Faking it with Mobile Apps

mobilesecurity.com [San Francisco, CA] As every kid knows, shaking presents on Christmas Eve is the only way to quench the need to know whether that big box is really filled with Super Structs or sports socks. It's hard to blame today's tech-aware kids for assuming *there's an app for that*. Imagine the disappointment that one reviewer faced when trying to use an X-Ray Scanner app for the iPhone: "I got this to see what I got for Christmas and that's when I figured out it was a total fake."

I think we can agree that the interesting smartphone apps available on the various markets is a great thing. This is mainly due to a wealth of developers working diligently to tap into the many capabilities of a smartphone (even stuff that most of us don’t even know about). In this article, I'll shed some light on their limits, as well as how those limits are being pushed.

Anyone who spent elementary school in the days of the calculator will be familiar with the tricks students play on each other with calculators. Mind reading and number guessing games are common activities, and this was on a device with only a numeric keypad. It's little surprise that with the power of today's smartphones comes a new wave of fake apps. At one end of the spectrum are ridiculous apps such as smell sensors and digital X-ray scanners. These are usually used as jokes or pranks, typically by tricking someone into thinking that a smartphone can do things that it can't really do.

While most fake apps are used simply as party tricks, there is a class of fake apps that

are dangerous. Phishing apps, such as the fake Android banking app *released in 2010 by Droid09, attempt to trick users into entering sensitive financial information into them which can then be used to access the victim's account.*

*In general, caution is advised on the mobile phone app markets.]*With the rapid pace of technology improvements to smartphones, it's understandable that it's difficult to keep up with their capabilities. An off-the-shelf iPhone 4 includes eight different sensors:

* accelerometer

* GPS

* ambient light detector

* dual microphones

* proximity sensor

* dual cameras

* compass

* gyroscope

[Source:

"An off-the-self iPhone 4, representative of the growing class of sensor-enabled phones. This phone includes eight different sensors: accelerometer, GPS, ambient light, dual microphones, proximity sensor, dual cameras, compass, and gyroscope."

From "A Survey of Mobile Phone Sensing"

Nicholas D. Lane, Emiliano Miluzzo, Hong Lu, Daniel Peebles, Tanzeem Choudhury, and Andrew T. Campbell, Dartmouth College

IEEE Communications Magazine, September 2010

www.cs.dartmouth.edu/~campbell/papers/survey.pdf]

Even familiarity with these sensors might not clue someone in to the fact that certain apps are fake. Fingerprint scanners are a popular prank app. These apps typically require the victim to place their thumb on the touchscreen of the phone, before a "scan" is initiated and the phone alarmingly notifies everyone around that it's matched the victim's thumb print to a wanted criminal on the FBI's most wanted list, or something along those lines.

There are two main types of digital fingerprint scanners: optical scanners and capacitive scanners. The optical version is similar to a digital camera and takes a high resolution picture of the fingerprint. Capacitive scanners are indeed similar to the capacitive touchscreens on mobile phones. However, the minimal standard for basic fingerprinting identification is 250-300 pixels per inch; the FBI's standard is twice that. Who knows when mobile phone hardware will support this, but current software capabilities aren't even close. Apple's iOS touch interface, for example, only provides app developers with a single set of coordinates. Finger diameter from touches isn't even available to app developers.

Of course, this doesn't stop app developers from releasing authentication apps that require a fingerprint scan. The FingerPrint app by ThinkChange requires the user to place their finger on the touchscreen. However, the fingerprint is not actually read but the amount of time the finger makes contact with the screen is used as an authenticator. This is a much weaker authenticator than an actual fingerprint.

Ghost hunting apps straddle the line between fake and real apps. These apps claim to make use of the phone's sensors to attempt to detect paranormal activity. Detection methods typically include electronic voice phenomena (EVP) and electromagnetic field (EMF) meters. It is possible for an app to monitor trace noise from the phone's microphone and interpret the results as words, and it's possible for an app to use the phone's compass as a crude EMF meter. However, there are many natural sources of electromagnetic interference and background noise in the average home, and so it's much more likely that these sources are being captured. None of this can stop ghost hunting apps from having the entertaining power of a Ouija board. One user goes so far as to use an EVP app as a chore reminder: "Yesterday was garbage day and I forgot to bring out the trash can. The EVP tool reminded me that I need to bring it out."

While there are a lot of fake apps on the mobile markets, there are some genuine examples of ingenuity in the use of smartphone sensors. One very common application of the video camera is in barcode scanning apps. Many useful apps today are built upon barcode scanning technology such as ZXing (zebra crossing).

A recent project at UC Berkeley involved using mobile phones as seismic sensors for earthquake detection. Perhaps as accelerometer sensors improve, our phones will eventually detect and relay useful seismic information to the National Earthquake Information Center.

Though most mood ring apps leave users disappointed, a project is underway at Northwestern University to use a smart phone as a real mood detector. The project known as Mobilyze attempts to use the phone's sensors to identify a person's mood, and offer treatment for depression-related symptoms in real-time. Technology that leverages the smartphone as a personal health monitor is a trend that will likely increase in the future as phones capabilities grow. Jawbone's Up and Nike's Fuelband are early examples in this area that make use of small bracelets to track exercise and sleep patterns.

And there is a real iPhone fingerprint scanner after all. The FbF mobileOne Fingerprint Scanner is a $600 attachment for the iPhone. The FBI is currently using it. Who knows, maybe one day mobile phones will be able to scan our fingerprints with no extra hardware.

In this article I've outlined a sample of the popular fake apps so you'll be better informed the

next time someone asks to scan your fingerprint with their phone. Hopefully you've also seen that the variety of real applications that have been created utilizing mobile phones is astounding. Expect the sensors to increase in sophistication and number in the years to come, and with this the ways that app developers will make apps that improve our lives.

Mobilesecurity