

Network Infrastructure for Academic IC CAD Environments

Pedro Coke*, Cândido Duarte*[†], André Cardoso*, Vítor Grade Tavares*[†], and Pedro Guedes de Oliveira*[†]

*Microelectronics Students' Group, Department of Electrical and Computer Engineering,

FEUP – Faculty of Engineering, University of Porto, Rua Dr. Roberto Frias, s/n, 4200-465 Porto, Portugal

[†]INESC Porto, Campus FEUP, Rua Dr. Roberto Frias, 378, 4200-465 Porto, Portugal

Abstract—This paper presents an initiative to involve ECE undergraduate students in the design and deployment of a network infrastructure for an academic laboratory. The project aims at attaining a reliable and secure network for an IC CAD environment. The students focused on employing secure authentication, accounting and storage with single sign-on, based on enterprise-grade, open-source protocols. This initiative proved to be highly motivating and allowed the students to develop knowledge and hands-on experience on the area of network security. The resulting network design and core infrastructure is herein described as well as its deployment in a real microelectronics design environment.

Index Terms—Extracurricular activities, cooperative learning, information technology, network security, CAD networks.

I. INTRODUCTION

It is well accepted today that modern higher education demands a paradigm change, a shift from a synchronous supervised learning to a more dynamic and student-centred methodology, where the acquisition of general skills is also central. For these purposes, new environments must be created where students are invited to take an active part in the planning of their own activities [1]. Extracurricular projects, in this respect, can take an important role in consolidating learning outcomes. It helps knowledge maturing, putting into practice subjects covered by the courses, with grounds for the student to decide what, when and how to learn. Moreover, keeping the student supervision to a minimum induces them to better self-organize, cooperate, establish and accept leadership, develop verbal communication and fully understand the importance of ethical behavior. Additionally, if well designed, extracurricular projects are a perfect testbed to understand the effectiveness of this new paradigm, and can adequately complement aspects of professional profiles that are difficult to cover within the regular courses. Naturally, the students participate on a voluntary basis, with little external intervention, besides suitable working conditions and an attractive project proposal.

In undergraduate courses it is often difficult to go deep on certain topics for lack of experience and training [2]–[4]. Contextualizing these topics using more realistic settings can help overcome difficulties [5]. Some efforts have been made to address these issues through project-based learning in engineering courses [6]–[8]. However, it is our experience that a valuable contribution to this methodology are extracurricular activities, as referred earlier, where students are less bound by

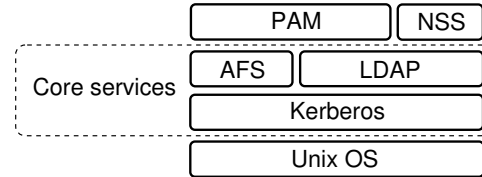


Fig. 1. Service structure overview

a scope of solutions and can freely explore their own topics of interest. Such a scenario lends itself to a cooperative learning approach.

The initiative described in this paper gathers students interested in computer networks. It provides them with an opportunity to further improve their knowledge through hands-on experience, addressing some crucial topics covered in-depth as a project with immediate application. The target consists of an Electrical Engineering laboratory for integrated circuit (IC) design. This is a type of infrastructure that requires heavy computation and a wide-range of computer-aided design (CAD) tools, supported by various network services. The students were encouraged to build a reliable and secure network infrastructure for this purpose.

This paper is organized as follows. Section II contains a project overview as well as the project goals. Section III explains the proposed network infrastructure, services and software used. Section IV discusses the results of the project. Finally, in Section V, some conclusions about this project are drawn.

II. PROJECT OVERVIEW

In the Electrical and Computer Engineering (ECE) Department of the Faculty of Engineering of the University of Porto, students have been invited and stimulated to take part in the development of IC projects joining the Microelectronics Students' Group [9]. This group established a well-suited working environment for IC design. Over time, however, more complex projects demanded an increasingly sophisticated framework. As such, there was a need for a more reliable and secure computer network, comprising several services and software as depicted in Fig. 1 – the main focus of the present work. The design of this network infrastructure was assigned to a group of three students: two undergraduate students – one

in Informatics and Computing Engineering and the other in ECE – and a graduate student enrolled in the Doctoral Program in ECE.

The students started by reviewing the existing solutions from a technical, administrative and user perspective to define the project requirements. Security was identified as the biggest concern. In fact, the University network to which the laboratory is connected is accessible to everyone and, in this sense, can be considered insecure. The option of isolating the laboratory network from the outside was not considered, since it would still be vulnerable to inside attacks. Moreover, since working with IC technologies very often means using confidential documents and files or intellectual property (IP), the need for a secure network is further reinforced. To implement such an infrastructure, in an insecure network, secure authentication and encryption methods are required.

From an administration and management standpoint, there are two important issues: software management and operating system (OS) deployment. In a typical IC CAD laboratory, the installed software requires frequent updates. Maintaining this software on numerous machines can be time-consuming, which calls for a centralized management. Deployment of the OS and subsequent configuration is a similar problem, where manual installation and setup can be a daunting process. Therefore, automation of this task is also a requirement.

From the user standpoint, remote access is a useful feature since it allows working outside the laboratory, using a Virtual Private Network (VPN) to the University. To further improve user experience, one should be able to log in any available computer and have access to personal data, as well as to licensed design software. By employing centralized authentication, accounting and storage systems with a single sign-on mechanism, the user is granted seamless access to all network services and software.

III. NETWORK INFRASTRUCTURE

The choice of an OS presents itself as a basis for other design and implementation decisions. The CentOS 5 Linux distribution is chosen as it is free, stable and includes a wide range of software packages as well as long-term core support [10]. Moreover, it is based on Red Hat Enterprise Linux (RHEL) – a commercial, enterprise-grade distribution – the operating system where most IC CAD software is designed to run on.

A. Core Services

Services that implement the minimum network operation requirements are considered core services. These include authentication, user management and accounting, and storage, which are structured according to Fig. 1.

1) *Authentication*: In computer networks, authentication is the act of establishing the authenticity of a user, service or host. To satisfy the requirements for authentication and provide encryption mechanisms, the Kerberos V protocol was chosen. It is a symmetric key protocol that provides secure authentication on insecure networks [11]. Through the

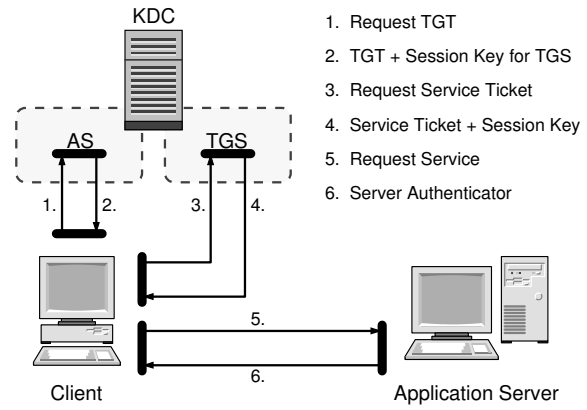


Fig. 2. Kerberos protocol overview

use of shared private keys, it enables mutual authentication between users, services and hosts – called principals. To ensure that the security methods used are suitable for the proposed requirements, there was a need for close examination of the protocol mechanisms. Due to the importance of Kerberos in the authentication process in which all other services rely, a brief description of the protocol is presented next.

Kerberos is based on the Needham-Schroeder protocol [12], which enables two parties to establish a shared session key for secure communication. This system builds up on an architecture where a trusted central entity, known as the Key Distribution Center (KDC), shares symmetric cryptographic keys with every principal in the network. The KDC is composed of two logically separated parts: an Authentication Server (AS) and a Ticket-Granting Server (TGS). The AS enables a principal to authenticate itself and obtain a Ticket-Granting Ticket (TGT), which is used to establish communication with the TGS and obtain specific cryptographic session keys for use with other network services.

An overview of the authentication process is shown in Fig. 2. The authentication phase starts with a request from the client, containing the principal name. If this name is found in the AS database the AS sends a packet containing the session key, which is required for the principal to communicate with the TGS. During this phase, all communications are encrypted with a key known only to the principal and the AS. Thus, if the user is able to decrypt the packet, the authentication is successful.

During this process, mutual authentication is assured through the use of shared session keys and authenticators [11]. This mechanism also provides data encryption, protecting against eavesdropping. In the proposed structure, the MIT Kerberos V implementation is used [13], and further integrated with storage and accounting protocols.

2) *Accounting*: Typical multi-user environments require an accounting structure to store OS specific user data. This includes the username, groups, home folder location and default shell. Since a user must be able to log in to any machine, accounting services need to be networked as well. Usually this is done by using what is called a directory service. A

simple example of a directory service is a phone book, which contains an organized list of names and organizations, each one with an associated phone number.

In the proposed implementation, the Lightweight Directory Access Protocol (LDAP) is used [14]. It is a simple, robust application protocol that can be easily implemented while, offering great flexibility through the use of schemas – sets of rules for the information that is stored. These schemas define types of data, and rules that govern its access and manipulation. In the implementation herein described, LDAP schemas are used to make OS specific accounting information available through the network (Fig. 3).

The OpenLDAP [15] software is chosen to provide the directory service server and client. By default, it does not use any kind of encryption for communication nor authentication. The Generic Security Services Application Program Interface (GSS-API) [16] is used to provide Kerberos authentication and encryption mechanisms to LDAP. Through the use of the Simple Authentication and Security Layer (SASL) [17], which interfaces with GSS-API Kerberos module, LDAP meets the proposed security and encryption requirements.

The Name Service Switch (NSS) facility in Linux is used to bind LDAP accounting information directly into the OS. This way, when the system checks for user attributes, such as the default shell, the LDAP server is queried instead of the local user database.

3) *Storage*: To complete the core service requirements, a storage protocol must be implemented as well. The Andrew File System (AFS) protocol [18] is chosen to provide networked storage services, specifically, the OpenAFS implementation [19]. It uses Kerberos to secure authentication, and employs its own mechanism to encrypt network data.

The AFS protocol also provides a very powerful volume management system. A volume can have a read-write (RW) mount concurrent with a read-only (RO) mount (Fig. 4). Changes on the RW mount can be performed while the RO mount is being used, and any modifications only propagate throughout the network when a release command is run. This is particularly useful for testing CAD software. The CAD manager can install, configure and test new versions of the software on the RW mount, while users remain unaffected, since they are using the RO mount. When the new software has been proven stable and is to be put into production use, a release command is executed and any changes in the RW mount propagate to the RO mount.

To increase performance in high-demand volumes containing CAD software, volume replication is used. This is a

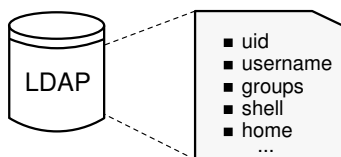


Fig. 3. LDAP schema for OS specific user data.

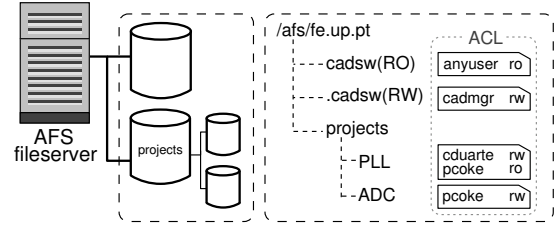


Fig. 4. AFS volume structure, directory structure, RO and RW mountpoints, and ACLs.

feature of the AFS protocol that allows for an RO mount to be replicated on up to eight AFS file servers for load-balancing resources. The AFS volume management system also includes incremental volume backups, which are used for creating snapshots of IC projects and for backup purposes. Management of IC projects involving many users can be eased through the use of Access Control Lists (ACLs), another feature of the AFS protocol.

It should be noted that, due to limited network bandwidth, performance bottlenecks can appear even when AFS volumes experience a moderate loads. To avoid this, a gigabit ethernet connection is used throughout the network.

B. Single sign-on

To provide the user with seamless access anywhere on the network to the services described, a single sign-on system has been implemented. The Linux Pluggable Authentication Modules (PAM) are configured to use Kerberos credentials to obtain access to services at login time. When the user inputs the username and password at login, Kerberos tickets are requested and OpenAFS access is granted, provided the user exists in the LDAP database.

1) *Remote access*: A remote access service is also implemented to allow the user a graphical login from outside the laboratory. An open-source implementation of the NX protocol, FreeNX, was used. It allows near real-time response even when connected through a typical home Internet connection, while maintaining the session encrypted.

C. System deployment and management

1) *Automated installation*: The CentOS installer, Anaconda, is configured to perform non-interactive installations. By using Anaconda kickstart files, SSH public key authentication, and custom scripts, configuration files are copied securely through the network during installation. Furthermore, a profile system has been implemented to differentiate between different hardware and apply configuration accordingly.

2) *System updates*: In order to increase control over the system, a local mirror of the official package repositories is configured. This not only speeds up installation, but more importantly, allows the system administrator to freeze the package versions and update them only when needed. Moreover, a local repository has been set up to provide custom packages, which sometimes are not available elsewhere.

TABLE I
NESSUS VULNERABILITY SCAN RESULTS

	Security severity				Open ports	Plugins ran
	L	M	H	C		
Server (1)	0	0	0	0	31	7725
Clients (8)	0	0	0	0	16	

L = Low, M = Medium, H = High, C = Critical

IV. RESULTS AND DISCUSSION

To ensure that the network complies with the security requirements, a vulnerability assessment was conducted. This is not always a straightforward procedure. A well-known vulnerability scanner, Nessus [20], was used to determine if any compromising security faults were present in the network clients and server. The results of the scans performed on these machines have shown no vulnerabilities, as it can be seen in Table I. Results are grouped by levels, which are derived from the Common Vulnerability Scoring System, an industry standard which evaluates how severe computer systems security vulnerabilities are.

The described infrastructure was deployed in the Microelectronics Students' Group laboratory network, consisting of one server and eight clients, and has been running in a production environment for five months without any major problems.

There are several similar projects running within the group, that follow the same general procedure. The students response has been enthusiastic and the group has been steadily growing. Very relevant results have been achieved leading to several conference proceeding publications and international prizes, attesting the effectiveness of extracurricular projects. Moreover, the students have taken these projects with responsibility and autonomy, self-organizing the group, sharing results and knowledge and building intrinsic motivation. All these are important goals of student-centered approaches and have been closely followed by the ECE department having led to similar initiatives in other fields.

V. CONCLUSION

This paper presents a project in which students successfully implemented a complete network infrastructure, motivated by its deployment on a production environment. The project goals initially defined, regarding usability, security and management, were fulfilled, and the resulting implementation was deployed in an IC CAD laboratory.

The project enabled students to take part in a team and further develop hands-on experience on subjects not thoroughly explored on Computer Science courses. Moreover, since no restrictions to the scope of solutions were imposed, it allowed the students to freely explore different alternatives to achieve the desired outcome.

ACKNOWLEDGMENT

This research work has been partly supported by Universidade do Porto under contract IPG148/2009, INESC Porto under Grant BII/INESCPorto/02, and Foundation for Science

and Technology – FCT, Portugal, under Grant BD/28163/2006. The authors would like to thank Sebastian Tabarce from Synopsys for his valuable insights during this project, and also to José M. Cruz from DEI/FEUP for his advices on network security assessment.

REFERENCES

- [1] S. J. Lea, D. Stephenson, and J. Troy, "Higher education students attitudes to student-centred learning: beyond educational bulimia?" *Studies in Higher Education*, vol. 28, Aug 2003.
- [2] N. Sarkar, "Teaching computer networking fundamentals using practical laboratory exercises," *IEEE Transactions on Education*, vol. 49, no. 2, pp. 285–291, May 2006.
- [3] J. Cigas, "An introductory course in network administration," in *Proceedings of SIGCSE technical symposium on Computer Science Education*, vol. 35, no. 1, Feb 2003, pp. 113–116.
- [4] R. Abler, D. Contis, J. Grizzard, and H. Owen, "Georgia tech information security center hands-on network security laboratory," *IEEE Transactions on Education*, vol. 49, no. 1, pp. 82–87, Feb 2006.
- [5] M. Young, "Instructional design for situated learning," *Educational Technology Research and Development*, vol. 41, pp. 43–58, 1993.
- [6] N. Linge and D. Parsons, "Problem-based learning as an effective tool for teaching computer network design," *IEEE Transactions on Education*, vol. 49, no. 1, pp. 5–10, Feb 2006.
- [7] M. Anisetti, V. Bellandi, A. Colombo, M. Cremonini, E. Damiani, F. Frati, J. Hounsou, and D. Rebecani, "Learning computer networking on open paravirtual laboratories," *IEEE Transactions on Education*, vol. 50, no. 4, pp. 302–311, Nov 2007.
- [8] M. Frank, I. Lavy, and D. Elata, "Implementing the project-based learning approach in an academic engineering course," *International Journal of Technology and Design Education*, vol. 13, pp. 273–288, 2003.
- [9] "Microelectronics Students' Group," <http://cmos.fe.up.pt>, 2010.
- [10] "The Community ENTERprise Operating System," <http://centos.org/>, 2010.
- [11] B. Neuman and T. Ts'o, "Kerberos: an authentication service for computer networks," *IEEE Communications Magazine*, vol. 32, no. 9, pp. 33–38, Sep 1994.
- [12] R. M. Needham and M. D. Schroeder, "Using encryption for authentication in large networks of computers," *Communications of the ACM*, vol. 21, no. 12, pp. 993–999, 1978.
- [13] "MIT Kerberos," <http://web.mit.edu/Kerberos/>, 2010.
- [14] J. Sermersheim, "Lightweight Directory Access Protocol (LDAP): The Protocol," *RFC 4511*, Jun 2006.
- [15] "OpenLDAP," <http://www.openldap.org/>, 2010.
- [16] L. Zhu, K. Jaganathan, and S. Hartman, "The Kerberos version 5 – Generic Security Service Application Program Interface (GSS-API) Mechanism: Version 2," *RFC 4121*, Jul 2005.
- [17] A. Melnikov and K. Zeilenga, "Simple Authentication and Security Layer (SASL)," *RFC 4422*, Jun 2006.
- [18] J. H. Howard, M. L. Kazar, S. G. Menees, D. A. Nichols, M. Satyanarayanan, R. N. Sidebotham, and M. J. West, "Scale and performance in a distributed file system," *ACM Transactions on Computer Systems*, vol. 6, no. 1, pp. 51–81, 1988.
- [19] "OpenAFS," <http://www.openafs.org>, 2010.
- [20] "Nessus," <http://www.nessus.org/nessus/>, 2010.