NSF-CONACyT Project: Development of Risk Assessment Models and Methods for Networked Information Systems.

P.I: Dr. Pedro Mejia-Alvarez. Seccion de Computacion. CINVESTAV-IPN.
Co-PI's: Dr. Arturo Díaz, Dr. Ana María Martínez, Dr. Francisco Rodriguez, (CINVESTAV-IPN) and Dr. Jesús Favela (CICESE).

Summary

The objective of this joint project between CINVESTAV-IPN and Texas A&M University (TAMU) is developing secure information sharing solutions for distance collaboration across the US-Mexico border. Secure and reliable collaboration across the border is an important and challenging issue that affects the performance of the extensive interactions between the US and Mexico organizations. This project is motivated by using the complementary technical capabilities of the two research teams to solve this challenging problem that will greatly benefit both countries.

The common objective of the two companion proposals from TAMU and CINVESTAV-IPN is to create a networking system that will support secure and efficient user interactions, without compromising their own policies, workflow, and system management. Our common goals in this joint project include 1) shared control of data access, 2) ubiquitous accessibility, 3) software risk modeling , 4) high security and reliability, 5) prevention of mutual and external intrusion, and 6) non-repudiation of transactions, to build a federated TTP cluster over the existing information systems. CINVESTAV-IPN team will focus on issues 1,2,3 and 4, and TAMU team will focus on issues 3,4 5 and 6. Of course the typical confidentiality, integrity, and authenticity requirements will be supported for end users.

The aim of CINVESTAV-IPN for achieving our 4 objectives, is to develop risk assessment models to support the development and operation of shared information systems in a distance collaborative environment. Specifically, the project consists of the following phases:

(a).**Develop Shared data access protocols**. We pretend to design and implement a persistent storage system on the top of the secure information sharing for distance collaboration system. The main idea is that a user with a wireless device can view data as it was located in a local server. The system will deal with proxy servers to consider control version, shared access and security issues. In addition, the system must deal with possible communication failures to minimize the risk of information lost. The goal is to extent the distance collaboration capabilities to mobile users.

(b). **Ubiquitous information access for groupware**. Groupware, or computer tools that support collaborative work have benefited from recent advances in computer and telecommunication technology. The research agenda in this field includes the development of software infrastructures that support ubiquitous access to shared resources and which allow for opportunistic interactions. When collaboration crosses organizational, cultural, and/or political borders secure information access becomes a primer concern during collaboration, since partners might still trust the colleagues with whom they collaborate, but not necessarily the security of their information systems. As part of this project we propose to take advantage of TAMU's know-how on the design of secure information servers to provide security guarantees to the PINAS, web-based replicated collaborative framework, on which he have been working in the last few years. To illustrate the application of the solutions being proposed, we will also develop two secure collaborative applications using this framework: one for the collaborative authoring of documents and a second one for the support of collaborative software development.

(c). **Create software security assessment models**. We will develop a framework for the unification of security and software models. Using the UML Object Oriented Model, we will specify the requirements for business collaboration rules, and design phases to model security features such as privacy, integrity, access control and reliability. We are also interested in constructing software systems with *Evolvable Security Features*. We will use *aspect oriented programming* to isolate pieces of software located in different parts of a distributed system for their development and maintenance. Also, we will use architectural *components* and *connectors* to address security concerns such as authentication and access control , together with on-line monitoring and maintenance.

(d). **Implement high performance cryptographic schemes**. In this project we will design, develop and implement well-known Public-key cryptosystems both, in software and hardware using state-of-the-art performance improvement techniques. Since it has been observed that Elliptic Curve Cryptography

(ECC) performs better than its rival RSA cryptosystem for most key-exchange protocol scenarios, we will devote special attention to the development of extremely high performance Elliptic Curve Cryptosystems. For symmetric encryption/decryption, this project will design a complete high-performance 4 Giga bits/S single-chip FPGA implementation of the Advanced Encryption Standard (AES). Obtained results for different cryptosystems and handshake protocols will be comparatively depicted and interpreted

1 Background and Related Work

Distance collaboration is an important information technology which has great impact on the quality of life and economic productivities across the US-Mexico border. Collaboration is motivated to extend services to more users for better efficiency, effectiveness, and convenience. When natural disasters strike, any of collaborating parties should be allowed to activate certain procedures to expedite processing of personal identities, health records, and other related information for emergency caring. Distance collaboration has significant implication on information ownership and authorization. For instance, when one party shares a file with its partner for certain use, the transfer would be permanent unless it can be nullified via fool-proof processes. To prevent abuse of collaborative privileges, when one party agrees to provide services to its partners, such accesses must not lead to security hazards, such as information leakage, by its partners. To prevent dispute of service quality, when one party acts on behalf of its partner, the performed services may be subject to validation later following undisputable protocols.

Obviously, an endless list of common rules may need to be defined and enforced for collaborating parties to maintain their partnership, and we cannot tackle all of them for the limited time and resource constraints. This project is motivated to study some fundamental problems related to distance collaboration in a realistic social setting. On the basis of sound theoretical work and credible prototypes, the research teams from Mexico and TAMU attempt to build a solid common foundation to explore this area in the long run.

Trust is the foundation of collaboration. In [Gerck98] the concept of trust is extensively investigated. More than 20 definitions/properties of trust are described for areas such as communication systems, law, linguistics, social science, commerce, etc. Mapping these abstract definitions/properties to a particular application is not easy. In [Salowey00] some explicit properties of trust for computing systems are defined: 1) provide correct information, 2) perform an operation correctly, 3) keep a secret, 4) perform a protocol correctly, and 5) not to misuse information or resources. Due to the limited resources available, in this project we limit our goal to create common ground between collaborating parties in order to further pursue more advanced secure collaboration features. Instead of broadly pursuing all the issues, we focus on developing a scalable, and *group-supported, group-monitored* (GSGM) communication model, so that no single party can corrupt the model in delivering or receiving services from each other. We will develop highly robust and secure communication models to prevent single point of failure or security breaching. That way, collaborating parties can use the model to implement their control and validation protocols for transactions and data accesses. The communication model is based on the *server anonymity* concept, to prevent single insider from corrupting the system. Roughly speaking, we translate these requirements into *non-repudiation of transactions, prevention of mutual and external intrusion,* and *high reliability and fraud detection of the interconnected systems*.

In our system model (see Figure 1), collaborating parties are divided into three tiers: local information systems, end users (clients), and the proxy servers for interconnection of the information systems. The local information systems provide the information services to the clients, and when necessary, they make request to remote information systems for needed data via the proxy servers. The adversary can either *passively* listen, to steal information, or *active*ly cause certain types of disruptions, such as denial of service attacks. An important issue in our study is prevention of *traffic analysis* by non-group members. Otherwise, the adversary could use network traffic patterns (volumes, peak times, etc.) to predict the interactions of group members without decrypting messages [Raymond00,Berthold00]. We assume that the collaborative parties have full ownership and control of their own information systems and customer services.

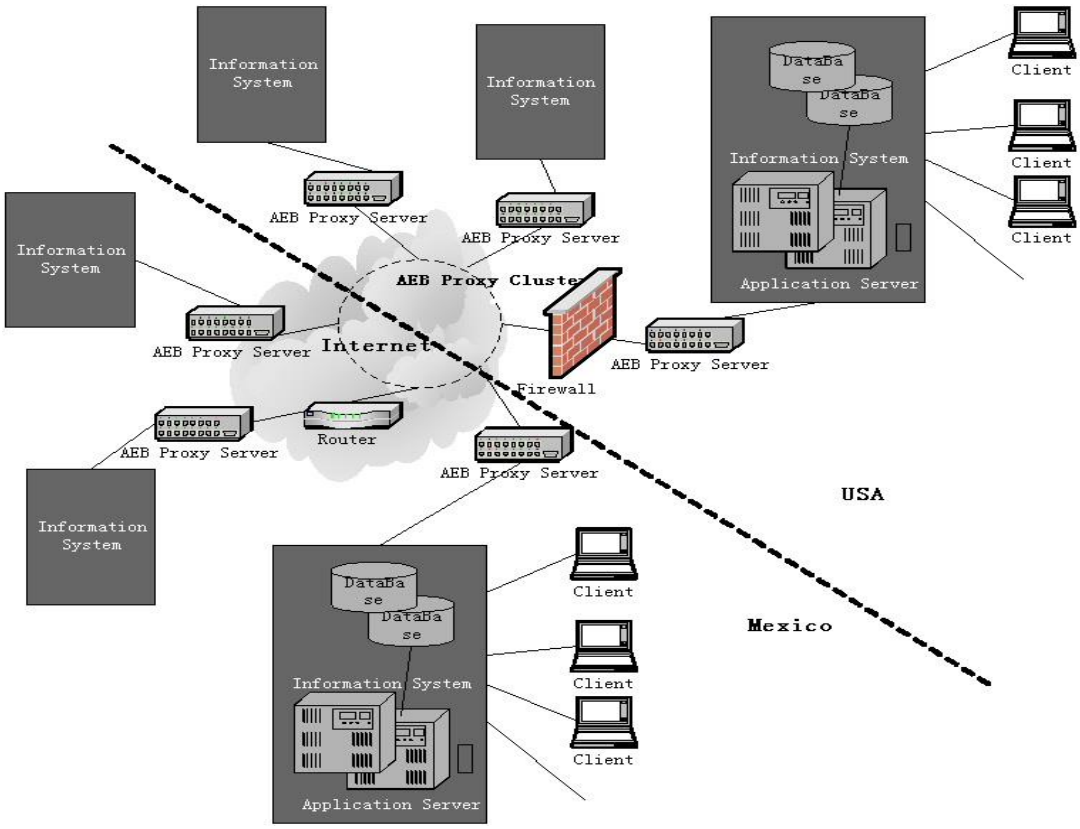

Figure 1. System Architecture

1.1 Importance of the Project for Mexico and US.

Mexico and US are two countries of one system, in which they have shared interests in practically every aspect of their social functions. People in the two counties are physically divided by the long boarder, but their information and telecommunications infrastructures are broadly interconnected and integrated. Even though partners across the boarder work in distance to achieve their common goals, one must not ignore the fact that they are operating in two different legal and ownership systems. Such issues, when not adequately addressed, may lead to costly disputes that call for costly remedial solutions. For instance, if one party decides that it will withdraw from a partnership, and will want its partner to relinquish its proprietary data or services, there will be no easy way to do it but manually verify the involved information systems, one by one. It is only through sound and proven design process that one could expect that sustainable solutions for information sharing and distance collaboration would emerge. It is only through the sound and proven protocols for distance collaboration that the partnership will be enhanced and improved. It is only through the secure information sharing technologies that one can expect that partners in the two countries can prosper from their joint efforts without worrying about side effects of information and services sharing.

Ample examples exist that will benefit from our proposed projects. For commercial applications, it is just common sense that one would want to make common services such as ATM, banking, and health care services across the boarder hassle free. Granted that many large commercial applications run by multi-nation corporations already integrate their world wide operations, but for medium and small businesses, being able to interact with their cross-boarder counterparts can mean new business, new venture and new services. For governmental collaboration, it could mean that the US agencies may delegate such functions as food inspection to their Mexico counterparts, with proven procedures and results to be performed in the field, not at the boarder gates. For rural communities, it could mean that as needed, a social worker can receive authorization to serve a traveler in need of services, regardless of his/her citizenship at the stranger land. Delegation of responsibility and authorization can be done over the phone or other media, but how could one prove or disprove that the counterpart has performed the functions in due process?

From the perspective of information sharing, we are interested in developing collaborative protocols and their assessment methodologies to solve this kind of problems piece by piece.

1.2.- Project Opportunities

The previously presented panorama displays magnificent opportunities for the development of the proposed project. These opportunities are the following

- Little or almost null investigation exists regarding to the networks security solutions for shared information problems between Mexico and US. The consulted publications present dispersed and not structured knowledge.
- This joint proposal is the result of a previous collaborative work between TAMU and CINVESTAV-CICESE in their proposed virtual software systems lab development. The TAMU team is building a software system lab that will allow for flexible design of large software systems in conjunction with their highly successful virtual networking lab. This research laboratory consists of a full array of networking equipment, ranging from high performance ATM switches, routers, QoS Servers, and fiber links. Through this proposed work, the Mexico Team will greatly benefit with the interaction with the TAMU Team, because of their experience and expertise on Networking, security and software engineering. Funding of this proposal will enable Mexico researchers to access some of the advanced networking and server equipment from TAMU that would be otherwise cost-prohibitive for them to own.
- Organisms such as CUDI (Mexico) and INTERNET2 (USA) report the need to face the problems related to security in networked information system environments.
- The trade agreements (e.g. NAFTA) have actually accelerated the speed of changes in engineering practices mainly in the fields of networking security and computer collaborative environments. Our project intends to motivate the creation of "Educational Engineering Programs" that consider "Network Security" and "Secure Information Sharing for Distance Collaboration" in their curricula, that help to prepare engineers for this new type of professional practice.

2. Shared Data Access Protocols for Light Mobile Devices.

Researcher: Dr. Arturo Diaz (CINVESTAV-IPN)

2.1 Abstract

In this project we would like to design and implement a persistent storage system on the top-layer of the secure information sharing for distance collaboration system. The main idea to be developed by our team is to create an environment where a given user connected to our system via a wireless device, can access data as it were located in a local server. Our system will deal with proxy servers to consider control version, shared access and security issues. In addition, our system must also be robust against potential communication failures in order to minimize risks of information lost. The main goal is therefore to extent the distance collaboration capabilities to the mobile-user wireless context.

2.2 Introduction

Light Mobile Devices (LMDs) like PDA's and cellular phones have a limited computational power with reduced capabilities for data processing, data storage and data communications. However, the information stored in a LMD is most of the time confidential and very valuable for its owner. In a distance collaboration framework, mobile devices may play an important role providing or getting information to/from servers where large amount of information is stored.

Security is a big issue for LMDs. However, due to power and memory limitations typically found in such devices, security implementations cannot expect to have extensive computation on the network's nodes. Hence, the computational complexity of the algorithms that can be executed by these devices is rather limited. Therefore, to integrate mobile devices to a secure distance collaboration system, it is necessary to develop simple but robust protocols for secure access. Another important issue on mobile devices is related to failures and fault tolerance. Mobile devices are typically exposed to very noisy and hostile

environments in which failures are quite common. Whenever a mobile device needs to access collaboration information from a server, it is quite desirable to have an environment capable of recovering from potential failures and/or communication disruptions. Thus, it is necessary to provide a robust storage system for mobile users where these kinds of faults can be largely tolerated.
A third big issue in mobile devices is associated to the mobility itself. While in the case of a wired user information is accessed via fixed and well-behaved access control points; a mobile user on the contrary may change access points almost constantly while in movement. Consequently, a collaboration system for mobile users must provide persistent environments for information access requests. To achieve that, mobile user state descriptors must be communicated among different access points to keep an accurate and update state of the transactions done by each one of them.

2.3 Research work

In this project we would like to design and implement a persistent storage system on the top-layer of the secure information sharing for distance collaboration system. The main idea to be developed by our team is to create an environment where a given user connected to our system via a wireless device, can access data as it were located in a local server. Our system will deal with proxy servers to consider control version, shared access and security issues. In addition, our system must also be robust against potential communication failures in order to minimize risks of information lost. The main goal is therefore to extent the distance collaboration capabilities to the mobile-user wireless context.

Two key aspects of the above problem are considered in this project:

- Hardware/software configurations for LMD, and
- Shared data access protocols for LMD.

In the following we will describe in more detail each one of these issues.

2.3.1 Hardware/Software configurations for LMD

Given speed and security requirements of LMDs, it is necessary that several functions, traditionally software implemented, be hardware implemented. LMDs are a special case of embedded systems in which various hardware and software components interact with the others. In addition, given the personal use of LMD's, many applications require to be customized for specific necessities of a user.

Hardware/software systems include a combination of programmable circuits and software components to perform a special task [Zhang02]. Software is being used for flexibility and it employs a general purpose processor. However, in LMDs it is necessary to have reasonable speed of computation with lower energy consumption; both characteristics are not often found in pure software components. Therefore, hardware components are used when speed and energy conservations are critical. The most important challenge in LMDs is to find an adequate balance between hardware and software [Lange02, Benini02].

Field-Programmable Gate Arrays (FPGA's) have the capability of building prototypes at reasonable cost and time. Their major advantage over previous technologies is based in two main features: high density available and re-configurability. Modern FPGAs include up to two millions gates for re-configurability, which allows to implement sophisticated functions. Not all applications are well suited for FPGA implementation. Those in which benefits usage of FPGAs has proven to be advantageous include: non-standard word-length arithmetic applications, logic and integer arithmetic applications with strong emphasis in bit-level operations and systolic processing applications [Diaz98,Barat02].

Sharing large multimedia documents (such as text, images, graphs, sound and video) with LMDs requires high efficient compression/decompression techniques. For example, image transmission to an LMD must be done considering LMD display resolution and communication speed. Speed and efficiency requirements of LMDs demand high-performance signal compression/decompression (codec) algorithms to reduce communication needs [Braun02].

For security purposes, it is necessary to have secure and efficient cryptographic algorithms in place. Since their computation requirements are normally prohibited high, we are forced to implement most of them on hardware. Implementing such algorithms on FPGAs, allows us to customize each cryptographic

algorithm to different user necessities [Goodman02]. Signal compression and data encryption are applications well suited for FPGA implementations. Both of them use non-standard word lengths, most of the computational time is consumed in bit-level operations and they require to perform as efficiently as possible according to LMD computing capabilities.

Research Methodology.

We pretend to study hardware/software architectures and circuit synthesis tools to build signal compression applications for LMDs. Designing hardware/software applications is not simple, since it is necessary to identify software and hardware components and inevitable interfaces in which interaction between hardware and software perform adequately, efficiently and coupled [Barat02,Rama02]. In addition, circuit synthesis tools are needed to map circuits from behavioral (high-level) descriptions onto FPGA devices [Weber01].

We pretend to achieve the following goals **(GOAL 2)**:

2.1. A research report on typical architectures for signal compression in LMDs.
2.2. Algorithm design and implementation for lossless signal compression based on Reed-Solomon codes.
2.3. A research report about hardware/software architectures for cryptography.
2.4. Hardware/software design and implementation for the AES algorithm.

2.3.2 Shared data access protocols for LMDs

LMDs have very limited storage capabilities. However, information stored in a LMD is usually confidential and of great value for a user. Because of its size, a LMD is subject to damage and lost, therefore, information lost can be very meaningful to its owner. For those reasons it is convenient to take previsions by considering transparent information backups. That means the possibility to keep information stored in safe places without user actions. On the other hand, it is also important to overcome the limitation on LMD's storage capabilities by providing a transparent storage extension.
In this project we would like to design and implement a persistent storage system on the top-layer of the secure information sharing for distance collaboration system. The main idea to be developed by our team is to create an environment where a given user connected to our system via a wireless device, can access data as it were located in a local server. Our system will deal with proxy servers to consider control version, shared access and security issues. In addition, our system must also be robust against potential communication failures in order to minimize risks of information lost. The main goal is therefore to extent the distance collaboration capabilities to the mobile-user wireless context.

There are some systems for stable distributed storage [Lee99, Rhea01, Yiani01]; they are connection oriented and require users to be closed to a server. We seek that a user with a LMD can access a distributed file system in a transparent way. The user must see a file as it were located in its LMD memory. The system will face all the communication and storage operations to handle a memory hierarchy with the LMD, near file server and remote server's memories as the main participant entities.

The system must consider also file replication, migration and diffusion. Taking into account the infrastructure of this project, the system will consider also document version control.

Research Methodology.

The following goals are going to be considered in this part of the project:

2.5. A communication protocol for a LMD and an associated distributed file system. It is necessary to consider file replication, migration, diffusion and control version.
2.6. A hierarchy memory system for a LMD with pre-fetching to avoid unnecessary delays. Some replacement data policies will be addressed.
2.7. Security issues of a distributed file system for a LMD.

2.4 Expected Results

Techniques, algoritmos, protypes and papers

1. A generic hardware/software architecture for encrypting information.
2. A generic hardware/software architecture for signal compresion
3. A memory hierarchy model for light mobile devices.
4. A communication protocol for a distributed file system and light mobile devices.

(At least one referreed international conference paper is considered for each result)

Graduated students

1. Hardware/software implementation for DES algorithm. Mizael Sánchez Santiago. Master program.
2. Hardware/software architectures for encryption. Nazar Abbas Saquib. PhD Program.
3. Hardware/software architectures for multimedia signal compression in light mobile devices. Esteban Torres León. Ph. D. Program (to initate in Sep. 03).
4. Two more graduated students considering the stable distributed file system.

3. Secure Information Sharing for Distance Collaboration

Researchers: Dr. Ana Martinez (CINVESTAV-IPN), Jesus Favela (CICESE, Mexico)

3.1. Abstract.

Groupware, or computer tools that support collaborative work have benefited from recent advances in computer and telecommunication technology. The research agenda in this field of research includes the development of software infrastructures that support ubiquitous access to shared resources and which allow for opportunistic interactions. When collaboration crosses organizational, cultural, and/or political borders secure information access becomes a primer concern during collaboration, since partners might still trust the colleagues with whom they collaborate, but not necessarily the security of their information systems. As part of this project we propose to take advantage of TAMU's know-how on the design of secure information servers to provide security guarantees to the PINAS, web-based replicated collaborative framework, on which he have been working in the last few years. To illustrate the application of the solutions being proposed, we will also develop two secure collaborative applications using this framework: one for the collaborative authoring of documents and a second one for the support of collaborative software development.

3.2. Introduction

In recent years, Computer Supported Collaborative Work (CSCW) has emerged as a result of the convergence of computing and telecommunications systems. CSCW's main research thrust is not only aimed at understanding how people produce joint work, but also to design and build appropriate computational tools to support this activity, particularly when participants are geographically distributed, or work at different times.

Security is a necessary concern to be taken into account in the design and development of robust collaborative systems under real conditions. There are many circumstances that demand information to be shared in organizations (or individuals that collaborate) and that need to maintain restricted access to information. Sharing information should not jeopardize the organization's security. How to balance the risks and advantages associated with collaboration is an open research issue that will be addressed in this project. As part of this project we seek to take advantage of TAMU's know-how on the development of secure information servers. The combined expertise of CINVESTAV and CICESE in the design and development of groupware, with that of TAMU on issues of security in information systems will allow us to propose alternatives for the design of secure collaborative systems.

3.3. Related work

Large-scale software development can be a collaborative activity requiring the interaction of specialists from different fields. These specialists need to communicate their decisions and coordinate their activities for the project to succeed. One of the main trends in software development has been the globalization of the software industry [Herbsleb01]. Frequently, software developers are required to work in groups that are geographically distributed and there has been considerable recent attention to the development of tools to support collaborative software development.

The collaborative systems group in CICESE has done extensive research in this area [Favela99]. In particular, we conducted a 3-year study of a distributed software engineering course with the participation of students from CICESE and MIT with support from a previous NSF/CONACYT grant (No. C024-A). In the courses conducted during this period all participants collaborated in the development of a software system using groupware tools developed in both institutions [Favela01b]. Professors Ana Martinez (CINVESTAV) and Jesus Favela (CICESE) together with Dr. Dominique Decouchant from LSR-IMAG, France have worked in the development of a framework to support collaboration activities on the Web: PIÑAS (Platform for Interaction Naming And Storage) [Decouchant, 2001] [Morán, 2002]. As part of this work we have dealt with issues of robustness, consistency, resource naming, user authentication, and resource replication. This on top of an ubiquitous information sharing infrastructure (the WWW) that was not originally designed to support collaborative, distributed work.

At the heart of the design of PIÑAS is the unreliability of the WWW to store shared resources that are accessed from distant sites. The approach of PIÑAS to address reliability is based on the idea of replicating resources on web servers that are local to the user. This replicated architecture not only increases the robustness of the system, but also provides support for nomadic users, since copies of their documents will be available in all sites where they normally work.

Our group has also done work in the field of mobile collaborative applications. On the one hand, the PIÑAS middleware supports nomadic work by providing ubiquitous access to resources stored in its servers. Additionally, we have been working on supporting opportunistic interactions by mobile users working in personal digital assistants [Favela02]. The development of applications on top of PIÑAS middleware have focused in the field of collaborative authoring, one of the most important areas of application in groupware, and one in which our groups had previous expertise [Decouchant99, Favela01]. More recently, we have developed two applications that work on top of our PIÑAS framework: AllianceWeb and COOPER. The AllianceWeb cooperative editor is developed on top of PIÑAS (Platform for Interaction, Naming And Storage) to provide support for cooperative authoring on the Web. COOPER is a collaborative authoring tool that supports distributed pair programming on the web [Natsu, 2003] The COPPER synchronous source code editor has its origins in this previous experience and the collaboration technology designed as part of the PIÑAS project. The tool allows two distributed software engineers to write a program using the pair programming technique. COPPER uses and implements characteristics of groupware systems such as communication mechanisms, collaboration awareness, concurrency control, and a radar view of the documents, among others. It also incorporates a document presence module, which extends the functionality of instant message and presence awareness systems to allow users to register documents from a Web server and interact with them in a similar fashion as they do with a colleague [Moran01].

3.4. Research work

Our plan in this project is to extend the PIÑAS middleware to support the development of secure collaborative applications for users connected to the Internet through mobile or fixed devices, so that they can access shared information and collaborate. We will study security issues related to the access, sharing, replication and update of information related to the support of mobile users.

In this project we are interested in addressing the following security issues in our PIÑAS framework:

- Privacy and confidentiality.
- Recovery of data from the analysis historical records: tracking actions (what actions and when they occurred) which cause loss of data and the corresponding recovery of some or the total contents of data.

In general the goal for this research is to combine the expertise of CINVESTAV and CICESE in the design and development of groupware, with that of TAMU on issues of security in information systems, to allow us to propose alternatives for the design of secure collaborative systems.
Specifically, the goals **(GOAL 3**) for this project are the following:

3.1. The establishment of the security requirements of the PIÑAS middleware in the server side and comparing them with the technical solutions proposed by TAMU
3.2. The incorporation of the security considerations in the PIÑAS middleware based on the solutions proposed by the TAMU team
3.3. Extending the PIÑAS middleware to support mobile users working on handheld devices and PDA's.

3.4. Adaptation of the COPPER pair programming tool to incorporate secure access to shared source code repositories.
3.5. Testing the distributed pair-programming tool on top of TAMU's secure server with students from the participating institutions working in collaborative programming exercises.

3.5. Research Methodology.

On a first stage we will establish de security requirements for a collaborative infrastructure. To accomplish this task we will first generate use scenarios based on realistic conditions or actual cases. These scenarios will be analyzed from the point of view of the security risks associated with them, clearly identifying the sources of those risks. No mitigation approaches will be proposed at this stage. We expect to use an early version of the Software Security Assessment Model being proposed as part of this work, both to help identify the risk requirements and as an early validation of the model.

Once the security constraints of the collaborative applications supporting the scenarios are identified, we will distinguish between those risks that are associated to the collaborative infrastructure, and those that are related to the application itself and have to be dealt with at a higher level of abstraction. We will concentrate on the former, since we are interested in making these security provisions at the level of the PIÑAS middleware.

At this point we will carefully evaluate the work being done by Prof. Steve Liu and his group at TAMU related to secure servers and non-repudiation of transactions. We will compare our technical requirements to the solutions proposed by them. This exercise will allow us, on the one hand, to design appropriate mechanisms for secure collaboration for our middleware, and on the other, to present new security problems to be tackled by the group in TAMU.

The security requirements identified in the previous stage will be taken in consideration for the redesign of PIÑAS. In this stage we will need to make a careful balance to make sure that the services provided by the infrastructure are not jeopardize during the redesign. Once our design is complete, we will proceed with its implementation and evaluation with development prototypes of collaborative applications.

Our work will be validated with the implementation of prototypes and experiments carried out on the secure server test-bed developed by TAMU. We will start by experimenting with the PIÑAS middleware on top of the secure server. Additionally, we will work in the development of distributed collaborative applications working securely on the Web. In particular, a collaborative editor currently under development (AllianceWeb) and a collaborative tool to support pair programming (COPER).

It is clear that the support of these applications demand security requirements to share resources, documents and code from different sites on the networking system proposed (Figure 1).

To perform the evaluation, a Mexican doctoral student will visit TAMU to install the applications on their infrastructure and perform test with other students working in CINVESTAV and CICESE.

3.6. Expected Results

Prototypes

At the end of the project we will deliver a prototype of at least one collaborative application working on top of the secure server.

Human Resources

Three graduate students will be directly involved in this part of the project:

- Moisés González García (a PhD student of the Computer Science Section of CINVESTAV-IPN, Mexico), who works in the organization and integration principles for the cooperative software processes.
- Natsu, Hiroshi (a PhD student of the Computer Science of CICESE, Ensenada), who works on distributed pair programming.
- Rolando Menchaca (a PhD student from CIC-IPN), who works in cooperative work.

Publications

One conference and one journal paper

4. Software Security Assessment Models.

Researcher: Dr. Pedro Mejia Alvarez. (CINVESTAV-IPN)

4.1 Introduction.

It is our aim to develop software security assessment models and methods to support the development of information systems in a networked environment. Specifically, we will relate our study to the development of Distributed Collaborative Information Systems.

Modern society and modern economies rely on infrastructures for communication, finance, energy distribution or transportation. These infrastructures depend increasingly on networked information systems. Attacks against these systems can threaten the security, or the economical or even the well being of people and organizations. Almost every networking software system deployed today must defend itself from malicious adversaries. Information Systems in modern countries, like USA and Mexico, are critically dependent on a wide range of networking software systems. Their need to exchange information and to develop and operate shared networking equipment and software demand that software engineers be cognizant of security threats from potential adversaries with credible defenses, while still delivering value to costumers. With the advent of the Internet, and increasing reliance on packet switching networks for e-commerce, distant collaboration, telecommuting, etc., the risk from malicious attacks are increasing, therefore, software systems designers must think not only of users, but also of adversaries.

Threats from a networking security breach could range from the very mild (such as defeat of copy protection in the access to the Information System) to the disastrous (such as malicious intrusion to the information system). Security vulnerabilities in networked information systems may arise from poor software development practices, unconsidered modes of attacks, unsecured links between systems, or miss-configurations [Pipkin00].

Developing secure software systems is difficult and error-prone. There are many causes of this difficulty [Pipkin00]. First, security requirements are intrinsically subtle, because they have to take into account interaction of the system with motivated adversaries that act independently. Thus some security mechanisms, for example security protocols, are notoriously hard to design correctly, even for experts. The increasing complexity of this software systems and the fact that parts of this systems are built on COTS components [Sommerville01] or rely on Legacy Systems [Sommerville01] further complicate the design of secure software systems, because software developers now face with the risk of constructing systems in continuous change and sometimes made out of unknown black boxes. Second, risks are very hard to calculate because of the unpredictable nature of failures and attacks to the system and because of a positive reinforcement in the failure occurrence rates over repeated system executions: security-critical systems are characterized by the fact that the occurrence of a failure (that is, a successful attack) at one system execution dramatically increases the likelihood that the failure will occur at any following execution of a system with the same part of the design. Thirdly, many problems with security-critical systems arise from the fact that their developers, who employ security mechanisms, do not always have a

strong background in computer security. This is problematic since in practice, security is compromised most often not by breaking dedicated mechanisms such as encryption or security protocols, but by exploiting weaknesses in the way they are being used [Anderson01]. Lastly, while functional requirements are generally analyzed carefully in systems development, security considerations often arise after the fact. Adding security as an afterthought often leads to problems [Anderson01]. Also, security engineers get little feedback about the secure functioning of the developments in practice, since security violations are often kept secret in fear of harm for a company's reputation. Ad hoc development has lead to many deployed systems that do not satisfy relevant security requirements. Thus a sound methodology supporting secure software systems development is needed.

For secure software systems, every phase of the software development cycle (from requirements engineering to design, implementation, testing and deployment) must include security-aware validation and risk assessment capabilities. Software developers of secure networked information systems face great challenges nowadays because currently there is a lack of security assessment models and tools for use in the software development and maintenance cycle that help to mitigate the discussed software vulnerabilities [Pikin00, Guilliam01].

4.2. Research Work.

On the basis of our framework, our specific goals in this joint project include:

- **Unification of Security and Software Models**. Specifically, the approach that we will follow will be based on adopting and extending the UML Object Oriented Model [Booch99] in the requirement specification/analysis and design phases to include modeling of security features such as privacy, integrity, secure information flow, access control, reliability, and secure communication link.
- **Construction of Software Systems with Evolvable Security Features.** We will use *aspect oriented programming* [Kiczales97] to isolate pieces of software located in different parts of a distributed system for their development and maintenance. Also, we will use architectural *components* and *connectors* [Clements03] to address security concerns such as authentication and access control, together with on-line monitoring and maintenance.

4.2.1 Unification of Security and Software Models.

Attention to quality on the early life-cycle development phases of a project (e.g., requirements and design) lead to defect detection and avoidance. It is well known that such defects, if undetected, can propagate downstream to the software product, where the cost of detection and removal are greatly amplified. The trend in must recent research studies suggest the use of high level, object oriented models (such as UML [Booch99]) early in the life cycle to support requirements analysis and design activities [Kiczales97]. So far, however, security issues have been treated separately or added after the development of the requirements specification and design. Also, there has been a lack of interaction between researchers working on requirements modeling and analysis and design (e.g., in the UML community) and security engineering researchers.

It is clear for us that development of this unifying approach in this project will provide developers of networked information systems with several advantages: (a) unified design of software systems and security policies, (b) modularity (through encapsulation) compactness and reuse, and (c) leverage of existing standards-based tools for design and analysis (forward engineering) as well as for analysis of legacy code (reverse engineering) activities.

Research Methodology.

A **primary challenge in this goal of our project** is to extend the syntax and semantics of the standard UML to address security concerns. In our knowledge, no research efforts have been dedicated to this line of research. It is our aim to develop tools and processes to help unify the design of secure networked information systems. In what follows, we will describe the security modeling requirements which will be included into our secure networked information system, and the diagrams of UML to be used in our project for describing object-oriented software systems.

The **security requirements** to be considered in our networked information system and which will be encapsulated in UML are the following:

- **Fair exchange**. This requirement postulates that, when information or goods are traded electronically, the trade is performed in a way that prevents both parties from cheating.
- **Secrecy/confidentiality**. One of the main information security requirements is secrecy (or confidentiality), meaning that only legitimate parties will know some information.
- **Secure information flow**. We will model security aspects in networked information systems where some degree of interaction between parties is always achieved. In this type of systems messages (or information) will be frequently shared between different parties around the network. This information will be intercepted, modified or deleted. Sometimes even a partial leakage of information must be by all means prevented. The notion of secure information flow ensures that where trusted parts of a distributed system interact with untrusted parts, there is not eve a partial leakage of secret information from the trusted to the untrusted part.
- **Secure communication links.** This requirement ensures that the physical communication links between different parts of the system give the required security guarantee regarding a given adversary model. For example, our networked information system will provide secure links against outside attackers.

UML consists of different types of diagrams describing views of a software system. Our goal is to design and develop an extension of UML to provide security requirements for networked information systems. We will concentrate on the following important diagrams of UML for describing object-oriented software systems.

- **Class Diagrams** define the static structure of the system. They define classes with attributes and operations (or signals) and relationships between the classes. We will use the class diagrams to ensure that exchange of information obeys security levels. To specify different security levels we will use the UML extension of a *tag*.
- **Statecharts Diagrams** give the dynamic behavior of an individual object. They help on the definition of events that cause state in change or actions. We will use them to prevent the alteration of values within an object from indirect information flows.
- **Interaction diagrams** describe interactions between objects via message exchange. We will use sequence diagrams to ensure correctness of security-critical interaction between objects (especially for the type of networked information system which form the basis of this project, see Figure 1). We will use them to ensure secure information flow.
- **Deployment diagrams** model the hardware used in implementing a system and the association between those hardware components. Components can also be shown on a Deployment diagram to show the location of their deployment. Deployment diagrams can also be used early on in the design phase to document the physical architecture of a system. Since security of a software system depends on the security of the underlying physical layer, deployments diagrams will be used to ensure that security requirements on communications are met by the physical layer.

The following goals **(GOAL 4)** are going to be considered in this part of the project:

4.1. Research on related work on UML and Security.
4.2. Definition and evaluation of the syntax used in UML for Class Models.
4.3. Development and evaluation of syntax rules of UML state Charts with security requirements
4.4. Evaluation of Sequence diagrams and Collaboration diagrams for security.
4.5. Include security requirements into Interaction diagrams.
4.6. Include security requirements into Deployment diagrams.
4.7. Development of a Tool that includes security Requirements in UML Diagrams.
4.8. Evaluate and Test case examples to introduce security into our Distributed Information System.

4.2.2. Construction of Software Systems with Evolvable Security Features.

Software designers have long recognized the need to incorporate non-functional considerations such as performance and security into software design processes. Nowadays, it is well understood that adding performance and security features after the design of software architectures may be difficult, too costly, and sometimes poorly effective.

Very few research works has been dedicated to include security features into the design of software architectures, and very often, security is included to pre-existing software systems (*legacy system*s), which leads to difficult challenges in the design of security enforcement mechanisms and for the re-design of the rest of the system. The novel solution proposed in this project is to refine the requirements and design processes to include security aspects in earlier development phases of systems that include legacy systems.

Research Methodology.

The **central problem** in modifying the security aspects of a legacy system is the difficulty of identifying the code that is relevant to security, changing it, and integrating it back into the systems. Our approach on solving this problem is based on the idea of designing software systems with *evolvable security features*. This line of research proposed in this project for including security features in legacy systems, will consist on the novel idea of integrating two software design methodologies: *Aspect Oriented Programming* [Kiczales97] and *Architectural Connectors* [Clements03].

Aspect oriented programming is an approach useful in simplifying software evolution. The idea is that some aspects of the code are naturally modular, such as data storage, which can be places into a database. Other aspects (usually non-functional requirements) such as functionality or security are scattered throughout the code. Identifying and changing security features of a legacy software system would involve the difficult tasks of location of the code, connection of the piece of code with the rest of the system, and functionality modifications due to the changes. Aspect oriented programming seek to isolate centrally the pieces of software located in different parts of the software system, with the purpose of facilitating its developing and maintenance. The task of re-scattering them back into the code prior to compilation is automated using program transformations called *aspect weavers*.

The other design methodology proposed to solve this problem arises in software architecture [3], where the most recent research has been based on the study of two mayor elements of the architecture: *components*, which form the centers of computation in the system and *connectors*, which are the loci of interaction between components. This conceptual elements of the architecture are design level elements.
Security features to be considered in this project such as authentication and access control, arise out of interactions between components, and can be considered into a software design by the use of architectural connectors. Thus security concerns are closely related with architectural connectors. Authentication, security policies, and enforcement mechanisms could be considered as different aspect of connectors. The roll of the *aspect weavers* in this project will be that of integrating these connectors with the rest of the system. In this context, security features would be easier to isolate and maintain.

The following goals are going to be considered in this part of the project:

4.9. Research in aspect oriented programming and software architecture.
4.10. Introduction of security requirements into the architecture of our distributed collaborative information systems using aspect programming.
4.11. Introduction of security requirements into the architecture of a software system using components, connectors, and aspect weavers.

4.3 Expected Results (Deliverables).

Techniques, Algorithms and Protypes.

- Software Tool that extends UML modelling lenguaje to include security aspects.
- New techniques for including security into software architectures.

Papers.

- 2 papers in International Conferences.
- 1 paper in Journal.

Graduated students

- MsC: Student: Juan Carlos Medina: Integration of Security Requirement in to UML Modelling Lenguaje.

- Msc Sudent: Leticia Davila: High Security Software Arquitectures. This student is expected to graduate in July 2003, and will enroll in our PhD Program.

5. High Performance Cryptographic Schemes for Secure Communication.

Researcher: Dr. Francisco Rodriguez (CINVESTAV-IPN)

5.1. Introduction.

During the last few years we have seen formidable advances in digital and mobile communication technologies such as cordless and cellular telephones, personal communication systems, Internet connection expansion, etc. On the other hand, with the advent of various radio access technologies, the deployment of sophisticated applications in network systems has been increased dramatically. In the foreseeable future, multimedia applications appear to be the most dominant network applications for both, wired and wireless networks. This has posed a set of unprecedented technical challenges, particularly within the context of mobile computing. Among those challenges, two of the most important ones are how to design/implement efficient Quality of Service (QoS) mechanisms and how to obtain reliable security services.

Wireless local area networks (WLANs) are generally characterized as high-speed wireless systems covering relatively small areas compared to other wireless systems such as cellular, PCs, and mobile data radio systems. WLANs are emerging as an attractive or complementary alternative to wired LANs because of several reasons. For instance, WLANs allow us to set up and reconfigure a given network system in an easy way, without incurring into the cost of wiring. Additionally, and undoubtedly even more significantly, WLANs have paved the way for ubiquitous pervasive computing, which is now poised to revolutionize people's style of life [Chandra02,Gast02]. Consequently, Security and QoS have already become one of the most critical network services in today's inter-networked world. Security mechanisms allow the presence of network services such as: User-proof of identity, information confidentiality and integrity, network's entities authentication and so on. More specifically, the techniques for the implementation of secure information handling and management are provided by cryptography, which can be succinctly defined as the study of how to establish secure communication in an adversarial environment. On the other hand, QoS mechanisms provide to system's users and/or applications an efficient access to network services and resources.

5.2. Related Work.

Efficiency and secrecy are two natural but contradicting goals in cryptography. Before the late seventies, all cryptographic systems designed by researchers were based on a secret key, needed to encrypt and to decrypt the information. In all these schemes, called symmetric or secret-key cryptosystems, it is assumed that the communicating parties are the only ones who have access to the secret key. Such methods implement symmetric encryption/decryption schemes, which contrast with the methods used in public-key cryptography, that were first proposed in the work of Diffie and Hellman in 1976. The Diffie-Hellman protocol allows two parties to agree on a shared, secret key, even though, they can only exchange messages in public. Shortly after them, Rivest, Shamir, and Adleman proposed the RSA cryptosystem in 1978. Today, RSA is one of the most widely known public-key systems. In the public-key paradigm, each party has a pair of keys, one secret and one public, and the encryption/decryption process is not symmetric anymore.

Network security service can be defined as the ability of a system to manage, protect, and distribute sensitive information. Usual security services include but are not exclusive to: authentication, access control, confidentiality, integrity and non-repudiation.

All the above named security services can be achieved by means of public key cryptographic systems combined with private or symmetric cryptographic ciphers. That can be accomplished by assigning to each entity in the network a unique private/public key pair. During communication, each entity on a server-client or peer-to-peer communication may be authenticated by using public key mechanisms (such as signature/verification and authentication schemes) together with well known key exchange protocols

(such as Diffie-Hellman, SSL/TLS handshaking protocol, etc). Integrity and non-repudiation can be obtained by signing/verifying all the messages transmitted between the entities under communication. Finally, in order to obtain confidentiality, network's entities may encrypt their relevant information using a random session key and a symmetric cryptographic algorithm such as the Advanced Encryption Standard (AES) for block ciphers and RC4 or A5 for stream ciphers. Several cryptosystems at different key strengths can be used in such exchange protocols.

In this project we will study three main relevant aspects related to today's modern security systems: Symmetric ciphers, public key cryptosystems and security services and quality of service in WLANs. In the rest of this section we present a more detailed discussion of these three aspects.

5.2.1. Symmetric Ciphers: The advanced Encryption Standard (AES)

In October, 2000, Rijndael block cipher algorithm was chosen by NIST as the new Advanced Encryption Standard (AES) [Daemen02]. Rijndael is a block cipher that can process blocks of 128, 192 and 256 bits and keys of the same lengths. Due to its enhanced security level, it is expected to replace in the near future DES and Triple DES in a wide range of applications [Daemen02]. There exist several reported implementations of AES in software, VLSI and on FPGA devices with variable performance results. Reported software implementations in which AES specification is manipulated to increase performance can be found in [Gladman01,Bertoni02]. Software implementations have a throughput that ranges from 300 to 800 Mbps depending on the specific architecture and platform selected by the designers.

AES hardware implementation poses a challenge since encryption and decryption processes are not completely symmetrical [Chandra02]. Some efficient AES encryptor/decryptor core VLSI implementations have been reported [Ichikawa00,Rudra01]. Achieved performance of VLSI implementations ranges from 2 to 7.5 Gbits/s.

On the other hand, FPGA implementations are attractive since costs of VLSI design and fabrication can be reduced. However, the asymmetric characteristics of AES encryption and decryption processes limit the implementation of high-performance AES cores, since the design of separated architectures for encryption and decryption processes would imply the allocation of a large amount of FPGA resources. Moreover, the area requirements of such design might be even impossible or difficult to meet in several FPGA families of devices. Partially because of this reason, designs reported by [Gaj00, Elbirt00,Saqiba03] have considered only the encryption part of AES. Only in [Mcloone,Saqibb03,Saqibc03] is reported an FPGA implementation of a full encryptor/decryptor AES core.

5.2.2 Public Key Cryptography

The security of currently used public key cryptosystems is based on the computational complexity of an underlying mathematical problem, such as factoring large numbers or computing discrete logarithms for large numbers. These problems are believed to be very hard to solve. In practice, only a small number of mathematical structures could so far be applied to build public-key mechanisms. When an elliptic curve is defined over a finite field, the points on the curve form an Abelian group. In particular, the discrete logarithm problem in this group is believed to be an extremely hard mathematical problem. Other well-know public cryptosystems are the Digital Signature Algorithm (DSA) [standard97] and the RSA cryptosystem [pkcs02].

High performance implementations of all those three cryptosystems depend significantly on the efficiency in the computation of the finite field arithmetic operations. Finite field arithmetic is the main mathematical tool needed for the implementation of these cryptosystems' primitives. In [Rodriguez00,Savas01] a high-performance software crypto-library was developed, while in [Rodriguez03,Rodriguez03a] efficient algorithms for implementing finite field arithmetic are reported. That library develops the three public key cryptosystems mentioned above with state of the art performance improving techniques.

5.2.3 Security Services and Quality of Service in WLANs

Security design on a wireless network needs to consider a number of issues that do not necessarily show up on wired networks. Bandwidth is perhaps the most important issue in wireless networks due to the

limited spectrum available for communication. This limitation extends itself to security. Security implementations in wireless networks should keep to a minimum the amount of control data they exchange. Due to the power and memory limitations typically found in mobile devices, security implementations cannot expect to have extensive computation on the network's nodes. This reduces the computational complexity of the algorithms that can be executed by the nodes.

Quality of Service (QoS) is the ability of a network element (e.g. an application, a host or a router) to provide some levels of assurance for consistent network data delivery [Ni]. The main metrics or constraints usually mentioned for QoS are: Time delay, time delay variation and data rate. The time delay constraint requires that data will arrive within a predefined critical time. The time delay variation requires that the time delay will be within certain bounds. The data rate specifies the bandwidth required to properly support the application. Inherently, QoS involves user requests for levels of services which are related to performance-sensitive variables in an underlying distributed system. Some examples of security variables suitable to become part of a quality of security service are: selection of different symmetric cryptographic algorithms using a variable number of rounds at different bit-lengths; variable of the user authentication mechanisms; selective percentage of authenticated packets, etc.

From these examples, it is apparent that the notion of security ranges is useful and thus, we can conclude that it is reasonable to consider such ranges within the context of a QoS manager.

5.3. Research Work.

5.3.1 Research Question or Problem Statement

The vast majority of digital information used in modern digital applications is stored and also processed within a computer system, and then transferred between computers via fiber optic, satellite systems, and/or Internet. In these scenarios, secure information transmission and storage has a paramount importance in the emerging international information infrastructure, especially, for supporting electronic secure transactions, share of information among distant parties and other security related services.

In this project we will study, analyze and evaluate some of the aspects that more significantly determine the efficiency and reliability of a security system. Due to the relatively high complexity of the problem and the diversity of scenarios involved in current modern applications, our team has divided this research project into three main cases of study: Symmetric ciphers; public key cryptosystems and; security services and quality of service in WLANs.

- For *symmetric ciphers* we are interested in the study, analysis and implementation of complete encryptor/decryptor cores for which encryption, decryption and key scheduling work efficiently. We are particularly interested in high-performance AES FPGA implementations such as the ones developed in [Saqibb03,Saqibc03].

- The study and analysis of hardware and software algorithms suitable for the efficient implementation of *public key cryptosystems* is a second main security aspect to be considered in this project. Particularly, we are interested in the problem of how to implement efficiently in hardware and software, three of the most well-known public key cryptosystems: RSA, DSA and Elliptic curve Cryptosystems used with some of the most common wired and wireless protocols used in the industry.

- In spite of the fact that *Quality of Service* (QoS) and *Security services* are two strongly related requirements of design for Wireless Local Area Networks (WLANs), up to now, very little have been done in order to consider both issues into the same wireless system design: Choices of security mechanisms impact directly the effectiveness of quality of service and vice versa. In this project we will investigate some of the challenges, factors and difficulties that designers need to face in order to combine QoS and Security service into a single implementation. This project will consider the delicate interrelation between security and quality of service mechanisms, quite particularly in the context of wireless systems.

5.3.2. Expected Contributions.

- To develop an analytical performance model for public-key cryptosystem operations used with different key exchange protocols. Different handshake protocols, different cryptosystems and key sizes will be considered in our formulations.

- To implement Public-key cryptosystems in software and/or hardware using state-of-the-art performance improvement techniques, yielding actual performance figures for individual cryptosystems. These figures and the analytical model will be used to calculate the cost of using public-key cryptosystems in different protocol scenarios. Obtained results for different cryptosystems and handshake protocols will be comparatively depicted and interpreted
- Performance of some special classes of elliptic curves will be considered, including Koblitz elliptic curves and Hessian elliptic curves that have proven to be particularly well-suited for high efficient implementations for both, software and hardware designs.

- For symmetric encryption/decryption we will investigate fully pipelined AES architectures for FPGA implementations. The designs to be developed should be efficient in terms of throughput and area requirements, which should be significantly lower than previous reported ones. The increase in performance will be achieved by means of a fully pipelined architecture design, where each block will be carefully designed in order to obtain a reduction in the total number of computations and the path delay associated to them.

- Additional research work for our team will be to explore lightweight public key cryptosystems for heavily constrained environments such as the ones typically found on wireless LANs.

5.3.3. Research Methodology.

In order to develop the tasks and goals that we have proposed for this project, we have a methodology comprises of the following seven phases or goals **(GOAL 5)**:

5.1 Study, analysis and evaluation of existing authentication protocols for both of them, wired and wireless LANs.
5.2 Evaluation of a high-performance software Crypto-library previously developed in [Rodruiguez00, Savas01].
5.3 Design and Software implementation of selected authentication protocols for wired and wireless LANs.
5.4 Evaluation, validation and analysis of high-performance AES FPGA implementations previously developed in [Saqibb03,Saqibc03].
5.5 Efficient lightweight cryptography algorithms devising for heavily constrained wireless environments.
5.6 To develop a test-bed for wireless environments, where we will evaluate the performance achieved by our authentication protocol designs.
5.7 To conduct experiments in the test-bed in order to obtain performance improvement of our cryptographic designs.

5.4 Expected Results (Deliverables).

The expected results of this project will be the implementation, validation and evaluation of each one of the designs specified in section 5.3.3. Moreover, we expect that this project will produce 3-4 M.S. theses and will directly interact with a Ph.D thesis currently in progress. Finally, we estimate that a total of two journal papers and 3-4 conference papers will be generated out of the results to be found in this research. Some of the designs proposed on this project will be fully or partially developed as part of the following graduate theses:

- Ph.D. Thesis: “Hardware/Software Approach for Implementing Cryptographic Algorithms on FPGAs” by Nazar Abbas Saqib (in progress).
- M.S. Thesis: ”Study, Design and Evaluation of Authentication Protocols for Wireless LANs” by Laura Reyes Montiel (in progress).

- M.S. Thesis: “Finite Field Arithmetic for Cryptographic Algorithms” (to start this coming September).
- M.S. Thesis: “Quality of Securite Services for Wireless LANs” (to start this coming September).
- M.S. Thesis: “Efficient Lightweight Cryptography Algorithms for Heavily Constrained wireless Environments” (to start this coming September).

6. Calendar

The activities of this project will last for 2 years, in synchrony with the TAMU project. The project is divided in 6 periods (each period of 4 months).

Quadterm	**Activities**				
	Goal 2 (Arturo Diaz)	**Goal 3** Ana Martinez-Jesus Favela	**Goal 4** Pedro Mejia	**Goal 5** Francisco Rodriguez	**Mexico Team**
1	2.1, 2.2	3.1, 3.4	4.1, 4.9	5.1, 5.2	*Meeting in Mexico City
2	2.3	3.1, 3.4	4.2, 4.3, 4.10	5.3, 5.4	*Visit of Dr. Decouchant to Mexico
3	2.4	3.2, 3.3, 3.4	4.4, 4.5, 4.10	5.3, 5.4, 5.5, 5.6	* Trip to TAMU (PhD Student) for 4 months * Trip to TAMU (Post-Doc Student) 6 Months.
4	2.5	3.2, 3.3, 3.5	4.6, 4.10	5.3, 5.4, 5.5, 5.6	Meeting in Texas A&M
5	2.6	3.2, 3.3, 3.5	4.7, 4.11	5.5, 5.6, 5.7	
6	2.7	3.3, 3.5	4.8, 4.11	5.6, 5.7	Meeting in Ensenada

7. References.

[Anderson01] R. Anderson, “Security Engineering: A guide to Building Dependable Distributed Systems”, Wiley, 2001.

[Barat02] F. Barat, R. Lauwereins and G. Deconick, “Reconfigurable Instruction Set Processors from a Hardware/Software Perspective"', *IEEE Transactions on Software Engineering*, Vol. 28. No. 9. Sep. 2002. pp. 847-862.

[Braun02] F. Braun, J. Lockwood and M. Waldvogel. “Protocol wrappers for layered network packet processing in reconfigurable hardware”, *IEEE Micro*, Jan-Feb. 2002. pp. 66-74.

[Benini02] L. Benini and G. de Micheli. “Networks on chips: A new SoC paradigm”, *IEEE Computer*, Jan. 2002. pp. 70-78.

[Bertoni02] Guido Bertoni et al: Efficient Software Implementation of AES on 32-bits Platforms: CHES2002, LNCS 2523, Springer-Verlag, 2002.

[Elbirt] J. Elbirt, W. Yip, B. Chetwynd and C. Paar: A FPGA implementation and Performance Evaluation of the AES Block Cipher Candidate Algorithm Finalists: The Third AES3 Candidate Conference, 13-14 April 2000, New York.

[Booch99] G. Booch, J. Rumbaugh, I. Jacobson, “The Unified Modeling Language User Guide”, Addison-Wesley, 1999.

[Chandra02] Praphul Chandra: Securing Wireless Links.: A Short History.: White paper, Telogy Networks, Available at: http://www.dolfin.com/sec_wireless.html, July 2002.

[Clements03] P. Clements, R. Kazman, M. Klein, “Evaluating Software Architectures: Methods and Case Studies”, Addison-Wesley, 2001 (2nd edition, 2003).

[Daemen02] Joan Daemen, Vincent Rijmen: The Design of Rijndael, AES-The Advanced Encryption Standard: Springer-Verlag Berlin Heidelberg, New York, 2002.

[Diaz98] Arturo Díaz Pérez. *Hardware Level Description of Dynamic Programming Algorithms*. PhD Thesis, CINVESTAV-IPN, July 1998.

[Decouchant01] Decouchant, D., Favela, J., and Martinez, A., PIÑAS: A Middleware for Web Distributed Cooperative Authoring. In Proc. of the 2001 Symposium on Applications and the Internet: SAINT'2001. IEEE Computer Press, San Diego, CA January 7-12 2001, pp. 187-194.

[Decouchant99] D. Decouchant, A.M. Martinez, and E. Martinez, "AllianceWeb: Cooperative Authoring on the WWW", In Proc. CRIWG'99, Fifth CYTED-RITOS International Workshop on Groupware, IEEE Computer Society, Cancun, Mexico, 15-18 September 1999.

[Favela99] Favela, J., Rodriguez, J., Licea, G., and Garcia, J.A. Collaborative software development over the Internet: Tools and experiences. Computación y Sistemas, July-Sept 1999, Vol. 3, No. 1, pp. 25-37.

[Favela01a] Favela, J., and Ruiz, D.: Collaborative Authoring and Reviewing over the Internet. WebNet Journal: Internet Technologies, Applications & Issues, Vol. 3, No. 3 (2001) 26-34.

[Favela01b] Favela, J. and Peña-Mora, F. An experience in Collaborative Software Engineering Education. IEEE Software. March/April 2001. Pp. 47-53.

[Favela02] Favela, J., Navarro, C., and Rodríguez, M. Supporting Opportunistic Interactions with People and Services in Pervasive Computing Environments. UBICOM'02 Workshop on Spontaneity'02. Gothenburg, Sweden, September 2002.

[Gaj00] K. Gaj, P. Chodowiec: Comparison of the Hardware Performance of the AES Candidates using Reconfigurable Hardware: The Third Advanced Encryption Standard (AES3) Candidate Conference, 13-14 April 2000, New York, USA.

[Garcia03] Mario Alberto García Martínez, Guillermo Morales Luna y Francisco Rodríguez-Henríquez: Descripción con VHDL de un exponenciador para campos finitos $GF(2^m)$: IX Workshop IBERCHIP, IWS-2003, 26-28 de Marzo de 2003, La Habana, Cuba.

[Gast02] Matthew Gast: Wireless LAN Security: A Short History.: Available at: http://www.oreillynet.com/, April 2002.
[Gladman01] Brian Gladman: The AES Algorithm (AES) in C and C++: URL: http://fp.gladman.plus.com/cryptography_technology/rijndael/index.htm, April 2001.
[Gerck 98] E. Gerck, "Toward Real-World Models of Trust: Reliance on Received Information", MCG, The Internet Open Group on Certification and Security (1998).
[Goodman02] J. Goodman and A. P. Chandrakasan. "An energy-efficient reconfigurable public-key cryptography processor", *IEEE Journal of Solid-State Circuits*, Vol. 36, No. 11, Nov. 2001. pp. 1808-1820.
[Herbsleb01] Herbsleb J.D. and D. Moitra.. "Global Software Development". IEEE Software. 2001. 18(2): 16-20 p.

[Ichikawa00] T. Ichikawa, T. Kasuya, M. Matsui: Hardware Evaluation of the AES Finalists: The Third Advanced Encryption Standard (AES3) Candidate Conference, 13-14 April 2000, New York, USA.
[Kiczales97] G. Kiczales, J. Lamping, A. Menhekar, C. Maeda, C.V. Lopes, J.M. Loingtier, J. Iwin, " Aspect-Oriented Programming" In European Conference on Object Oriented Programming (ECOOP), Springer Verlag, LCNS Series No. 1241. 1997.
[Lange02] K. Lange, G. Blanke, and R. Rifaat. "A software solution for chip rate processing in CDMA wireless infrastructure", *IEEE Communications Magazine*, Feb. 2002, pp. 163-167.
[Lee99] Yui-Wah Lee, Kwong-Sak Leung y Mahadev Satayanarayanan. "Operation-based Update Propagation in a Mobile File System", *Proceedings of the USENIX Annual Technical Conference*.
[Moran01] Moran, L., Favela, J., Martínez, A., and Decouchant, D., "Document Presence Notification Services for Collaborative Writing". Proc. of CRIWG'2001. IEEE Computer Press. Darmstadt, Germany, Sept. 6-8, 2001, pp. 125-133.
[Morán02] A. L. Morán, D. Decouchant, J. Favela, A. M. Martínez, B. Gonzalez Beltrán, and S. Mendoza, "PIÑAS: Supporting a Community of Co-Authors on the Web", Distributed Communities on the Web; Edited by: John Plaice, Peter G. Kropf, Peter Schulthess, and Jacob Slonim, LNCS 2468; pp.113-124, Springer Verlag,, April 2002.
[Natsu03] Natsu, H., Favela, J, Morán, A., Decouchanat, D, and Martinez, A.M., Distributed Pair Programming on the Web. Submitted to ENC'03.
[Mcloone01] Maire McLoone and J.V McCanny: High Performance FPGA Rijndael Algorithm Implementations: C. Koc, D. Naccache, and C.paar(Eds): CHES2001, LNCS 2162, pp. 65-76, Springer-Verlag, 2001.
[Ni] Qiang Ni, Lamia Romdhani, Thierry Turletti, and Imad Aad: QoS Issues and Enhancements for IEEE 802.11 Wireless LAN: Technical report available at: http://www.inria.fr/rrrt/rr-4612.html.
[Pipkin00] D. L. Pipkin. "Information Security", Prentice-Hall 2000.
[pkcs02] PKCS #1 - RSA Cryptography Standard: Available at: http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/: Version 2.1, June 2002.
[Raymond00] J.F. Raymond, "Traffic Analysis: Protocols, attacks, design issues and open problems" , In Proc. Workshop on Design Issues in Anonymity and Observability (25-26 July 2000), ICSI TR-00-011, pp-7-26.
[Rudra01] A. Rudra et al: Efficient Rijndael Encryption Implementation with Composed Field Arithmetic: CHES2001, LNCS 2162, pp. 65-76, Springer-Verlag, 2001.
[Salowey00] J. Salowey, "Trust in AAA" Interim meeting Dublin, Authorization, Authentication and Accounting, Architecture research Group (2000). http://www.aaaarch.org/dublin/salowey/aaatrust.html
[Salowey00] O. Berthold, H. Federrath, and M. Kohntopp. "Anonymity and unobservability on the Internet", In Workshop on Freedom and Privacy by Design, 2000.
[Rama02] N. Ramasubramanian, R. Subramanian and S. Pande. "Automatic compilation of loops to exploit parallelism on configurable arithmetic logic units", *IEEE Transaction on Parallel and Distributed Systems*, Vol. 13, No. 1, Jan. 2002. pp. 45-66.
[Rhea01] Sean Rhea *et. al*. "Maintanance-free Global Data Storage", *IEEE Internet Computing*, September-October, 2001, pp. 35--39.
[Rodriguez00] F. Rodríguez-Henríquez: New Algorithms and Architectures for Arithmetic in GF(2m) Suitable for Elliptic Curve Cryptography: Ph.D. Thesis: Department of Electrical & Computer Engineering, Oregon State University, June, 2000.
[Rodriguez03] F. Rodríguez-Henríquez and C. K. Koc: On fully parallel Karatsuba Multipliers for $GF(2^m)$: International Conference on Computer Science and Technology CST 2003, May 19-21, 2003, Cancún, México.
[Rodrigueztocs] F. Rodríguez-Henríquez and C. K. Koc: Parallel Multipliers based on Special Irreducible Pentanomials IEEE Transactions on Computers (to appear).

[Saqiba03] Nazar A. Saqib, Francisco Rodríguez-Henríquez and Arturo Díaz-Pérez: Sequential and Pipelined Architectures for AES Implementation: International Conference on Computer Science and Technology CST 2003, May 19-21, 2003, Cancún, México.
[Saqibb03] Nazar A. Saqib, Francisco Rodríguez-Henríquez and Arturo Díaz-Pérez: A 4 Gbit/s Single-Chip FPGA Implementation of an Encryptor/Decryptor AES Core, submitted to Cryptographic Hardware and Embedded Systems-CHES 2003, Koln, Germany 8-10 September 2003.
[Saqibc03] Nazar A. Saqib, Francisco Rodríguez-Henríquez and Arturo Díaz-Pérez: Two Approaches for a Single-Chip FPGA Implementation of an Encryptor/Decryptor AES Core: 13th International Conference on Field Programmable Logic and Applications, September 1-3, 2003, Lisbon - Portugal.
[Savas01] E. Savas, C. Koc, F. Rodríguez-Henríquez et al: Renewable Cryptography Library Version 1.0: Technical report of the Information Security Lab, Oregon State University, 2001.
[Sommerville01] I. Sommerville, "Software Engineering". 6th Edition. Addison Wesley 2001.
[Strandard97] American National Standard for Financial Services x9.30: Public Key Cryptography For The Financial Services Industry: Part 1: The Digital Signature Algorithm (DSA): X9 - SECRETARIAT AMFRICAN BANKERS ASSOCIATION, 1997.
[Weber01] S. J. Weber, J. M. Paul and D. E. Thomas. "Co-RAM: Combinatiol Logis Synthesis Applied to Software Partitions for Mapping to a Novel Memory Device". *IEEE Transactions on Very Large Scale Integration VLSI Systems*, Vol. 9, No. 6. Dec. 2001. pp. 805-812.
[Yiani01] Peter N. Yianilos y Summet Sobit. "The Evolving Field of Distributed Storage", *IEEE Internet Computing*, September-October, 2001, pp. 35--39.
[Zhang02] T. Zhang, K. Chakrabarty and R. B. Fair. "Design of reconfigurable composite microsystems based on hardware/software codesign principles", *IEEE Transactions on Computer-Aided Design of Integrated Circuit and Systems*, Vol. 21, No. 8, Aug. 2002. pp. 987-995