"Dimitrie Cantemir" Christian University
**Knowledge Horizons - Economics**
Volume 7, No. 3, pp. 176–179
P-ISSN: 2069-0932, E-ISSN: 2066-1061

www.orizonturi.ucdc.ro

# SECURITY FOR VIRTUAL PRIVATE NETWORKS

**Nicoleta Magdalena IACOB**

*"Dimitrie Cantemir" Christian University, Faculty of Finance, Banking and Accountancy, E-mail: nicoleta.iacob_2007@yahoo.com*

***Abstract*** *Network security must be a permanent concern for every company, given the fact that threats are evolving today more rapidly than in the past. This paper contains a general classification of cryptographic algorithms used in today networks and presents an implementation of virtual private networks using one of the most secure methods - digital certificates authentication.*

**Key words:**
Virtual private network, public key infrastructure, certificate authority, ipsec
**JEL Codes:**
L86

## 1. Introduction

Over the years, many cryptographic algorithms have been developed and utilized in different protocols and network security components. Recent progresses in the science of cryptanalysis made possible to adopt stronger algorithms for network defense in order to adapt to updated security threats (Baron et al, 2014; Boyles, 2010). In general, cryptographic algorithms can be classified into the following:

- Symmetric key algorithms: These algorithms use the same key for encryption and decryption. In this class of algorithms are included Triple Data Encryption Standard (3DES) and Advanced Encryption Standard (AES).
- Public key algorithms: These algorithms use different keys for encryption and decryption. In this class of algorithms are included Digital Signature Algorithm (DSA) and the Rivest-Shamir-Adleman (RSA) algorithm.
- Elliptic curve algorithms: These algorithms are based on points that belong to elliptic curves. In this class of algorithms are included Elliptic Curve Diffie-Hellman (ECDH) and Elliptic Curve Digital Signature Algorithm (ECDSA).
- Hash: These algorithms map digital data of arbitrary size to digital data of fixed size and their most important property is irreversibility.

## 2. Public key infrastructure

This paper will describe how to improve the authentication method used to create ipsec encrypted tunnels between different sites that host the distributed database of an e-learning platform as presented on doctoral thesis "Distributed databases. A dynamic model fully decentralized and automated (Ciobanu-Iacob, 2014) by implementing a public key infrastructure. A public key infrastructure use public and private cryptographic key pairs that are mathematically related and are provided by a certificate authority. Certificate authority provides services that authenticate the identity of entities in a network and act as the central point of trust in a public key infrastructure (Ciobanu-Defta & Ciobanu-Iacob, 2012; Iacob, 2014; Iacob, 2015; Iacob & Defta, 2014; Iacob & Defta, 2015).

In the scenario from the thesis, there are three sites – Bucharest, Timisoara and Paris that are connected in a virtual private network using Cisco equipment, a worldwide leader in routing and switching domain. In every location there is a Cisco router that acts also as a firewall and that create ipsec tunnels over the connection from internet service provider. The IP classes allocated to each location are:

Bucharest 10.1.0.0 with network mask 255.255.0.0
Timisoara 10.2.0.0 with network mask 255.255.0.0
Paris 10.3.0.0 with network mask 255.255.0.0

The authentication method used to create the tunnels was pre-shared key:

```
crypto isakmp policy 1
encr aes 256  //256 bit aes encryption is used
```

authentication pre-share //authentication is made using a preshared key

group 5 //for key exchange in a non-secure medium was used Diffie Helman algorithm using 1536 bits according to RFC2412

crypto isakmp key test_key address 3.3.3.3 // this is the key for authentication with Paris router

The security improvement presented in this paper consists of installing a certificate authority on the Bucharest router in order to use certificate-based authentication method instead of pre-shared key authentication that could more easily be compromised. In a public key infrastructure, each participant holds a digital certificate that has been issued by a Certificate Authority. The certificate contains a number of attributes that will be used when a secure connection will be established. The benefits of public key infrastructure deployment are:

• simplified management of the security infrastructure;

• increased security through difficulty of compromising certificate-based security;

• improved management integration for all secured services.

### 3. Implementation

In the following paragraph we will show the implementation of the concepts presented above.

BUCHAREST router
BUCHAREST(config)#ip domain-name domain
BUCHAREST(config)#crypto key generate rsa modulus 2048
The name for the keys will be: BUCHAREST.domain
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]
//Next will create the certificate authority server
BUCHAREST(config)#crypto ca trustpoint IOS_CERT
BUCHAREST(ca-trustpoint)#usage ike
//This certificate has been defined to use for IKE peer authentication.
BUCHAREST(ca-trustpoint)#subject-name CN=BUCHAREST,C=RO
BUCHAREST(ca-trustpoint)#enrollment url http://10.1.1.1
//Enrollment url is the ip address of the router
BUCHAREST(config)#crypto ca authenticate IOS_CERT
Certificate has the following attributes:
Fingerprint MD5: 01883E9C A5E46B10 ANV97362 C07C8963
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
BUCHAREST(config)#crypto ca enroll IOS_CERT
% Start certificate enrollment .
% Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate.
Password:
Re-enter password:
% The subject name in the certificate will include: CN=BUCHAREST,C=RO
% The subject name in the certificate will include: BUCHAREST.domain
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
BUCHAREST(config)#
%PKI-6-CERTRET: Certificate received from Certificate Authority
BUCHAREST(config)#crypto isakmp policy 10
BUCHAREST(config-isakmp)#encr aes256 //256 bit aes encryption is used
BUCHAREST(config-isakmp)#hash md5
BUCHAREST(config-isakmp)#authentication rsa-sig
BUCHAREST(config-isakmp)#group 5
BUCHAREST(config-isakmp)#crypto ipsec transform-set MYSET esp-3des esp-md5-hmac
BUCHAREST(config)#access-list 120 permit ip host 10.1.1.1 host 10.3.1.1 //access-list that permit traffic between Bucharest and Paris
BUCHAREST(config)#crypto map CRYPT 10 ipsec-isakmp
BUCHAREST(config-crypto-map)#set peer 3.3.3.3 //external ip address allocated by internet service provider to Paris router
BUCHAREST(config-crypto-map)#set transform-set MYSET
BUCHAREST(config-crypto-map)#match address 120
BUCHAREST(config-crypto-map)#exit
BUCHAREST(config)#int f0/0
BUCHAREST(config-if)#crypto map CRYPT //cryptographic settings are applied on outside interface of the router

PARIS router
PARIS(config)#ip domain-name domain

```
PARIS(config)#crypto key generate rsa modulus 2048
The name for the keys will be: PARIS.domain
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]
PARIS(config)#crypto ca trustpoint IOS_CERT
PARIS(ca-trustpoint)#usage ike
PARIS(ca-trustpoint)#subject-name CN=PARIS,C=FR
PARIS(ca-trustpoint)#enrollment url http://10.1.1.1
// the enrollment url is the address of the Bucharest router
PARIS(config)#crypto ca authenticate IOS_CERT
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
PARIS(config)#crypto ca enroll IOS_CERT
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
Password:
Re-enter password:
% The subject name in the certificate will include: CN=PARIS, C=FR
% The subject name in the certificate will include: PARIS.domain
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
PARIS(config)#
%PKI-6-CERTRET: Certificate received from Certificate Authority
PARIS(config)#crypto isakmp policy 10
PARIS(config-isakmp)#encr aes256 //256 bit aes encryption is used
PARIS(config-isakmp)#hash md5
PARIS(config-isakmp)#authentication rsa-sig
PARIS(config-isakmp)#group 5
PARIS(config-isakmp)#crypto ipsec transform-set MYSET esp-3des esp-md5-hmac
PARIS(cfg-crypto-trans)#access-list 130 permit ip host 10.3.1.1 host 10.1.1.1 //access-list that permit traffic between Paris and Bucharest
PARIS(config)#crypto map CRYPT 10 ipsec-isakmp
PARIS(config-crypto-map)#set peer 1.1.1.1 //external ip address allocated by internet service provider to Bucharest router
PARIS(config-crypto-map)#set transform-set MYSET
PARIS(config-crypto-map)#match address 130
PARIS(config-crypto-map)#int f0/0
PARIS(config-if)#crypto map CRYPT
//cryptographic settings are applied on outside interface of the router.
```

## 4. Conclusions

Now more than ever, every company depends on their network availability for the most important business operations. Most business transactions are done today over the Internet and if the network is compromised, there could be serious consequences for every company. For these reasons, companies should adapt to newest security threats and protect their virtual private networks with the one of the most secure methods - digital certificates authentication.

## References

• Baron, C., Șerb, A., Iacob, N.M. & Defta, C.L. (2014). IT Infrastructure Model Used for Implementing an E-learning Platform Based on Distributed Databases, Quality-Access to Success, Vol. 15/S2/2014, pp. 195-201.

• Boyles, T. (2010). CCNA Security Study Guide, Wiley Publishing.

• Ciobanu (Defta), C.L. & Ciobanu (Iacob), N.M. (2012). Methods for Securing Routing Protocols in Ad-Hoc Networks, SYNASC 2012 - 14th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, September 26-29, 2012, Timișoara, Romania, IEEE Computer Society Conference Publishing Services (CPS), 2013, pp. 341-348.

• Ciobanu (Iacob), N.M. (2014). Distributed databases. A dynamic model fully decentralized and automated/Baze de date distribuite. Un model dinamic complet descentralizat și automatizat, Editura Pro Universitaria, București, 2014, ISBN 978-606-26-0095-2.

• Iacob, N.M. (2014). Information security for web and SQL services, Proceedings of the 9th International Conference on Virtual Learning 2014. Models & Methodologies, Technologies, Software Solutions, University of Bucharest, Faculty of Psychology and Educational Sciences, Siveco Romania, October 24-25, 2014, pp. 408-412.

• Iacob, N.M. (2015). Data Security for E-Learning Platforms/Securitatea datelor în platforma E-learning, Conferința Naţională "Politica fiscală a României şi impactul ei asupra dezvoltării societăţii

româneşti, Ediţia a II-a“, Universitatea Creștină "Dimitrie Cantemir", 25-27 Martie 2015, Bucureşti, România.

• Iacob, N.M. & Defta, C.L. (2014). Information Security for Web Services – Proactive and Reactive Security Techniques, Knowledge Horizons – Economics, Volume 6, No. 4, pp. 135–138.

• Iacob, N.M. & Defta, C.L. (2015). HTTP Protocol security for E-learning platforms, Conferinţa Ştiinţifică Naţională Anuală “Noi tendinţe pentru o economie bazată pe cunoaştere şi globalizare”, Facultatea de Finanţe, Bănci şi Contabilitate, Universitatea Creștină "Dimitrie Cantemir", 14-15 Mai 2015, Bucureşti, România.

• www.cisco.com – ASA configuration guides, accesed 2015.