TEAM MEMBERS: John Doe

ADVISOR: John Doe

PROJECT TITLE: Secure Communications

INTRODUCTION

Message encryption has been used for years throughout emails, social networking websites, and mobile devices as well. Message encryption is the process of encoding messages to protect information from an unknown source that has somehow gained unauthorized access to your data.

For this project, we will be performing a demonstration of having two computers or cellular devices send an encrypted message from one device to another, using a communication application that we will design. A third device will play the role of an anonymous source (or hacker) attempting to gain illegal access to our data. The purpose of this research project is twofold; to show that secured asynchronous communication can remain just as easy as text messaging while having extra layers of security. In our current age of technology, data protection is very important because it helps us to avoid identity theft, cyber-crimes, and also helps us protect overall data integrity.

RESEARCH QUESTION

There are several questions we hope to answer with our research. First: What network architecture would be best suited to demonstrate our project? Secondly: Which networking protocol would be best used for this project? Third: Can people easily communicate asynchronously while still maintaining secure communications from intruders? Finally: Is it practical to introduce the extra overhead in the form of encryption algorithms and extra security measures onto a mobile device?

By answering these questions through our research, we hope to increase the autonomy of PC’s or Androids communication applications by the way of increased security measures. We also hope to develop this secure communication channel while maintaining a relative ease of use for your average user. To assist us in our research, we are using a collection of technological devices combined with the Python programming language and socket programming techniques.

METHODOLOGY

It is necessary to establish open communications between multiple devices in order for us to successfully complete our research project. We will make use of computer hardware, software tools, and a variety of knowledge-based resources. The following is a complete categorized list of these assets:

Hardware:

* Two to Three Computers. A third computer may be used later to help demonstrate that we have successfully carried out our research project.
* Router/Modem – Used to provide communications between networked devices.

Software:

* A python IDE – IDLE will be used to develop a chat or IM type application.
* Socket programming will be used to establish communications between multiple applications on multiple devices
* Pycrypto, a library add-on toolkit, will be used to add an encryption feature
* We will explore using AES encryption/decryption techniques.
* Kivy – an open source python library for developing applications on multiple platforms, including Android cell phones.

CONCLUSION

By the use of our finished product, users should be able to easily send and receive secure data across the Internet, using a chat application we design. Users should feel an increased sense of security knowing that their chat dialogs and text messages cannot be easily intercepted and read by unscrupulous individuals. Above all, by the end of our research, our team will have gained valuable knowledge in the fields of socket programming and Internet security.

TIMELINE

We have broken down and organized our workload into seven phases. Each phase will be spearheaded by a phase leader to manage the finer details of each phase and to practice project management.

January (phase 1) - All members will do basic research on our project. Focus will be on understanding socket programming using python and understanding the tasks and requirements to complete this project. Phase leader: John Doe

February, weeks 1 and 2 (phase 2) - The physical network architecture will be setup using PC’s. Simple test programs will be made to ensure we can establish open communications between applications on our network. Phase leader: John Doe.

February, weeks 3 and 4 (phase 3) – A network program will be developed using the socket programming techniques we previously studied. Phase leader: John Doe.

March, weeks 1 and 2 (phase 4) – Add encryption and additional security features to our network program. Phase leader: John Doe.

March, weeks 3 and 4 (phase 5) – Attempt to recreate our network program for use by Android cell phones. Phase leader: John Doe.

April, weeks 1 and 2 (phase 6) – Feature creep and heavy testing/quality assurance will be done. Phase leader: John Doe.

April, weeks 3 and 4 (phase 7) – The group will start work on the final presentation. Our research and project will be organized into a presentable format and rehearsed to satisfaction. Phase leader: John Doe.

May, week 1 – The final presentation will be given.

Additionally, every Monday the group will meet at 2pm at SBE 229 to collaborate and present our progress to our supervisor, John Doe