International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-3 Number-3 Issue-11 September-2013

Importance of Network Security in Internet of Things

Bhagyashri H. Katole[1], Suresh V.[2]

Abstract

In today's Era of Internet of Things (IoT) where more and more things having heterogeneous nature are brought in the environment with additional Bring-Your-Own-Device (BYOD) concept and promise of IoT to extend "anywhere, anyhow, anytime" computing to "anything, anyone, any service", the network security plays important role in keeping infrastructure up and running. This paper discusses about most common network security threats with exploration of network security components. It also explains the role of network security in IoT environment. It also discussed about security service and its components in our proposed IoT framework. This paper also discusses about present challenges of network security.

Keywords

IoT (Internet of Things), DoS (Denial of Service), Zero-day attack, IPS (Intrusion Prevention System), IDS (Intrusion Detection System), BYOD (Bring Your Own Device)

1. Introduction

As the name "Network Security" itself defines it deals with securing the network. This includes protecting the network and overseeing various operations being done. The network security starts with authentications that includes one-factor authentication like username and password, two-factor authentication including security token and with three factor authentication like fingerprint and retinal scan. Once authenticated, network users are able to access the network services allowed by access policies enforced by firewall. Though this system of firewall is effective to prevent unauthorized access, it may fail to check harmful content like computer worms or Trojans that being transmitted over the network. Techniques used by attackers can be studied by deploying honeypots in the network as surveillance and this is also useful to keep a watch on new exploitation techniques. Such analysis will strengthen the security in actual network. This paper introduces common network security threats in section 2. The section 3 describes network security components. The section 4 introduces the role of network security in IoT environment. The section 5 discussed about security service components in our proposed IoT framework. The section 6 talks about challenges in network security. The section 7 includes the conclusion.

Bhagyashri H. Katole, Senior Technical Officer**,** Networking & Internet Software Group, C-DAC, Pune, India.

Suresh V. Joint Director, Networking & Internet Software Group, C-DAC, Pune, India.

2. Network security threats

Today, many network security threats are spread over the internet. Some of important network security threats are explored below.

- Malicious code and hardware – This category includes viruses, worms, Trojan horses, and spyware. Trojan horses are malicious programs that entered as harmless applications like screen savers, free software. Viruses are malicious bits of code that are hidden in executable programs, a disk's boot sector, or in executable macros. A worm replicates itself through network connections to any machine. Spyware is program that is installed on computer to secretly gather information about you and then information is forwarded to advertisers, companies, or individuals interested in your internet surfing habits. In case of hardware, the threat is that networking hardware made by untrusted companies and counterfeit hardware made in China or elsewhere, may contain malicious hardware or firmware code. This provides a backdoor into corporate systems. [1]
- Zero-day attacks – Here the "zero-day" refers to unknown hole in software that is exploited by the hacker. This exploit is called as zero-day attack. The hackers use these types of attacks in infiltrating malware, spyware or allowing unwanted access to user information. Companies release patches to rectify this vulnerability. Zero-day attacks leads to one of serious type of security risks. [2]
- Packet sniffing and packet forgery – Packet

sniffing is method of tap that is applied to computer network so that each packet on the network can be read. Ethernet cards have a filter that helps to prevent the machine from seeing traffic addressed to other machines or stations. Sniffing programs turn off the filter, and thus able to track every machines or stations traffic. [3] Packet forgery forges packets and sends them in network as part of the normal communication stream. This leads to degradation of user's ability to utilize network resources.

- Denial of Service attack – The basic denial of service (DoS) attack includes overloading a server with too many packets. [4] Distributed denial of service (DDoS) make hosts into "zombies" that will attack on command.
- Identity theft – The hacker attempts to commit privacy breach and gathers personal information concerning individuals in order to do fraudulent acts by tracing their web surfing related activities. There are different types of identity thefts like financial identity theft, criminal identity theft, driver's license identity theft, social security identity theft, synthetic identity theft, and business identity theft. [5]

3. Network security components

There is no single solution that will provide complete security from all types of threats. One needs multiple layers of security. If one layer fails to stop the threat, other layer will filter the same. Network security is accomplished through hardware and software. The software must be constantly updated and managed to protect from emerging threats. If all components work together in network security system, then it minimizes maintenance and improves security. Following are network security components as shown in Figure 1.

- Anti-virus and anti-spyware.
- Firewall, to block unauthorized access to your network. For best results, one can use a firewall that uses user-based authentication. This is especially important for secure access over a WAN, because a firewall that grants access based on an IP address (rather than based on user credentials) allows users through if the IP address of the server running terminal Services has been granted access.
- Intrusion prevention systems (IPS), to identify fast- spreading threats, such as zero-day or zero-hour attacks. The system can be a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. Virtual Private Networks (VPNs), to provide secure remote access. It is a private network that uses a public network (usually the Internet) to connect remote sites or users together.

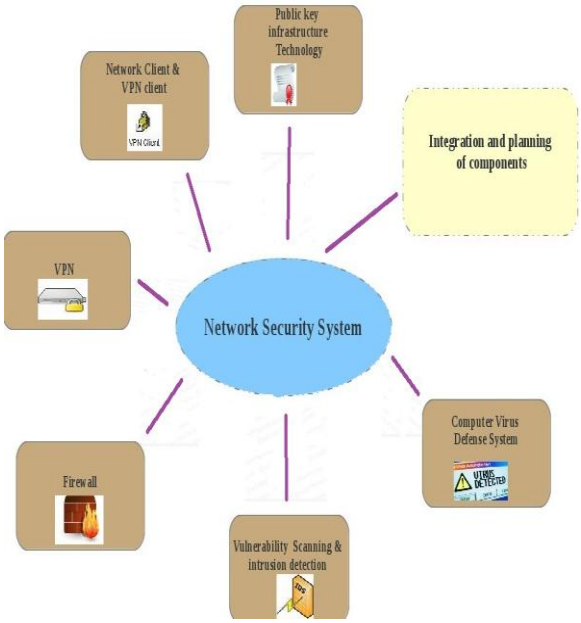

Figure 1: Components of Network Security

4. Network security in IoT

The IoT denotes the interconnection of highly heterogeneous networked entities and networks. The plethora of things like systems, machines, equipments and devices connected to each other and provide intelligent information to users in IoT environment. This leads to the need of security in IoT environment. Following are security threats and vulnerabilities of a network of things in the IoT.

- Reproduction of things – The untrusted manufacturer can clone the physical characteristics, firmware/software, or security configuration of the thing and then sold them at a cheaper price in the market. One can implement additional functionality

like backdoor with cloned thing. [6]

- Malicious substitution of things – During installation, things may be substituted with similar variant of lower quality because of cost saving without being detected malicious things.
- Eavesdropping attack – If security information like keys, security settings are exchanged using wireless medium in network, it is susceptible to eavesdropping and hence authenticity and confidentiality will be compromised.
- Man-in-the-middle attack – Device authentication or device authorization may be nontrivial, or may need support of a human decision process. Thus, even if the key establishment protocol provides cryptographic device authentication, this knowledge on device identities may still need presenting a weak link in the network.
- Firmware Replacement attack – An attacker may be able to exploit a firmware upgrade by replacing the things with malicious software, thereby influencing the operational behavior of the thing.
- Extraction of security parameters – A thing deployed in the ambient environment such as sensors, actuators, etc. is usually physically unprotected and could easily be captured by an attacker. Such an attacker may then attempt to extract security information such as keys or try and re-program it to serve his needs.
- Routing attack – Routing information in IoT can be spoofed, altered, or replayed, in order to create routing loops, attract/repel network traffic, extend/shorten source routes, etc.
- Privacy threat – Attacker tracks all information of user and deduce behavioral pattern and then sold information to interested parties in market.
- Denial-of-Service attack – Things including devices in IoT environment have tight memory and limited computation, they are more prone to resource exhaustion attack. Attackers can continuously send requests to be processed by specific devices so as to deplete their resources. [4] This is especially dangerous in the IoT since an attacker might be located in the backend and target resource-constrained devices. This can be done by flooding the network with so many packets. [7]

In IoT, overall security is required to be achieved in each layer of IoT architecture from providing secured IDs to devices to support of secured protocols like TLS/DTLS. This approach will definitely solve problems for secure IoT in constrained and heterogeneous environment.

5. Security Service In Proposed IoT Framework

Our proposed IoT framework that will take care of standardization, interoperability aspects with the help of which various domain specific applications can be built. [8] The security service of IoT service layer is one of important service that will take care of security aspect in the proposed IoT framework. The security service will consists of various components explored below and shown in Figure 2.

- Authorization component – It provides access control to data that guarantees integrity and confidentiality and it also provides service access control for service privacy and availability. This component is used to perform access control decisions whenever request to access restricted resource comes.
- Authentication component – It is used to provide authentication and accountability for service user. This includes different types of authentications like Knowledge based e.g. Password, PIN, Possession based e.g. memory card, token and Biometric based e.g. fingerprint, iris scan.
- Identity management component – This provides management of identities and related access policies to provide user privacy and service privacy. In case of IoT, creating temporary identities of things will not be enough to secure interaction as malicious subject would be able to track the same. Hence, it deals with creating secure IDs, allocation and management of secure IDs to the things and services.
- Key Exchange and Management component – This deal with exchange of cryptographic keys to provide confidentiality and integrity for communication.
- Trust component – This will calculate user reputation score and calculate trust levels for users and corresponding services.

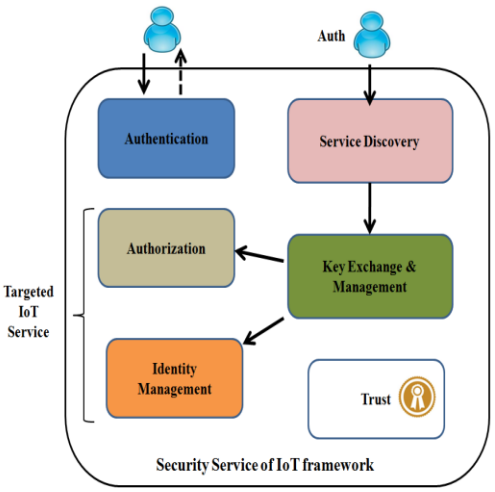

Figure 2: Components of Security Service of Proposed IoT Framework

6. Challenges

Now days, security threats for computer networks have become more technically organized and harder to detect. Because of their technical sophistication, failure to block these threats is increasing. With these observations, following are key challenges for security professionals.

- Network damage because of espionage – Current security technologies and best practices are not effective at preventing security attacks. This fact was known this year when a malicious program called Flame was discovered after evading detection by anti-virus software for years. The consequences of missing attacks like 18 undisclosed security vulnerabilities by Symantec Research Labs can be significant, as it severely affects companies. Hence in order to fight with these attacks, there is need to develop tactics that will focus on behavior of software, systems and actors in the computer network. This analysis and research will certainly help in differentiating suspicious behavior in the network.
- Denial of Service (DoS) attacks – Hackers and attackers are giving more priorities for distributed denial of service (DDoS) attacks. The DDoS mitigation firm Prolexic reported an 88% increase in the number of DDoS attacks launched in Q3 2012 versus a year earlier, with increase in both the duration of the attacks as well as the amount of bandwidth involved. Furthermore, the websites of several large U.S. financial firms were disrupted by a DDoS attack that reportedly exceeded 60 Gbps – much larger than the typical 5-10 Gbps attack. The firms that are effective at protecting their networks against these incidents have: Assessed the risk in advance; developed processes for responding in the event that one of those scenarios occurs; and have tested those processes with real drills in order to ensure that they work as expected when needed. This procedure need to be at top priority for any firm with this era of Internet presence.
- The loss of control – Today, world is moving towards IT consumerization where more features like the cloud are adopted. When workloads move into the cloud, organizations lose control over who can access the computer systems that those workloads are running on. [9] They also often lose visibility into what resources were accessed, when they were accessed and from where. These types of problems are not just limited to cloud, but the technology like Bring-Your-Own-Device (BYOD), there is certainly the loss of control over software load, configuration of network. As the large addresses are more difficult to scan, IPv6 is also going to provide assessment and visibility gaps. Hence, there is need that organizations have to start demanding their network visibility back. The focus is needed to build and design new information technologies with the capability of providing security controls to people who need them. It is the matter of exposing the right information and regaining control in the right way.
- The password disaster – Attackers are constantly scanning the Internet to expose. In 2012, there was large disclosure of passwords and passwords hashes from major websites like YahooVoice, Linkedln, Zappos etc. that were breached. The fact is that passwords, as a security technology, are reaching the end of their useful life. Hence, users need to pick longer passphrases, and proactively auditing networks for weak passwords so that this will help to some extent in providing security. Right now, one need to focus and prepare for attack activity

where attackers enter into networks with access credentials without firing exploit and hence the chances that system like intrusion detection will be helpful in future become less.

- The insider threat – Many organizations have found challenges to develop effective programs that manage the risk of these types of threats. The insider threat has traditionally been viewed as a high-consequence but low-frequency risk. The book like The CERT Guide to Insider Threats is invaluable guide that will help in managing the risk. [10]

We are doing online banking and shopping most of time, it is direct result of working of security professionals. 2013 and coming years promise to be another challenging years for those professionals, but being adequately prepared to address the above threats to keep businesses running and critical infrastructure secure.

7. Conclusion

Today, the IoT is already more than a concept and growing in every aspect. By complying with security requirements, it can fully bloom into a paradigm that will improve many aspects of daily life and provide intelligence. Though standardardization bodies all over the world are working on standardized platform including communication and addressing for the IoT environment, future research must also carefully consider the legal frameworks covering network security aspect with innovation. This will ensure stable progress toward realizing and securing the network of IoT.

References

[1] Hongbo Gao, Qingbao Li, Yu Zhu, Yong Liu, "Code- controlled Hardware Trojan Horse",Information Computing and Applications, Communications in Computer and Information Science, Volume 308, 2012, pp 171-178.

[2] Constantin Musca, Emma Mirica, Razvan Deaconescu,"Detecting and analysing zero day attacks using honeypots" 19th International Conference on Control Systems and Computer Science,2013, pp 543-548.

[3] Ansari, S. ; Rajeev, S.G. ; Chandrashekar, H.S. "Packet sniffing: a brief introduction" published in Potentials, IEEE Vol. 21, Issue: 5, 17-19,2003

[4] Sahil Seth, Anil Gankotiya, "Denial of Service attacks and Detection Methods in Wireless Mesh Networks", International Conference on Recent Trends in Information, Telecommunication and Computing, 2010, pp 238-240.

[5] Esma A¨ımeur, David Schonfeld , "The ultimate invasion of privacy: Identity theft", Ninth Annual International Conference on Privacy, Security and Trust, 24-31, 2011.

[6] Alessandro Brawerman, John A. Copeland, " An Anti-Cloning Framework for Software Defined Radio Mobile Devices", IEEE International conference on communications, 2005, Vol. 5, pp 3434-3438.

[7] IETF draft on Security Considerations in the IP-based Internet of Things,Available http://tools.ietf.org/html/draft-garcia-core-security-05.

[8] Bhagyashri Katole, Manikanta Sivapala, Suresh V., "Principle elements and framework of Internet of Things",Research Inventy: International Journal of Engineering & Science Vol. 3, Issue 5, July 2013, Issn(e): 2278-4721, Issn (p):2319-648, pp 24-29.

[9] Ingo Muller, Jun Han, Jean-Guy Schneider, Steven Versteeg, "Tackling the Loss of Control: Standards-based Conjoint Management of Security Requirements for Cloud Services", IEEE 4th International Conference on Cloud Computing 2011, pp 573-581.

[10] Web: Tom Cross "5 Key Computer Network Security Challenges For 2013" online at http://www.forbes.com/sites/ciocentral/2012/12/11/5-key- computer-network-security-challenges-for-2013/(As of 2nd September 2013).

Bhagyashri Katole is working as Senior Technical Officer of the Network and Internet Software Group (NISG) at C-DAC in Pune, India and has 8+ years of experience. She completed M.S in software systems and having specialization of computer science in B.E. Her areas of interest include network security and cryptography, computer networking, emerging technologies like Internet of Things (IoT) and embedding of products on various embedded platforms. She is currently working on design and development of IoT framework.

Suresh V. is currently working as Joint Director of the Network and Internet Software Group (NISG) at C-DAC in Pune, India. He completed his B.E and MBA. He has a strong 12+ years of experience in area of telecommunication and information technology. His area of interest includes Network Management Systems, Wireless Sensor Network, IoT and cloud computing.