Investigation into VoIP Communications fraud and TDoS attacks and solutions required for the corporate environment

Paul Carroll

Supervisor: Aideen Keaney

A dissertation submitted to the University of Dublin in partial fulfilment of the requirements for the degree of MSc in Management of Information Systems

08 June 2018

Abstract

Voice Over Internet Protocol (VoIP) systems continue to disrupt and alter traditional telecommunications technologies, whilst increasingly converging with a multitude of heterogeneous computing platforms and systems across both commercial and consumer domains. With internet connected devices now almost ubiquitous, VoIP is becoming an increasing popular technology for both business organisations and end consumers. Park (2009, p. xvii) suggests that *'Voice over Internet Protocol (VoIP) has been popular in the telecommunications world since its emergence in the late 90s, as a new technology transporting multimedia over the IP network, and that today people commonly make phone calls with IP phone or client software (such as Skype or iChat) on their computer or send instant messages to their friends'*. Organisations continue to integrate voice and data as this convergence offers greater flexibility and the potential for cost savings such as utilising shared infrastructure to deliver voice and data communication services to end users. Flanagan (2012, p.1) contends that *'Packet voice, Voice over IP and Unified Communications (UC) technologies are remaking telephony in a fundamental way that hasn't been seen since the 1960s'*

This research began with an in-depth review of VoIP and UC technologies including a detailed overview of their key features, advantages and disadvantages and known vulnerabilities and security risks. This included a detailed analysis of the known vulnerabilities and security risks that these technologies present to organisations whilst exploring several potential solutions and risk mitigation strategies for same. The research highlighted the growing trend of VoIP and the move towards UC technologies, a trend reflected in 2018 where four out of the top five UC vendors are cloud/software companies as opposed to traditional telecoms providers.

The research findings highlighted in the Literature Review and subsequent Findings and Analysis chapters demonstrated that VoIP and Unified Communications are complex technologies which are fast becoming standard communication systems in today's modern organisations. Following comprehensive qualitative research conducted with leading subject matter experts from Information Security and Telecommunications industries, it was confirmed that as these technologies continue to converge with existing data networks and computing platforms they are susceptible to many forms of cybercrime namely, toll fraud, data breaches and denial of service attacks. International Revenue Share Fraud (IRSF), Premium Rate Fraud and Wangiri call back schemes were identified as the most common and serious types of toll fraud due to the potential financial impact these can have on an organisation.

The majority of the academic literature was in general agreement regarding the numerous types of security vulnerabilities and risks associated with VoIP and Unified Communications implementations. Similarly, there was also a general consensus amongst all interviewees that VoIP and Unified Communications fraud was a real threat and growing concern for today's organisations. The new GDPR legislation which came into effect in the EU on the 25th May 2018 was also specifically called out as a key concern and security driver for all interview participants, all of whom unanimously agreed that VoIP security was very much a GDRP issue today.

The findings from this research will be of practical benefit to anyone working with or planning to implement VoIP or UC technologies in their corporate environment.