The Symantec Smartphone Honey Stick Project

Symantec

CONTENTS

Executive Summary

The Symantec Smartphone Honey Stick Project is an experiment involving 50 "lost" smartphones. Before the smartphones were intentionally lost, a collection of simulated corporate and personal data was placed on them, along with the capability to remotely monitor what happened to them once they were found.

Sites Visited by Lost Smartphone #N2

Chief among the findings is that there is a very high likelihood attempts to access both sensitive personal- and business-related information will be made if a lost and unprotected smartphone is found by a stranger. Secondarily, the owner of a lost smartphone should not assume the finder of their device will attempt to make contact with them. Even when contact is made, the owner of the device should not assume their personal- or business-related information has not been violated.

The goal of this research is to show what smartphone users should expect to happen on their phones if they are lost and then found by a stranger. In today's world, both consumers and corporations need to be concerned with protecting the sensitive information on mobile devices. While devices can be replaced, the information stored and accessed on them is at risk unless users and businesses take precautions to protect it.

Introduction

In today's highly connected world, smartphones have become a key asset for individuals in everyday life, for both business and personal use. Their vast storage capability, together with unprecedented computing power and Internet-connected applications make smartphones carried by employees a significant information asset that businesses must now include in their security plans. Furthermore, because smartphones are also a consumer item, individuals must consider the risks to their personal information stored and accessed using smartphones.

The theft or accidental loss of a smartphone can expose businesses and individuals to loss of any data stored on the device, as well as data residing in corporate systems or cloud applications to which the device might have direct connections. The use of consumer smartphones within a corporate environment further complicates the issue of data protection, as information may flow onto or through devices that are not fully controlled by the business.

Threats and Risks Facing Smartphones

The risks to information are determined by the likelihood and capability of threats, as well as weaknesses in protection of data, wherever it may be. In recent years, security researchers have conducted many studies and performed demonstrations on the weaknesses found in smartphone operating systems, as well as in the apps themselves. This type of research helps identify vulnerabilities that need to be strengthened in the devices and apps. While understanding and addressing these weaknesses is extremely important, it is difficult to know which of them are likely to be exploited without knowing more about the threats facing a mobile device in an everyday scenario.

In late 2011, Symantec commissioned Scott Wright of Security Perspectives Inc., to conduct a study in this area. Sprint also was a sponsor of the study. The Symantec Smartphone Honey Stick Project – North American Edition is designed to help businesses and individuals in understanding some of the most likely threats to smartphones and their associated information that arise when a smartphone is lost. A person finding a lost phone is defined as a human threat as opposed to a technical threat from attackers who use tools or techniques to attack a smartphone from a remote location via the Internet or via direct radio communications with the device from nearby.

The basic question answered is: "What types of information will the finder of a lost smartphone try to access, and how persistent will they be?"

By better understanding this type of human threat, businesses and individuals will be better able to choose appropriate safeguards in terms of policies, procedures, training and technology for employees using mobile devices. In today's world, both consumers and corporations need to be concerned with protecting sensitive information on these devices.

Scope and Setup

The scope of this study involved configuring 50 smartphones for deployment in New York City, Washington D.C., Los Angeles and the San Francisco Bay Area within the U.S., as well as Ottawa, Canada. The devices were intentionally lost in a number of different environments such as elevators, malls, food courts, public transit stops and other heavily trafficked, publicly accessible locations. As finders picked up each device and attempted to access apps and data on them, details of those events were centrally logged to produce a



database of anonymous threat data that can be used by businesses when performing risk assessments on their information systems.

No security software or features (e.g. passwords) were enabled on any of the devices, in order to enable finders to initiate virtually any action without any complications. The objective in leaving devices unprotected was to observe what actions a human threat would take if there were no barriers to accessing any of the apps or information on a phone.

Objectives

The basic objectives of the study were to characterize the following aspects of human threats to a lost smartphone's data, and the corporate systems to which it might be connected:

- Likelihood of a finder attempting to access data on the smartphone
- Likelihood of a finder attempting to access corporate applications and data
- Likelihood of a finder attempting to access personal applications and data
- Likelihood of attempted access to particular types of apps
- Amount of time before a lost smartphone is moved or accessed
- Likelihood of a finder attempting to return a device to its owner

In the context of a lost smartphone, the human threat is simply an average person finding a lost device, with no apparent owner in sight. The finder may choose to either ignore the device, turn it in to a person or place of authority such as a store proprietor or a "lost and found," or they may try to access the device themselves. A person – either the finder or somebody to whom the finder has given the device – may try to access apps or data on the device for various reasons. Some of the logical reasons for accessing the apps or information on the device might be:

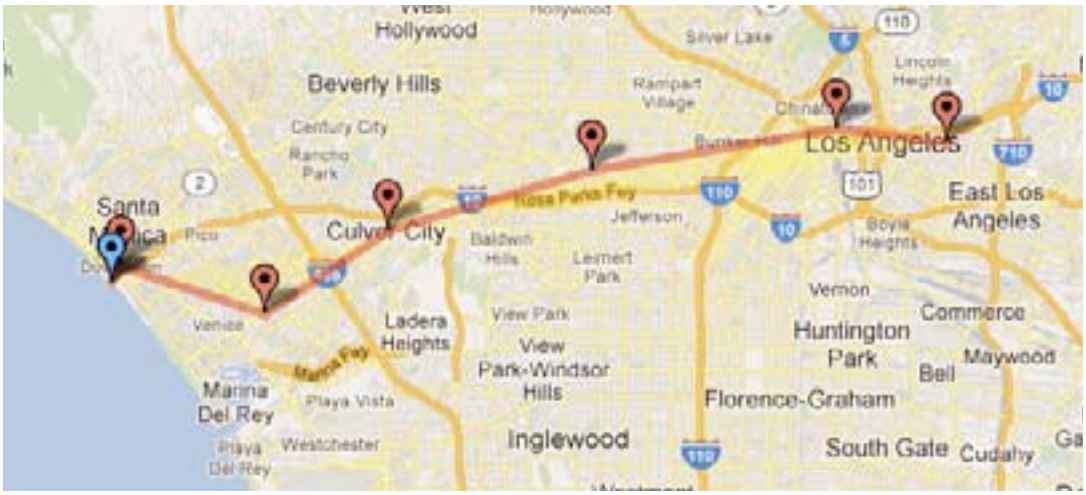
- They are trying to locate the owner so the device can be returned to them
- They are curious about what is on the device
- They are looking for information of value to them
- They want to use the device in the short term for free calls or Internet connectivity
- They are trying to reset the device so that it can be permanently re-used or sold

Regardless of the motivation of the person accessing the phone, the fact that they may be accessing sensitive data should be a major concern to the device's owner, and possibly their employer.

Believing that a finder is likely to return a lost device is potentially reassuring to a smartphone's owner, but if the finder attempts to access other information on the device, it could be a considered a major security breach. For example, opening a corporate email app might immediately give the holder of the phone access to confidential corporate information such as intellectual property, financial plans, bid pricing or personal information about employees. This type of confidentiality breach could cost the employer significantly in lost revenue opportunities or even legal actions.

From a personal point of view, such a confidentiality breach on a personal or corporate smartphone could result in major embarrassment, psychological stress or even extortion or discrimination, depending on the nature of information accessed.

If they have never lost a mobile device, many smartphone owners might focus on whether or not their device can be retrieved should it become lost. However, a smartphone owner may not realize that, even though the finder may offer to return the device, the likelihood of them accessing sensitive information on the phone may still be high.



Methodology

Each smartphone was loaded with a set of simple apps that had icons and names that would likely be recognizable to a finder. These simulated apps had no real functionality but were able to transmit simple event data to a central logging facility to indicate which app was activated and at what time. Typically, in most cases an error message or other plausible reason for the app to not work was displayed.

The data collected for apps on each device included:

- Device ID
- App name
- Time of app activation

The simulated app types installed on each device and the associated information category (i.e., Corporate, Personal or Neutral) are shown in the table below:

App Type	Information Category
Social Networking	Personal
Online Banking	Personal
Webmail	Personal
Private Pix	Personal
Passwords	Neutral
Calendar	Neutral
Contacts	Neutral
Cloud-Based Docs	Neutral
HR Cases (PDF)	Corporate
HR Salaries (Spreadsheet)	Corporate
Corporate Email	Corporate
Remote Admin	Corporate

A GPS tracking mechanism was also used to log each phone's position occasionally, which might aid in later analysis such as determining if a device was turned in to police, sold at a pawn shop, etc. The GPS mechanism was also used to determine if the device was still operating normally, even if no apps were accessed.

Note that on most smartphones, there is not an easily accessible file system as there is on personal computers. So, document type files less commonly appear on the home screens of most smartphones. Therefore, the majority of the icons on the devices leveraged for this study represented apps that initiate a program on the device. However, in an attempt to highlight corporate data during the study, files such as "HR Cases" and "HR Salaries" were represented on home screens with icons that looked like recognizable document types such as the PDF format or popular business- or productivity-oriented file types.

Measuring Intentional Access to Sensitive Information

Several apps had a simulated login page with a username and password prefilled to see if people would try clicking through the authentication of an app. This might be considered to be an unethical access attempt, since an explicit login page was presented to the user after clicking on the apps' icons.

There was one app titled "Contacts" which had only a small number of entries, including one entry that had the tag (Me) beside the name, so finders could easily identify the owner of the device. It included an email address and phone number for the apparent owner of the smartphone.

Data Collection

Ten devices with fully charged batteries were dropped in each metropolitan area, all within a period of a few days. As log data was accumulated, it was stored in a database for analysis. Data was collected for each device for seven days, by which time most devices had stopped reporting data. When finders attempted to contact the owner by phone or email, this fact was logged as well.

Significant Experimental Error Possibilities

This type of experiment, in a public domain, has many variable factors. In particular, logging of the apps depends on the device having Internet access. Therefore, if a finder manipulates the device in a certain way, it is possible that no data will be recorded. This situation would result in an under-reporting of access frequency.

Conversely, the most significant over-reporting error would be an individual who was aware of the intent of the study, and performed repeated accesses as a way to manipulate the results to be more significant than would normally happen. This would require both technical knowledge to reach this conclusion, as well as a motivation to influence the study results. This considered to be a low experimental risk.

Key Findings

1. **96 percent** of lost smartphones were **accessed** by the finders of the devices
2. **89 percent** of devices were accessed for **personal** related apps and information
3. **83 percent** of devices were accessed for **corporate** related apps and information
4. **70 percent** of devices were accessed for both **business** and **personal** related apps and information
5. **50 percent** of smartphone finders **contacted the owner** and provided contact information

Expanded Findings and Conclusions

1. *When a business-connected mobile device is lost, there is more than an 80 percent chance an attempt will be made to breach corporate data and/or networks.*

    - A total of **83 percent** of the devices showed attempts to access **corporate-related** apps or data.
    - Attempts to access a **corporate emai**l client occurred on **45 percent** of the devices, which could potentially represent an attempt to contact the owner of the device, but still expose sensitive information.
    - A file titled **"HR Salaries"** was accessed on **53 percent** of the phones and another titled **"HR Cases"** was accessed on **40 percent** of the devices.
    - Attempted access to a **"Remote Admin"** app was recorded on **49 percent** of the devices.

This finding demonstrates the high risks posed by an unmanaged, lost smartphone to sensitive corporate information. It demonstrates the need for proper security policies and device/data management. This is especially true in the age of the consumerization of IT and Bring Your Own Device (BYOD), when mobile devices are flowing into and out of corporate infrastructures at previously unheard of rates. If an unmanaged, employee-owned device is used for corporate access unbeknownst to the organization and that device is lost, the consequences of having no control over that device – for example, to remotely lock or wipe it – can be devastating.

2. *People are naturally curious, but when a lost mobile device is discovered, curiosity can lead to the violation of personal privacy and the exposure of sensitive personal information.*

    - An attempt was made to **access** at least one of the various apps or files on nearly all – **96 percent** – of the devices.

- A total of **89 percent** of devices showed attempts to access **personal** apps or data.
- Attempts to access a **private photos** app occurred on **72 percent** of the devices.
- An attempt to access an **online banking** app was observed on **43 percent** of the devices.
- Access to **social networking** accounts and **personal email** were each attempted on over **60 percent** of the devices.
- A **"Saved Passwords"** file was accessed on **57 percent** of the phones.
- **66 percent** of the devices showed attempts to **click through** the login or password reset screens (where a login page was presented with **username** and **password** fields that were pre-filled, suggesting that the account could be accessed by simply clicking on the "login" button).
- There was an average time of **10.2 hours** before an access attempt was made; with a median time of **59 minutes** (based on actual access attempts).

These findings show how important it is for mobile device users to protect their privacy and sensitive information by using security tools, such as those featuring remote lock and wipe capabilities on their devices.

3. *If a mobile device is lost, the owner has only a 50 percent chance of being notified by a finder that their smartphone was found. However, just because they offer to return the device does not mean they are not taking liberties with the owner's information.*

    - Of the 50 devices, the owner only received **25 offers to help**, despite the fact that the owner's phone number and email address were clearly marked in the contacts app.
    - **89 percent** of finders accessed personal information and **83 percent** accessed **business** information.
    - **68 percent** of devices were **accessed prior to being moved** by the finder (32 percent were moved before being accessed).
    - **5 percent** of devices were moved, but were not accessed during the 7 days of the study.

This finding highlights the fact that in many cases, regaining possession of lost device may be a losing battle. But protecting the information on it does not have to be if the right precautions are taken. While devices can be replaced, loss of control over the information kept on these devices can result in far greater consequences.

Recommendations

Corporations should take the following steps to ensure mobile devices and sensitive corporate information remains protected:

- Organizations should develop and enforce strong security policies for employees using mobile devices for work; this includes requiring password-enabled screen locks. Mobile device management and mobile security software can aid in this area.
- Companies should focus on protecting information as opposed to focusing solely on devices, securing information so it is safe no matter where it ends up.
- Organizations should educate employees about the risks both online and physical associated with mobile devices, such as the impact of a lost or stolen device.
- Companies should take inventory of the mobile devices connecting to their networks; they can't protect and manage what they don't know about.
- Businesses should have a formal process in place so everyone knows what to do if a device is lost or stolen. Mobile device management software can help automate such a process.
- Companies should integrate mobile device security and management into the overall security and management framework and administer it the same way. In essence, treat mobile devices as the true endpoints they are.

Recommendations

Consumers should take the following steps to ensure mobile devices and the personal information on the devices remains protected:

- Smartphone users should use the screen lock feature and make sure it is secured with a strong password or "draw to unlock" pattern. This is the most basic security precaution and requires minimal effort on the part of the user, yet can provide a critical barrier between personal information and a stranger.
- Consumers should use security software specifically designed for smartphones. Such tools can stop hackers and prevent cybercriminals from stealing information or spying on users when using public networks. In addition it can often help locate a lost or stolen device and even remotely lock or wipe it.
- When out and about, users should make sure mobile devices remain nearby and never be left unattended, being mindful of where they put devices at all times. It is also a good idea to make sure they can differentiate their device from others that might be sitting in the immediate vicinity; adding distinguishing features such as a sticker or case may help.

About the Researcher

Scott Wright is a security coach, consultant and researcher, based in Ottawa, Canada. His first Honey Stick Project in 2008 (at www.honeystickproject.com) was based on lost USB memory sticks configured to log access by finders, in an effort to measure risk decisions and the level of security awareness in the general public. In that study, 65% of finders made risky decisions that could have led to malware infections on their computers.

Scott's company, Security Perspectives Inc. (at www.securityperspectives.com) helps businesses concerned with risks related to employees using the Internet.

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. More information is available at www.symantec.com.

Appendix

Number of Devices Accessing Each App

App Accessed	# of Devices on Which App was Accessed
Contacts	38
Private Pix	34
Social Networking	30
Webmail	28
Passwords	27
HR Salaries	25
Calendar	23
Remote Admin	23
Cloud-Based Docs	22
Corporate Email	21
Online Banking	20
HR Cases	19

*47 devices total reported