International Journal of Communications, Network and System Science, 2014, *, **
Published Online **** 2014 in SciRes. http://www.scirp.org/journal/ijcns
http://dx.doi.org/10.4236/ijcns.2014.*****

Reactive Data Security Approach and Review of Data Security Techniques in Wireless Networks

Arif Sari, Mehmet Karay

Department of Management Information Systems, Girne American University, Kyrenia, Cyprus
arifsari@gau.edu.tr mehmetkaray@gau.edu.tr

Received March xxth 2015

Abstract

There have been various security measures that deal with data security in wired or wireless network, these measures helps make sure that data from one point to another is intact, by identifying, authenticating, authorizing the right users and also encrypting the data over the network. Data communication between computers has brought about countless benefits to users, but these same information technologies has created a gap, a vulnerable space in the communication medium, the data that's been exchanged or transferred, thereby causing threats to the data. Especially data on wireless network are much exposed to threats because the network has been broadcasted unlike a wired network. Data security in the past deal with integrity, confidentiality and ensuring authorized usage of the data and the system. Less or no focus was placed on the reactive approach or measures to data security which is capable of responding properly to mitigate an attacker and avoid harm and also to prevent future attacks. This research is going to expose the mechanisms and measures of data security in wireless networks from the reactive security approaches point of view. Reactive security defender learns from previous attack against future attack instead of relying on the last attack. This paper discusses the reactive approach to data security as well.

Keywords

Reactive Security; Data Security; Mobile-Wireless Network; Proactive Security; encryption; decryption; cryptography.

How to cite this paper: Author 1, Author 2 and Author 3 (2014) Paper Title. *********, *, **-**.
http://dx.doi.org/10.4236/ijcns.2014.*****

1. Introduction

Securing data have not been completely achieved over the years due to different network types and their characteristics, but to a more percentage, data have been secured over a secure network as well. The flexibility of wireless network always makes the access to the network open, because the SSID is always broadcasting. Data are transferred through the use of radio waves and thus making the data available through everywhere in space, enabling the corresponding users to receive the information anytime with the right device in this case a radio receiver. Due to this data protection becomes a pressing issue to deal with. Wired networks are traditionally protected or secured via firewalls, shields etc. while this cannot be done in the case of wireless data protection. Protecting data in wireless environment or networks need a different mechanism altogether, in other to give the users a secure feel in data transfer and have accuracy, reliability, availability, integrity, and confidentiality.

In a world of diverse communication between nodes, wired and wireless devices, and mobile-wireless devices. Data communication has reached a significant point in Information Technology that security of data gives the user an opportunity to share or exchange information securely using the right and appropriate tool. Today banks, government, defense systems all have changed the way data are been exchanged or transmitted, transaction have been compromised in different ways. The communication medium that is been used for data communication are vulnerable to different attacks. The protection of these systems is very important and prominent and this leads to more attacks and loss of important and confidential information when the right measure or system is not installed [1]. Threats comes from hackers, spies, corporate raiders, terrorists, professional criminals etc. they objective are either financial or political gain [1].

In trying to solve the security challenge of today's threats, network professionals became aware of the Proactive and Reactive approach to tackling security vulnerabilities [2]. The Proactive approach secures data by predicting the future of an attack and tends to mitigate that attack. While the reactive approach on the other hand learns from the past attack and use that knowledge to prevent future attacks from happening [2]. The reactive approach to data security in mobile-wireless network is like an Anomaly Detection System, which learn from the previous attack and based on the knowledge gained, it mitigates future attack by crosschecking the behavior of the attack in its database. The reactive approach is a much easier method compared to the proactive method [2].

This paper highlights the security advantage of the reactive security approach in data security in a mobile wireless network and discusses data security in wireless networks. Section two discusses the proactive approach to data security and common attacks known to data in wireless environment. Section three discusses reactive approach to data security and different security mechanisms to ensure data security in wireless network environment. Section four describes topics on cryptography algorithms for data security while section five draws a conclusion on the reactive approach security and concludes research on data security in wireless networks.

2. Data Security

In securing data in the Information Technology environment, more than one method or mechanism is usually applicable to provide availability, integrity and confidentiality. Data communication over public networks should be encrypted using a good encryption algorithm and also a two-authentication method that would only give access to the right user, biometric approach can also be utilized as an authentication method. In data security, these services need to be put in mind:

Table 1. Handling Data Security Issues

Objective	Technique
Confidentiality (privacy)	Symmetric / Private key cryptography
Integrity (has not been altered)	Asymmetric / Public Key Cryptography
Authentication and Non-repudiation (who created or sent the data)	Hashing Algorithms
Data Hiding	Steganography

The Wired Equivalent Privacy (WEP) design is met for securing wired LAN by encryption which uses the Rivest Cipher 4 (RC4) algorithm encrypting messages with a shared key and using a two-side data communication that is the sender and the receiver [3-4]. Data in broadcast or transmission is also prone to threats and they can be manipulated and compromised before it gets to its intended destination. In this kind of environment, (a) Data confidentiality and Integrity must be strong, and there should also be protection for replay messages, this can be achieved by using a cryptographic tool that has the replay protection techniques available. (b) Mutual Authentication, which provides a medium for users communicating to authenticate their identity, and subsequently a key combination is integrated and flexible authorization policies with secured access can be deployed to restrict users. (c) Availability which is also an important measure in data security, the network should be able to stop attackers form shutting down or manipulating the connectivity of the entire system on the network, if this is done appropriately it could prevent denial of service attack DoS or it can mitigate it.

The WiFi Protected Access (WPA), also utilizes the RC4 for data encryption in a wireless network, but it also adopts a Temporal Key Integrity Protocol (TKIP) for its confidentiality. In detecting replay packets or messages in WPA, a sequence mechanism is used to increase the sequence number of each message or packet [4]. The WPA improved authentication methods are Pre-Shared Key (PSK), which authenticates the connected users with a 128-bit encryption key and a distinct 64-bit Message Integrity Code (MIC) which is gotten from the PSK. Also, the IEEE 802.1X and the Extensible Authentication Protocol (EAP) which can be provide a stronger authentication [4]. The IEEE 802.11i provides an improved MAC layer security, provides authentication protocols, key management protocols, and data confidentiality protocols. Another techniques is the use of a Closed System Authentication which hides the SSID broadcast [5]. This only gives access to users who knows the SSID of the network to gain access to the network and join. Other methods to secure a WLAN outside the MAC layer such approach are:

- Physical Layer approach, choosing a good antenna,K and positioning can cut the rate at which signal is lost or leaked, thereby improving security in the network [6].

- RF firewall design which help to protect the WLAN [7]. This requires the 802.11 to be modified in the physical layer.

- IPsec, SSL and SSH are also different approach to securing network connection.

*Special description of the title. (dispensable)

3. Mechanisms for Data Security

Protecting confidential data either in broadcast, transmission or at the intended destination, requires data encryption which is one of the most used mechanism for protecting or securing data in wireless networks.

3. 1 Encryption

This is a process of securing data that is to be transferred between computers. The data needs to be scrambled in a way that it cannot be read without having the right code or key to decode the data [8]. If the message seem hard to break that means the security system is very secure. As shown in Figure 1, a common use of encryption and decryption techniques; in the figure, an unsecured message which is the (Plain Text) is encrypted using an encryption techniques that made the message unreadable (Cipher Text) without having the right decryption code or key. The message is sent over the network and the receiving end decrypts the message with the right key to view the content.

In securing data, the encryption procedures are categorized into two which is Asymmetric and Symmetric encryption techniques. These techniques depends on the type of security key that is been deployed to encrypt or decrypt the data that was secured.

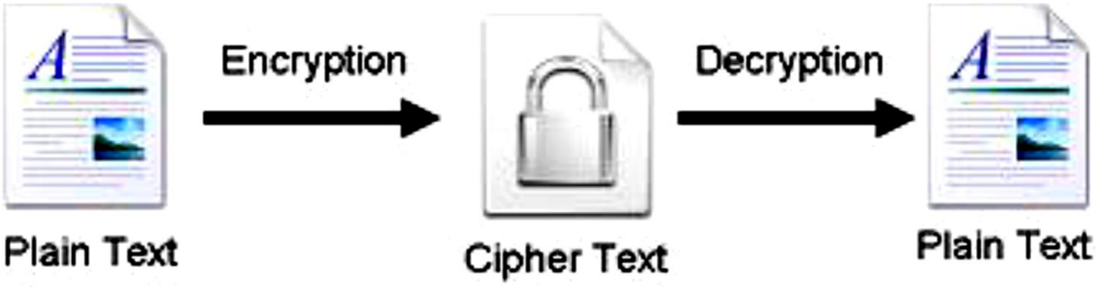

Figure 1.Data Encryption

In general, an RBF network can be described as constructing global approximations to functions using combinations of basic functions centered around weight vectors. In fact, it has been shown that RBF networks are universal function approximators. Practically, however, the approximated function must be smooth and piecewise continuous. Consequently, although RBF networks can be used for discrimination and classification tasks, binary pattern classification functions that are not piecewise continuous (e.g., parity) pose problems for RBF networks Thus, RB The RBF network used in this work is given in Figure 1. It consists of an input layer, one hidden layer and an output layer.

3. 1.1 Symmetric Encryption

This method of encryption give the sender and the receiver the right to set and agree on a shared key, that would be used in encrypting and decrypting the message or data that is to be sent. Afterwards they use the shared key they decided on to encrypt and decrypt their message, this is shown in Figure 2, where Node A and Node B first agree on the system of encryption (cryptosystem) then they move forward to agree on the shared key for encryption then Node A encrypts the message with the key and send over the network, while Node B decrypts the message with the same key to read the actual information.

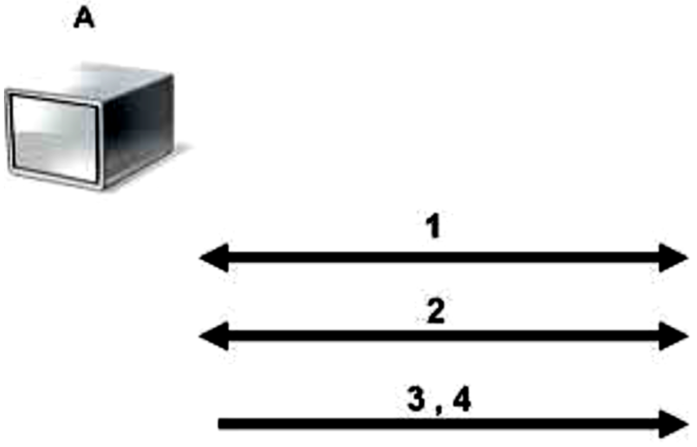

Figure 2.Symmetric Encryption

One of the drawbacks of the symmetric encryption is the means of sharing the secret key between the two nodes that are involved. The whole cryptosystem would fail if the secret key is known by a third party, then it is no longer secret [9].

3. 1.2 Asymmetric Encryption

In this type of encryption, two types of keys are used instead of one shared key compared to symmetric encryption method. That is for example a data is encrypt using KEY1 only KEY2 can decrypt and vice versa. This is because those are the two keys that was created for the encryption and decryption purpose. The public and private key can also be used, the Public Key Cryptography (PKC), the first key is made know to the public (which is the key for encrypting the data) while the private key is only know to the destination user (the one used for decrypting the data). Figure 3, depicts the process of the asymmetric encryption between node A and node B.

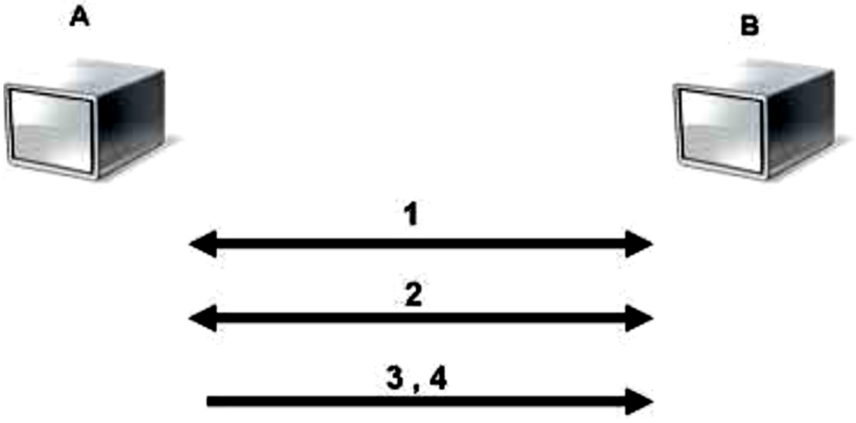

Figure 3.Symmetric Encryption Encryption

In figure 3;

1- Node A and Node B agree on a cryptosystem.

2- Node B sends its public key to Node A.

3- Node A encrypts the message using the agreed public key (Cipher) and Node B’s public key.

4- Node B decrypts the coded message using its private key and the agreed cipher from 1.

Asymmetric encryption techniques are slower than symmetric encryption techniques; this is because they asymmetric encryption techniques need more computational processing power to carry out its process [9-10]. To fix this a hybrid system is usually advised, using the asymmetric encryption method to share the keys while the symmetric method to transfer data between Node A and Node B.

Table 2. Comparison of Symmetric and Asymmetric Algorithm

Symmetric key encryption algorithm	Asymmetric key encryption algorithm
Simple Encryption/Decryption process	Process is Complex
Single Key – Private	Pair of Keys; Private is secret & Public is published to the world
Requires less processing Power & Time	More
Secret Key Management is difficult	Easy Management and maintenance

The table 2 above shows the final comparison between Symmetric and Asymmetric key. This comparison covers different classifications.

4. Major Classification of Data Chiper

BLOCK CIPHER: The data encryption and decryption method used is in a block form, whereby the sender divide the plain text into blocks of plain text and it is inputted into the cipher system which in turn generated blocks of cipher text that would be send over the network to the desired destination. The block cipher have different types that are used such as: ECB (Electronic Codebook Mode), CBC (Chain Block Chain Mode), and the OFB (Output Feedback Mode).

ECB: This form or block cipher, where the data blocks are encrypted and generated directly to form its corresponding ciphered blocks as shown in Figure 4.

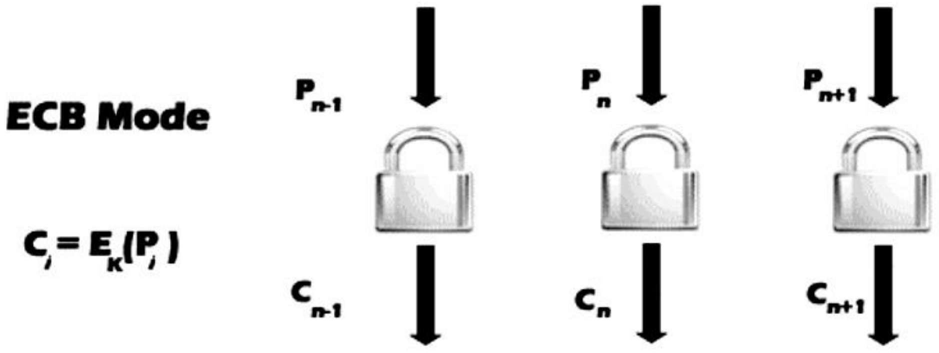

Figure 4.Block Chiper: ECB Mode

CBC: This makes use of the previous cipher block in the current cipher block, forming an encryption-chain process.

OFB: This works more like a stream cipher that uses plain text, where the encryption key that is used on current steps or process depends on the encryption key that has been used before [9-10-11].

STREAM CIPHER: The stream cipher consists of two components: a key stream generator and a mixing function. The stream cipher processes a data bit by bit.

The stream cipher is in two forms:

Synchronous Stream: this form of stream cipher, the cipher key stream generator is dependent on the base key used for encryption, this is shown in Figure 5; how the synchronous stream works, where the sender uses only the shared base key to encrypt the stream that is going out, while the receiver uses the same shared key to decrypt the key. The downside to this method is that if the key is known by a third party, the whole system is compromised.

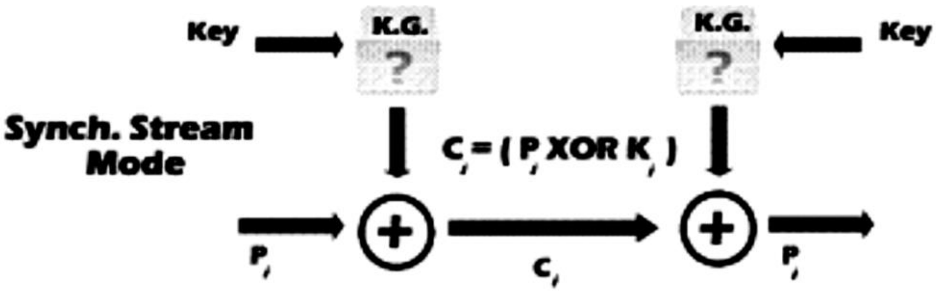

Figure 4.Stream Chiper: Simple Mode (Synchronous System)

Self-Synchronizing Stream Cipher: In this method, the key that is been used at a point or instant depends on the states of the cipher text bits. This method is slower than the synchronous stream method, but it is more secured. Figure 5 shows its process of encrypting and decrypting of data.

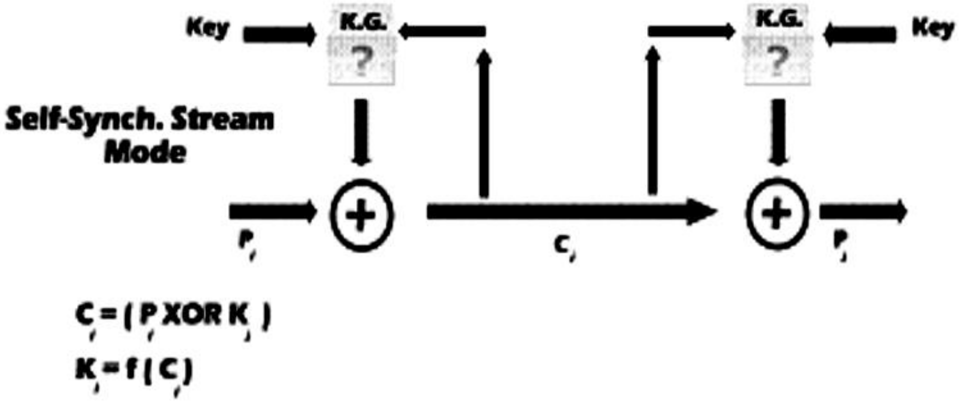

Figure 5.Stream Chiper: Self-Synchronizing Stream Chiper

The speed and simplicity of the stream cipher makes it more preferred compare to the block cipher, but the block cipher is more secured, so the block cipher is recommended [11].

5. Hash Algorithms

Hash algorithms function by converting data of random length into a smaller fixed length, this is commonly known as a message digest [12]. These types of algorithms are considered one-way functions. The generated output varies, making them very efficient when it comes to detecting alterations that might have been made to a message. Hash algorithms are often generated by the DES algorithm to encrypt online banking transactions and other communications where messages can't afford to be corrupted. In Figure 6, the public key is available although it can be distributed alongside the message, although the private key is secret and it is never included in the message. A digital signature it created and is verified by the asymmetric public/private key pair for authentication purposed. Then the sender signs the message content and adds his private key to the message and sends the message with the digital signature that was created earlier to the corresponding receiver or recipient. The digital signature is verified by the receiver with the sender's public key.

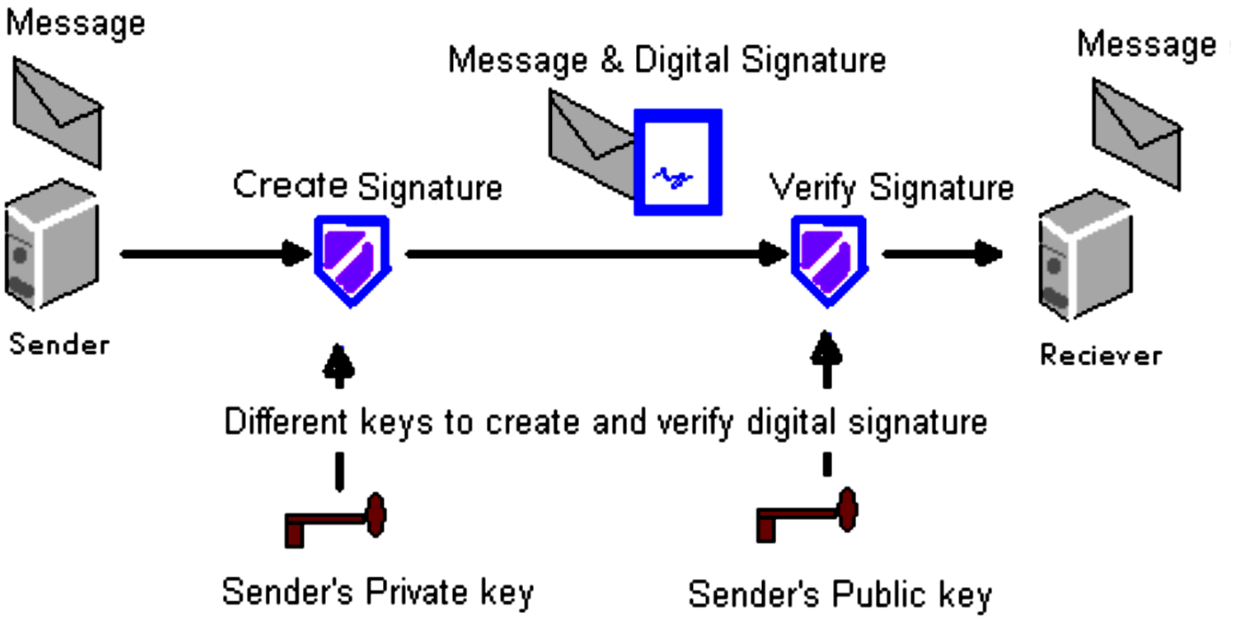

Figure 6.Hash Algorithms

6. Proactive Approach for Data Security

The fact that security threats and risks are apparent in information technology, some threats might be successful while other might not be. The main view of the proactive security is that it reduces the impact of successful attack on the system and prevents loss of data or information while the system is still operational and secure. Proactive security approach in an organization for example, allows the organization to manage their security infrastructure and the values those infrastructure delivers [12].

In proactive security, a). The redemption efficiency is identified proactively and also maximized, that is the weakness of the system is exploited so as to provide a good proactive security agent for future attacks. b). proactive security access the real impact of a potential risk by tracing the paths of critical and non-critical information systems. c). proactive security also assign security resources intelligently in order to fully focus on critical risks while the system is still operational, this helps to minimize or reduce interruptions of business time.

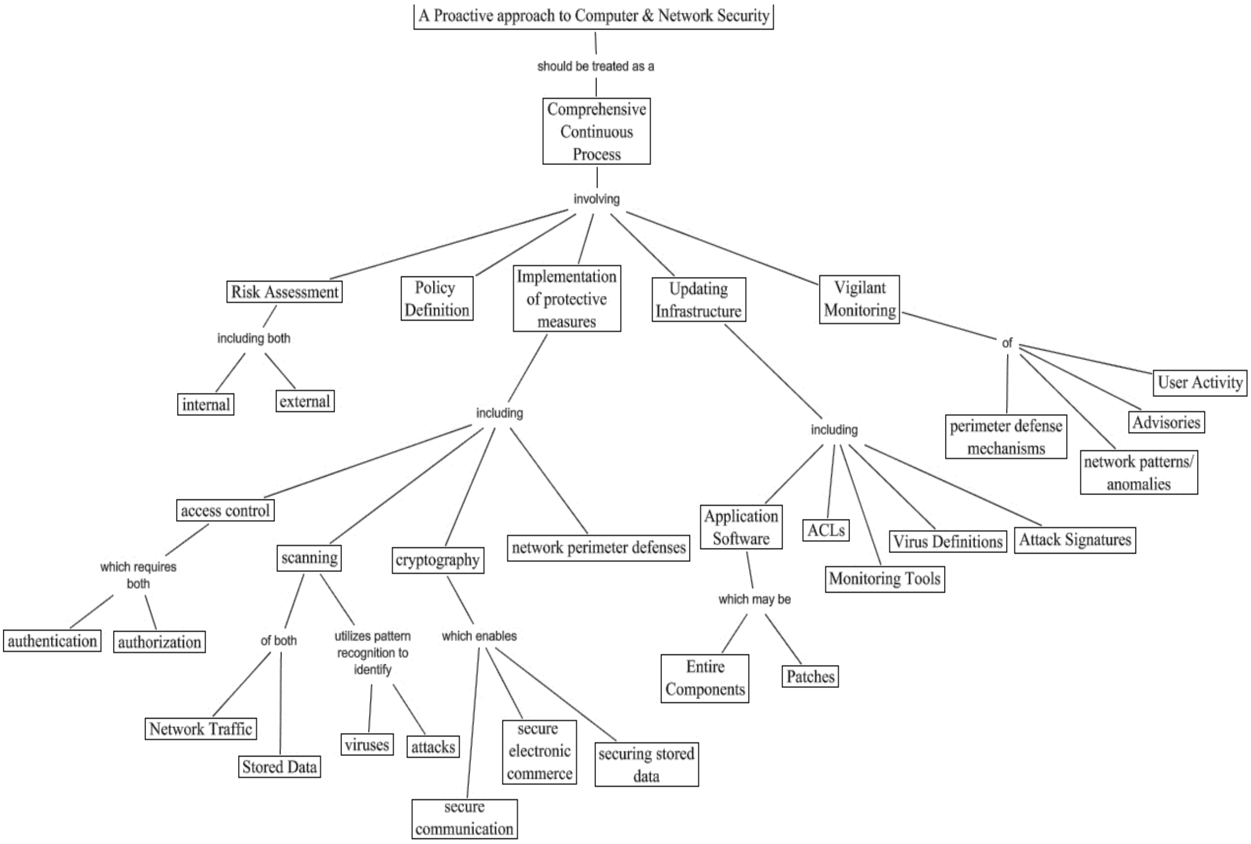

Figure 7.Proactive Approach Architecture

As discussed earlier in the proactive security approach, it anticipates threats behavior, prevent threats or attacks from occurring in the future. The proactive security system is a continuous learning system.

From Figure 7, the proactive system is responsible for risk assessment definition of policies, implementation of proactive measures, updating infrastructure, and vigilant monitoring.

A. Risk Assessment: The proactive system assesses internal and external risk, so as to quickly create a preventive measure if it occurs. This uses a lot of resources because it creates a possible scenario before it happens and also creates a reactive solution to it.

B. Policies Definition: It defines security policies of the network due to its continuous learning capabilities.

C. Implementation of Protective measure: The proactive security system implements the following measure.

- Access Control: This requires both the authorization and authentication process.

- Scanning: It scans the traffic on the network for potential risk scenario and also the stored data traffic is scanned and protected. This is because access would be granted to data stored remotely over the network. The scanning protective measures utilizes recognizable patterns to identify virus threats and attacks on the network.

- Cryptography: This enables the secure communication between nodes in the network, secure electronic commerce for online transaction, and securing data. With this the transaction between the organization and customers would be secured [14 -15].

- Network Perimeter Defenses: this creates a security measure around the full network.

D. Updating Infrastructure: This include the update of various software such as: Application software, monitoring tolls, virus definition, attack signature, and access control lists (ACL) [16].

E. Vigilant Monitoring: This monitors the system for threats and attack signature. The proactive system is responsible for monitoring the perimeter defense mechanisms, network patterns, anomalies, advisories and user activities.

7. Reactive Approach for Data Security

The reactive approach distinguishes itself from the proactive approach by being responsible for securing data after an attack or during an attack. The proactive method of security cannot necessarily be deployed without the reactive method that handles the risk afterwards. In reactive security some measures are put in place like; disaster recovery plan, switching to alternate systems in other locations, re-installation of OS and application if a system is critically compromised [17]. These set of reactive response towards an attack can also be implemented further in the proactive method [17].

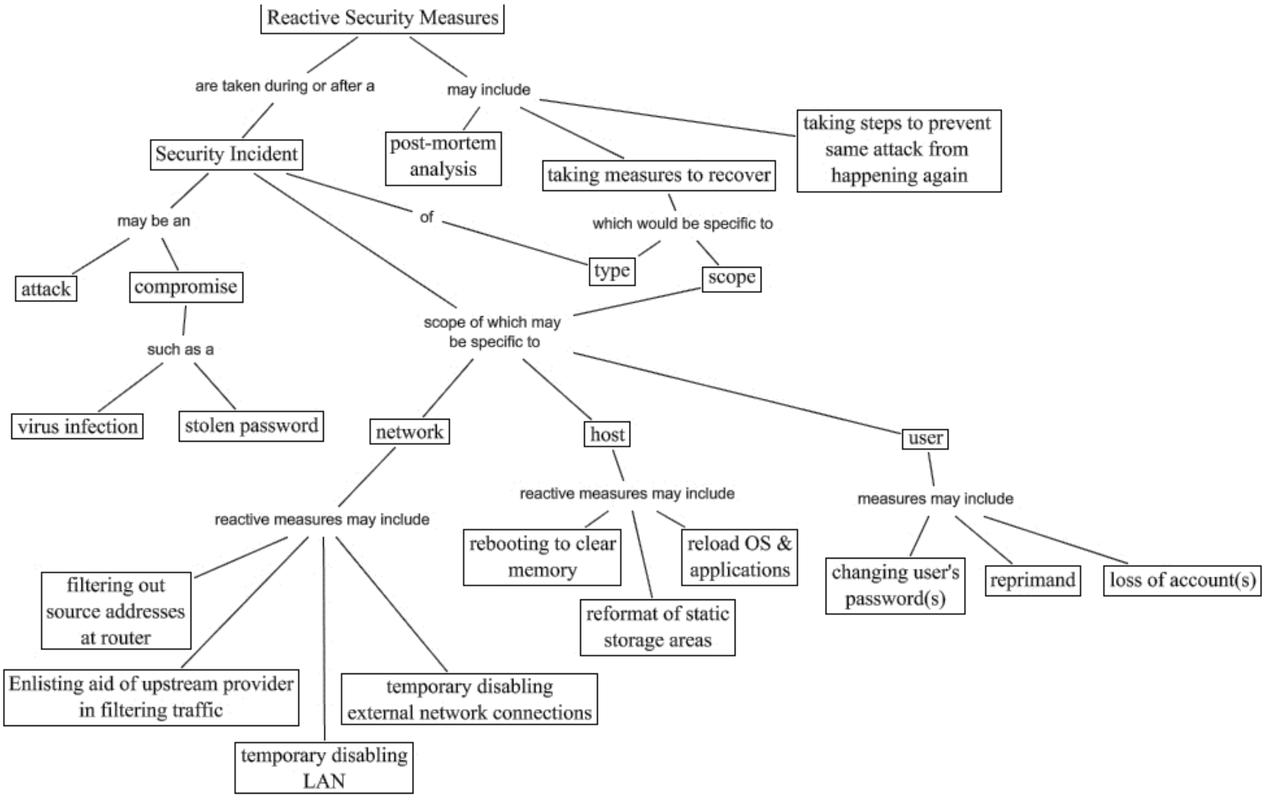
Reactive Security Measures
are taken during or after a
may include
Security Incident
post-mortem analysis
taking measures to recover
taking steps to prevent same attack from happening again
may be an
of
which would be specific to
attack
compromise
type
scope
scope of which may be specific to
such as a
virus infection
stolen password
network
host
user
reactive measures may include
reactive measures may include
measures may include
filtering out source addresses at router
Enlisting aid of upstream provider in filtering traffic
temporary disabling LAN
temporary disabling external network connections
rebooting to clear memory
reload OS & applications
reformat of static storage areas
changing user's password(s)
reprimand
loss of account(s)

Figure 8.Reactive Approach Measures

The reactive security measures are different from that of the proactive security measures, this is because the reactive measures are deployed after or during an attack. From Figure 8, the reactive security measures system is responsible for; security incident, post-mortem analysis, recovery measure, taking steps to prevent same attack from happening again.

A. Security Incident: The incident may be an attack or a compromise such as a virus infection, or a stolen password. In such cases a quick reactive measure is taken to disinfect the file or system if it’s a virus attack and restrict access or cut off users from accessing the corresponding files or system in the stolen password scenario.

The scope of the security incident may change to network, host or user.

- Network: If the network is faced with threats or an attack, the reactive security system will implement the following; filtering out the source address from the router, enlisting aid of upstream provider in filtering traffic, disabling the LAN temporarily and also other external network connection.

- Host: If the host is attacked the reactive measures may include: rebooting to clear memory, reformat the static storage areas, and reload the OS and other application.

- User: In the case of the user, the reactive security system measures may include: changing users password(s), reprimand, loss of account(s).

Reacting to dynamic environment resulted to reactive architecture, where reactive systems obtain their intelligence from the interactions they have with their environment. In the reactive architecture, there's a specific module that is responsible for starting up a direct reaction in response to a specific situation that occur in the environment [14-18]. There is more than one module in the system, if one of the modules fails due to any reason, other modules continue their task. This causes the fault tolerance system of the reactive system to be robust [18-19]. Variety of researches conducted different types of researches in the literature to secure Wireless networks however due to the nature and vulnerable infrastructure of wireless networks, different mechanisms forced reactive data security approaches to become more popular [20-21] .

8. Conclusion

This paper has carefully highlighted reactive security system and how they work. The reactive security system does not observe attacks like the proactive; it looks for the best way to secure the system. The deployment of the reactive security system or measures in either during or after an attack, it depends on the state of the attack. In this paper, we saw that in the reactive architecture the system has more than one module in its corresponding system, if one module goes bad, others will continue to function. This is like an anomaly detection system that detects threats and attacks by continuous learning. The reactive system is good in solving threats or tries to recovery and restricts attacks coming from network, host, or user region in the system.

In data security, it is best to use more than one security measure. In this paper, the proactive security mechanisms is designed to observe ad anticipate threats and or attacks, while the reactive is for recovering data and the state of system under attack or after the attack. Much research has not been done in this area of data security. Our future work would be conducting a comparative and performance evaluation study on the reactive security system over the proactive security system.

References

[1] http://webcache.googleusercontent.com/search?q=cache:OD5cxQI2vHkJ:www.enpointe.com/blog/proactive-vs-reactive-security+&cd=9&hl=en&ct=clnk

[2] B. Schneier. Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley and Sons, New York, second edition, 1996.

[3] IEEE P802.11i/D10.0. Medium Access Control (MAC) security enhancements, amendment 6 to IEEE standard for Information technology - Telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements - Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications, April 2004.

[4] M. Lynn and R. Baird. Advanced 802.11 attack. Black Hat Briefings, July 2002.

[5] T. Marshall. Antennas enhance WLAN security, October 2001.

[6] A. Roy and H. Chang. Physical Layer security of WLANs.

[7] Jason Bonde, Wireless Security, University of Minnesota UMM CSci Senior Seminar Conference Morris, MN.

[8] Real 802.11 Security: Wi-Fi Protected Access and 802.11i ,". Addison Wesley 2003

[9] Security In Wireless LANS And MANS ,". Artech House Publishers 2005

[10] Bulletproof Wireless Security : Gsm, Umts, 802.11, and Ad Hoc Security (Communications Engineering) ,". Newnes 2005.

[11] Reaktive Sicherheit, Ulrich Flegel, Hochschule fur Technik Stuttgart "Reactive Security" IT 54 2012.

[12] http://reseauconceptuel.umontreal.ca/rid=1H030L1LW-2PGQ17-2B22/Proactive%20Security%20Measures.cmap

[13] Darsana Josyula, Reactive Architectures, Dissertation, Department of Computer Science, University of Maryland, Janu-

ary,2006. http://www.cs.umd.edu/~darsana/papers/dissertation/node151.html

[14] L.A. Gordon and M.P. Loeb, "The Economics of Information Security Investment," ACM Trans. Information and System Security, vol. 5, no. 4, pp. 438-457, 2002.

[15] K. Hausken, "Returns to Information Security Investment: The Effect of Alternative Information Security Breach Functions on Optimal Investment and Sensitivity to Vulnerability," Information Systems Frontiers, vol. 8, no. 5, pp. 338-349, 2006.

[16] T. August and T.I. Tunca, "Network Software Security and User Incentives," Management Science, vol. 52, no. 11, pp. 1703-1720, 2006.

[17] http://skat.ihmc.us/rid=1062103427730_993770580_2325/Reactive%20Security%20Measures.cmap

[18] N. Fultz and J. Grossklags, "Blue Versus Red: Towards a Model of Distributed Security Attacks," Proc. 13th Int'l Conf. Financial Cryptography and Data Security, 2009.

[19] A. Barth, B.I.P. Rubinstein, M. Sundararajan, J.C. Mitchell, D. Song, and P.L. Bartlett, "A Learning-Based Approach to Reactive Security," Proc. 14th Int'l Conf. Financial Cryptography and Data Security (FC '10), pp 192-206, 2010.

[20] Sari, A. (2015) "Lightweight Robust Forwarding Scheme for Multi-Hop Wireless Networks". International Journal of Communications, Network and System Sciences, 8, 19-28. doi: http://dx.doi.org/10.4236/ijcns.2015.83003.

[21] Sari, A. (2015) "Two-Tier Hierarchical Cluster Based Topology in Wireless Sensor Networks for Contention Based Protocol Suite". International Journal of Communications", Network and System Sciences, 8, 29-42. doi: http://dx.doi.org/10.4236/ijcns.2015.83004.