Computer Networks 60 (2014) 60–74

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Performance evaluation of current and emerging authentication schemes for future 3GPP network architectures

Zoltán Faigl [a,*], Jani Pellikka [b], László Bokor [a], Andrei Gurtov [c]

[a] Mobile Innovation Centre, Budapest University of Technology and Economics, Bertalan Lajos u. 2., Z building 301., H-1111 Budapest, Hungary
[b] Centre of Wireless Communications, University of Oulu, P.O. Box 4500, FI-90014 Oulu, Finland
[c] Department of Computer Science and Engineering, Aalto University, P.O. Box 15400, FI-00076 Aalto, Finland

ARTICLE INFO

Article history:
Received 3 April 2013
Received in revised form 26 November 2013
Accepted 17 December 2013
Available online 24 December 2013

Keywords:
User authentication
Performance evaluation
Host Identity Protocol
Network architecture evolution
Evolved Packet Core
Wireless Personal Area Network

ABSTRACT

One of the key issues in recent mobile telecommunication is to increase the scalability of current packet data networks. A challenging topic of scalability is the efficient handling of rapidly growing Machine-type communication, which comes along with the requirement of low-cost network attachment and re-attachment procedures.

In this paper we present the results of a comprehensive testbed-based performance evaluation on a set of authentication schemes over "centralized", "distributed" and "flat" mobile network architecture alternatives in terms of computational cost, memory utilization, authentication delay, and signalling overhead. The aim of our measurement and analysis is to facilitate decision making on authentication scheme selection in future mobile networks and in Wireless Personal Area Networks. We also show that the optimal distribution level of the network architecture is "distributed" with respect to the authentication delay. The studied authentication schemes seem to hinder seamless handover provision in case of frequent gateway changes, except the Host Identity Protocol-based Diet Exchange extended with 3GPP Authentication and Key Agreement authentication scheme over Wi-Fi access.

1. Introduction

Current trends in telecommunications prognosticate that mobile and wireless networks will face continuous and massive traffic volume growth in the packet switched domain during 2011–2020 [1–3]. To date, this traffic explosion is mostly driven by Internet applications providing almost an unlimited scale of interaction, information, and entertainment services for people. However, with the widespread deployment of autonomous, networked and inter-operating sensor technologies, another form of communications called M2M (Machine-to-Machine) or MTC (Machine Type Communication) is emerging, which has the potential to become the leading traffic contributor for mobile Internet evolution in the near future [4]. According to recent estimations [5], there could be 225 million mobile and wireless M2M devices by 2014 with infinitesimal traffic per node but resulting in significant growth in total, mostly in the uplink direction. Emerging application areas are, e.g., remote controlling, monitoring, measuring, road safety, security/identity checking, or video surveillance functions in Smart Grid [6], Intelligent Transportation Systems [7] and mHealth [8]. The scale of the traffic volume and Internet of Things (IoT) expansion poses serious research challenges for mobile architectures [9–11]. In this paper we focus on the architectural, security and seamless handover related questions from this complex and diverse problem space.

This paper evaluates the performance of six signalling schemes for mutual authentication and key agreement. In general, those results support the decision procedure of user access authorization technology selection for

* Corresponding author. Tel.: +36 1 4633420.
E-mail addresses: zfaigl@mik.bme.hu (Z. Faigl), jpellikk@ee.oulu.fi (J. Pellikka), bokorl@hit.bme.hu (L. Bokor), gurtov@ee.oulu.fi (A. Gurtov).

1389-1286/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.bjp.2013.12.015

emerging services in future mobile Internet scenarios. Table 1 summarizes the most relevant terms and abbreviations in the paper.

All investigated schemes provide access authorization to network services, and control the establishment, update and deletion of IPsec SA pairs between end-nodes. Most of the schemes are fully standardized by the Internet Engineering Task Force (IETF), thus enjoy broad industry support. They have support in different types of operating systems or in different layer-three VPN solutions. Two of the schemes are an exception to that. At the time of writing, DEX is specified in IETF draft [17], and is a candidate key management protocol for Low-Rate WPANs [19]. DEX-AKA was introduced in [18] and has not yet been standardized.

The main reference scheme in our measurements is EAP-AKA, utilized in 3GPP technical specifications, e.g., [20]. It is recommended in scenarios where a user connects to the mobile operator's services through non-3GPP radio access networks, e.g., Wi-Fi, managed by third parties. The other three evaluated schemes are EAP-TLS, PSK, and BEX.

Different authentication schemes have different costs in terms of resource utilization, but also provide different security levels and functionalities. Furthermore, their choice would represent individual deployment and configuration tasks for the mobile network operator. The general goal is to find the best security configuration that fits to the needs of a given application in a given environment. We note that this paper deals with the performance evaluation of the authentication solutions and the implication of performance results. The suitability of the methods to a wider set of requirements has been discussed in [21].

The characteristics of the environment, such as network link delay or the computational capacity of the nodes, influence the resulting performance metrics, e.g., the overall delay of the security process or the utilization of the links and nodes. Hence it is worth selecting such performance indicators that decrease the influence of factors from the environment. Using the terminology of queueing theory, we are curious about the size of the jobs caused by one authentication flow on average in terms of computations, memory usage, and network processing.

The performance evaluations in the literature, described in Section 2, do not make possible the comparison of the authentication techniques in our focus. The used metrics (e.g., authentication delay, throughput of higher layer protocol) blur the information on the number of jobs

Table 1
Main terms and abbreviations.

Abbreviation	Description
IPsec	Internet Protocol security is a standardized protocol suite to provide encryption, integrity, message origin authentication and anti-replay protection for IP datagrams between hosts
SA	An IPsec Security Association (SA) is the bundle of algorithms and parameters on two end-hosts, being used to encrypt and authenticate IP datagrams filtered by traffic selectors in one direction. Therefore, in normal bi-directional traffic, the flows are secured by a pair of SAs
IKEv2 RFC 5996 [12]	Internet Key Exchange v2 is the most widespread security control protocol for dynamic SA negotiation between pairs of nodes. It provides strong ephemeral Diffie–Hellman key exchange, session key material generation for SAs, strong protection against Denial-of-Service, replay and man-in-the-middle attack. The integrity, message origin authenticity, and confidentiality of control messages can be guaranteed on high security level. IKEv2 supports fine-grained policies, therefore, optionally more than one SA pairs can be negotiated between a pair of nodes for different types of flows
PSK RFC 5996 [12]	It refers to IKEv2 with Pre-shared Key Based authentication in the paper. PSK implements a simple authentication method where the parties verify the knowledge of a shared secret by the remote peer. PSK is suitable only for small-scale scenarios, and it is considered to be a weak solution due its dependency on out-of-band key management
EAP-AKA RFC 5448 [13]	It refers to IKEv2 EAP-AKA in the paper. EAP-AKA scheme is based on a long-term secret key that is stored in the USIM of the subscriber and in the Home Subscriber Service of the operator. EAP-AKA is the standard user access authorization scheme in untrusted non-3GPP access networks, e.g., Wi-Fi hotspots operated by third parties
EAP-TLS RFC 5216 [14]	It is an abbreviation for IKEv2 using EAP-TLS authentication in the paper. EAP-TLS provides strong mutual authentication based on public-key certificates and public-key signatures. It is the only method among the evaluated IKEv2 schemes that can provide non-repudiation of information exchange, when signed messages are logged at a secure place with secure timestamps. It requires Public Key Infrastructure and the inherent certificate authorization, distribution, revocation services. It is typically deployed in corporate Virtual Private Network (VPN) scenarios
HIP RFC 4423 [15]	The Host Identity Protocol (HIP) is protocol suite for the control of the establishment, update and deletion of SA pair between pairs of hosts. Its main difference compared to IKEv2 is the separation of addressing mechanism into identity-based addressing on the application-layer and locator- or IP- based addressing in the network-layer. Every HIP-aware node in the network has one or more own, globally unique public and private key pairs. The public keys represent the Host Identities (HIs). A HIP message, which conveys a public-key signature and the HI is self-certifying with respect to message origin authenticity. For user and operator-level authentication, the HIs must be mapped to user or operator identities using access control lists or certificates
BEX RFC 5201 [16]	It refers to HIP Base Exchange in the paper. It is the basic HIP procedure for SA establishment, provides exchange of ephemeral DH keys and generation of key material, strong mutual authentication of the parties and non-repudiation of communication. It also gives protection against Denial-of-service (DoS), replay, man-in-the-middle attacks
DEX draft [17]	It refers to the HIP Diet Exchange protocol in the paper. DEX is operationally similar to BEX, but uses lightweight elliptic curve cryptography primitives. Compared to BEX, it has weaker resistance to DoS attacks. It does not provide support for perfect forward secrecy due to static DH key exchange. It does not provide non-repudiation due to lack of public key signatures, and does not encrypt the HI. DEX is designed to run on resource-constrained devices, e.g., in Wireless Personal Area Networks (WPANs)
DEX-AKA [18]	It signifies HIP Diet Exchange extended with EPS-based AKA authentication. This method is based on DEX, but extends it with the 3GPP Authentication and Key Agreement method, which provides strong mutual authentication