EPC Protocol and Application Security Evaluation

Denver D. Abrey and Neco Ventura
Department of Electrical Engineering
University of Cape Town, Private Bag X3, Rondebosch 7700, South Africa
Tel: +27 21 6502699, Fax: +27 21 6503782
email: {neco, dabrey}@crg.ee.uct.ac.za

Abstract-The Evolved Packet Core (EPC) has been developed to provide the backbone IP infrastructure required to create true end-to-end IP based carrier networks. It provides a large number of different functions, including charging, Quality of Service (QoS) and security. As a carrier class solution, the EPC must maintain a high level of security, even when connecting users, core components and 3rd party service providers. This paper explores some of the more subtle security issues inherent in the design of both the EPC and its underlying protocols. It also details a number of possible attack vectors, and briefly describes what the impact of these may be if exploited successfully.

Index Terms— application security, evolved packet core, protocol security, security ,

I. INTRODUCTION

The Evolved Packet Core as specified by the 3GPP is a multi-access core network based on the Internet Protocol (IP), facilitating access to services from both trusted and untrusted access networks. It provides a multitude of required functionality to allow reliable and secure service delivery while remaining access network agnostic. Key features include Authentication, Authorization and Accounting (AAA), mobility and connectivity management, Quality of Service (QoS) as well as Policy Charging and Control (PCC) [1].

The 3GPP specifications allow for a number of operating scenarios, from an EPC only deployment, to many interoperability setups, allowing different "hybrid" networks to be created. This allows for realistic migration paths, as existing infrastructure can be used alongside the EPC if necessary. Many interworking functions have been defined for this purpose [2].

This paper aims to expose a number of issues that should be taken into account when considering an EPC implementation. These will be used in creating an EPC targeted automated vulnerability assessment and discovery framework in the future.

II. EPC SECURITY

The EPC specifications have taken security very seriously, and as such almost all interfaces make use of some form of IP Security IPSec or encryption. Key separation has also been implemented to mitigate the threats caused in the unlikely event of a compromise. A new mutual authentication process called EPS Authentication and Key Agreement (AKA) has also been defined to secure access to the EPC and the services provided over it [2].

While the heavy use of IPSec would appear to eliminate almost all "traditional" network based vulnerabilities, it should rather be seen as reducing the number of attack vectors. However, due to the complex nature of the EPC, there are a number of subtle methods an attacker may use with malicious intent. These are outlined below.

A. Access Network Security

The access agnostic nature of the EPC means that it will be accessed via untrusted non-3GPP networks. An example is the ubiquitous WiFi networks available almost anywhere. While the EPC avoids any threat of eavesdropping, identity theft or integrity compromise by the use of EAP-AKA and IPSec, it should be noted that the client or user itself still has a somewhat more "open" view of the interface to the EPC. In this case, the "S2b" interface connecting the UE to an evolved Packet Data Gateway (ePDG).

Unlike previous topologies, the access interface is no longer obscured by a baseband processor or complex wireless access technology as with 3G. In previous architectures, the user had no way of viewing the equivalent interface without highly specialised (and expensive) equipment. Now, it is merely an IPSec tunnel, terminated at the UE with standard IP flowing through it. The UE termination therefore allows an unobscured view of the IP traffic itself to the user. This in itself is not a problem for most users, but a malicious user could take advantage of this and begin an automated "fuzzing" process to begin finding protocol vulnerabilities within the interface to the ePDG itself. This would yield implementation specific attack vectors if successful. The fact that the ePDG is normally a trusted element in the EPC means that its compromise could be detrimental to the entire core and service delivery network. Extensible protocol testing frameworks are already available, and could be modified to perform the attack above. This has in fact already been done for the Diameter protocol [3] used in the EPC for AAA . Diameter is the successor to the Remote Access Dial-In User Service (RADIUS) protocol.

B. Protocol Security

Fortunately most new protocols appearing in the EPC architecture have been specified with great focus on security. One notable and rather fundamental exception to this is of course the underlying reliance on IP. While IPSec and strict mutual authentication ensure no data is leaked or modified, the transport networks may still be vulnerable to IP specific Denial of Service DoS attacks. This is again related more to

the IP based access networks used to connect to the ePDG.

The partial reliance on DNS when connecting via untrusted access networks also creates the possibility for another rather trivial DoS attack. In the case where DNSSEC is not required for a client, one can perform a number of interesting activities. These include the possibility of poisoning a local DNS server. DNS poisoning is an attack on caching nameservers which causes them to return incorrect data to clients, for example associating an attackers IP with a legitimate domain name.

Flooding replies to the client (more difficult as this requires the client to receive a reply with a correct sequence number), or performing an IP man-in-the-middle attack and spoofing DNS altogether are also potential threats. While this would usually lead to a victims IP traffic being disclosed, the use of IPSec makes this a Denial of Service only attack.

In contrast, the newer protocols may in fact bring with them their own problems. For example, if a protocol specification contains a fundamental flaw which allows an attacker to perform a malicious action, this could have far reaching implications, as all implementations would be vulnerable to such an attack. This would be a similar case to that of the SMB Relay vulnerability that persisted in many Microsoft operating systems for almost 7 years. [4]

Another more related example is Mobile IPv6. Mobile IPv6 has been known to be vulnerable to an attack whereby data destined for a mobile user can be redirected to an attacker [5]. A number of other threats related to MIPv6 are also outlined in [6]. Fortunately IPSec would likely be in use to protect data and signalling integrity when accessing the EPC, leaving only the possibility of a Denial of Service attack. A number of interesting issues have also been raised with IPv6 itself and are outlined in [7]. With IPv6, the type of attack is again limited to Denial of Service when IPSec is in use.

C. Application Security

The EPC is a composite entity, consisting of many different components, which may well come from different vendors. Implementation is therefore left up to the individual vendors, and can often be the source of security issues. As mentioned previously, the ability of a user, or indeed a content provider, to easily reach the actual traffic and signalling to various components can pose a security hazard. This demonstrates one of the more serious security threats to the EPC, as a compromised core component or application server may be used to mount further attacks without hindrance. Compromising a trusted component such as the ePDG could allow an attacker access to almost any network resource, as it is both trusted and able to communicate with other core components. This also extends to content providers, which may reside within the carrier's infrastructure, but fall into the administrative domain of an external provider. While such systems should hold fewer privileges than core network components, they can still be used to an attacker's advantage. This could result in at the very least a DoS for all users of the service, while subscriber details may be leaked in an extreme case.

III. CONCLUSION AND FUTURE WORK

The 3GPP has focused strongly on security and mandated IPSec on many internal interfaces, and almost all external interfaces. With their use of key separation and mutual authentication, almost all possibilities of traffic interception are eliminated. The above evaluation demonstrates that while this encryption is a huge step forward, it cannot be relied on to eliminate all possible attack vectors.

Careful analysis of protocol specifications and implementations can lead to new attacks, aided by the ability of users to access the IP traffic readily and easily. The opening up of carrier networks to content providers and their associated application servers also creates the possibility of further attacks, either by malicious users or content providers, particularly if an interface can be abused even momentarily to reach or spam a large amount of users, or even harvest user details.

Future work will make use of the outlined attack vectors and attack discovery mechanisms to create an EPC and IMS targeted framework to automate discovery of vulnerabilities using the above mentioned attack vectors. This would be similar to the xmlgen and PROTOSS combination used to perform testing on the Diameter protocol as in [3].

IV. REFERENCES

[1] T. Magedanz, "Service Platforms for Next Generation Networks and Next Generation Mobile Networks", Fraunhoffer Fokus, Two day course at UCT, Feb 2010.

[2] M. Olsson, S. Sultana, S. Rommer, L. Frid, "SAE and the Evolved Packet Core: Driving the mobile broadband revolution", Elsevier, 2009.

[3] D. Wang, "An XML-Based Testing Strategy for Probing Security Vulnerabilities in the Diameter Protocol" in Bell Labs Technical Journal 12(3), 79-93, 2007

[4] J. Fontana, "Microsoft patch closes 7-year-old OS hole", Network World, Nov 2008. [Online] Available: http://www.networkworld.com/news/2008/111208-microsoft-seven-year-security-patch.html

[5] P. Nikander, "An Address "Ownership" Problem in IPv6", Ericsson NomadicLab, Feb 2001

[6] A. Mankin et. al., "Threat Models Introduced by Mobile Ipv6 and Requirements for Security in Mobile Ipv6", IETF draft-ietf-mipv6-scrty-reqts-02, May 2001.

[7] J. Kempf, E. Nordmark, "Threat Analysis for IPv6 Public Multi-Access Links", IETF draft-kempf-ipng-netaccess-threats-00, April 2002

Denver Abrey received his undergraduate B.Sc in Computer and Electrical Engineering degree in 2009 from the University of Cape Town. He is presently studying towards his Master of Science degree at the same institution. His research interests include network security, VoIP and the EPC.