Trinity Lutheran College

The Security of Near-Field-Communication

Constance Wohlford

INFO 270: Information Security

Mark Barnum

November 25, 2013

Passports, bus passes, school ID cards, cell phones, and library books all have one thing in common. They can all have NFC (near field communication) devices embedded inside (one5). These devices or chips store information about the owner of the item. Some of these, with less secure encoding, can be read with simple smart phone applications, but fortunately, some cannot. Humans seek out ways to interact with their world, and NFC is a great, secure, tool in that interaction.

Near field communication uses weak radio waves to send messages either from one device to another device, or from a chip to a device (Braue). NFC as a category includes Radio Frequency Identification (RFID). RFID devices are commonly used by veterinarians to microchip family pets. They are also used to pay commuter tolls using a sticker attached to the front window of a car. Both NFC and RFID are closely related. The primary differences between them are: RFID technology does not allow two way communication. NFC does. RFID works wonderfully over larger distances of several meters. NFC is limited to less than 10 cm. Therefore, the reading device for must be close to the sending device (Chandler). While RFID chips are already common in the United States, NFC is not yet integrated fully into common use in American society. I believe that while RFID will continue to be used, its growth potential will be limited. NFC, on the other hand has huge room to grow. It will become much more common and useful.

NFC, probably due to its slow rollout, has been rather security breach free. The advantages of NFC over other communication tools is distance, cost, and convenience. Distance is a security feature of NFC. This is because the reading device has to be close to the chip that is being read. Which means that with an NFC capable mobile phone, someone is not likely to accidently share or receive messages from a chip or device just by walking by it. Also, each phone and device can be uniquely identified. One phone can serve many NFC purposes and it can all be linked back to one handset. This is an advantage because phones are hard to duplicate. By looking at a locked phone someone could not replicate stored information the way they could if they looked into a wallet. For instance, all the information someone needs to purchase something online with a stolen credit card is accessible in most wallets; card number, billing address, card security code, etc.

NFC chips that can be read by consumer devices are about a dollar each, and likely more economical when bought in bulk. The same consumer devices can also program the chips. This eliminates expensive infrastructure, and makes NFC very convenient. Android, iPhone, and Windows phones all can come with NFC technology built in. According to Forbes.com, 50% of American adults have smart phones (Rogowsky). This makes NFC technology a convenient way to transfer information. Shoppers can place their phones near a billboard and be linked via mobile web to shopping sites, where they can look at prices or purchase the advertised item immediately. Movie goers who put their phones near a movie poster will be able to access show times for the nearest theater, or the theater of their choice.

One area that has embraced NFC technology is public transportation, though not flawlessly. The Pacific North West's ORCA card uses NFC. Commuters pay for the bus simply waving their wallets in front of the reader on the bus. There is no need to fish for cards or cash. This is an important aspect for personal safety.

Corporate security, however, has been breached. Another city's transportation system, the San Francisco Muni, was recently hacked, leading to loss of revenue. According to an article at Gizmodo.com, two men from the Intrepidus Group were able to create an Android app that allowed them "take a train card with zero rides, and refill it repeatedly, for free" (Limer). Since then the transportation companies have been warned to make the cards not rewritable. I do not know if they have yet corrected the flaw.

Another area of growth for NFC technology is to replace credit cards. The customer's phone can be passed near the NFC reader and the credit card data will be read; all without the need for a physical card taking up wallet space. The short reading distance of the technology adds to safety because the phone can be kept away from unauthorized readers. Currently, by design, NFC devices usually have to be within four cm of each other in order for data to transfer. This is a good safety feature, but, as demonstrated by the San Francisco example, it is not fool proof. According to an article in Engineering and Technology, researchers from the Department of Computing at the University of Surrey using a shopping cart as an antenna "have shown NFC data transmission between a card and a reader can be intercepted at a distance of up to 60cm - with almost 100 per cent accuracy" (Pultarova, Hayes, and Bodhani). They were able to 'sniff' the data transfer, giving them a copy of the transmitted information.

This leads to the question of what companies can do to make NFC more secure. Just as internet communication can be encrypted, NFC data should be able to be encrypted. If that is not possible then a token, time based, one time password should be included in each transaction. This way, if the transaction was intercepted, the message would only be valuable for one minute. After one minute a new token password would be required. Overall, NFC is not a technology that should be adopted prematurely. Most flaws have been discovered by researchers and the technology is improving in response to this research. Finally, smart phone users should be wary of where they place their phone, and what messages they accept. NFC should be turned off when not in use.

On the other hand, if security features are implemented I see mobile phones replacing school ID cards, credit cards, frequent shopper cards, billboard advertisements, and car keys. It is costly for colleges to replace lost programmable ID cards. It would be a lot less expensive for them to reprogram the existing NFC chip in students' cell phones. In the world of advertising, as customers walked into a shopping mall they could load to their phone all the daily specials; leading to increases in revenues to the stores and lower prices to the consumer. Another replaced item could be expensive bulky cameras. A New York Times article mentioned a prototype camera that used NFC technology to turn a phone into a large lens enabled camera, like those on SLR cameras. The phone would slide into the back of the lens and act as the brains (Pogue). This is a great idea, and shows just how exciting this technology is.

Near field communication has the potential to be a revolutionary boon to commerce, advertising, travel, and access ID technology. As with any new technology, there are potential flaws. However, this is a fortunate time because there are large communities of hackers hunting for potential weaknesses in these new systems. This has led to slower rollout of features and an increase of education to the populace. RFID, with its static information transfer, and longer range, will continue to be the primary mode for simple information transfer. NFC with its more detailed and more secure transfer will not replace RFID but will instead be implemented into more of the items we use every day. Americans will no longer be passive consumers of information but will be active in interacting with their created world.

Works Cited

Braue, David. “Inside NFC: how near field communication works” 17 Aug. 2011 APCMag.com 22 Nov. 2012 <http://apcmag.com/inside-nfc-how-near-field-communication-works.htm>

Chandler, Nathan. "What’s the difference between RFID and NFC?" 07 Mar. 2012. HowStuffWorks.com. 22 Nov. 2013. <http://electronics.howstuffworks.com/difference-between-rfid-and-nfc.htm>

Limer, Eric. “UltraReset Is an NFC-Hacking App That Hands Out Free Train Rides” 23 Sep. 2012 Gizmodo.com 22 Nov. 2013 <http://gizmodo.com/5945669/some-nfc-hackers-managed-to-develop-a-free-train-ride-app>

one5. “[List] Things to scan with your NFC Phone.” 9 Jun. 2012. XDA-Developers Forum 21 Nov. 2013. <http://forum.xda-developers.com/showthread.php?t=1701644>

Pogue, David. “A Whole New Idea: Half a Camera” *New York Times.* 25 Sept. 2013. Web. 24 Nov. 2013. <http://www.nytimes.com/2013/09/26/technology/personaltech/sonys-whole-new-idea-half-a-camera.html?pagewanted=1&_r=0>

Pultarova, Tereza, James Hayes, and Aasha Bodhani. "Is Contact Less A Soft Touch For Hackers?." Engineering & Technology (17509637) 8.11 (2013): 48-50. Academic Search Premier. Web. 24 Nov. 2013.

Rogowsky, Mark. “More Than Half Of Us Have Smartphones, Giving Apple And Google Much To Smile About” 6 Jun. 2013 Forbes.com. 22 Nov. 2013. <http://www.forbes.com/sites/markrogowsky/2013/06/06/more-than-half-of-us-have-smartphones-giving-apple-and-google-much-to-smile-about/>