Project 1 :: StealthNet
Computer & Network Security 2011

Matt Barrie
mattb@ee.usyd.edu.au
Department of Electrical and Information Engineering
University of Sydney

March 6, 2011

Due: To be marked in labs 28th March

1 Introduction

It is 2011 and Big Brother is way ahead of schedule.

Naturally the Internet by now is fully tapped by the first world countries as part of ECHELON, and other partner SIGINT networks.

Committed to the global war on terrorism, the world's terrorist organisations plan to develop a global information exchange using the civilian infrastructure (ie. the Internet).

Naturally, none of the terrorists involved want to necessarily be identified as the buyers or sellers of this information (even to each other!) - hence the need for an secure, anonymous platform for facilitating this exchange.. layered on the Internet!

This exchange will be used by cells to trade classified information and dirty secrets through a wholesale information exchange.

- SIGINT on known military units e.g. email, voice transcripts
- Blueprints and 'eyeballs' of bases and capitalist agent identities
- Classified agency documents
- Private video collections of dictators around the world
- The occasional bootleg Britney Spears mp3

2 Part 1 :: Securing the Channel

Your group has been hired by a rogue cypherpunk cell to build a secure communications application for underground messaging and file transfers. You can think of it as a secure version of ICQ (www.icq.com). You may assume that anonymity will be handled by the underlying BLACKNET network layers, however you must implement all other security functionality. In the first part of the project you will assemble a team of two crack cryptographers and complete the following tasks:

- Key exchange between the client and server on initialisation of a connection.
- Key exchange between client and client on initialisation of a chat session or file transfer.
- Confidentiality through encryption of client-server and client-client messages with a block cypher in CBC mode or stream cypher.
- Integrity through use of a MAC appended to all messages (client-server and client-client).
- Resistance against replay attacks using a mechanism which you are to devise.

The project will be written in Java with cryptographic library support. You have been provided with skeleton (insecure) source code for the system.

This part of the project counts for 1/3 of your total project mark.

3 Authentication

You are to implement key exchange to strengthen the system against a passive attacker. You may use any form of key exchange discussed in lectures, including Diffie-Hellman or methods using public key encryption. You are free to implement Merkle Puzzles provided you can come up with a solution that uses network bandwidth within an order of magnitude of that of Diffie-Hellman and provides comparable security.

You are to use the result of the key exchange to derive the block cypher key, CBC IV and MAC key, or seed for the stream cypher. You should do this by using a hash of this secret as a seed to a PRNG.

4 Confidentiality

Confidentiality of messages is to be achieved through encryption of each message with either a block cypher in CBC mode or a stream cypher. You may use any

block or stream cypher you wish, provided that it would give most intelligence agencies from second world nations a run for their money. The IV and key must be derived through a key exchange mechanism as described above.

Note: Each session between client and server, as well as between different clients must be secured with a new key. This implies that key exchange is performed everytime a communications link is established.

5 Integrity

Message integrity is to be achieved through appending a MAC to each message between clients and the server. This is to foil an active attacker from modifying messages in transit. Again, the key to the MAC must be derived from the key exchange above in the method described above. You may use any type of MAC you wish, provided it provides an adequate level of security to the system (industrial strength).

6 Preventing Replay

You must devise a scheme where the system is resistant to messages being replayed by an active attacker. The exact mechanism by which this occurs is part of your project.

7 Implementation

You will be implementing StealthNet in Java using Java 2 SDK which contains the Java Crypto Extensions (JCE).

A prototype StealthNet system is supplied for your reference. This system has no cryptography, and is completely insecure. You may modify this code (make sure you update the header comments to reflect this) or start completely from scratch if you wish. This source, together with documentation on the skeleton system is available on the StealthNet page on the project website.

`http://www.ee.usyd.edu.au/~mattb/2011/project`

8 Documentation

You are to write a two page design document outlining the security you implemented within your system. Your choices for authentication, confidentiality, integrity, and replay prevention must be justified. Explain how the current protocol can be exposed to a chosen plaintext attack (CPA). Make sure that your code is commented and in neat order.

9 Help

We will be continually monitoring the StealthNet forum (on the course website) for questions regarding the project. This is the first place you should look.

Tutors are also present during the labs to answer any questions. As a **last resort**, you should email elec5616@ee.usyd.edu.au for help.

10 Marking

Your project is to be marked **during your scheduled lab times**. You **must** have your project marked during labs to receive credit. We will not be marking projects outside of labs (no exceptions). We will not be marking projects received by email, nor those provided on floppy disk, tape, punch cards, print outs or any other relic of the 20th century.