Building more secure and privacy enhanced smart grid infrastructure - a network security perspective

Sandeep Kadagathur Vadiraj, *Masters in Cybersecurity, University of Southern California*

Abstract-- The proposed Smart-grid infrastructure aims to make use of the existing public networks such as internet to send the data collected from the houses of the customers to the public utility network. The Smart-grid (smart grid) adopts smart-meters which basically collect vast amounts of data that can provide the holistic view of the customers behavior and preferences pattern relating to the power and water consumption. The smart-grids provide benefits to the utilities and consumers alike. For utilities the benefits are real time data collection, ease of power management, reduced requirement of personnel. The benefits for the users on the other hand are real time data based on usage, information on ways to minimise the power usage, monetary savings to list a few.

Since, the smart-grid uses the existing public networks the utilities do not have the burden of laying the cables or installing any new infrastructure (except for installing the smart-meters, themselves) so the utilities find it advantageous. But, the downside to using the public network is that they are susceptible to variety of network attacks if not guarded well against. This paper talks about the various network architecture vulnerabilities that exist in the Smart-grid networks and measures to patch those.

Index Terms--
IP networks, Network, Privacy, Public keys, Smart Grid, VPN

I. Introduction

The Smart Grid network makes use of the IP technology to make a two-way communication between the customer site and the power utility. The networks carrying smart-grid data carries with them sensitive data like power usage of the customers, health and behavior of the assets, along with control class of the information to control the smart grid equipment remotely. This calls for the approach which has to secure the infrastructure on several layers. The most important of the layers that needs to be guarded is the network or the IP layer. It is because the network layer is responsible for packet forwarding including routing through intermediate routers, whereas the data link layer is responsible for media access control, flow control and error checking.

The OSI model is based on the layered approach. It divides each of functionality into separate layers. It is due to this approach taken in the OSI layer there is no inherent mechanism to communicate the occurrence of an event such as attack to another layer. To overcome this limitation it becomes necessary to defend or secure each of the layers in the OSI model separately.

The IP is a routed protocol meaning, IP is designed to be routed over and through different networks.

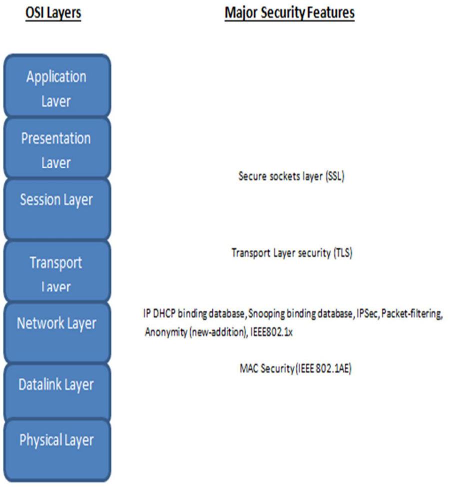
The network layer provides the functional and procedural means of transferring variable-length data sequences from a source to a destination host via one or more networks, while maintaining the quality of service functions. The protection of this layer becomes the most essential part of any network architecture making use of the IP technology.

Each of the OSI layers has several key functions and for communication between the OSI layers they usually employ different protocols. Each layer employs several different protocol/s and is often subject to attacks by the malicious users. In the evolution of these technologies several mechanisms have been developed to defend against such attacks.

There are several methods to provide security at application (Layer 7), transport (Layer 4) and data link layer (layer 2) of network but network layers (Layer 3) security has not been adequately addressed. Even though switches (L3) and routers have built in security features they are not enough to fully ensure the security of network layer. Security at each layer is discussed in detail under section II. The presentation (Layer 6), session layers (Layer 5) and the physical layers (Layer 1) themselves are mostly passive and no attacks are devised to subvert their functionality

The IPSec is often looked as the one stop solution to solve all of the layer-3 vulnerabilities. It will no doubt address major problems like providing confidentiality to the data using cryptographic protocols. But, the information needs to be protected from the confidentiality aspects but we also have the responsibility of guarding the network resources to provide the integrity and accountability which form the complete security triad.

The OSI layer with the primary security features are depicted below:


OSI Layers
Major Security Features
Application Laver
Presentation Laver
Session Layer
Transport Laver
Network Layer
Datalink Layer
Physical Layer
Secure sockets layer (SSL)
Transport Layer security (TLS)
IP DHCP binding database, Snooping binding database, IPSec, Packet-filtering, Anonymity (new-addition), IEEE802.1x
MAC Security (IEEE 802.1AE)

II. LAYER 3 SECURITY THREATS ON THE SMART-GRID NETWORKS

There are broadly three types of attacks one with motivations to disrupt the smart-grid network, the second type of attack is the analysis of the smart-grid network to collect confidential user information traveling over the smart-grid. The third is the attack to confidentiality and integrity of the data by false data injection or changing the data in transit. The threat to the availability of the services on the smart-grid is an active attack and such attacks are felt immediately and the other is the threat to privacy of the user information which falls under the passive attack are harder to detect.

The businesses handling the data from the Smart-grid are accountable for the protection of the privacy of the consumer's data from leaving the infrastructure. So, this paper tries to counter such problems by adding Chaum's mixer network to provide the privacy aspect of the security as well. Along with it a new approach to security is proposed.

By encrypting the data at Layer 3 we can secure everything above it and prevent lot of vulnerabilities. Layer 3 security alone is quite essentially the demarcation point of network security.

In any network including that of the smart-grids we have three different types of traffic flowing through namely the management plane traffic(management goals of the network), the control plane traffic(in order to restrict and police) and the data plane traffic(the user data is carried on this plane).

The attacker will try to compromise the network security by attacking the vulnerabilities in any of the above planes. Of all the planes upon which the attack can be leveraged it is easier for the attacker in the smart-grid to defeat the security mechanisms in the data plane. This is because the data plane traffic in the smart-grid case originates from the homes of the consumers and is most often unmonitored.

Some of the attacks that can be leveraged on the layer 3 of the smart grid are: IP Spoofing, IP Routing attack, Denial of Service (DoS) attack, Attacks such as MITM to spoof the destination address, Attacks such as passive network monitoring to get data traffic to collect the private information such as usage details and billing information.

A. IP Spoofing attack:

In computer networking, IP address spoofing or IP spoofing is the creation of Internet Protocol (IP) packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system. This attack is usually combined with the DoS attack or to repudiate the integrity of the source.

IP Source address validation can prevent the IP address spoofing attack. There are primarily two methods available to block these attacks they are Ingress filtering as mentioned under the RFC 2827. This technique lacks the ability to distinguish the spoofed source IP packets if they are originating from the same network. A better approach to this is the Source Address Validation Improvements (SAVI) [2]. The SAVI technique actually binds the IP address to its data link layer address and enforcing the IP source addresses match the binding to which they are bound.

The attacker might sometimes try to spoof the IP address of the DHCP servers. If security features are not enabled on the layer-2 (like DHCP trusted port) then the attacker might be able to fake the DHCP server and improperly route all the traffic the way he wishes.

The SAVI technique can be added when DHCP snooping is enabled on an untrusted interface. After IP Source Guard (IPSG) is enabled on an interface, the switch blocks all IP traffic received on the interface except for DHCP packets allowed by DHCP snooping. A port access control list (ACL) is applied to the interface. The port ACL allows only IP traffic with a source IP address in the IP source binding table and denies all other traffic. This way we will have finer granularity in identifying the spoofed IP addresses in a DHCP environment.

B. *IP Routing attacks:*

These are the control plane attacks on the network devices with an intention to spoil the routing table of the layer-3 devices such as router, firewalls and gateways. Most of the routing protocols today have the ability to authenticate the peers prior to sharing the routing information with other routers and this feature has to be enabled on all the layer-3 devices for forming the neighborship. The RIPv2 supports the plain-text password feature [3] to authenticate peers and also a much advanced security feature like keyed MD5 hashing security [4] feature to authenticate peers before forming neighborship.

OSPFv2 in its initial RFC supported the MD5 hashing to authenticate the peers. New security features have been proposed to include the HMAC-SHA authentications in the later RFCs. BGP which is an exterior routing protocol which has the same problems as the interior routing protocol. It also has the security features that require to be enabled to provide the authentication to form neighborship [6][7].

C. *Denial of Service (DoS) attack*

This attack mainly targets the availability of the service. The server providing the service is overwhelmed with the service requests upto a point beyond which it cannot handle. DoS attacks can be leveraged against poor software quality. It can cause application resource exhaustion, Operating system resource exhaustion and triggered lockouts and quota exhaustion [8]. Under the DoS mitigation strategies at the network level we must take care to provide Redundancy and Distributed Service, authenticate routing adjacencies and isolate router to router traffic [8].

D. *Man in the middle (MITM) attack*

This is the attack which typically occurs between the source and the destination. Not necessarily all the time do we have the source and the destination connected directly or with no hops. Often times the packet has to travel multiple hops (different routers) to connect to the destination. The attacker will leverage this fact to fabricate himself as the destination by displaying fake routing tables or in the LAN does the ARP spoofing(a layer-2 attack) to cheat the sender to send his traffic to the attacker. Then the attacker will either reply back as the original destination or drop without responding causing a type of DoS to the user. This type of attack can be prevented if we have a mechanism to authenticate the server from the client so that the client will send the packets only after the server is verified to be legitimate. Hence using the TLS or SSL to verify the server from the client before the packets are exchanged is a good idea to protect the integrity of the source and destination at the same time.

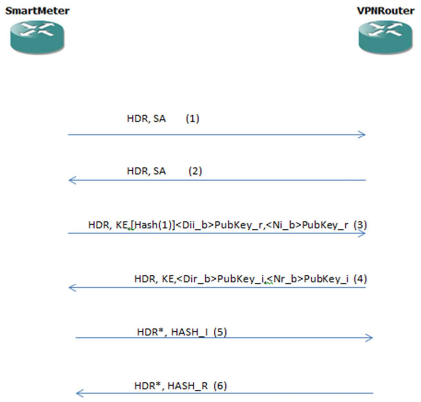
E. *Network monitoring attack*

Since the packets flows across multiple hops before reaching the destination the packets flow across multiple networks and the attacker leverages this fact to sniff the network packets for the packets of his interest. If the attacker is motivated to take down the network he will be interested in taking down the access to management plane and will look at the usernames and passwords. If he is interested in making financial gains he will be targeting the information such as credit card numbers etc. Some of the attackers might make a heist by selling the consumer's personally identifiable information such as SSN, address, power usage, address of residence etc. These attacks can go undetected for long. Hence all the information flowing through the smart-grid network must flow in an encrypted manner. This provides confidentiality to the data. To provide the confidentiality to the data normally IPSec VPNs are used. Initially the keys are exchanged in the VPN establishment phase by Internet Key Exchange (IKE) protocol.

III. IPSec SECURITY

Applying IPSec security directly between the consumer networks and the billing sites will decrease the bandwidth on the server side. The service is also affected by the overhead the server's CPU experience to encrypt the packets flowing to and from the clients. Apart from these issues it also causes the dilemma as to who will be exchanging the keys between the smart-meters and the servers. The other problem is the key revocation. Identifying a trusted third party would be even harder. So the IPSec VPNs using asymmetric key cryptography is the only viable option. The Trusted Platform Modules can be used in the generation of keys (public and private keys) in the smart meters because of the advantage it provides. Although TPM itself might be vulnerable to side channel attacks the communication occurring using the TPMs are resilient to such attacks.

The diagram below shows the IPSec VPN setup using the public-key:


SmartMeter
VPNRouter
HDR, SA (1)
HDR, SA (2)
HDR, KE,[Hash(1)]<Dii_b>PubKey_r,<Ni_b>PubKey_r (3)
HDR, KE,<Dir_b>PubKey_i,<Nr_b>PubKey_i (4)
HDR*, HASH_I (5)
HDR*, HASH_R (6)

The messages 1 and 2 form the IKE security association negotiation phase, the messages 3 and 4 establishes the Diffie-Hellman Key exchange, and the messages 5 and 6 authenticates the peer. In the above diagram the PubKey_r means the public key of the router and the PubKey_i means the public key of the smart meters. HDR means the ISAKMP header and KE is the key exchange. HDR*: denotes that ISAKMP payload is encrypted, this mean that identities (IDii and IDir) are protected during authentication exchanges (the last 2 messages) [9][10][11].

A. Advantages of IPSec VPN:

1. All communication occurring above the network layer gets encrypted and passes in the tunnel.

2. The confidentiality of the data is provided because the message is passed in an encrypted manner.

B. Limitations of IPSec VPN:

1. The intermediate firewalls must be configured to allow the traffic to flow through

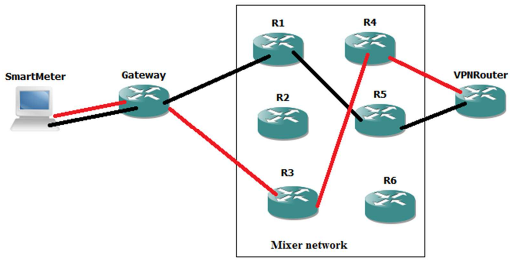
2. The terminating of tunnels on the VPN router will consume bandwidth and the processing power of the VPN router.

3. The privacy is not provided meaning the person performing a traffic analysis will still be able to identify the source and the destination.

IV. PRIVACY IN THE SMART-GRID

Since the businesses are mandated by several state laws and federal laws there arises the need to protect the privacy of the consumer data. The attackers might perform known text attack on the VPN traffic and in a long term might be able to decrypt the traffic. Hence, it is essential that a separate privacy protection mechanism be provided by design of the smart-grid.

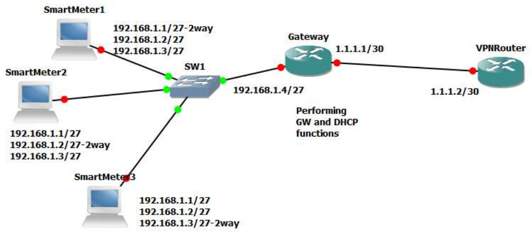
The solution proposed here is that of the Chaum's mixer network. Chaum's mixer network has been in use for protecting the privacy of the users, for web browsing using onion router. It has also been used in the anonymous mailing system. Below is the proposed solution which is similar to TOR architecture (the difference here is that it is layer 3 encrypted traffic flowing unlike layer 7 traffic):



Many of the smart-meters are connected to a gateway (only one is shown for simplicity). The traffic flowing from the source to gateway is encrypted by the public key of the last hop router by the gateway and then by the public key of the previous hops successively. Each of the routers successively decrypts in the reverse way and finally the IPSec packet moves to the destination. The black and red routes depicted are two of the different methods by which the traffic can flow through the mixer network.

Advantages of this method are that the attacker on the internet cannot perform analysis just based on the source IP and destination IPs as these are transformed by the mixer networks. Another advantage is that we have removed the need for another dedicated directory server (as in TOR). Limitation is that the analysis is possible if the attacker is present on the same LAN and we do not have layer-2 security features like MAC binding.

The second approach is that involving making changes to the DHCP protocol. The idea is to allow the DHCP server to provide a set of IP addresses that it possess in its pool to the pool of clients. Ask the clients to make use of the IP addresses based on some random manner, such that the IP address used by the same client varies each time while communicating. However for two way communication to be possible to occur using such there must be some device in between which has a track of the MAC to IP binding and the NAT sessions.



Consider the scenario of the three smart meters for the sake of working. The Gateway provides the allowed DHCP IP address list or pool IP to all the three smart meters and assigns one of the IP as its permanent IP address (purpose being two way communications). Now suppose the smart-meter has three different packets to be sent then it starts out by sending randomly from the pool of its IP address allowed to be used in the pool it received from the Gateway. For the first packet it sends it from the IP of 192.168.1.2 and second packet by IP 192.168.1.1 and the third one by IP of 192.168.1.3. The person monitoring the network will assume the first and the third packets came from SmartMeter2 and SmartMeter3 thus getting deceived in attributing it to a particular consumer.

Now what happens if the two smart-meters happen to get the same IP addresses at an instant? Still, it should not be problematic if the protocol is defined properly. Ideas on how to develop this protocol:

1. The DHCP (GATEWAY) server will maintain the IP to MAC table for each request sent just to maintain the logs.

2. Maintain a permanent IP to MAC address binding on the DHCP server and communicate the two ways IP address a particular host must reserve one particular IP which the DHCP server has provided as the two-way IP address. In simple sense the client has to listen to the replies sent on that particular IP only.

3. No LAN host can communicate on the IP address of the 2way IP address if the permanent host is receiving the packets from external IP.

4. The simpler approach would be to create a pool of IP address that is unused and share it with the hosts to use it randomly.

So how should server attribute the packet to the correct host or resolve the host properly? The solution is to send the MAC address of the Smart Meter in the data packet which will be encrypted. For the server to communicate to a particular host it has to get the 2way-IP address from the gateway and then communicate back on that particular IP.

To further obfuscate the IP address we can clear the permanent IP to MAC mapping in the DHCP (used for 2way) frequently. Thus by randomising the source IP address using the DHCP we will be able to communicate the data over the internet with assurance of privacy.

V. CONCLUSION

This paper is mainly concerned about the network layer security or OSI layer 3 securities in the smart grid network. The security discussed in the paper is inclusive of the CIA triads with an additional emphasis on privacy.

Important aspects of security at each OSI layer and the security threats at OSI Layer 3 have been described in this paper. Further an overview of the privacy preserving mechanism has been provided. Apart from the Chaum's Mix networks solution a new solution based on the new DHCP model has been made.

Based on the study of the different security threats at each layer and the possible solutions, the paper concludes that privacy of the customer can be best protected at layer 3 using the techniques mentioned.

VI. REFERENCES

[1] Network ingress filtering RFC 2827 by P Ferguson and D Senie

[2] Source Address Validation Improvement (SAVI) Framework by J. Wu, J. Bi et al. in RFC 7039

[3] RIP version 2 authentication feature RFC 2453 by G Malkin.

[4] RIPv2 Cryptographic authentication RFC 4822 by R Atkinson

[5] OSPFv2 RFC 2328 by J Moy

[6] BGP authentication RFC 1325 by R Rivest

[7] TCP authentication option RFC 5925 J Touch A Mankin and R Bonica

[8] Internet Denial-of-Service Considerations M. Handley, Ed. UCLA E. Rescorla, Ed. Network Resonance

[9] Deploying Cisco IOS Security with a Public-Key Infrastructure – Cisco Deployment guide.

[10] Requirements for an IPsec Certificate Management Profile RFC 4809 by C. Bonati, S. Turner et.al.

[11] IPsec VPN, Main mode Vs Aggressive mode by Salah HENDEL

[12] Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms by David Chaum Communications of the ACM February 1981 Volume 24 Number 2

[13] Wikipedia article on mix network

[14] TOR and HTTPS by Electronic Frontier Foundation

[15] Layer 2 security for Smart Grid networks by Indukuri N R Published in: Advanced Networks and Telecommunications Systems (ANTS), 2012 IEEE International Conference on Smart Grids

[16] Cisco guide to harden cisco ios devices by Shashank Singh.
[17] Dynamic Host Configuration Protocol (DHCP) by R Droms RFC 2131

[18] An analysis of smart grid attacks and countermeasures by Zubair A Baig and Abdul Raoof Amoudi Journal of Communications Vol. 8, No. 8, August 2013

[19] Mediating Cyber and Physical Threat Propagation in Secure Smart Grid Architectures by Clifford Neuman and Kymie Tan Proceedings of the 2nd International Conference on Smart Grid Communications (IEEE SmartGridComm), October 2011, Brussels