1 Executive Summary

Our work has resulted in the design of a novel approach to public key assurance by providing a new approach to PKI. This critical function underpins the ability to create end-to-end encrypted communications channels, our interest lies specifically of their use within social networks.

To place our work in context, we describe the background of interpersonal computer based communication examining email and then chat and instant messaging communications and their movement from Bulletin Board Systems onto the early Internet. We follow this with observations about the cryptosystems which were then developed afterwards to deliver confidentiality and integrity guarantees. We demonstrate why systems evolved the way they did by looking at the history and why there was a lack of development on the security aspects of popular communications systems from the outset.

We touch briefly on the growth of instant messaging platforms generally and in some specific arenas [76, 80] in the communications system space. This explosion of growth explains their importance to users. For threat actors these platforms are similarly important targets for exploitation; we assert these systems should provide effective security from mass surveillance. We do not limit this activity to nation states and extend it to include criminal groups and vendors. We also examine the usability challenges and the inability of users to make meaningful risk decisions.

We then review two differing public key trust models; Certificate Authorities and the Web of Trust, both of which have allied goals, to enable the proper authentication of public key components, when employed in conjunction with technologies like PGP, S/MIME and SSL [3, 5, 77], ensuring the authenticity of the endpoint our communications are destined for.

We later turn to recent revelations on mass surveillance to put the threat and consequently the risk into perspective. In broad terms we found that whilst this activity doesn’t change the threats as they have been reasoned about for decades, it has fundamentally altered the way we quantify the risk. Capable nation state threat actors were not assumed to be practically engaged in their work in the way they have turned out to be and that has had a profound effect on the way they are perceived by both the technical community and wider society [28].

We go on to explore these models and their practical challenges; the web of trust in terms of its usability issues and lack of popularity when compared with certificate authorities. Additionally we look at certificate authority compromises in recent times which have led to a number of novel approaches to the web PKI problem [12, 13] and see if there is anything that we can learn from this.

We design a protocol where we combine concepts from the Certificate Authority model and the Web of Trust to propose our own hybrid trust protocol. This is discussed in depth; looking at the assumptions we can make for the operating environment, the problem it proposes to solve and then performed detailed security analysis of the protocol.
We then validate the behaviour of social networks and their nature in supporting the protocol operation. Finally we draw conclusions on the analysis, discuss implementation details and future work.