Maze Mentality: The Insecurity of Modern Technology

Stevie Lomack

Metropolitan Community College, Omaha, Nebraska

Maze Mentality: The Insecurity of Modern Technology

Many people often question if the modern technology items in our households could be described as secure. When in all actuality these items are no where near being secure. Unfortunately, we are not properly informed of the vulnerabilities and issues to efficiently better our efforts to securing them. Our first mistake was assuming the manufacturers of cell phones, items similar to Alexa, other home products; as well as, providers such as Cox, CenturyLink, etc. were providing safe and secure services. Trusting product manufacturers and the providers of internet/other services to protect home technologies is far from ideal. Which is why it should soon come to a stop.

For starters, people today trust and believe in the programming of modern technology devices which leads us to the assumption of modern technologies performing their duties safely for us. As previously stated, this is far from the truth. In comparison to human beings, the programmers and programs we trust in are not perfect. Due to the products working efficiently and with minor issues, people tend to believe the products are perfect or close enough.

Alfred Basta, author of college textbook *Computer Security and Penetration Testing* describes the evolution of programming exploits. (Basta, 2014) He displays the mindset of industry inventors who hold the mentality of software as a finished product that can be used for years. Instead, the ideas of those products are never finished, and it is likely to be replaced before it is perfected. This means the products you receive are not completely finished items and could cause you to be compromised in the long run.

Trying to fully secure their products may cause manufacturers to never be able to release their technology. This is one of the reasons products are not made in a way that considers security as the main point. There are multiple arguments from people who think the Internet providers secure our connections on their side through their router configurations, due to devices

being hooked through the Internet and having security protocols on our Internet; basically, you are trusting the foundation of the Internet and the service providers.

Thinking back to when I was in a customer's home installing a smart home wireless alarm system, the first thing I checked was the router modem access. During the check I was able to access the router because it was set with default user name and password, if I had been a hacker full access would have been granted to me. Alongside that, government regulations usually require companies to disclose terms and use information of their products they don't ask for them to be perfected security wise.

All of us have built in characteristics and behaviors that reside in us as being human better known as mankind instincts. Sometimes these are good for us but other times they betray us and cause loss, pain, and lack of understanding. Therefore, many people today trust the creditability of large businesses, and organizations. We trust the government will be regulating these entities, to keep us safe. We live this way because we experience our own issues with our up's and down's while still trying to hold on to our life visions.

A new day with its' challenges and relationship focuses keeps us in a constant repeating cycle of busyness. I prefer to call this the 'Maze Mentality' because it symbolizes the mice who search their way through the maze without being able to see where it actually leads them; they smell the cheese and it drives them to continue. This is not to put us down as people because we are all wonderfully made by God with a purpose.

However, we do have a few flaws and chinks in our armor. The good news is we are able to work things out and unlike the mice we have more going on for us then just worrying about finding the cheese. Personally, I've lived in the Maze Mentality most my life then, in 2015 I started to take a few classes in hopes to obtain a degree in Cyber Security. Slowly, my eyes were being opened to realities I never took the time to think about. Prior to taking these courses I never processed what the Internet truly was nor did I know where it came from, whether or not it

was safe, what viruses were, and last but not least I wasn't aware of all the new technology that functions through the Internet. There are a lot of things out there that we are unaware of that could potentially hurt us in many ways.

People often use the argument that the Internet is safe/secure and well-fortified with a long background of history and foundational building blocks that make it solid and upcoming. But in reality, it's old and fading away and will soon be replaced with a new better foundation made for today's technology. People believe if there was a major problem then everyone would be aware of it because of the Internet and the advancement of technology today.

Think about understanding the picture of using a foundation from 1969 and protocols or governors from 1983 this may help you clearly understand the true problem with todays Internet. Also, touching the view of where we fight from considering the foundation of ARPNET and the OSI model along with TCP/IP protocols (ARPNET is the original Internet from 1969 that we are still using and the OSI model, and TCP/IP is the 1983 systems that govern the worldwide Web of today). They are out of date and insufficient to truly secure your technology devices that need it to operate.

Additionally, to layout some background information everyone should know; this information covers the Internet itself and the structures that rule it. This is open common knowledge I wrote about in 2015, "now, beginning with the hereditary foundations, systems, protocols, and traits handed down to this generation of Internet users; starting with (ARPANET). Consequently, there was no reason for security in and infrastructure with private inter circle connections points and being the only ones with this technology it made no sense to think about a future like the one we have now with the Internet back then. Besides, the TCP/IP protocol of 1983 has multiple wholes and attack vectors that attackers' prey on to access systems." (Lomack, 2015)

Professor Samuel McQuade holds a Doctoral degree, he teaches and conducts research inclusive to cybercrime and security studies, he breaks down the beginning of the Internet. “In 1960 under guidance of J.C.R. research scientist and engineers throughout the United States were commissioned by the Department of Defense to create a way for people separated over long distances to communicate using computers. They created what is known as ARPANET (Advanced Research Project Agency Network), which was initially activated in 1969. This became the Internet of today or the World Wide Web. By connecting mainframe computers; at Stanford research Institute, the University of California- Santa Barbara, the university of California-Los Angeles (UCLA), also the University of Utah. Thereupon, these universities and research institutions established communications with each other and within two years 15 other universities and research institutes across the United States had also connected with one another. Never the less, ARPNET’s Foundational use of packet switching technology that allowed data to be separated in bytes consisting of eight digits (1’s and 0’s) as a result, the bytes could be sent electronically from one computer or computing device to another as digital string messages; these were sent through telephone wires and wireless cellular phone satellite connections.

In the early 1980s, ISO began to work on a universal set of specifications that would enable computer platforms across the world to communicate openly. The result was a helpful model for understanding and developing computer to computer communication over a network. This model is called the OSI model which is an acronym for Open Systems Interconnection. “Indeed, the OSI model consist of seven layers” (McQuade, 2008). This defines the beginning of the Internet of today that we all think to be this awesome piece of technology that allows us to perform all of our technical resources needs. However, we never think about what it is and what it’s capable of doing in our lives.

In terms of home listening devices like Alexa, and the other systems that control devices in our homes; people tend to believe there is a low risk of being hacked. People think it’s not

worth the hacker's time to get some important information listening in on them. Hackers are more interested in your banking information than listening in on you also, the level of effort to do this is too high in the vast majority of cases. Also, the way smart speakers operate makes them less vulnerable to hackers than your other internet-connected devices.

Many of us heard about the Target hack that exposed all the credit card information of many, this was accessed through a third-party company who had access to Target's network to monitor and maintain their heating and ventilation systems. All of these devices have access to your network. The bottom line is attacking these devices can provide a benefit to hackers and can cause you a world of hurt.

Along with everything else, manufactures promote the products and their services to be safe. People believe in the credibility of the manufacturers and their products. You don't hear many stories of negative events happening with these products and the manufactures that make these products are better known for potentially make our lives easier. In reality most people that are hacked don't even known they were hacked.

Bill Nelson author of college textbook *Guide to Computer Forensics and Investigations* shares programming and software information (Nelson, 2016). All of the software languages have vulnerabilities from C, C++, .NET Framework, HTML5, Java, and Java Script along with all the other languages. The bottom line is some languages have strengths to aid in locating errors and some of the older languages depend on the programmer to find and trouble-shoot errors. Whether it's a low-level programming language or a high-level one, neither are perfect they all depend on the company and programmer to add security that helps. The only difference is the low-level is easier to convert to machine languages but is harder to understand. For the high-level languages they are closer to natural language which make it easier for mankind to understand what the program is doing. However, these are the foundations of coding for these new technology devices. So, the issues are all laid out a long with the potential countering

methods. What this means is those technology items are pretty much in the same shape as your 1969 Internet because you depend on someone else to protect you.

Anyway, I'm not going to get into the countering methods because they are irrelevant to you and me, they are only beneficial to the one's who have the power to use them for the true full securing of the products we are discussing.

Therefore, making this an ongoing battle with feelers out at all times this gives us some advantage to learn and stop potential attacks before they even have a change to begin. Also, when we ignore security protocols for ease of use and convenience to our new technology items advantage hackers.

In contrast, soon this IPv4 environment will be depleted and obsolete which means your Internet of today will be finished. Don't worry IPv6 is already in affect with a foundation of security features and almost finite IP addresses this is the new Internet. So, taking in account all the evidence that has been laid out stop trusting others to protect you and start taking part in protecting yourself by using the security updates and other information to take a stand against the 1969 Internet that all our new technology items are subject to function. Bottom line don't leave your security to someone else be smart with this information and stop the old trends be the frontline to the defense of your home technology devices.

Another Argument is these new Apps help make life more orderly and easier and the developers of these products are trust worthy and looking out for a better future. Along with the same analogy that the Internet is safe because of providers and its security. This is not reality and here is some foundational material that may help you see a clearer picture of the truth.

It is important, to understand some mobile device security information. Mark Ciampa is the author of *Security+ Guide To Network Security Fundamentals* which is a College textbook used to teach Network security and its fundamentals Ciampa (2015). We normally install unsecured applications, but we should stick to the vendors who make our products or other

reputable sources but for the most part we use third party developers these apps have you disable the security provided by the manufacturer once you grant access. You now give rights to your information which is usually sent to these developers unencrypted where any hacker can access it. But the real bad news is, they probably sell your information to analyst companies and advertiser networks. If you still want that new game app, be careful, it may cause you a world of pain through accessed personal information about you and your friends remember this app needs access to your photos, phonebook, location, and text messages. Ask yourself if you're willing to release this information to play a game or any other thing that you think you need on your phone.

Most people feel they don't need to worry about updates and being aware of the latest attacks or issues because in their eyes it can only happen to big companies and people with a lot of money. A hacker could run a program to steal five or ten dollars from thousands of people and you could be one of the many or maybe it could be your information he sells which is why you should not count yourself out.

National Cybersecurity and Communications Integration Center part of the Cybersecurity and Infrastructure Security Agency (CISA) who specialize in now day Internet and world security issues and back these Cybersecurity common sense prevention instructions.

For example, most people don't see any benefits to staying on top of updates and the latest security threats. One can do this by signing up for Home Land Security news updates from the National Cyber Awareness System which keeps you on top of the latest information made known to them. On their site it states, "The article posted on December 28, 2018 by Home Land Security informing and warning people During the holidays, internet-connected devices also known as the Internet of Things (IoT) are popular gifts from smart TVs, watches, toys, phones, and tablets. This technology provides a level of convenience to our lives, but it requires that we share more information than ever. The security of this information, and the security of these devices, is not always guaranteed" (CISA, 2018).

Even though, this is available to everyone that subscribe to it; most people walk around with no idea of what's happening in the background with these items they enjoy so much. Maybe the genre should have been the 10 o'clock News with a just in News-flash your information just has been stolen and the culprits have escaped with your help.

In conclusion, with this foundational information we may start to see the state of the Internet for the users of today. It was not meant to be this big and to encompass the world as it has, now there has been many attempts to secure things but you must remember without security built into the foundation we are just patching an over whelming number of holes. So, the next time you install that new app or buy that new home technology item think about what stand you will take when it comes to your secure future on the web.

References

Basta, A. (2014). Programming Exploits. In *Computer Security and Penetration Testing* (2nd ed., pp. 249-259). Stanford, CT: Cengage Learning.

Ciampa, M. (2015). Mobile Security Part V Wireless Network Security. In *Security + Guide to Network Security Fundamentals* (5th ed., pp. 357-382). Boston, MA: Cengage Learning.

Lomack, S. J. (2015, March 7). *The OSI Model info 1023*. Unpublished manuscript, Metropolitan Community College, Omaha, NE.

McQuade, Samuel, (2008) and Neel Sampat. *Survey on Internet and At-Risk Behaviors*. Rochester: Rochester Institute of Technology Libraries,

Nelson, B. (2016). Cloud Forensics. In *Guide to Computer forensics and Investigations* (5th ed., pp. 481-491). Boston, MA: Cengage Learning.