Strong Virtual Network Authentication using EAP-TLS Smart-Cards

Fouad Amine Guenane, Guy Pujolle
UPMC - LIP6 - PHARE
University of Paris VI; 4 Place Jussieu, 75005 Paris, France - E-mail: FirstName.FamilyName@lip6.fr

***Abstract*—The future Internet is a term commonly related to research topics on new architecture for Internet. In fact, the Internet of tomorrow will rely on virtualization and cloud networking, which open the door for new security threats and attacks and address many problems related to identification, authentication, secure data transfer, and privacy in virtual networks and clouds. The purpose of our work is to define an architecture for strong authentication and identity management in virtual networks using EAP-TLS smart cards technology. The architecture is based on a Grid of EAP-TLS smart cards, as an authentication server, able to manage users' access to their virtual networks by authenticating either the user and the virtual network.**

***Index Terms*—Virtual networks, Security, Authentication, Identity management, Smartcard, EAP-TLS, Grid server.**

I. Introduction

ACtually, with the growth of Internet and facilities it offered, user have to manage multiple identities to access different services : Web mail, social networks, bank account, etc. These identities are digital ones. It is a set of personal data that describes and refers to a unique person. This data is used by a system to manage user authorization to gain access to protected resources. The first step is to identify and authenticate users through networks using the traditional id/password method. However, this method can no longer be used for identification and authentication for the future Internet simply because it cannot prevent from unauthorized access.

In fact, the future internet will rely heavily on virtualization and clouds which still need improvements concerning security aspects seeing a strong authentication and identification mechanisms and ensure privacy within virtual networks, things that cannot be provided by traditional authentication methods and not even SSL authentication protocol (widely used by WEB applications).

We propose an architecture for authenticating and identifying clients by the Virtual Network Provider (VNP) using embedded SSL in smartcard. This solution is based on EAP-TLS smartcard that guarantees a trusted computing environment

This paper is organized as follows. Section 2 describes some proposals for authentication and identity management solution for cloud. Section 3 presents the solution model and architecture. Finally, section 4 concludes and proposes prospects of our work.

II. Related Works

Cloud computing and virtual environment become a hot research topic in the recent years. In fact, while dealing with cloud, there is a lack of possession of the data that can't be fully trusted by users, which makes identity management and authentication of both users and services are a significant issue for the trust and the security of cloud computing.

Several works have addressed the question of authentication and identity management and proposed different solutions to this problem. The user centric identity management approach provides a stronger mutual authentication between user and service providers by enabling the storage of identifiers and credentials from different service providers in a single resistant hardware device called Personal Authentication Device (PAD) [2]. A Hierarchical identity-based cryptography scheme was proposed in [3]. This scheme was considered as new solution for cloud computing security with federal identity management [4]. In fact, the federated identity management deals with problems between external user and internal network and *vice versa*. This approach creates a federated identity domain so that user identity can be recognized across different networks.

Our work will rely on smartcard technology, precisely EAP-TLS smartcard, as a solution for authentication and identity management presented in [5] [6]. The use of smartcard offers:

- Convergent identity system called "SSL-identity" that requires a mutual authentication between the user and the authenticator.
- An authentication server and the TLS-Tandom Technology that enable EAP-TLS to perform authentication and key export from the smartcard
- An Open-ID Provider

The SSL identities are stored securely in the smartcard, allowing to the user an easier access to service providers. Therefore, this constitutes a convergent, user-centric and secure solution for identity management.

The authentication solution, presented in [6], specifies a new design for a RADIUS server, commonly used for authentication, and associated to the Grids of EAP-TLS smartcard. The Radius server will only process RADIUS datagrams and perform user authentication using EAP-TLS. We have to notice that the choice of EAP-TLS was not arbitrary.To resume, the benefits of implementing EAP servers into the secure elements are:

- The server private key is secretly stored and used by the secure element.
- The client certificate is autonomously checked by the EAP server
- The SSL stack processed by the secure element is trans-

parent to the RADIUS server and the OS in which it has been implemented; the stack can be easily updated in case of major patches of SSL
- If the EAP client also runs in a secure element, the TLS stack is channeled from card to card and the EAP session is then fully processed by a couple of tamper resistant devices, working as Secure Access Module (SAM)

All previous works provide a specific solution to deal with authentication and identification problems in cloud environment. But there was no real work done in the context of virtual networks. For this purpose, and since the EAP-TLS smartcard technology has shown remarkable results within cloud computing authentication, we expect to have the same results with virtual network environment.

III. Model and Architecture

The objective of this work is to design and develop a coherent security architecture for virtual networks and clouds. The proposed architecture will allow the management of communications security between a virtual network especially virtual nodes and a VPN's administrator.

We admit that an attack can affect either the physical node or the virtual node by putting them out of services. This action can also threat the client privacy by impersonating the client (i.e. user's identity theft). We define the different entities involved earlier:

- The physical node PNd (physical machine) is a hardware entity that can be either a router that can hold up to N independent and non duplicated virtual nodes.
- The virtual node VNd is an OS entity running on a unique real machine and offering routing services to users allowing him to manage the network. This entity is located at a single physical equipment at a specific time but can migrate (change location) from one physical node to another to respond to security or Quality of Service QoS requirements.
- Service is a set of virtual nodes forming a virtual network VN according to the Service Level Agreement SLA previously discussed with the client.
- The client is a user who attempt to access a virtual machine in order to configure it and manage his own network.
- The Grid server is an authentication server with a particularity. It is an array of smartcard associated to a software bloc and a data base containing different information concerning clients, virtual networks and their constituent virtual nodes. This Grid server has three roles:
  - authenticating the client and VNd
  - managing authentication of VNd in case of node migration
  - The Grid server is considered like a trusted third party (TTP)in our architecture.

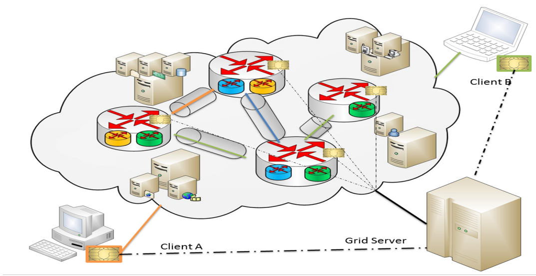

Figure 1 : Authentication Architecture for Virtual Networks

Our work provides a robust identification scheme and a strong authentication system using secure micro-controllers. The solution must take in consideration virtual environment specificities, it should identify both the client and the VNd and guarantee a secure VNd identity migration when needed.

The architecture that we proposed is based on five key elements: Client *C*, Grid Server *GS*, physical network *PNd*, virtual network *VN* and Virtual nodes *VNd*.

- *A* is a set of *PNd*. $|A| = K$
- *VN* is a set of *VNd*.
- P is a set of *VNd* which can be located in a *PNd*.$|P| = N$, Each *PNd* can support up to N *VNd*, consequently each PNd is equipped by N smartcard
- *VNd* are identified by his location: $\forall z \in A, \forall i \in P :$ VNd_{zi}
- Each *VNd* has a pair of secure elements (ie smartcard):
  - Secure Element in Physical Node: $\forall z \in A, \forall i \in H :$ $SEPNd_{zi}$
  - Secure Element in grid Server: $\forall z \in A, \forall i \in H :$ $SEGP_{zi}$ (double of $SEPNd_j$)
- H is a set of clients: $|H| = M$.
  $\forall j \in H : \ C_j \, is \, a \, client$. Each client has a pair of secure elements:
  - secure element in his possession : $\forall j \in H : \ SEC_j$
  - Secure Element in the Grid server: $\forall j \in H :$ $SEGC_j$ (double of SEC_j)
- The *GS* is an array of smartcard and it can support:
  - up to M clients
  - up to $(K \times N)$ virtual nodes
  - total number of clients and virtual nodes equal to $M + (K \times N)$

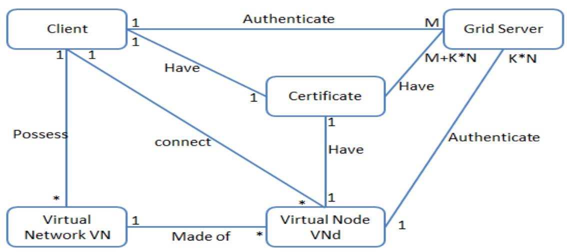

Figure 2 : Our Solution Model

As shown in Fig. 2, both client and virtual node need to be authenticated by the server. Each client and virtual node has a unique certificate stored in its smartcard unlike the server because it has certificates as much as he can support clients and virtual nodes together. However, virtual networks are not authenticated and do not dispose of certificates. In fact, the server memorizes virtual network identities for a given client and a list of virtual nodes realizing the VN. A client can have access to multiple virtual networks and benefits from services according to the Service Level Agreement SLA discussed beforehand with the Virtual Network Provider VNP. After authentication, the client can access all virtual nodes through an SSL connection.

This solution is adapted to virtual environment specificities and should take into consideration VNd migrations. In fact, this aspect is easily managed since we have a central authentication server that keeps all necessary information about a given VNd. This can change the location of different physical node without changing its IP address. So any node can be all time reachable via the network. In this case, the server have just to re-authenticate the VNd without a notification of the user.

The solution implementation is shown in the Fig. 3 below.

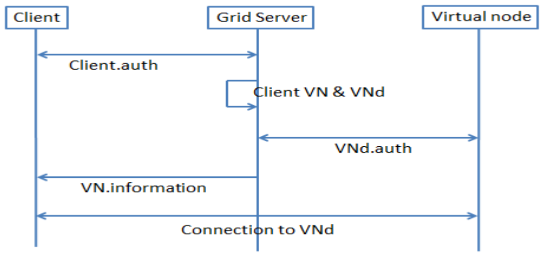

Figure 3 : Solution Implementation

We admit that the client needs to access a given virtual node in order to manage it. This access can not be allowed until the authentication step success. The proposed solution can be divided into 4 major steps :

1) client authentication
2) virtual nodes authentication (implicitly virtual networks authentication)
3) client data recovery
4) client secure access to his virtual domain

The first step is to authenticate the client by the trusted server who interrogates its database to identify all virtual networks of the client, and consequently the set of virtual nodes that constitute the client's virtual networks. The next step consists of VNd authentication. In fact, these steps are performed by a pair of smartcards in a transparent way for the client and processes EAP-TLS protocol.

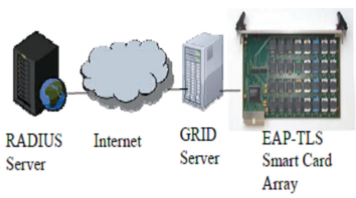

Figure 4 : The EAP-TLS smartcard array

Once authenticated, the server sends to the client all information about his virtual networks and authenticated VNd, allowing him the full access to all his resource. If possibly one virtual node migrate to another physical node, the user does not notice any changes and continue to work normally seeing that there was no change in IP address of the virtual node, but it is up to the server to re-authenticate it. As regards the performed tests, we wanted to evaluate the impact of the overhead generated by our authentication solution on bandwidth, buffer and CPU consumption. Our proposed Smartcard enabled RADIUS server is typically a classical RADIUS server which has been splitted into two main components: a RADIUS authentication server and distributed EAP servers. The RADIUS authentication server is located on a distant host and is in charge of the following tasks:

- It sends and receives RADIUS datagrams from and to the NAS, thanks to UDP sockets.
- It builds or analyses RADIUS messages and more specifically encapsulates EAP messages from the smartcard into RADIUS datagrams forwarded to the NAS, and reciprocally extracts RADIUS datagrams from the NAS into EAP messages forwarded to the appropriate server smartcard.
- It parses and builds APDUs which are communication units used to interact with the smartcard as explained below
- It handles the RADIUS secret and computes or checks the associated authentication digest and attributes
- It opens stream sockets with the smartcard grid and associates an incoming session with a single smartcard and its related connection

we are in the process of testing the performance of the solution and first results are encouraging and promising

IV. Conclusion

In this paper, we present a new architecture for virtual network authentication based on the use of smartcard as secure micro controllers, identification and authentication of all actors of the virtual environment are essential for network security. A virtual environment can be a vector (source) of attacks. Our architecture can provide a trusted and highly secure environment. In addition, we should notice that only VNd can migrate from one physical node to another, the result is that a virtual node loses its network security policies and they should be reconfigured by the administrator. We thought that it will be more interesting and practical if we can perform network security policies migration with its related virtual node.

References

[1] Bonneau, J., Mironov, I., "Cache-Collision Timing Attacks Against AES",Cryptographic hardware and embedded systems, 2006
[2] Pope, S., Josang, A.,"User Centric Identity Management", AusCERT Conference, 2005.
[3] Gentry, C., Silverberg, A., "HierarchicalID-Based cryptography",Zheng, ASIACRYPT 2002.
[4] Yan L., Rong C., Zhao G.,"Strengthen Cloud Computing Security with Federal identity Management Using Hierarchical identity-based Cryptography",CloudCom,2009.
[5] Urien, P., Marie, E.,Kiennert, C., "A New Convergent Identity System Based on EAP-TLS Smart Cards",(SAR-SSI), 2011.
[6] Urien, P., Marie, E.,Kiennert, C.,"An Innovative Solution for Cloud Computing Authentication: grids of EAP-TLS Smart Cards",(ICDT), 2010.