SMART CITY, LARGE CITY, CHALLENGES FOR PROTECTING THE CITIZEN AND HIS TELECOMMUNICATIONS

SCOTT W CADZOW
Cadzow Communications Consulting Ltd
Email address: scott@cadzow.com

Abstract. These instructions are intended to guide contributors to the *Visual and Spatial Reasoning in Design Conference* when preparing papers. The abstract is in 10 pt Times with 11 pt leading.

1. Introduction

Very large distributed systems that aim to offer natural interaction with their human users fail to address the everyday nature of trust and its establishment at their peril. In human interactions trust builds slowly, it builds contextually, and it builds by association. In contrast most software systems make assumptions regarding user behaviour and do little to learn at the natural pace of the user, this leads to an unnatural relationship between the user and the software, system or service they are using. When the system they are using is also the one they live, work and play in, as is envisaged for the smart city, then failure to protect the citizen from the system, and the system from the citizen, could lead to collapse of the relationships needed between city and citizen that are critical in making a city work.

2. Security and privacy

When security experts are asked about protection they often, too often, think in terms of cryptograph and the advantages that can bring in proof that security solutions work. The cycle of conventional good security work is shown in *Figure 1* where the aim is to identify risks or threats to the system, and sequentially prevent them, make preparations if the threat is enacted and respond to that scenario. Quite properly this cycle has a pessimistic view of the world – no matter what we do in identifying and preventing bad things

we will be affected at some point. These are all activities, i.e. things we need to do to assure ourselves that something is secure.

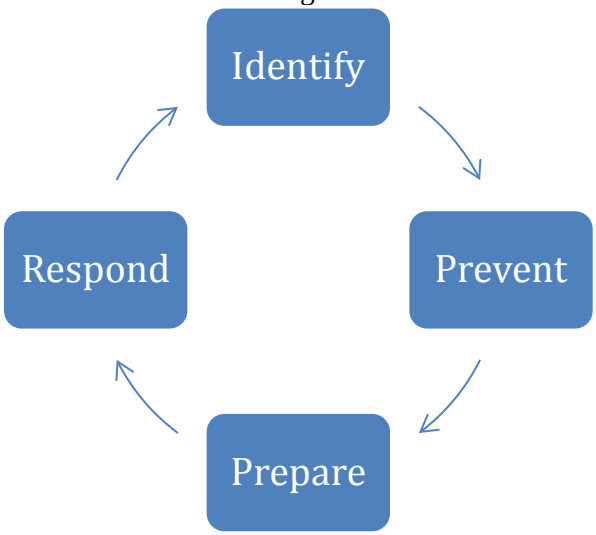

***Figure 1*: The security cycle**

Where security experts take a mostly negative view of the world the general public is remarkably positive about how they interact with the world both real and virtual. However the positive view can very rapidly become negative if and when someone suffers identity theft, a virus infection, or even a simple component failure. Part of the problem is complexity: Modern ICT systems are massively complicated and the point where the human being sits is often at the end of a very long chain. When we consider the complexity of protecting the user we should very simply and crudely consider the number of variables we have to have control of and taking the factorial of them. So a system with say only 4 variables has a complexity measure of 24, adding just one more variable takes this measure to 120, adding 2 takes it to 720 and so on. We can think of many ways to consider complexity but the simple rule is that the more there are the more complex is our control of the system and the greater the likelihood of missing something (identifying ways of controlling and eliminating 24 problems is obviously less error prone than controlling and eliminating 120).

Security experts in general also try and consider ways to simplify a system to one that allows them to solve only 4 problems:

1. Confidentiality
    a. Ensuring that data transmitted by Alice to Bob can only be seen by Bob
    b. Conventionally provided by encryption across open networks

2. Authority
    a. Ensuring that if Alice is trying to do something that she actually is allowed to
    b. Enabled by a large number of techniques including Access Control Lists (list of identities allowed to access the system), and various access control schemes based on identity, role, consent, trust, location. Many are managed by policy control engines.
3. Integrity
    a. Internal consistency or lack of corruption in electronic data
    b. Ensuring that changes to the system can be identified
    c. Often provided for data using cryptographic hashes
4. Identity
    a. Ensuring that Alice is really Alice and not Bob pretending to be her
    b. Often achieved by Identity Management infrastructures and strong authentication

There is an impact of applying these measures – they change the system and that has to be factored in too. In other words how do you protect the system from the changes imposed by the protection?

In addition many security measures are privacy negative. What this means is that in order to provide strong proof of identity you may need to declare additional private information, e.g. there are more than 2 Alices in the world, so how do we distinguish good Alice from bad Alice? Or from the other good Alice? Similarly, to determine authority this may be dependent on your physical location, e.g. are you allowed to make an international phone call from your current location?

It is also worth noting that these words as applied by security experts are slightly adrift of normal, particularly literature based, interpretations. For example Killinger (Killinger 2010) states that "Integrity is a personal choice, an uncompromising and predictably consistent commitment to honour moral, ethical, spiritual and artistic values and principles." For a network or machine system to demonstrate integrity of this nature is quite different from simply expecting it to be “whole” when measured against a known state of being whole.

3. The role of trust

Trust is a complex concept but one that we grow into as human beings such that it becomes instinctive. The translation of trust to machines and machine based decision making is not straightforward. Furthermore like many other

things in the ICT domain words from natural language like trust have a different meaning or degree of interpretation.

Of course trust in human relationships breaks down so let's not expect to be perfect in the machine world too – but at the same time let's not accept failure as part of our goal.

At the root of trust is communication and in the 21st century communication is often remote through the telecommunications infrastructure. As we evolve in our environments the smart city and how citizens interact with it will become more and more critical in the development of a trusted environment. Furthermore as ICT becomes inseparable from social contact the reliability, security and safety afforded by the infrastructure becomes the underlying root of societal trust. So how does the underlying security provision of the telecommunications network support the security expectation of its users, and how does the capability of the same underlying telecommunications network map to the communications modes of people in their social context? Where there are gaps how are we filling them? Can workarounds be avoided and added to the core as capabilities? If social requirements are provided in the core can they adequately address trust?

4. A smart city primer

What distinguishes a smart city from any other city? Caragliu et al considered that a city can be defined as 'smart' when investments in human and social capital and traditional (transport) and modern (ICT) communication infrastructure fuel sustainable economic development and a high quality of life, with a wise management of natural resources, through participatory action and engagement. (Caragliu et al. 2009).

Smart cities can offer services to their citizens, and allow contributions from their citizens, in ways that some may suggest we always should have been able to. Feeding information on what to do, how to do it, where to do it, how to get to it, how to integrate one activity with another, can all be enabled in a smart city. For example if you want to solar enable your building you can ask for data on the solar power potential (this is being addressed in the SUNSINE project), if you need to access a building and are wheelchair bound then the smart city should be able to guide you (this is being addressed in the i-SCOPE project). Citizens should also be able to contribute and this is being looked at for sound mapping (in the i-SCOPE project) and at transport congestion (in the i-Tour project).

Big cities offer such a mixing pot of cultures, activities and opportunity that effective communication is essential. This covers a huge gamut of capabilities: ITS for effective movement of traffic; Smart advertising; Smart lighting; Crime prevention and detection; Citizen safety; In-building

mapping; Street mapping; Support to visitors; Support to residents; … and the list could be endless. In making smart cities effective we also need to make then inclusive and this needs to address how the user makes use of the system. A city cannot afford to discriminate against (say) iOS users in favour of Android users, or have some services available only to smartphone users, similarly it can't afford to favour use of expensive connectivity and discriminate against those who can't afford it.

The aim in smart city therefore is to bring technology infrastructures to bear that aim at improving quality of life for the citizens.

5. The role of telecommunications in addressing privacy and security

The challenge we need to address is making sure that Telecommunications as infrastructure is able to meet our evolving needs for communication. Part of the new world is the requirement to ensure that the city and its citizens become part of a mutual trust and respect community. Technically this is not an insignificant challenge but is being slowly considered and developed in the security community through a number of developments that include the following:

1. Trust Based Access Control
    a. Developed within the iTour project as part of the aim to ensure that recommender systems can be trusted to give some level of authority to recommendations made on websites, events, locations.
    b. Non-cryptographic measure that builds up over time, ensures some form of prior relationship is established to give greater trust in any recommendation made.
2. Pseudonymous authorisation
    a. This is the basis of the ITS work being done in ETSI and allows services to process data and requests from unknown parties with authority granted by mutually trusted 3rd parties.
    b. The serving processor cannot gain knowledge of the true identity of the requestor other than through collusion with multiple 3rd parties and this is inhibited by the nature of the relationships between the parties
3. Consent Based Access Control
    a. This is an approach that is being developed in the i-SCOPE, SUNSHINE and i-Tour projects that takes an Obligation of Trust protocol and considers the privacy obligation for non-repudiation, in other words prove you have/had consent for holding and processing my data.

The aim in smart city therefore is to bring technology infrastructures to bear that aim at improving quality of life for the citizens.

Smart city represents a significant rethinking of the role of ICT as part of the infrastructure of cities. For city planners this means that power, transport, water are no longer the infrastructure but share that infrastructure with ICT. For a city to serve its citizens the way in which this extended infrastructure brings trust and integrity, in a human way, is critical.

The technologies being explored in the EU FP7 projects i-SCOPE and SUNSHINE should go a long way to building that humanity into the smart city. What this may mean is that we no longer think about ICT as discrete technologies or as "the internet", or "broadband access for all" but as a framework for building society and binding societies together.

Whilst provision of water to all households improved the health of nations, and the distribution networks for gas and electricity have improved the comfort of all, so the next (r)evolution will be in making ICT work alongside these traditional infrastructures to make a new bonded infrastructure. Thus ideas such as smart metering, smart generation will work for all.

6. **Conclusions and future work**

As stated above the smart city represents a significant rethinking of the role of ICT as part of the infrastructure of cities. For city planners this means that power, transport, water are no longer the infrastructure but share that infrastructure with ICT and work to have that infrastructure build societies for people to live, work and play in.

Acknowledgements

i-SCOPE: *The project has received funding from the European Community, and it has been co-funded by the CIP-ICT Policy Support Programme as part of the Competitiveness and innovation Framework Programme by the European Community (http://ec.europa.eu/ict_psp), contract number 297284. The author is solely responsible for it and that it does not represent the opinion of the Community and that the Community is not responsible for any use that might be made of information contained therein.*

SUNSHINE: *This project is partially funded under the ICT Policy Support Programme (ICT PSP) as part of the Competitiveness and*

SMART CITY, LARGE CITY, CHALLENGES

Innovation Framework Programme by the European Community (http://ec.europa.eu/ict_psp).

References

Caragliu, A; Del Bo, C. & Nijkamp, P (2009). "Smart cities in Europe". Serie Research Memoranda 0048 (VU University Amsterdam, Faculty of Economics, Business Administration and Econometrics).

Killinger, Barbara: 2010, *Integrity: Doing the Right Thing for the Right Reason*. McGill-Queen's University Press. p. 12. ISBN 9780773582804. Retrieved 2013-10-15.

Links

iTour: http://www.itourproject.eu

i-SCOPE: http://www.iscopeproject.net/

SUNSHINE: http://www.sunshineproject.eu/