Detecting the Infringement of Personally Identifiable Information of the Elderly

Rebecca Rogers [1], Edward Apeh [1], and Christopher Richardson [1]

[1]Faculty of Science and Technology (SciTech),
Bournemouth University,
Poole House, Talbot Campus,
Fern Barrow,
Poole BH12 5BB
{rrogers1, eapeh, cjrichardson}@bournemouth.ac.uk

Abstract

Socio-technical systems are generally designed to be functional and easy to use by a cross-section of society, including the elderly. The elderly, by their nature, are physically, emotionally and financially vulnerable and are therefore more susceptible to be exploited. This makes the socio-technical systems that are designed for their use, and through which their personal information flows, highly attractive to hackers and fraudsters. Much work has been done in designing socio-technical systems so they are functional and easy to use by the elderly. However, very little work has been done to secure the data that is collected, processed, stored and transmitted by these socio-technical systems. Using human factors approaches, this paper proposes a complex socio-technical system for monitoring, tracking and the early detection of the infringement of personally identifiable information of the elderly. In particular it uses personas to describe the interaction between the elderly and these complex socio-technical systems, with the goal of highlighting the problem of data loss and misuse. It also analyses and presents how the proposed system monitors, detects and reports the infringement of personally identifiable information using soft systems techniques.

Keywords: human factors; soft systems methodology; vulnerability; elderly; digital watermarks

vulnerable not just in terms of their physical frailty but also as an easy target for exploitation and fraud. Furthermore, not only is their data vulnerable when it is in their ownership, this vulnerability increases when it is shared or transferred across the socio-technical systems they interact with. For example, there have been several reports about the data of elderly members of society being stolen, lost or misused including incidents of Doctors sharing clinical notes via whatsapp [6], USB device with unencrypted data lost by health service provider employee [7] and a Laptop with unencrypted patient data stolen from a GP [8]. If these recent reports of elderly data misuse and abuse is anything to go by, the collection and sharing of their data is not treated with the same level of care that is required for a highly valuable and vulnerable information asset.

This paper uses human factors techniques to describe the problem of elderly personal data infringement and proposes a solution by way of digital watermarks for tracking the personally identifiable information of the elderly and early detection of the infr [(f)7(o)-Dnm8(crs)5(et)3rDetrD-12(o)-7-12(p4 t)-12(l)]TJ 0TJ -0.001 Tc(g(i)-5i(hl)-

3. The flow of personally identifiable information of the elderly in socio-technical systems

Typically, the first point of contact for the elderly tends to be agencies such as, banks, health care providers, government agencies, etc. who collect and store the information within a secured information infrastructure. Such agencies are regulated by way of policies and procedures for governance, risk and compliance which they are required by law to adhere to. However, the need for information sharing for collaborative reasons, which is facilitated by modern society's infrastructure, tends to lead to sometimes unintended sharing of data. This inevitably puts the data in the hands of perpetrators of fraudulent activities. In order to represent the complex socio-technical problem, I have used a rich picture

- Points where information could be shared with organisations or entities which fall outside the trusted primary group.
- Threats from external fraudsters, intent on accessing the personally dentifpable information and using it for criminal purposes.

Furthermore, it cae seefrom the ricicture in Figure 1, that information tends to be duplpcated and shared frequently wpthin the inner circle of trusted organisations. While the data is being shared within this trusted inner circle, it-8( ) ps often possible to track and montor the information, however more and more frequently it-tends to find its way to individuals or groups for whom the data was not originally intended, the outer circle (or untrusted organisations). This could happen for a variety f reasons and is often a necessity due to, for example, care needs of the ind8( ) pvidual. All to8( ) o frequently the information move into the outer circle due to bad information magee where ind8( ) pviduals within thes e trusted organisations use personal devices and accounts to share the information. Once outside the trusted inner circle, where it-is harder to track and monitor its use, it-ps used by unscrupulous and untrustworthy parties to target the indivdual, most often for some form of financial fraud.

3.1 The elderly Persona in the socio-technical system

As shown in the rich picture, the elderlypersonas in a socio -technical system tend to share information in a socio-technical system for various reasons with well-established and trusted entities such as family, healthcare providers and financial institutions. Ths personal pnformation is then collected, processed, stored and shared as necessitated byhe social needs (e.g. healthcare) of-the elderlyersonas. There is therefore a high level of trust at this-point of interaction with the socio-technical system. Appendix A provides an example of-a tyical elderlyersona.

- keep it secure;
- ensure it is relevant and up to date;
- only hold as much as they need, and only for as long as they need it; and
- allow the subject of the information to see it on request.

Appendix B provides an example persona of a person working within a trusted organisation who strives to adhere to the rules outlined in the Data Protection Act and is overseen stringently by the Information Commissioners Office.

3.3 Un-trusted persons within the socio-technical system

It can also be seen from the Rich picture in Figure 1, that there are instances where information is shared with parties who require the information in order to undertake required tasks for the elderly but who fall outside of the known, approved and trusted group of organisations. It is this point that the risk of data loss and infringement is at its highest.

Appendix C provides an example persona of a person working within a perceived un-trusted organization who may have less control over the storage and use of its data and potentially does not have the resources to fully adhere to the Data Protection Act.

3.4 The data states of personally identifiable information of the elderly

The personally identifiable information of the elderly can be secured, monitored and tracked through the various stages of data states, i.e. data in use (process), data at rest (storage) and data in motion (transfer) [10].

Data is usually collected and used by organisations to perform a required task or for the purpose of meeting an obligation. In the case of the elderly, this could be the dispensing of drugs based on the diagnosis obtained from test results or identifying the course of physical therapy based on the information collected during a visit to a hospital after a fall.

Data security techniques such as encryption can be used to secure this data however it typically needs to be decrypted in order to be processed. If the receiver of the data has the encryption key, their systems tend to suffer performance issues in the decryption process and if the key is not available to the recipient of the data, it is virtually unusable. For example, if a ciphertext is incorporated in a socio-technical system such as a healthcare database application some of its features such as search, sort and index functions become inefficient without additional advanced keyword search schemes in place [11]. This highlights the problem of the balance between security and performance [12]. Custodians of personally identifiable information of the elderly tend to therefore be reluctant to encrypt personal data unless perceived as absolutely necessary. This also applies to other data hashing security techniques such as digital signatures as well as security mechanisms such as defense-in

These strong security approaches have the same effect on data at rest on which information is stored on file servers and information repositories such as exchange servers. Moreover, while security techniques like encryption can make it difficult for stolen data to be accessed, using these strong security techniques do not help in determining the point at which data has been infringed particularly in the case where information sent between trusted entities is intercepted by an untrusted entity.

Digital watermarking can however be used to monitor and track data in motion i.e. data sent over networks as well as data at rest and in use.

A digital watermark is digital data that can be embedded into all forms of data [14]. Special software is available for embedding imperceptible information via subtle changes to the data of the original digital content. Digital watermarks can be easily detected and read by computers, networks and a variety of digital devices, thus facilitating data tracking and actions surrounding that data.

Because digital watermarking is a passive protection tool, i.e. it just marks data, but does not degrade it or control access to the data, it is therefore necessary that it is used in conjunction with other data protection techniques such as encryption, IPsec, digital certificates, digital signatures, etc. when the data is transmitted to un-trusted personas.

For the purpose of this paper, digital watermarks provide a mechanism for monitoring and tracking the data as it moves from within the trusted circle to its fringes. This ability of the proposed system to monitor and track the data within the trusted circle allows for the efficient operational functionality and accessibility of systems without the bottleneck that would otherwise be caused by intensive security of data such as excessive encryption among trusted personas.

This feature also allows for security protection techniques that affect the operation of socio-technical systems to be applied to the entities at the fringes of-and-beyond the trusted circle. This will mean, for example using the rich picture in Figure 1, that the encryption and security at the point of transmitting data from a primary healthcare provider within the trusted circle to a third party care provider at the fringe of the trusted circle would be stronger than the data when it is transmitted from the elderly person to the primary healthcare arena.

4. The proposed system for tracking and early detection of elderly personal information infringement using soft systems techniques

The previous section used situational awareness by way of personas to describe the problem space for the early detection of the infringement of personally identifiable information of the elderly, this section will present the proposed system using soft systems methodology.

4.1 Root definition

To assist in reducing the complexity and in the identification of the areas of concern of the proposed system for early detection of the infringement of personally identifiable information of the elderly a root definition is stated below. Hicks [15] states that a root definition should be ‘a concise verbal description of the system'. Checkland and Scholes state that it should ‘express the core purpose of a purposeful activity system and express the core or essence of the perception to be modelled [16].

‘A system to monitor, track and report on the transmission of the personal identifiable information of the elderly by means of digital watermarking and appropriate levels of data encryption in order to increase the trustworthiness of socio-technical systems amongst the elderly.’

4.2 CATWOE

Furthermore, to provide a deeper understanding of the problem space the CATWOE elements of the root definition are provided below.

C ‘customers’: The elderly person whose personally identn.(xp)-12(u1)-7(d0)prwa1(r)-d (C ‘)o(o)-7(v(id3(r)-

describe the proposed system for early detection of personally identifiable information of the elderly.

Figure 2: Conceptual model of proposed system for detecting infringement of PII of the elderly

The conceptual model highlights the data flow from its initial input into the system to its being watermarked, stored and transmitted to trusted and non-trusted entities. It also highlights the increase in strong security as the personally identifiable information is shared from trusted to non-trusted entities. The conceptual model also highlights that the system is adaptable in that the defined trust parameters can be changed and updated based on feedback from the alerts received from the data custodians if infringed by an otherwise trusted entity.

5. Conclusion

This paper, using human factors techniques has proposed as system to identify the infringement of the personally identifiable information of the elderly.

In order to do this this paper has critically reviewed the benefits of addressing socio-technical problems in particular the need to align security with the inherent functionality and usability of these systems. Also it has; analysed the usability techniques of elements of its performance around the concept of security; conducted situational awareness by way of personas to show the user experience of certain types of entities that interact with the proposed system; applied soft systems methodology to analyse real world situations for the proposed system, i.e. the complex interaction between the elderly and the socio-technical systems that host their personally identifiable information.

There is still much work to be undertaken in increasing the trustworthiness of socio-technical systems used by the elderly, in particular there is a need for awareness especially as the elderly population is on the increase. In particular

their per(s)3(o)-7(n)5(s)2-3(ll)-12(y)5(id)-7(e)-3(n)512(f)7(ia)-3(b)-7(le)-6 inirpe25 0 i5

References

1. Andreas Holzinger, Kizito Ssamula Mukasa, and Alexander K Nischelwitzer, "Human-Computer Interaction and Usability for Elderly," , Berlin, 2008, pp. 18-21.
2. Alan F Newell, "HCI and older people," , Leeds, 2005, pp. 29 -30.
3. Mirja Kalviainen, "Elderly as content providers in their everyday life supporting services," , Helsinki, 2012.
4. Sri Kurniawan and Panayiotis Zaphiris, "7th International ACM SIGACCESS conference on Computers and accessibility," , Newyork, 2005. [Online].

051.213 Td (3.)Tj 11.08 Tf 0 Tc 0 Tw 0.747 0 Td ( )Tj /231 1 Tf 0.007 Tc 0.49 Tw 0.64 9.58Td [(M)3(i)5(65(K)

APPENDICES

Appendix A – Typical Elderly Person Persona

Muriel is seventy-nine years old and has enjoyed a lengthy, healthy retirement

Appendix B - Persona of a person working within a trusted organisation

Chris a General Practitioner for the NHS, he accesses his patients' data as and when they come into the surgery. Also, he refers patients to other healthcare services and providers both in the NHS and privately. In doing so Chris must share certain personally identifiable information.

Information that Chris has immediate access to on his system are:

- Patients

Appendix C - Persona of a person working within an un-trusted organisation

Clair works for Care, a private care agency who provides a variety of support to people in their own homes. Clair works for a variety of clients, some who employ Care directly and some whose care is commissioned by local authorities. Care is registered with the Care quality commission who regulate and inspect it.

Care holds personally identifiable information on 2,000 individuals such as name, date of birth, address and it also includes data regarding their personal care plans, medication, key safe codes. Most of this information was obtained from the social care agencies who commissioned them on behalf of the elderly people in the community in need of assistance and much of the information regarding their health issues came directly from GP's.

Clair uses a laptop as well as paper notes when visiting her clients to keep abreast of their changing health needs. Updates to client information is fed back through the social care channel to hospitals and GPs. Clair also liaises with therapists and other medical professionals regarding clients day to day care needs.