Security, Trust and Privacy – A New Direction for Pervasive Computing

JAMALUL-LAIL AB MANAN¹ MOHD FAIZAL MUBARAK¹, MOHD ANUAR MAT ISA¹
¹Advanced Information Security Cluster, MIMOS Bhd,
57000 Technology Park Malaysia, Kuala Lumpur, MALAYSIA.
{jamalul.lail, faizal.mubarak, anuar.isa}@mimos.my

ZUBAIR AHMAD KHATTAK²
²Universiti Teknologi PETRONAS, Department of Computer & Information Sciences,
Toronoh 31750 Perak, MALAYSIA
zubair_g00953@utp.edu.my

Abstract: -Information which used to be privileged only for the rich and powerful few has become crucial part
of our life. Everyone is now very aware of the need to protect sensitive and valuable information from
unintentionally being presented to other individuals or organizations. In the open environment such as the
internet, there are suspicious individuals with insincere motives who are cautiously trying to get personal gain
or trying to meet political propaganda. Clearly, there is a need for a framework for data to travel uninterrupted,
unchanged and unseen by unscrupulous recipients. This framework should address issues in security, trust and
privacy in a unified form. We present our proposed framework in a holistic approach. This paper discusses the
global phenomenon of information security divide, major security, trust and privacy (STP) challenges, related
works by past researchers and the proposed STP framework. The Framework, when implemented in pervasive
computing environment would address how sensitive personal data could travel uninterrupted, unchanged and
unseen by unscrupulous recipients.

Keywords: - Security, trust and privacy, Unified Framework

1 Introduction

Information which used to be privileged only for the rich and powerful few has become crucial part
of our life. Everyone is now very aware of the need to protect sensitive and valuable information from
unintentionally being presented to other individuals or organizations. In the open environment such as
the internet, there are suspicious individuals with insincere motives who are cautiously trying to get
personal gain or trying to meet political propaganda. Clearly, there is a need for a framework for data to travel uninterrupted,
unchanged and unseen by unscrupulous recipients. While we do not have any Framework that address
security, trust and privacy, we should develop it now so that future services can be rendered to users
with confidence.

In a future scenario whereby any two devices that communicate over the public untrusted networks,
they are bound to face security, trust and privacy issues. Questions such as the following will have to
be addressed:

Users:
• Do I know enough of this user? How does he/she use any mechanism to secure
credentia(l)s, so that I can trust him/her?
What application(s) do I allow him/her to have access? Which privacy policy does
he/she use?

Servers:
• Which and what type of server I am connected to? Is the server security enabled and trusted? Is there any trust or
privacy mechanism in place in the server?

Trusted Third Parties:
• Is the trusted third party for this application behaving correctly and security compliant? Is there any corporate privacy
compliance adopted by this third party?

Systems architect, engineers, designers and developers constantly review these questions
because they are still struggling to create a secure, trustworthy, and privacy preserved environment for
us to do business, transactions and collaborations. In the case of security, we need to address
confidentiality, integrity and availability issues. In the case of trust, we need to make sure that the
platform that we are working on and the communication channels are indeed trusted. In the case
of privacy, it is crucial to protect sensitive and
valuable information from being handed over to unintended individuals with insincere motives. Recent advances in networking, handheld computing and sensor technologies have driven forward research towards the realisation of ubiquitous computing (variously called pervasive computing, ambient computing, active spaces, the disappearing computer or context-aware computing). These advances have led to the emergence of smart environments with that is extensively equipped with sensors, actuators and computing components [1] as well as the need to consider other factors such as security, trust and privacy in critical and sensitive sectors such as financial services[2] and business transactions. [3] Most of existing security solution does not cater for trust and privacy protection. This lead to the ever growing and most unresolved problem of lost and leakages of personalised and dynamic data that contributes to the security and privacy problems. Unfortunately the manner of tracking, collection and analysis of these personalised and dynamic data by bad guys will not be obvious or active. Hence, the potential for collection and misuse of information is massive. To resolve these issues, guidelines have been produced. [4]

As shown in Figure 1, today’s security solution is still non-unified in dealing with STP issues. Many solutions address issues in silos, perhaps because of STP complexities, non-compliance to international standards or gaps within these standards still exists, such as identity management and privacy. The effect is non-unified compliance layers within the solutions. There are also other areas not fully covered, under international regulatory and legal framework. Hence, Service Providers, Collaborators and Trusted Third Parties are not able to work in harmony to bring about the confidence in using services in the open environment such as the internet.

Figure 2 shows the Defence In-Depth Solution of today’s technologies that address STP issues. In general, STP issues are mitigated in silos, non-unified approach and focus very much at the server and network infrastructure level. Very little has been done to protect user identity, data and platform. The Defence In-Depth has been skewed towards service providers and computing hardware and software providers. We are going to face with future which is even more complicated involving irregular policies between cross border countries, more variants of devices, sophisticated trust relationships, complex ownership relationship, and with multi-facet user composition. It is thus the intention of this paper to highlight the significance of a STP framework.

It is the intention of this paper, to present a more balanced STP Framework that provides basis that caters for user needs, such as user identity, data and platform protection.

The rest of this paper is organized as follows: In section 2, we present related works on STP research, and in Section 3 we propose the preliminary STP Framework and finally we conclude the paper with future work directions.

2 Related Works

Trust in online transactions is vital for the sustained progress and development of electronic commerce (EC). Chellappa [5] proposed a combination of security, trust and privacy that influence their trust in online transactions. He showed that consumers exhibit variability in their perceptions of privacy, security and trust between online and offline transactions even if it is conducted with the same store. He then developed and validated measures of consumers’ perceived privacy and perceived security of their online transactions which are then theorized to influence their trust in EC transactions.
Riguidel [6] discussed the relationship between Security, Trust and privacy in future internet which must be solved by further research. He showed that security and trust are mutually influencing each other in e-commerce, similarly security and privacy are mutually influencing. However, there is no attempt to combine all the three areas, namely security, trust and privacy together. Lakshmi Eswari et. al. [7] described the security and trust management issues, and their respective models, but no attempt to include privacy in their analysis.

In reference [8], the authors put forward the following challenges in Security, Trust and Privacy research:

- Understanding and developing privacy-friendly identity management schemes;
- Rethinking privacy and trust in future ambient environments (incl. networked sensor environments and the Internet of Things): new privacy models and information control paradigms; privacy enhancing technologies;
- New frameworks and reference architectures integrating fragmented approaches for managing personal information and for data sharing and exchange under users' control;
- Understanding how trust emerges and evolves, and the related notions of reputation formation, monitoring, evolution and management;
- Developing novel trustworthy and usable means, including trust services, that take account of the situation and context and help users make informed decisions about which information, services and systems they can trust;

From all the above discussions, we can safely say that we need an overall framework that combines security, trust and privacy. Following the early publication on Analysis of Privacy Principles in 2007, International Security Trust Privacy Alliance (ISTPA), produced another document that describes Privacy Management Framework [9] which includes a Privacy Reference Model. Huanchun Peng et. al. [10] has produced a framework with the goal of privacy promise compliance and accountability, which may help such situation before sound privacy answers may be realized. The authors have also discussed some relevant technical and non-technical components which are needed in the privacy scenario as well as some research challenges towards the implementation of the framework. Their work is our main reference in developing the proposed Security, Trust and Privacy Framework in this paper.

3 Security Trust and Privacy (STP) Framework

3.1 Overview
The main goal of this STP Framework is to fulfil the objective of combining Security, Trust and Privacy into one Framework. It is based on the assumptions that STP policies, technologies, processes and law are merged together in presenting to the users the right ecosystem that enhances STP requirements.

3.2 Scope
The scope of the STP Framework is to cover areas that will make future solutions realizable in terms of implementing user and system security mechanisms, platform trust and privacy preserving mechanisms for protecting user personal and working data. We assume that the legislative aspect of the STP Framework will also be covered in Data Protection Law and implemented in each participating countries or regions. This will include the necessary balance between STP are achieved through generally accepted principles. The scope of the R&D on STP Framework is as shown in Figure 3. As it can be seen from the figure, we need to be able to combine STP requirements in a unified manner, so that there is some kind of balance between them. In reality and practically, this means some compromising has to be done.

3.3 Objectives
The STP framework will help to support for managing and developing elements of STP technologies that will promote e-transactions, e-business, e-government and national defence in trust-based privacy-enabling ways. It will also cover the necessary STP enhanced balanced ecology for user centric e-business, pervasive and
There are three main objectives that cover technology, process and social aspects as follows:

**Technology**
To develop new STP-based privacy technologies, services and products.

**Process**
To achieve balance of current opposing requirements of STP.

**Social**
To achieve a balance between STP through laws, enhanced by assurances where possible procedures and audits where it is not.

Figure 4: Future STP Scenario
Figure 4 shows the targeted future STP scenario. Besides being able to handle STP Compliance Regulatory and Legal layers, we aim to be able to achieve STP compliance between Service Providers, Collaborators and Trusted Third Parties. Another crucial aspect is to enhance client end with STP enhanced platform, besides the necessary STP Authentication, Authorization and Accountability.

Figure 5: Future Defence In-Depth Solution
Figure 5 shows the targeted outcome of the Defence In-Depth Solution based on STP Framework. Our main target is to enhance Defence In-Depth at the client end, in line with enhancement at server and infrastructure.

3.4 High level Goals
The overall expected high level goals to be achieved are as shown in Figure 7. The Framework consists of three models, namely, Security, trust and privacy models all combined together to form a unified STP architecture. In this figure, Security Model consists of a layered model of the Security Defence In-Depth. The same layered model is applied to Trust and Privacy. Hence, a final version of the STP framework would consist of all the three models combined together.

Figure 6: Relationships between STP Systems
Figure 6 shows the expected relationship between STP systems based on the works of Zheng Yan & Ronan MacLaverty [11].

Figure 7: Holistic STP Framework
Take the special case for implementation in government services. The Government requirement should address all for STP protections when citizens perform transactions with government services. Let us discuss how STP framework would be helpful in achieving the above stated objectives. From security point of view, users need to be authenticated adequately to ensure that personal identifications (IDs) are not hijacked by hackers who would do more harm either to the person’s private data or to the entire service. From trust point of view, the client platform, host platform and entire infrastructure on which services and
applications run, must be trusted (perform according to the expected way), which means that trust foundations of trusted computing must be in place. From privacy point of view, we should review how information about citizen is handled within government services when they use information technology (IT) to collect new information, or when agencies develop or buy new IT systems to handle collections of personally identifiable information. It also involves how the system handles information that individuals provide electronically, so that the public has assurances that personal information is protected through privacy preserving technologies.

![Figure 8: Implementation Strategy for STP Framework](image)

### 4 Preliminary Studies

Our work has just started last year and we decided to focus on trying to achieve some kind of integration between STP Models as shown in Figure 8. In this diagram we decided to apply the STP concept on a particular environment, such as Analysis of Open Environment Sign-in Schemes-Privacy Enhanced & Trustworthy Approach [12].

### 5 Conclusions

This paper discusses the global phenomenon of information security divide, major security, trust and privacy (STP) challenges, related works by past researchers and the proposed STP framework. We have presented the STP concept and framework and we hope that it can be considered as a step towards implementation of a better Security, Trust and Privacy environment which is necessary in future pervasive computing. We presented our proposed framework in a holistic approach. The Framework, when implemented in pervasive computing environment would address how sensitive personal data could travel uninterrupted, unchanged and unseen by unscrupulous recipients.

### References


