INTERNATIONAL RESEARCH JOURNAL ON ADVANCED SCIENCE HUB
e-ISSN : 2582 - 4376
Open Access
RSP SCIENCE HUB
(The Hub of Research Ideas)
Available online at www.rspsciencehub.com

Special Issue of Second International Conference on Innovation in Engineering Sciences (ICIES-2021)

NB^{2}M – Mechanism for Magnifying Micro Level Bugs for Secure Software System

D Anil Kumar [1], Susanta Kumar Das[2], Murali Krishna Senapaty[3]
[1,2]Berhampur University. Berhampur, Odisha, India
[3] GIET University, Gunupur, Odisha, India
anil.ritwika@gmail.com[1]

Abstract

People speak greatly about the electronic gadgets in the past, present and in future. Nobody spells that it is secure or insecure in terms of safety. More inventions are carrying into the society but in behind there are lot of pitfalls which could damage personal or organizations from upper level to ground level. It is very important to build secure systems to have safe usage of electronic gadgets. USA government is spending millions of dollars on secure data because in future their total dependency is on data. Technology is growing and the hackers (persons) who damage or steal our information and bank balances are similarly increase in parallel. Bug bounty hunting is the new technique that is enforced for finding the software security in the newly build software or year's long existing software. New bug bounty methodology teaches us how to identify our software is secure or not and what the flaws or bugs in the software. NB2M mechanism gives the sources of cyber-attacks and study preserved producers for cyber-crimes. This process may be benefitted for organization as well as software professional who can gain lump sum dollars. It is better go for one to two years for bug bounty.

Keywords: Malware, bug, bug bounty, cyber-crimes, cyber-attacks

1. Introduction:

Malware is a kind of computer software, which we also call Malicious Software; it is a kind of corrupted software which has the same purpose to damage the computer of people. The malware created goes with the same purpose that it can harm our or any specific user's computer; it can have many other purposes like stealing your data, stealing your password, or deleting your computer's data. Malicious software can come to your computer in many ways like either you download them by mistake by yourself or through a spam email or through a website. Because there are many websites on which links to malicious software are available and in a single day, many people get spam emails, out of which many people also download malware and fall prey to them.

2. Types of Malicious software:

There are many types of malicious software that work in different ways or say that it damages our computer and data, the way they work is different, some types of malware [7] are like this.

2.1.Virus:

Viruses are programs or software that spoil the programs lying in our computer, lab top, mobile and tab, infecting the files lying in them. Files that are very important to us, such as document files, image files, or video files, and many other files that are very important to us, affect those files. The way viruses spread in humans, like TV virus, cold virus and many other types of virus, we feel that living viruses are not like that virus in computer or laptop is a program. Which is named as virus which spoils our files. So this virus was named in 1983 by an American scientist named Fredrik B. Cohan, he first named such software as virus.

Whole form is - Vital Information Resource Under Siege. The virus, named Creeper, was the first virus that spread on the network in 1970 in ARPANET (Advanced Research Project Agency Network). Creeper caused infected systems to print the message, " I'M THE CREEPER : CATCH ME IF YOU CAN. " Just as there are many types of viruses spread on the Internet today, in the same way a network was created for the US Defense Military named ARPANET Station, in which the network virus was spread. The first virus to spread to PC was ELK Cloner, which spread in 1982. The virus was created by a 15-year-old Richard Scranta for the Apple II (Dos 3.3) operating system, which was stored on floppy diskettes. When the computer is booted from the floppy disk infected with the elk cloner, the virus infects the PC. And our computer malfunctions.

2.2.Worms:

Worms are very much like computer viruses but the special thing is that it can make many copies of itself, that is, it spreads and can be infected by going to all or any computer connected to your network. It does not need any instructions to spread it, it can come in your computer during email, internet surfing, downloading, it can damage or crush your data like a virus.

2.3.Trojan Horse:

The Trojan horse had its beginnings in ancient times, when the Greeks built a large wooden horse to attack Troy, a city in Turkey, in which many soldiers went inside the turkey and at night They had attacked the turkey, this large wooden horse was given the Trojan horse. Similarly, there are Trojan horses inside the computer which after installation is able to control our computer. Just after getting control of the Trojan horse computer, it gets attacked by viruses and other malware which corrupts our data.

2.4.Ransom ware:

Ransom ware as the name suggests, ransom ware is encrypted in our computer once installed, all our data is encrypted i.e. it is locked or simply kidnapped and unlocked or decrypted. We are asked for money in the same way as after kidnapping someone to ask for ransom or ransom in return. Most payments for ransomware are made by bitcoin or crypto currency so that the developer of ransomware or the sender of the ransomware cannot be caught.

2.5.Spyware:

Spyware's job is to monitor all the activities and data that you have in your computer and send them to someone else. Just like a spy, it can be installed with any unknown software because it can be much installed. Are small. Spyware is created by targeting a particular person, place or a particular computer and its job is only to monitor your data.

2.6.Adware:

The special purpose of Adware is not to harm your device or data, but after it is installed, you start to advertise on the home screen without opening any app, it is often seen in the smartphone, this kind of crooked website. Anything from can be downloaded. Figure 1 carries the concept of attackers attack on client-server based machines.

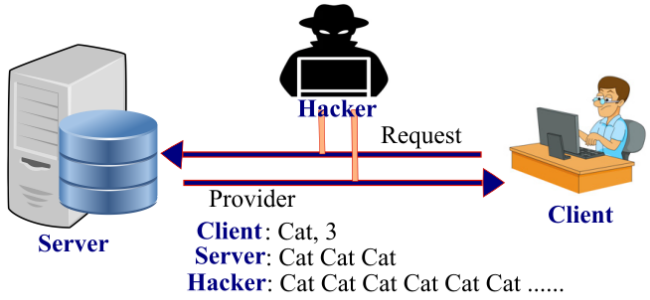

Fig.1: Mis-concept between Client, Server and Hacker

Figure 1 is based on a real time example where there will be mis-concept between client, server and hacker. We can easily identify that the network is hacked or not. There will be an understanding between client and server, and hacker may not go for guess work because he cannot predict the understanding info between both parties. The stream of communication is like a follow and in between a flow an unrelated data occurs that means it hacked.

3. Literature Survey:

American government is spending lot of money for secure software because there is future is dependent up on computers and stored data and similarly some of the gulf countries are engaging Chinese black hat hackers against American government. Day to day there are preparing new compositions and new techniques to get or corrupt large volumes of valuable data that cannot resist.

3.1.Ways to avoid malware:

To avoid malware, you have to take care of only a few small things, but sometimes we do not know this, due to which we get to see or face many

problems, then let us know these small things. First of all, always check before downloading anything that the website is original or there is a fake website. If the website is not so popular, then you can find out how it is by commenting on that website. If you do not get it, do not download from there. Open the email attachment after seeing it properly and after downloading, scan them properly with an antimalware software. If someone can keep an eye on your computer or has some important data in it, do not open the email attachments sent by untrusted or unknown person. While downloading the software, use only the official website of the software or trusted and well-known website. Do not get caught up in downloading pirated things like movies or paid software for free, it is wrong and it can cause danger to you and your valuable data. [1] Andreas Kuehn and Milton Mueller, working paper that represents recent improvements in bug bounty programs. Paper balances on secure and insecure in the software. Any organization depends upon computer applications and they are openly available to the world. When they expose to internet, then there will be different problems arising, that to unknown. To resist this type of bugs, software should be persistent. For that purpose bug bounty programs are introduced and they should be for knowing flaws in their own software and based on ground reports, the software should change its dimensions. Because of code vulnerabilities many corporate companies are in danger now. By enhancing bug bounty programs they can protect their own software from cyber-attacks. [2] Nirav Bhojani, Day-to-day impact of malware is becoming a head to most business organizations and author discusses about two types of malware analysis, static and dynamic malware analysis which have some limitations and cannot be focused on present situations. [3] Divya Manusha Seethalam, et. al, Technology is growing and security is playing a ley role, there are lot of testimonies related to short/small bug which caused giant damage to the systems as well as human life. Historical example that carries from years to years be Ariane 5 disaster which we loss human life's also. Our devices should be user friendly not user enemy. Author focuses on design issues because they play a key roles in implementing the software. [4] Prathipati Ratna Kumar, et. al, various software technologies are introduced to work on various platforms with complex process. Detection of software defects at the earlier stage is more important to have a secure software application. Author focuses on ABC (Ant Bee Colony) – Model using machine learning techniques to identify the critical areas that should be test prior to deployment. Author design and implemented an improved technique using probabilistic ABC based classification model.

[5] Prathipati Ratna Kumar, et. al, Bug detection is like a solving a big mathematical puzzle and it is a complex process. Author focuses collects the dataset and identifies the features based on weights. Based on weights critical features are selected where that parameters should be focused more in the software testing process. It is a pre-processing based classification model for finding multiple bug from datasets and based on weights identifying critical areas and making them persistent or secure software which can resist attackers. Confusion matrix true positive and low error rate can concerned. [6] Prathipati Ratna Kumar, et. al, population is growing, business production is growing and dependency upon software is increasing with pressure. Heavy pressure is on software developers who write the code. They have to take a new parameter to the software development life cycle that is security. It plays a key role in every software development; it should be made to resist the attackers. Machine learning is the concept add to all domains for accuracy purpose. There are so many classification techniques helpful in making secure software. Author focuses on the software metrics that are useful for making secure software. Based on clustering techniques, process of feature selection we can predict the areas which are critical and focus on them. [7] Tebogo Mokoena, Tranos Zuva, Story of malware is not new to software professionals, it is taking it is own shape from years, Malware can be any malicious software which can destroy or steal or corrupt your computer. Author focused on viruses, worms, Trojan, backdoors and adware few examples, and to resist malware. Author focused on static and dynamic malware under sandbox lab environment and proved that any malware can be detected. After detection we can resist. [8-10] S Megira, et. al, Almost all now a days everybody are speaking

about anti-virus and some malware can hide in anti-virus and infect your anti-virus also. Author focuses on how to analyze malware in the system by a by studying it is previous behaviors and based on them any one can protect the system.

4. Existing System:

As a long as computer are stable enough to be useful, people find to cause problems. Most effective mischief on computer to spread malware, worm or virus. Cyber docs are responsibility for malware. Mostly business or individuals are found to face cyber-attacks. Any business can face different cyber threats like malware, phishing, password attacks, DDoS, man in the middle, drive-by download, malvertising and rogue software. Malware is a variety topic that is used for cyber-attacks. It is loaded with computer virus, spyware, worms, Trojan horse and adware. Malware is a word that is related to malicious, which can spoil your computer or devices. Malware will do damage to your system. Malware related virus can be email attachments, software downloads and operating system vulnerabilities. Stopping malware by not clicking on suspicious links, updating firewalls and updating operating systems. Phishing attacks are send by email request and ask users to click and enter the personal data. Most of the attacks are on financial institutions the past 3 years have NOT been through brute force attacks on firewall appliances, it has been through acquiring users' passwords, this technique is called Phishing. Phishing is used for stealing confidential data, harvesting login credential and impersonating as shown in figure 2.

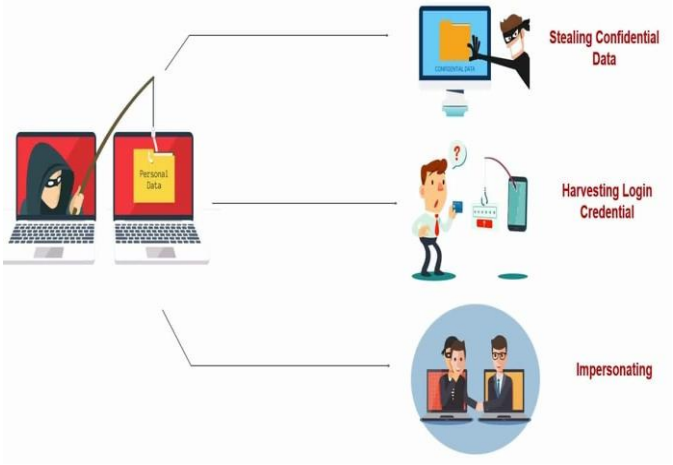

Fig.2 Phishing concept

Phishing email is given as <management@mazoncanada.ca>, where the user thinks he got mail from amazon and provides all the personal info. To avoid please always check the sender email address, look out for common generalized addressing and always hover over links to check the redirect address. Password attacks are an attempt to obtain or decrypt a user's password for illegal use. Hackers can use cracking programs, dictionary attacks, and password sniffers in password attacks. Defence against password attacks is rather limited but usually consists of a password policy including a minimum length, unrecognizable words and frequent changes. Types of password attacks Brute Force Attacks, Dictionary Attacks and Keylogger Attacks. Distributed Denial of Service (DDoS) attacks are a subclass of denial of service (DoS) attacks. A DDoS attack involves multiple connected online devices, collectively known as a botnet, which are used to overwhelm a target website with fake traffic. Man in the middle is between you and the bank. Main in the middle will see all your communication between bank and you. We can prevent MITM by using encrypted WAP, always check the security of you connection (HSTS/HTTPS) and invest in a VPN. Drive-by download attacks occur when vulnerable computers get infected by just visiting a website. Findings from latest Microsoft Security Intelligence Report and many of its pervious volumes reveal that Drive-by Exploits have become the top web security threat to worry about. Malvertising is the name we in the security industry give to criminally-controlled adverts which intentionally infect people and businesses. These can be any ad on any site – often ones which you use as part of your everyday internet usage. It is a growing problem, as is evidenced by a recent US Senate report, and the establishment of bodies like trust in Ads. Rogue software also called smitfraud, scareware, or rogue security software, this type of software is defined as malware – it is designed specifically to damage or disrupt a computer system. In this case, not only is the software going to disrupt your system, it's going to try and trick you into making a purchase using your credit card. To overcome these attacks any organization call for bug bounty scheme to know the vulnerabilities related to their software and go for secure policies which may carry ten percentage of the actual cost of the project. If this exercise is done intervals in between years, it is safe.

According to latest articles the cyber-attacks can arise in future as technology is growing as shown in below fig.3.

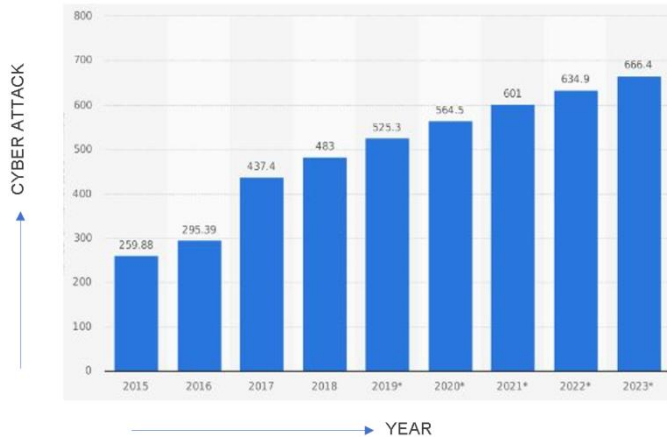

Fig.3 increase ratio of cyber-attacks/crimes

5. Proposed system:

Prerequisites:

1. HTML & bit of CSS
2. Java script
3. Linux command line & shell scripting
4. SQL
5. Programming language -python
6. Basic networking protocols like -HTTP, HTTPS, SSH, FTP &TCP/IP

5.1. Algorithm:

Targeting a bug is not a matter of luck. Instead, it is considered to be a matter of skills and luck. Don't waste time on finding the already reported bugs. Otherwise, you may end up being depressed by the duplication. It is suggested to spend time on understanding the functionality of the application. Also, try making notes and have a track of suspicious endpoints. To earn satisfactory amount for the known issues if you are too early or the first one to report. If you are too early or the first one to report.

5.2. Algorithms steps

Step 1: Reading Books
Step 2: Practicing what you learn
Step 3: Reading proofs of the concept
Step 4: Learning from reports
Step 5: Starting bug bounty hunting by choosing target (like Bugcrowd, HackerOne, Zerocopter etc.,)
Step 6: Chosen target then find the subdomain of the target or we can get IP blocks of the targets which we can get from ASN
Step 7: Subdomain takeover vulnerability
Step 8: Analyze target
Step 9: Subdomain enumeration
Step 10: Extracting subdomain from NSEC

OWASP Top 10: The OWASP Top 10 application risks that should overcome.

1. Injection. Flaws that can be injected can be as follows SQL, NoSQL, OS, and LDAP, malicious data send as a sql command or question. User may not understand the trick query and may click to execute, they malware will inject into the database.
2. Broken Authentication. Weak passwords may be generated based on unsecure software creation and may be carrying problems related to passwords.
3. Sensitive Data Exposure. There are two types of code; one is secure code and other one insecure code. Secure code is protected and whereas insecure code is not protected. That insecure code is not protected and there is a possibility of theft that code and use for some other purposes like cyber crimes. This happens in between the browsers, users and beneficiary party like hackers.
4. XML External Entities (XXE). Many of the attacks are possible because of the years long back web applications code, no security to the present trends and it is very difficult to maintain such code in force of time.
5. Broken Access Control. When policy making on web applications or client/server architecture machines may not be maintaining properly. At that time, it is time for our fellow hacker friends to gain lump sum dollars so there should be proper policies and rules and regulations on the data to protect it.
6. Security Misconfiguration. Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.
7. Cross-Site Scripting (XSS). XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or

escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

8. Insecure Deserialization. Insecure deserialization of the can lead to dangerous problems.
9. Using Components with Known Vulnerabilities. Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.
10. Insufficient Logging & Monitoring. Third party detecting that an business organization or bank or any amount related company is being hacked after a long days.

Web application risks that should be focused before building any software. Likewise there are so many check lists are released by CERT for building secure software, uploads the details of the latest security breaches, vulnerabilities, cyber-attacks and cybercrimes.

6. Model:

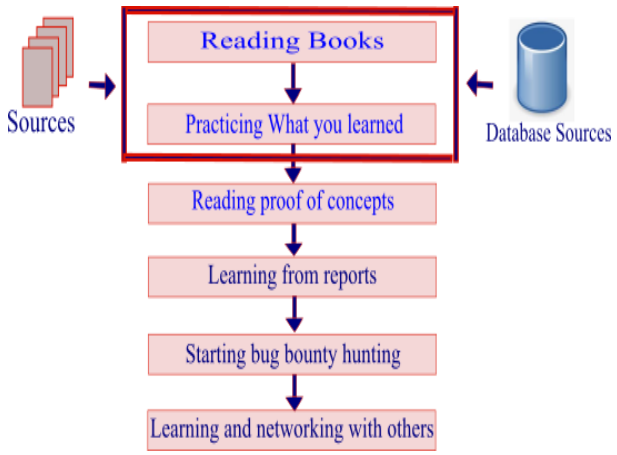

Fig.4: Bug Bounty Methodology

A bug hunter is the reporter who is rewarded for finding vulnerabilities in websites and software as shown in figure. 4. No certificate or qualification is required to become a bug bounty hunter but the architecture of the application and the security issues in application should be read thoroughly. Becoming a bug hunter is also not a matter of age, so get that out of the way. To become a bug hunter, the crucial aspect is to team about web application technologies and mobile applications technologies. These are the things that will kick-start your career as a bug bounty hunter. Usually, if you form a team with a friend or kins, it will help you bounce off ideas and work more closely with them in order to produce better reports and results. There are many books, youtube videos are available online to guide and help you in learning the basics and fundamentals of penetration testing and bug hunting. As bug bounties generally are about to comprise website targets, it is advised to start with website hacking and then move forward. It is essential to focus on the interesting and exciting area of hacking. At the time of learning, it is crucial that you understand and retain whatever you learn. Practice what you have learned in real time. Vulnerable applications and systems are great ways to test your skill set in virtual environments. This will also provide you with an estimate of what you are going to contribute in the real world. Following the tips, by now you may have acquired a brief understanding of how to look for and deal with security vulnerabilities. So, the next step is to check what other bug bounty hunters are finding out and working on. Fortunately, the security community is pretty generous in sharing knowledge and a list of write-ups and tutorials is available to enhance your understanding. This can be done by viewing reports.

Starting of bug bounty is strategic process that can be implemented. By time you read POCs, you are almost to start bug bounty hunting. But to start off with bug bounty hunting, you need to learn how the bug bounties work and how to get started with the procedure. When you are new or at a beginner level, then it is suggested not to try to hack the most public and common bugs. If you start off with hacking, Microsoft, Google, Facebook and other popular platforms, it is likely that you will end up frustrated because these sites are source, as they have received and resolved many bug reports. Instead of targeting such sites, try to focus on the bounties that go ignored and unnoticed by other hackers and hunters. The most exciting thing about hacking is that it is a long journey of learning.

There is always something new and interesting going around about hacking. A number of new articles and presentations are always available to learn from. There are many interesting people and experts to meet at conferences which, creates more opportunities to pursue in this field. Starting bug bounty hunting by choosing target like BugCrowd, HackerOne, Zerocopter and soon. If it is not possible to target the main domain, choose target to find the subdomain of the target or we can get IP blocks of the targets, which we can get from ASN. Sometimes targeting the main domain is not possible to find the bugs which will frustrated to the noobs. There are many tools to find the subdomains like sub finder. In the community have already publish lots of write-ups for sub-domain takeover vulnerability.

https://github.com/EdOverflow/can-i-take-over-xyz

Analyze subdomains how to connect to the target to get the lump sum. Discover the new targets to reach main target domain. Already we are have urls related to target and find whether any leak of week data is available or not, for analyzing this we can use Gobuster tool. Aquatone is used to know whether that website is active or not. Platform identification plays a key role and CVE searching. The bug bounty conducted by various companies as shown in figure 5 and vulnerabilities in table. 1.

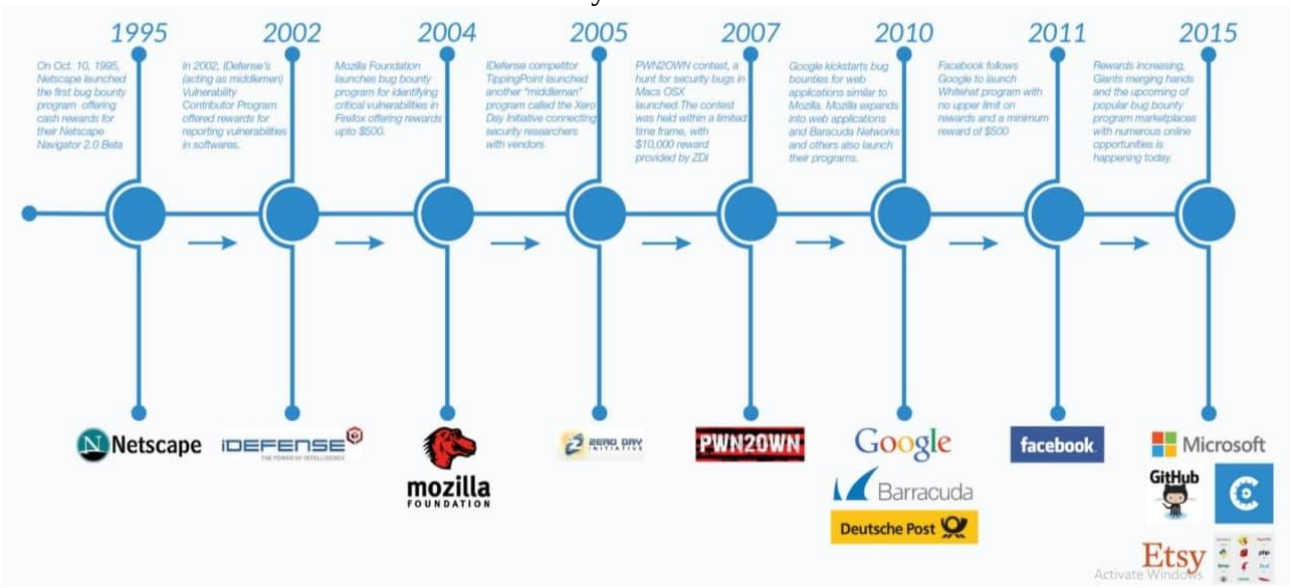

Fig.5 Bug bounty conducted by various companies

Table.1. Vulnerabilities attacks according to CERT

Year	Cases per year in %	Vulnerabilities attacks
2019	52	525.3
2018	48	483
2017	43	437.4
2016	29	295.39
2015	27	259.88

According cert, the attacks are increasing year by year, business or individuals will lose confidence in using stable computer. This never ending process should be stopped immediately. By bug bounty hunting we can prove that whether the written code is secure or insecure. Best example for this is password settings, suppose you were said to have six small letters password such as uae, us, aunty, anitha, kumar and wxyzww – then the space would contain 26^6 or 308,915,776 possibilities. The size of the password space is the product of the possibilities or 26 X 26 X 26 X 26 X 26 X 26 = 26^6. Similarly, if we take two letters password then there can be 26^2 = 676 possibilities to break your password. When we have capital letters, small letters and special characters they the breaking of password is difficult, hackers create software programs to break the passwords that reason for software professionals insist to change the passwords regularly. The size, T, of the possibility space is based on the length, A, of the list of valid characters in the password and the number of characters, N, in the password and D is the time spend by hacker. The size of this space ($T = A^N$) may vary considerably.If A = 26 and N = 2,

then T = 676, D = 0.0000001 computing hour X = 0; it sure that hacker break password.

Conclusions:

We heard about people solving puzzles and buzzwords and big bug bounty programs are also similar programs. Main organizations like amazon, facebook, google, microsoft are focusing on such kind of programs and declare lump sum amount because they want their software to be persistent from cyber-crimes. This is reduce the level of severity and significance of a security vulnerability markets particularly with regard of bug bounty programs. It is important to note that software industries must develop software products with good qualities. NB^2M is the process of find whether the software is secure or not and recommend for safety measures to be followed by the organization/company/industry. The cost of bug bounty may be 10% of the software cost. It is better to check for one year or two years of span for bugs and changes should be made to the software for security of the software.

References:

[1]. Andreas Kuehn and Milton Mueller, "Analyzing Bug Bounty Programs: An Institutional Perspective on the Economics of Software Vulnerabilities", 2014 TPRC / 42 nd Research Conference on Communication, Information and Internet Policy, George Mason University School of Law, Arlington, Virginia, September 12-14, 2014.

[2]. Nirav Bhojani, "Malware Analysis", October' 2014, Conference: Ethical Hacking, Nirma University, DOI: 10.13140/2.1.4750.6889.

[3]. Divya Manusha Seethalam, Valiveti Karthik,, Valluru Gowthami, Gudikandula Radha Krishna Murthy, Prathipati Ratna Kumar, "Software Bug Lilliputians which cause Giant Damage to Systems", available source: 13.pdf (irdindia.in)

[4]. Prathipati Ratna Kumar, Dr. G P S Varma, "A novel probabilistic-ABC based boosting model for software defect detection", A novel probabilistic-ABC based boosting model for software defect detection - IEEE Conference Publication.

[5]. Prathipati Ratna Kumar, Dr. G P S Varma , "Novel Cluster based cross defect classification technique for multiple software defect databases:", www.jardcs.org/backissues/abstract.php?archiveid=2596

[6]. Prathipati Ratna Kumar, Dr. G P S Varma, "A Novel Multi-level based cross defect prediction model for multiple software defect databases", Volume 117 No. 19 2017, 293-301, International Journal of Pure and Applied Mathematics.

[7]. Tebogo Mokoena, Tranos Zuva, "Malware Analysis and Detection in Enterprise Systems", Malware Analysis and Detection in Enterprise Systems - IEEE Conference Publication.

[8]. S Megira, A R Pangesti and F W Wibowo "Malware Analysis and Detection Using Reverse Engineering Technique", Malware Analysis and Detection Using Reverse Engineering Technique - IOPscience

[9]. Satya Narayan Tripathy, S. K. Das, Brojo Kishore Mishra, Om Prakash Samantray, " A Study on Malware Taxonomy and Malware Detection Techniques", A Study on Malware Taxonomy and Malware Detection Techniques – IJERT

[10]. Aayushi Priya, Kajol Singh, Rajeev Tiwari" A Review on Malware Analysis by using an Approach of Machine Learning Techniques", International Journal Online of Sports Technology & Human Engineering, ISSN: 2349-0772| Volume III Issue V October 2016.