A LIGHTWEIGHT RECONFIGURABLE SECURITY MECHANISM FOR 3G MOBILE DEVICES

Jalal Al-Muhtadi
Dept. of Computer Science
Univ. of Illinois at Urbana-Champaign
almuhtad@uiuc.edu

Dennis Mickunas
Dept. of Computer Science
Univ. of Illinois at Urbana-Champaign
mickunas@uiuc.edu

Roy Campbell
Dept. of Computer Science
Univ. of Illinois at Urbana-Champaign
rhc@uiuc.edu

ABSTRACT

Wireless communications are advancing rapidly. We are currently at the verge of a new revolutionary advancement in wireless data communications: the 3rd Generation of mobile telecommunications. 3G promises to converge mobile technology with Internet connectivity. Wireless data, multimedia applications and integrated services will be among the major driving forces behind 3G. While wireless communications provide great flexibility and mobility, they often come at the expense of security. This is because wireless communications rely on open and public transmission media that raise further security vulnerabilities in addition to the security threats found in regular wired networks. Existing security schemes in 2G and 3G systems are inadequate, as there is a greater demand to provide a more flexible, reconfigurable and scalable security mechanism that can evolve as fast as mobile hosts are evolving into full-fledged IP-enabled devices. We propose a lightweight, component-based, reconfigurable security mechanism to enhance the security abilities of mobile devices.[*]

1. INTRODUCTION

Wireless communications are advancing rapidly. We are currently at the verge of a new revolutionary advancement in wireless data communications: the 3rd Generation of mobile telecommunications, and GPRS, the stepping-stone preceding 3G. Wireless data, multimedia applications and integrated services will be among the major driving forces behind 3G. While wireless communications provide great flexibility and mobility, they often come at the expense of security. This is because wireless communications rely on open and public transmission media that raise further security vulnerabilities in addition to the security threats found in regular wired networks.

To realize the full potential of wireless data while providing secure communications, a more robust and flexible security mechanism is needed in mobile devices, particularly, mobile phones, portable communication services (PCS) and 3G devices. This security mechanism has to be lightweight, reconfigurable and capable of capturing the dynamism and agility of mobile environments. Moreover, our objective is to base the proposed security mechanism on a proven commercially available security infrastructure that is widely used in existing IP networks. Thereby granting us flexibility, scalability and the ability to interoperate securely with existing security mechanisms like Kerberos [Ker] and [Neu94] or SESAME [Ses]. Such a system should be able to provide confidentiality, authentication, integrity and non-repudiation services. Moreover, we aim at providing security services that are flexible enough to secure IP-based applications and meet e-commerce security needs while providing enhanced security and authentication for regular voice communications.

Our approach is to employ a component-based, lightweight, portable security mechanism that we developed based on the SESAME architecture: *Tiny SESAME.* This paper discusses Tiny SESAME and its deployment in mobile networks. This paper is organized as follows. Section 2 briefly describes the evolution of Tiny SESAME and motivates its use in mobile environments. Section 3 discusses Tiny SESAME's architecture. Section 4 describes the use of Tiny SESAME in mobile networks. Section 5 briefly mentions Tiny SESAME implementation and the test-bed we used to experiment with mobile communications.

2. TINY SESAME

SESAME is a European security architecture for distributed systems. SESAME extends Kerberos by providing additional services. These services include support for asymmetric cryptography, use of special certificates called PACs (Privileged Attribute Certificates) to authenticate principals and identify their privileges, security attributes and access rights. SESAME also provides authorization services through the Role-Based Access Control (RBAC) model [San96]. Moreover, SESAME defines different key management protocols and cryptographic profiles while maintaining backward compatibility with Kerberos. In

[*] This research was funded in part by the Motorola Center for Communications at the University of Illinois at Urbana-Champaign and NSF 98-70736.

order to allow application developers to utilize its security services, SESAME adopts the Internet standard GSS-API (*Generic Security Services Application Programming Interface)* [Lin93] and [Lin97]. GSS-API is a standard programming interface for generic security services. ECMA standardized SESAME in [Ecm96a] and [Ecm96b]. Further details about the original SESAME architecture and implementation can be found in [Kai94], [Mcm95] and [Kai98].

The popularity and widespread of mobile and handheld devices, and the evolution of mobile telecommunication technologies demand a lightweight, component-based, reconfigurable security mechanism that is able to adapt to environments with scarce resources. Nonetheless, this component should be able to reconfigure and evolve as soon as further resources can be spared. The SESAME system with its various protocols and complicated data structures demands high resources in terms of memory and processing power which exceed the typical capacity of mobile devices. *UIUC SESAME* [Cha99] is a portable version of SESAME implemented completely in Java. *Tiny SESAME* is a component-based subset of UIUC SESAME that supports authentication, protocol negotiation, various levels and strengths of encryption, and access control based on the RBAC model. Tiny SESAME's Light-weightiness is achieved through the employment of a dynamically reconfigurable component-based architecture. This architecture allows Tiny SESAME enabled devices to negotiate dynamically the security services, protocols, and cryptographic support needed. Further, it omits the more advanced capabilities of SESAME such as restricted delegation, PV/CV, and intensive auditing. Tiny SESAME employs a Java-based GSS-API that enables applications on the mobile device to interface with the security services.

3. TINY SESAME ARCHITECTURE

In this section, a brief description of Tiny SESAME's architecture is in order.

3.1 General Overview

A secure environment that utilizes Tiny SESAME consists of at least three major components (Figure 1): the client application or the initiator who is attempting to securely contact a server or get a service, the application server or the service, and the security server which authenticates the users and makes access control decisions. The client and server use GSS-API to authenticate and request security services for the communication channel. A detailed view of the architecture is shown in Figure 2.

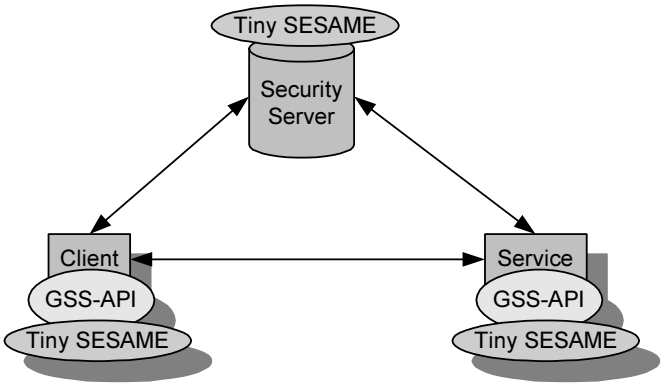

Figure 1: General Overview

3.2 Client side

The client side is the client application that would like to incorporate security services to access a service or an application server. The client application resides on some *user sponsor.* The user sponsor could be a personal computer, a handheld, a mobile host or any device capable of running Java. The SACM (Secure Association Context Manager) provides data integrity and confidentiality services for the communication between the client and the service.

The GSS-API on top of SACM provides Java programs with a standard interface to access SACM services.

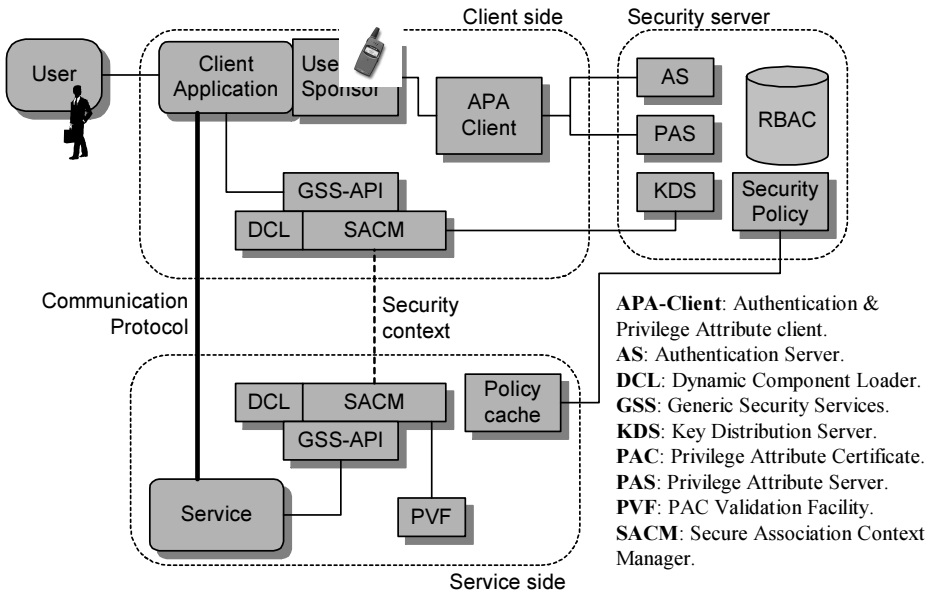

Figure 2: Tiny SESAME Architecture

Since SESAME's protocols are rather complex and resource demanding, in Tiny SESAME different protocols, cryptographic profiles and access control models are implemented as separate software components. These components are loaded dynamically on demand. Once a component is no longer needed it can be unloaded on the fly, allowing only necessary components to be loaded in memory at one time. The DCL (Dynamic Component Loader) is responsible for on-demand loading of required components. Section 3.5 describes the currently implemented components in Tiny SESAME. The APA-Client (Authentication and Privilege Attribute Client) is responsible for secure connections with the authentication server.

3.3 Security server

The security server includes an AS (Authentication Server), which provides a single sign-on point for the distributed environment. Tiny SESAME supports two authentication methods. The first is based on Kerberos authentication, which is based on passwords and symmetric keys. The second is based on the X.509's strong two-way authentication protocol [Itu93], which uses public-key cryptography.

The KDS (Key Distribution Server) manages the cryptographic keys that are used for mutual authentication between the client and remote server. Like its Kerberos counterpart, it relies on symmetric encryption. It is worth noting that in SESAME, if the PAC validation facility (PVF) uses long-term public-keys then the KDC can be bypassed. In this scenario, the session keys are generated by the client side's SACM, consequently, the security server is not able to decrypt the communication between the client and the application server.

The PAS (Privilege Attribute Server) provides information about the privileges and security attributes of users and user sponsors. This information is provided to principals in the form of a special data structure referred to as the PAC. The PAC is signed, as a protection against tampering, using the private key of the PAS. Different PACs can be issued to different users and entities to identify them. The PAC can contain the role-names assigned to a particular principal. The PAC and the security attributes and roles contained within are used for access control decisions based on an RBAC (Role-Based Access Control) model [San96]. RBAC is employed for its power of expression and flexibility. RBAC makes it easy to define well-structured rules and practices for regulating and managing sensitive data and resources. These rules and regulations form "security policies" that are defined and stored within the security server. An example of a security policy may include restricting access to subscription-based services or reserving certain bandwidth for emergency services, etc.

3.4 Service side

The service side represents the application servers providing specific services that users try to access remotely. Here the SACM, GSS-API and DCL are present and function exactly as their counterparts on the client side. The PVF (PAC Validation Facility) is the component responsible for checking the validity of PACs and detecting any tampering. The policy cache provides caching for security policies relevant to the service. This eliminates the need to consult the security server for every access decision.

3.5 Component-based architecture

Mobile devices differ greatly in their capabilities, processing powers and security needs. What is needed is a security model that can adapt to the particular capabilities and security requirements of a mobile or an embedded device. Tiny SESAME achieves this by incorporating a component-based design for the client and service sides. In this design, the different security services, protocols and cryptographic profiles are implemented as separate components that can be loaded, unloaded or reconfigured on demand. Thus, the security requirements of a device determine which components, or code modules, are loaded, effectively keeping Tiny SESAME's size manageable.

Tiny SESAME consists of a core component that contains the essential functionality. This includes the Tiny SESAME factory object, the DCL and the GSS-interface without the actual implementation of the security services. The DCL is capable of loading other Tiny SESAME components from the device's built-in memory, on demand. The Tiny SESAME package contains several components. Currently, these include several components that implement SACM using different encryption algorithms (SACM-RC5, SACM-DES, and SACM-A5), the SACM with a full-crypto library (includes the most popular encryption algorithms together in one component), the APA-client component, and the PVF component. For security reasons, Tiny SESAME's critical components are loaded only from local memory. However, it is possible to extend or update Tiny SESAME's components, through special add-on components that are certified and digitally signed by a trusted certificate authority. Upon verifying their integrity and trustworthiness, the components can be loaded into Tiny SESAME. Additional cryptographic algorithms can be written as certified and digitally signed code modules that can be loaded and used.

4. EMPLOYING TINY SESAME IN 2G/3G

4.1 Existing Security

In this section we present a brief description of the existing security in 2G and 3G systems. Further details for 3G security can be found in the 3GPP specification [Gpp].

While the detail of the 2G security is documented in the GSM standard [Gsm].

Initially, the mobile host identification number is transmitted to the base station (BS) unprotected. The receiving BS identifies the mobile host and contacts the home environment of the subscriber. In both 2G and 3G systems, a random challenge (RAND) is generated by the subscriber's HLR and AuC. Additionally, a session key (SK) is derived. From this random challenge and the subscriber's individual key (K), which is stored on the 2G SIM card or the 3G USIM card, the expected response (RESP) is calculated and the session key is derived at the mobile host. This session key is 64-bits in 2G systems, and 128-bits in 3G systems. Moreover, in 3G systems security is further enhanced through the use of a 128-bit integrity key (IK) and an authentication token (AUTN) that serves to authenticate the home location to the mobile station, enabling mutual authentication. At the subscriber's HLR, the security information is grouped together to form a *triplet* in the 2G case: $<CHAL_{2G}, RESP_{2G}, SK_{2G}>$ and a *quintuplet* in the 3G case: $<CHAL_{3G}, RESP_{3G}, SK_{3G}$, IK, AUTN>. This information is sent to the requesting VLR. In 2G and 3G the authentication of the user is based on his or her knowledge of the individual key (K). Upon receiving the random challenge, the mobile host calculates the response (RESP) and derives the session key. If the mobile station returns the correct response, then the authentication is complete in 2G systems and data transmitted will be encrypted with the session key. In 3G systems, however, additional steps are required, during which the AUTN is sent to the mobile station for mutual authentication. Finally, the 3G mobile host derives the integrity key, and data can be encrypted and validated.

4.2 Limitations of Existing System

Existing authentication and security in 2G/3G have several limitations. First, the subscriber's ID confidentiality is threatened as a result of the initial sending of the mobile host's identification number unprotected. Second, the key sizes and the encryption and decryption algorithms are fixed. This makes the existing systems inflexible and less secure, whenever a security vulnerability is discovered in an existing algorithm, as the case for GSM's A5/1 algorithm [Bir99]. Having a dynamic security mechanism that is able to negotiate and load new encryption modules with different key lengths on demand allows greater flexibility. In addition to securing mobile communications, the security mechanisms in mobile devices should be able to provide security services for multimedia applications and IP-based services. Moreover, the security mechanism should have the potential to provide more advanced security services that include the creation and enforcement of flexible security policies that are customized for individual services, network administrative domains, organizations and users.

4.3 Using Tiny SESAME for Initial Authentication and Call Setup

In our existing work, Tiny SESAME for mobile devices supports two different authentication protocols. Due to its component-based design, additional authentication protocols can be added later through additional add-on loadable modules. The following subsections will briefly discuss the different approaches. Further details of the protocols will be included in the full paper.

4.3.1 3G Compatibility Mode

This is the default authentication mechanism. It is backward compatible with the proposed authentication and security aspects for 3G [Gpp]. This involves the formation of the security quintuplet (or triplet in case of 2G system) exactly as described in the previous section. The mobile host's ID is transmitted unprotected. For this mode, the network parts of a 3G system do not need any modifica-

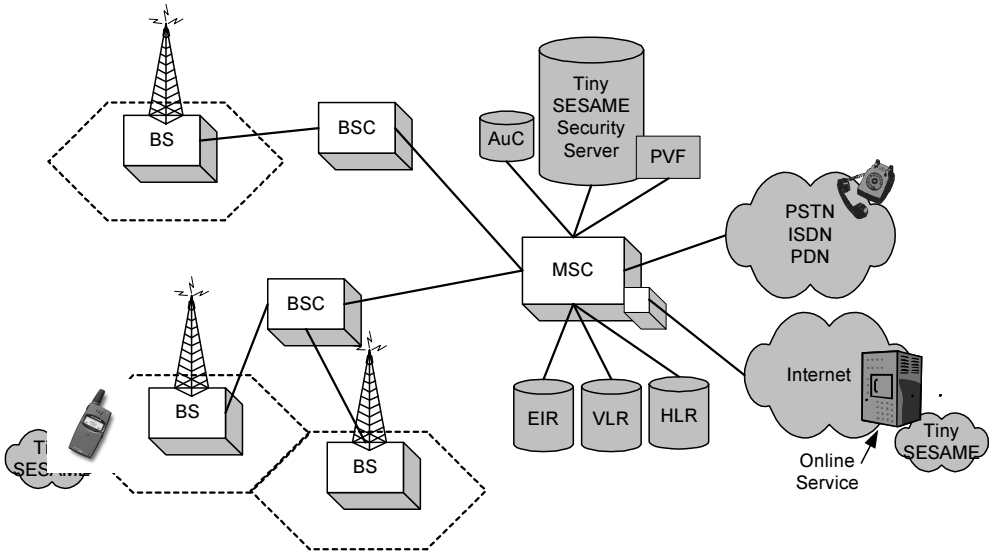

Figure 3: 2G/3G Architecture with Tiny SESAME

tion.

4.3.2 Tiny-SESAME Authentication

In this model, a Tiny SESAME security server should be added to the mobile switching centers (MSCs) (Figure 3), alternatively, the authentication center (AuC) can be enhanced to provide Tiny SESAME security server's services. The Tiny SESAME security server will host the AS, KDS, PAS and PVF components (as described in Section 3). To be able to access the services securely, users are authenticated to the system by the AS component within the security server using an enhanced version of the Kerberos authentication scheme. This scheme will authenticate a user based on his or her knowledge of the subscriber's individual key stored in the SIM or USIM. Initially, the host's ID (unprotected) and an authentication request are sent by the mobile host to the BS. The BS securely passes the request to the security server to authenticate the user. Upon a successful authentication, the user sponsor obtains a PAC from the PAS. The PAC contains the user's roles, security attributes and the basic key. This basic key will be used to derive the session key for securing the communication. The PAC is signed using the private key of the PAS. This PAC can now act as a proof of identity for that user. Further, the security attributes and role names stored in the PAC identify which services that user may access and can be used in creating security policies.

Since a PAC has security attributes that protect it from tempering and has an expiration period, it can be stored within the mobile host. This improves performance and limits the messages exchanged as the mobile host can use the PAC to authenticate itself to different base stations without waiting for security information to come from the HLR of the subscriber's home environment. The security server at the MSC will validate the PAC through its PVF component. In case the PAC was issued from another domain, the SESAME inter-domain authentication protocol can be employed (details are in the full version of the paper).

Last, but not least, through a slight modification of the protocol, a higher subscriber confidentiality can be achieved. In this case, the asymmetric cryptography capabilities of Tiny SESAME are utilized to encrypt the host's ID with the public key of the nearby MSC rather than sending that information unprotected.

4.4 Using Tiny SESAME to provide Security Services for Multimedia Applications

In addition to adding security to voice and data calls, in mobile devices Tiny SESAME can be used to provide security services for multimedia or IP-based applications. This is essential, particularly in an all-IP 3G network. Since Tiny SESAME is backward compatible with Kerberos, applications on the mobile host can interact securely with "Kerberized" or "Sesamized" applications or services (like the ktelnet application and others [Ash98]). When the mobile host wishes to use network services, the stored PAC is sent using the SACM to the desired service. The data sent is transferred by any protocol (radio signals and/or IP etc.) to the service. If the service employs SESAME as well, then it passes the PAC to the PVF, which verifies, from the integrity protection, that the PAC is genuine and a secure association is established over which the user can communicate with the remote service. However, if mutual authentication is desired, where a mobile host wants to make sure it is contacting the intended service, the PAC of the target device is sent back before the establishment of the secure association. Once all PACs are validated successfully, the secure association can take place.

5. TINY SESAME IMPLEMENTATION

Tiny SESAME was originally implemented in Java. To experiment with security in mobile devices, a version of Tiny SESAME was ported to PersonalJava™ running on Windows CE 2.11 devices.

Our test platform was an HP Jornada 680, running Windows CE 2.11. The Jornada has a Hitachi SH3 processor running at 133 MHz, 16 MB RAM, and a screen resolution of 640x240, 256 colors. The Jornada is equipped with wireless Ethernet. We wrote code to simulate the functionality of VLR, HLR, and the AuC and ran it on fixed workstations on the LAN. Using the Jornada we were able to get some performance results of selected encryption algorithms on the Jornada (Table 1). We assume this would be close to the performance of a 3G device. We tested the different authentication and call setup schemes mentioned in Section 4.3 and got the preliminary performance measures shown in Table 2[1].

Table 1: Encryption/Decryption Speed

DES 56 encryption (for 32 bytes of data)	82.0 ms
DES 56 decryption (for 32 bytes of data)	82.4 ms
RC5 128 encryption (for 32 bytes of data)	42.05 ms
RC5 128 decryption (for 32 bytes of data)	47.45 ms
RSA 512 encryption (for 32 bytes of data)	384.0 ms
RSA 512 decryption (for 32 bytes of data)	236.0 ms

[1] The results are obtained under the assumption that the propagation delay between the mobile unit and the BS is 1 ms. and the propagation delay between the VLR and HLR is 5 ms., with a maximum bandwidth of 2 Mbps (wireless Ethernet).

Table 2: Performance of the proposed authentication and call setup schemes

3G compatibility authentication	8.04 seconds
Tiny SESAME authentication through PACs.	10.02 seconds
Tiny SESAME authentication with higher-subscriber confidentiality (through public key encryption).	16.34 seconds

6. FUTURE WORK

We are using OPNET Modeler to more accurately simulate 2G and 3G security aspects and measure the impact of employing Tiny SESAME in different scenarios and comparing the results with conventional 2G/3G security. We are also working on porting Tiny SESAME to Java 2 Micro Edition Mobile Information Device Profile (J2ME MIDP). The J2ME MIDP is a targeted Java API for writing wireless applications that run on all mobile phones and pagers supporting the MID profile.

7. REFERENCES

[Ash98] P. Ashley, M. Vandenwauver, and B. Broom. "*A Uniform Approach To Securing Unix Applications Using SESAME*" in C. Boyd and E.Dawson, editors, proceedings of the 3rd ACISP Conference - LNCS 1438, pages 24-35, Springer-Verlag, 1998.

[Bir99] A. Biryukov and A. Shamir, *"Real-Time Cryptanalysis of the Alleged A5/1 on a PC"*, Preliminary draft, December 1999.

[Cha99] M. Chandak, "*UIUC-SESAME: Achieving a Portable Authentication, Access Control, and Delegation Protocol*", Masters Thesis at Department of Computer Science, University of Illinois at Urbana-Champaign, 1999.

[Ecm96a] ECMA-219, "*Authentication and Privilege Attribute Application with related key distribution functions*", 2nd edition, European Computer Manufacturers Association, March 1996, http://www.ecma.ch

[Ecm96b] ECMA-235, "*Security in Open Systems – The ECMA GSS-API Mechanism*", European Computer Manufacturers Association, March 1996, http://www.ecma.ch

[Gpp] 3GPP Draft Technical Specification 33.102: *"3G Security Architecture"*.

[Gsm] European Telecommunication Standard GSM 02.09: "*Digital cellular telecommunications system (Phase 2+); Security aspects*".

[Itu93] ITU-T Recommendation X.509 (revised), *The Directory – Authentication Framework,* 1993, International Telecommunication Union, Geneva, Switzerland.

[Kai94] P. Kaijser, T. Parker, and D. Pinkas, "*SESAME: The Solution to Security for Open Distributed Systems*", Computer Communications, 17(7):501-518, July '94

[Kai98] P. Kaijser, "*A review of SESAME Development*", Proceedings of the 3rd ACISP Conference, pages 1-8, 1998.

[Ker] MIT's Kerberos Homepage, http://web.mit.edu/kerberos/www/index.html

[Lin93] J. Linn, "*Generic Security Service Application Program Interface*", September 1993, RFC 1508

[Lin97] J. Linn, "*Generic Security Service Application Program Interface Version 2*", January 1997, RFC 2078.

[Mcm95] P. McMahon, "*SESAME V2 Public Key and Authorisation Extensions to Kerberos*", in proceedings of the symposium on Network and Distributed System Security, pages 114-131, February 1995.

[Neu94] B. Neumann and T. Ts'o, "*Kerberos: An Authentication Service for Computer Networks*", IEEE Communications Magazine, 32(9): 33-38, September 1994

[San96] R. Sandhu, E. Coyne, H. Fienstein, and C. Youman, "*Role Based Access Control Models*", IEEE Computer, 29(2), February 1996.

[Ses] SESAME. The SESAME homepage https://www.cosic.esat.kuleuven.ac.be/sesame/