Sinteza
Međunarodna naučna konferencija Univerziteta Singidunum

Impact of Internet on Business Activities in Serbia and Worldwide
Uticaj Interneta na poslovanje u Srbiji i svetu

DOI: 10.15308/SINTEZA-2014-620-624

# ANALYSIS OF THE PULL METHOD FOR CRL DOWNLOAD BY THE PKI SIMULATION MODEL

**Aleksandar Mišković[1], Srđan Atanasijević[2]**
[1]Singidunum University, Serbia
[2]Technical College of Applied Studies Kragujevac, Serbia

**Abstract:**
This paper presents a simulation model of a PKI which establishes the service of secure electronic mail exchange where users of the PKI use pull method for CRL download. It describes the method of making a simulation model of PKI in OPNET IT Guru Academic Edition virtual network environment, and presents the results of the simulation. The simulation model of the PKI is methodologically simplified, elements of the PKI are presented with appropriate models, and their interactions are simulated using the appropriate network applications and profiles. The analysis of simulation results points to the advantages of using decentralized servers for distributing the CRL in a PKI.

**Key words:**
Public Key Infrastructure;,
Certificate Revocation List,
Pull method,
OPNET IT Guru Academic Edition.

## INTRODUCTION

A complex system that ensures secure communication over an insecure communication channel is called Public Key Infrastructure - PKI. PKI is a combination of hardware and software elements that connect users, digital certificates, Certification Authority - CA, database of valid and invalid certificates, and all their mutual interactions in a single unit.

One of the services of the PKI is a secure e-mail exchange. In order for participants to communicate using this service they must use digital certificates issued by the CA of the PKI. A digital certificate is a digitally signed document that connects a public key with a person to whom the key belongs to. Participants in this communication must be confident that the partners they communicate with are not intruders who falsely present themselves. A sender digitally signs an e-mail message with his digital certificate thus guaranteeing the authenticity and integrity of the e-mail messages. To ensure secrecy, the sender encrypts the message with his private key, and the recipient decrypts this message using the public key of the sender.

Users of the PKI verify digital certificates and consequently also the public keys through the CA or through some other body authorized for that job by the CA. Certificate Revocation List - CRL enables entities that communicate in a given PKI to check the validity of digital certificates of the other party in communication.

OPNET IT Guru Academic Edition is a virtual network environment which enables modelling, simulation of operation and analysis of collected statistics, as well as graphic representation of the results of different network topologies, with the selection of appropriate network devices, protocols and applications.

## THEME AND PURPOSE OF THE RESEARCH

Digital certificate has a limited validity period, written in an appropriate field, and upon the expiry of this period it must be revoked. It often happens in practice that a digital certificate is revoked before the expiration date. The CA is obliged to publicly announce a list of revoked certificates, and there are several ways to distribute the list to the users of the PKI.

The most widespread protocol used in the PKIs for accessing the CRLs within the X.500 directory is LDAP (Lightweight Directory Access Protocol). In addition to the LDAP, the method of sending a CRL to all users (push method) is also used, as well as publishing the CRL on an appropriate web site of the certification authority from which users can download the CRL file (pull method, such is also downloading a CRL from the X. 500 directory server).

In this paper we analyse two ways of downloading the CRL by the PKI users, a centralized and a decentralized way. Users will use the pull method to download the CRL and the research conducted in this study will show differences in the use of these methods and indicate their advantages and disadvantages.

The goal of this paper is to present a PKI from the aspect of using a service for secure exchange of electronic mail. The users of this system will download and revoke digital certificates, exchange digitally signed and encrypted e-mail messages. However, since the CRL distribution is one of the key problems faced by each PKI, the focus of the analysis is put on this issue.

## SIMULATION MODEL

The simulation model of the PKI is methodologically simplified and reduced to running appropriate services and use of appropriate applications. Corresponding elements of the PKI are presented by relevant models in the simulation, and the behaviour of entities is presented and simulated using the appropriate network applications and profiles.

The architecture presented by the simulation model in this paper implies that the PKI has a CA that is used for the issuance and revocation of digital certificates created in accordance with the standard X.509 v3 [1], the registration bodies for registering new users and a database of revoked certificates through which the CRL will be distributed to the users.

The operation process that actually represents a flowchart of the simulation model is shown in Fig. 1.

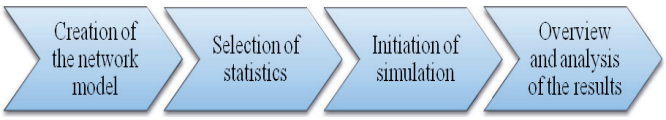


Fig. 1. Flowchart of the simulation model

Due to software restrictions implemented in the OPNET IT Guru Academic Edition, related to 50 million simulation events, the number of simulated PKI users and duration of the simulation had to be customized to this parameter.

### Setting a model

The simulation model presented in this paper represents a PKI schematically equivalent to the PKIs used in our country. Those are hierarchical PKIs that are not connected to each other. Schematic view of such PKI is shown in Fig. 2.


Fig. 2. Hierarchical model of the PKI

Fig. 3 shows four sub-networks named after the cities in which the users and other elements of this imaginary PKI are distributed. All the sub-networks are connected via the Internet to a remote e-mail server, which may be located anywhere in the world.

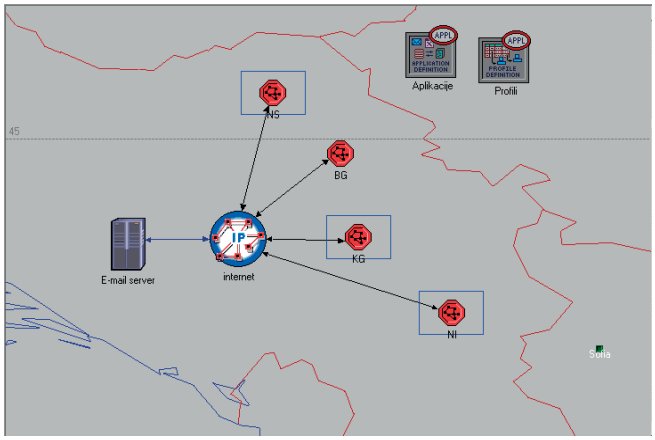


Fig. 3. Simulation network model that uses a PKI

The role of the e-mail server in this simulation is to serve the users of the PKI who periodically send and receive e-mail messages.

From the perspective of the simulated PKI, the sub-network labelled BG (Belgrade) contains the main elements of a PKI such as CA Server, CRL Repository and local RA Server, while the sub-networks labelled NS, KG and NI contain, depending on the scenario, a local RA Server and a local CRL server.

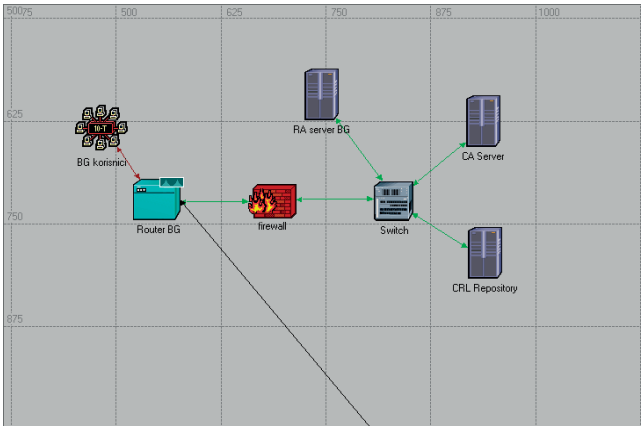


Fig. 4. BG subnet - scenario 1

CA Server is a server of the certification body responsible for issuing and revoking digital certificates. In this simulation model, its role is limited to these two activities and has little impact on the network itself.

CRL Repository is a database or a directory containing a list of revoked certificates signed by the CA. Users of the PKI will periodically access the CRL server and download the list of revoked certificates. Due to the already mentioned software limitations related to the number of simulation events, the CRL that is downloaded by the user is of constant size, although in practice this is not the case. The parameters that were monitored in the simulation model are related to the load of the CRL server when downloading a CRL in two different ways, centralized and decentralized. Performances of the CRL servers are essential for the operation of this type of network, and therefore all the parameters that affect their operation have been monitored.

Table 1. OVERVIEW OF THE SUBNET TOPOLOGY

| Name of the object | Model of the object |
|---|---|
| Servers | ethernet_server |
| Users | 10BaseT_LAN |
| Routers | CISCO 7000 |
| Switches | ethernet16_switch |
| Firewall | ethernet2_slip8_firewall |
| Links | 10BaseT and 100BaseT |

RA servers BG, NS, KG and NI are the servers of the registration body and are responsible for identification and authentication of new users on the basis of which a request for a digital certificate is created that is sent to the CA after data processing. The role of the server is also limited to these two activities and these servers do not have a big impact on the network itself.

Users of the simulated PKI are grouped into LAN objects using 10Base ethernet links, while the entities of the PKI are connected with other objects in the network via 100BaseT links. Other objects belong to standard network facilities and have no impact on the results of this simulation.

## Network services – applications and user profiles

Application Config object is used to specify the applications that will be used for configuration of user profiles.

Fig. 5 shows that in addition to the standard model of application for e-mail messages exchange another four application models have been added which serve the users of the PKI.

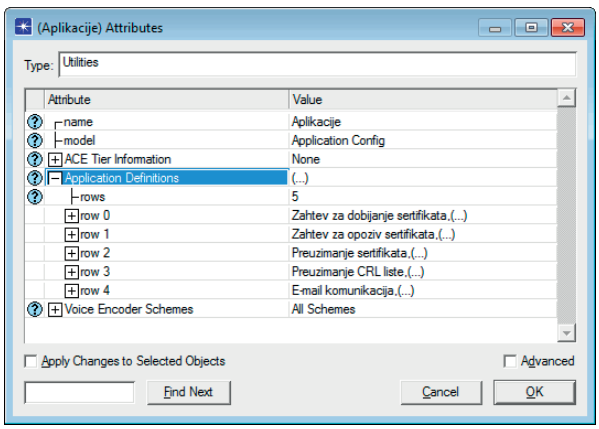


Fig. 5. Application Config object

Profile Config object describes the activity patterns of users or groups of users in relation to the application that they use during a certain period of time. Before starting the configuration of user profiles, applications that will be used in the network must be defined.

For the purpose of this simulations five profiles were created for users of the simulated PKI. Each of these profiles was configured separately and it was precisely defined when would each profile run during the simulation, how long it would be running, whether it would be repeated during the simulation, etc.

Table 2. ACTIVITIES OF THE USERS` PROFILES

| Profile name | Description of activities |
|---|---|
| e-mail | Application starts 190-200s after the beginning of the simulation, which represents time needed for the users to download certificates and a CRL, and it runs until the end of the profile. |
| Request for certificate | Application starts 5-10s after the beginning of the simulation, it runs only once during the simulation and last for 10 seconds. |
| Certificate download | Applications starts 20-30s after the beginning of the simulation, it runs twice during the simulation within a time interval of 900s lasting for 180s. |
| Request for revocation | Application starts 900 after the beginning of the simulation and it lasts for 60s. |
| CRL | Application starts 35-40s after the beginning of the simulation, it runs six times during the simulation and last for 180s. |

## Simulation scenarios

The scenarios help us to look at the complete simulation model from different aspects, and to compare the obtained results based on the changes of certain object parameters or the simulation model objects themselves.

In this paper two scenarios for the simulated PKI model were created. In this way, the reconfiguration of the network i.e. of the PKI was carried out, so that a part of the local transport networks NS, KG and NI was redirected to local servers for downloading the CRL.

Configuration of the sub-network BG was not changed, and the load was removed from the central CRL server by adding local CRL servers in the local sub-networks. The Fig. 6 shows the configuration of the KG sub-network, which is identical in terms of object models it contains with the sub-networks NS and NI of the second scenario. To this sub-network, a server of ethernet_server type named “Local CRL KG” was added, and 80% of the users of the local network were redirected to a new local server. The redirected users are presented by the 10BaseT_LAN object and connected to the network via router through the link of 10BaseT type.

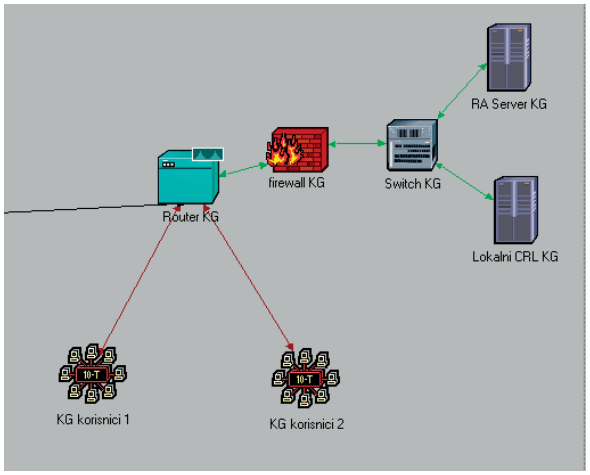


Fig. 6. KG subnet - scenario 2

For the second scenario another application was created, in addition to the existing ones, named "CRL local download" and will be applied only to local users and CRL servers. Attributes of this application are the same as the attributes of the already presented application in the first scenario called "CRL download."

In addition, for 80% of users who will use the application a new profile was created named "CRL locally" which has the same attributes as the already presented profile of the first scenario named "CRL locally", but this profile is directed towards running a newly created application for the second scenario.

Selection of statistics and configuration of simulation

The simulation statistics is a collection of one or more values that describe certain aspects of the behaviour process during the simulation.

Statistical data collected in this simulation were selected according to the theme and purpose of the research. Performances of the main CRL server in both scenarios were monitored and the following statistical parameters were selected for monitoring:

- Load (requests / sec) - collects the number of active sessions on the server.
- Task Processing Time (sec) - time needed for the server to process client's request.
- Traffic Received (bytes / sec) - average rate of incoming traffic.
- Traffic Sent (bytes / sec) - average rate of outgoing traffic.

As regards the work of the server, in addition to these statistics, statistics of the application running on the BG client side was followed. In accordance with this statistical parameter Page Response Time (sec) was selected, which represents time needed for downloading the entire HTML page that actually represents a CRL in this simulation model.

For the simulation model of the PKI, in both scenarios duration of the simulation was set to 30 minutes. In both simulation model scenarios the work of 10 users of each sub-network was presented, which amounts to a total of 40 users, having in mind that in the second scenario 80% of the local sub-networks NS, KG and NI users were redirected to local servers.

## ANALYSIS OF THE SIMULATION RESULTS

Analysis of the simulations results is carried out on the basis of the collected statistics for the selected network devices and applications running in the network environment.

Fig. 7 and 8 present data for the CRL Repository server. On Fig. 7 given intervals may be noticed at which the users of the application called "CRL" access the server. The Figure shows that the number of active sessions on the server is lower when applying a decentralized method for distributing the CRL. By decentralization the CRL Repository server is considerably relieved of load. This may be seen on Fig. 8 where it is noticeable that the time needed for the server to process clients` requests is significantly shorter than when a centralized method is concerned.

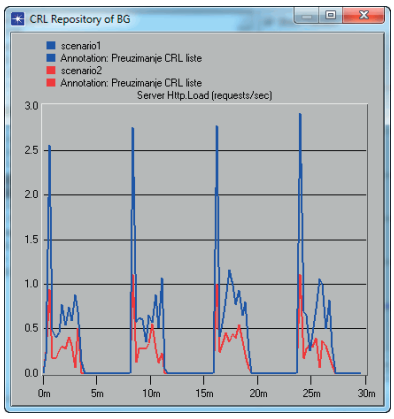


Fig. 7. Load (requests/sec)

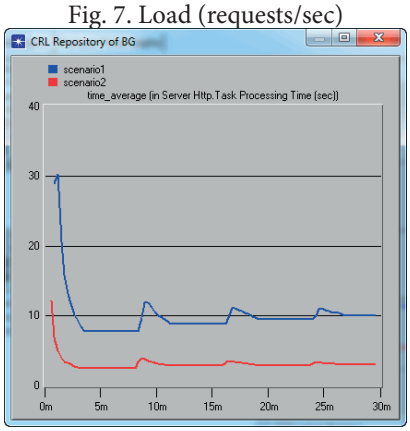


Fig. 8. Task Processing Time (sec)

By further analysis, the Fig. 9 and 10 show the average rate of incoming and outgoing traffic.

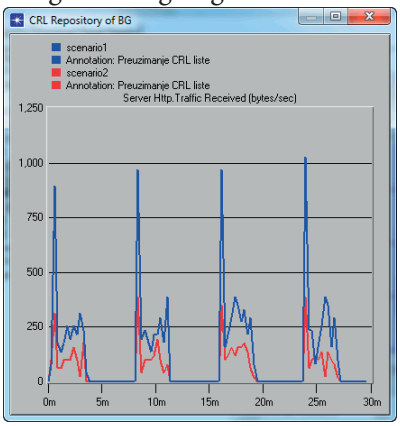


Fig. 9. Traffic Received (bytes/sec)

In these graphs given intervals according to which the users of the application called "CRLs" access the server are clearly shown. It may be seen on the graphs that the generated traffic is lower due to the application of the decentralized method for the CRL distribution.

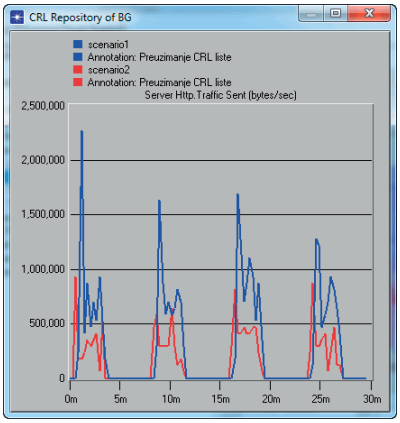


Fig. 10. Traffic Sent (bytes/sec)

Having examined these statistics it may also be concluded that the CRL Repository server has been significantly relieved of the load by using local servers for CRL distribution.

Finally, the Fig. 11 shows how the use of local servers to distribute the CRL impacted the speed of downloading a CRL by the BG users.

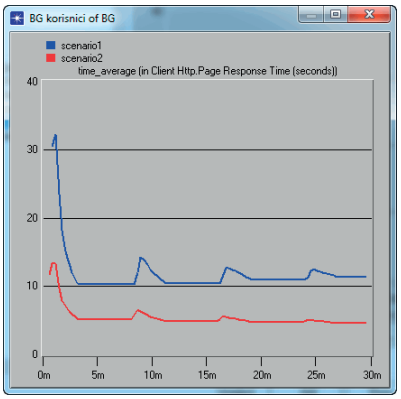


Fig. 11. Page Response Time (sec) BG users

## CONCLUSION

The results presented in this study are not representative in the real world and are intended to showcase techniques of modelling and simulation of a PKI. The simulation model presented in this paper is simplified and adapted to the study. The PKI itself is much more complex and can be analysed in detail using a more advanced version of the OPNET Modeler software.

The theme of the research in this paper was the pull method for downloading the CRL from the directory server of the PKI. The research has shown that there are differences between the centralized and decentralized method for distributing CRLs, thus fulfilling and goal of the research.

This research does not cover all methods for distributing a CRL to end users of the PKI. It is necessary to go deeper into this problem, which is very important in terms of the validity of digital certificates, but also to expand it by including in further work all known methods for revocation and validation of digital certificates by using appropriate protocols. Also, for further research in this area, simulation model of the PKI should be expanded, all protocols under which it operates should be presented, and possibly, a better and more efficient solution for validation of digital certificates should be reached by changing the way these protocols are run.

## REFERENCES

[1] D.Cooper, S.Santesson, S.Farrell, S.Boeyen, R.Housley, W.Polk: RFC5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, 2008.

[2] Kelley R. Klepzig: Modeling and Simulation of Public Key Infrastructure Applications, SANS Institute, 2003.

[3] Jun Wang, Bill Yurcik, Zahid Anwa, Suvda Myagmar: Secure Large-scale Network Systems: Key Management Scalability Modeling & Simulation, NCSA Security Research, University of Illinois at Urbana-Champaign, 2006.

[4] Adarshpal S. Sethi, Vasil Y. Hnatyshin: The Practical OPNET User Guide for Computer Network Simulation, CRC Press, 2012.

[5] Zheng Lu, Hongji Yang: Unlocking the Power of OPNET Modeler, Cambridge University Press, 2012.

[6] Information about why the size of a digitally signed or encrypted e-mail message increases in Exchange 2003,

[7] http://support.microsoft.com/kb/927469, online access: 15.03.2013.

[8] Chao Yang, Jianfeng Ma, Xuewen Dong: A New Evaluation Model for Security Protocols, Journal of Communication, vol. 6, no. 6, septembar 2011.