Summary

This work informs the reader about various aspects of Unified Communication (UC), methods used and the problems and solutions faced by real-life organisations in its implementation surrounding firewall traversal and related security considerations.

The beginning provides an introduction into the various definitions that will aid in the reading of this document including the past, present and future of Unified Communication followed by an introduction to the various protocols used, with particular focus on Session Initial Protocol (SIP). With the help of examples it is explained how Session Initial Protocol works in concert with relevant industry standards including new technologies such as WebRTC.

Some time is spent discussing the problems of firewall transversal and network address translation (NAT) as this is a significant issue faced by organisations around the world. There is a focus put on the various solutions for these issues and their shortfalls. Hole Punching, STUN, TURN, ICE and SBCs are all featured, with examples and flow diagrams to aid understanding of how these methods are implemented.

A close look at existing literature and standards has been taken, to ensure that most common technologies, including the up to date approaches are covered. For demonstration purpose a dedicated test environment has been used with working examples of how the identified technologies work using genuine industry products as case studies.

A large section of this study is focused on UC security, as this is a major concern for all organisations and their users and customers. Firewall traversal and NAT is still a major issue, but there are solutions, and these solutions are covered within the scope of this document. Mention is also made of the need for high quality UC and UC that the average person will take up and use without complaint that it is too complicated or not fit for purpose.

During the research for this dissertation, and by experience of the author, it has been discovered that insecure UC is abused and several examples of this are given in this document. Poor or in-consequent implementation of the highlighted security services can have devastating effects on an organisation, with data security, reputation and financially.