Artificial Hygiene for Computer Systems

Ashu Sharma
Department of Computer Science
Anand Engineering College
Agra – 282007 (India)

Neha Singh
Department of Computer Science
College of Engineering Roorkee
Roorkee-247667 (India)

ABSTRACT
Artificial Hygiene is the thought taken from the concept of hygiene in daily life. Hygiene is an old concept related to medical, as well as to personal and professional practices that are taken to be care related to most aspects of living. Hygiene practices that are employed as preventative measures to less incidence and spreading of disease, like hand hygiene cleaning the hands before taking food, respiratory hygiene covering the face with hands or hanky on sneezing, food and water hygiene-always put the food and drinking water covered, etc. so hygiene can also be applied on computer machines. So in Computer network, if a system in network is infected the artificial hygiene should ensure that unauthorized or malicious traffic never leaves the infected system/host to other in a network. Hygiene refers to the set of rules that an individual follows in a community to be associated with the preservation of healthy living for whole community that avoid or reduce disease and the spreading of disease in social society. Periodical hygienenical habits may be considered good practices by a society while the neglect of hygiene can be considered disgusting, disrespectful or even threatening. So for this we have to give some rules that an individual computer have to follow to impart hygiene to computers society that means computer network so that the system know how to behave against threat to protect itself as well as help others on the network so that other can also protect themselves from the threat.

Keywords
Antivirus, Digital society, Eradication, Hygiene, Malwares.

1. INTRODUCTION
Artificial hygiene is the approach which prevents the infection to spread among the systems in the network. The infections in the system are due to malwares [5]. Integration of biological community helps to transfer infection from individual to society. Likewise, the computer systems are also connected with each other through networks which provide infection a platform to spread itself to other systems in that network, So for digital disease prevention, digital devices need to take care of both personal and public hygiene. Like, we cover our mouth while sneezing and coughing; in various countries, A law is implemented that an AIDS (Acquired Immune Deficiency Syndrome) patient contains the, 'HIV' (Human Immuno Deficiency Virus) virus should require that the virus should be within himself or herself. These are all part of hygiene, which is **a** process of prevention of propagation of disease**.** In this work I introduce the philosophy of hygiene for digital systems. We call this philosophy "Artificial Hygiene" [1] (AH) for the digital society. Because it is only a digital device that can function as a carrier for digital virus, it must necessarily participate in the mechanism to prevent spread of viruses. Through AH, the device will prevent spread of digital viruses [3]. AH in a device will ensure that a computer protects itself from diseases, also ensure that it does not function as a carrier of a communicable disease as well as it will also alert others so they can also prevent themselves from that disease .

Prof Asoke K Talukder has proposed Artificial Hygiene for email malwares in the paper "Artificial hygiene: a critical step towards safety from email viruses" [1]**,** in which he classified the malwares into different categories and proposed a model which specify which malware lies in which category. He totally stick on email viruses and said nothing about the viruses from other medium. So I decided to work on implementing Artificial Hygiene for computer systems.

In computer networking, artificial hygiene is to ensure that unauthorized or malicious traffic never leaves the infected system/host to other in a network. It's like some peoples in a group sitting at a restaurant and ordered tea for all. After waiter serve tea to every one and one of the person in the group randomly by taking a sip of tea, he realizes that milk in the tea is stale and the tea can make his colleagues sick. Then, what will he do after taking a sip of tea? Simply he will alert others that tea is stale and advice them to avoid it. So others will not take the tea which can make them sick. So same behavior I proposed for computer system.

2. ARTIFICIAL HYGIENE
As we use anti viruses software's for prevention of malwares attack. Anti viruses are also capable of detecting and removal of malwares from the computer systems. They works on signature matching by which the software match the files signatures that are on the computer system to the stored malwares signatures that are in the data bases with the anti viruses. In digital world very high rate of development of malwares is going on, so static malwares bases do not works. That is why antivirus needs to update its virus base within a regular interval. Hence for complete prevention from malware a computer system should regularly update its anti virus base. Generally the antivirus development team provides a server that regularly generates the new malwares signatures and all the anti viruses updates their virus bases from this server, so by all this the antivirus works well. But what if:

- A computer system not able to connect itself to the server.
- Server itself not aware about the new malware for which one of the computer system is suffering.

So if above condition occurs the systems become vulnerable. This problem can be removed if the individual computer system becomes capable to discover new malwares. But discovering all malwares for each system is very much tough task. Where we already having viruses banks that are regularly detected by various antivirus companies. So we have

used both signature matching as well as intelligent malware detection techniques that can detect new malwares. So by using both techniques the computer system does not require extra effort/computation to discover the viruses that we already have with are available virus bases. That is why implementing these methods on computer system make the system secure. But still we are dealing with the computation for discovering new malwares; this computation becomes overhead if we consider more than two systems attached with same network. If a new malware for which we are not having a signature in our virus base attack more than one system, so more than one system have to detect for same malware and have to spend their resources to discover that malware. So this seems to be wastage of resources for same malware which can be even done by only one system. So we have proposed another technique that broadcasts the signature of new discovered malware to other computer systems so that they don't have to waste their resources in discovering the already discovered malware. So combining both techniques we can make the computer system secure as well as optimized in usage of resources.

2.1 Methodology

Analogy to the hygiene rule in daily life we can draw some algorithm for artificial hygiene for the computer system. In this we have to consider the infection caused by the malware and if any of the system get to know that it is infected by some malware then for the sake of hygiene it has the responsibility to inform other system about that malware. So we have to make the algorithm in two phase in first phase the algorithm detects the infection on system and after getting the infection the algorithm should do some action against that infection and in second phase algorithm should make message for other computer systems on the network that an infection is caught by the system and alert other computer systems so that they can do some action against the infection before being infected from that infection and deliver that message to others. This proposed approach is social which means that it does not work only for individual computer system protection from infections but it will work also for other computer systems on the network. Countermeasures to malware fall into three general categories.

- Detection [2]: The ability to recognize and locate malware on a system, in a file on that system, and/or in software, hardware, or media not yet installed on the system.
- Eradication [2]: Removing malware and all of its associated traces (files, processes, system changes), and restoring the system to its pre-infected state.
- Alerting: In this the system should alert other computer systems about the new malware detected in first category. This method helps other systems to counter measure that detected malware.
- These all components should be contained in artificial hygiene algorithm for computer system.

2.2 Proposed Algorithm

In computers the infection can be caused by malwares on the system so the system should be able to detect the infection caused by any malware this detection can be done by an antivirus but generally they work on matching the signatures in their databases so if the malware on the system is new and signature of that malware is not present in their databases then they have to be updated their database and this procedure may take long time. That is why artificial hygiene in computer systems has to implement some intelligent technique to detect the infection on the system. Once the infection is detected then it should search the malware which generate the infection, after getting the cause it will generate the signature of that malware and can update its antivirus database. For implementing hygiene it will send the signature to others on the network to updates their virus databases and prevent them from the infection caused by that malware.

Steps to implementing artificial hygiene

1. Detecting the infection on the system.
2. Detecting the cause of the infection.
3. Evaluation the signature [4] of the malware which causes the infection.
4. Broadcasting the signature of the malware to the network.

In detection of the infection we can use various methods [6] such as

- Behavior detection of malware [9]: malware is detected on the basis of the activities that a malware do.
- Blueprints of malware: we can determine the properties of malware and make profile of malware and by the profile we can decide that the selected file is malware or not.
- Thresholds on usage of resources: we can make threshold on resource usage that an process can use, if a process is using more that resource than that process is declared a malware.

When we know that the process is a malware than we can easily generate signature of that process by any signature evaluation algorithm. after evaluating the signature of detected malware we have to simple alert others by broadcasting that signature of the network so that other can prevent them self from that malware.

2.3 Designed Model

To model the above algorithm is divided into two phases. In first phase detection of malware, evaluation of signature of detected malware and the broadcasting of malware is done. The second phase is divided for receiver side of the signature where the receiving of signature and updating of signature base is done.

In figure 1 the illustrated model of Artificial Hygiene for a computer system, here the whole problem is divided into ten modules to implement Artificial Hygiene as follows.

1. Scanning of the system: Scan the whole file system of the system.
2. Search for the infection: With scanning it check each file for infection.
3. Evaluate the signature: If infection found evaluate the signature of the infection.
4. Broadcast the signature: The discovered signature is broadcast to its network in this module.
5. Encode the transmission: For the reason of secure transmission the broad casting message before transmission is encoded with some encryption mechanism.
6. Decode the transmission and verify the signature: On receiving the broadcast message the receiver will decode the message and verify the integrity of the message.
7. Update the database: In this module the virus data base is updated with the received signature.
8. Regular scan to evaluate signature of system processes: In this module also at the time of

scanning the signatures of each files are re evaluated.

9. Comparison of signatures: This module verifies each file to not be malicious software infected by matching regularly to signature stored in virus bases.
10. Eradication of malware: this module takes the complete responsibility of removal of malicious code from the system.

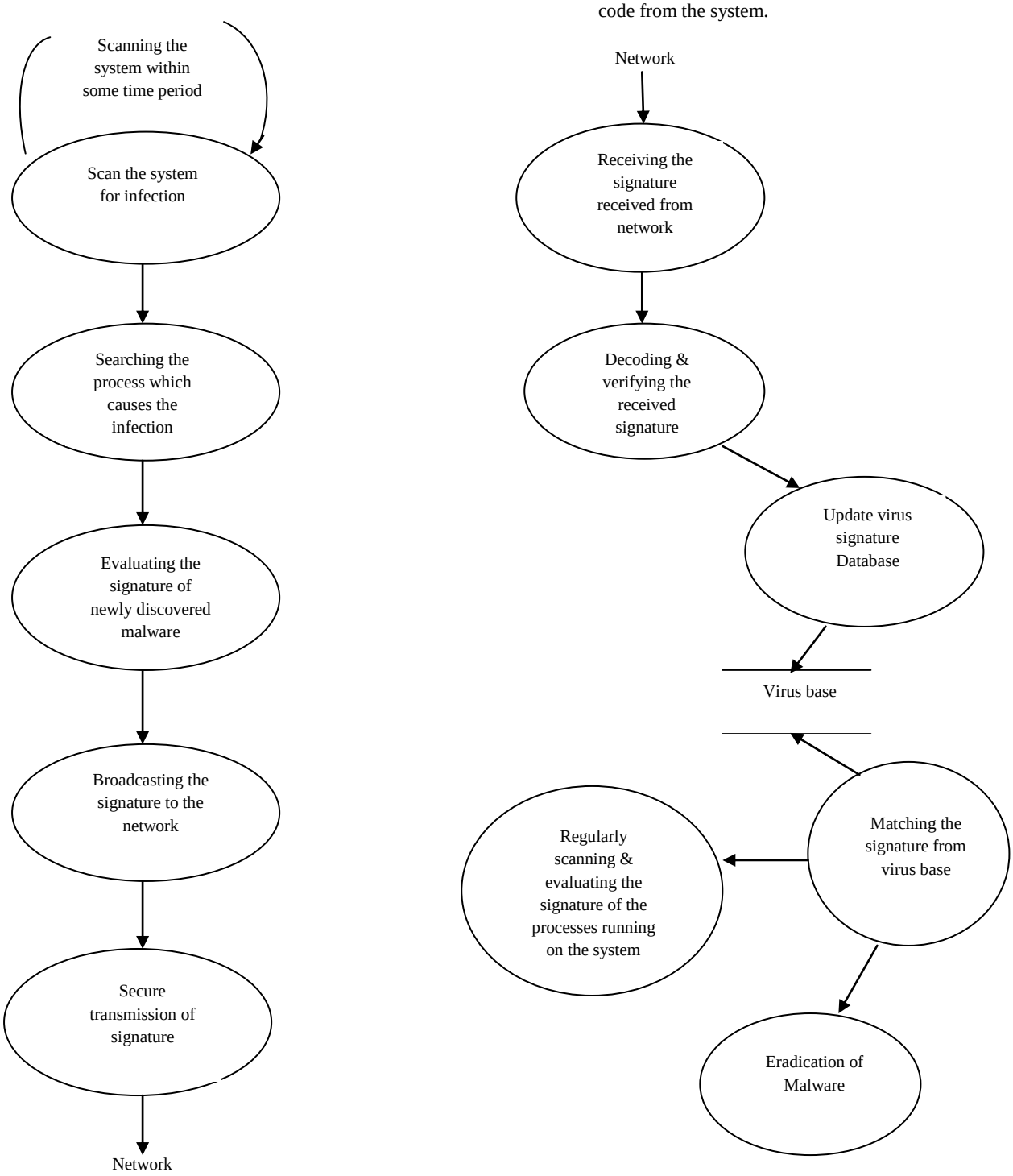

Figure 1: Artificial Hygiene Model for Computer System

3. CONCLUSION

As antivirus can become single point of failure as if the machine acting as a virus base server fails so all the client machine should not be able to update them self and become vulnerable toward the malware attacks. As the above algorithm specified (in sec. 2.2.) for Artificial Hygiene for computer Systems provide us the way to implement the hygiene on computers society which remove this problem because all the systems are not totally depends on a single

machine as they are able to detect new malwares on their own and also can regularly updated by other systems on the network as new malware is detected by any one of the system on the network. As Artificial hygiene makes the computer systems more secure so Artificial Hygiene can replace antivirus for malware security.

As all the systems should able to detect malwares so it use various methods of malware detection and these methods should be regularly added to make the system more capable to detect new malwares. For future work the research to detect new malwares can be done. And another area is to make the transmission of signatures of new discovered malwares more secure otherwise there may be some attacks on the network that may generate false positive malware signature.

4. REFERENCES

[1] Talukder, A.; Rao, V.; Kapoor, V. & Sharma, D. 200.Artificial hygiene: a critical step towards safety from email viruses, India Annual Conference, 2004. Proceedings of the IEEE INDICON 2004. First, 2004, 484-489

[2] Goertzel, K. 2007. Software Security Assurance: A State-of-Art Report (SAR), DTIC Document.

[3] Katerinakis, T. 2010 Graduate Portfolio of Theodoros Katerinakis.

[4] Mell, P.; Kent, K.; Nusbaum, J.; of Standards, N. I. & (US), T. 2005. Guide to Malware Incident Prevention and Handling, US Dept. of Commerce, Technology Administration, National Institute of Standards and Technology.

[5] Erbschloe, M. 2005. Trojans, worms, and spyware: a computer security professional's guide to malicious code, Butterworth-Heinemann. Feinstein, K. 2004. How to Do Everything to Fight Spam, Viruses, Pop-Ups, and Spyware, McGraw-Hill, Inc.

[6] Grimes, R. 2001 Malicious mobile code: Virus protection for Windows, O'Reilly Media.

[7] Scambray, J. & McClure, S. 2007. Hacking Exposed Windows, Tata McGraw-Hill Education.

[8] Kirda, E.; Kruegel, C.; Banks, G.; Vigna, G. & Kemmerer, R. 2006 Behavior-based spyware detection Usenix Security Symposium.

[9] Talukder, A. & Chaitanya, M. 2008 Architecting secure software systems, Auerbach Publications.