TJHSST Computer Systems Lab Senior Research Project
Evaluation and Comparison of Real-time Network Latency
2008-2009

Phillip Marlow

October 10, 2008

Abstract

Mobile applications are becoming essential to modern society and as a result it is necessary to provide security. However, security needs to be as invisible as possible to the end user - the time it takes to provide security being critical to usability. This project aims to establish the feasibility of implementing security without making a noticeable impact on the end user's time. This project will focus on the security provided by the KoolSpan TrustChip^{TM}.

Keywords: cellular network, EDGE, encryption, GSM, KoolSpan, local network, network latency, security, TrustChip

1 Introduction

1.1 Scope of Study

This project is designed to be incremental, in order to allow expansion if time allows. Phase 1 involves the development of a program which allows User A to communicate insecurely with User B over a standard IP network. Ideally it will operate over both TCP and UDP protocols. This program must also include timing mechanisims to measure the round trip latency involved in communication. Phase 2 involves the development of a program which allows User A to communicate securely with User B over a standard IP network. As with Phase 1, this program must also be able to measue round trip latency and work over both TCP and UDP protocols. Phases 3 and 4 extend the programs developed in Phases 1 and 2 to work over a broadband 3G cellular network.

At the completion of each phase of development, measurements will be taken and statistical calculations made. Planned statistics to be calculated include: minimum, maximum, and average latency, as well as standard deviation for the measurments. Statistics will be collected (when possible) under different network loads to give a complete view of experienced latencies. The minimum requirement for completion of the statistical analysis, and therefore this project, will be completion and analysis of Phases 1 and 2.

1.2 Expected results

This project is expected to show that it is possible to provide excellent security without imposing an unreasonable time requirement on the end user. What exactly "unreasonable" means will be taken from previous research.

1.3 Type of research

This project aims to confirm a proof of concept for using high grade secuity over various network types and loads without imposing an unreasonable time requirement on end users.

2 Background and review of current literature and research

There have been several previous studies on both network latency and on security, however there have been relatively few studies which look at both. In nearly every case studies have focused on large, interconnected networks, rather than the relatively small user-to-user interaction proposed for this project. Instead of focusing on average latencies for the network as a whole, this project aims to look at average latencies as applicable to the real life user.

Despite this lack of close matches to the project, several things can be learned from previous work. Iheagwara and Blith (2001) look at the effect of security layering on latency in distributed environments. They present finding on latency caused due to network load as well as due to different security schemes. This can be used as a baseline against which to compare the findings of this project to assure validity of data. Szymaniak et al. (2007) also provide analysis of latency caused due to network load.

Alan Percy of Brooktrout Technology$^{\text{TM}}$wrote an industry paper on latency in IP Telephony. It outlines the main causes of latency, both within an application and from the network. It also presents reasonable values for acceptable latencies. Although not an industry standard, this provides a yardstick against which to meausre the latency measurements from this project.

3 Procedures and Methodology

3.1 Phase 1

Requirement: This phase of development will produce a program that allows two users to communicate insecurely with each other over a standard IP network.

Specifically this will be a text-only instant messaging program with the built in capability to send and recieve timing packets. This method of timing is similar to the method used by Szymaniak et al. However, instead of using a SYN/SYNACK/ACK methodology as they did, this program will implement a SYN/ACK method. This was chosen for both its simplicity and for the reduction in network useage it provides. This program will use both the TCP and UDP protocols to provide a wider range of data to compare against.
Output: This program will produce a large set of timing data for insecure communication over a standard IP network.

3.2 Phase 2

Requirement: This phase of development will produce a program that allows two users to communicate securely with each other over a standard IP network.

This will be an extension of the program developed in Phase 1. The

main difference will be the addition of an option to use a secure connection. This security will be implemented through the use of the KoolSpan TrustChip^{TM}Developer's Kit (TDK).
Output: This program will produce a large set of timing data for secure communication over a standard IP network.

3.3 Phase 3

Requirement: This phase of development will produce a program that allows two users to communicate insecurely with each other over a broadband 3G cellular network.

This will be an extension of the program developed in Phase 1. This phase aims to add the 3G cellular network capability to the chat program. This will require both ends of communication to have a broadband cellular card operating on the same cellular carrier. These cards will be configured as a network interface on each end so that minimal program changes will be necessary. Because of the difficulties presented by the use of a cellular network, TCP will be the first priority as it ensures that all sent packets are recieved on the other end. UDP capability will follow if time allows.
Output: This program will produce a large set of timing data for insecure communication over a 3G cellular network.

3.4 Phase 4

Requirement: This phase of development will prduce a program that allows tow users to communicate securely with each other over a broadband 3G cellular network

This will be an extension of the program developed in Phase 3. This phase will add the option to create a secure connection. As in Phase 2, this security will be provided through the use of the KoolSpan TrustChip^{TM}Developer's Kit (TDK).
Output: This program will produce a large set of timing data for secure communication over a 3G cellular network.

3.5 Statisical Analysis

For each phase of development, statistics will be calculated for the produced timing data. At a minimum these statistics will include: maximum round-trip latency, minimum round-trip latency, average round-trip latency, and standard deviation in round-trip latency. In addition, the total number of messages sent and the spacing of these messages will be recorded. These two numbers will help determine the validity of the statistics as well as playing their part in determining network load.

4 Expected Results

This project expects to show that it is feasable with current technology to provide secure communications without imposing an unreasonable time requirement on the end user. Comparison of round-trip latencies by network load, protocol, and network type will be shown together on a graph to give readers an indication of exactly how much extra time is required to provide high grade security.