# Making A CASE for PACE: Components of the Combined Authentication Scheme Encapsulation for a Privacy Augmented Collaborative Environment

GEOFF SKINNER
Faculty of Science and IT
The University of Newcastle
University Drive, Callaghan, NSW
AUSTRALIA
Geoff.Skinner@newcastle.edu.au http://www.newcastle.edu.au

*Abstract:* - Digital Collaborations are proving themselves as ideal environments for increasing the productivity and knowledge exploration capabilities of their members. Many organizations are realizing the diverse range of benefits they provide to not only their organization as a whole but also to individual employees. The challenge in environments that encourage the sharing of resources, in particular data, is finding a sustainable balance between the need to provide access to data while also insuring its security in addition to the privacy of the entities it may pertain to. In this paper we propose an authentication framework that uniquely combines both traditional and biometric methods of authentication with an additional novel audiovisual method of authentication. The CASE (Combined Authentication Scheme Encapsulation) methodology, the name of our solution, provides an effective visual representation of both the authentication and information privacy hierarchies associated with data requests within digital collaborative environments.

*Key-Words:* - Information Privacy, Data Security, Authentication, Personal Identity, 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. In addition, related research priorities include improved data management and smarter information use which includes the protection of national information infrastructure. 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 digital architectures.

The research proposes to address and contribute to a number of important fields, particularly within the Australian Information and Communication Technology (ICT) sector. Currently Australia, like many other nations, faces a number of obstacles in not only finding effective means to encourage employees to partake in creative process to foster innovation, but also for them to share their ideas with others in a collaborative environment. To further complicate the situation a lack of suitable collaborative security and privacy controls as well as inadequate, confusing and inaccessible information on available controls contribute to employee's pessimism when contributing personal data and ideas to digital collaborations. To resolve some of these problems we have developed and continue to develop a number of solutions to improve data security and information privacy within digital collaborative architectures. Further, our solutions also make security and privacy information accessible to collaboration members presenting it in an easy to comprehend visual manner dynamically updated with each new personal or sensitive data access request.

Contained within this paper are details of two foundational components of our proposed Combined Authentication Scheme Encapsulation (CASE) methodology. In addition we include an introductory overview of new application we are developing for fostering Innovation within digital collaborative architectures. As research is ongoing at the time of writing the full methodology and remaining elements 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. Our Collaborative Innovation Analysis (CIA) application is briefly explained in Section 6. Background and related work are reviewed section 2, followed by an overview of a PACE in section 3. Section 7 provides a conclusion followed by 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 Mulitbiometric 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].

From an application perspective the utility of collaborations for smart information use has been highlighted by Australia's current National Research Priorities [19]. In addressing two main research priorities, that is, smart information use, and fostering innovation, it is a logical step to combine the two objectives in developing a solution. Further, literature and history shows that the ICT evolution is heavily linked with the core concepts of creativity which enables new technologies to emerge. Gupta [20] introduced the idea of creative knowledge networks that have the capacity to "unfold tremendous creative energy of our society by helping people dream and converting these dreams into reality by networking with other individuals and institutions." Likewise, the importance of collaboration, for our focus digital or virtual collaboration, is identified as being a valued commodity for successful innovation [21]. The authors of [21] examine the i-Land environment which is an interactive landscape for creativity and innovation. The literature identifies the i-Land application environment and educational setting as a prime example of ICT creativity and the fostering of creativity to support ICT development. Essentially, the i-Land innovation has shown that creativity is an important part of ICT development and that the evolution and implementation of ICT also has an equally significant impact on the creative aspects of information organization and in producing new innovative processes and ideas.

## 3 A 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 [22, 23]. 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) [22], and the TLC-PP framework (Technical, Legal, and Community Privacy

Protection) [23]. 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.

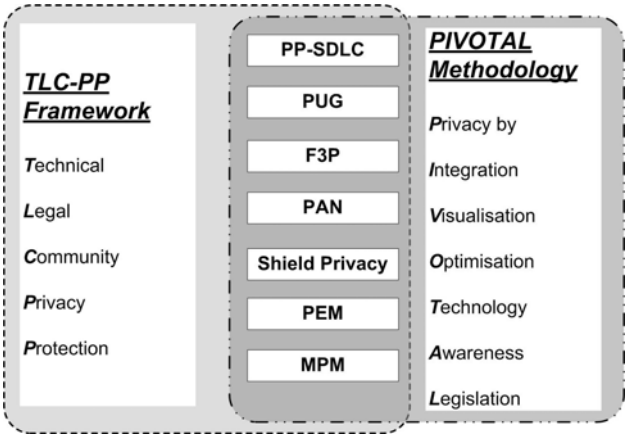

Fig. 1: PACE Components

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, access control, and personal identification. That is, a member entity of PACE, the data provider (DP), was able to manage their personal or sensitive data. The DP was able to decide which other member entities had access to their data and how it could be used. The actual physical and system controls were still managed by the host systems, but the DP if given control could make informed decisions on who SHOULD have access and who SHOULD NOT. However, the data owners and therefore DP's were not able to verify with a high degree of certainty the 'personal' identity of the entity requesting data access, the data requestor (DR).

We highlighted this as a common problem in a digital collaboration and one we have termed authentication theft in our research context. Authentication theft refers to the specific problem encountered in PACE we address within our recent work detailed in this paper. 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. That is, the imposter has managed to become a potentially valid and authenticated DR. 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 [24]. 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 authentication standards for 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 literature defines an ideal collaborative environment as one that not only at the highest level has collaborators operating as a team to achieve a common purpose by working together and gaining new insights, but also provides an additional seven capabilities. Those additional capabilities are defined as the following:

- Rapidly find the right people with the right expertise
- Quickly organize and conduct virtual teams and meetings
- Enable cross-organizational collaboration to support business lifecycle
- Build, find, and exchange information across organizational boundaries
- Deliver the right information to the right people as soon as it is available
- Provide and maintain sufficient security
- Employ technology and community standards

According to these capabilities the primary function of ideal collaborations is knowledge discovery and effective information management to ensure availability and accessibility. The last two capabilities hint at privacy protection but there is no explicit consideration or recognition of its importance. One of the main reasons for the absence of information privacy is the widely held misconception that information privacy is counterproductive to knowledge discovery.

Our PIVOTAL methodology and TLC-PP framework dispels that misconception and proves that objectives of information privacy protection, personal data management, and knowledge discovery can work in perfect harmony in collaborative environments. The result is a Privacy Augmented Collaborative Environment (PACE). Through the application of a successfully validated PIVOTAL and TLC-PP to a digital collaboration stakeholders and user interests can both be satisfied. Stakeholders can be assured that their collaboration will still provide knowledge discovery utility, while users can also be ensured that their information privacy will be protected, in addition to facilities for managing their personal data during collection and retention within PACE. The next section details the proposed combined authentication scheme that should be integrated with the privacy protection measures used in PACE.

# 4 TAB Authentication 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.

Fig. 2: A typical node in a CASE for PACE configuration with TAB authentication

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 authenticates 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 [25] 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 a single paper we have focused on two of CASES unique elements and primary contributions. 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. As GRAPH is still under development no operational screen shots are available, however figures 3 and 4 respectively show the conceptual representations of what an 'Entity Node' and what we have termed 'DEAN' (Dynamic Entity Association Network) graph will convey when produced by the completed GRAPH application.

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, as shown in figure 3, it therefore was 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.

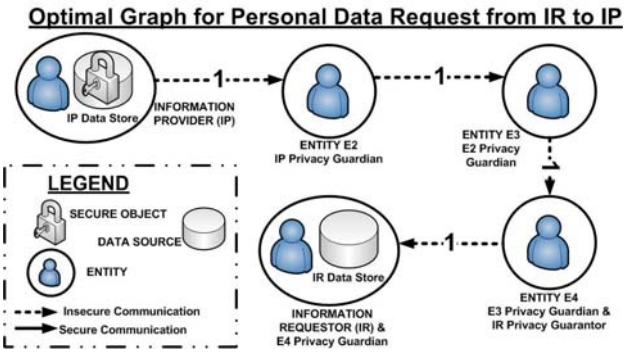


Fig. 2: Previous PUG presentation of data security and information privacy relationships

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 3 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 3, 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.

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 them selves 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 but form another important component of the overall CASE and PACE proposals. It should be noted, that as part of our privacy protection design approach, 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.

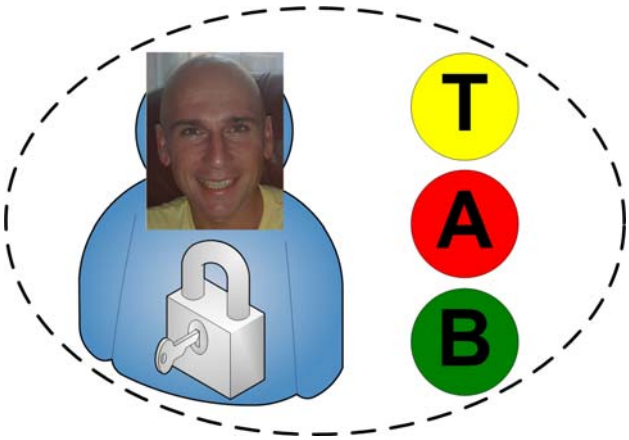


Fig. 3: Entity node representation using the GRAPH collaborative application for security and privacy relationships

As shown in figure 4 not all node entities represented in the DEAN produced by GRAPH have photos associated with them. However, like the previous PUG application we have still used a number of other visual indicators for representing information privacy, data security, and trust relationships. For example, in figure 4 dotted lines still represent insecure communications lines between entities while solid lines mean communication is secure. This simply means that data in transit from one entity to another may be encrypted, making a secure communication medium. Further, a padlock and key over the entity node implies that data at rest stored by this entity is secure; again a practice of encrypting the data while it is being stored indicates a secure data storage

node. The weightings on the graph remain as for PUG but their definitions and details are beyond the scope of this paper, refer to [1, 26].

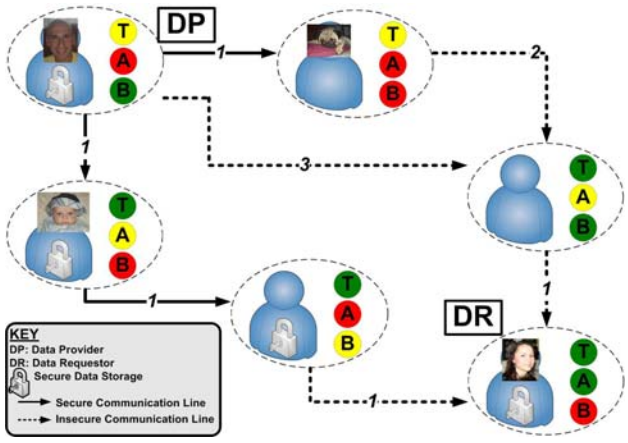


Fig. 4: Representation of DEAN (Dynamic Entity Association Network) generated conceptually using the GRAPH application

## 6 Collaborative Innovation Analysis

In collaboration with our industry partner we set out to develop and implement an application that improved the discovery and exploration of potentially latent knowledge within an organization. The application is for integration in secure collaborative environments is capable of dynamic capturing, managing and refining innovative ideas from within or from outside an organization. The challenge for the application was to promote the free flow of data and ideas between collaboration members while also protecting the privacy of the member and the security of the data they were providing. SOUP was the name of the initial prototype application. Formally, SOUP is an interactive forum for proposing ideas and gathering data on the support or critic of ideas put forward for peer review. SOUP maximizes participation by incorporating a range of mechanisms that actively encourage everyone in a collaboration to contribute. In order to avoid creating an unmanageable deluge of information, SOUP applies the rules of Darwinian evolution to ensure that only the 'fittest', most relevant ideas survive. Fellow participants are able to feed or poison ideas depending on their individual preferences. With a limited amount of food only the preferred ideas rise to the top of the soup for further consideration and development.

SOUP is an ideal concept with a number of possible uses, including many that can benefit privacy protection. Some possible functions SOUP can provide include:

- Policy Development
- Product Enhancement
- Requirements Development
- Cyber Brainstorming
- Industrial Democracy
- Inter-team Communications
- Community Consultation
- Planning
- Customer feedback and market appraising

From a privacy context SOUP has utility in a number of areas for privacy protection development. For example, SOUP can be used to assist in privacy policy development. Ideas such as what type of privacy policy should be developed, feedback or ideas from the information providers on their expectations can be gathered, and an industrial democracy can be used to elect the best privacy policy. Further, users of SOUP represent Information Providers and therefore any data they provide must be protected especially if it is personal in nature. Additionally the supporting infrastructure the application is hosted in should also be a Privacy Augmented Collaborative Environment.

SOUP has proven to be a useful application but after its initial testing period found to be inadequate in truly fostering innovation and creativity. Therefore, we have revised and updated the application with a focus on Collaborative Innovation Analysis, which is also the name of the revised application (CIA). In addition, we referred to our previous work that defined an information privacy taxonomy for virtual collaborations [27] in order to formalize the types of entities that would interact with CIA in an information privacy context. As a result the three different types of entities that may use CIA are individuals, groups, and organizations. Each entity can come together within a PACE and collaborate in the generation, review, and development of innovative ideas. Such an application is extremely beneficial to these types of entities in regions such as Australia that have limited and very competitive access to venture capital funding.

Small to Medium Enterprises (SME's) are able to come together using a PACE and combine their knowledge for the management of innovation and its evolution into intellectual property (IP). By combining their resources the SME's are able to remain competitive on a global marketplace against much larger organizations and enterprises. Further, they can be assured that with the information privacy and data security controls provided by PACE their IP will be well protected.

# 7 Conclusion

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 such as the CIA application are continually being modified and improved as a result of ongoing analysis and testing. Further work also needs to be done on completing the GRAPH application, as we need to find a better method for graph generation. Currently only a very simple method using web pages accessing a database that stores all the information the graph's use has been implemented. Also, at time of writing a number of dual eye biometric iris scanners were being integrated into the PACE prototype that need configuration..

*References:*


[1] G. Skinner, "A Privacy Augmented Collaborative Environment," Ph.D. Dissertation, Curtin University of Technology, Perth, WA, Australia, 2007.

[2] L. Kagal, T.Finin, A. Joshi, and S. Greenspan, "Security and Privacy Challenges in Open and Dynamic Environments," IEEE Transactions on Computers, vol. 39, iss. 6, pp. 89-91, June 2006.

[3] C. Yang, F.O. Lin, and H. Lin, "Policy-based Privacy and Security Management for Collaborative E-education Systems," in Proceedings of the 5th IASTED International Multi-Conference of Computers and Advanced Technology in Education (CATE 2002), Cancun, Mexico, May 2002.

[4] J.B. Spira, "Privacy in the Collaborative Business Environment," KM World, November 2004.

[5] A.K. Jain and A. Ross, "Multibiometric Systems," Communications of the ACM, vol. 47, no. 1, January 2004.

[6] H. Gamboa, A.L.N. Fred, and A.K. Jain, "Webbiometrics: User Verification Via Web Interaction," in Proceedings of Biometrics Symposium, 2007, pp: 1-6.

[7] S. Krawaczyk and A.K. Jain, "Securing Electronic Medical Records using Biometric Authentication," Lecture Notes in Computer Science, vol. 3546, 2005, pp: 1110-1119.

[8] L. Johnson, "Managing Intellectual Property for Distance Learning," Educause Quartley, vol. 29, no. 2, 2006.

[9] M. Angelaccio, A. D'Ambrogio, "A Model Transformation Framework to Boost Productivity and Creativity in Collaborative Working Environments", Proceedings of the 3rd International Conference on Collaborative Computing: Networking, Applications and Worksharing, New York, USA, November 12-15, 2007.

[10] L. Pearlman, V. Welch, I. Foster, C. Kesselman, and S. Tuecke, "A Community Authorization Service for Group Collaboration," in Proceedings 3rd International Workshop on Policies for Distributed Systems and Networks, 2002, pp: 50-59.

[11] D. Argarwal, M. Thompson, M. Perry, and M. Lorch, "A New Security Model for Collaborative Environments," Lawrence Berkeley National Laboratory, University of California, CA, USA, Paper LBNL-52894, 2003.

[12] E.F. Churchill, D.N. Snowdon, and A.J. Munro, Collaborative Virtual Environments: Digital Places and Spaces for Interaction, Springer-Verlang, 2001.

[13] I. Traore and S. Khan, "A Protection Scheme for Collaborative Environments," in Proceedings of the 2003 ACM symposium on Applied Computing, 2003, pp: 331 - 337.

[14] P.A. Dargon, "The Ideal Collaborative Environment," The Journal of Defence Software Engineering, vol. 14, no. 4, April 2001, pp. 11-15.

[15] R. Sandhu, "A Perspective on Graphs and Access Control Models," Lecture Notes In Computer Science (LNCS), vol. 3256, November 2004, pp. 2-12.

[16] M. Kock et al, "A Graph Based Formalism for RBAC," in ACM Transactions on Information and System Security (TISSEC), vol. 5, iss. 3, 2002, pp. 332-365.

[17] National Research Priorities – TO DO
[18] A. K. Gupta, "Community Information Services: A Proposal for creating Knowledge Networks for Creativity," in Proceedings of Conference on Information Today and Tomorrow, Central Leather Research Institute, Chennai, September 1998.
[19] Streitz, Geibler, Holmer, Konomi, Muller-Tomfelde, Reischel, Rexroth, Seitz & Steinmetz, "i-LAND: an interactive landscape for creativity and innovation," in Proceedings of the SIGCHI conference on Human factors in computing systems, Pittsburgh, Pennsylvania, United States, 1999, pp. 120 - 127.
[20] R. de Paula et al, "Two Experiences Designing for Effective Security," in Proceedings of the 2005 symposium on Usable privacy and security, vol. 93, 2005, pp. 25-34.
[21] E.J Dodd, "Visualization and Collaboration for the On-Demand Upstream Petroleum Enterprise," IBM Industry White Paper, May 2004, http://www-03.ibm.com/industries/ca/en/chemicalspetroleum/petroweb/wpapers.html.
[22] G. Skinner, "The TLC-PP Framework for delivering a Privacy Augmented Collaborative Environment (PACE)", in proceedings of The 3rd International Conference on Collaborative Computing, Networking, Applications and Worksharing, New York, USA, November 12-15, 2007.
[23] G. Skinner, "Setting the PACE: a Privacy Augmented Collaborative Environment using the TLC-PP Framework", in proceedings of First International Workshop on Sustaining Privacy in Autonomous Collaborative Environments (SPACE 2007), July 30th – August 2nd, 2007, Moncton, New Brunswick, Canada.
[24] G. Skinner, Shield Privacy: A Conceptual framework for Information Privacy and Data Access Controls, *WSEAS Transactions on* Computers, Iss. 6, Vol. 5, 2006, pp. 1375-1384.
[25] Precise Biometrics, Precise 200MC, http://www.precisebiometrics.com/?id=229&cid=397.
[26] G. Skinner, Managing Privacy, Trust, Security, and Context Relationships Using Weighted Graph Representations, *WSEAS Transactions on Information Science and Applications*, Iss. 2, Vol. 3, 2006, pp. 283-290.
[27] G. Skinner, A Taxonomy for Information privacy in Virtual Collaborations, *WSEAS Transactions on Inormation Science and Applications*, Iss. 6, Vol. 3, 2006, pp. 1108-1115.