BLUETOOTH SECURITY

Dennis Keritsis

I. Intro

Modern cellphone usage is becoming pervasive and is becoming integrated into people's daily lives. In order to meet the daily needs of users, mobile devices are becoming more powerful. (Jamaluddin, 2004). Also, these devices are storing more confidential information such as: phone numbers, calendar information, pictures, and the like. Personally, I like to store my doctor appointments in Google Calendar. Similarly, I like to have access to my Bank Account information through a mobile application. Lastly, the thing I love the most is my digital wallet with my plurality of credit cards. These are all juicy targets for attackers.

Further, in addition to storing confidential information, mobile devices are just storing a lot of information in general (Mitnick, 2014), including personal information about users. This allows attackers to do information gathering (i.e. recon) that may be used down the line in the attack-kill-chain in order to hack into a more secure environment such as a Bank Account or 401(k) account.

In essence, the mobile phone market is picking up where PCs left off. That is, for modern user experience, mobile devices are the device of choice. For example, mobile devices capable of using the internet and accessing email. (Jamaluddin, 2004). Personally, I check most of my email through my mobile device, not my desktop. As a result of this PC type usage, mobile devices are being exposed to the same types of attacks as PCs since mobile devices are essentially small computers. (Kaur, 2020). For example, Trojans may be launch through Bluetooth (Jamaluddin, 2004), wherein Trojans were traditionally found on the PC.

This paper will discuss vulnerabilities related specifically to Bluetooth technologies since Bluetooth is becoming more pronounced in society today due to mobile usage. (Kaviarasu, 2016). That is, Bluetooth is a new attack vector for mobile devices. (Kaviarasu, 2016).

II. What is Bluetooth

It is important to start with the PHY layer when talking about Bluetooth. Put simply, Bluetooth is just radio waves. Bluetooth is inherently vulnerable given that the radio waves are freely available and can be sniffed by anyone with an antenna or the right hardware. (Kaur, 2020). In the past, computers only talked with one another through a wired connection. (Kaur, 2020). In modern day, many user devices have wireless capabilities. For example, 77% of Americans in 2011 had a smart phone and the majority of smart phones have Bluetooth. (Lonzetta, 2018). To show how pervasive Bluetooth technology is, a team of Researchers visited a public place and placed a Bluetooth sniffer inside the suitcase. Just within 10 meters of the suit case, the Researchers could pick up on 1400 devices in 23 hours (Lonzetta, 2018). In short, Bluetooth is inherently vulnerable given that is just transmitted radio waves and members of the public, including attackers, can freely read information encoded in those radio waves.

III. Bluejacking

III (A). Bluejacking What is Bluejacking

The first type of attack to be discussed is Bluejacking. Bluejacking is a coined term made up of "Bluetooth" and "Ajack." (Bhatia, 2014). Originally, vCards were to be used for business purposes only and where introduced in 1996. (Kaviarasu, 2016). However, over time the "hack" of sending unsolicited messages using the vCard scheme developed. (Browning, 2009; Kaviarasu, 2016). The hack being, the sending of unsolicited messages. That is, Bluejacking is not a hack in and of itself. Rather, it is a form of spam that is sent to users by hijacking the vCard's original use. (Bhatia, 2014). Again, as noted above, spam is something that is typically associated with PC usage, not mobile devices.

III (B). Bluejacking Technical

Bluejacking typically occurs within crowded areas. (Lonzetta, 2018). This makes sense since Bluetooth technology range cannot go above 100 meters. (Khanpara, 2015). When Bluetooth is in range, Bluejacking works by leveraging the OBEX protocol (Bhatia, 2014; Browning, 2009; Kaur, 2020) sometimes with the vCard (Browning, 2009). Typically the vCard with the "from" field is left blank or replaced with a message (Kaur, 2020) to provide anonymity. (Jamaluddin, 2004; Kaviarasu, 2016).

OBEX is a session layer protocol (Kaur, 2020) or a type of transfer protocol. (Kaviarasu, 2016). Similar to HTTP, OBEX has both push and pull mechanisms. (Kaur, 2020). In contrast to HTTP, OBEX is more balanced when it comes to pushing a pulling whereas HTTP is more pull. (Kaur, 2020). Additionally, the OBEX protocol is used in ad hoc networks to exchange data such as file, pictures, and the like. (Kaur, 2020). In order for the OBEX protocol to be leveraged, devices must be paired. (Jamaluddin, 2004; Khanpara, 2015; Musale, 2012).

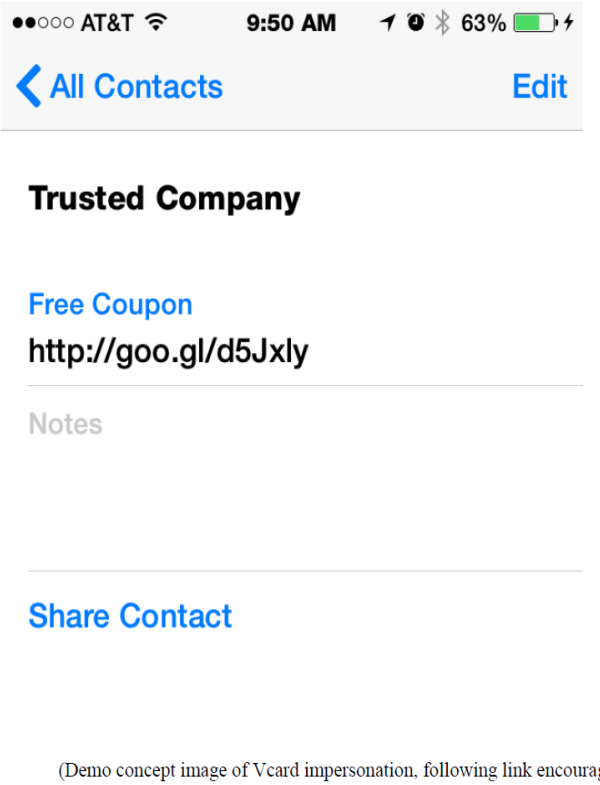
III (C). Bluejacking Spam or DoS

If the victim does pair, the spam/hack will follow. However, no damage per se will occur in a vacuum. It can be viewed as a type of DoS attack since it is spam. A DoS attack from Bluejacking is called Blueballing. (Mitnick, 2014). This spam is an annoyance or joke. (Bhatia, 2014; Kaviarasu, 2016; Khanpara, 2015). Although, within our CIA triad, a flurry of Bluejacking messages might interfere with the "Availability" of others legitimate Bluetooth devices from connecting. (Bhatia, 2014). Either way, there is still social loss that can occur due to be many users being bombarded with spam or DoS.

Sometimes this spam is not intended as a joke, but rather, it is a type of guerrilla marketing tactic. (Kaur, 2020; Khanpara, 2015). With respect to marketing, marketers might use Bluejacking for location base services. (Khanpara, 2015). For example, a customer might be shopping at a super market and the super market might notify users of specials while they are shopping. (Khanpara, 2015). These messages are unsolicited and therefore are categorized as Bluejacking although they might serve some positive social function.

III (D). Bluejacking Damage with URL

As noted above, Bluejacking is not a hack per se. However, Bluejacking used in conjunction with social engineering may cause harm to the victim of the Bluejacking attack. Bluejacking uses the vCard scheme. (Browning, 2009), wherein the vCard scheme allows for URLs to be entered. (Bhatia, 2014; Kaviarasu, 2016; Mitnick, 2014). As such, the URL might lead to a pernicious website to install a type of virus on the mobile device. (Jamaluddin, 2004.)



(Demo concept image of Vcard impersonation, following link encouraged)[14]

Figure 1 Reproduced from Mitnick, 2014 showing URL embedded in a vCard

Similarly, Bluejacking can also deliver Trojans. (Jamaluddin, 2004). In both of the examples of Trojans and Viruses, these are items typically associated with PCs, not mobile devices. (Jamaluddin, 2004). Lastly, Bluejacking may also deliver overflow attacks which affect the cache of the mobile phone with some older OS models. (Mitnick, 2014). Again, mobile devices are being the targets of hackers as mobile devices continue to server a PC type function for users in the day-to-day activities.

IV. Bluesnarfing

IV (A). Bluesnarfing What is Bluesnarfing

Both Bluejacking and Bluesnarfing are types of hijack attacks. (Kaur, 2020). However Bluesnarfing is much more dangerous. (Kaur, 2020). Bluesnarfing is defined as the process of gaining unauthorized access through pairing and gathering confidential information. (Mitnick, 2014).

IV (B). Bluesnarfing Technical

Bluesnarfing utilizes a OBEX push (Browning, 2009) or connects with the OBEX transfer protocol and pairs with the device. (Lonzetta, 2018). This can be seen in the figure by Lonzetta, 2018.

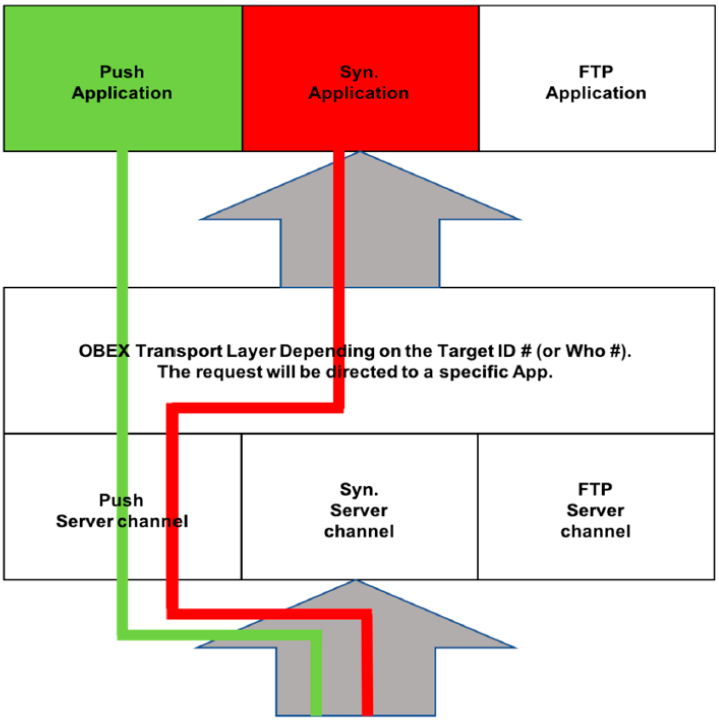


Figure 10. BlueSnarfing Attack.

Figure 2 reproduced by Lonzetta showing an OBEX push

When SSP pairing is used by the potential victim, as opposed with legacy PIN paring, an attack might still be able to pair with social engineering. (Mitnick, 2014). For example, an attack could add the label of "SAMSUNG_HANDSFREE" when there is pairing request while at a cell phone store.[1] (Mitnick, 2014). Generally the device needs to be in discoverable mode before launching an attack (Browning, 2009). However, Bluesnarfing may also occur in non-visible mode. (Jamaluddin, 2004). An attack also needs a Bluetooth MAC address[2] (Martínez, 2011), and this can be done with "BlueScanner" from Aruba Networks. (Martínez, 2011).

IV (C). Bluesnarfing Attack

Once the attacker has access, Bluesnarfing allows an attacker to right and write to the file system of the phone (Browning, 2009) though a data link. (Martínez, 2011). Further, this attack can

[1] This is very similar to spoofing a valid SSID such as "Starbucks Guest" at a Starbucks whereby a victim could connect to a rouge or evil twin access point.
[2] Martinez uses the language of MAC address but this is probably the same thing as the BD_ADDR.

occur without any trace of the attack to the victim. (Jamaluddin, 2004). As noted above, mobile devices contain very important confidential information, and Bluesnarfing would allow an attacker to access contact, calendar information, and images. (Lonzetta, 2018). Also, a link may be set up between multiple devices creating a man in the middle attack (MITM). (Mitnick, 2014.) In our class, it was noted that our Keyboards might be paired with a malicious device and monitor our key stokes. One possible way to attack the victim would be to pair between the keyboard and the computer and launch of MITM attack. An attacker would intercept the key strokes from the keyboard searching for sensitive passwords (e.g. passwords for bank accounts).

V. Bluebugging

V (A). Bluebugging What is Bluebugging

Bluebugging is an attack that can do everything Bluesnarfing can do, but more.(Hossain, 2011) That said, Bluebugging is one of the most power attacks on Bluetooth (Browning, 2009; Hossain, 2011) since it can take control over the victim's phone. (Browning, 2009). Further, it can connect to the victim without ever being noticed (Lonzetta, 2018), and execute commands as if he was the owner of the device (Lonzetta, 2018).

V (B). Bluebugging Setting up Connection

Bluebugging uses the AT command parser that can send AT commands (Lonzetta, 2018) while using the RFcomm protocol (Lonzetta, 2018). Specifically, Bluebug exploits a vulnerability caused by a bug in the implication for the Bluetooth stack by connecting to the RFcomm serial port of the phone. (Martínez, 2011). Thereafter, the attackers cause AT (Attention Terminal) commands to give instruction

to the mobile device. (Martínez, 2011). This establishes a serial connection (Martínez, 2011). When in control, the attacker may make calls, read SMS, read and write to contact lists, phone numbers, connect to the internet, and forward calls. (Browning, 2009; Hossain, 2011).

V (C). Bluebugging with Social Engineering

Call forwarding is particularly interesting because this attack could be coupled with social engineering. With a Bluebugged serial connection, the attacker could do recon by looking at a list of mobile applications and discover a banking application (e.g. Chase banking app). The attacker could reasonably ascertain that the user probably has a bank account associated with a specific bank (e.g. Chase). Further, the use might have a bank in the contact list and come to the same conclusion. Regardless of the method used, the attack could determine what financial institutions the victim is associated with.

That said, the attacker with the AT commands could set up call forwarding such that when the user calls their financial institution (e.g. Chase bank) it forwards them **to the attacker's line**. At this point, the user is under the impression they are talking to a financial institution representative, and would be willing to disclose all their personal information such as routing number, account number, social security number, telephone, address, birthdays, and the like. Simply put, coupling call forwarding with social engineering can have deleterious effects!

VI. Countermeasures

VI (A). Countermeasures and Updates

The paper at this point has focused on exploits. From 2003-2008, many Bluetooth exploits occurred. (Mitnick, 2014). However, when Bluetooth v2.1 came out, this addressed many of the security flaws discussed above and introduced SSP. (Mitnick, 2014). Further, encryption and the link layer protocols during the paring process were updated, and this was in part due to the release of the NIST Guide of Bluetooth Security. (Mitnick, 2014). As such, it is important for users to keep their devices up to date, and purchase new versions of mobile devices. Many users have the mentality of "if it works do not fix it." That is, if they are comfortable with their phone, they will continue to use it. However, legacy devices are more vulnerable given firmware/hardware constraints. Accordingly, users need to trash their old phone and upgrade in order to maintain security. Additionally, security might range from vendor to vendor. For example, iOS since 2007 has been immune to bluejacking (Mitnick, 2014). That is, iPad and iPhone restriction Bluejacking. (Kaur, 2020). Old Nokia models were suspensible to Bluesnarfing and Nokia was aware of it and fixed it with firmware update (Musale, 2012).

Table 2. The relationship between attacks and telephones.

Mobile phone	Bluejacking	BlueSnarfing	BlueBug	BluePrinting
Xpress music 5610	X	X	X	X
Nokia 6131	X	X	X	X
Motorola WX295		X		X
Blackberry 8220		X		X

Figure 3 reproduced from Martinez comparing phones from vendors

VI (B). Countermeasures and Wireless

Bluetooth is more secure than 802.11 protocol due to weak WEP and WPA protocols. (Musale, 2012). Further, Bluetooth uses FHSS which has roots in military anti-jamming technology. That is, due to the spread spectrum, the information is not on any specific channel in the ISM. This is in contrast to the 802.11 protocols that typically use OFDM. With this noted, the PHY layer offers an inherent level of

protection because sniffing Bluetooth is not easy since attacker devise must be in sync (i.e. be on the same piconet after pairing). Therefore, when v2.1 came out with SSP, (Mitnick, 2014), attacker either has to break SSP, either with social engineering or technical methods, in order to get on the piconet.[3] This made Bluetooth over all more secure since many exploits can take place during the paring process.

VI (C). Countermeasures and Personal Action

Even though Bluetooth is secure, there are plenty of active steps individuals can take and developers can take. This includes a laundry list of items such as: turning off Bluetooth when not in use (Kaur, 2020; Musale, 2012); keeping distance with strangers (Kaur, 2020); resetting the phone if hacked (Kaur, 2020); using strong passwords (Kaur, 2020); designing a friendly UI that allows users to manage Bluetooth settings (Lonzetta, 2018); operating at low power (Lonzetta, 2018); using SSP instead of the legacy PIN pairing (Lonzetta, 2018); and denying a vCard you do not know (Mitnick, 2014).

VII. Conclusion

Bluetooth devices are essentially are on every smart phone. The paper discussed only three exploits through Bluetooth and noted that v2.1 remedied many of these attacks. However, there is no such thing as a perfectly secure device, and even new devices such as the I-phone 12 will always have vulnerabilities that will be discovered. In the end, however, users should educate themselves not on the myriad of different types of attacks. Rather, users of mobile device should become aware of social engineering tactics and have a basic understanding of how their devices operate in order to protect

[3] Alternatively, an attack could use a wide band receiver but this type of hardware can be expensive on the order 10,000 dollars plus.

themselves. By taking simple security measures, like turning off Bluetooth in a public setting, users can protect themselves.

References

Bhatia, P. (2014). An Outlook on Bluejacking Technology. *International Journal of Engineering Research & Technology (IJERT), 3*(4).

Browning, D., & Kessler, G. (2009). Bluetooth Hacking: A Case Study. *Journal of Digital Forensics, Security and Law*. doi:10.15394/jdfsl.2009.1058

Hossain, H. (2011). Modified Approach of RFCOMM Implementation to Protect Bluetooth Technology from Bluebug Attack. *IJCIT, 1*(2).

Jamaluddin, 2004, J., Zotou, N., Edwards, R., & Coulton, P. (2004). Mobile phone vulnerabilities: A new generation of malware. *IEEE International Symposium on Consumer Electronics, 2004*. doi:10.1109/isce.2004.1375935

Kaur, A. (2020). BLUEJACKING: ITS OVERVIEW, PROCESS OF BLUEJACKING AND PREVENTIVE MEASURES. *JETIR, 7*(5).

Kaviarasu, 2016. (2016). (PDF) Bluejacking Technology: A Review - ResearchGate. Retrieved December 13, 2020, from https://www.researchgate.net/publication/314233155_Bluejacking_Technology_A_Review

Khanpara, 2015, P. (2015). Bluejacking: Pimal Khanpara, 2015 , Param Khanpara, 2015. Retrieved December 13, 2020, from https://www.scribd.com/document/456552659/BlueJacking-Academic-Science-pdf

Lonzetta, 2018, A., Cope, P., Campbell, J., Mohd, B., & Hayajneh, T. (2018). Security Vulnerabilities in Bluetooth Technology as Used in IoT. *Journal of Sensor and Actuator Networks, 7*(3), 28. doi:10.3390/jsan7030028

Martínez, B. L. (2011). Direct attacks on mobile phones by bluetooth for forensic analysis. *Scientific Research and Essays, 6*(30). doi:10.5897/sre10.1098

Mitnick, D. (2014, December 12). Into the Blue Depths - Department of Computer Science. Retrieved December 13, 2020, from http://www.cs.tufts.edu/comp/116/archive/fall2014/dminnick.pdf

Musale, V., & Apte, S. S. (2012). Security Risks in Bluetooth Devices. *International Journal of Computer Applications, 51*(1), 1-6. doi:10.5120/8003-1308