Security for a Privacy Augmented Collaborative Environment With a Combined Authentication Scheme Encapsulation

GEOFF SKINNER
Faculty of Science and IT
The University of Newcastle
University Drive, Callaghan, NSW, 2304
AUSTRALIA

Abstract: - The uptake and utility of digital collaboration’s continues to grow as organizations are realizing the diverse range of benefits they provide to not only their organization as a whole but also to individual employees. However, like many information and communication technologies the implementation push often overshadows a proper evaluation of data security and information privacy risks that may be inherent with the technology. This paper details our ongoing research for addressing a number of authentication and personal entity identification issues encountered in digital collaborative architectures. We propose an authentication framework that uniquely combines both traditional and biometric methods of authentication with an additional novel audiovisual method of authentication. Further, the CASE (Combined Authentication Scheme Encapsulation) methodology provides an intuitive privacy protecting visual representation of a member entity’s authentication methods, which is accessible by other member entities for help in assessing the risk of sharing ‘sensitive’ data with other collaboration entities.

Key-Words: - Authentication, Data Security, Information Privacy, Biometrics, Digital Collaborations

1 Introduction
The underlying focus of many of the current Australian National Research priorities revolves around the idea of collaboration. Specific to the Information and Communication technology sector involves the promotion of digital collaborative architectures. Our ongoing research and the topic of this paper is centered on digital collaborations, in particular their use and support for fostering innovation. The evolution of innovative and creative ideas represent sensitive data that needs to be protected, more so when performed within shared environments like digital collaborations. As part of our continuing funded research in this field a number of technologies have been and are being developed to ensure sound data security and information privacy across collaborative architectures.

Contained within this paper are details of two foundational components of our proposed Combined Authentication Scheme Encapsulation (CASE) methodology. Due to space limitations the full methodology and remaining parts are not included. Rather, detailed discussion in section 4 is given to our novel Traditional, Audiovisual and Biometric (TAB) Authentication framework for integration with Privacy Augmented Collaborative Environments (PACE) [1]. Secondly, in section 5, we explain our unique Graphs Representing Authentication and Privacy Hierarchies (GRAPH) collaborative application. Background and related work are reviewed section 2, followed by an overview of a PACE in section 3. Section 6 provides a conclusion and section 7 the list of references.

2 Background and Related Work
The research issues we are addressing in relation to the areas of authentication and identification are driven by international recognition, academic and commercial, of problems with current security and privacy methods for data management [2]. While recent work [3, 4] has made some progress on improved data security and information privacy in collaborations, our research is unique in its plans to use a combination of authentication methods. To date no solutions have been proposed that uniquely combine traditional, audiovisual and biometric authentication methods into a single framework. The only similar proposals to our own have been work done on Multiibiometric Systems [5] involving the use of multiple biometric devices, Webbiometrics [6] using soft biometric traits with a conventional login, and using a combination of an online signature with voice modalities [7].
The management of intellectual property within an organization [8] is another widely acknowledged problem, which becomes increasingly more difficult when organizations are engaged in collaborative activities [9]. As collaborations have shown to be highly effective means of increasing growth while saving costs for organizations [10], the members must remain conscience of the potential risks to the data they are sharing within the digital environment [11], including new innovative and creative ideas. Most current technologies are unable to provide adequate protection of ‘sensitive’ data in digital collaborative environments [12, 13, 14].

Previous research involving the use of graph representations has focused primarily on access controls and other security specific components [15] and [16]. However, recent literature detailed similar approaches to our own but only the visual representation of configurations, activities, and implications of security mechanisms [17]. The most significant similarities are the use of a ‘pie’ graph which represents the ‘Impromptu Client Interface’. Importantly, industry leaders recognize the importance of visualization and collaboration describing them as being the ‘. . .strategic enablers of the upstream enterprise’ [18].

3 Privacy Augmented Collaborative Environment (PACE)
Recent research by the author in the fields of Collaborative Architectures, Data Security and Information Privacy delivered a number of solutions for addressing privacy issues within digital collaborations [19, 20]. Inclusive to the research was the symbiotic combination of the individual components to produce a Privacy Augmented Collaborative Environment (PACE) [1] as represented in figure 1. The two foundational elements of a PACE include the PIVOTAL methodology (Privacy by Integration, Visualization, Optimization, Technology, Awareness, and Legislation) [19], and the TLC-PP framework (Technical, Legal, and Community Privacy Protection) [20]. Through the application of the PIVOTAL methodology and the TLC-PP framework collaboration owners can ensure sound data security and information privacy practices and protections that can be maintained within their digital collaborative environments. The remainder of this section explains the privacy protections of PACE and why a PACE should be used in combination with the proposed Combined Authentication Scheme Encapsulation (CASE) methodology proposed in this paper.

While the work of PACE was very successful in addressing information privacy problems in collaborative architectures it was unable to address a number of security issues related to member entity authentication and personal identification. That is, a member entity of PACE was able to manage their personal or sensitive data, such as determining which other member entities had access to their data and how it could be used. However, the data owners were not able to verify with a high degree of certainty the ‘personal’ identity of the entity requesting data.

A common problem in digital collaborations is what we term authentication theft and refers to the problem encountered in PACE. Authentication theft unlike identity theft implies that only an entity’s means of authentication are stolen. So if using traditional authentication methods an imposter would steal the username and password of a member entity known to the data owner. The imposter could then request sensitive data from a member entity data owner under a false authenticated identity within the collaboration. From a digital collaboration systems perspective the provided username and password are correct so the imposter would be granted authentication into the collaboration. But the actual personal identity is false and therefore the data owner would be providing personal data to the imposter. Therefore the privacy protections provided with PACE need to be complimented with more stringent authentication methods that include the ability to verify what we term a ‘personal’ identity rather than just a ‘system’ identity in the context of our work.

The Privacy Protecting System Development Life Cycle (PP-SDLC) was the Integration element of the PIVOTAL methodology. It used a traditional form of the system development methodology that had information privacy considerations integrated into each of the life cycle phases. A similar approach should be used when integrating the ‘personal’ identity techniques into a digital collaborative architecture. The Visualization element is termed PUG for Privacy Using Graphs. PUG is an application available to member entities that can be used to dynamically map relationships between different entities. The details on the maps represent such things their degrees of separation from different entities in social structures, methods of security for both data at rest and in transit used by each member entity and also the level of access each mapped member entity has at time of graph generation. It is proposed that a similar application
could be developed for CASE to represent the level or methods of ‘personal’ authentication each member entity has completed for their current session.

The Optimization element involved the creation of what is termed F3P for Fair Privacy Principles and Preferences. F3P uses XML technology to represent a member entities privacy preferences pertaining to items of their personal or sensitive data. Again it is possible that in future work the preferences can be extended to support data representing the methods of authentication used by a member entity. The remaining three elements of Technology, Awareness, and Legislation were closely coupled with the TLC-PP framework.

To ensure comprehensive privacy protection within a digital collaboration three foundational factors are required as embodied with the TLC-PP framework. Firstly, the collaboration must continually integrate and update Privacy Enhancing Technologies within the collaboration. This principle is just as applicable to authentication technologies. Further, the current legal requirements must be enforced by the owners and administrators of digital collaborations. As legislation may develop to govern information systems collaborations must ensure the laws are enforced in their environments. Lastly, the member entities making up the collaboration’s Community must be Aware of their privacy rights and also their privacy expectations. Therefore, as part of the collaboration’s education efforts, details of authentication procedures can also be made available and publicized to the collaboration community. The next section details the proposed combined authentication scheme that should be integrated with the privacy protection measures used in PACE.

4 TAB Authentication Framework for Collaborations

One of the key authentication contributions within the proposed CASE methodology is what we have termed the TAB framework. TAB represents a combined authentication scheme uniquely encapsulating Traditional, Audiovisual, and Biometric methods of authentication. The framework is composed of the respective three tiers of authentication that can be integrated into any digital collaborative architecture and customized to each individual situation. Depending on the collaboration’s data security and information privacy needs, in addition to the resources available, the TAB framework configuration can be modified to adapt and evolve with the collaboration.

The three levels or layers of the TAB framework and their methods of use are as follows:

- **Traditional**: in the context of our work the term Traditional refers to the more commonly available and frequently used methods of authentication that have been associated with weak levels of reliability. Traditional methods of authentication in our framework include the use of username/password combinations, Public Key Infrastructure (PKI) and Digital Signatures, Tokens, and Smartcards. In each form of Traditional authentication we classify them using the term ‘System Authentication’. As mentioned in the previous section this implies that no personal individual identification of an entity is used in the authentication process.

For example, while a username/password combination may be unique to a single entity, a malicious entity may steal the username and password and use that to gain access to the digital collaboration and its resources. From the systems perspective it does not care who is using the username and password, it only matters that the correct username and password are provided. The same issue holds true for stolen smartcards, false tokens, and malicious use of stolen private-public key combinations with PKI. The motivation for our research is in part related to this inadequate method of authentication. In particular, we are concerned on its current common use for digital collaborative environment authentication. It is imperative in collaborative architectures that involve the sharing of personal or sensitive entity data, that the owner or custodian of the data in question can verify the ‘personal’ identity of the entity requesting the data.

As part of the CASE operational guidelines, we recommend that if a digital collaboration is only using Traditional means of authentication, then either member entities are made well aware of the
potential risks to their data or the collaboration is
only used for the sharing of non-sensitive or non-
personal data. Preferably collaboration owners
integrate the whole TAB framework into their
architecture, so traditional means of authentication
can be used in combination with more ‘personally
identifiable’ methods of authentication.

Our implemented prototype uses both
username/password combinations in addition to
Biometric enabled Smartcards. The smartcards used
are Precise BioMatch Smart Card 64 which are Java
based and for operation with Precise 200MC
biometric readers. At time of writing plans are
underway to integrate a PKI and generate
public/private key combinations for use by all
prototype member entities during further testing.

- **Audiovisual**: the second tier of the combined
  authentication framework involves the use of readily
  available audiovisual equipment. The uniqueness of
  the proposed approach is in the method of
  application of the tools for their use as real time
  authentication devices. Audiovisual authentication,
in the context of our research, utilizes devices such
as microphones or more preferably web cameras to
stream live audiovisual footage of an entity, such as
a data requestor, to another entity such as the data
provider. The audio and streaming picture of an
entity can be verified against registration media of
the entity to provide real time authentication.

Verified registration media for the framework
involves the submission of a recorded voice message
of the registering entity in addition to submission of
a high resolution image of them selves. The
collaboration owners and administrators are tasked
with ensuring the authenticity and verification of the
initially provided media. An alternative we have
investigated and implemented previously is the use
of other ‘trusted’ member of the collaboration to
verify and confirm the personal identity of a new
member during registration. It would then be the
responsibility of these entities to verify and ‘certify’
the authenticity of the provided media (voice print
and digital photo) matching it with the known voice
and personal appearance of the new registering
entity.

The uniqueness of this approach is that through
the use of a simple web camera a data provider can
see, hear and interact with a data requestor at the
time of the request. Our proposal is different from
the formal biometric voice recognition
authentication method, but provides many of the
same benefits but in a more informal and real time
setting. These benefits include audio and visual
identification of an entity which provides a log or
history of interaction. That is, once the personal

identity of an entity has been seen and heard by
another entity, that information is committed to
memory. Therefore, after an initial audiovisual
authenticated session it becomes increasingly harder
for another entity to impersonate another.

Other advantages include a more personal level
of interaction in addition to the relatively low cost of
ownership for setting up the authentication
infrastructure. As digital collaborations have
benefits for all types of entities with equally diverse
financial resources, audiovisual authentication offers
a reliable, unique, and cost effective security
solution. Our prototype environment uses entry level
Logitech USB webcams and common messenger
service applications to manage the streaming of
audiovisual data. It is planned that we will develop
our own collaborative environment plug-in
application that integrates all three tiers of the
combined TAB authentication framework and will
manage audiovisual live streaming as part of its
functionality.

- **Biometric**: the third or ‘top’ tier in the TAB
  framework hierarchy is Biometric authentication.
  There is considerable literature, as discussed in
  Section 2, supporting biometric devices as being the
  most reliable form of authentication and
  identification currently available. However, in the
  three classifications used for the TAB framework, it
  also represents the most expensive and resource
  intensive to purchase, install, and manage. As such
  we have placed biometric authentication in the third
tier and recommend its use for collaborations that
manage personal or sensitive data on a regular basis.
To do envisage and encourage with our own
framework that as prices for biometric devices
continues to decrease then biometric authentication
would be mandatory in all forms of digital
collaborative environments.

The TAB framework is designed for maximum
flexibility and adaptability. Therefore, the TAB
conceptual framework does not require a specific
biometric device; rather any biometric device can be
used for authentication when implementing TAB.
With much debate in the literature on what is a more
reliable form of biometric device the TAB
framework accommodates a broad spectrum of
biometric preferences. The only requirement is that
an ‘enrollment and test’ is carried out for each
member entity. That is, when a new entity registers
to become a member of the digital collaboration
they must have their biometric information (the
template) securely collected and stored within the
collaboration. Then each time the member entity
authenticate with the collaboration their biometric
scan is tested for a match with the stored template.
In this manner the TAB framework uses Biometric authentication for both verification and identification. Our working prototype currently uses the Precise 200 MC fingerprint reader from Precise Biometrics [21] at each of the collaborations test nodes. Theses devices have a combined fingerprint and smart card reader providing all required biometric matching and smart card functionality that is securely processed within the device or the smart card.

The TAB framework is intentionally flexible in nature and design so it may be integrated with many forms of digital collaborative architectures. Rather than each tier specifying a specific method of authentication, there is sufficient scope to adjust to individual preferences at each distributed site or node of the collaboration. This conceptual approach to the design of the framework allows the implementation to continually evolve with updates in technologies and authentication processes. The next section explains how the TAB framework is visually represented in a digital collaboration so its members can determine how each of the other member entities is currently authenticated with the collaboration. The TAB framework in addition to the visual representation of the authentication methods are two key components of the CASE methodology.

5 Visualizing the CASE 4 PACE

The main contributions of this paper are the proposals and defining of two key components of the CASE methodology. That is, rather than trying to just outline the complete CASE methodology in the limited space provided we have focused on two of CASES unique elements. The first being the TAB framework proposed in the previous section. The second, and subject of this section, is our novel GRAPH (Graphs Representing Authentication and Privacy Hierarchies) collaborative application for assistance in managing data security and information privacy in digital collaborative architectures. The remainder of this section is used to explain the details of the GRAPH application including its integration into a digital architecture and its role within the CASE methodology.

The GRAPH application represents on evolution of a previous information privacy management software utility we have developed entitled Privacy Using Graphs (PUG) [1]. As PUG already provided a visual representation of information privacy relationships between entities within a digital collaboration it therefore was well an ideal foundation for adding security representations such as an entity’s method or methods of authentication. The next step was to devise a minimalist method of visually representing the three authentication classifications or tiers defined by the TAB framework. It was envisaged that the application would be used in global collaborations so a universally recognized representation was required which was also capable of conveying a number of different states within each tier’s representation.

It was decided that a set of three traffic light signals should be used, one for each tier of the TAB framework. The color of each respective authentication traffic light (green, yellow, or red) corresponds to the completeness of meeting the authentication conditions within each tier for the current session. That is, the different colored lights have analogies similar to real world traffic lights. RED: indicates that no authentication conditions are fulfilled under this tier. For example, in figure 2, the audiovisual authentication traffic light (A) is red and therefore the entity in question is not currently using audiovisual authentication, neither audio nor visual. YELLOW: indicates that only partially authentication conditions are fulfilled under this tier. For example, in figure 2 the traditional authentication traffic light (T) is yellow so the entity in question may have provided only a username and password but not completed a smart card or PKI based authentication process during this session. GREEN: indicates that all authentication conditions are fulfilled under this tier. For example, in figure 2, the biometric authentication traffic light (B) is green indicating that in our prototype the entity in question has used either finger print or iris scanning authentication processes during this session.

![Fig.2: Entity node representation using the GRAPH collaborative application for security and privacy.](image)

An additional personal identification feature we have included with GRAPH involves displaying on their graph node. Member entities at time of registration and enrolment have the option of
providing a high resolution photo of themselves which is then subjected to verification and certification for use in the collaboration. Each session when an entity authenticates with the collaboration they will have the option of making their personal identification photo available for public access on their node within the GRAPH application, in addition to it being accessible as part of their collaboration profile. The individual elements of a collaboration profile, such as the personal photo, can be configured for accessibility by other members of the collaboration. The details of this are beyond the scope of this paper due to space limitations. As part of our privacy protection design approaches the provision or even the accessibility of a personal photo is not mandatory. The entity must specifically ‘opt-in’ to provide and have their photo available for viewing by other member entities.

6 Conclusion and Future Work
The proposed GRAPH collaborative application used in combination with the TAB authentication framework can be used by member entities as a means of evaluating both the data security and information privacy risks of interacting with other member entities. Security concerns are accommodated through access to other entities authentication and personal identification methods, while privacy protections are already present as part of integrating the complete Combined Authentication Scheme Encapsulation (CASE) methodology into a Privacy Augmented Collaborative Environment (PACE).

As an evolutionary prototyping methodology has been followed since project inception CASE, PACE, and their respective components are continually being modified and improved as a result of ongoing analysis and testing. At time of writing a number of dual eye biometric iris scanners were being integrated into the PACE prototype. Further, we are currently updating a secure collaborative application that can be used for fostering and managing innovation within a PACE.

References:


