Chapter XXIV
Generic Application Security in Current and Future Networks

Silke Holtmanns
Nokia Research Center, Finland

Pekka Laitinen
Nokia Research Center, Finland

ABSTRACT

This chapter outlines how cellular authentication can be utilized for generic application security. It describes the basic concept of the generic bootstrapping architecture (GBA) that was defined by the 3rd generation partnership project (3GPP) for current networks and outlines the latest developments for future networks.The chapter will provide an overview of the latest technology trends in the area of generic application security.

INTRODUCTION

Applications in wireless networks require a very reliable method for user authentication and communication security. We will outline the reason for the security needs for mobile application compared to Internet application security. It starts with the application specific security approach used today by many mobile operators and describes the motivation that lead into the development of the generic bootstrapping architecture (GBA) of 3rd generation partnership project (3GPP).

The main function of GBA and also its dialects and variations are explained. GBA has been adopted by various standardization bodies and used by many applications. GBA was first embraced by mobile applications, like the 3GPP Mobile Broadcast Multicast Service, open mobile alliance (OMA) presence service, OMA broadcast smart card service protection profile, GBA Profile, and so forth.

The ongoing convergence of fixed and mobile network resulted in the adaptation of GBA-based application security for fixed and cable networks. We close with a snapshot of the ongoing work for

application security in beyond third generation (B3G) networks.

APPLICATION SECURITY FOUNDATIONS IN MOBILE NETWORKS

Special Requirements for Mobile Application Security

Applications in wireless networks require a very reliable method for user authentication and communication security due to their special environment. There are the following security reasons for this:

- The communication to the service provider goes over the air and can be eavesdropped or modified, if not properly secured.
- The service may be offered over any kind of IP-based channel, then the protection of the service by the underlying bearer protocol can not be taken for granted. The authentication and the service usage may be performed over different channels.
- Username/password authentication is not very secure or user friendly on a mobile device with numeric keypad; hence the temptation to choose too short or easy-to-write passwords is even greater than in the fixed network environment.

Operators or third parties that provide server-based applications in mobile networks have to face additional challenges that reflect on the choice of a potential security solution for application security:

- **Roaming agreements:** The home operator of a user maybe liable to roaming partners or application providers, if an unauthorized user uses a service. This potential liability could even be exploited by malicious application providers. This is no empty threat, as the malicious usage of premium short message service (SMS) usage is an existing problem.
- **Development costs:** Development of mobile applications is much more expensive than that for Internet usage, hence if an application is seriously compromised, then the resulting loss is much higher.
- **Updating problem:** In the fixed network environment security patches and updates are a daily occurrence, this is not that common in the mobile environment. Even if some mobile software platforms offer the possibility to be updated via a PC or over-the-air (OTA) mechanisms.
- **Protection of investments:** Mobile operators make big investments in their network infrastructure; hence reusage of deployed network nodes needs to be taken into account. Especially, when new services are rolled out, these services should work in a harmonic way with the existing nodes.
- **Existing smart card base:** Operators hand out smart cards to their subscribers, these cards have very different capabilities (e.g., subscriber identity module (SIM) cards, universal SIM [USIM], etc.), and operators are unlikely to replace already handed out smart cards. It is more likely, that the user replaces the device. A smart card is replaced, when a user changes operators.
- **Service usage costs:** The cost of browsing is bound to the type of access the user is using. When mobile access is used, this may imply some significant costs for the user. Also, some mobile service fees already include the access cost, that is, the user does not have to pay twice for the content and the delivery. Hence, user authentication comes in mobile applications "earlier" than in the Internet case.
- **Reliability and availability:** If an Internet application does not work, because the authentication database crashed, then in many cases this is not that severe an issue and the user can still use other services (except for those 100% online shops like amazon.com). But if the operator's subscriber database can not be reached, users can not make phone calls, roam, send SMS messages, and, in the end, the operator has no opportunity to offer