Human Centred Security - Individual Essay

Joseph Cameron

Essay: The use of smart speakers to control home security systems
Essay Word Count (Excluding References): 1622

Recently, smart speakers such as Amazon Alexa, Google Home and Apple's newly released HomePod have exponentially increased in popularity. It is now estimated that one in six (39 million) Americans owns a smart speaker [1]. Smart speakers typically accept user voice commands and carry out various tasks with respect to those commands. Common use cases for smart speakers include reading emails, online shopping and general everyday queries that can be answered by search engines. However, these smart speakers are quickly finding evermore use cases, one of which is home security, where the speaker is the medium through which a user can secure their home. Recent systems such as ADT Pulse allow users to issue voice commands to Amazon's Alexa in order to activate or deactivate locks, arm or disarm alarm systems and even change various household settings such as lighting and temperature [2][3]. While the integration of smart speakers in home security may be fun, exciting and seamless, it may pose many usability, privacy and security issues. It is important to start identifying and understanding these issues in order to propose practical solutions.

A major security issue can be instantly identified in the integration of Amazon Alexa with ADT Pulse. To perform any 'secure' actions, by the standards of ADT, a user typically has to verbalise their four-digit PIN after certain commands. An example of such a command from the ADT Pulse website could be, "Alexa, ask ADT to disarm the system with PIN 1911" [3]. Obviously, if a guest is present while issuing such a command, the user's PIN would be compromised along with the exact command needed to perform the action. This also presents a usability issue, as users may be less willing to interact with their home security systems in fear of compromising their PINs in the presence of guests, leading to an unhealthy reinforcement of refusal to secure their homes. Of course, the heart of the issue here is the action of revealing secret authentication information by speaking it out loud. According to ADT, these actions are justified as they best utilise the capabilities of Amazon Alexa to provide the user with a more comfortable, hands-free experience to secure their home [3]. However, on a more serious note, if an unknown external attacker could record these crucial commands with a carefully placed or hidden device such as a microphone, the security of a user's home is severely compromised. Unwanted access may be readily granted by just repeating the same commands and corresponding PINs for each particular security task. To avoid speaking the PIN out loud, it may be wise to consider prompting the user to enter the PIN via a traditional keypad interface before accepting security-related commands. Although this degrades the hands-free experience ADT Pulse seeks, it crucially prevents the PIN from becoming compromised due to simple eavesdropping.

This observation brings another issue into view that is directly associated with the use of the smart speaker itself. One advantage of owning a smart speaker is that anyone can ask it to complete tasks. However, this means that anyone, and I repeat, anyone, can use the smart speaker to reveal private information, such as emails, about the account it is linked to or even purchase items if purchasing mode is on [7]. Of course, there are privacy and security issues associated with this feature. In the context of home security, this means an intruder could go undetected and ask the speaker to carry out a multitude of tasks involving the home security system without any question [8]. In an everyday context, it is beneficial to seamlessly interact with a smart speaker to access many wells of information, including private information, and companies such as Amazon and Google continually push these use cases in their advertisement of the smart speakers [9][10]. Although, a more prominent effort should be made, by organisations such as Amazon, to effectively communicate the potential implications of so little authentication for certain services especially when concerning issues of high importance, such as home security. This issue can be solved though through giving users the option of compartmentalised authentication,

where specific services such as home security and email are only accessible after appropriate authentication measures. After all, no one would ever like to know that their email account can be accessed without a password, so why allow this to be the case through a smart speaker when a stranger visits your home?

Another issue with smart speakers takes the form of a privacy issue that is directly linked to the functionality of smart speakers themselves. Many smart speakers store recordings of user commands on servers located within company headquarters [6]. Furthermore, many smart speakers never stop recording, according to their default settings, leading to potential exposure of users' most private and intimate conversations without the user necessarily being aware or explicitly consenting [8]. Again, concerning the ADT Pulse system with Alexa integration, every security-related command involves waking Alexa first. The wake word for Alexa is 'Alexa', and from then on the speaker will record your speech and store it on Amazon's servers. This means that when using ADT Pulse, the security commands including the PIN are all stored on a server as audio. If these servers were to be hacked, there could potentially be many, many homes at serious risk. The only way to alleviate the damage from a user's point of view is to delete recordings that Alexa has taken regularly. However, the procedure required to do so is not made clear to the user unless the user explicitly knows that they wish to delete voice recordings. This highlights a clear usability issue, as many users may not be aware of Alexa's actions due to a lack of communication from Amazon's default settings [11]. In fact, once the procedure to delete recordings has been found, Amazon may display a message discouraging the user from doing so [6]. Obviously, the improvement of Alexa's performance depends on Amazon having access to as much raw training data as possible, so they are understandably reluctant to allow users to delete recordings so easily. However, Amazon must communicate the implications of not regularly maintaining voice recordings more effectively, so customers can understand what happens to the data collected by Alexa, and thus provide information for deleting recordings more readily to the casual everyday user. Once users have more control over what information may be available about their home security systems, there may be less damage if, for example, Amazon's servers were attacked.

A couple of glaring security and privacy issues have been identified with smart speakers, although the smart home security systems themselves also have a few usability issues. For example, the ADT Pulse system [3] requires precise commands to carry out essential security operations. These commands also heavily depend on particular settings and names that have been specified in the ADT Pulse app. Every Pulse device, which can be a lock or a garage door, has its specific name, and security actions will only be taken if the name is perfectly spoken [4]. For one or two Pulse devices, this may not be a big issue. However, if a user decides to expand their smart homes to include more than ten Pulse devices, the user may find the task of remembering these names very mentally taxing. As shown by Ryan West [5], the usability of a system significantly impacts the overall security of a system. A user who feels hindered by specific security measures may become discouraged to interact with security at all, and this could lead the user into a vicious cycle of disinterest for security measures, which is entirely against the point of a smart home security system in the first place. A security blogger from California correctly identifies the issue with this phenomenon in the Amazon Alexa ADT Pulse system [4], as they describe feeling temporary frustration when Alexa would only respond to perfect and precise commands. The main usability issue with issuing voice commands to a smart speaker is that there is no interface where the user can be assisted in remembering the details of the system. This could be solved by allowing Alexa to reveal the names of all Pulse devices at will, but then this may introduce the same security issues that have been identified in

previous paragraphs, where an intruder could potentially access all information concerning the home security system.

Overall, it is clear that in a security system, the system is only as secure as the weakest link. In terms of securing a home through the use of a smart speaker, this means that a home is only as secure as the smart speaker used to secure it. Throughout this essay, many potential security, privacy and usability issues with the use of smart speakers in the context of home security have been identified. Unfortunately, the suggested solutions to all of these identified issues follow a pattern of fundamentally degrading the advantages of using a smart speaker in the first place. For example, the best solution to preventing a verbal recording of authentication secrets is not to verbalise the authentication secret. Similarly, all other suggested solutions to the identified issues effectively void the hands-free experience a smart speaker offers, thus questioning the role a smart speaker could play in home security. The purpose of a smart speaker is to assist users in their everyday life effortlessly. Although, tasks such as home security should not be taken so lightly, as the consequences of lousy home security are far more severe than an accidental order for cat food [12]. It is clear that home security is possible through the use of a smart speaker. However, the most secure method of securing homes given today's technology may not be as hands-free as Alexa would like.

References:

[1] Sarah Perez. 2018. 39 million Americans now own a smart speaker, report claims. (January 2018). Retrieved February 16, 2018 from https://techcrunch.com/2018/01/12/39-million-americans-now-own-a-smart-speaker-report-claims/

[2] Jason Cipriani. 2017. ADT taps Amazon's Alexa for Pulse system control. (May 2017). Retrieved February 16, 2018 from http://www.zdnet.com/article/adt-taps-amazons-alexa-for-pulse-system-control/

[3] ADT. ADT Pulse and Amazon Alexa Home Security and Home Automation. Retrieved February 16, 2018 from https://www.adt.com/alexa

[4] Greg Barker. 2017. Alexa Has a New Skill: ADT Pulse Security and Home Automation is Listening. (April 2017). Retrieved February 26, 2018 from http://www.californiasecuritypro.com/blog/alexa-has-a-new-skill-adt-pulse-security-and-home-automation-is-listening

[5] Ryan West. 2008. The Psychology of Security. Commun. ACM 51, 4 (April 2008), 34-40. Retrieved February 26, 2018 from DOI: https://doi.org/10.1145/1330311.1330320

[6] Rory Carroll. 2015. Goodbye privacy, hello 'Alexa': Amazon Echo, the home robot who hears it all. (November 2015). Retrieved February 26, 2018 from https://www.theguardian.com/technology/2015/nov/21/amazon-echo-alexa-home-robot-privacy-cloud

[7] Lory Gil. 2017. How to stop Alexa from ordering stuff without your permission. (January 2017). Retrieved March 5, 2018 from https://www.imore.com/how-stop-alexa-ordering-stuff-without-your-permission

[8] Herb Weisbaum. 2017. 'Hey Alexa, how secure are voice-activated assistants like you?'. (November 2017). Retrieved March 5, 2018 from https://www.nbcnews.com/tech/security/hey-alexa-how-secure-are-voice-activated-assistants-you-n824566

[9] Tim Nudd. 2016. Amazon Made More Than a Hundred 10-Second Ads Asking Alexa the Funniest Things. (October 2016). Retrieved March 5, 2018 from http://www.adweek.com/creativity/amazon-made-more-hundred-10-second-ads-asking-echo-funniest-things-173901/

[10] Rebecca Stewart. 2017. Google is making a play to own the smart home, but can it echo Amazon's early triumphs?. (May 2017). Retrieved March 5, 2018 from http://www.thedrum.com/news/2017/05/08/google-making-play-own-the-smart-home-can-it-echo-amazon-s-early-triumphs

[11] Kim Komando. 2017. 3 essential privacy settings for your Amazon Echo. (December 2017). Retrieved March 6, 2018 from https://www.usatoday.com/story/tech/columnist/komando/2017/12/08/3-essential-privacy-settings-your-amazon-echo/933944001/

[12] Maham Abedi. 2018. Amazon Echo mistakenly orders cat food after hearing TV commercial. (February 2018). Retrieved March 6, 2018 from https://globalnews.ca/news/4025172/amazon-echo-orders-cat-food-tv-commercial/