A SURVEY ON NETWORK SECURITY AND CRYPTOGRAPHY

Vikas Lokesh[1], Srivathsan Jayaraman[2], Dr. H S Guruprasad[3]

[1,2] UG Student, [3]Professor and Head,
Dept. of CSE, BMSCE, Bangalore (India)

ABSTRACT

In this paper we describe some of the recent research going on in the field of cryptography and network security. Discussion of these research papers emphasizes the security vulnerabilities of existent as well as new technologies in the field of Computer Networks. We classify the research topics based on their implementation across the seven layers of the familiar OSI reference model, and group the papers together based on their content. The main motivation behind each research paper is explained and the proposed solution is stated briefly, in light of brevity.

Keywords: Network Security, Cryptography, Security Challenges.

I INTRODUCTION

We are living in the information age where information needs to be kept about every aspect of our lives. This information can be thought of as an asset, and like every other asset, this information needs to be secured from attacks. To be secured, information needs to be hidden from unauthorized access (confidentiality), protected from unauthorized change (integrity), and available to an authorized entry when it is needed (availability). Thus, confidentiality, integrity and availability can be termed as the three most important security goals.

Computers have undoubtedly become ubiquitous in today's world and as a result, most of this information is made electronic. Furthermore, with the advent of the internet, this information is now distributed. Authorized users can now send and retrieve information from a distance using computer networks. Although the three aforementioned security goals- confidentiality, integrity and availability- still remain of prime importance, they now have some new dimensions. Not only do the computers containing the data need to be secure, the network also needs to be equally secure.

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Cryptography constitutes an important technique in Network Security. Cryptography is a term used to refer to the science and art of transforming messages to make them secure and immune to attacks. Cryptography involves three distinct mechanisms: Symmetric-Key Encipherment, Asymmetric-Key Encipherment, and Hashing. Symmetric-Key Encipherment uses a single secret key for both encryption and decryption whereas Asymmetric-Key Encipherment uses two keys: one public key and one private key. The sender encrypts the data

using the public key and the receiver decrypts the message using a private key. In Hashing, a fixed-length message digest is created out of a variable-length message, and both the message and digest are transmitted which ensures data integrity.

Although numerous techniques have been developed to ensure security, threats to the network never cease to exist. Consequently, a plethora of research is being carried out in the domain of Network Security. The need to document these researches in an orderly fashion is evident. This paper presents some of the important research papers recently published in the domain of Network Security.

II LITERATURE SURVEY

Shouhuai Xu et. al.[1] proposed new complex systems that can be developed by exploiting trust based social networks (such as Facebook) to store protected data in a distributed manner, using threshold cryptography, to develop certain functional qualities.

Lo-Yao Yeh et. al.[2] discuss peer to peer online social networks that are currently vulnerable without a solid batch authentication method. Three new protocols are proposed, including one way hash function, proxy encryption, and certificates as underlying cryptosystems. These have lower computational cost than the standard methods.

Ralf Kusters et. al.[3] discuss the problem of establishing a standard framework of cryptographic verification of Java and Java like programs which are still open. The noninterference properties of Java like programs can be used to provide cryptographic guarantees; in particular, computational in distinguishability, using simulation based security. This is achieved using a new extended language called Jinja+ , which extends from Jinja. Jinja provides major Java functionality. It is used to provide the framework for cryptographic verification required.

Idoia Aguirre et. al.[4] explain a typical scenario in any corporate network where the network security analysts independently decide on appropriate measures to respond to security alerts. This paper proposes a framework for Security information and event managers (SIEMs) of different domains to collaboratively make decisions in response to security threats which improves security aspects of the corporate network and at the same time significantly reducing the workload.

Mai Abdelhakim et. al.[5] discuss Byzantine fault tolerance which is a subfield of fault tolerance inspired by the famous two generals' problem where a small fault in the initial stages can burgeon into a more complex and complicated problem. The proposed solution in this paper is the q-out-of-m rule which is popular in distributed detection and can achieve a good tradeoff between miss detection probability and false alarm rate in a computer network, which works as such: 'm' random sensors are polled, and if 'q' of them report 1, then the system reports the target as present. However, this scheme is unfeasible for large networks due to high computational complexity; therefore, this paper presents a linear q-out-of-m scheme that can be easily applied to large networks. The paper also proposes an effective malicious node detection scheme and provides simulation examples to illustrate the performance of proposed approaches.

Geetha et. al.[6] discuss Mobile Agent which is a program that moves from host to host performing a specific task. Trust and Reputation Management is a reputation based system where each host has a trust and reputation index. A secure path can be established using TRM for Mobile Agents, allowing several standard attacks to be avoided and networking with remote hosts to be safe and secure.

Jesus Tellez Isaac et. al.[7] explain about the proliferation of mobile systems being used for payments has paved way to expose certain security vulnerabilities. Money transfer can take place through mobile phones via SMS, GPRS, RFID etc and are faced with certain security issues. One of the main issues is that the keys generated by the public-key cryptography technique are too large and augments to the overhead. A new type of cryptography is introduced, Elliptic Curve Cryptography (ECC), which help circumvent this particular problem. The paper discusses another persistent problem which is restricted internet connectivity wherein the merchant has no internet access at the time of payment which exposes the system to security threats. The paper concludes by pointing out that m-payment user and m-payment transactions will see an explosive growth in the upcoming years and security in these m-transactions will remain a paramount issue.

Kui Ren et. al.[8] explain how the data stored in the cloud is extremely vulnerable and needs to be encrypted. However, efficient searching and utilizing the data which is encrypted poses a big problem. The proposed solutions include searchable encryption techniques where users with appropriate tokens can search through data without decrypting it first and thus significantly reducing overhead. The paper then explains how some problems still persist in the techniques of secure multi-keyword semantic search, secure query, and search in non-textual data such as graphs. Another daunting vulnerability is that the integrity and availability of data in the cloud is not guaranteed. The paper concludes by stating that much work needs to be done for a trustworthy public cloud environment to become a reality.

Sakir Sezer et. al.[9] discuss the concept of Software Defined Networking which is a new approach to designing, building and managing networks. It separates the network's control (brains) and forwarding (muscle) planes to make it easier to optimize each. In this environment, a Controller acts as the "brains," providing an abstract, centralized view of the overall network. Through the Controller, network administrators can quickly and easily make and push out decisions on how the underlying systems (switches, routers) of the forwarding plane will handle the traffic. The paper agrees that SDN is capable of supporting the dynamic nature of future network functions and intelligent applications while lowering operating costs through simplified hardware, software, and management. However, many challenges in the area of performance, scalability, security, and interoperability need to be overcome.

Salah k et. al.[10] proposes and analyzes a general cloud-based security overlay network that can be used as a transparent overlay network to provide services such as intrusion detection systems, antivirus and antispam software, and distributed denial-of-service prevention. The paper analyzes each of these in-cloud security services in terms of resiliency, effectiveness, performance, flexibility, control, and cost.

Yu Zhang et. al. [11] discuss bout the authenticity of nodes in an ad hoc network which cannot be guaranteed. Hackers misuse this fact and simulate an active node in the network to carry out malicious activities. An audit based technique is proposed. Nodes which continuously or selectively drop packets are termed misbehaving and this mechanism enables to detect and isolate these misbehaving nodes in a wireless ad hoc network. The paper bolsters its proposed solution by explaining that this technique does not require cumbersome acknowledgement schemes and works well even with encrypted traffic.

Jie Yang et. al. [12] discusses the spoofing attacks in computer networks which have become very common and requires a robust algorithm to detect and localize such attackers. Identity of a node can be verified by cryptographic techniques and digital signatures but it incurs a significant amount of overload. The proposed solution for this is using the technique of special correlation of received signal strength (RSS) to detect spoofing attacks. The paper also proposes cluster based mechanisms to determine the number of attackers which further uses Support Vector Machines (SVM) to locate the attackers.

Shiyu Ji et. al. [13] discusses about the wormhole attacks that are most dangerous as they are independent of MAC protocols and immune to cryptography. Two or more colluding attackers record packets at one location, and tunnel them to another location for a reply at that remote location. This interferes with RIP in the network and poses a fake shortest path to the attacker and the packets are forwarded there. A more complex and robust technique Intrusion Detection is proposed to detect such attacks.

Mohammed et. al. [14] propose stimulating node cooperation, regulate packet transmission, and enforce fairness using a report based payment scheme for multihop wireless networks. Instead of receipts, lightweight payment reports are submitted to the accounting center and undeniable security tokens are stored in the form of "Evidences", so any node suspected of cheating can be asked to submit its "evidence" to verify its authenticity.

Udi Ben-Porat et. al. [15] discusses Distributed Denial of Service attacks that degrade server performance of not only the host but of every client by repeatedly transmitting trivial packets across the network. The study on one of the most common data structures in Network Systems (Hash Tables), attempts to establish effective protection mechanisms against DDoS attacks. This study also contrasts Open vs Closed hashing from a security perspective.

Nayot et. al. [16] discusses the quantification of the overall security of a network. For this, the measure of individual components must be composed in relation to one another. Attack graphs are used for this purpose and can be formulated to determine vulnerabilities in networks. However, models like attack graphs are inadequate when come to measuring the causal dependencies between network states. This paper thus introduces the concept of Bayesian Attach Graphs. Bayesian graphs are directed acyclic graphs with random variables as nodes and edges as conditional dependencies. The paper then proposes a risk management framework using Bayesian Attack Graphs which enables a network administrator to quantify the security level in a deployed network.

Walter Cerroni et. al. [17] explain the recently formulated HTTPS protocol which increases the security aspect of the older HTTP protocol by adding another authentication layer in the form of TLS encryption between HTTP and TCP. The use of digital certificates in electronic communication makes it seem completely secure. This paper explains how an attacker can intercept data transfer by using the techniques of ARP poisoning. The ARP protocol as you may recall, helps in determining the physical address of a node when the logical address is known. Deliberately providing a faulty physical address for a logical address for malicious intentions is what is known as ARP spoofing. The paper then provides a simple but pragmatic example how an attacker can possibly intercept data flow from an otherwise secure connection.

Ahmed et. al. [18] discusses the Digital TV band insecurity against Primary User Emulation Attacks. An AES encryption standard can be implemented to further secure it. By allowing a shared secret between the sender and receiver, the sync bits of DTV data frames can be used to regenerate the sender signal to identify authorized users, thus stopping PUE attacks. It can also detect a malicious presence whether the primary user is present or not.

Guilin Wang et. al. [19] discusses Single Sign On protocol which enables a user with single credential to be authenticated by multiple service providers in a distributed network. This paper explains the Chang-Lee SSO scheme which was assumed to be completely secure and exposes certain fallacies in the scheme. The impersonation attacks may occur in mainly two ways. Firstly, a malicious service provider may use user's credentials to gain access to his account on other legitimate service providers. Lastly, an outsider without credentials may enjoy services freely by impersonating a legal user. The paper then concludes by proposing the use of verifiable encryption of RSA signatures proposed by Ateniese in order to make Chang-Lee scheme more robust.

Yossi et. al. [20] begins by discrediting a commonly believed notion that the internet is vulnerable only to man-in-the-middle attacks and various security measures and protocols have been developed to curb this issue is sufficient to enforce security. A lesser known fact is that the internet is also vulnerable to off path hackers who cannot interject or eavesdrop on packets but can spoof being the host and inject faulty packets into the traffic flow. These so called off path hacker's function mainly in two ways. The first one is termed DNS cache poisoning. Here, the current challenge-response mechanism is inadequate in providing security. The familiar NAT also has certain loopholes which can be misused by keen hackers. The second one is termed TCP injection where the off-path hacker can observe the IP and port addresses and the sequence number in the TCP packet and can easily inject faulty packets in the otherwise genuine stream. The paper concludes by recommending deployment of Cryptographic techniques besides the existing to prevent such off-path hackers.

Stainslaw et. al. [21] discusses A Group Key Agreement cryptographic method by which an entire network can share a single secret key regardless of network/node failures. A GKA can either be flexible but not efficient or efficient but not robust, but new methodologies allow for a fault tolerant GKA to send logarithmic sized messages.

Andrew et. al. [22] discusses about the Authenticated Key Exchange, such as Diffe-Hellman Key Exchange, require both security and privacy. Advantages such as forward deniability, session transcripts that can be generated from DH exponents and non-traceability of the peer involved in message and key exchange are required by Privacy Preserving Authenticated Key Exchange.

Ning Cai et. al. [23] proposes wiretap networks which is a relatively new model. Using the concepts of network coding, the nodes in a network can encrypt the received information from the input links which maximizes security. The Wiretap Network incorporates this concept of network coding with information security. This model includes secret key sharing in classic cryptographic techniques. The construction of secure linear networks is proposed which can be formulated by satisfying the graph-theoretic condition. The paper then discusses several traditional approaches to cryptography in a wiretap network and proposes a rWN, where r subnet wiretap users can legally access the encrypted information.

Takao et. al. [24] discusses about Wolves and Lambs who are those users of biometrics who intentionally or accidentally trigger false positives respectively. A fusion algorithm to prevent wolves and lambs from tampering with biometrics is implemented, using minimum log likelihood ratio based sequential fusion scheme.

Lane Harrison et. al. [25] explain the importance of the concept of visualization not only in representing the prodigious data but also for analysis, specifically network analysis. Several state-of-the-art visualization tools are examined and neatly presented which can perform effective analysis of the security aspects of the network. The paper concludes by explaining how these visualization techniques possess valuable characteristics which are not present in other techniques.

Fan Zhang et. al. [26] discusses WLAN systems which offer shared medium for several nodes to communicate; even encrypted data on a wifi network is susceptible to packet analysis. Traffic Demultiplexing is a new method by which the traffic is shaped to prevent analysis, using the MAC virtualization layer, without any noticeable performance degradation or overhead.

Daniele et. al. [27] discusses about the Real network flows that are an invaluable resource to the research community, including applications like network traffic simulation, etc. Obfuscation of sensitive data involves anonymizing the data involved in the flow so as to ensure that certain attacks cannot be exercised against the flow itself.

Andrey et. al. [28] describes the dilemma faced by the security analysts when they are largely unaware of the motive of the attackers. The defensive mechanism could include considerably fortifying the most valuable nodes and leaving other nodes vulnerable or to fortify all the nodes but not achieve a great degree of security. The paper proposes a solution where the rival's strategies can be carefully analyzed and an appropriate defence mechanism could be incorporated.

III CONCLUSION

As the relevance and importance of privacy of data is continuously increasing, the importance of network security and cryptography is increasing parallely. Providing Network Security is never an absolute process, but rather an iterative one. Hence, Network Security and Cryptography are on the cutting edge of research today.

REFERENCES

1. Shouhuai Xu, Xiaohu Li, Timothy Paul Parker, Xueping Wang, “Exploiting Trust based Social Networks for Distributed Storage of Sensitive Data”, IEEE Transactions on Information Forensics and Security, Volume 6, Issue 1, 2011, pp 39-52, DOI: 10.1109/TIFS.2010. 2093521.
2. Lo-Yao Yeh, Yu-Lun Huang, Anthony D. Joseph, Shiuhpyng Winston Shieh, Woei-Jiunn Tsaur, “A Batch-Authenticated and Key Agreement Framework for P2P-Based Online Social Networks”, IEEE Transactions on Vehicular Technology, Volume 61, Issue 4, pp 1907-1924, 2012, DOI: 10.1109/TVT.2012.2188821.
3. Ralf Kusters, Tomasz Truderung, Jurgen Graf, “A Framework for the Cryptographic Verification of Java-like Programs”, IEEE 25th Computer Security Foundations Symposium, Cambridge, MA, 25 - 27 2012, pp 198 -212, DOI: 10.1109/CSF.2012.9.
4. Idoia Aguirre, Sergio Alonso, "Improving the Automation of Security Information Management: A Collaborative Approach", IEEE Security and Privacy, Volume 10, No. 1, pp 55-59, January/ February 2012, DOI: 10.1109/MSP. 2011.153.
5. Mai Abdelhakim, Leonard E. Lightfoot, Jian Ren, Tongtong Li, "Distributed Detection in Mobile Access Wireless Sensor Networks under Byzantine Attacks", IEEE Transactions on Parallel and Distributed Systems, Volume 25, No. 4, pp 950-959, April 2014, DOI:10.1109/TPDS.2013.74.
6. I G Geetha, C Jayakumar, “Implementation of Trust and Reputation Management for Free-Roaming Mobile Agent Security”, IEEE Systems Journal, Issue 99, 2014, pp 1 - 11, DOI: 10.1109/JSYST.2013.2292192.
7. Jesus Tellez Isaac, Zeadally Sherali, "Secure Mobile Payment Systems", IT Professional, Volume 16, No. 3, pp 36-43, May-June 2014, DOI:10.1109/MITP. 2014.40.
8. Kui Ren, Qian Wang, "Security Challenges for the Public Cloud", IEEE Internet Computing, Volume 16, No. 1, pp 69-73, January/February 2012, DOI:10.1109/MIC.2012.14.
9. Sezer S, Scott-Hayward S, Chouhan P K, Fraser B, Lake D, Finnegan J, Viljoen N, Miller M, Rao N, “Are We Ready for SDN? Implementation Challenges for Software-Defined Networks”, IEEE Communications Magazine, Volume 51, Issue 7, pp 36 - 43, July 2013, DOI: 10.1109/ MCOM. 2013.6553676.

10. Salah K, Alcaraz Calero, J.M, Zeadally S, Al-Mulla S, Alzaabi M, "Using Cloud Computing to Implement a Security Overlay Network", IEEE Security & Privacy, Volume 11, Issue 1, pp 44 - 53, Feb 2013, DOI: 10.1109/MSP.2012.88.

11. Yu Zhang, Loukas Lazos, William Jr. Kozma, "AMD: Audit-based Misbehavior Detection in Wireless Ad Hoc Networks", IEEE Transactions on Mobile Computing, Issue 99, pp 1, Dec 2012, DOI: 10.1109/TMC.2012.257.

12. Jie Yang, Yingying (Jennifer) Chen, Wade Trappe, Jerry Cheng, "Detection and Localization of Multiple Spoofing Attackers in Wireless Networks", IEEE Transactions on Parallel and Distributed Systems, Volume 24, No. 1, January 2013.

13. Shiyu Ji, Ting Ting Chen, Sheng Zhong, "Wormhole attack detection algorithms in wireless network coding systems", IEEE Transactions on Mobile Computing, No. 1, pp 1, PrePrints, DOI: 10.1109/TMC.2014. 2324572.

14. Mohamed M.E.A Mahmoud, Xuemein (Sherman) Shen, "A Secure Payment Scheme with Low Communication and Processing Overhead for Multihop Wireless Networks", IEEE Transactions on parallel and Distributed Systems, Volume 24, Issue 2, pp 209 - 229, 2013, DOI: 10.1109/TPDS.2012.106.

15. U. Ben-Porat, A. Bremler-Barr, and H. Levy, "Vulnerability of network mechanisms to sophisticated DDoS attacks", IEEE Transactions on Computers, Volume 62, No. 5, pp 1031 - 1043, 2013, DOI: 10.1109/TC.2012.49.

16. Nayot Poolsappasit, Rinku Dewri, Indrajit Ray, "Dynamic Security Risk Management Using Bayesian Attack Graphs", IEEE Transactions on Dependable and Secure Computing, Volume 9, Issue 1, pp 61 - 74, Feb 2012, DOI: 10.1109/TDSC.2011.34.

17. Walter Cerroni, Franco Callegati, "Man-in-the-Middle Attack to the HTTPS Protocol", IEEE Security & Privacy, Volume 7, Issue 1, pp 78 - 81, Feb 2009, DOI: 10.1109/MSP.2009.12.

18. Ahmed Alahmadi, Mai Abdelhakim, Jian Ren, Tongtong Li, "Defense against Primary User Emulation Attacks in Cognitive Radio Networks using Advanced Encryption Standard", IEEE Transactions on Information Forensics and Security, Volume 9, No. 5, pp 772 - 781, May 2014.

19. Guilin Wang, Jiangshan Yu, Qi Xie, "Security Analysis of a Single Sign-On Mechanism for Distributed Computer Networks", IEEE Transactions on Industrial Informatics, Volume 9, Issue 1, pp 294 - 302, Feb 2013, DOI: 10.1109/TII.2012.2215877.

20. Yossi Gilad, Amir Herzberg, Haya Shulman, "Off path hacking: The Illusion of Challenge-Response Authentication", IEEE Security & Privacy, Issue 99, pp 1, Oct 2013, DOI: 10.1109/MSP.2013.130.

21. Stainslaw Jarecki, Jihye Kim, Gene Tsudik, "Flexible Robust Group Key Agreement", IEEE Transactions on Parallel & Distributed Systems, Volume 22, Issue 5, pp 879 - 886, May 2011, DOI: 10.1109/TPDS.2010.128.

22. Andrew Chi-Chih Yao, Yunlei Zhao, "Privacy-Preserving Authenticated Key-Exchange over Internet", IEEE Transactions on Information Forensics and Security, Volume 9, Issue 1, pp 125 - 140, Jan 2014, DOI: 10.1109/TIFS. 2013.2293457.

23. Ning Cai, Raymond W. Yeung, "Secure Network Coding on a Wiretap Network", IEEE Transactions on Information Theory, Volume 57, No. 1, pp 424 - 435, Jan 2011, DOI: 10.1109 /TIT.2010. 2090197.

24. Takao Murakami, Kenta Takahashi, Kanta Maatsura, "Toward Optimal fusion algorithms with security against wolves and lambs in biometrics", IEEE Transactions on Information Forensics and Security, Volume 9, Issue 2, pp 259 - 271, Feb 2014, DOI: 10.1109/TIFS.2013.2296993.

25. Lane Harrison, Aidong Lu, "The Future of Security Visualization: Lessons from Network Visualization", IEEE Network Magazine, Volume 26, Issue 6, pp 6 - 11, Dec 2012, DOI: 10.1109/MNET.2012. 6375887.

26. Fan Zhang, Wenbo He, Yangyi Chen, Zhou Li, XiaoFeng Wang, Shuo Chen, Xue Liu, "Thwarting WiFi side channel analysis through Traffic Demultiplexing", IEEE Transactions on Wireless Communications, Volume 13, No. 1, Jan 2014, DOI: 10.1109/TWC.2013.121013.121473.

27. Daniele Riboni, Antonio Villani, Domenico Vitali, Claudio Bettini, Luigi V. Mancini, "Obfuscation of Sensitive Data for Incremental Release of Network Flows", IEEE/ACM Transactions on Networking, Issue 99, pp 1 - 15, Mar 2014, DOI: 10.1109/TNET.2014. 2309011.

28. Andrey Garnaev, Melike Baykal-Gursoy, H. Vincent Poor, "Incorporating Attack-Type Uncertainty into Network Protection", IEEE Transactions on Information Forensics and Security, Volume 9, Issue 8, pp 1278 - 1287, Aug 2014.