6-3-2004

Testing the Greenpass Wireless Security System

Kimberly S. Powell
Dartmouth College

Technical Report TR-2004-512
Department of Computer Science
Dartmouth College

Testing the Greenpass Wireless Security System*

Kimberly Powell

Dartmouth College
Hanover, New Hampshire USA

Submitted to the Department of Computer Science on June 3rd, 2004 in partial fulfillment of the senior honors thesis

_____
Sean Smith

* Concurrent theses [3] [7]explore the implementation of the Greenpass Wireless Security System.

Abstract

Greenpass, developed by Nick Goffee, Sung Hoon Kim, Meiyuan Zhao and John Marchesini under the supervision of Sean Smith and Punch Taylor, is a wireless security solution that implements SPKI/SDSI delegation on top of X.509 keypairs within the EAP-TLS authentication protocol. This system aims to model the decentralized way that authorization flows in real-world enterprise settings and provide a seamless solution that allows for easy access to all resources in the network by both registered users and authorized guests. These goals are achieved through the deployment of a delegation tool, which allows an active entity associated to the organization's network to grant authorization to another entity previously unauthorized to use the network.

This paper describes the testing process of the first prototype for this system. It examines trust and usability issues of the Greenpass Wireless Security System and determines the accuracy of the system's implementation in relation to its objectives. It then addresses the planning and execution of a small-scale demo for this prototype based on the examined issues and makes projections for further tests on a larger scale.

1 Introduction

Wired Local Access Networks (WLANs) have quickly become a standard form of connecting computers in a network. WLANs have prevailed in public areas such as airports and cafes; institutional and business settings, and in the smaller, closed setting of the home. Enterprises and homeowners alike have increasingly chosen this form of connection over its predecessor, the Local Area Networks (LAN), due to the easy installation and the relatively inexpensive alternative that it offers. However, unlike LAN access, securing these networks remains a great concern with very few reliable, clear and flexible solutions. As a result of wide-range access to wireless networks, limiting the persons who can connect proves to be a greater challenge than for location-specific LANs.

The Greenpass wireless security system was developed in response to the need for a flexible solution to this security issue, particularly in large institutions [11]. The software-based solution aims to secure wireless networks from unauthorized access while providing guest access in a seamless and intuitive manner. Designed as a distributed authority system, Greenpass extends the responsibility of authorization to registered users in the network through the process of delegation. The goal of this implementation is to simulate the way that delegation

works in the real world and thus reflect true social networking. As a result of this emphasis, the role of the user as well as the general understanding of the human-computer interaction becomes more significant in establishing security in the network, and analysis of this system's reliability depends on the investigation of these issues.

Once the developers of the Greenpass security system produced a working prototype of their design, the human issues along with the general functionality of the solution had to be examined to determine whether the goals of the system had been met and to predict changes that would ensure fulfillment of the fundamental objectives of the system. **Section 2** examines the Greenpass system's primary features in more depth and provides the framework for the testing process. By analyzing the goals of the security system, I was able to formulate a testing scheme aimed at simulating its practical usage and uncovering any existing flaws or concerns. Questions that were raised included: Does access occur as stipulated by the system's objectives? What limitations are imposed by the protocols implemented in the underlying design? How easy and understandable is the set up and tools? **Section 3** outlines the general guidelines for the areas and levels of testing for the initial demo. Within these guidelines, I also examine the sociological factors of the distributed authority structure of the system as explained in **Section 4**. This section of the study reaches beyond the technical reliability of the system in order to address the human-computer interaction and to determine the users' role in establishing network security in a distributed authority system such as this one.

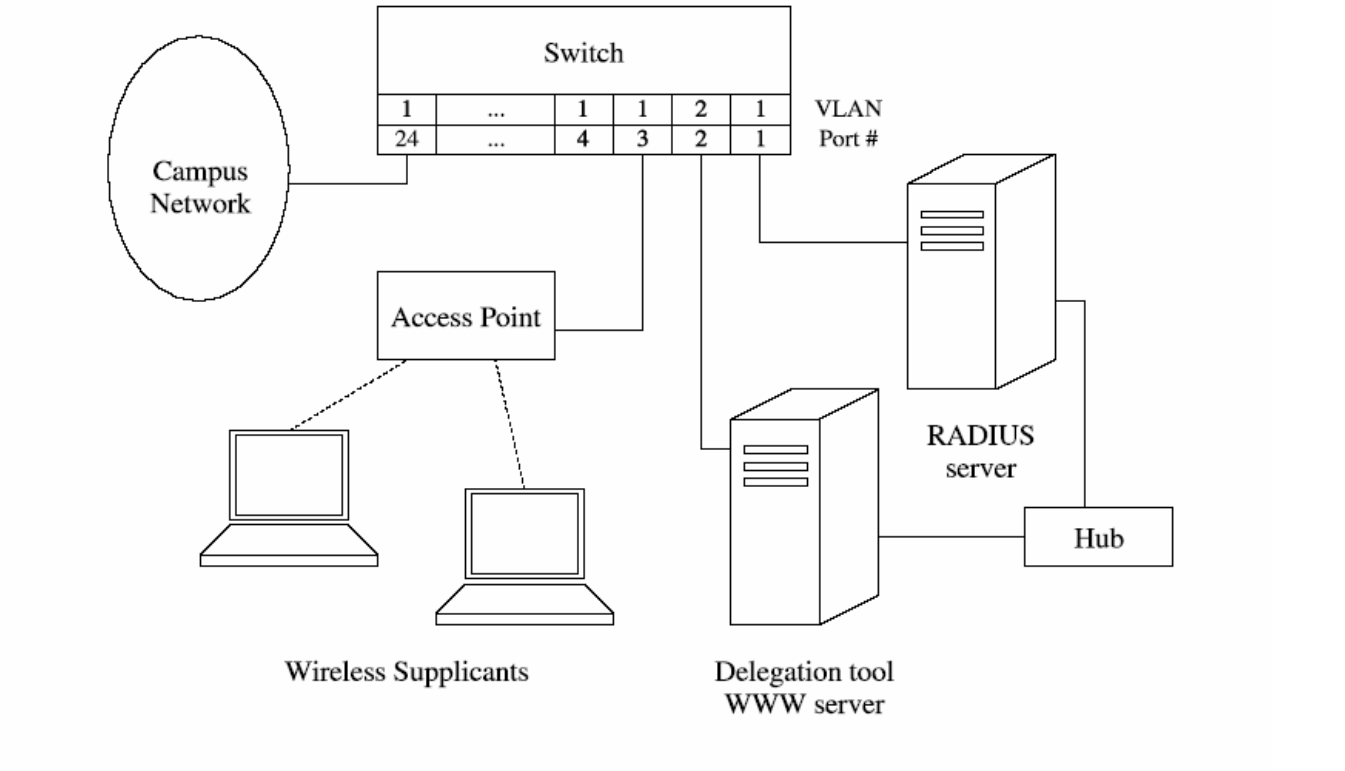
With the guidelines established and the initial analysis completed, we executed the first demo of the system. The implementation of this pilot is explained fully in **Section 5**, with the results and observations detailed in **Section 6**. Using the observations from the pilot, projections for further directions in the testing process are extrapolated in **Section 7.** Lastly, in **Section 8,** I extend the analysis of the system's security by investigating the complexity of related protocol issues and briefly describe future directions for the system and testing.

2 Features of Greenpass

Greenpass was developed using the EAP-TLS authentication protocol which Aboba and Simon fully detail in the RFC for this set of rules [1]. This design combines the *Extensible Authentication Protocol* (EAP) to handle the handshaking between the access point and the station with *Transport Layer Security* (TLS) which uses *Public Key Infrastructure* (PKI) and creates session keys for communication between the supplicant and the authenticator. The IEEE 802.1x series of standards serves as the transmission interface in this system due to its widespread use, compatibility with the EAP-TLS protocol, provision of built-in data encryption, and compatible construction of communication layers between the access points and stations [4]. Greenpass builds on the Wi-Fi Protected Access (WPA) security standard associated with the 802.11i standards by using *Simple Public Key Infrastructure* and *Simple Distributed Security Infrastructure* (SPKI/SDSI) certificates to achieve guest access and delegation functionality. On the back-end, a *Remote Authentication Dial-In User Service* (RADIUS) server or any number of such servers communicates with the access points in order to authorize or deny requests for access.

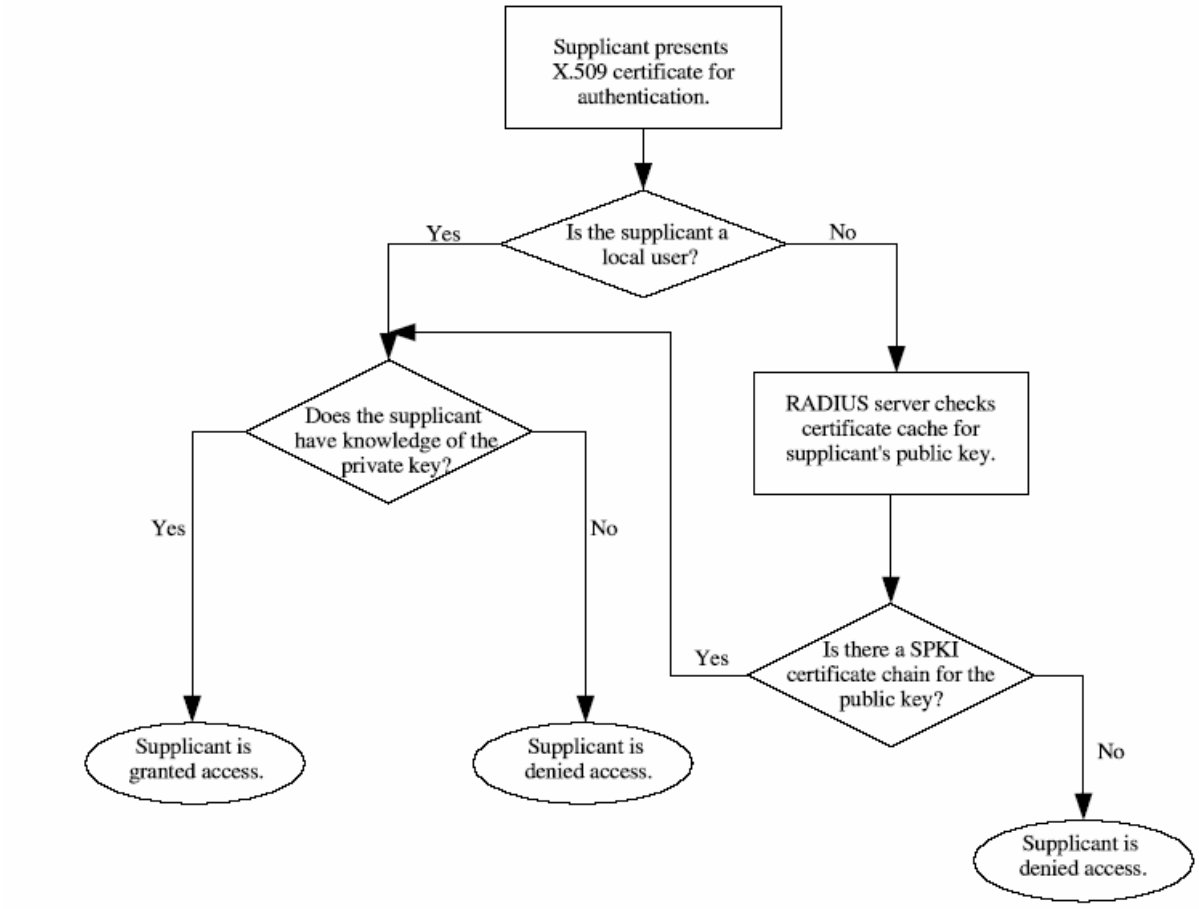
The general functionality of the Greenpass system is divided into two parts associated to the kind of access requested: **registered user access** and **guest access**. In order to handle these different access types, *Virtual Local Access Networks* (VLANs) are implemented to handle routing control for guest access and registered access. The current system has each access point assigned to two SSIDs: one for guest access prior to delegation named **"Greenpass Test"** and the other for registered users called **"Dartmouth User."** The diagram of the physical structure of the system as published in [11] is in **Figure 1** (below).

Figure 1: Diagram of the physical construction of the Greenpass system at the time of the pilot [11]



The "Dartmouth User" SSID is not broadcast and is mapped to VLAN1 which handles authentication of registered users and authorized guests to the entire network. The broadcast SSID is associated to VLAN2 which simply contains the system's guest page to guide the supplicant through the delegation process. If an unauthorized guest attempts to gain access to the system through VLAN1, without being delegated, the system automatically associates the guest to VLAN2 and the delegation page is loaded (**Section 2.1**). The decision flowchart of this design is illustrated in **Figure 2** (below) and also was provided by [11].

Figure 2: Decision Flowchart of the Greenpass System [11]



The specifications for each of the features of the Greenpass system are specified in further detail in the concurrent master's theses on this system, specifically delegation tools by Goffee [3] and RADIUS server configuration by Kim [7]. The following two sections provide a summary of the authorization process depicted in the decision flowchart above.

2.1 Registered User Access

Registered users are assigned X.509 keypairs that are stored on the back-end RADIUS server and the clients' systems. Following the PKI specification, users are provided with a public key certificate (PKC) associated to their assigned keypairs. This security certificate is issued and signed by an authorized Certificate Authority (CA).

It binds the owner's identity to the public key and identifies the user to the network during the handshaking process. Once the user has set up the system to use the wireless connection associated to the non-broadcast SSID of the network, he/she can attempt to associate to the access point. This action triggers the EAP handshaking process secured by TLS. Request and response packets are sent between the client station and the RADIUS server via the access point (which serves as a "middle man" at this point).

In the handshaking process, the supplicant presents an X.509 certificate to the RADIUS server which checks whether the supplicant knows the private key associated to the public key of the presented certificate. The server also ensures that the certificate was issued by the local CA. If these checks pass, access is granted and the user is associated to VLAN1. Otherwise, the certificate may be associated to an authorized guest (the certificate is signed by an authorized user) so the server checks for a valid SPKI chain that vouches for the supplicant. If this is found, then the supplicant is granted access; otherwise, he/she is reverted to the guest access page with the delegation tool on VLAN2.

Currently, the prototype uses certificates issued by the Greenpass Certificate Authority that was developed for the purpose of testing. Privacy-Enhanced Mail (PEM) or *Personal Information Exchange* PKCS # 12 (.p12) certificate files issued by this CA are sent to registered users along with the root security certificate file (.der) that allows the system to recognize the Greenpass CA as a valid and trusted issuer. The latter file will not be necessary once the system is fully implemented and certificates are issued by a CA backed by a large commercial authority. For the purposes of the demo, we are using an independent CA that requires this extra step. Additionally, these test conditions are not ideal for real-world application and will be modified accordingly. Keypairs should not be mailed to users as this direction compromises the integrity of the private key which should not be exposed to unprotected communication channels. In the future, these keys will be generated on the registered user's disk more directly. The developers are also considering eliminating the PKI requirement of this system and allowing authentication of local users in other ways that may already exist in a network.

2.2 Guest Access

The supplicant without a valid X.509 certificate for the Greenpass system attempts to gain access using the broadcast SSID ("Greenpass Test") or is redirected there by a previous failure to connect to the main server. The delegation page loads, and the guest presents an X.509 certificate to be signed by an authorized user. The system is designed to use pre-existing certificates in order to limit the number of certificates and keys that a user needs to authenticate with different systems. If the supplicant does not have a certificate to present, the prototype allows the user to obtain a self-signed, dummy certificate via a Greenpass CA reserved for this purpose. The guest submits general information (name and e-mail address) and the Web browser generates a private and public keypair for the individual. The private key is stored on the guest's system and the public key is sent to the dummy CA to generate the certificate for this keypair. The certificate produced does not authorize the guest to access the network as it lacks an attached signature (which will be obtained through delegation) that vouches for the guest's authorization to use the network. Instead, this process simply serves to provide an X.509 keypair and associated certificate to the guest, thus enabling the TLS communication for the authorization process.

Once a certificate is presented, a visual hash of the guest's public key is displayed on the screen along with a four digit identification number. The supplicant must then request for a registered user with delegation rights to delegate using this visual hash and number. Under this construction, the delegator and the guest are presumed to be in the same room in order to share the visual hash. The delegator accesses the delegation page and enters the number associated to the guest. The delegator must then select the name and number on the screen that corresponds to those on the guest's screen. After submitting this request, the delegator is presented with sixteen unique visual hashes, from which the corresponding image should be selected. At this point, the authorization will pass and the delegator's SPKI is used to sign the guest's certificate. The guest is now authorized to use the network and the SPKI/SDSI chain is stored as a cookie in his/her browser. When the guest tries to associate to VLAN1, the user must present knowledge of the private key associated to the presented certificate. Once this step

is authorized the server looks for the SPKI/SDSI chain that vouches for the guest's authorization and upon authentication, grants the guest access to the entire network.

3 Testing Objectives

The reliability of a software system depends on the bugs and design problems within the software implementation and the exposure of these errors through usage and analysis [9]. With a working prototype and a firm understanding of the system's capabilities, proving the reliability and usability of the system is the next task in the development process. In this phase, we introduced the system to a group of test users through an initial demonstration, aimed at revealing unanticipated exceptions and obtaining feedback from these test users. A variety of participants, situations and platforms are essential in challenging the functionality of the software, increasing the possibility of encountering undiscovered limitations and thus gaining a more sound determination of the general usability of the system.

With the prototype of the Greenpass system available, we divided the formal testing phase into five parts to be undertaken in this order:

1. Analysis of the objectives of the Greenpass system
2. Formulation of relevant questions and informal testing
3. Strategic planning of concrete levels of testing
4. Implementation of a demonstration with volunteer users unfamiliar with the system
5. Examination of the results received and projection for future tests and recommended changes

Before the first demo and before any test user was introduced to the system there were many stages of analysis and planning necessary for establishing the testing goals. First and foremost, we had to determine what we specifically hoped to learn about the system through each demo. What were the aspects of the solution that could

lead to problems or need further testing? What usability concerns should be addressed? How closely could we model the intended purpose of the system with test situations and users? By internally examining and testing the system for the first half of this project, we were able to implement a plan of action to address these questions.

At the beginning of the testing project, we partitioned the accuracy and usability issues into smaller, testable sections (**Section 3.3**). By breaking the problem into these manageable segments, each aspect could be targeted specifically and substantially explored. We first determined that we would address platform compatibility issues before leading up to the initial demo that would incorporate many different systems and provide insight into the usability concerns of the tools. Once the prototype was stabilized, we could test the system's features in a variety of controlled settings, starting with the first small test set.

The introduction of a number of users with varying levels of trust was the primary focus of the testing plan. Acknowledging that the user plays a significant role in the overall security of a distributed authority system, we aimed to account for the various human trust issues and networking schemes within the analysis of the system's own design. We wanted to uncover unanticipated risks in the security scheme and therefore had to observe firsthand the human-system interaction and how it affected the solution's accuracy. Before we could approach this aspect, we had to define trust and its role in security systems. Fundamentally, human trust is important in a distributed authority system insofar as distributed systems are an extension of social interactions that are guided by trust [6]. The security risk intrinsic in delegation directly relies on these formulations of trust, both interpersonally and between the human and the software. We further discuss the human trust and security systems correlations in **Section 4** and apply these concepts throughout the pilot.

Based on the determined factors, the first demo's purpose was two-fold: (i) further assess the functionality and reliability of the system and (ii) account for user input in the system's overall accuracy. We arranged the demo in a way that permitted each user to implement as many of the tools as time would permit and assess the three possible roles in authentication. This increased the scope of usability, since we could gain multiple perspectives

on each specific role (**Section 5**). The questions posed regarding each step emphasized the extent of the user's understanding of the system. The results of these questions provided us with a means to analyze the human-computer interaction and comprehensibility of the system from the user's own evaluations. We emphasized these factors for the influence they can have on the security in such a distributed authority system. An example of a situation where security could be compromised by the misconceptions of the user is in the case of a user that was not aware of the implications of delegating to an untrustworthy entity and simply delegated at will or granted delegation rights to every guest permitted access to the network. Another situation could be imagined where a delegator who not understand the purpose of matching visual hashes and successfully authorizes an adverse entity. These scenarios would severely affect the network security and can be avoided by establishing a clear and simple interface with the user. Our testing plan sought to evaluate this overall usability and clarity to make a determination of the system's functionality.

3.1 Analysis of the System's Objectives

The determination of the features and aims of the software represents the first phase in the formal testing process. To ensure that the testing plan would address the important issues of the Greenpass system, we outlined the principal objectives of the system to serve as a set of guidelines for test areas. The fundamental goals of Greenpass as defined by the developers of the system are to:

- Permit access to the network for registered users and authorized guests
- Support standard client platforms
- Easily integrate in existing networks and serve as a standalone service
- Provide a seamless solution for authorizing guests to use the network

- Model the flow of authorization in realistic ways by providing the authorization of guest access through registered entities within the network and not solely through a centralized authority system.
- Protect against malicious attacks
- Extend to other authorization needs
- Scale to various access policies and institution sizes

Beyond the structure and accuracy, the set up and use of Greenpass' tools should also be easy to understand and should be intuitive. The original paper of this system delimits these objectives [11].

For the initial demo, only a subset of these goals could be tackled in keeping with the targeted testing scheme.

3.2 Formulation of Relevant Questions and Informal Testing

After we reviewed the purpose of the system, we started planning for a series of informal tests of the various features. Persons already familiar with the projected conducted and participated in these tests. At this point, we introduced additional platforms into the test, used the delegation tool extensively, monitored the efficiency of the steps and examined any software/hardware requirements. Due to the EAP-TLS protocol, only 802.11i compliant wireless cards and operating systems that supported these cards could be used. Additionally generic system updates may be required to fully support the authorization scheme.

Previously the developers tested Greenpass on two personal machines running Mac OS 10.3 (Airport) and Windows XP Home (Cisco Aironet 350). We established that Windows 2000 could also be supported using at least Service Pack 3 as well as newer versions of the Mac OS 10.3. Surprisingly, when we introduced the Windows XP Professional operating system with an Intel PRO 2100 internal wireless card, authentication failed.

We determined that the operating system was not the issue as the Service Pack (v. 1) and updates on the system were up-to-date as compared with similar platforms that we tested successfully. Additionally, the given platform could support other plug-in wireless cards. Therefore, the compatibility of the Greenpass system with the wireless card was the problem. After careful analysis, we determined that the server's system firmware was a plausible source of the incompatibility, and we were able to resolve the problem by performing a BIOS upgrade of this system. Another unexpected issue that we encountered in the initial testing pertained to the java applet plug-in. Greenpass uses this plug-in to show the visual hashes in the delegation process. A more recent version (1.4 and above) of the plug-in must be downloaded to support this feature. The exact cause of the failure of earlier versions to support this application has yet to be determined. This limitation is not a concern as it does not compromise the system's flexibility for supporting standard platforms.

Once these issues were resolved, we could refocus on implementing the demo and searching for the remaining questions to answer. In regards to the system's accuracy, we now knew that the system supported some standard platforms. We sought to ask more general questions such as: Does the system grant registered users and authorized guests access as it should? How flexible is the solution? As regards delegation: How understandable is the process? What difficulties or unexpected errors do the users encounter? How effective is the visual hash in the identification process?

As we have discussed, distributed authority poses the challenge of accounting for human trust issues within the reliability and security of a network. Greenpass is no exception and these issues were addressed in the demo by allowing each person to rate the level of understanding and ease-of-use for each step of the process. Here we attempt to answer the questions of flexibility and operability: how easy is the system to use? How much effort was needed to set up the system to use the connection?

Additionally, the protocol and network-dependent questions also arose in relation to the sociological implications of the distributed authority feature: How should revocation rules be handled? Who is considered a guest? Who

should be given delegation rights? Undoubtedly, these questions will change from institution to institution; however, there are general evaluations that can be made to making these determinations. These issues were not evaluated within the pilot itself but we explored them independently.

3.3 Levels of Testing

The purpose of the investigation and testing phase is very extensive due to the wide-spectrum of goals therefore using a structure similar to a divide and conquer algorithm serves as the best method for obtaining results. Instead of planning one grandiose demo in which we try to locate and resolve all the problems within the system, a series of specific, well focalized demos were proposed in line with the objectives of the system. In this way, the system can be improved gradually through specific changes supported by thorough testing. We determined these levels of testing in the investigation and analysis phase prior to the first demo. An outline of the major steps is given below:

The first level of testing manifests itself in the pilot. The pilot was intended to expose the system to a small test group of six to ten persons unfamiliar with the system. The goals of the demonstration were to test the goals of the system unrelated to differing policies and resistance to attack. The test was implemented to determine the level of usability for users of varying degrees of networking familiarity, the system's accuracy in authenticating users, and to a very small degree the modeling of social networking. In order to achieve the last stipulation, participants were chosen based on their relationships with the other participants. The controlled setting makes this test less useful, however, than a larger test group with more intricate social ties.

After the pilot was completed the plans for future testing needed to be amended based on the results gained, however it was established early on that another set of small demonstrations of a similar nature would be necessary as the development of the prototype progressed. These additional small-scale tests (an intermediary step between the first and second step of testing) would involve a few persons who could re-evaluate the system based

on the adjustments made to improve usability. The suggested changes from the first prototype are outlined in **Section 6.** Tentatively, the same subjects from the first demo could be requested to analyze the system once more and make comparisons to the first demonstration.

The second level of testing is a medium-sized control case in which there exist multiple layers of social networking. The goals of this test would encapsulate that of the pilot, as well as a greater focus on how the system parallels and incorporates itself in human interaction in the real world. We explored the specifications on how to implement this case and give a possible suggestion for the test space in **Section 7**. More test cases can be implemented and theoretical testing such as modeling guest activity can be done in order to determine the complete functionality and readiness of the prototype.

Beyond this level, the third stage should encapsulate more integration into an existing network. At this point, the system should be precise in meeting the basic goals and ready to be implemented on a large scale. The user set would be much greater than the medium-size case as the system is ported over to an existing construct. A gradual incorporation of the system would be most effective following the guidelines of the previous testing schemes. One can imagine implementing the system from one branch of an office to the next in an enterprise or from one dorm space to the other in an educational institution. These tests would give invaluable insight into protocol issues, scalability and integration capabilities of the system. The final stage of testing should slowly expand the size of testing and observe trends in guest access in order to refine the protocol or flexibility of the system within the network.

3.4 Implementation of User-Dependent Demonstrations

The Greenpass system models one way interpersonal networking occurs in the real world. Person A knows and trusts person B, and therefore will enter a trust relationship with that person. Such trust relationships could include living with the person, delegating a responsibility to that person, sharing a secret or authorizing that person to use a closed network. The type of trust that is established is dependent on the type of relationship. Person A may only trust person B in certain situations and thus may limit the extent of the interactions which require this faith. These scenarios represent the trustworthiness of person B according to person A's analysis, and explains the trust judgments of the latter [4]. They also reveal the complexity behind the concept of trust. This sociological study is expanded in **Section 4**.

In order to factor in the idea of trust on the human side, testing the system in situations that reflect true social interaction and networking is essential. The small scale demos serve as a foundation from which more realistic tests that closely model the practical use of the system can be implemented. Once the focus of the test and the format was established (as detailed above), we assembled a group of volunteer participants and led them through different scenarios and instructions that exercised the features of the system. The full details of the pilot of this system are presented in **Section 5**.

3.5 Examination of Results and Projections

In order for a test to be a useful study, the outcomes, difficulties and successes must be examined and projected on to future work. The first pilot offered the first set of results regarding the usability of the system. We analyze the results for this demonstration in **Section 6** and provide immediate directions regarding the remaining stages of testing in **Section 7**.

4 Sociological Implications

Many security systems rely on the concept of human trust. Stating that a system is secure implies that it can be trusted to protect certain data or appropriately limit a program's functionality. Therefore, security systems are the basis by which a user generally chooses to depend on (i.e. *trust*) a system's ability to secure information that is input or transferred through it. They allow an organization or single entity to control their network and protect it from malicious outside sources. They protect the identity of individuals associating to the particular system. They protect against the corruption of data and allow for non-repudiation schemes.

This relationship between trust and security is crucial to systems such as Greenpass. In terms of security, Greenpass aims to protect the network and allow users to participate in the control of guest access. As relates to trust, the system incorporate human assessment on three levels:

(i) Network administrators trust the system's ability to accurately control the users allowed on the network

(ii) Network administrators trust delegators to delegate with discretion

(iii) Individual delegators trust the persons to whom they delegate.

Once the structure of the system is proven correct (influencing the first level of trust), the human interaction with the system has to be considered before claiming that the system is a trusted one (establishing the remaining levels of trust). This is due to the fact that a trusted system does not characteristically have trust embedded in the system, but is one in which a user assesses its trust value [9]. A security system that depends on its users' decisions to establish trust without examining the determinations of trustworthiness fails to secure the associated system as the expectation and certainty involved in establishing human trust is removed. Logically, delegators must be chosen carefully so as not to compromise the system's security, but how do we establish whether a particular person is a risky choice? What elements influence a particular person's trust of another individual?

Beyond analysis of the personal trust values, observance of interaction with the system reveals another concern in human-system trust: the protection of users from their own misconceptions. It is equally important for a user to trust a system as it is for that individual to understand the foundations of that trust otherwise the security can be compromised. For instance, in the case of internet security and spoofing, users can be led to believe that a system is secure by mimicking the features that users generally use to determine a web server's security [14]. In a wireless network, a user may believe that all communications are secure because the wireless card that is in his/her system supports encryption although the feature is disabled in the network settings. For a distributed authority system, it is necessary to understand this concept of trust in order to formulate correct integration of this factor in the security design. The level of understanding that users have of the steps in delegation is key to this analysis. The interface should be simple and informative so that a delegator cannot inadvertently delegate to a malicious entity.

4.1 What is Trust?

Trust has been defined in many ways, and there has been much written on this concept in an effort to measure it. Trust is a complex concept due to the many different manifestations and the variance of its usage. It can serve as a human trait (one is trusting or trustworthy), a verb implying certainty (I trust you), a legal obligation (established confidence through contract) and a verb implying a desire (I trust that something will happen). Typically, trust is an expectation about the future based on experience and prior observations [4] [7] [13].

According to McKnight and Chervany in [7], trust is categorized in four different ways:

(i) *Impersonal/Structural*: refers to confidence based on institutional structures

(ii) *Dispositional*: trust based on the personality of the trusting individual

(iii) *Personal*: one person trusts some person, group or thing in a specific situation

(iv) *Interpersonal*: two or more entities trust each other in a specific situation

All four are relevant to the Greenpass system and its distributed authority structure.

4.2 How does trust relate to the Greenpass System?

The integration of the Greenpass system into institutional structures can gain the user's trust solely through this association. There may be a transferal of trust in which individual entities within the organization, trust that a secure system will be chosen in the interest of the group, and thus these individuals will trust the system. This models the case of *impersonal or structural trust*. Before an organization will elect a system, however, it is hoped that they too will seek proof of the security of the system before this transferal occurs. This situation also demonstrates structural trust as one group gains confidence in the system based on its structure or perhaps based on the developers who produce it.

The remaining categories of trust are exhibited in the Greenpass system through the delegation tool and the influence of the user in the establishment of a trusted system. The distributed authority integrates the social networks that exist in human interaction into the network security.

To determine whether a given entity poses a security threat as a delegator in a distributed authority system, we often want to determine the *dispositional trust* of the individual. This trust factor refers to a characteristic of the individual, namely, whether the person is intrinsically trusting or distrusting. A common misconception is that persons who are trusting by nature are greater security risks in protection schemes and real life situations as they are gullible and more likely to breach protocol in order to accommodate someone who may be untrustworthy. In reality this assumption has proved unfounded [4] [13]. Although trusting individuals tend to place faith in others, they also tend to be very scrupulous and therefore do not unconditionally pose a threat to security. Monitoring this trait in delegators as it related to the overall distributed authority system's security and authorization of strangers may be an interesting avenue to explore in the future.

Personal and *Interpersonal trust* are manifest in the social interactions that build trust relationships and webs of trust. In personal trust, one individual may trust another individual in a specific situation but the trust is not reciprocated: person A trusts person B. Interpersonal trust extends this category since it involves more than one dimension of trust: person A trusts person B and person B trusts person A etc. Delegation incorporates both forms of this trust but does not distinguish them. In order for delegation to occur, only personal trust is necessary since the delegator is the only entity demonstrating trust in another individual. The guest may or may not trust the delegator in the same way as this is trivial in this scheme. Therefore, the risk factor involved in each of these types of trust can be assumed equivalent, though this has to be explored further. In essence, delegation relies on

the personal trust relationships that exist in social networks. However, interpersonal and dispositional trust often influence personal trust and, thus, cannot be discounted in the scheme.

A person's dispositional trust directly affects the personal trust relationships that he/she may enter. If the individual is so distrusting that no relationships are established, then the security risk of this individual as a delegator is negligible. Likewise, however, a very trusting individual may trust and delegate to a wide range of trustworthy persons and the effect is the same. Once a person enters the network, they include themselves in an expansive interpersonal network of guests, delegators and the system.

The levels of trust are as complex as the determinants that produce them. We have extrapolated a few factors in trust, however, there are many more that render this human factor unpredictable. We would like to determine who can be trusted. Who is most likely to authorize a stranger? Who tends to trust the untrustworthy? Unfortunately, these questions cannot be answered definitively as there are an infinite number of factors and scenarios. The trust someone places in a stranger is based on factors such as appearance, tone of voice, age, as well as the solicited person's dispositional trust, mood, location etc. For a distributed system to account for the unpredictability of user behavior and trust, then, they must form the decision based on other trust formulae: analysis of past behavior and establishment of legal obligation.

Contracts establish a level of trust between the entities involved in the agreement. These agreements serve as the foundation for which each entity trusts the other as it offers an incentive to each party. Protocols serve as a type of this contract. Any breach of the stipulations of this standard can lead to the termination of the relationship; in this case, the retraction of the valid status of the user in the network or delegation abilities. Distributed authority systems can establish a level of trust, and choose the delegators with less precision of trustworthiness based on the establishment of obligation. Given these consequences, delegators may use more discretion in granting authorization. Supplemented with an analysis of past behavior of loyalty or trustworthiness, this approximation of a secure network can be fairly accurate without the need to scrutinize each individual's level of personal trust.

5 First Demo

The Greenpass pilot took place on May 19, 2004 on the Dartmouth College campus, a highly wireless-friendly environment. The participants of the demo were members of this community, taken from various sections of the institution. There were seven test users of which two were graduate students of Computer Science; two were graduates of the Dartmouth undergraduate program currently working for an office affiliated to the college, and the remaining were undergraduate students with varying concentrations (Table 1). The demonstration employed the access point and RADIUS server that had previously been set up and used in the internal testing and analysis phase thus creating a stable arrangement from which to gain results.

Before beginning the process the participants were given a brief verbal explanation of the system and the features that they would be testing. They were also presented with a written summary of these instructions. The first part of the demo consisted of a series of general system security questions in order to gain a perspective on the user's point of view on the importance of security mechanisms in a network and how they determine whether a connection is secure. Questions included:

- How important is a secure connection to you?
- Do you think the current wireless system is secure?
- Should a network control the persons that are allowed to access it?
- How do you determine if the wireless network you are using is secure?
- Do you take any extra precautions when conducting sensitive information transmissions?

Responses to these questions were varied and are detailed in Section 6 (below).

Additionally, questions regarding the specific features and protocols of Greenpass (certificates, EAP-TLS, PKI, cookies) were also posed in order to attain levels of understanding of security concepts prior to the set up and

trials. As shown in Table 1, all participants had set up a wireless connection before the demo, and were familiar with the operating system with which they were working.

At first, the demo intended to incorporate a study of how the system modeled the flow of information in the real world and analyze the security risk. However, due to the complexity of the sociological factors which determine whether a particular person would be a potential threat as a delegator the demo shifted focus to primarily gaining an understanding of the human-system interaction. The general security questions and a single situational question were posed in order to gain some insight into the complexity of people's determination of trustworthiness and security. In order to model the expected use of these tools, the majority of the participants were already acquainted and some level of trust existed among them. Due to constraints, it was not possible to have a fully networked set of users, but they were advised as to the situation that they were simulating once delegation began.

Table 1: Cross-section of Users and Platforms Tested in the Pilot

	User 0 (YX)	User 1 (SS)	User 2 (LS)	User 3 (MB)	User 4 (CM)	User 5 (EW)	User 6 (LF)
Gender	M	M	F	M	M	M	F
Age	26-35	18-25	18-25	18-25	18-25	18-25	18-25
Major	Computer Science	Computer Science	Studio Art	Govern-ment	Math & Engineering modified with Studio Art	Computer Science	Religion
Level of Education	BA	UG	UG	BA	UG	BA	BA
Job	Graduate Student	Student	Student	Policy Assistant	Student	Graduate Student	Admissions Officer
Platform	Windows XP	Mac OS 10.3	Mac OS 10.3	Windows XP	Windows XP	Mac OS 10.3.3	Windows XP
Wireless Card	Intel 802.11b	Airport Extreme	Airport Extreme 3.3b1	Intel PRO 2100 3A Mini PCI Adapter	Broadcom 802.11g Network Adapter	Airport Extreme	Dell True Mobile 100 WLAN Mini PCI Card
Familiar system	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Prior Set up of Wireless	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Months using Wireless	24	17	9	18	36	48	Intermittent

The second part of the demo involved the deployment of the Greenpass tools and "role-playing". The first step in this process was the set up and usage of the system as a registered user. At the time of the demo, the development of the human computer interface (HCI) component was very basic, but the functionality was in place for testing. In order to test the understanding in each step, the user was presented with thorough explanations of the technical aspects of the features and guided through each step in detail. Based on the testing platforms, two sets of instructions were provided from the wiki page for the system: one for Mac OS 10.3 and the other for Windows platforms. The sets of instructions were very different and provided a good way of gaining feedback on the

comprehensibility of the entire system based on the presentation of the concepts. It also proved to have a great impact on the final results.

Each person was given the opportunity to be a registered user, guest and delegator. These sections were divided into three parts and specific questions directed at each role. For each section, the user was asked to note the start and end time in order to monitor the time of each stage relative to the usage. The user was also asked to rate (on a scale from one to ten) the level of understanding and complexity of each step.

Scenario 1: Registered User Access

Prior to the start of the demo, the volunteers were sent certificate files for their personal identity and for the root certificate. The set of instructions provided from the wiki guided them through the installation of these files and the configuration of the network properties to use EAP-TLS, 802.1x, and the network "Dartmouth User." Once the user was connected, he/she browsed the internet and monitored any unusual activity such as excessive prompts for re-authentication or selection of appropriate keychain.

Scenario 2: Guest User Access

Four of the seven users were asked to remove the identity certificate they installed in the first scenario and to undo the changes made to their network settings. These persons then attempted to associate to the "Greenpass Test" network which directed them to the guest access page. The users presented their certificates (and obtained one if necessary) and sought out someone in the room to grant them access. Once someone was found the instructions were followed to complete the delegation process using the visual hash and number associated to the guest's identity. At that point, the guest could disassociate from VLAN2 and re-associate to VLAN1 by restoring the network settings of the initial stage. After browsing and evaluating this stage, the users were asked to assume the role of delegator using the certificates that they had just altered.

Scenario 3: Delegator

All users were initially guests because of the need for a SPKI/SDSI chain to sign certificates. An administrator of the demo delegated to the first three delegators and then allowed them to be solicited for delegation by the other participants acting as guest users. Once delegation was complete, these three users assumed the role of guest and underwent the delegation process once more.

6 Results and Observations

Overall, the first demo revealed the system's capability to accurately authenticate both registered users and authorized guests as proposed by the design. The compatibility of the Greenpass system with the available cards and platforms produced no unexpected complications. Complications did arise, however, in the comprehensibility of the system and the users' understanding of the different stages (**Table 3, Figures 5 - 6**).

In general, the participants could understand the premise of authorization – who is a guest, who is a delegator, why does the system make a distinction – however there was much confusion regarding the steps of each stage. This negatively impacted the general usability of the system as illustrated by the times taken for each step (**Table 2, Figures 3 - 4**). Furthermore, the java applet produced two unanticipated errors unrelated to the previous complications with old plug-in versions. Lastly, guests using the certificate issued by the dummy CA were not capable of delegating despite having the authorization to do so. This is due to the fact that a certificate needs to be exported as a PKCS #12 in order to correctly digitally sign another certificate for authorization. This is not a permissible feature of the dummy certificate and impeded many of the participants from completing this step. These problems are further explored below.

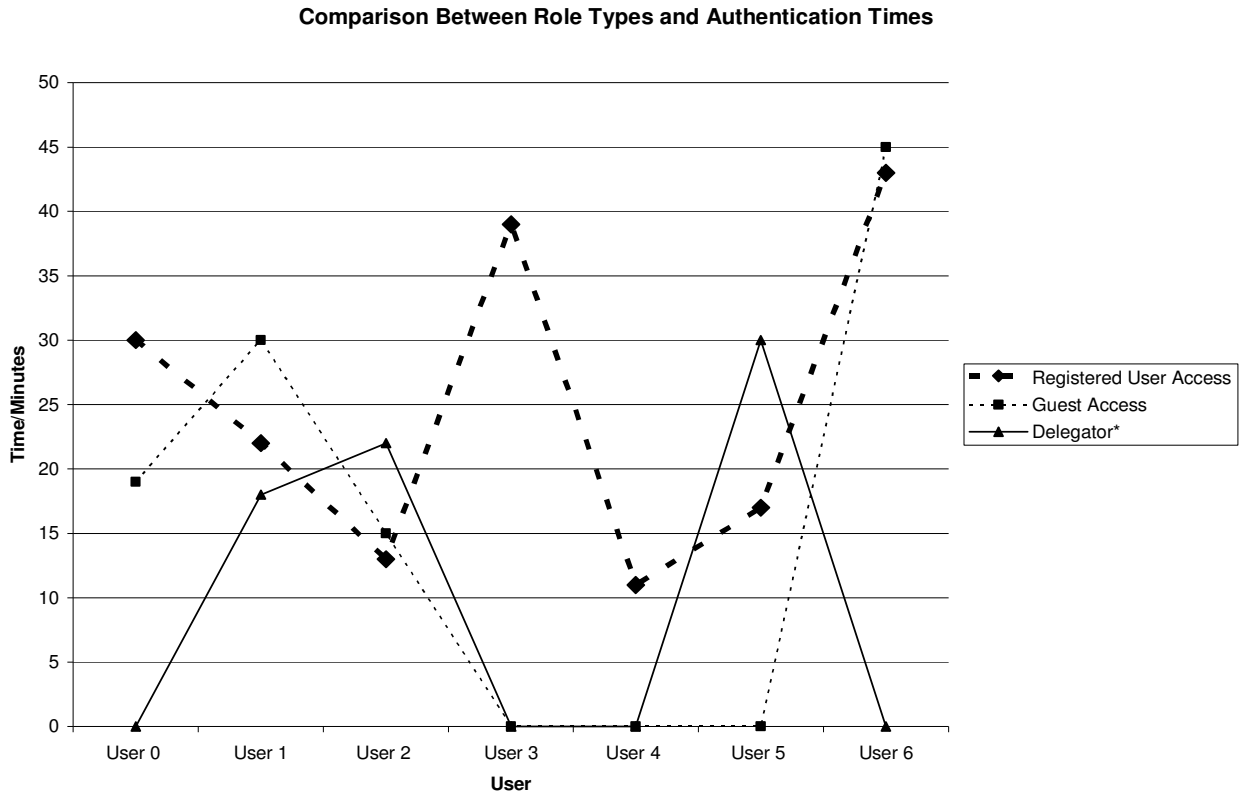
Table 2: Duration of time for each set up scenario

	User 0 (YX)	User 1 (SS)	User 2 (LS)	User 3** (MB)	User 4 (CM)	User 5 (EW)	User 6 (LF)
Registered User Access	30 mins	22 mins	13 mins	39 mins	11 mins	17 mins	43 mins
Guest Access	19 mins	30 mins	15 mins	-	-	-	45 mins
Delegator*	-	18 mins	22 mins	-	-	30 mins	-

*Participants that used the certificate issued by the Greenpass dummy CA could not export their certificate to delegate. Time elapsed before they were able to return the Registered User Access and become functional delegators

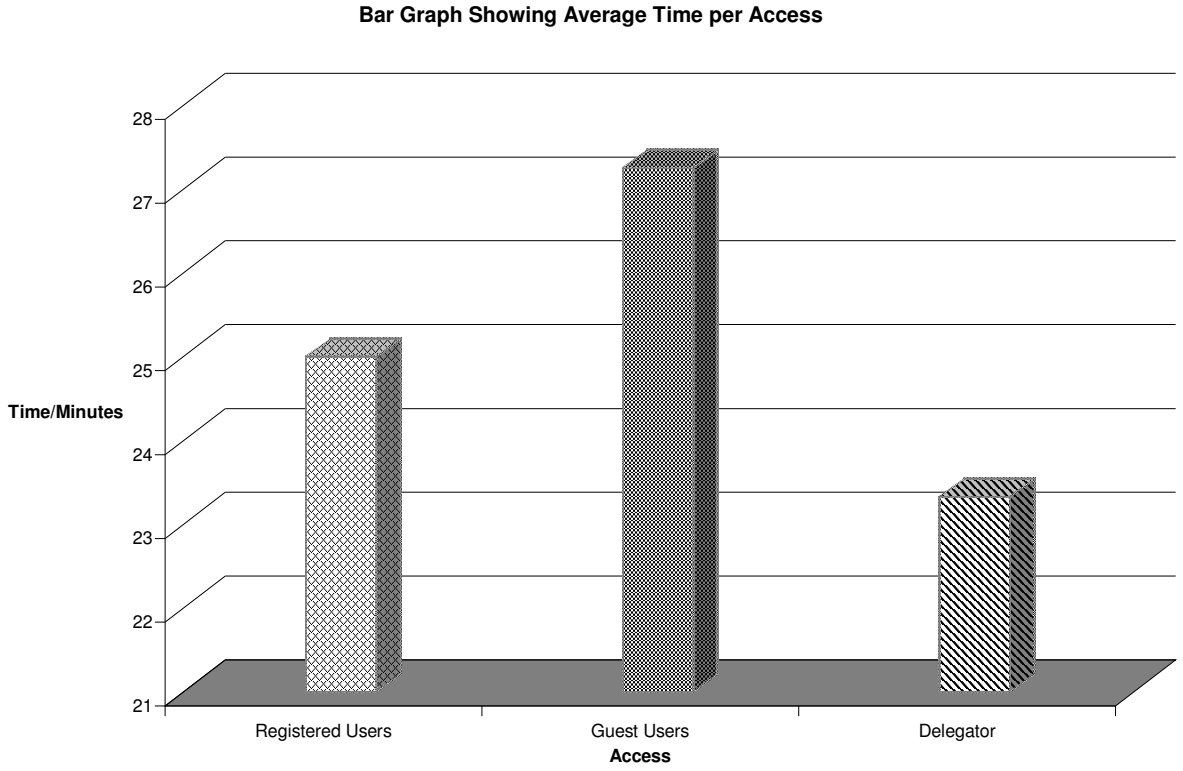
** User 3 was unable to complete the guest/delegator steps due to unrelated computer problems along with use of an incompatible operating system

Figure 3



As predicted, the authentication for registered users generally required the longest time over the other access methods because of additional set up time. Delegator access and user access took longer than anticipated due to the complications with the Java Applet and certificates.

Figure 4



On average, guest access required the longest time. Once again, this is accounted for in the complications that arose in this pilot and the disparity in numbers.

6.1 Registered Users: Setting up the Greenpass System Wireless Connection

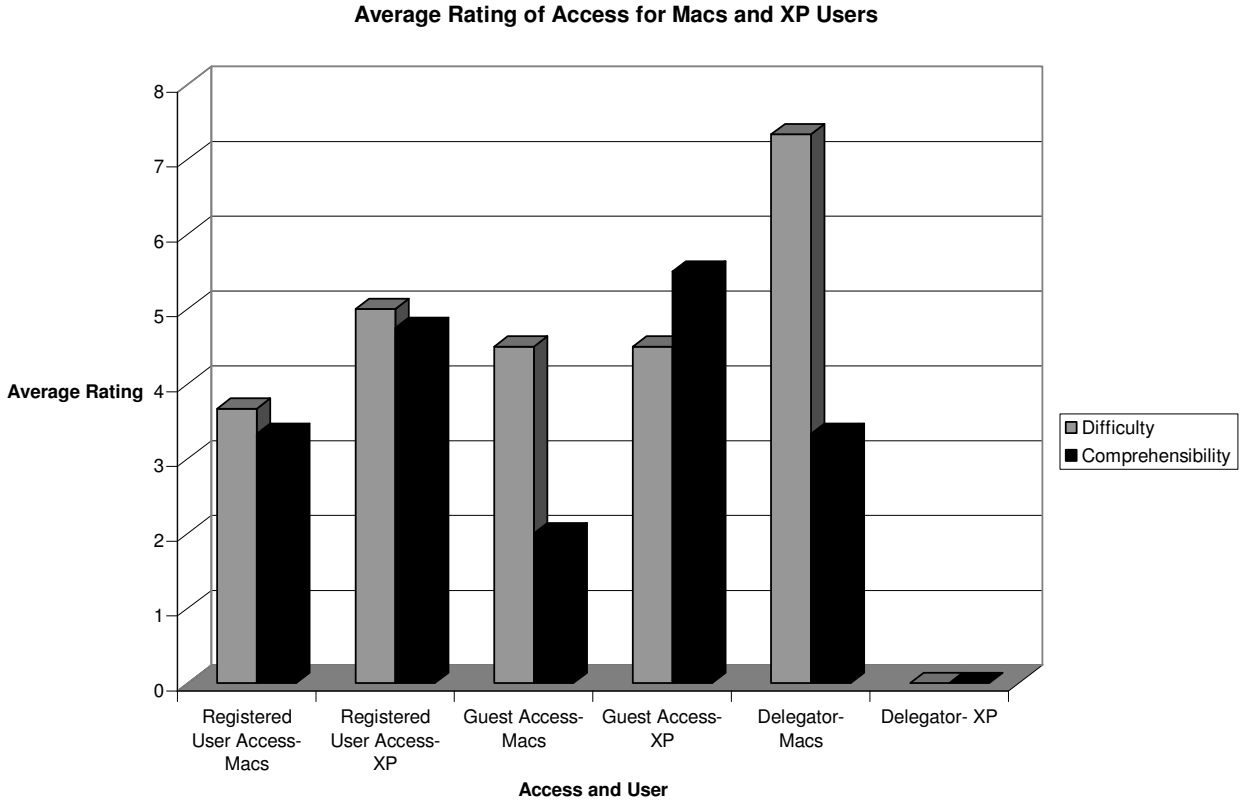
The set-up of the Greenpass system for registered guests requires the user to access different settings of the system, for example, the keychain store for Mac OS X and the "Internet Options" window for Windows. Although all users were familiar with their systems and had previously set up a wireless connection, accessing these settings was an unfamiliar domain. We should keep in mind, that there are wireless networks which simply require the user to enter the correct SSID in order to establish a connection. Despite instructions to guide users through this process, in terms of comprehensibility, this stage proved to be a complicated one for most (**Table 3**).

Table 3

	User 0 (YX)	User 1 (SS)	User 2 (LS)	User 3 (MB)	User 4 (CM)	User 5 (EW)	User 6 (LF)
Registered User Access							
Difficulty	7	4	3	7	3	4	3
Comprehensibility	8	2	2	4	5	6	2
Guest Access							
Difficulty	5	7	2	-	-	-	4
Comprehensibility	9	2	2	-	-	-	2
Delegator							
Difficulty	-	8	7	-	-	7	-
Comprehensibility	-	2	2	-	-	6	-

This chart represents the user responses to the difficulty and level of understanding in each stage. The lower scores indicate a low level of understanding and low difficulty, the higher scores represent high understanding and great difficulty.

Figure 5



This graph indicates the information provided in **Table 3**. The overall comprehensibility is very low and the difficulty varies but is about average.

The set up instructions provided for the user are still under development and improvements may alleviate some of the issues that were encountered there. In the pilot version of these instructions, the Windows version appeared to have too much detail that it was not as effective as it could have been (**Table 3, Figure 5**). Users indicated the inclusion of pictures was very helpful in the process, and so I suggest including more of these to increase the understanding of the procedure. The Mac OS version of the instructions seemed to utilize the pictures very well, as indicated by user feedback. The difficulty in this set up procedure was primarily due to the keychain store difficulties. In the Mac OS, the user was required to remove the other certificates in the keychain store to force the operating system to use the right certificate. This caused a great deal of confusion for the participants and probably lowered the level of understanding in this step (**Table 3**, **Figure 5**).

In the future development of these instruction sets, I recommend giving bulleted instructions with many screenshots and only brief explanations of the reasoning behind these steps. The overall system can (and should be) documented carefully in a public space preceding the actual sets of instructions. Another alternative worth exploration is to develop a set up utility that will guide the users through each step. Future testing situations should also include a projected presentation on the features and set up.

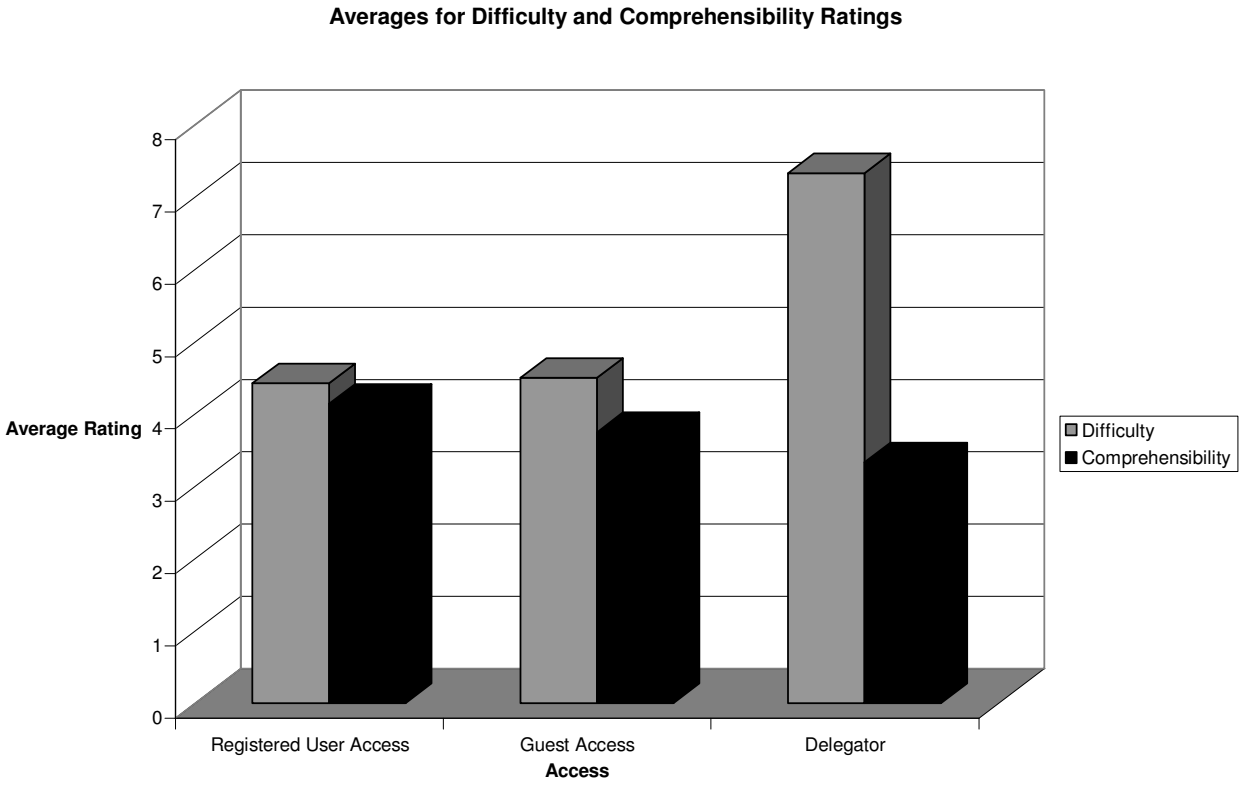
6.2 Delegation and Authorized Guest Access

Unfortunately, only one test user successfully delegated due to the non-exportable dummy certificates issued during the guest access, time constraints and the java plug-in errors with the visual hash. Five of the participants were able to act as guests however, and indicated an understanding of the delegator role. On average, guest access required the longest time (**Figure 6**), however, on a per person basis the difference between registered user access and guest access was not greatly significant. As noted in **Figure 6**, the comprehension and difficulty for these two stages were on par.

The level of usability can be improved upon by providing more options in regard to the visual hash. Ironically, the developers used the visual hash in order to increase the usability of the system [10], but due to the

cumbersome task of sharing the image (requiring that the two parties be in the same room for maximum security) I recommend having a word hash as an option, so that user's may choose their preferred method. This would increase the flexibility of the solution and allow for delegation to occur over the phone. The prototype required the delegator to choose both a number and a visual hash, so we should explore having the option to choose one mechanism, as both may be redundant. The majority of the participants mentioned that this step was relatively straightforward and so the explanation regarding this aspect proved effective.

Figure 6



7 Projections

Using the results from the previous section, we propose to advance to the next stage of testing: the medium scale test. In this testing phase, we hope to model the flow of authorization as it exists in the real world more closely by using pre-existing social networks in a more realistic testing scenario. Such a scenario that has been suggested is the PKI Summit Conference that is scheduled to take place in the second week of July at the Hanover Inn on the Dartmouth Campus. The conference proposes to include approximately 50 individuals from various enterprises interested in systems security. This test setting promises to be more realistic than the pilot as it presents a situation for which this system has been designed: a registered user of the Greenpass network may delegate to visiting conference members to give them access for the duration of the conference. For this demo, I propose that, in keeping with the participants' real status, we let all members of the conference be authorized guests of the network. This is an ideal opportunity also to observe what issues arise if everyone in the network is considered a guest, which has been proposed in the future work of [11].

In this test phase, a group of volunteers of a pre-meeting session aimed at introducing PKI are taught the approach of the Greenpass system. I recommend that a projected demonstration of the process of delegation and authentication be executed in this session to aid in the understanding of the system prior to its usage. For practical training in PKI concepts, these individuals will obtain their own keypairs and identity certificates which can later be used for this Greenpass "pilot." The administrator of the test, using a valid SPKI/SDSI chain, delegates to this first set of test users and grants them delegation rights. Along with this authority, the participants should be advised on the importance of prudence in delegating so as to preserve the true flow of authority in similar situations. They should also be advised to debrief any person to whom they delegate on the specifications of the system as a supplement to the information presented in the conference. When delegation has been accomplished, these users can now authorize other members of the conference to be authenticated to the network. Given the unpredictability of the number of persons involved in the first meeting, other individuals should be authorized to

delegate upon registering, particularly for groups that are represented by few persons. Once again careful instructions should be provided to these individuals.

For documentation and results purposes, each participant in the study should record the number of delegations that they make and indicate the relations that they have with the particular guests. Hopefully, the test will reflect the social networking that already exists and give further indications regarding the sociological implications explained in **Section 4**. Additionally, participants should answer general questions to reflect their understanding of the process and the overall usability.

8 Protocols

The authority granted to a delegator may compromise the overall security of the system if this power is misused. Therefore, the decision to bestow delegation privileges on a user must be scrutinized carefully by system administrators. How can one determine whether a person can be trusted to be a delegate? What restrictions should be applied? What revocation techniques would be most appropriate? Protocols will vary with the institution, however these represent the fundamental questions that should be addressed in this scheme. Understanding the impact of trust in these determinations is also significant and indications as to its role are provided in **Section 4**.

9 Future Work

For future developments planned for the Greenpass system, refer to the papers describing its development [3] [7] [11]. Proposed explorations include: limiting access points, supporting other mobile devices for increased flexibility (for example, RFIDs), applying the solution to other authentication scenarios and scaling the solution to various sizes. Once these goals have been achieved, similar targeted testing procedures should be used to exercise each feature thoroughly. With the current design, there are many aspects remaining to test. Of paramount importance is roaming and scalability. How will the system handle both authorized guest and registered user's

mobility? How can we predict the guest usage? How many RADIUS servers will a particular network need? These questions can be explored both theoretically, through simulation and using testing cases such as this one.

10 Conclusion

In this paper we gave an overview of the Greenpass Wireless Security System and outlined the testing strategy designed to determine the system's usability and accuracy. There were five stages of testing: analysis, question formulation, strategic planning implementation, and projections. Within this overarching methodology, we devised three general levels of testing implementations: small scale, medium scale and institution size (through gradual integration).

The pilot of the system, despite a few complications, proved that the system's capabilities were in place but improvements are needed in bridging the gap between the user and the system to ensure proper usage and added security. In accordance with the focus on the human-system interaction, we explored the sociological definitions of trust and connected them to the distributed authority system. We concluded that, Greenpass incorporates social networks within the construct of authentication and can maintain security using incentives and past trends that may indicate reliability.

Finally we made projections on the next steps, and a possible second pilot in the coming month to gain more understanding of the issues presented in this paper.

Acknowledgements

I would like to express my gratitude to Cisco Systems for providing the Greenpass team with both the funding and equipment which made this pilot possible. I especially thank Graham Holmes and Krishna Sankar for their role in obtaining these contributions. I would also like to extend my sincere thanks to my thesis advisors Sean Smith and Denise Anthony for there invaluable guidance, input and support in this project. Special thanks are also due to Nicholas C. Goffee and Sung Hoon Kim for their advice and assistance throughout my research and particularly in the execution of the pilot. Lastly, I extend my thanks to all the members of the Greenpass team whose work and dedication provided the basis for this paper.

BIBLIOGRAPHY

[1] Aboba, B. and Simon, D. PPP EAP TLS Authentication Protocol. RFC 2716, October, 1999.

[2] Denning, Dorothy. A New Paradigm for Trusted Systems. New Security Paradigms Workshop, ACM SIGSAC. 1992.

[3] Goffee, Nicholas C. Greenpass Client Tools for Delegated Authorization in Wireless Networks. Master's Thesis. Department of Computer Science, Dartmouth College. June 2004.

[4] Hardin, Russell. "The Street-Level Epistemology of Trust". Politics and Society, Vol. 21 No. 4, December 1993 505 – 529.

[5] IEEE Standard for Local and metropolitan area networks - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. October 2001.

[6] Josang, Audun. The right type of trust for distributed systems, in *Proceedings of the 1996 Workshop on New Security Paradigms*.

[7] Kim, Sung Hoon. Greenpass RADIUS Tools for Delegated Authorization in Wireless Networks. Master's Thesis. Department of Computer Science, Dartmouth College, June 2004.

[8] McKnight, D. H. and Chervany, N. L. The meanings of trust. *Trust in Cyber-Societies – LNAI* 2246:27–54, 2001.

[9] Palma, J., Tian, J. and Lu, P. Collecting Data for Software Reliability Analysis and Modeling. *IBM Testing Symposium*, Boca Raton, Florida, May, 1994.

[10] Perrig, Adrian and Song, Dawn. Hash Visualization: A New Technique to improve Real-World Security, in *Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce*.

[11] Smith, Sean; Goffee, Nicholas C.; Kim, Sung Hoon; Taylor, Punch; Zhao, Meiyuan and Marchesini, John. Greenpass: Flexible and Scalable Authorization for Wireless Networks. *3rd Annual PKI Research and Development Workshop.* NIST. April, 2004.

[12] Spencer, E., Gupta, A. and Bell, D. Enhancement of the Software Process: Human Factors as an Integral Component. SPI'95, Barcelona, November 1995.

[13] Yamagishi, Toshio. "Trust as a Form of Social Intelligence". *Trust in Society* Vol. 2, 2001 121-147.

[14] Ye, Zishuang (Eileen) and Smith, Sean. "Trusted Paths for Browsers". *11th USENIX Security Symposium*. August 2002.