The Internet of Things is the network of devices such as vehicles and home appliances that can connect, interact and exchange data. The concept of IoT, explained simply, means adding internet connectivity to a system of interrelated computing devices, mechanical and digital machines, objects, animals, and/or people. By connecting to the internet, things become smarter because they have the ability to send or receive information. However, devices that connect to the internet may bring about a number of serious vulnerabilities if they are not properly protected. Therefore, IoT security, the act of securing connected devices and networks in the IoT, is crucial.

The biggest and most obvious security challenge with IoT devices is the inability to easily upgrade or patch them. In all software there exists the possibility for undiscovered vulnerabilities. However, the discrepancy is that even though some companies are able to remotely patch things like routers and modems, this is rare (Schneier, 2018, p.37). Even worse, various embedded devices have no way to be patched. Additionally, security patches are rarely released immediately by vendors when the vulnerabilities are disclosed. In 2016, one survey found that about 20% of all vulnerabilities were not solved through corresponding available patches the day of disclosure. Of the rest, only 1% will be patched within a month, indicating that many vendors may never issue a patch (Schneier, 2018, p. 38).

Experts predict the number of IoT devices will reach 75 billion by 2025 (Newgenapps, 2018). As IoT advances into our everyday lives, the more insecure and vulnerable the embedded devices are, the more risk the critical systems and data around the world will have. Hackers can launch attacks to cripple infrastructure, down networks, and infiltrate and leverage thousands or millions of unsecured devices (IoTforall, 2017). Those attacks may very well put human lives and property in jeopardy. The seriousness of this problem can be seen from the following real world examples.
On October 21, 2016, the Dyn cyberattack, a series of distributed denial-of-service attacks (DDoS attack), targeted the servers of Dyn, a company that controls much of the internet’s domain name system (DNS) infrastructure. The Dyn cyberattack brought down almost all Americans’ internet, as well as sites such as Twitter, the Guardian, Netflix, Reddit, CNN, and many others in Europe and the US, by using a new weapon called the Mirai botnet. Unlike many other botnets, the Mirai botnet is made up of IoT devices such as digital cameras and DVR players. What makes this especially problematic is that there are huge number of vulnerable IoT devices that can be infiltrated by the Mirai attack. Therefore, Mirai was the “primary source of malicious attack traffic,” according to a blogpost by Dyn, and its DDoS attack was the largest of its kind in the history, as many experts said (Woolf, 2016).

The more frightening fact is that hacking can endanger human health. On January 9, 2017, the FDA confirmed that St. Jude Medical's implantable cardiac devices, such as pacemakers, defibrillators, and resynchronization devices, have the vulnerabilities to get cybersecurity intrusions and exploits. The St. Jude Medical's Merlin@home Transmitter is an IoT device that transmits and receives signals connecting to the patient's implanted cardiac device and reads the data stored on the device. If vulnerabilities exist in this product, they can be exploited by allowing unauthorized users to remotely access the device and modify code in the implanted device which can deplete the battery and cause incorrect pacing or shocks (Larson & FDA, 2017). Right behind the St. Jude cardiac devices is the Owlet WiFi baby heart monitor, “the worst IoT security device in 2016”, according to the Register. Top computer security researcher Jonathan Zdziarski bought the Owlet to monitor his baby’s vital signs, but discovered that the wireless network can be accessed without authentications, which means anyone can control the system, monitor the babies, and silence the alert (Thompson, 2016).

Numerous examples show the importance of IoT security as it becomes more and more ubiquitous, and the urgency of improving IoT security as its failures increasingly affect people’s lives, property, and health.

Patching is an important security paradigm that allows for problems, including security vulnerabilities, to be fixed post-production, resulting in improved security for the software.
These security vulnerabilities are dangerous and can have significant and far reaching impacts. For example, malware can be made to target these vulnerabilities, using it to access the software and do things such as “allowing hackers to take unauthorized control of your computer,” according to Norton Antivirus. Additionally, malware can also “install spyware that steals sensitive information from your computer” (“Zero-day”, n.d.). While these affect a single computer, in the age of IoT, this malware can have a much greater real world impact. For examples, hackers can use vulnerabilities to shut down power plants, take control of cars or impair pacemakers (Schneier, 2018, p. 1-2,4). There are multiple factors contributing to this paradigms failure.

Firstly, companies that make IoT products are rarely security oriented, favoring faster turnaround and maximum profit. As Schneier points out, “companies don’t reward security quality in the same they reward delivering products ahead of schedule and under budget” (Schneier, 2018 p. 20). Additionally, these products are often shipped with a myriad of bugs that were not fixed during production, which often have the possibility of becoming a security vulnerability (Schneier, 2018, p. 20-21). Often times these companies make products where there is no way to make patches, which leaves them permanently vulnerable to exploits (Hawkins, 2018).

Another contributing factor to this problem is that even when exploits and vulnerabilities are found, they rarely make it to the public eye. For example, the NSA and other espionage organizations will often not release exploits they have found so that they can potentially use them for offensive attacks at some time in the future (Schneier, 2018, p. 162-163). Additionally, researchers whose goal is to find these vulnerabilities face a myriad of restrictions and disincentives when trying to research or release information about a software. Regulations such as DMCA (Digital Millennium Copyright Act) and the CFAA (Computer Fraud and Abuse Act) mean that researchers can face legal ramifications for publishing information about software, including any vulnerabilities it may have (Lawrence, 2017). Another disincentive for researchers is that academic institutions and security firms that may otherwise fund them are hesitant to do so for fear of legal repercussions or inability to publish the findings (Jones, 2016). Even when
researchers wish to contact the company directly, instead of publishing the results to the public, they still face issues. In a report commissioned by the IoT Security Foundation, it was found that more than 90 percent had no form of public vulnerability disclosure policy, meaning that researchers had no direct way to contact them about found exploits (Winder, 2016). While not being able to publicly post the details of a vulnerability online seems like it would be beneficial, as hackers would not be able to easily find said information, researchers take this route for a reason. When researchers disclosed vulnerabilities to the vendors only, and even when they publicly disclosed that the software had a vulnerability, the company would do little if anything to remedy the problem (Schneier, 2018, p. 35). Researchers found that “the only solution that spurred vendors into action was for researchers to publish details about the vulnerability” and as such “publication has become the stick that motivates vendors to quickly release security patches” (Schneier, 2018, p. 35) This push against exploits being made known to the public also contributes to another issue that is preventing the patching paradigm from being successful.

Lack of consumer cooperation and knowledge contributes to the ineffectiveness of patching. Simply put, patches are useless if they are not installed. Some users simply don’t know how to update their software, or ignore reminders to do so (Armerding, 2012). Others intentionally do not patch, often for fear of breaking other critical applications (Grimes, 2016). Other reasons consumers have for not patching include fear of it slowing down their computer or it being buggy (Armerding, 2012). Others still do not patch because they do not understand what the upgrade will do or believe it has no benefit (Armerding, 2012). This lack of education means that patches are not installed when they should be, leaving vulnerabilities active that would otherwise be fixed. It is likely that more users would patch if they understood the security ramifications of the updates, which would improve the effectiveness of the patching paradigm. Regardless, the paradigm itself is insufficiently implemented for it to be effective, causing negative impacts on IoT security.

With the convergence of various causes discussed above, there emerge many possible solutions that address the disparate problematic roots. These solutions tend to fall into the frames of market solutions or government solutions.
The first question one might ask when searching for solutions is how this problem may be addressed, if at all, by the free market.

The plight of IoT security has sprouted a plethora of IoT security companies (“Internet of Things Security Market”, n.d.). A report by Grand View Research finds that identity and access management is responsible for 32.7% of revenue for the IoT security industry, which was worth $1.24 billion globally in 2017 (“Internet of Things Security Market”, n.d.). Identity and access management ensures that the owner of the device is the only person who can access the device. Approaches can vary from enforcing complex authentication chains to simply avoiding a default password. While identity and access management is an important first step, cyber security expert Daniel Elizalde says a good solution should address security issues on all levels of the stack (Elizalde, 2018).

With a full stack solution in mind, some companies such as IOActive offer to find security flaws in your products. Assuming these IoT security companies are capable, there appears to be ample chance for companies, even those inexperienced with security, to get IoT security right. The problem is that these services come at a price, and often one too expensive for smaller brands. As Schneier writes, “the companies involved [with developing IoT products] simply don’t have the budget to make their products secure, and there’s no business case for them to do so.” (Schneier, 2018, p. 39). The lack of a business case comes from IoT companies not tending to compete on security (Schneier, 2018, p. 39). An effective market solution would therefore develop the business case infrastructure by educating consumers about the importance of IoT security.

One approach to address consumer ignorance about security is through automatic updates. With automatic updates, the consumer does not need to have any knowledge about the update taking place nor skill with embedded devices. An example that Schneier gives of this occurring in the market is how Tesla’s automatic updates gives it an advantage over Chrysler, which had to mail a USB drive with an update to every owner (Schneier, 2018, p. 38). Schneier suggests that market forces will gradually push companies toward automatic patching (Schneier, 2018, p. 38).
While automatic updates may carry value in the market, a non-solution is for the government to require companies with IoT products to have automatic updates. Automatic updates put devices at risk of becoming a botnet if a hacker compromises the update authentication (Tozzi, 2017). Based on their industry type, frequency of patches, and content of patches, companies should make this choice for themselves.

A more practical government solution than automatic updates is to incentivize companies to support products for longer periods of time. The government has already made progress in this vein by providing security researchers with an exemption to DMCA (“DMCA security”, 2016). This should incentivize researchers to find vulnerabilities and encourage companies to patch them or risk a poor brand reputation.

Tying in with fostering consumer demand for security, incentivization could mean requiring companies to make clear to consumers how long their products are supported with updates and can be reasonably expected to be secure. A flaw in this approach is that it becomes difficult to legally define how much effort companies should expend on updates and what should be considered reasonably secure. If Congress were to pass such a law, the executive branch would be responsible for clarifying these expectations.

A less ambitious incentivization avenue is requiring companies to make products patchable. As discussed above, some products have no patch support from the developer. As Schneier puts bluntly, “Right now, the only way for you to update the firmware in your hackable DVR is to throw it away and buy a new one.” (Schneier, 2018, p. 37). Congress passing a law requiring patchability would be a purposeful early step incentivizing companies to maintain IoT products. A law would have to address the infrastructure of the patchability, which gets complicated. How (and should) users be notified of a patch? Would it be acceptable to mail a USB to users? How can you provide a patch if some devices do not have stable connection to the internet?
Whatever the specifics of the approach, the sooner we enact it the better as IoT products have indefinite lifespans and historically unsupported products may contribute to security issues for years to come.

We’ve discussed potential solutions to this problem, but we need to evaluate which are the most feasible and which have the most desirable outcome. In general, it’s important to know: how do we determine if a solution is effective once we’ve implemented it?

The effectiveness of a solution can be evaluated by a set of criteria. One, standardization of automatic updates. As discussed, many users either don’t understand or ignore opportunities to allow updates to their IoT software. Making these updates automatic removes the user as a point of failure in the security of these devices. As a result, critical vulnerabilities in the software are much less likely to be persist if the default option is to install the patch instead of not to install the patch.

Another criterion is the ability of security researchers to examine software for bugs. But the financial disincentive, running into copyright laws (DMCA, CFAA), public image, and many other factors contribute to a lack of research on buggy IoT technology. If we want to see an improvement in the quality of this technology (and a resulting improvement in security), then we need to promote research.

The last and arguably most important criterion is that we see companies held responsible for flaws in their security. Changes in government are most likely the best way to accomplish this. The corporations who develop buggy IoT software are ones who must be held accountable for the consequences of the security failures of that software. This metric is most important because it is the greatest incentive for companies to care about the quality of the code they produce. If we don’t hold companies culpable, the current issues in IoT can only worsen.

Patching is failing as an IoT security paradigm, and it must be addressed at the risk of security, privacy, and even the health of users of IoT devices (read: most people). If we can create a solution to the problems discussed that satisfy all three of these rules, then we will see a subtle but significant improvement to the lives of technology users.
References


Thompson, I (2016, 13 Oct). *Wi-Fi baby heart monitor may have the worst IoT security of 2016.* Retrieved from https://www.theregister.co.uk/2016/10/13/possibly_worst_iot_security_failure_yet/?mt=1476453928163


