James (Jimmy) Allah-Mensah

October 16, 2020

COVA CCI Undergraduate Research

The Hidden Advantage Among Digital Natives within Bug Bounty Programs

Abstract:

Bug bounty programs are a great way for companies and organizations to help keep their systems and information secure; however, there are only a limited number of white hat hacking participant spots. With only so many seats available at the table, being able to determine the most qualified group of individuals is critical to the efficiency of the program at large. Digital natives, people born into the digital age, provide an instinctive approach when dealing with technology. On the other hand, digital immigrants, people who grew up before the digital age and had to adapt to new technology, evidently utilize experience. This paper focuses on the observation and analysis of each group's ability to identify critical inconspicuous vulnerabilities within presumably attack proof products. The goal was to identify how the younger generation's ability to utilize technologies in unanticipated ways could provide security insights often overlooked by more experienced security professionals. We present members of each group six different newly released tech products asking them to, without effort, identify an uncommon usage and vulnerability for each. Their responses are then scored based on classification. After careful classification and analysis, it was determined that millennials with a technical background were the ideal candidates.

Introduction:

As technology advances, so does the level of calculated risk associated with its wrongful misuse. In a world where almost every aspect of our lives is reliant on the constant use of technology, it's essential that all information is protected and adheres by the standards of the CIA triad (Confidential, Integrity, and Availability). This means that vulnerabilities that lead to the unauthorized access and misuse, alteration, or obstruction of data must be identified and

mitigated as soon as possible. With the numerous ways in which technology can be used also come a plethora of ways in which attackers can get creative in exploiting vulnerabilities. Although security training, antiviruses, and software patches are some of the ways in which users can protect themselves from cyber attacks, the presence of zero day exploitations completely surpass all methods of protection.

A bug bounty program is a service provided by companies, organizations, and websites that incentivize white hat hackers to disclose any bugs, vulnerabilities, and security exploits identified within their system or product. These programs are intended to act as another layer of security as bug bounty programs offer often overlooked security insights. However, there are some downsides. Not all participants report discovered vulnerabilities, there's potential for participants to sell vulnerabilities to criminal hacking groups, and many low-level flaws are reported taking time away from security professionals. These downsides limit the number of white hat hackers to those deemed the most qualified. However, what qualifications make up a qualified participant?

Digital natives are people born after 1996 who have grown up in the digital age. From the time when they were in diapers through adulthood, they've relied on technology in practically all aspects of their daily lives. These people are made up of Generation Z and Generation Y. On the other hand, digital immigrants consist of people who were born before 1996, who had to adapt to the new immersion of technology in their daily lives. They're made up of the Millennials, Generation X, and the Baby Boomers. Within each of the two groups there are technical people, those who have some type of background in a technology based career field, and those that are non-technical who merely use technology for entertainment and convenience.

Evidently when debating if there is a specific group who would be more qualified to participate in bug bounty programs, a lot of factors come into play. However the main dilemma is as follows: Technical digital immigrants have much more experience working in technology driven career fields than digital natives; on the other hand, being born into a digitized world produces a different way of thinking that can possibly trump experience.

In his interview with *EHS Today*, Keith Barr, CEO of Leading2Lean, a manufacturing operations oriented management platform, contends that any workplace composed of primarily Generation Z employees "has a very different level of competence or capability as it relates to using technology in their lives" (Valentie). Dr. Ian Watson, a Northumbria University Faculty Member who would most likely concur with the preceding statement, shares the proposition of Marc Prensky, the catalyst of the digital natives versus immigrants theory, which explicitly suggests that "today's students think and process information fundamentally different from their predecessors" (Watson).

With this in mind, we wanted to determine how their relatively different ways of thinking provide security insights or innovations that tend to be overlooked by more experienced security professionals. We propose that today's younger generation, born into a fully digitized world, offers unique insight into how commercial products are used, and by extension, provide often overlooked perspectives into the vulnerabilities of those applications. The goal of this research is to provide bug bounty programs insight into which group of white hat hackers will be the most effective in identifying critical vulnerabilities, which in return would benefit organizations by securing their systems and participants by introducing cybersecurity employment opportunities.

Research Question:

Focusing on the younger generations' ability to utilize technologies in unanticipated ways, how could their relatively different way of thinking provide security insights or innovations that tend to be overlooked by more experienced security professionals?

Hypothesis:

Today's younger generation, born into a fully digitized world, offers unique insight into how commercial products are used, and by extension, provide often overlooked perspectives into the vulnerabilities of those applications.

Background:

Over the past decade, there has been numerous attempts to bridge the gap between comprehending the dynamically asserted relationship between the generation of security professionals or attackers and their ability to identify vulnerabilities within a security system. Through our external research methods, we were able to identify a common theme among several sources revolving around a difference in the thought process of a digital native versus that of a digital immigrant.

The whole digital natives versus digital immigrants theory was introduced by Marc Prensky, a writer and educator from Yale University and Harvard Business School, in 2001 in his article, *On the Horizon* (Presnsky). At the time, the theory became the topic of discussion in the K-12 education world; however, little did he know what long term effects his writing would have in the world of technology in the near future.

In 2003, Dr. Claus Tuly of the German Youth Institute claimed that the significance of technology in the daily lives of young people remained largely unexplored. With this discovery,

he attempted to dive into the minds of the younger generation to determine its influential factors. In his research experiment, which involved 4,500 young people from the ages of fifteen to twenty-six along with eighty additional qualitative interviews, he conducted surveys with questions that first identified the participant's interest in technology. He then asked questions to determine their outlook on society in many aspects of everyday life such as the importance of owning a car and their position on environmental friendly behavior. In his conclusion, he introduces a concept that divides the term "technology" into two types. The first, Technology I, determined by spatial, factual, and social terms. The latter, Technology II, where the use is not described; more specifically, "the hardware is not designed for specific tasks, and it is, consequently, suited for nearly any task" (Tuly). The presence of "Technology II" disclosed by Tuly, allows a more narrow discussion involving how digital natives viewed the purpose of devices under this categorization of technologies versus that of a digital immigrant.

Through the surveys provided with this research, we intend to shine a light on whether this split in viewpoints on "Technology II" devices directly correlates to a greater ability of identifying vulnerabilities within a bug bounty program.

Methodologies:

In order to obtain the data needed to accept or reject our hypothesis we decided to take the approach of a voluntary participation based survey.

Survey Method:

The two main goals of the survey were to 1) Determine whether or not the unique way of thinking of a digital native contributes to insightful perceptions on how commercial products are

used? 2) Identify how effective these insights can be in the cyber security workforce in terms of noticing typically indistinguishable vulnerabilities within commercial products.

For the first goal, in order to understand the correlation between unique thinking and noticeable insights we focused on the following four main aspects of the survey: 1) Effort Required, 2) Response Format, 3) Question Complexity, and 4) Category of Displayed Products. Since one of the main components that we attempted to unravel dealt with instinctive decisions, it was essential that participants weren't taking a long period of time to give answers. Responses under a minute were encouraged which ensured that they were fully natural and there was no external research put into them. Next, the responses had to be completely fill in because multiple choice eliminates creativity. Additionally since one of the additional components deal with creativity which is contradicted by multiple choice answers thought up by the researchers. When designing our questions we wanted to ensure that nontechnical participants understood specific terms such as "vulnerability" and "use case," and that there was no ambiguity in what was being asked. To fulfill this requirement we gave participants a brief introduction at the beginning of the survey defining these key words as well as putting into context the goal of this survey. In terms of the format of the questions, they were short, explicit, and very easy to understand.

For the second goal, allowing us to associate findings with cyber security, we had to tie in a security question and bring to the attention of the participants to avoid stating normal use cases of the displayed products. By just displaying a product and asking participants to identify an uncommon use case, we were developing insight on the creativity of each participant. This is important because creativity is very important in cyber security; however, creativity alone isn't enough to credit or discredit participants on their theoretical level of white hat hacking ability

without any practical application. To provide such, we explicitly asked participants, “what could an attacker do with this product.”

Participation:

The survey sampling was voluntary and the initial desired sample size was one hundred participants. Of this sample size, we wanted an equal technical and nontechnical representation of each of the following groups: Generation Z, Millennials, Generation X, and Baby Boomers. To encourage participation we sent the survey out to family members, friends, classmates, students, coworkers and technical managers. As a last resort, we posted the survey link on LinkedIn with a short yet catchy description.

Groups:

The eight categories that participants fell into were as follows: Generation Z (Technical), Generation Z (Non-Technical), Millennials (Technical), Millennials (Non-Technical), Generation X (Technical), Generation X (Non-Technical), Baby Boomers (Technical), and Baby Boomers (Non-Technical). Generation Z make up the digital native population whereas Millennials, Generation X, and Baby Boomers combine to make up the digital immigrant population. The term technical and non-technical are used to describe if the participant has a background in technology, specifically relating to computer science or cybersecurity.

Generation	Age Range
Generation Z	5-25 Years

Millennial/Generation Y	26-40 Years
Generation X	41-55 Years
Baby Boomer	56-76 Years

Products:

The selection of the products that were presented to participants was fairly difficult. We wanted to ensure that the products abided by the following three properties: 1) Relatively New Release Date, 2) Main Unambiguous Use Case, 3) Self Explanatory Product Name. A relatively new product ensures that there are not too many easily accessible reviews on the product that can identify inconspicuous use cases and vulnerabilities. We set the release date of these products to be either from the current year (2020) or late of the previous year (2019). Next, by limiting the products to one with a single main use case, developing additional ones would require a great deal of thought. If participants could do so, without effort, their natural ability would stand out in the scoring. Lastly. a self explanatory product name provides participants with an understandable definition that layers onto the already provided description. The description and product name combined offer no need for participants to perform external research on determining the product functionality. The six products were as follows: 1) A Smart Power Strip Wifi Surge Protector, 2) Amazon Kindle Paperwhite, 3) SNOO Smart Baby Sleeper and Bassinet, 4) Master Lock Biometric Padlock, 5) Phonesoap UV light Sanitizer and Charger, and 6) Phillips Sonicare Smart 9500 Electric Toothbrush

Classification:

Once the survey responses were recorded, there needed to be a method of analyzing and scoring them based on the level of sophistication presented in their answer. We created a use and vulnerability classification table with ten rows of three columns. The headers of the table going from left to right were as follows: Classification Number, Use Basis, and Vulnerability Basis. The classification number was used to represent the level of sophistication within one's answer relating to either the use case that the individual disclosed or a potential vulnerability that was identified. The table scoring guidelines were determined with the help of Microsoft's Xbox Bounty Program report quality submission guidelines. The number ranges from 1-10. The ranges are summarized in the table below.

Classification Number	Use Basis	Vulnerability Basis
1	Same as the intended use or not attempted.	Low Severity Level (Limited adverse effect on organizational operations/assets).
2	Contains part of the intended use.	Can use information to find other vulnerabilities
3	Similar to the intended use.	Can use information to exploit known vulnerabilities
4	Non-primary (additional but evident use)	Moderate Severity Level (Serious adverse effect on organizational operations/assets).
5	Non-primary (additional but not evident use)	Can use information to gain access to security settings.
6	Unnoticeable	Takes control of the device.
7	Inconspicuous (very unnoticeable)	High Severity Level: (Catastrophic adverse effect on organizational operations/assets).
8	Innovative (Hard to come up with)	Leakage of highly sensitive information.
9	Unique (Difficult to come up with and first time hearing)	Significant data loss or downtime.

10	Extraordinary (Eye opening)	Zero-Day Exploit if made public

Final Survey:

The first part of the survey consists of a questionnaire. Within that questionnaire is a description of the goal of the survey which is used to provide context for the participants. After the description are a series of personal questions used to classify the participant into one of the eight categories. The questions ask the participant to identify their age/generation, highest level of education, and whether or not they had a technical background. For the actual survey portion, there was an option of two sets of products displayed. The first set, located in Form A, consisted of the Amazon Kindle Paperwhite, PhoneSoap 3 UV Light Sanitizer, and the Master Lock Biometric Padlock. The second set, located in Form B, consisted of the Smart Power Strip Wifi Surge Protector, the SNOO Smart Sleeper, and the Philips Sonicare Smart 9500 Electric Toothbrush. For each product listed, there are two long text response fields. The first asking a user to identify an additional use case of the product. The second asking "What could an attacker do with this device." When done with the last question, they're given an option to enter any additional products with unnoticed use cases and vulnerabilities.

Results:

Finding enough individuals to participate in the research experiment by taking the survey was fairly complicated. With the coronavirus putting a complete stop to the lives of college students across the nation, the survey was released at a time where everything was starting up again and taking a survey wasn't a priority for a lot of people. Fortunately, we were able to use Linkedin, a business oriented social media platform, to obtain some additional responses.

When analyzing our responses we wanted to ensure that 1) our participants were qualified enough to provide adequate solutions, 2) participants were exposed enough to technology to provide adequate answers, 3) there was a similar representation in participants with and without a technical background to ensure findings aren't skewed. The total number of participants came out to be 61 (sixty-one). Of that population, 16.4% were from the Baby Boomer generation, 13.1% from Generation X, 18% from Millennials, and Generation Z at 52.5%. To address the first concern involving the quality of responses, 95% if participants had at least a high school diploma and almost 82% of participants had, at minimum, been exposed to some college coursework. Addressing the concern involving the participant's experience with technology, almost 97% of participants use technology on a daily basis, and among that representation 59% of participants consider themselves "Tech Enthusiasts" meaning that they enjoy using computers and electronics. To address the last concern involving equal technical and non-technical representation, only 39% of participants had a cybersecurity background and a little more than half (54%) had some type of programming experience.

Findings

The two principle numbers for each of the sixty one responses represent the average classification use case and vulnerability identification numbers. Each participant is scored in the two areas per each of the three products within the set. The average of these three numbers is then calculated which is where the two numbers come from. For each participant, these two values are added with the rest of values from the other responses and averaged out. The results can be viewed on the table below.

Based on this data, Technical Millennials were found to be the category with the ability to identify the most critical vulnerabilities, with Non-Technical Millennials coming in second place. For use cases, the Technical Generation X category was found to be the category with the ability to think up the most inventive use cases, with technical millennials coming in second place.

Generation	Technical	Non-Technical
Baby Boomer	UC: 2.539, V: 2.995	UC: 1.732, V: 3.527
Generation X	UC: 4.330, V: 4.208	UC: 1.25, V: 2.208
Millenial/Generation Y	UC: 4.066, V: 4.885	UC: 3.299, V: 4.365
Generation Z	UC: 2.493 , V: 4.269	UC: 3.520, V: 4.043

Analysis:

Our initial hypothesis was that the younger generation, Generation Z, due to them being born into a fully digitized world, would allow them to offer unique insights into how commercial products are used, and by extension, provide often overlooked perspectives into the vulnerabilities of those products and applications. Simply put, we believed that Generation Z would be the category to identify the most critical vulnerabilities and think up the most inventive product use cases. Based on the survey results, our statistical data disproves our hypothesis in which the younger generation provide often overlooked perspectives into vulnerability identification. In terms of Generation Z's ranking in the study, their non-technical category came in third for use cases and fifth for vulnerabilities within their technical category.

There are many possible reasons and explanations for why the Millennial generation outperformed everyone in both categories. The most logical consists of the fact that millennials were of learning age during the rise of the digital age.

Additionally, the majority of participants from the Generation Z category were full time college students at the time the survey was conducted. Out of that entire population, around 90% had given at least one response that was classified as either "not attempted" on the use case side or "low security level" on the vulnerability side. Since the participant pool consisted of a little more than half of Generation Z participants, the frequency of this score may have significantly skewed our findings.

Future Scope

With the findings from my research, I hope to provide insights and promote further critical thought regarding the participation pool of white hat hackers within a bug bounty program. Now that we know that millennials are the ideal generation to identify the most critical vulnerabilities within a system, this insight can be used in a variety of ways. Although the intention of this research involved providing Bug Bounty programs with important insight on determining their most effective participation population category, another desired area of exploration dealt with the proposition of a new career field focused specifically on white hat hacking aimed at Millennials.

The term, "Cybersecurity," is always a buzz word in the tech field as many associate it with a belief in an excess number of available jobs; however, this isn't the case. Breaking into the cybersecurity field as a Cyber Analyst, Security Engineer, or any other related position requires a long path of expensive certifications, IT help desk experience, and often a four year

degree, which many young aspiring cyber security students will most likely not have at the start of their career. Although each stepping stone will provide adequate transitional cyber security knowledge for the workplace when the time is right, is all of it really necessary? On another note, instead of focusing on ways to prevent attackers from identifying and exploiting vulnerabilities within a system, program, or device, what if there was the same level of energy aimed at identifying these vulnerabilities before the release of the product at large?

Conclusion

Bug bounty programs supply companies and organizations with a mutually beneficial way to keep their systems and information secure. However, white hat hacking requires a very unique way of thinking that allows white hat hackers to identify vulnerabilities within a system that not many of them possess. It is believed that Generation Z or digital natives, people born after 1996, are the closest category of people who possess this distinctive eye for identifying vulnerabilities; however, the findings of this research provided an alternative. Millennials from both technical and nontechnical backgrounds proved to be the generation that is most effective at identifying vulnerabilities within a system or product. With this information, we hope to not only provide bug bounty programs with insight into their best chance at securing their systems but to also propose new opportunities that feed off of the unique way of thinking of millennials interested in a career in cybersecurity.

References

Prensky, Marc. “Digital Natives, Digital Immigrants.” On the Horizon, vol. 9, 5 Oct. 2001.

Tuly, Claus J. “Growing Up In Technological Worlds: How Modern Technologies Shape the Everyday Lives of Young People.” Bulletin of Science, Technology & Society, Dec. 2003.

Valentic, Stefanie. “Q & A: How Generation Z Is Shaping the Workforce.” *EHSToday*, Endeavor Business Media, 10 Oct. 2019.

Watson, Ian Robert. “Digital Natives or Digital Tribes?” Universal Journal of Educational Research, vol. 1, no. n2, 2013, pp. 104–112.