A Guide for Security Design

– **Naufil Kazi**
Student of Computer Engineering, Amity University Mumbai
naufilkazi26@gmail.com

– **Deepa Parasar**
Department of Computer Engineering, Amity University Mumbai
deepaparasar@gmail.com

– **Fauzia Siddiqui**
Professor, Department of Mechanical Engineering, JECRC Foundation, Jaipur
fauzia.hoda@gmail.com

Article History
Paper Nomenclature: Scrutiny Tip (ST)
Paper Code: CYBNMV1N6NOV2019ST1
Submission Online: 02-Nov-2019
Manuscript Acknowledged: 10-Nov-2019
Originality Check: 11-Nov-2019
Originality Test Ratio:1%
Peer Reviewers Comment: 14-Nov-2019
Blind Reviewers Remarks 15-Nov-2019
Author Revert: 21-Nov-2019
Camera-Ready-Copy: 22-Nov-2019
Editorial Board Citation: 27-Nov-2019
Published Online First: 22-Jan-2020

With the increasing number of security threats and data breaches it's very necessary to set up a security solution for any system. One can either pay someone to do it or do it himself. Both ways there is always a chance of missing out on something unless we have a perfect guide to tick the completed work. This article intends to do exactly that by putting light on all the factors which are needed to be considered while setting up any system. One may think that this is purely for business purposes but even personal rigs will benefit from this. This is because personal rigs are the ones who have users of different ages and understanding. From where to start and what to consider to what to choose and how much to pay (or do you need to pay) is what the article intents to deliver.

Keywords : System Setup | Security | Threats | Guided Methodology

Introduction

Over the last few years, there has been a trend amongst computer enthusiasts to not use protection for their computers. It might seem okay for everyday use but every so often we get outside our usual list of websites and land up somewhere which might not be particularly safe.

It might also happen that the websites which we were comfortable with have had an attack and are no longer safe.

If that happens there is no way we will be informed about it until a lot of damage is done. The point is that not having a security solution is as good as leaving all your data on the mere hope that it will be safe.

To put light on how a security attack works an experiment was conducted where ransomware was deliberately downloaded to check how it affects the computer.

The site from which it was downloaded offered movies and TV shows for free on the application which was to be downloaded.

To the people who don't consider every movie worth their buck or every streaming service worth monthly pay yet are willing to see most of them are the potential audience of such websites.

Immediately after installing the .exe file an application named 'disk part 32 bit' showed up on the processes tab in the task manager. This was never installed by the tester nor did it come pre-installed in the OS. In the blink of an eye, all the pictures, downloads and videos of the subject computer were replaced by encrypted containers and a 'please read' text file.

The message read, "Oops your important files are encrypted. You will not be able to access them anymore. Your files will be lost on January 7th. Send 600 Dollars' worth of bitcoin."

One may think that a bit of precaution would've stopped this from happening but there is always a window for mistakes. Also, it's not always just one person using a computer, there are many. To expect the same type of reasonable behaviour from those who aren't much familiar with the environment is not a good idea.

So the question arises is what if exclusively only one person will be using a system? In that case, the user may be conscious about the websites he or she visits and the stuff they download. But what if the computer or laptop is destroyed by fire or breaking.

Or simply the laptop is stolen and the hacker makes his way in through the password protection. In such cases, the amount of loss can scale from nothing to everything based on what the user was using the system for.

More on the later side as if the system was used exclusively by one person then it surely had important stuff. Hence, security design is a must no matter whom or how many people are using the system.

Now that we have understood why security should be the main concern in a system let have a look at the factors to be considered before designing the security of a system.

Planning

As mentioned above a security solution is extremely necessary before using any system but how to do it is the main question. Clearly, we can just pay off some service provider to do it for us but even then we won't be sure about what factors the service provider took into considerations.

For example, how many users the provider assumed will be using the system? To obtain complete control and satisfaction about your system security a perfect plan must be made.

Making the plan would take efforts but it's a one-time hard work for overall completeness. The following is a list of things to consider while making the plan.

Vision

Before making anything, not just a security solution, it is very important to know who the potential users of the system are. The system could be installed at a school where students would use it, at the house where family members would use it or at the office where trained professionals would use it.

Also, the environment in which the system would live must be recognized. A place where there would be more than one systems or a place where garbage collection is more has a higher chance of fire than a place with the open wide area around the system.

The average temperature of the room, the stress the system would face, how often the system would be used etc. are some of the points we must visualize before beginning to plan the security solution.

Mission

With the visualization of the conditions the system will live in is done, we need to set a mission or a goal for the system. This will be calculated based on the type of demands the user has.

Different type of users will have different types of needs with their systems. A system for gaming must have a graphics processor, a system for daily tasks must stay cool in temperatures, a system with important files must be safe for external and internal threats etc.

It can be a system which would never be connected to the internet in that case the only security it will need is backup. Hence the mission of the system is important to make any decisions.

Objectives and Strategy

Once we have the vision ready and we know what our mission is regarding the system security we can plan how the security of the system should be designed.

This is done in two stages, first writing down thee objectives and second making a strategy.

For e.g. let's say we are designing the security solution for a school.

Vision:

- Many systems will be kept one besides the other.
- Most of the times the system will be used by kids of age 8-12.
- The systems will be put in a room which will be fully air-conditioned.
- Since it's a school the teachers handling the system may or may not have the complete idea of how the network works.
- A centralized server will be present to monitor the systems.
- The systems will be connected to the internet.

Mission:

- Since the setup will be in a school, a strong system configuration is not necessarily required.
- The systems will be connected to the internet so a firewall will be necessary.
- Students are more likely to click on click baits hence an active antivirus check is needed.
- The systems being used by the students don't necessarily need backup but at the same time, the systems used for updating the school database and also the database needs at least two layers of backup.
- An active website blocking algorithm to keep the kids away from untrusted or harmful websites.

Now since the Mission and Vision are ready we will do the **SWOT** analysis on our system.

Strength: It is an internal concept which determines what is the positives aspects regarding the system internally.

In our example since the system is made for a school, the kids aren't much trained to know how to mess with the system.

They won't visit websites until told to and will not be able to do much until showed how it's done.

Weakness: It is another internal concept which determines what is the negative aspects regarding the system internally.

In the example, since mostly untrained users are using the system, an unintentional error as clicking on clickbait or deleting an entire folder while trying to copy-paste could happen.

Opportunities: This is the concept where we determine how the system will be used for benefits externally.

In our example, the teachers may use the systems to teach the children how to play YouTube videos or how to send a mail.

The kids may also learn how to send files over the internet and download them when needed.

Threats: Directly following the opportunities are the threats.

The kids who have recently learned to make Google searches or put website link can try to put in various websites they hear about around them.

They can also download untrusted files from the internet which at worse could destroy the entire network or use it for cryptocurrency mining.

After the **SWOT** analysis is done we prepare the action plans.

Action Plans

Since we have a complete idea of what kind of a system is needed to be designed we make various plans and present it to the user who will be using it.

The plans will be based on budget and quality. The more the quality of security, the higher will be the budget.

The designing of security should be such that it minimizes the budget and maximizes the quality.

In our example, the systems require a basic antivirus but a strong firewall. Not all systems require backup but those who do need a high level of backup. The hardware needs to be frequently changed as they will be regularly used. A yearly cleanup of software installed by the kids and the files downloaded is necessary. Separate admin login and student login must be created; the student login should not have the allowance to make system changes.

Basic Security Rules

Other than planning our security, there are certain rules everyone should follow in order to ensure a secure system. The following is the list of those rules.

Backup

An ideal user should maintain at least three levels of backup.

1. On System Backup
2. External Backup
3. Offsite backup

An offsite backup will turn out to be helpful in case of hazards such as fire etc.

Updates

Sometimes a security threat is so widespread that the developers themselves make security updates to defend the software against them. So it is very important to at least do all the security updates one receives on their system.

Stock Protection

Some people are against the idea of paying for security as they don't see others using their systems. In that case, it is at least suggested to use the stock protection which comes with the OS.

Though the dangers are high, one can manage to run a system with just stock protection.

Common Sense

Unlike what's shown in the movies, most of the security threats happen because of the user error. So make sure to use common sense before downloading any file or visiting any website. Have a constant look over the website to check if you aren't redirected or being fished.

Conclusion

Data and system security is something that we can fall prey to even if we aren't targeted. Thus it is always necessary to take precautions before we use our system. One doesn't necessarily need to spend money over it but some spending can give much better security. Especially if the system has important documents and is connected to the internet.

Once a plan is ready it needs to be regularly updated as with every new day the attackers are getting stronger. Also, some attackers disguise as security providers so only install a security service if it's trusted.

Reference

- Eastlake, Donald E. "Domain name system security extensions." (1999).
- Bishop, Matt. "What is computer security?." IEEE Security & Privacy 1.1 (2003): 67-69.
- Balu N, Bertram T, Bose A, Brandwajn V, Cauley G, Curtice D, Fouad A, Fink L, Lauby MG, Wollenberg BF, Wrubel JN. On-line power system security analysis. Proceedings of the IEEE. 1992 Feb;80(2):262-82.
- Riedel E, Kallahalla M, Swaminathan R. A Framework for Evaluating Storage System Security.InFAST 2002 Jan 28 (Vol. 2, pp. 15-30).
- Bishop M, Klein DV. Improving system security via proactive password checking.Computers & Security. 1995 Jan 1;14(3):233-49.
- Caceres MG, Richarte GG, Friedman AA, Quesada R, Notarfrancesco L, Friederichs O, Burroni J, Ajzenman G, Becedillas G, Leidl B, inventors; Core SDI Inc, assignee. Automated computer system security compromise. United States patent US 7,228,566. 2007 Jun 5.

Mr. Naufil Kazi is a M. Tech student of Computer Science & Engineering at Amity University Mumbai. He has developed projects entitled "Blind Man Help" which helps Blind People to navigate from one place to another through vibrating signals generated from the Navigation belt. His areas of interest are Python programming, Machine Learning and Security. naufilkazi26@gmail.com

Dr. Deepa Parasar is currently working as Associate Professor at ASET Amity University Mumbai. She has been working in the area of Machine Learning, Artificial Neural Network, Deep Learning and Image Processing. In these fields she has developed projects related to Phishing URLs, Disease Characterization etc.She has been awarded *"Best Faculty of the year 2019"* under sub category Best Faculty - Funded Research - either govt or industry funded research projects at the CSI TechNext India 2019 - Awards to Academia. deepaparasar@gmail.com

Dr. Fauzia Siddiqui Professor & DY HOD of Mechanical Engineering Department Jaipur Engineering College & Research Center(JECRC), Jaipur, Worked as Professor and HOD in Mechanical Engineering Dept. At Saraswati College of Engineering, Khargar, Navi Mumbai since July 2015 till 28.6.18. Awarded as "BEST HOD OF THE YEAR- 2018" by Computer Society of India (CSI) - "TechNext India 2018" held on 10th & 11th Feb 2018, at IIT Bombay. Awarded as a major contributor of ISHRAE Mumbai Chapter in 2017-18. Patent on Solar Electric power distribution and management system for Agriculture purposes.on 5.4.2019. Patent on Design of Compact Paper Recycling Machine on 23.5.17 Member of ISTE,ISHARE & IAENG. fauzia.hoda@gmail.com

Annexure I

Submission Date	Submission Id	Word Count	Character Count
11-Nov-2019	D62285631 (urkund)	2353	11396

Urkund Analysis Result

Analysed Document: paper on security design.docx (D62285631)
Submitted: 11/11/2019 2:56:00 PM
Submitted By: scholastic.seed@gmail.com
Significance: 1 %

Sources included in the report:

https://link.springer.com/10.1007%252F978-0-387-39940-9_523

Instances where selected sources appear: 1

Note: Cybernomics runs an Urkund plagiarism tool for the originality check of an article before publication. Urkund is developed by Prio Infocenter AB based in Stockholm, Sweden.

Disclaimer: All Views expressed in this paper are my own, which some of the content are taken from open source website for the knowledge purpose. Those some of i had mentioned above in references section.

Reviewers Comment

Reviewer Comment 1: Cybercrime is committing a crime with the aid of computers and information technology infrastructure.

Reviewer Comment 2: I think the Cybercrime is committing a crime with the aid of computers and information technology infrastructure.

Reviewer Comment 3: The Hacker culture is an idea derived from a community of enthusiast computer programmers.

Editorial Excerpt

This article has 1% plagiarism; itdefies the security,crime and the use of computers and networks to perform illegal activities such as spreading computer viruses, online bullying, performing unauthorized electronic fund transfers, etc. Most cybercrimes are committed through the internet. Some cybercrimes can also be carried out using Mobile phones via SMS and online chatting applications. Organizations around the globe are investing heavily in information technology (IT) cyber defense capabilities to protect their critical assets. Hence it is marked under **Scrutiny Tip** (ST) category.

Scholastic Seed Inc.
www.scholasticseed.in

Citation

Naufil Kazi, Dr Fauzia Siddiqui and Dr Deepa Parasar
""A Guide for Security Design"
Volume-1, Issue-6, Nov 2019. (www.cybernomics.in)

Frequency: Monthly, Published: 2019
Conflict of Interest: Author of a Paper had no conflict neither financially nor academically.