest spike with a value of 0.52 found at 138.9 MHz contained the clearest compromising emanations.

Figure 4.1: Normalised cross-covariance measuring between the I²C reference signal and an average based on several conducted emanations emitted by the power supply cable in the SCB. Each color represents one kind of compromising emanations. The white graph contains three points of interest, depicted as the three white spikes all with a value higher than 0.4. By manually inspecting each point it was concluded that the highest spike with a value of 0.52 found at 138.9 MHz contained the clearest compromising emanations.

The conducted emanations from the single-board computer was measured using an absorbing clamp. The clamp was placed around the power supply cable connected to the SCB. Figure 4.1 shows the normalised cross-covariance between the I²C reference signal and an average based on several conducted emanations measured by the absorbing clamp, calculated using the AUTO-RÖS software. Each color in figure 4.1 represents one kind of compromising emanation. The legend in the top left corner of the figure describes the type of emanation related to each color.

Figure 4.1 contains three points of interest in the white graph at 125.0, 138.9 and 166.7 MHz. Each of these points contain spikes where the cross-covariance value is higher than the selected cutoff value of 0.4. By manually studying the conducted emanations at each frequency listed above it was concluded that the clearest emanations was found at 138.9 MHz. It also coincides that the spike at 138.9 MHz is the highest of the three with a cross-covariance value of 0.52.

Figure 4.2 contains two graphs, the yellow graph is the I²C reference signal and the green graph is an average based on several conducted emanations measured with the absorbing clamp at 138.9 MHz. Comparing the two signals with eachother shows four points of interest each marked with a red box and a number in figure 4.2. At the first and fourth point three spikes in the conducted emanations correlate with a wide high value in the reference signal. Given that the conducted emanations stay high and only return to a lower value once the reference signal has returned to low is used to decide the emanation type captured. The emanations captured are of the first version explained in section 2.1 meaning it has the potential to carry the full signal transmitted by the system.

The second and third point marked in figure 4.2 show two examples of correlation between a single spike in the conducted emanations and a small high value in the reference signal. Each
4.2. Compromising emanations

Figure 4.2: Graph depicting the single-board computers I²C reference signal in yellow and an average based on several conducted emanations at 138.09 MHz in green. Studying the signals a relation marked 1 can be seen as a wide block in the reference signal and three green spikes in the measured signal. A similar relation can be seen marked 4 and a weaker relation can be seen between the thin blocks and the spikes marked 2 and 3 small block in the reference signal is a bit in the I²C communication and it is correlated by a single spike in the emanations, based on this it can be assumed that the spiky nature of the emanations is generated by the clock signal used by the system.

Finally, studying the signals after the fourth point of interest it seems the correlation patterns described above no longer apply. A possible explanation to this is the transfer direction of the data, after the fourth point the transfer direction changes causing the signal to be generated by the microcontroller in the touchscreen instead of the single-board computer.

4.2.2 Radiated emanations from the single-board computer

The radiated emanations from the SCB was measured using a near-field probe. The probe was placed at a 5 cm distance behind the SCB. Figure 4.3 shows the normalised cross-covariance, between the I²C reference signal and an average of several radiated emanations measured by the probe, calculated using the AUTO-RÖS software. The figure contains two points of interest in the white graph centered around 225.0 and 250.0 MHz. Applying the method used for conducted emanations above a manual inspection showed the clearest emanations at 225.0 MHz with a cross-covariance value of 0.68.

Figure 4.4 contains two graphs, the yellow graph is the I²C reference signal and the green graph is an average of several radiated emanations measured with the probe at 225.0 MHz.
4.2. Compromising emanations

Figure 4.3: Normalised cross-covariance measuring between the I\textsuperscript{2}C reference signal and an average of several radiated emanations emitted by the SCB. The graph contains two points of interest, depicted as the two white spikes. By manually inspecting each point it was concluded that the highest spike with a value of 0.68 found at 225.0 MHz contained the clearest compromising emanations.

Comparing the two signals with each other shows three points of interest marked with a red box and a number in figure 4.4. In the first red box, marked 1, an inverted correlation can be seen between the reference signal and the radiated emanations. This is seen in the emanations as a spike aligned to the reference signals low value followed by a low value in the emanations aligned with the high value in the reference signal.

A similar inverted correlation is identified in the second red box, marked 2, where the two wide gaps in the emanations line up with the high values in the reference signal. The third and final point of interest, the red box marked 3, follows the same pattern with a wide gap in the emanations aligned with a wide high value in the reference signal.

The same spiky nature caused by the clock signal described in the conducted emanations can be seen in the radiated emanations and the change in correlation pattern directly following the transfer direction is apparent after the third point of interest. These similarities between conducted and radiated emanations are expected as the signal conducted in the power supply cable is likely the same as the one radiated from the system.

4.2.3 Radiated emanations from the smartphone

The radiated emanations from the smartphone was measured using a near-field probe. The probe was placed at a 5 cm distance behind the phone. Figure 4.5 shows the normalised cross-covariance, between the I\textsuperscript{2}C reference signal and an average of several radiated emanations measured by the probe, calculated using the AUTO-RÖS software. The figure contains several points of interest, each with a cross-covariance value above 0.4. Manually inspecting each frequency results in emanations that all look like the emanations shown in figure 4.6. The specific frequency 211.7 MHz contained slightly clearer emanations than the rest and had the highest cross covariance value of 0.47.

Figure 4.6 contains two graphs, the yellow graph is the I\textsuperscript{2}C reference signal and the green graph is an average of several radiated emanations measured with the probe at 211.7 MHz. Comparing the signals shows the following points of interest marked in the figure. In the first red box, marked 1, a strong inverted correlation can be seen between the two wide high values in the reference signal aligned to the two wide low values in the emanations. The high values in the first red box in the reference signal also correspond to the data indicating the start of a new data transfer. This allows the first point of interest, marked 1, to be used as an alignment when studying the signal further.
4.2. Compromising emanations

Figure 4.4: Graph depicting the single-board computers I²C reference signal in yellow and an average of several radiated emanations at 225.0 MHz in green. Studying the signals a inverted relation, marked 1, can be seen as a wide block in the reference signal and a gap in the measured signal. A similar inverted relation can be seen marked 3 and a weaker inverted relation can be seen between the thin blocks and the gaps marked 2.

Figure 4.5: Normalised cross-covariance measuring between the I²C reference signal and an average of several radiated emanations emitted by the smartphone. The white graph contains several points of interest, all with a value higher than 0.4. By manually inspecting each point it was concluded that the highest spike with a value of 0.47 found at 211.7 MHz contained the clearest compromising emanations.
4.2. Compromising emanations

Figure 4.6: Graph depicting the smartphones I²C reference signal in yellow and an average of several radiated emanations at 211.7 MHz in green. Studying the signals a clear inverted relation can be seen at 25 μs between the two blocks in the reference signal at and the gaps in the measured signal. A similar inverted relation can be seen with the repeated thin gaps in the measured signal and the corresponding thin blocks in the reference signal, these thin blocks in the reference signal correspond to the ACK bits used by I²C.

The second point of interest in figure 4.6, marked 2, shows a repeating gap with a fixed interval length. This interval lines up with the high values in the reference signal, marked 3. Further studying the I²C data contained in the reference signal shows that the values at the marked interval is the Acknowledge bit sent between each byte transferred.

While the Acknowledge bits are easily identified in the measured signal there is no clear indications of a correlation between the smaller spikes in the measured signal and the bits in the reference signal. To reliably measure and identify compromising emanations from the smaller spikes would require a more delicate and fine-tuned method.
Chapter 5
Discussion

Throughout this thesis several choices had to be made. In this chapter arguments for these choices and how they affect the thesis are made.

5.1 Related Work

It is common to present the reader with a section covering other published articles written in the same field as the thesis. However, as the field of compromising emanations, specifically in touchscreens is very narrow few other published articles was found.

While the attack vector developed by Cai et al. [15] uses an application installed on the device it is based around a side-channel attack. By studying the variation in device orientation data when a user touches the touchscreen the application was able to correctly infer more than 70% of the keys typed on a smartphone.

A case study presented by Spreitzer et al. [16] proposes a categorization of side-channel attacks for mobile devices. However, their study does not focus solely on compromising emanations instead they include other categories such as network traffic analysis and software-only attacks.

By widening the field to include input devices other than touchscreens many good articles can be found. Both Vuagnoux et al. [2] and Asonov et al. [3] provide good insight in to how electromagnetic- and acoustic emanations can be used to identify the keystrokes on a keyboard.

Given that very few articles related to compromising emanations in touchscreens were found may indicate several things. The field is too small or insignificant for any large amount of research to be done, the majority of devices are secure and no interesting findings are ever discovered or the field is still relatively new and will grow with time.

5.2 Method

The method and test equipment selected for this have been in use for several years. Before this thesis it has been used as a part of development and testing at Sectra. However, while it has proven a great tool there are some concerns that need to be addressed.

5.2.1 Alternative environment setups

Acquiring and setting up the equipment needed to measure electromagnetic emanations is not easy. For starters, the price tag alone puts this kind of equipment outside the scope of a private person. In addition to the price, the equipment used must be compatible with each other and properly calibrated to ensure the measurements are correct. Based on this, for the scope of the thesis it was an easy call to decide that they equipment already available at Sectra would be used.

However, it is important to consider the possible impact the selected equipment may have had on the measurements.
First, accuracy, both the spectrum analyzer and oscilloscope worked great during testing and provided results that proved the existence of compromising emanations in the SCB and partial emanations in the smartphone. Using more expensive equipment capable of measuring even smaller differences in the signal may be enough to extract more information from the emanations generated by the smartphone. On the other hand, using cheaper equipment may be enough to find the same information that was found in this thesis.

Secondly, AUTO-RÖS, the software was developed at Sectra and the existence of alternatives were never researched. While AUTO-RÖS does not decide the existence or absence of compromising emanations, the user running the scan may trust the software leading to false negatives. This is further discussed in the following section 5.2.2.

5.2.2 Cross-covariance as a measurement

As mentioned the method chosen has been in use at Sectra prior to this thesis. As such, the choice was heavily based on the fact that all the equipment needed and the knowledge required to use it could be found inhouse. Disregarding the reasoning behind the choice it is important to evaluate alternative methods that could have been used.

As described in section 2.4.5 the cross-covariance calculated is not a proof of the existence of compromising emanations. Manually calculating the cross-covariance between two signals for a single bandwidth at a single frequency does not give an answer to whether or not compromising emanations exist. However, by automating the process, as has been done in AUTO-RÖS, it is possible to scan large frequency spans quickly and use the graph generated to find areas more likely to contain compromising emanations.

An alternative to using a tool such as AUTO-RÖS would be for the operator to manually search through the frequencies similar to looking through radiochannels on an old analogue radio. This reduces speed and accuracy when searching but may be beneficial in some cases. For example, it is possible that the compromising emanations are shaped in a way causing their cross-covariance to be lower than expected leading to a false negative in AUTO-RÖS while the operator performing the manual search notices the pattern between the original signal and the compromising emanation.

However, a manual search may also cause false positives due to the operator imagining a pattern between the original signal and the compromising emanation when there are none. Manual searching is therefore highly dependent on the skill of the operator.

5.2.3 Risk for false positives

During initial testing several false positives were detected. More specifically, while testing radiated emanations from the single-board computer it was discovered that the equipment indicated strong compromising emanations regardless of the distance or angle between the device and the antenna used to pick up the emanations. After troubleshooting, the source of the problem was confirmed to be the wire connecting the reference signal from the device to the oscilloscope. By changing the wire to a optical connection the false positives no longer appeared and all results presented in this thesis have been done using an optical connection.

While one source of false positives was discovered and solved the risk of an undetected error affecting the validity of the results during testing always exists. However, as the equipment have been used by Sectra for a lot of tests it should be safe to assume that most issues affecting the validity of the testing have been found and removed. Although, the risk for false positives should never be ignored.

5.2.4 Far-field testing

All radiated emanation testing in this thesis have been done using a near-field probe. While this is sufficient to test whether any radiation exists it only works in very close proximity to the
device. In order to test the entire electromagnetic radiation an antenna capable of handling the far-field is required. For best results this antenna would also have to be tuned to the frequency band being tested.

5.3 Results

Overall, the results were expected as neither of the devices were designed to prevent compromising emanations. Testing the smartphone for conducted emanations could have shown stronger emanations, but in order to facilitate an attack using conducted emanations on a battery powered device it would have to be connected to something with a cable. The signal leaked through conducted emanations may contain equal or possibly even higher amounts of information than radiated emanations. However, the necessary conditions to perform an attack are harder to achieve leading to a overall lower security risk.

In most cases compromising radiated emanations pose a greater threat than conducted emanations for both battery powered and installed devices as conducted emanations require physical access.

5.3.1 Attacking the device

It is important to note that these results only indicate the existence of compromising emanations in these devices. In order to confirm this as a security vulnerability and then further implement a functioning attack vector would require several steps not covered in this thesis.

5.3.2 Future risks

The results of this thesis alone shouldn’t be seen as touchscreens are unsafe and no one should use them. It is important to know that these results were achieved using expensive, high quality equipment in a controlled environment. Given the price point, it is safe to say that the average user don’t have to worry about protecting themself from compromising emanations.

However, given that technology grows more accessible and cheaper over time it is still a risk that should be taken in to account for the future. Already today, there exists an area of software known as Software-defined radio (SDR). SDRs are capable of measuring electromagnetic radiation using only the limited hardware in a personal computer. With time this evolving area may be powerful enough to be used in place of the expensive equipment counterparts, making it a lot more affordable and accessible for the average user.

Therefore, it is important that the risk is taken into consideration to ensure that compromising emanations does not become a problem for touchscreens in the future.

5.4 The ethical problem of disclosure

Research surrounding compromising emanations is a very sensitive subject considering the results may directly reveal a weakness in a system previously thought to be safe to use. Depending on the system being studied the societal impact may need to be considered. What if a study reveals a flaw allowing wireless access to an ATM? Would it be ethically right by the author to publish his findings? Or would it be worse to not publish his findings?

Regardless of what is the right/wrong choice it is important to consider the possible implications for all users when studying systems with the possibility to affect a lot of people. During the initial stages of this thesis one path considered was developing a method for automatically converting the data in the compromising emanations to coordinates allowing them to be used as an attack vector for reading out where a user is clicking on the screen. Given the ethical implications of describing the development of such a tool in detail for the report I am glad another path was choosen. Further on, the method and results shown in this report can not be directly used as an attack vector.
In addition to not pursuing the path of implementing an attackvector, prior to the publication of this thesis affected vendors were contacted and given a chance to comment on the content. By providing advance notice to the affected vendors they are given additional time to identify the root of the problem and, if possible, come up with a solution.
Chapter 6
Conclusions

In this thesis two different systems using touchscreens have been evaluated in regard to the possible leakage of information due to compromising emanations. The thesis covers both conducted and radiated emanations originating from the touchscreen in the system studied. While only two systems have been evaluated it is important to put in perspective what these systems and touchscreens in general represent. In today’s society touchscreens show up in more and more places. If a business needs a way for a customer or employee to input information it is likely that a touchscreen is used. The system it is used for may range from something harmless like a refrigerator to something more important like an ATM. Either way protecting the information is important and some systems may not have a touchscreen with a higher quality than the one in the single-board computer.

Similarly with smartphones, previously phones were used to make calls and send textmessages. Today, people use smartphones to do everything from send emails to perform bank transfers and almost all smartphones use touchscreens. As such, the smartphone evaluated is a perfect reference for a system where somewhat sensitive information is processed.

From these two different systems similarities can be found and possible conclusions drawn. While being from two very different areas both in price and usage they both use a \( I^2C \) bus between the touchscreen and the device. While it may be a lucky coincidence it can also indicate that \( I^2C \) is the go-to solution for connecting touchscreens. Based on this it is important to consider, how are other devices faring when it comes to compromising emanations?

Furthermore, as concluded below, given that both devices radiate emanations related to their touchscreens, with the SCB emanating directly compromising information, should it be seen as another lucky coincidence or is it possible that issues with conducted and radiated emanations is common in other touchscreen devices as well?

Based on the results presented the questions that constitute the basis of this thesis are answered below.

6.1 Can you detect conducted compromising emanations from a capacitive touchscreen?

Studying figure 4.2 shows a correlation between the single-board computers' \( I^2C \) data signal in yellow and the emanations detected in green. This is a direct sign of compromising emanations as traces of the original signal are visible in the emanations. Based on this it can be concluded that conducted compromising emanations can be detected from the SCB.

As the smartphone is a battery-powered device it was not tested for conducted emanations. Theoretically, the smartphone could be vulnerable to conducted emanations during charging as the charging cable is connected. This was not tested and as such no conclusion can be drawn. In addition to this, another common side-channel attack usually performed on the power cable of the system is power consumption analysis. In today's smartphones it is often possible to access the power consumption of the device using the API provided by the OS, this allows an app installed on the smartphone to read out the power consumption and send
6.2 Can you detect radiated compromising emanations from a capacitive touchscreen?

Studying figure 4.4 shows a correlation indicating that the signal has leaked through the radiated emanations from the single-board computer. Unlike the conducted emanations, the signal here is inverted but it still carries traces of the original signal. It is therefore concluded that radiated emanations can be detected from the SCB.

Following in the footsteps of the SCB, a study of figure 4.6 shows a correlation between the smartphones I²C data signal and the radiated emanations. In 4.6 it directly shows a leakage of the startbit used by the I²C bus (the two largest spikes to the left in the figure), it also shows a repeated correlation between the I²C ACK-bit and the thin gaps in the radiated emanations. Based on this it can be concluded that the smartphone radiates emanations related to the touchscreen.

However, the startbit and ACK-bit alone can not be seen as a leakage of information. Based on this the emanations radiated by the smartphone can not be concluded to be of compromising nature.

With a sample size of only two different devices it is hard to draw any general conclusion. However, with two devices both radiating emanations, one of which has a compromising nature, at the very least it is possible that other devices will also radiate emanations related to the touchscreen.

6.3 Future work

This thesis only covers a small part of the possible research concerning compromising emanations from touchscreens. In order to help ensure the security of touchscreens there are several areas that can be expanded and improved.

First and foremost, sample size, there are a lot of devices using touchscreens and this thesis only covers two examples. In order to draw a more general conclusion regarding touchscreens an empirical study with a large sample size would be helpful.

In addition to device sample size this thesis only covers the I²C bus used by capacitive touchscreens. There are several other parts with the potential to emit compromising emanations such as the conductive layer in the screen or the control chip used to convert the data to coordinates on the screen.

Also, section 2.1.4 mentions the existence of shielded equipment. To protect devices it may become necessary to find new ways of shielding them. One method of shielding consists of covering the shell of the device in a thick metal layer, while this may work for installed devices it heavily reduces mobility and may be undesirable for devices such as a smartphone. A common way of protecting screens is by covering them with a metal mesh allowing it to be used while preventing electromagnetic emanations. However, it is possible that the metal mesh prevents the function of a capacitive touchscreen and therefore can not be used. In order to find suitable ways of protecting touchscreen devices further research is needed.

Finally, capacitive touchscreens are the focus of this thesis as they are currently the most used. However, other technologies such as optical and resistive touchscreens still have a use and need to be studied to ensure their security as well.
Bibliography


