Justin Loo

204 600 399

Computer Science 35L

TA: Sophia Yang

8 June 2017

Quantum Technology and Mobile Payments

Mobile payments are quickly becoming an essential part of our daily lives. They can be used to buy everything, ranging from gas to groceries to a meal at a restaurant. Basically, if the merchant or store has a compatible paying terminal, mobile payments can be used. There has been a slow adoption rate for these services in the United Kingdom amid security concerns (Oxford). They are afraid that their phones can be hacked and credit card numbers stolen. The University of Oxford hopes to alleviate these concerns with their new quantum device, seen below, which adds an even greater layer of data security to the payments (Oxford).

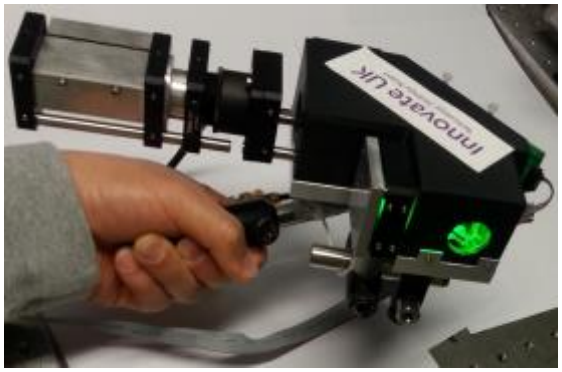

Figure 1: Prototype of the Quantum Gadget (Oxford)

A major reason for the security concerns for mobile payments lies in the data transmission technology used for the payments. Most mobile payment services, including Android Pay and Apple Pay, use near field communication, or NFC, for the data transmission (Betters; "Apple Pay Security and Privacy Overview"). NFC has a fatal flaw in that it does not detect or protect against eavesdropping (Haselsteiner 7). Eavesdropping is when hackers intercept the data that is sent before it reaches its destination. The only way to prevent the data being sent is mainly encrypting it using methods like 3DES and AES (Haselsteiner 8). Thus, even if the hackers intercept the data, they will not be able to read it easily. Google also came up with ways to combat the eavesdropping using a token based system for Android Pay. The service does not send the user's real credit card number; it sends an encrypted "token card" to the merchant along with a cryptogram for the merchant to decrypt the card (How Payments Work - Android Pay Merchant Help"). It is a one-time use card, so even if the hackers do get the card number, it will be useless. These methods appear to work for the most part, but they still do not truly solve the problem of eavesdropping.

The solution to this is the quantum gadget developed by Iris Choi and a University of Oxford collaboration, along with Nokia and Bay Photonics (Oxford). This gadget not only detects eavesdropping, but it also will shut down any ongoing data transmission if eavesdropping is detected. It works by using "movable mirrors" and "ultrafast LEDs" to send millions of particles of light as encryption keys (Oxford). There are six pairs of these LEDs with each pair being positioned and polarized differently. There is only one circularly polarized pair, and it serves as the main key while the others verify the integrity of the signal.

The gadget protects against eavesdropping by ensuring that the light particles go to an exact position on the receiver. Even if the light paths are altered a miniscule amount, the system will detect an error. Thus, if hackers try and intercept the signal, unless they find a way to perfectly retransmit the signal, they will cause the system to shut down. To make sure that the lights go to their exact positions, the researchers at Oxford University came up with an "innovative" steering system (Oxford). While making sure the lights go as intended, it also cancels out the natural motion that humans have when they are trying to hold items still. They were able to find the exact measurements of the movement and use that to calibrate the design of the system.

Now, the challenge facing the team at Oxford is trying to make the quantum gadget a component that can be put into phones. As seen in the Figure 1, the prototype is a very clunky, handheld device. In its current state, it is impossible to put it into a phone without sacrificing mobility. However, Dr. Choi believes that it is possible to miniaturize the prototype and make it a usable component in phones, an area where Nokia specializes in. This is further supported by the fact that the prototype was created using “off the shelf” materials (Oxford). It seems to me that if very little to no custom materials were needed to build it, then it should be somewhat easier to compact the technology. Yet, like with all technology, making it smaller will still be challenging.

The future of this technology does not solely lie in mobile payments. It has the possibility to be applied to other parts of phones involved with data transmission and encryption. The article states that the quantum technology could be used to create secure connections for indoor Wi-Fi networks as well as other uses for NFC (Oxford). Additionally, if this technology is adopted in mobile payments, then the hope is that the public’s trust in mobile payment security and adoption rates will grow. To me, this is the most exciting part of this article. Technology should not be impeded by fear, but if it is, then something should be done to quickly get rid of those fears. This is the what the quantum technology will do for mobile payments.

Works Cited

"Apple Pay Security and Privacy Overview." Apple Support. Apple Inc., 27 Mar. 2017. Web. 30 May 2017. <https://support.apple.com/en-us/HT203027>.

Betters, Elyse. "What Is Android Pay and How Does It Work?" *Pocket-lint*. Pocket-lint Ltd, 8 Feb. 2017. Web. 8 June 2017. <http://www.pocket-lint.com/news/135017-what-is-android-pay-and-how-does-it-work>.

Haselsteiner, Ernst, and Klemens Breitfuß. "Security in Near Field Communication (NFC)." In Workshop on RFID Security (2006): n. pag. Web. 8 June 2017. <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.475.3812>.

"How Payments Work - Android Pay Merchant Help." Google. Google, n.d. Web. 8 June 2017. <https://support.google.com/androidpay/merchant/answer/6345242?hl=en>.

University of Oxford. "New Quantum Gadget Could Make Contactless Payment More Secure." EurekAlert! N.p., 28 Mar. 2017. Web. 8 June 2017. <https://www.eurekalert.org/pub_releases/2017-03/uoo-nqg032817.php>.