ITaaU Network

IT as a Utility Network+ scoping meeting: security and trust in IT utilities

10 June 2013, University of Southampton

1. Introduction

When the ItaaU network+ was set up and topics for investigation were considered, it soon became clear that security and perceptions of security in relation to IT utilities would be an important issue. This meeting was convened to scope out the area and to plan future activity. The key proposal on the table was for a larger event to be held in autumn 2013 and a goal was to plan some of the specifics of that meeting: how long it should last, who should attend and what it might cover. However, the network was open to other ideas, including funding research papers and a specific call for pilot projects and secondments. With such a wide-ranging subject as cybersecurity, the meeting also needed to decide what would be out of scope as well as in scope.

As a scoping meeting, participation was intentionally limited. A small group of experts in the field were gathered for the discussion and included the directors of academic, industry and applied research centres on technology and security.

There were two main prompts for discussion – a presentation outlining some of the challenges around "trust" and "trustworthiness"; and an overview of the ITaaU's preliminary "security and trust" literature survey. Topics discussed included issues of terminology, information assurance, cybercrime, psychology and risk, methodology and identity as a utility.

The meeting ended with a firm proposal and defined structure for an in-depth event to be held in winter/spring 2014.

2. Topics discussed – an overview

i. Trust and trustworthiness – terminology and other challenges

Trust is the main issue for users of internet technology but problems arise when the level of trust gets out of balance with the level of trustworthiness (security). If too much trust is placed in technology, people use systems without due care and get burned. If there is too little trust, a system may be adequately secured but the benefits are never realised because people do not use it. This topic is highly relevant to the ITaaU network as it is within the inter-disciplinary area where technical meets human/social - the socio-economic-technical area.

But there is a problem with terminological in-exactitude. What do "trust" and "trustworthiness" actually mean? IT Innovation, an applied research centre at the University of Southampton, has a project to address the issue of terminology using semantic models. It's a long path.

There are also other challenges than terminology. Trustworthiness is an issue for security technologies such as identity management, cloud infrastructure, big data protection, mobile security and multi-tenancy, low-power cryptographic methodologies. Making a trustworthy methodology for developing applications and systems is not so easy.

On the side of trust, security assurance is a problem – what does it really mean in the ITaaU world? How do you communicate and engender trust in users - what are the metrics for trust and how do you make them transparent to users? With trust management and maintenance, developing reliable reputations is an issue, especially important for mobile.

> *"People do not trust technology. Unless it is technology they use on a regular basis and then they trust it insanely."*

ii. Trust and risk

There are different views of trust related to the organisation and the individual. For example, elderly patients with surveillance (to alert carers if there is a problem) in their home often switch it off because they do not trust the technology. The developer has to understand the trust issues in such a person. But the two worlds do overlap - the person delivering the system has to take an organisational approach while taking account of the individual.

And, regarding trust levels, age is apparently one of the big correlates. An older person might switch the technology off while a 35-year-old with Alzheimer's will keep it on. Clearly the amount of time that a person has spent acquiring familiarity with the digital world is the key factor. We need to bear this in mind when examining age-related behaviours.

Understanding and expertise is negatively correlated. The more we know, the less we trust. If you're trying to negotiate and appropriate level of trust, is it ever ethical not to tell the patient that there may be a fault with the system? If you do, they will turn it off resulting in more risk.

It's about understanding the risk, conveying the risk to different users - the "out there" of wider users who are unclear about risk and have a low understanding of it but also the insurance industries. For example, credit card industries took the decision not to have a totally secure system but to trade off security for convenience and push the charge back to the insurers. Who is being insured by whom? If you quantify the risk well, the cost of ameliorating that risk falls.

iii. Assurance and architecture

At the highest level (government, Nato, EU) the current concept is that trustworthiness is information assurance. There is a move away from a security agenda to an assurance agenda. This is following an American drive in this space and in Europe we are just starting to follow that. Assurance is taking a new role. Last year the European Commission had to make information assurance one of its top levels.

For the communities of interest engaging in that space it's about the situational awareness of environment, the common operating picture – who's doing what, where, when and how. The human-computer interface. It's about looking at security not just in terms of information but also the people involved in that environment. On the other side, risk management is always a big issue; also trust management and resilience (eg in disaster management, survivability, usability and tolerances. Most models are not tolerant of a security event). The big catch-all concept is the "architecture". A whole new area of information assurance is developing around architecture – how business processes are aligning with technology, the architecture of interoperability.

From an ITaaU Network+ perspective, it might make sense to have a theme on information assurance and then do something else on the user-centredness of trust and trustworthiness to cover that other side of it, eg why people trust things that they shouldn't. It might require two separate meetings.

> *"With trust and utilities are we talking information assurance. Building trust is about assuring information. These are the code words people are looking for."*

iv. Cybercrime

As two-step ID can now be sidestepped there is a need for another level of identity assurance. There are some biometrics developments which may or may not prove to be useful alongside ideas of how encryption may take a role. The internet of things is equally interesting in this sphere.

There is a degree to which trust in ecommerce is a tipping point. How far off are we from the ratio of genuine to illegitimate transactions, in the financial sense, on the internet?

> *"Big movements of money indicate that the drugs trade is going down and cybercrime is going up."*

v. Literature survey – psychology and risk

ITaaU Network+ commissioned a preliminary survey, conducted by a librarian, focusing on attitudes to security and trust and some of the factors that influence trust, the comprehension of risk and the inclination to protect.

The preliminary survey is not intended to be comprehensive but to be an initial information retrieval exercise to gain an impression of the scope of publications in the area, to appreciate the extent to which various aspects of the area are covered and to obtain a rough and ready classification of the coverage. The survey was limited to 2011 onwards (narrowed down from an initial 2009 onwards) and picked out 55 articles as the "tip of the iceberg".

The literature survey highlighted the human aspects of the subject – key notions included voluntary self-disclosure and risk-taking propensity (your perception of the risk you are taking). The articles were divided into application aspects and psychological aspects. Of the former, about 20% were concerned with mobile services. Health, online transactions (encompassing banking, shopping and the influence of website design) were also featured. The social media aspect spanned the technological and the human side. Social media represented a trust in invisible communities – people place their trust in a collection of individuals, a community, that they do not know. This is an unsafe assumption. There were a number of articles about general perceptions, behavioural aspect (user assessment of trust), education (how far can you go in educating people about online responsibilities), children and older users.

> *"It is perhaps unsurprising to find much of the focus in IT and computer security being drawn towards the technical aspects of the discipline. However, it is increasingly recognised that technology alone cannot deliver a complete solution, and there is also a tangible need to address human aspects."*

Furnell, S, & Clarke, N. (2012). Power to the people? The evolving recognition

vi. Methodology

Questions were raised about methodologies in this area. There was interest in further research into the psychology of risk and trust - attitudes, perceptions and ongoing development in the methodologies to find out people's perceptions.

A participant pointed to an extensive investigation with social scientists from other countries [Ref here from Mike needed?]. What's clear is that there are some things that are stable whatever you are talking about in relation to trust - it does not need to be IT-focused. Many of the findings in economics or other subjects apply. But studies specific to factors that arise in IT and the internet show that things are in a state of flux, even today. People are more trusting than ever before in some ways. But running through that is a thread of scepticism. Of interest is the group that started with this technology at a young age and are now getting older. Generally, as you get older you get less trusting but if you have been familiar with this technology for a long time then you might make different judgements. And then there are now those who have never known anything else and they are making different judgements.

Suggestions for further activity in this area included requesting a report from a research group about the status of the types of investigations that are going on and whether conclusions can be drawn yet or not. There is a need to discover how stable is the methodology and whether it is more stable than the moving target. Could commission preliminary work before a further workshop on this that delegates could consider before meeting

> *"Everything is in flux."*

vii. Identity as a utility

Identity as a utility was identified as a rich topic. What identity and what are we trying to identify? There are potentially three aspects of the human in the system – the physical person, the cyber persona and, possibly, an agent.

A workshop theme on identity as a utility would be interesting. Open notebooks to support open science still require people to identify themselves as non-attributed comments are not allowed. So even in an open work you need identity. The interplay between trust and privacy is an interesting research topic. Trust is very much based on reputation. In order to make a comment you need to say who you are or it might be enough to know that you are a doctor. People can desire a degree of privacy or even anonymity when dealing with public/searchable situations. But, at the same time, these people may have a need to at least partially identify themselves in order to benefit from their reputation. It's a kind of gradation from completely anonymous to a level of being recognisable as a user of the system with others not knowing who you are and then the grade goes up to full disclosure and access to photos, articles etc. Does there need to be an identifier? Should it be trackable rather than traceable? There is the issue of trying to protect yourself as a user from the other users as much as from the system itself.

Do trust and privacy bring responsibility? – what are the responsibilities that users have and what are the responsibilities that they may be given (eg with credit cards)? What is it reasonable to expect them to provide and how does that discussion/negotiation take place? Is it simply Terms and Conditions that flash past on a glossy website?

3. Ideas to be taken forward

The key outcome that emerged from the discussion was agreed support for the follow-up meeting.

The event would cover three days (two half days with a full day in the middle) with two main themes – trust and trustworthiness - which could also be presented as assurance and perception – interspersed with breakouts, presentations, case studies that feed into the bigger picture.

So, a user-centric approach and information assurance approach, both focusing on ITaaU, with some scenarios running through them which become a focus for breakouts. Every hour there would be a pitch on some interesting issue and participants then go back into the breakout to discuss and feed it back in.

Overarching question: Is there a role for utilities in the digital economy.

What do you see your role as a utility in the e-world? What are the security issues?

March was identified as the most suitable time for the event. The target audience would be large, small and medium enterprises, researchers from the social sciences, psychology and IT. Researchers from Birmingham and Loughborough should be invited as well as other institutions, and the legal aspects covered too. Plus utility/privacy companies and suggestions were the Post Office, Tallis, Cassidian, GE, Liberata, IBM and Siemans.

Next steps were identified as:

- Landscaping of where the research is going on in the UK
- Further literature survey
- Further investigation of the topic through a few studies, to be completed before the event to enable participants to arrive fully briefed
- Draft structure for the event
- Target list of sessions

4. References to note / follow up

Examples of the utilities the network might explore: http://openidentityexchange.org/

Trilateral Research and Consulting - trilateralresearch.com - a niche research and advisory consultancy bringing together strategy, technology and policy. It specialises in research and the provision of strategic, policy and regulatory advice on new technologies, privacy, trust, risk and security issues