Computational Trust for Enhanced Network Security

Tom Wallis

University Name	Glasgow University
Supervisor Name	Timothy Storer
Nationality	Scottish / British
Email Address	2025138w@student.gla.ac.uk

`Abstract` —

Sociotechnical systems research — which can cover everything from workflow modelling, to analysing responsibility, to modelling the nature of human-like concepts like Trust — can be deep and often powerful, but see too little application in the real world. We seek to apply an analysis of trust, an active topic of research, to network security in order to create new and novel security techniques. This untapped research potential would allow a new layer of network security where intelligent agents assess their peers in a dynamic, resilient manner which humans can easily reason about.

The sociotechnical field of Trust

As sociotechnical systems research continues to grow as a field, a greater number of human factors studies have fallen somewhat under its remit. For example: workflow analysis allows us to better identify organisational error; responsibility modelling allows us to better model systems such as electronic voting; computational trust gives both a human-like quality to machine learning & AI, but *also*, we propose here, to security.

Computational Trust, and its relation to security, combine to make an especially deep subject of study which can often be neglected as a security measure in practice. There are good reasons why this might be: sociotechnical systems research can be difficult, and these systems themselves can be notoriously complex in practice.[1] Many trust models exist, however, and are getting more detailed and expressive as the field grows.

We see this as a wasted opportunity. Computational Trust models allow software systems to intelligently assess the safety and security of a system when faced with a given situation. As such, it can allow for security systems which grow in depth and complexity while remaining usable. For example, security requirements could increase beyond what would ordinarily be considered usable if the security system's degree of trust in the user rapidly declined.[2]

[1]

[2] One can imagine constructing a computer system which governs its own security, allowing humans it knows and trusts to pass rigorous but less frustrating security tests for the user. This would permit a very high degree of security while minimising the error humans introduce when faced with security challenges they perceive as "difficult", like remembering complex passwords.

The opportunity missed

Unfortunately, few applications of trust models to network security exist in the modern world. *Why?* Moreover, why have these models failed to see application in real-world multi-agent systems, where multiple intelligent agents report to each other?[3]

While a small amount of work *has* been published, most work is done by logicians and those interested in the modelling of the Trust system. Only a small amount of work has been published on real-world trust applications, which was commercially driven as opposed to academically studied in any case[4]. This does not promote a healthy, rigorous environment of scientific enquiry.

[3] In the case of, for example, inter-drone communication, a malicious agent could feed bad intelligence into other learning systems, causing them to act under improper training. To avoid these scenarios, it is imperative that agents can learn whether to *trust* one-another, and re-assess that trust as other agents appear more or less trust-worthy.

[4]

The proposed work

I therefore propose that important work is to be done on the application of trust to security. Trust is clearly a useful academic endeavour that could see both commercial and academic success, and could lead to an entirely new approach in information security.

As an example of the possible outcome of the work, a network

monitoring artificial agent could be produced which analyses network security threats, categorised by origin and predicted intent, and filters trustworthy and untrustworthy sources such that appropriate security measures can be put in place. This agent could also flag potentially untrustworthy activity to human system administrators.

This agent could take advantage of the slew of approaches to computational trust, as well as advancing the field's theoretical boundaries by providing a real-world application to test future models of trust against. Examples include modal logic approaches by Kramdi in 2015[5] or social trust analysis from Urbano, Rocha and Oliveira in 2014[6]. Urbano et. al's work shows that current computational trust models can be enhanced through a greater social awareness of the system, and provide an example of a computational trust mechanism which achieves this. Kramdi's work enhances the logical frameworks used by many modern trust models, achieving a greater degree of rigour and implementing an abductive reasoning model for trust.

[5]

[6]

My Suitability

My own interest in sociotechnical systems is backed by research in the field. In 2015 and 2016 I completed my honours project, a workflow modelling system which used my own novel approach to program mutation to simulate human error in a sociotechnical model. For this, I won the 2016 Best Software Product prize for my year.[7] I am now pursuing an MSci, for which my project is an adaptation of Trust models to create a model of computational responsibility. In doing this, I have grown an appreciation of the breadth and nuances of various models of trust, and look to employ this knowledge in PhD research.

[7] A paper on the work is currently being written, alongside my project supervisor, Tim Storer. A working copy of the paper can be compiled from LaTeXsource at https://github.com/probablytom/fuzzimoss-paper

Aside from sociotechnical modelling, I am a part-time Python and project management consultant for a fintech startup in London[8]. I also pursue non-computer science research in a bid to broaden my horizons, such as the software engineering-inspired Project Albert[9], a set of design patterns for improvising children's bedtime stories. I am certain that my proven understanding of software engineering, strong familiarity with various sociotechnical modelling techniques, and clear zest for research make me an ideal PhD candidate.

[8] This particular consulting contract follows my internship work for them doing software engineering this summer.

[9] More can be found at projectalbert.net