Security Analysis of User Mobility in Triple-play Systems

Sasa Mrdovic, Darijo Raca and Kenan Turbic
Faculty of Electrical Engineering
University of Sarajevo
Bosnia and Herzegovina
Email: sasa.mrdovic, draca, kturbic@etf.unsa.ba

***Abstract*—Users of triple-play systems expect to be able to use their services on different locations. That opens an issue of extending security to include mobile triple-play users. Mobile users need to authenticate to the system and vice-versa. Users expect confidentiality of their communications. Content providers request copyrights to be respected. Protocols for session control, SIP. and media transfer, RTP, have their secured versions, SIPS and RTSP. That solution would require multiple protocols and keys and would be a burden on users and system administrators.**

This paper proposes an architecture that uses IMS to provide services and VPN to secure them. IMS provides convenience of user mobility. VPN provides authentication, confidentiality and integrity. Additional security provided by VPN does not translate to additional work for users, It is completely transparent for them. Proposed design is implemented and tested. IMS with different services was available, through VPN, to mobile users connected to the Internet with different devices and connections. The testing confirmed security and usability for mobile users.

I. Introduction

Systems that enable users to access the Internet, make telephone calls and view television through a single access network are called triple-play systems. Such systems are convenient for users, because they simplify consumption and payment of services. For providers they are a new business opportunity. Providing these three, previously separate, vertically integrated services through one transmission network is achieved through horizontal integration. These systems are a true example of next generation networks (NGN). Creating such systems brings new challenges because it means consolidation and convergence of different systems.

A common architecture of triple-play system consists of an access network, core network and application servers. Access network connects users to the core network. Core network enables efficient distribution of multimedia content from the service area to the user as well as from user to user. Application servers implement all the services that the system provides, and support functioning of the system. This support includes systems for authentication, authorization and accounting. It is one of the basic components of security of these systems. The second component of security, is the system of digital rights management. This system is usually implemented using cryptography. Content that is not available to everyone is encrypted before it is sent to customers. Only users who have the appropriate key can decipher the contents. Distribution of keys to authorized users is managed through customer premises equipment (CPE), usually set-top box (STB). STB communicates with application servers in charge of cryptographic keys distribution. After successful authentication and authorization STB is provided with appropriate keys and consumption of services is records for accounting purposes.

Triple-play systems are generally implemented for users who are on a fixed location. STB takes on the role of a user agent that interacts with application servers. STB sends authentication credentials, asks for access to resources, acquires cryptographic keys and uses them to decrypt the content. Authentication could be location based and does not require users to supply any credentials.

Contemporary service models assume that users are mobile and want to consume services from different locations and via different devices. It opens up new security issues.

This paper proposes architecture that extends security to mobile triple-play users. It is based on existing protocols and components. It requires minimal changes to existing infrastructure.

The rest of the paper is organized as follows. Related work is considered in section 2. Section 3 explains the proposed approach to problem solution. Implementation of test system is described in section 4. Testing procedure and results are presented in section 5. Conclusion and discussion on future work are in section 6.

II. Related work

There are several security aspects of user mobility in triple play systems that were analysed by different researchers. We preview related work divided by user authentication, user privacy and content confidentiality protection and performance.

User authentication in fixed triple play systems usually does not require users to enter any credentials by themselves. User agent implemented in some kind of set top box authenticates user. For IPTV service standard practice is for set top box to authenticate to video head-end with client certificate [1]. Triple-play providers that use DSL often authorize physical line or DSL port in addition to username and password [2]. SIP, as dominant control protocol, authentication procedure and its processing load have been studied in paper [3]. Issue of IMS authentication in environments that provide fixed mobile convergence, like the one we are proposing, has been

a subject of [4]. New authentication scheme for IMS using identity based cryptography was proposed in [5]. Recent paper [6] describes attack on IMS AKA authentication on Android mobile devices. The paper is interesting since it uses Android clients for IMS services like we do, but our approach is not vulnerable to this type of attack.

Content confidentiality in VoIP ensures user privacy while in IPTV and VoD it protects copyrights of content owners. VoIP privacy and voice confidentiality have been important issuees since VoIP introduction [7]. Good overview of attacks on VoIP privacy and possible deftnesses is given in [8]. Paper [9] proposes framework that could provide protection of user identity in SIP based systems. Recent IETF RFC7202 [10] discuses why there can not be a single solution for securing RTP.

All security mechanisms use resources and that could impact performance that is very important for real time systems like triple-play. Authentication performance in IMS systems is analysed in [11] Influence of TLS on SIP server performance was tested in [12]. VPN technology that we propose for protection could be implemented using different protocols. Performance of two most common, IPsec and TLS, are compared in [13].

This an active area of development and research but have not found any theoretical work or testbed similar to the one we propose.

III. Proposed Approach

Our idea was to combine IP Multimedia System (IMS) with Virtual Private Network (VPN). IMS provides convenience of user mobility. VPN provides authentication, confidentiality and integrity. Before explanation of the complete set-up we provide a quick overview of IMS and VPN.

A. IMS

IP Multimedia Subsystem was originally developed as an extension for UMTS mobile networks, bringing a multimedia service over IP protocol to mobile users. However it became a essential part of 3G, cable TV and fixed next-generation networks [14]. The rapid explosion of Internet and it's worldwide acceptance has led to a plethora of new and innovative applications, which changed the way people communicate. As a best-effort protocol, IP could not guarantee a good performance and satisfying quality of service. On the other hand telecommunication networks were built around reliability and delivering high quality service to the users. Main point of Internet model is its open architecture while traditional networks are mostly proprietary and closed. Merging these two concepts has led to IMS architecture. IMS delivers QoS enabled real-time applications over any type of networks (IP, traditional, mobile). At the same time it allows development of new innovative applications that meet user needs. SIP protocol was chosen as a signalling protocol responsible for delivering voice, video, text and multimedia services to the end users [15].

B. VPN

Exchange of information over Internet introduces a number of security risks. Internet architecture does not provide any mechanism for securing information exchange from potential attacks which can lead to leaks or unauthorised alteration of confidential information. One solution is straight-forward: simply building a network on a private infrastructure. Main problem with this approach is it's expensiveness where only few institutions/companies could afford it, especially if two branches of same company are geographically very distant. Second and widely used solution today is building a virtual private network over existing IP network. This solution uses cryptographic algorithms for encrypting a message before it enters a public domain, e.g. Internet. There are different types of VPNs based on protocol used in deployment. L2TP/PPTP represents VPN technology operates on link layer, while IPSec and SSL operates on network and above transport layer respectfully. VPN on higher layers is easier to configure, however low layers enable support for wider range of upper-layer protocols [16].

C. IMS over VPN

Default IMS provides only authentication. Control and media sessions could be secured separately. SIPS, SIP over TLS, provides confidentiality, integrity and authentication for control messages exchanged using SIP protocol. Secure RTP (SRTP) does the same for media streams. Using VPN instead of SIPS and SRTP has two benefits. It does not require two security protocols to manage and enables additional protection of IMS infrastructure. VPN protects all data exchanged with IMS, both media streams and control messages. With VPN IMS servers can be positioned within organization network hidden behind firewall. External access is possible only through VPN. There is a question of authentication of VPN clients. It should not be an additional burden for mobile users with another password to remember and manage. Thus, we propose using certificate based VPN authentication. For this authentication both clients and server authenticate to each other via public key certificates and proof of possession of corresponding private key. Client certificates and private keys are stored on the device that user uses as IMS user agent. Access to private key could be protected with OS or IMS password and made transparent to user. VPN tunnel could be established when needed without asking user for any additional input.

IV. Implementation

In order to test proposed solution we implemented a system that provides all mentioned functionalities. We then tested its usability. As an IMS solution we used Open IMS Core [17]. This is open-source IMS core implementation for IMS technology testing and IMS application prototyping for research purposes. The Open IMS Core implements the core elements of IMS/NGN architecture as specified today within 3GPP, 3GPP2, ETSI TISPAN and the PacketCable intiative, including Call Session Control Functions (CSCFs) and subscriber database, i.e. Home Subscriber Server (HSS). The

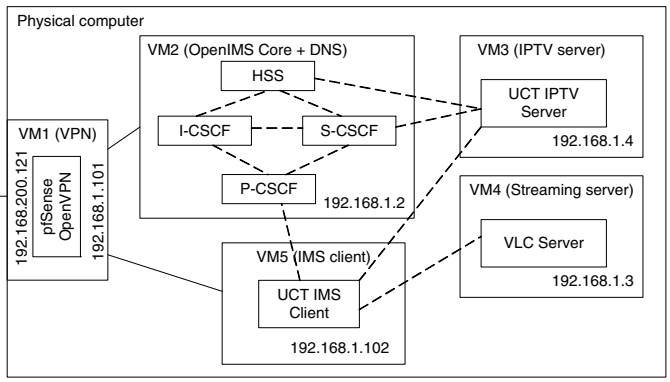

Fig. 1. IMS behind VPN

four components, P-CSCF, S-CSCF, I-CSCF and HSS, are all based upon Open Source software (e.g. the SIP Express Router (SER) or MySQL). A more detailed information can be found in [18], [19] and [20]. VPN was implemented using OpenVPN. OpenVPN is open-source software tool which can be used for secure communication between two or more remote devices/facilities over the Internet. It implements SSL/TLS VPN technology for authentication and key exchange. It can be installed on different kind of OS platforms, e.g. Linux, Unix, Windows and Mac [21]. We used OpenVPN as a part of pfSense, popular open source firewall.

Complete IMS with all its servers and one test client, together with VPN were installed as five virtual machines on one physical computer. The computer was HP Z420 Workstation with Intel Xeon E5 processor and 32 GB of RAM. Virtualization software used was VirtualBox version 4.3.12. Function of each virtual machine with software used and IP address is given on fig. 1. Further details are provided in the text bellow.

A. IMS

OpenIMS Core was installed on Ubuntu 12.04 operating system. It was rather standard installation described in the Installation Guide for OpenIMS Core. All three CSCF functions: Proxy-CSCF, Serving-CSCF and Interogating-CSCF were running on the same machine. User database HSS, implemented with OpenIMS core component FHoSS, was also running on the same machine. In addition, a DNS server for domain name translation of all IMS servers was configured within the same virtual machine. That machine is VM2 in fig. 1.

In addition to core IMS functions two application servers were configured to support video streaming. IPTV server was referenced in HSS as a point where information on available video streaming channels could be found. It was implemented using UCT IPTV server installed on Ubuntu 12.04 OS (VM3 in fig. 1). IPTV server provided clients with RTSP address of video files available on streaming server. Streaming server functionality was provided by VLC installed on Ubuntu 12.04 OS (VM4 in fig. 1).

B. IMS user agents

Three different IMS clients for there different OS were used for testing.

UCT IMS client version 1.0.14 was selected as IMS client on Linux. It was installed and tested on Ubuntu 12.04 (VM5 in fig. 1). Of all available clients for all operating systems (OS) it had the best support for other triple play services in addition to VoIP. Especially when used with OpenIMS Core since both pieces of software come from the same source. This client was used to test functionality of IMS system. User registered in HSS was able to log in and stream selected video from streaming server, via IPTV server.

IMSDroid version 2.548.870 was only working Android IMS client available. It was installed and tested on three different mobile devices: Google Nexus 7 tablet, Google Nexus 5 mobile phone and Prestigio Multipad 2 tablet. Mobile devices used for testing were accessing IMS through VPN as it is described later.

Boghe IMS Client version 2.0.106.1013 showed to be the best selection for Microsoft Windows OS. It was installed and tested on desktop computer HP Compaq Pro 6300 MT with Intel i5 processor and 12 GB of RAM with 64-bit Windows 7 SP1 OS. Computers used for testing were accessing IMS through VPN as it is described later.

C. VPN

OpenVPN software application was used to provide virtual private network for clients accessing IMS. OpenVPN was installed as a part of pfSense router/firewall software distribution version 2.1.3 (VM1 in fig. 1).

OpenVPN server was set to accept remote connections on UDP port 1194. TLS certificates used were issued by pfSense local CA created just for this purpose. VPN tunnel network was set to 192.168.100.0/14, and VPN clients were given access to VPN server local network 192.168.1.0/24 where all IMS servers are located. Clients were provided with IP address of DNS server 192.168.1.2 for resolving domain names of IMS servers. Keepalive parameter was changed from its default value 10 60, to new value of 10 300. This ensured longer periods of inactivity, up to five minutes, before VPN connection needs to be re-established.

Two pfSense users, alice and bob, were issued TLS certificates. VPN clients authenticated using these certificates.

Since the VPN server is in local network, its outside IP address is a private one. In order to enable IMS clients to access IMS servers through VPN, port forwarding was set up at external firewall. External firewall accepted incoming VPN connections on a public IP address and selected UDP port and forwarded them to outside OpenVPN server IP address, 192.168.200.121, and UDP port 1194. In this way IMS services were available to public Internet through VPN.

V. Testing

Implemented functionality was tested using all above described IMS clients. One Windows client was positioned in local network and the other one was connected to the Internet

with 802.11 connection. Linux client was at residential area connected to public Internet through ADSL. Android clients on mobile devices, mobile phone and tablet, were tested with two types of connection, 802.11 and 3G connection. Fig. 2 provides overview of testing set up.

Tests on Linux with UCT IMS client included video streaming of selected channel from IMS servers and VoIP, voice and video, calls to other users. Tests on Windows with Boghe IMS clients and on Android with IMSDroid clients include only voice and video calls due to lack of support for video streaming in these clients.

A. Security

We have recorded network traffic between different IMS clients and IMS servers. The traffic was captured and analysed at various points between client devices and VPN outside port. The traffic was encrypted and it was not possible to get any call data from it. Both control and media streams were confidential. User privacy was protected. IMS user names and passwords were also protected since they were not exchanged as clear text. Additional layer of authentication was provided with client TLS certificates. The certificates were installed on devices effectively enabling only devices with certificates to establish VPN connection and log into IMS servers. Since both IMS user name and password and TLS certificate protected with password are required for authentication, we have achieved two factor authentication.

B. Usability

Increased security in this case was not paid by additional burden on users. TLS certificates and their corresponding passwords were stored on mobile devices and there was no need for user to enter them each time when VPN connection was needed. IMS user names and password were also stored on mobile devices. Users were able to make calls just by selecting an IMS contact as with standard mobile phone calls.

C. Mobility

Users could also enjoy full mobility. All they needed in order to make a IMS phone call was an Internet connection. They had access to all IMS features of their organisation. They were also available on their local IMS numbers wherever they were located. This availability required established VPN connection and active IMS client. This could be a burden on battery and cause additional data transfer. We have not tested longer periods of usage. Preliminary test showed that VPN connection was using less battery and transferring less data than a number of standard Android applications.

Although service was available with any Internet connection, ADSL, 802.11 or 3G, call quality and dependability varied.

D. Call quality

1) Local calls: The first test was a call between Boghe IMS Client in local network and UCT IMS Client on VM in IMS network. That call did not go through external firewall. Nevertheless, it did go through VPN. We completed 10 calls, including both voice and video, initiated from both sides.

All calls were established without delay. Call quality, sound and picture, was excellent.

Our first conclusion was that with excellent network connection additional VPN processing does not have adverse effect on call quality.

2) Remote calls over WiFi: Our second set of tests included calls from different IMS clients connected to the Internet over WiFi. Calls were established between those remote IMS clients and IMS clients in local network and between remote clients. All calls went through external firewall and VPN. Some of them, between remote IMS clients, twice. For each couple of clients we have completed 10 calls, including both voice and video, initiated from both sides.

All calls were established with minimal delay. Call quality, sound and picture, was very good. Quality levels depended on the quality of network connection, as it might be expected. Since the most of our connections were very good so was the call quality. Wherever we had connection that was good enough for other Internet activities it was good enough for IMS calls.

Our second conclusion was that even with good network connection additional VPN processing does not have adverse effect on call quality.

3) Remote calls over 3G: Our third set of tests was similar to the second one. The difference was that this time remote clients were connected to the Internet over 3G mobile network. Connection speed and quality depended on the location. Calls were initiated from different locations resulting in different connection qualities.

Unfortunately, the call quality was not as good as we expected. There were delays in IMS registration, call establishment and break up. The delays were inconsistent. The only rule we were able to establish was that it was getting worse with time. Logging out of IMS, closing IMS client and VPN connection usually helped but for the short period of time. The interesting fact is that once the call was established, the quality was good and comparable to calls over WiFi. We tried using different VPN and IMS configurations as well as 3G connection set up on mobile devices with little success. We still ended up with unreliable IMS connection. This issue needs further investigation that we plan to do next.

Our third conclusion was that with our current set up IMS clients connected over 3G get unreliable IMS service. Once the call is established the quality is good but new call might require re-establishment of all connections VPN and IMS.

VI. Conclusion

Combination of IMS and VPN could secure triple-play services for mobile users. Proposed architecture is convenient for users since it enables them to securely use services without additional work. Security mechanisms are implemented on mobile devices they use. They are able to consume services from any location or device with Internet access.

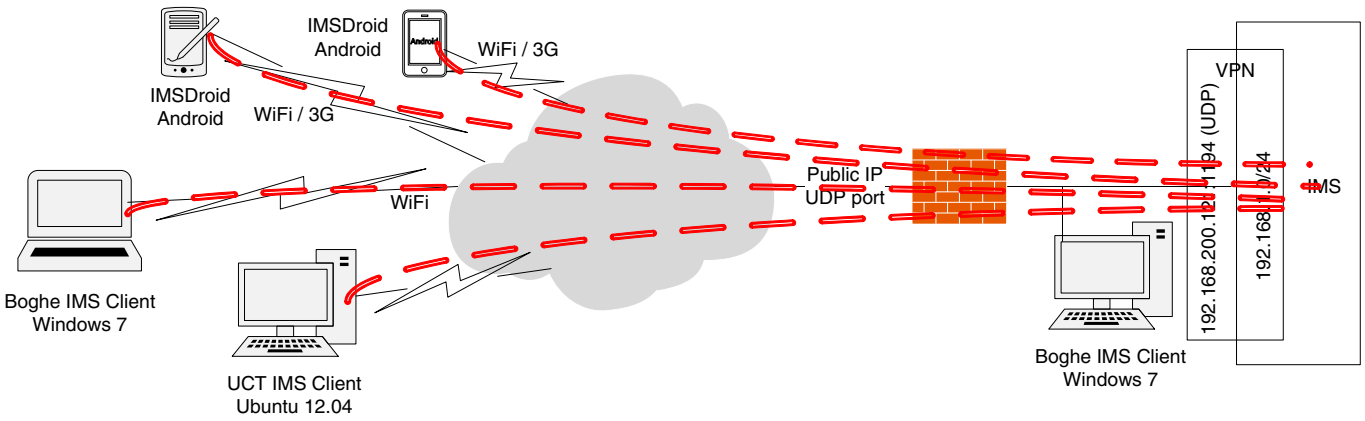

Fig. 2. Clinet access to IMS through VPN

The main issue we discovered was reliability and call quality when users are connected to the Internet over 3G connection. Although it is sometimes good it is not always reliable. We are concentrating our future research efforts on finding out causes and solutions for this question.

ACKNOWLEDGMENT

The authors would like to thank Federal Ministry of Education and Science in Bosnia and Herzegovina which funded this research.

REFERENCES

[1] G. O'Driscoll, *Next Generation IPTV Services and Technologies*. New York, NY, USA: Wiley-Interscience, 2008.

[2] C. Hellberg, D. Greene, and T. Boyes, *Broadband Network Architectures: Designing and Deploying Triple-Play Services*. Upper Saddle River, NJ, USA: Prentice Hall PTR, 2007.

[3] S. Salsano, L. Veltri, and D. Papalilo, "Sip security issues: the sip authentication procedure and its processing load," *Network, IEEE*, vol. 16, no. 6, pp. 38–44, Nov 2002.

[4] M. Matsumoto, "A study of authentication method on fixed mobile convergence environments," in *Telecommunications Network Strategy and Planning Symposium, 2006. NETWORKS 2006. 12th International*, Nov 2006, pp. 1–6.

[5] M. Abid, S. Song, H. Moustafa, and H. Afifi, "Efficient identity-based authentication for ims based services access," in *Proceedings of the 7th International Conference on Advances in Mobile Computing and Multimedia*, ser. MoMM '09. New York, NY, USA: ACM, 2009, pp. 260–266. [Online]. Available: http://doi.acm.org/10.1145/1821748.1821798

[6] J. G. Beekman and C. Thompson, "Breaking cell phone authentication: Vulnerabilities in aka, ims and android," in *Proceedings of the 7th USENIX Conference on Offensive Technologies*, ser. WOOT'13. Berkeley, CA, USA: USENIX Association, 2013, pp. 5–5. [Online]. Available: http://dl.acm.org/citation.cfm?id=2534748.2534755

[7] D. C. Sicker and T. Lookabaugh, "Voip security: Not an afterthought," *Queue*, vol. 2, no. 6, pp. 56–64, Sep. 2004. [Online]. Available: http://doi.acm.org/10.1145/1028893.1028898

[8] M. Srivatsa, A. Iyengar, L. Liu, and H. Jiang, "Privacy in voip networks: Flow analysis attacks and defense," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 22, no. 4, pp. 621–633, April 2011.

[9] G. Karopoulos, G. Kambourakis, S. Gritzalis, and E. Konstantinou, "A framework for identity privacy in {SIP}," *Journal of Network and Computer Applications*, vol. 33, no. 1, pp. 16 – 28, 2010. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804509001052

[10] M. W. C. Perkins, "Securing the RTP Framework: Why RTP Does Not Mandate a Single Media Security Solution," Internet Requests for Comments, RFC Editor, RFC 7202, April 2014. [Online]. Available: http://www.rfc-editor.org/rfc/rfc7202.txt

[11] S. Song, M. Abid, H. Moustafa, and H. Afifi, "Performance evaluation of an authentication solution for ims services access," *Telecommunication Systems*, vol. 52, no. 4, pp. 2205–2218, 2013. [Online]. Available: http://dx.doi.org/10.1007/s11235-011-9543-z

[12] M. Kulin, T. Kazaz, and S. Mrdovic, "Sip server security with tls: Relative performance evaluation," in *Telecommunications (BIHTEL), 2012 IX International Symposium on*, Oct 2012, pp. 1–6.

[13] I. Kotuliak, P. Rybar, and P. Truchly, "Performance comparison of ipsec and tls based vpn technologies," in *Emerging eLearning Technologies and Applications (ICETA), 2011 9th International Conference on*, Oct 2011, pp. 217–221.

[14] 3GPP TS 22.228, "Internet Protocol (IP) Multimedia core network Subsystem (IMS)," 2014.

[15] M. Wuthnow, M. Stafford, and J. Shih, *IMS A New Model for Blending Applications*. Boca Raton : CRC Press: McGraw-Hill, 2010.

[16] Y. Lin, R. Hwang, and F. Baker, *Computer Networks: An Open Source Approach*. 1221 Avenue of the Americas, New York, NY 10020: McGraw-Hill, 2012.

[17] FOKUS, Fraunhofer Institute for Open Communication Systems, "The open ims core project," http://www.openimscore.org.

[18] T. Magedanz, D. Witaszek, and K. Knuettel, "The ims playground @ fokus - an open testebed for next generation network multimedia services," in *Proceedings of the First International Conference on Testbeds and Research Infrastructures for the DEvelopment of NeTworks and COMmunities*, ser. TRIDENTCOM '05. Washington, DC, USA: IEEE Computer Society, 2005, pp. 2–11.

[19] D. Vingarzan, P. Weik, and T. Magedanz, "Design and implementation of an open ims core," in *Proceedings of the Second International Conference on Mobility Aware Technologies and Applications*, ser. MATA'05. Berlin, Heidelberg: Springer-Verlag, 2005, pp. 284–293.

[20] ——, "Development of an open source ims core for emerging ims testbeds, the academia and beyond," *J. Mob. Multimed.*, vol. 3, no. 2, pp. 131–149, 2007.

[21] OpenVPN Technologies, "Open Source VPN," https://openvpn.net/.