# Dynamically Routed VPNs with Policy Distribution

## Executive Summary

**Supervisor: Dr Stephen Hailes**
**Group members: Kai Duan**
**Ying Shi**
**Qian Yang**
**Oliver Priest**

For the Degree of Master of Science

Department Of Computer Science
University College London
Gower Street, London.

September 2004

## Overview

Secure computer networking has risen in popularity over the last 20 years seeking to address the security concerns of individuals and organisations alike. With the introduction of advanced encryption and decryption algorithms and the decreasing cost of powerful microprocessors, the Virtual Private Network (VPN) has become a popular choice for decision makers who own and maintain secure computer networks.

For our group project, we have decided to focus on dynamically routed VPNs. There are currently scaling problems when a large number of VPN endpoints exist within the VPN. Traditional VPNs often operate using a fully meshed network topology. By introducing dynamic routing mechanisms and a partially connected infrastructure, new security problems arise. The definition and implementation of domain-wide high level security policies becomes necessary to provide routing and additional security policy controls.

## Objectives

The overall goal of the project is to design and implement an expandable software infrastructure that will support dynamic routing and policy distribution within a VPN network containing numerous endpoints.

The main objectives of the project are:

- The design and creation of a set of software daemons used for VPN communication between a set of VPN endpoints.
- The design and creation of low-level security policy structures used to enforce security policies with the VPN.
- The design and creation of a dynamic routing protocol used to maintain reachability information between VPN endpoints.

## Design

The design of the software is based on a client/server mechanism used for topology initialisation. Routing and security policy updates are then sent in a peer-to- peer manner between the various VPN endpoints. SSL sockets are used to send and receive data and policies between VPN hosts. Policy distribution occurs initially in a centralised fashion with XML used to represent the initial topology information. Once the VPN topology is fully established, updated routing and security policy information can be passed separately across the VPN allowing the policies to be updated in real time. Routing policies are updated periodically.

The application is broken down into several distinct modules, each of which provides a specific function to the overall application. The RIP algorithm is used as a routing protocol within the VPN to maintain dynamic routing information between VPN hosts.

## Conclusion

Overall, the project group managed to meet all of their project objectives producing a working prototype that implements dynamic routing in partially connected VPNs. The project also opens up possibilities for future work in the area of security policies and dynamically routed VPNs. Dynamic routing in VPNs is a particularly complex subject that requires a detailed understanding of the problem domain. We hope that our work will be able to inspire others at looking at new and novel ways of dealing with existing VPN problems. Future work could involve expanding the functionality of our software and introducing new features that will be of benefit to end users and network administrators.