Introduction to the Persona Model

Author:
Radovan Semančík

Date:
September 2005

Version:
1.1

Abstract:
This essay provides introduction to the Persona Model, that may be used to describe different identity-based interactions in computer networks. Basic ideas used to form the model are provided in this introduction as well as some of it's possible uses.

1 Introduction

The landscape of Internet is changing. Not that much on the surface that can be seen, but there are strong currents deep inside the Internet technologies. The models and other constructs used in the stand-alone computer systems are seldom applicable in a massive network environment. This short paper provides an introduction to a model, that can be used as a base for the networked identity thinking.

Only a basics of the model are provided in this document. The model is work in progress, any comments and suggestions are welcomed.

2 The Digital World

The world that a computer system perceive is very different from the world as is seen by us, human beings. The elements that we consider "virtual" are basic building blocks of computer system – data structures, processes, software modules, etc. If a computer was alive, it will consider these elements the "real things" and it will see pieces of our world (buildings, cars, etc.) as virtual entities. The computer will see the world "from the inside".

The same is true for user's of computer systems. Being a physical object, the users are virtual entities for a computer. They are not real. Think for a minute how today's computers see user's interaction with digital world: press of a key on keyboard, motion of a mouse, sound waves captured by microphone, photoelectric signals converted to pixels by a digital camera chip. Not much to make good idea of the person that sits in front of the computer.

And it becomes even stranger when it comes to determining the identity of the person. The computer see username and password that is entered on the keyboard. The computer may expect that there is "someone" who entered the password, but it cannot really determine if it is the expected human being or a monkey hitting the keyboard. The computer must compare entered username and password with something that is "real" in it's world, some data entity. And from this point on, the data entity is the thing that matters, not that physical object that pressed the keys on keyboard. The processes are executed on behalf of the data entity. New files are marked with the data entity's identifier to indicate ownership. Notification messages are shown on the screen that is associated with that data entity. Physical user does not really exist in the digital world, only his data entity is seen there.

nLight
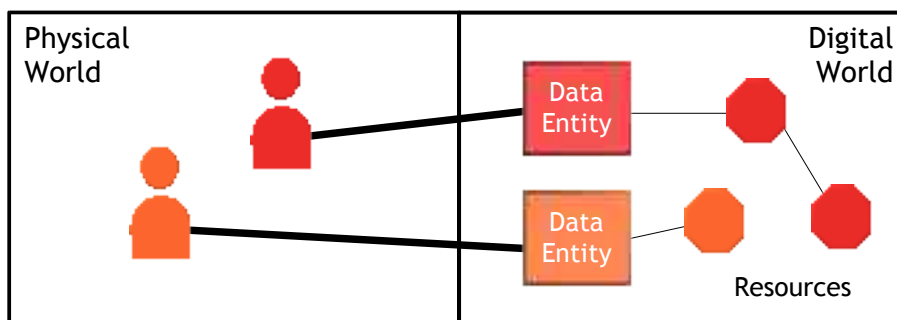
3 Persona

We will call the data entity that represent user in computer system *Persona*. The data entity that represents user in computer system usually describes some characteristics of physical person, for example name, sex or age. Persona has usually an identifier (or several identifiers) that are used to distinguish different persona instances. Being a data entity, persona may also be linked to other data entities (even to other personae), grouped, sorted, transformed or destroyed. The persona may exist only for a short time, or it may be persistently stored for a long time. It may be processed almost in any way, it's just a data entity.

The personae will be usually implemented as accounts or profiles in computer systems. These long-living persistent personae will include a mix of real-world attributes (e.g. Full Name) and digital-world attributes (e.g. home directory). But personae can be seen in other places also. Web session data entity may include a transient, short-living a possibly partially anonymous persona.

It is also expected that single user will employ several personae while interacting with computer systems. These personae may be employed in a "serial" way, for example to

Serial Persona Use
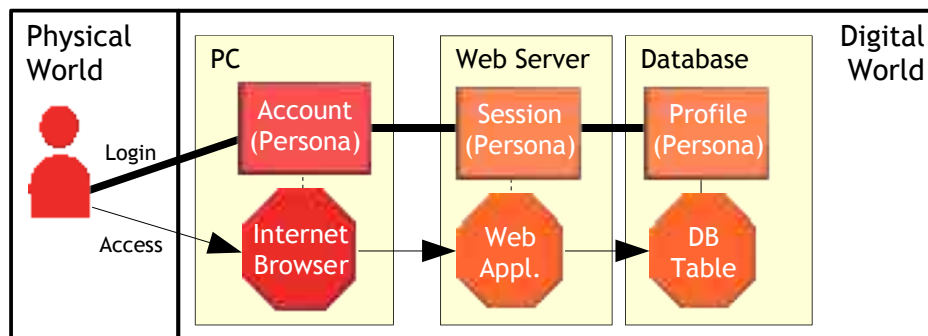
Parallel Persona Use
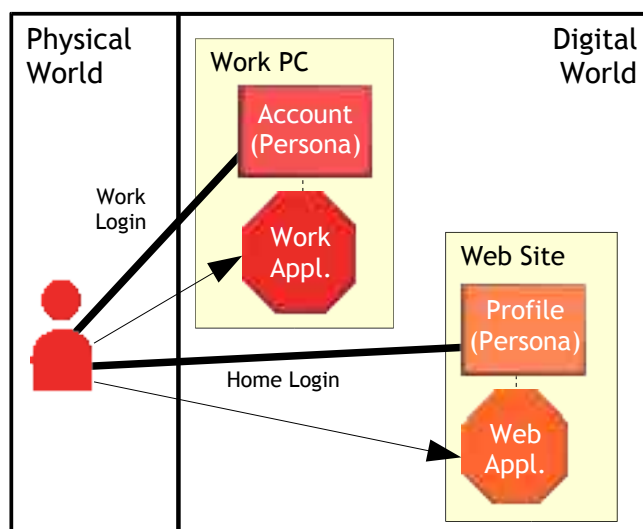
indicate different accounts and sessions used to utilize single resource. Or the personae may be used in parallel to represent different personalities or parts of a personality. For example a single user may have a persona set up for his business duties, that is used at home and yet he may use different persona to carry out his private interactions while at home. The two situations are described on following picture. The first part show a user accessing batabase-based web application using an internet browser on a PC workstation. The second part show a user accessing stand-alone application on his work PC, where login is required to run the application. And later then, while at home, the user is accessing Internet web application using his home Internet appliance. The personae are used in both serial and parallel ways at the same time in practice. It is usually required to use several personae (e.g. a PC account and a browser session) to access single resource, while a physical user may access several such resources at the same time using different accounts or sessions.

The persona may describe non-physical persons also. For example a physical person may use reality-based personae in business or when he chooses to employ his civil rights, but he may also use an entirely imaginary persona for a purpose of a computer network game. Or a physical person may choose to use "pseudonym" persona for a specific community if he wishes not to expose his real identity.

The reality-based persona of a single person and his imaginary persona may be very different. In fact, they may have nothing in common except the fact that they are used by the same physical person. But that relation is outside the digital world and may not be directly detectable by a computer system. The computer may expect two entirely different physical entities using these two personae.

4 Persona Linking

Personae can be linked to indicate relations. Two personae (accounts) in different computer systems may be linked to indicate that they belong to the same physical person (e.g. for Single Sign-On purposes). The different personae may be linked to represent membership in the same workgroup or role (e.g. for access control purposes). The personae may also be linked by a third party, for example by a party that discovered that the data in these personae are very similar and they probably represent the same user. This kind of linking may be legal and helpful (e.g. to fight fraud) or may be illegal and harmful (e.g. illegal user profiling).

The linking is usually implemented by sharing a common identifier. Both local identifiers (shared by only two parties) and global identifiers (shared by more parties) can be used to link personae. The persona linking has many implications, especially while considering privacy issues.
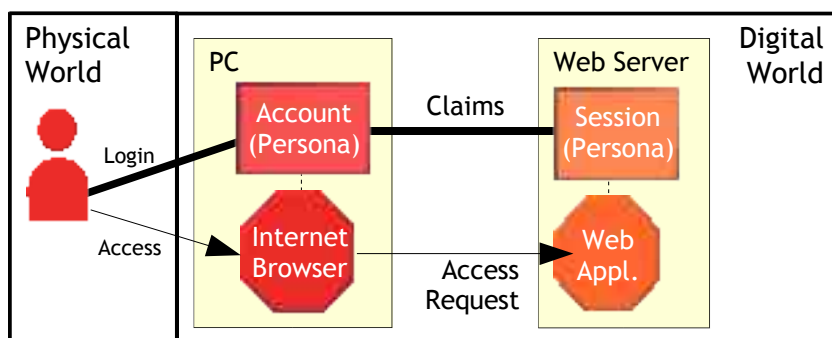
The computer system in itself has no means to determine the correctness of the data included in persona. It must believe that the data truly describe the characteristics of "the other world" or doubt it, but it usually has no means to check it. One computer system may believe in the correctness of the data in a persona more that other. The computer systems may exchange the statements about their beliefs in a form of claims, assertions or certificates and thus propagate their beliefs to other systems.

Internet applications today usually have first-hand data, entered by physical person (user) directly. But that situation is likely to change when different Single Sign-On systems and other "identity" services will spread on the Internet. In this situation only a few systems will have first-hand data about a specific physical person. Most systems will rely on claims about persona attributes issued by other systems (see following picture).

In this multi-layered situation it may not be feasible for a computer system to evaluate how well do attributes of a specific persona describe the characteristics of a physical person. The

Current Situation
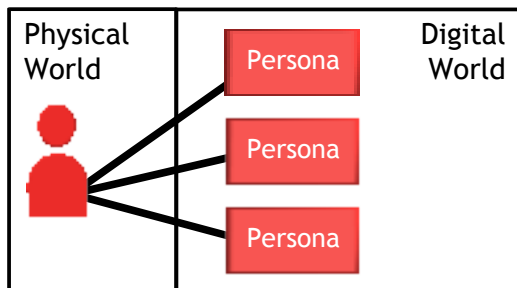
Expected Future Situation
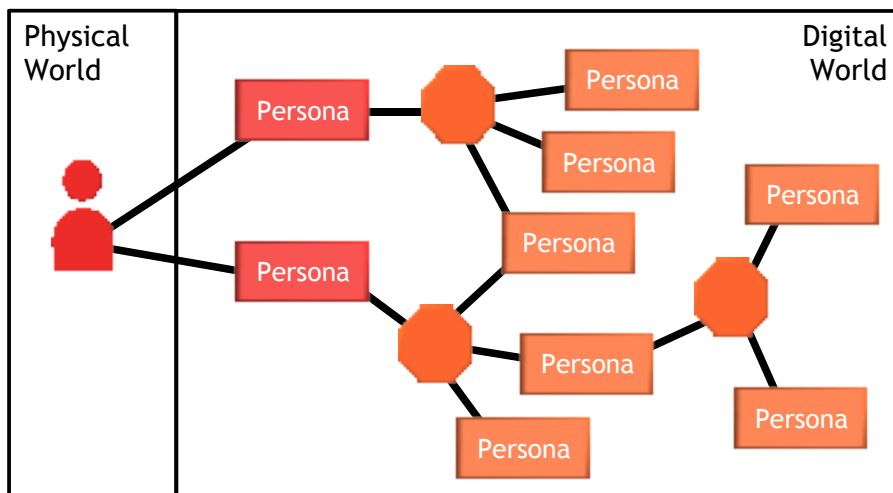
evaluated persona may be several "hops" away from the primary persona and the original claims may be transformed by "identity bridges", anonymization services, etc. And for imaginary personae (e.g. a character in computer game) there may be nothing physical to compare to. The evaluation process for a specific persona can only work with claims from neighbor systems and has to come to decision based only on that information.

5 Conclusion

The digital identity technologies are on their rise. And while we cannot foresee the scope of changes that these technologies will trigger, we expect that these changes will be significant. The simple methods traditionally used in computer security area to model user interaction with single computer system are likely to fail in the complicated network environment. We propose a base for a new model, that takes into account the distributed nature of large computer network and Internet in particular.

The Persona Model is in it's early development stage, but we expect that it may help form ideas and consider implications of digital identity technologies.