Building Security Perimeters to Protect Network Systems against Cyber Threats

A novel way to avoid cyber threats.

By Deepak Puthal, Saraju P. Mohanty, Priyadarsi Nanda, and Uma Choppali

Due to the wide variety of devices in computer network systems, cyber security plays a major role to secure and improve the network or system performances. Although Cyber security is gaining lots of global interest in recent years, it remains an open research space. Current security solutions in network based cyber space give an open door to attacker by communicating first before authentication thereby leaving a black hole for an attacker to enter the system before authentication. This article gives an overview of cyber threats, traditional security solutions, and the advanced security model to overcome current security drawbacks.

1. BACKGROUND

Information and communication technology (ICT) is the key in the realization of the Smart Cities [1]. The underneath technologies including the wireless sensor networks (WSN), Internet of Things (IoT), and cyber physical systems (CPS), facilitate design and operations of such smart cities [1], [2], [3]. The bottom line of all these is connectivity of network wired or wireless networks, to Internet. In the IoT and smart cities, hierarchical IT infrastructure connected sensors, cloud, and command and control center.

TCP/IP (Transmission Control Protocol/Internet Protocol) is still being used as one of the basic communication protocols involving both private as well as public networks (Internet). There are several security methods implemented over TCP/IP protocol such as Internet Protocol Security (IPsec). IPsec is a secured network protocol across IP based networks whose main purpose is to authenticate and encrypt the data packets on an end-to-end basis. IPsec protects data flows between the hosts or any network devices. IPsec supports network-level peer authentication, data integrity, data confidentiality through encryption [4]. However, TCP/IP based security solutions do not provide strong foundation of security as it allows devices to first communicate and then authenticate. In such situations, attackers get a chance to enter into the data transmission process before authentication takes place. To overcome from this situation, Cloud Security Alliance (CSA) proposed a novel idea to authenticate first before communication happens and is called “Software Defined Perimeter (SDP)” [5]. **Fig. 1** shows the clear difference between traditional TCP/IP based security and software defined perimeter.

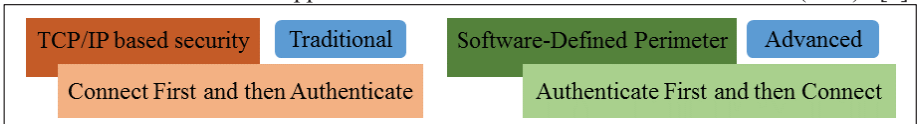

Fig. 1. Difference between traditional security and software defined perimeter

According to the Gartner’s Top 10 Strategic Technology Trends for 2017, adaptive security architecture is listed in the top 10 list [6]. Security in the cyber space is challenging. Multilayered security along with use of user and entity behavior analytics will become a requirement virtually for every enterprise in future. Many security solutions work efficiently under the assumption that the devices and users are fully protected by traditional perimeter defense mechanisms [7],[8],[9]. In several applications, the perimeter-based protections are not feasible since network devices (i.e. sensors) are positioned in unattended environments [10]. Hence, a new security designing approach is appropriate to avoid such circumstances. Recently, industries have advocated three promising approaches as follows: (1) zero trust, (2) deperimeterization, and (3) software-defined perimeter (SDP) [10] [11].

The Zero Trust always follow the principle “never trust, always verify” to architecture the framework [12]. Zero Trust allows for no default trust for any entity (devices, applications, packets, users etc.) regardless of its type or whether it is on or related to the corporate network. Hence, zero trust is appropriate for securing devices as well as users. The term “deperimeterization” is defined a hardened perimeter security strategy which is impossible to sustain within an agile business model [13]. By using encryption and dynamic data level authentication, deperimeterization secure user data on many levels. This multi-level approach fits to the most advanced computing systems such as IoT, cloud computing, edge computing etc., as this work with multilayered architecture. The CSA launched the SDP research initiative in December 2013 with the goal of limiting network-based cyber-attacks against the application infrastructure [14]. Currently, SDP is gaining a lot of interest from global researcher by combining cloud, edges, network devices and users.

2. SDP BASICS

Current IT infrastructures are more hybrid and diversified. At present, the IT infrastructure is moving from hardware-based infrastructure to software-based infrastructure. At the same time, the current IT technology is changing from static environment to dynamic, where users get multiple services simultaneously according to the individual requirement. There is shift from network-centric security solution to user or identity centric approach. This approach will give a better way of security from user perspective and not from network perspective.

In most advanced CSA survey, they found that 68% of the organizations are concerned about security for several reasons such as protecting systems, infrastructure, economic etc. A significant number of the industries are concerned about security. According to the survey, 80% cloud infrastructure are hybrid. In these cloud, the users access to both public and private cloud to perform their tasks. The same survey revealed that 65 % of the IT resources are offside.

SDP alleviates cyber threats in network-based cyberspace by building simple and dynamic security perimeter in any space in cyber data center. In order to provide basic level of security, the SDP begins zero availability and zero visibility. The SDP powerfully constructs systems to authorize applications only after the client has been authenticated. Organizations use SDP to ensure applications visibility on the Internet, for example, cross-organization coordinated effort, and their immigration to IaaS and SaaS services. Organizations use SDP to protect secure inward business basic applications for non-representative and BYOD access, in addition to isolated critical applications.

3. SDP ARCHITECTURE

The threat against application infrastructure increases with the adoption of current critical cyber infrastructure. Since traditional security mechanism cannot protect service provider and edge data center, SDP creates a cryptographic perimeter from a source device to the edges and cloud data center. SDP provides user-centric security solution by creating a perimeter to enclose source and destination within the perimeter. This also dynamically adjusts according to the user requirement. **Fig. 2** provides clear understanding of software-defined perimeter and user access.

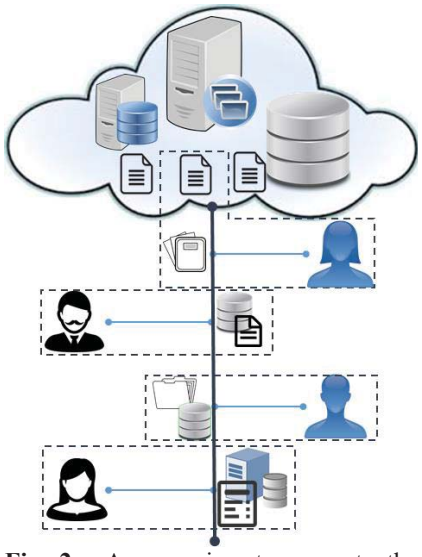

Fig. 2. An overview to generate the simple and dynamic perimeter.

SDP is designed with three major elements [5]: (1) a security model to verify the device identity, or for the users, the roles for access before granting access into endangered systems. (2) Cryptography technique to guarantee the security model was fool-proof. (3) Security solution to address above issues to be demonstrated in broad daylight space security controls.

CSA published the SDP version 1 concept in April 2014. In this design, an Initiating Host transmits user and device identity to a Controller over a mutual TLS connection. The Controller thus would associate with an Issuing CA to an Identity Provider to confirm client identity after checking hardware identity. Once checked, the Controller would then arrange mutual TLS connection between the Initiating Host and the proper Accepting Hosts after proper verification. Once confirmed, the Controller would then arrange at least one common TLS associations between the Initiating Host and the proper Accepting Hosts. More importantly, the SDP can avoid all forms of network attacks including DDoS (Distributed Denial-of-Service) and Man-in-the-Middle.

There are three major components for the SDP designing such as client, SDP controller and set of SDP gateways as shown in **Fig. 3**. The SDP controller initiates the hosts to become a client and a gateway. The Client of SDP architecture grips an extensive range of functions such as user identity to device verification and local to remote applications routing. The Client is formed progressively to guarantee the testament based shared TLS VPN associates with services the client is approved for. The SDP Controller works a trusted third party between the client and SDP gateway. This also provide the services such as a Certificate Authority and Identity Provider to client. SDP Controller arranges both the client and SDP gateway continuously to arrange a mutual TLS

association after verifying the client's authenticity. The SDP Gateway is mainly deployed at the destination end and the TLS connection from the Client terminates at this point.

SDP controller seats online of the network to protect the applications. Wherever SDP controller is a central authentication point and policy store, it always connects to the specific policy model such as, PKI and IM. When user connect to the network, the connection will be authenticated by the SDP controller, followed by controller to evaluate the policies to find whether the requested services are open to that specific user at that time.

When user starts communicating, or accesses the resources from data centers, a secure tunnel is established between user and SDP gateway. Then SDP gateway evaluates the second level of policy evaluation in real-time to determine condition when user is allowed to access these resources. There are three possible situations that arises from this real-time policy evaluation, such as (i) user is allowed to access the resources, (ii) users are blocked and are not allowed to access the resources, and (iii) users need more authentication steps to get access. All these situations ensure that the SDP gateway performs the real-time access control to protect against unauthorized access. SDP works with consistent and meaningful policies.

The network traffic is encrypted from user devices to the gateway by creating secure tunnel. In the process, high level of security is enforced in the network traffic by maintaining data integrity and confidentiality. SDP gateway is always dynamic in nature; it not only checks the user access but also checks the data center resources whether they are allowed or disallowed for user access. SDP protects the high sensitive data by deciding which data should be accessible to which user based on user-access control policies.

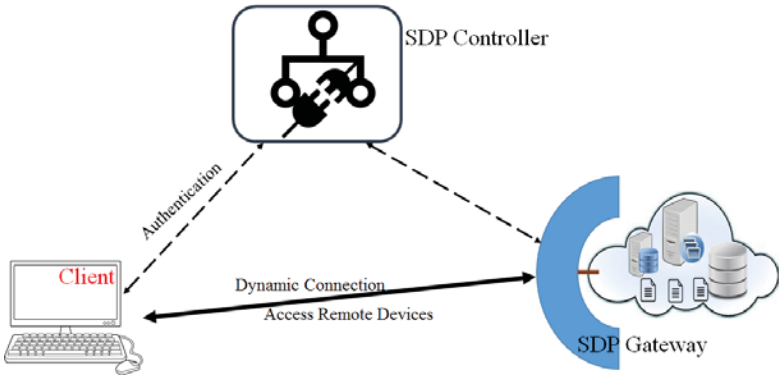

Fig. 3. Authentication process to draw a dynamic perimeter

4. CYBER THREATS ANALYSIS OF SDP

In the network system's possible threats, there are three major possibilities such as: (1) server exploitations, (2) credential theft from users, and (3) attacks during communication [14]. VIDDER's report describes the defeating attacks on network based cyber space as shown in **Fig. 3**. The major possible attacks associated with severe exploitations are DDoS, misconfiguration, and vulnerabilities, where attackers from the Internet try to compromise the server. SDP introduced a gateway named as SDP gateway deployed at datacenter, which always checks the identity and the policies associated with that specific user. SDP isolates the data center and protects using single packet authorization and dynamic firewall functionalities. In result, any kind of malicious requests or query are going to be dropped at the SDP gateway without reaching the data center. In an analogous way, the threats with user or client's credentials are phishing, brute force attacks etc. In SDP architecture, a combination of mutual TLS and client's fingerprint (client's own secret key) is utilized as transparent multifactor authentication. Therefore, no one gets the client's credentials without getting help from SDP controller. Finally, most common attack space in network system is attack on communication, where man-in-the-middle, certificate forgery, DNS spoofing attacks are some of the common cases around [15]. SDP architecture follows first authenticate and then connect by creating a secure tunnel between client and SDP gateway before communication happens as described in previous section. SDP controller provides IP addresses instead of DNS server, so DNS poisoning is not possible. Therefore, it is quite difficult for an attacker to break the security perimeter. Hence, it is evident from above discussion that SDP provides a new level of security to protect networked systems and defending against cyber-attacks.

5. CONCLUSIONS

SDP provides simple and user-centric security solution instead of network or data-centric solution. In an organization, not everyone can see all the network resources rather only the resources allowed for him/her. As network resources are not visible to outsider, this acts as a significant benefit as only inside of the perimeter can see those resources. As SDP adopt technique to authentication first and then communicate, users never get

chance to assess properties of security. Therefore, attackers have very limited information to perform the network-based attacks.

ABOUT THE AUTHORS

Deepak Puthal (Deepak.Puthal@uts.edu.au) is a Lecturer in the School of Computing and Communications at University of Technology Sydney (UTS), Australia. His research interests include cyber security, Internet of Things, distributed computing, and wireless communications. He has a Ph.D. in Computer and Information Systems from UTS, Australia. He has published in several international conferences and journals including IEEE and ACM transactions.

Saraju P. Mohanty (saraju.mohanty@unt.edu) is a Professor at the Department of Computer Science and Engineering, University of North Texas. He is an inventor of 4 US patents. He is an author of 220 peer-reviewed research articles and 3 books. He is currently the Editor-in-Chief (EiC) of the IEEE Consumer Electronics Magazine. He is on the editorial board of peer-reviewed journals such as IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems and ACM Journal on Emerging Technologies in Computing Systems. He has been the Chair of Technical Committee on Very Large Scale Integration (TCVLSI), IEEE Computer Society (IEEE-CS) to oversee a dozen of IEEE conferences. He serves on the steering, organizing, and program committees of several international conferences. More about him is available at: http://www.smohanty.org.

Priyadarsi Nanda (Priyadarsi.Nanda@uts.edu.au) is a Senior Lecturer in the School of Computing and Communications at University of Technology Sydney, Australia. He has over 26 years of experience in the area of Cyber Security, IoT Security, Networks Quality of Service (QoS), Assisted Healthcare using Sensor Networks, and Wireless Sensor Networks. He has a Ph.D. from University of Technology Sydney, Australia. He has published over 70 refereed research articles.

Uma Choppali (umachoppali@gmail.com) is currently an adjunct faculty at Brookhaven College, Dallas. She obtained a Ph.D. from the University of North Texas in 2006. She has a Masters from Indian Institute of Technology Bombay, India. She has authored a dozen of peer-reviewed articles.

REFERENCES

[1] S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything You wanted to Know about Smart Cities", *IEEE Consumer Electronics Magazine*, Volume 6, Issue 3, July 2016, pp. 60--70.

[2] M. L. Rajaram, E. Kougianos, S. P. Mohanty, and U. Choppali, "Wireless Sensor Network Simulation Frameworks: A Tutorial Review", *IEEE Consumer Electronics Magazine*, Volume 6, Issue 2, April 2016, pp. 63--69.

[3] S. Sharma et al., "Rendezvous based Routing Protocol for Wireless Sensor Networks with Mobile Sink," The Journal of Supercomputing, vol. 73, no. 3, pp.1168-1188, 2017.

[4] S. Raza, S. Duquennoy, J. Höglund, U. Roedig, and T. Voigt, "Secure communication for the Internet of Things—a comparison of link-layer security and IPsec for 6LoWPAN", *Security and Communication Networks*, Vol. 7(12), pp. 2654-2668, 2014.

[5] Cloud Security Alliance (CSA), https://cloudsecurityalliance.org/group/software-defined-perimeter, Accessed on 15:05:2017.

[6] Gartner's Top 10 Strategic Technology Trends for 2017, http://www.gartner.com/smarterwithgartner/gartners-top-10-technology-trends-2017/, Accessed on 15:05:2017.

[7] D. Puthal, S. Nepal, R. Ranjan, and J. Chen, "DLSeF: A Dynamic Key-Length-Based Efficient Real-Time Security Verification Model for Big Data Stream", *ACM Transactions on Embedded Computing Systems (TECS),* Vol. 16(2):51, 2017.

[8] D. Puthal, X. Wu, S. Nepal, R. Ranjan, and J. Chen, "SEEN: A Selective Encryption Method to Ensure Confidentiality for Big Sensing Data Streams", *IEEE Transactions on Big Data*, (In press), 2017. DOI: 10.1109/TBDATA.2017.2702172

[9] A. Nanda et al., "SecureGLOR: An Adaptive Secure Routing Protocol for Dynamic Wireless Mesh Network", in *Proceedings of the 16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-17)*, 2017.

[10] D. Puthal, S. Nepal, R. Ranjan, and J. Chen, "Threats to Networking Cloud and Edge Datacenters in the Internet of Things", *IEEE Cloud Computing*, Vol. 3(3), pp. 64-71, 2016.

[11] E. Bertino, K-K. R. Choo, D. Georgakopolous, and S. Nepal, "Internet of Things (IoT): Smart and secure service delivery", *ACM Transactions on Internet Technology (TOIT),* Vol. 16(4):22, 2016.

[12] National Institute of Standards and Technology, "Developing a Framework to Improve Critical Infrastructure Cybersecurity", NIST RFI 130208119 -3119-01, submitted 4 Aug. 2013.

[13] Jericho Forum, "de-perimeterization", https://collaboration.opengroup.org/jericho/presentations.htm, Accessed on 15:05:2017.

[14] Vidder, "Software Defined Perimeter," 2016; www.vidder.com/why-vidder/software-defined -perimeter.html.

[15] D. Puthal, "Secure data collection and critical data transmission technique in mobile sink wireless sensor networks", *Masters Thesis, National Institute of Technology, Rourkela*, 2012.