Towards a Risk Management Perspective on AAIs

Christian Schläger and Thomas Nowey

University of Regensburg, Universitätsstrasse 31, D-93053 Regensburg, Germany
{christian.schlaeger, thomas.nowey}@wiwi.uni-regensburg.de

Abstract. Authentication and Authorisation Infrastructures (AAIs) support service providers on the internet to outsource security services. Motivations for their usage stem from software engineering and economics. For the latter an assessment of inherent risks is needed. In this work the authors deduct an appropriate, formalistic risk assessment method for AAIs and analyse outsource able security services in comparison to traditional – non AAI involved – service providing. To achieve the assessment of risks various methods for risk management have been analysed and finally a suitable qualitative method has been chosen. As AAIs differ in their potential to cover security services, combinations of these services are compared. The given risk assessment method enables providers to decide on a special infrastructure for their purpose and lets users of AAIs determine if given advantages surpass the immanent risks. This work also enables service providers to estimate costs for such an infrastructure and calculate potential savings.

1 Introduction

Service providing on the internet has been a huge success story. Although ease of use is proclaimed in many advertisements, the usage of a service on the internet – e.g. to buy a book or to use a geographic routing service – is not trivial at all. The purchase of a book is not simply a link to click on but it stands at the end of a sequel of security and data intensive processes – most of them hidden from the user. The complexity of doing business over the internet has increased both for customers and vendors. Concentrating on security connected processes we find a chain of distinctive services linking the user's request with the service providing as shown in Fig. 1. The given chain of security services is enhanced by an attribute infrastructure like deduced from OASIS' XACML and SAML standards in [14].

Risk is an omnipresent factor in internet transactions. Risks have to be identified and valuated to decide upon appropriate controls and monitoring mechanisms. Basically, one has the options to either avoid, reduce, shift, or accept a certain risk.

In [14] and [15] it is argued that Authentication and Authorisation Infrastructures (AAIs) can be used to source out security services in order for the service provider to concentrate on core competencies, raise the overall level of security, provide new, flexible, and more powerful access control services like ABAC (attribute-based access control), and strengthen the usability through user's Single Sign-On (SSO). However, the usage of a new architecture, especially if not entirely under the control of a service provider, raises questions about risk assessment in comparison to

S. Fischer-Hübner et al. (Eds.): TrustBus 2006, LNCS 4083, pp. 41 – 50, 2006.

traditional methods of service providing on the internet. The authors show that different approaches to AAIs are available each with inherent benefits and shortcomings. Differences result from the architecture, the level of outsourcing, and specific use cases.

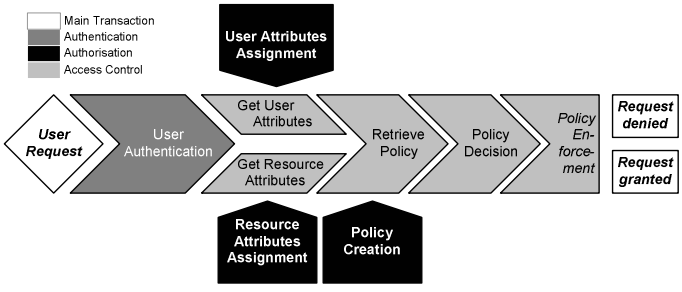

Fig. 1. Security services for accessing a resource in an attribute enhanced infrastructure

In this paper we identify and measure risk factors in traditional e-commerce surroundings versus e-commerce applications with an AAI. Although AAIs are by nature generic architectures, e-commerce has been taken as an example.

2 Related Work

The topic of AAIs as a tool for service providers on the internet has been discussed on a technical level by [9], making a comparative survey, and in more detail by [15] in 2005. Various architectures of research projects and products have been analysed and motivation for the parties has been given: e.g. [14] proposed a reference architecture for an AAI respecting privacy and flexibility. The idea of Single Sign-On has been discussed in the field of identity management. A classification of architectures can be seen in [5]. A quite technical paper by [7] has analysed the risks in the Microsoft Passport protocol. All work that can be found today on AAIs, the most recent given here, has so far neglected the risk assessment in these architectures in comparison to traditional service providing.

That risk in e-commerce is immanent is being reported regularly by intelligence agencies, other governmental institutions, or the media. The interested reader is pointed to [6] for a survey of general risks in e-business.

Risk management techniques have become a vital element of modern security management. A risk is an unwanted event that has negative consequences [12] and can be described as the “combination of the probability of an event and its consequence”.

Systematic risk assessment is especially helpful when it comes to the economic evaluation of information security investments [11]. In literature and in practice numerous methodologies and frameworks for conducting risk analyses exist [17]. Virtually all of today's existing approaches use qualitative metrics to assess risks. Quantification is regarded an important issue but due to many challenges in this field there is, to our knowledge, no methodology for our purpose up until now. Thus we are

going to use a qualitative scale. The concept of Annual Loss Expectancy has a long tradition in risk management and is the basis for the Return on Security Investment.

[2] and [4] pointed out that a holistic cost-benefit evaluation of security investments should also consider the motivation and possible return for an attacker.

3 Methodology

To correctly and completely assess risks in e-commerce or internet transactions, one has to follow a structured approach to fully comprehend and expose all relevant aspects. As shown in section 2, several procedures are known. The authors have opted for [13] with slight adoptions. Risks distinguish themselves from other events due to a loss associated with the event, a measurable frequency of the occurrence, and by a chance to change the outcome of the event. Consequently we are going to divide the holistic process of accessing a resource into separate steps, distinguishing between several forms of implementation for different architectures. We measure the impact for the stakeholders and the according frequency. Finally, we evaluate architectural decisions on their impact and suggest, based on the risk assessment on the pros and cons, the usage of an AAI. The Return on Security Investment (RoSI) is used to economically justify an AAI usage.

Let l_i be the frequency of a successful attack on i in one year. L_i is defined as the expected loss for i in the case of a successful attack. Consequently, the Annual Loss Expectancy for i is defined as

$$ALE_i = l_i \cdot L_i \tag{1}$$

4 AAI Architectures

Usually, the usage of AAIs is motivated from a software engineering point of view – outsourcing non functional activities into an infrastructure [16], and from an economic point - outsourcing security services to concentrate on core competencies gaining competitive advantages and raising the security level through third party know-how [15]. Referring back to Fig. 1 we see that several security services build on each other to compute an access decision. Again, taken the SAML and XACML termini as a guideline, we can deduct four separate steps of services: Authentication Assertion, Attribute Assertion, Policy Decision Assertion, and Policy Enforcement. One, all of them, or combinations can be outsourced by a Service Provider into an AAI.

The characteristics of an AAI can be determined with the help of the given four sub-services in combination with the two prevailing architectural paradigms. AAIs are to this day build either centrally with a central database or provider in the middle or as a federation where service providers act as AAI providers themselves. The best examples of these two archetypes are of course Microsoft's centralised .NET Passport versus the distributed Liberty Identity Federation Framework.

In this paper we restrict the introduction of current AAIs to four representatives, each enhancing the other by or specialising in one of the given sub-services. For a more detailed analyses see [14, 15].

4.1 Microsoft .NET Passport

Microsoft .NET Passport, although often criticised, was the first and the largest commercial AAI so far. Passport concentrates on Single Sign-On (SSO) for the user who gets his passport account with every hotmail account, using a central database to keep all client information. Passport relies heavily on the usage of cookies imitating to some extend Kerberos's ticketing functionalities. The login to a SP is redirected to Passport requiring his username and password. The SP's ID is transmitted via URL encoding enabling Passport to redirect the client and storing several cookies. At the SP a software agent is needed – the so called Passport-Manager. This software reads URL encoded data and stores additional cookies into the SP's domain permitting an access control decision. At another vendor the passport cookies are used to enable a SSO [10]. The vendor decides about access of resources using his authorisation and access control mechanism of choice. Passport is a centrally organised SSO system meaning that it only asserts the user's authentication.

4.2 Liberty Alliance Identity Federation Framework (ID-FF)

Liberty was the open source community's answer to Microsoft Passport in 2001. In Liberty a Circle of Trust (CoT) establishes a Liberty system [8]. Each partner provides the authentication for his users with his own methods while they themselves can login to all other partners with a SSO. The user authenticates at his IdP and, if he wishes, a cookie is stored under a common domain where every member hosts a server so they all can access the cookie. If a user moves to a CoT member the cookie is read, the IdP asks for appropriate authentication, and an assertion is awaited. Communication is based on the SAML protocol. A CoT has to decide on the implementations. The SAML assertions can carry any attribute the CoT agrees upon. Liberty's architecture is distributed. The IdP is not fixed like in Shibboleth or centralised like in Microsoft .NET Passport. It is possible to login at different points of the CoT thus resulting e.g. in different user names or attributes that are transferred. The identity of the user is not revealed in the process of requests and assertions. For risk assessment purposes we call Liberty identity and attribute federated.

4.3 PERMIS

The EU project PERMIS [3] is closely integrated into the target system. This can be e.g. an apache web server. Instead of using the apache security functionality PERMIS is used to derive the user's role names and a PERMIS policy used to control access. The target application is responsible for user authentication. PERMIS uses X.509 attribute certificates (AC) binding the user's distinguished name to a role. An XML policy authorises roles and targets. If a user desires access the PERMIS access control enforcement function will delegate his request to the access control decision function which determines the correctness of the AC and its compliance with the policy. If access is granted the decision is given back to the enforcement function which grants the access or not. The centrally stored ACs can contain any information an Attribute Authority has assigned. Of course different authorities can work together creating an attribute storage LDAP. The decision and enforcement functions have to be implemented into the web server at the SP.

4.4 PAPI

PAPI (Point of Access to Providers of Information), developed in 2001 by RedIRIS, a Spanish research network, could be regarded as a maximised AAI. It forms a distributed access control system for digital resources accessible over an institution's intranet or the internet. The user has to authenticate at the authentication server (AS) of his home domain. As PAPI is agnostic to the form of authentication the user's domain is responsible to supply a distinguish name. After successful authentication a website is given back to the user containing all accessible digital resources. Clicking on a link, the user is redirected to the Point of Access (PoA) taking with him an encrypted key identifying the AS. The PoA fetches the resource and delivers it to the user. PAPI acts as a proxy server and handles all interaction for the associated clients and servers. Consequentially, PAPI forms the maximal AAI [1].

5 Risk Identification

Assets under risk are the identities of clients and service providers, attributes about resources and users, the service or the good requested, as well as the system itself. All assets are prone to loose the three major security goals: Integrity, confidentiality, and availability. [13] has shown the types of vulnerabilities one might find for hardware, software, and data. Adopting that notion, the vulnerabilities are interruption, for example via a Denial-of-Service-attack, interception of the communication, for example via a Man-in-the-Middle-attack, the modification of the asset, for example attributes granting access to the resource only if the user is over 18 could be changed to access under 16, and finally fabrication of new identities. Fabrication would occur if a bogus merchant is created luring the client to log-in with his SSO credentials.

To assess the risk of each asset we make use of the introduced frequency for a successful attack. The frequency is affected twofoldly – firstly by the technical barrier *T* one raises to prevent an attack and secondly by the motivation of the attacker, the so called "return of attack" – *RoA*.

$$l_i = f(T_i, RoA_i) \tag{2}$$

$$ALE_i = f(T_i, RoA_i) \cdot L_i \tag{3}$$

The higher *T* the less likely a successful attack occurs; the higher *RoA* the higher the attacker's motivation and the resources employed and consequently the likelier an attack. The *RoA* can be seen as more or less stable as a service provider per se is doing business by offering something of value. He will not stop providing services to minimise risks. However, *T* is completely in the hands of the service provider. Outsourcing security services to an AAI can inflect on *T* and therefore on the frequency of a successful attack.

If the outsourcing of security services inflects the *ALE* the question remains which security services should be outsourced and to what extent. Different AAI approaches and architectures are able to perform one, all, or combinations of these services. We will take each sub-service and analyse the risks associated as can be seen in Table 1. Each sub-service can be interrupted via a Denial of Service or the deletion of its data.

Table 1. Security sub-services with associated risks and consequences

Service	Risks for user	Risks for provider
Authenti-cation Assertion	**Identity theft**: Identity is intercepted and/or misused. Provider's identity is forged and the user lured into signing-in or paying for services never to be received.	**Identity theft:** User identity is forged or intercepted resulting in delivery without access rights. The theft of the provider's identity results in a loss of reputation.
Attribute Assertion	**Attribute forging or modification**: If resource attributes are modified, not complete, or added, the following decision can't be trusted. It might be that access or privileges are not granted.	**Attribute forging or modification:** If user attributes are modified, not complete, or added, the following decision can't be trusted. False denies result in loss of business or user motivation to change the provider. False access can be used for fraud.
	Attribute interception: A bogus merchant could use the attributes to misuse credentials like a credit card number, conduct illegal profiling, or sell the information.	**Attribute interception**: an attacker could gain secret knowledge about processes or products.
Policy Decision Assertion	**Decision forging or modification:** Access could be wrongly denied.	**Decision forging or modification:** Access could be wrongly denied or granted.
Policy Enforcement	**Enforcement modification:** Access could be wrongly denied.	**Enforcement modification:** Access could be wrongly denied or granted.

As the effect is devastating but trivial - no provider or user can conduct business – it is not shown explicitly.

5.1 General Implications of AAI Usage

With the usage of an AAI various changes occur in the business surrounding. For once, the potential number of customers for one provider enlarges. The number of users of an AAI that merges *N* service providers is at most the sum of all users (4).

$$n_{AAI} \leq \sum_{i=1}^{N} n_i \tag{4}$$

The technical barrier for an attack T is no longer just one single T_i but has to be seen as a combination of all barriers for the given sub-services, each potentially outsourced: T_i^{AuthN} - for the Authentication, T_i^{Attrib} - for the Attribute Services, T_i^{PD} - for the Policy Decision, and T_i^{PE} - for the Policy Enforcement. T_i can't be computed by the sum of all barriers but is determined by the minimum: the weakest link in the chain determines its overall strength (5).

$$T_i = \min(T_i^{AuthN}, T_i^{Attrib}, T_i^{PD}, T_i^{PE}) \tag{5}$$

5.2 AAI Architectures and Their Implications

If using an AAI like Microsoft's .NET Passport the authentication of the user is relayed to Passport. The provider uses Passport's technical barrier to prevent misuse of the authentication sub-service for his business. His ALE_i, consequently, depends on the following equation (6):

$$ALE_i = f(\min(T_{AAI}^{AuthN}, T_i^{Attrib}, T_i^{PD}, T_i^{PE}), RoA_i) \cdot L_i \tag{6}$$

Using PERMIS T^{Attrib} and T^{PD} depend on the AAI. T^{AuthN} has to be managed by the SP or another AAI providing SSO. The enforcement needs to be handled by the target system.

For one single provider the loss and supplied return of attack stays the same. However, in the case of a fully developed AAI – like in PAPI – where all security services are outsourced and the AAI provider acts as a proxy for all N service providers, a successful attack on one security service results in a breach of all N vendors. T_i is substituted by T_{PAPI}. The AAI resembles a middleman. Consequently, the RoA is the sum of all returns (7).

$$ALE_i = f(T_{PAPI}, \sum_{i=1}^{N} RoA_i) \cdot L_i \tag{7}$$

(6) is true if the barrier T is set by one AAI provider like Passport, PERMIS, or PAPI. However, if the AAI is distributed like the Liberty ID-FF the technical barrier can't be estimated as easily. As N SPs act also as identity and attribute providers for other SPs in a CoT and use their own means of authentication the notion of the weakest link once more takes effect (8):

$$\begin{aligned} ALE_i = f(&\min(\min(T_1^{AuthN}, ..., T_N^{AuthN}), \min(T_1^{Attrib}, ..., T_N^{Attrib}), \\ &T_i^{PD}, T_i^{PE}), RoA_i) \cdot L_i \end{aligned} \tag{8}$$

Please note that although no AAI is introduced in detail here having a federated policy decision of this type is also possible.

6 Towards Risk Assessment in AAIs

To correctly assess the risk of the usage of an AAI the authors make use of a qualitative method. As the Annual Loss Expectancy ALE in an AAI for SP_i is, with the exception of a proxy approach, independent of his L_i and RoA_i, one can narrow the effect to the technical barrier of the security sub-service (5), (6). The technical barriers of the four sub-services, when provided by SP_i himself, are taken as the normalised value. The outsourced value T_{AAI} is either more (+), less (-), or equal (~). Table 2 states the risk assessment. A distinction is being made if the sub-service is federated or centralised.

Table 2. Risk assessment for service providers in AAIs

	$T_{AAI,\ centralised}$	$T_{AAI,\ federated}$
T^{AuthN}	+: Although n_{AAI} exceeds n_i, the potential of granting SSO with a hard password in a controlled environment argues for a stronger authentication. The usage of complex identification methods like a PKI is more preferable.	-: As SP_i is in no control of all other SP the weakest link in the chain dictates the barrier for identity theft and alike. A controlled, standardised approach for each SP is not mandatory.
T^{Attrib}	+: Merging all attributes balances modified or forged information. With a pattern of the user's behaviour suspicious behaviour can be detected.	+: Same as centralised approach.
T^{PD}	+: Centralised policy decision enables complex, flexible, and specialised access control like XACML policies through synergies and a broader information base.	~/-: As policy decision making has to be provided by every SP no synergies can be utilised. The weakest method sets the highest barrier for attacks.
T^{PE}	-: The usage of a central proxy strongly affects the potential *RoA* resulting in a higher l_i (PAPI, (7)).	Not feasible.

Identity theft and fraud are the user's two main concerns in e-commerce. Assuming the SP himself is acting trustworthy, an attacker could only harm the user if a technical barrier fails. Consequently, the user has a strong interest in high security but is in no position of influencing the barriers directly. An exception has to be made as far as the authentication is concerned. Using weak passwords is making identity theft easy. SPs usually shy at demanding strong passwords or the usage of a PKI, fearing increased help desk costs or shrinking user acceptance. With a SSO these disadvantages could be reduced. However, the user has to trust the IdP not to misuse his data. The discussion about .Net Passport and the development of the Liberty ID-FF shows an interest in privacy and missing user acceptance. A user has to evaluate privacy aspects versus the ease of use through SSO and a potentially higher and transparent security system.

7 Methods for Deciding on AAI Usage

In section 6 we have assessed risks depending on different AAI structures and services. The question remains whether an AAI is economically useful.

To determine the cost effectiveness of security investments the RoSI approach has been widely accepted. ALE_{old} depicts the expected loss without additional security investment. C are security costs to reach ALE_{new}, R is additional revenue in cause of the membership in an AAI Federation, e.g. through wider adoption of the service, a larger customer base, or a better corporate image.

$$ALE_{old} - ALE_{new} - C + R = RoSI \tag{9}$$

For economic reasons the RoSI must be at least positive. Taking into consideration that *ALE* is defined by the weakest point of the security sub-services T^{min} and that the cost for sub-service *x* at SP_i is c_i^x we can deduct two reasons for outsourcing security sub-services. r_i^x defines the additional revenue for SP_i when outsourcing *x* due to the reasons mentioned above.

First, if the outsourced sub-service T_i^x is not $T^{\min}$ but $T_i^x \leq T_{AAI}^x$, then

$$ALE_{old} - ALE_{new} = \Delta ALE = 0 \text{ from (9)} \tag{10}$$
$$-C + R \geq 0 \rightarrow C \leq R \rightarrow c_{AAI}^x \leq c_i^x + r_i^x$$

Meaning that if no strengthened barrier against an attack results out of the decision to use the AAI's service it can be economically reasonable to use the AAI if cost-savings are higher or additional revenue is gained for example through a larger customer base.

Second, if the outsourced sub-service T_i^x is $T^{\min}$ and $T_i^x \leq T_{AAI}^x$, then

$$ALE_{old} - ALE_{new} = \Delta ALE > 0 \text{ from (9)} \tag{11}$$
$$c_{AAI}^x < c_i^x + r_i^x + \Delta ALE$$

The amount to be invested in an AAI is the sum of reduced costs through outsourcing, additional revenue through a larger customer base, and the saved *ALE*. Please note, when changing more than one sub-service in (11) the additional revenue r_i^x is not affected proportionally.

Using AAI services does not automatically change the risk assessment of a business process. As seen in Table 2 the decision has to be carefully evaluated if additional risks are worth the enhancements. Furthermore, the decision of outsourcing doesn't have to depend on risk but can be seen as an entirely economic decision (10).

However, as shown in (11) the implication of fewer risks – or lesser *ALE* - motivates higher investments for the AAI usage as well as sums up to potential savings.

8 Conclusion and Future Work

Unfortunately, empirical data about the risks of AAIs is missing. Therefore, our approach stays conceptual and follows the qualitative methods by [13]. However, our approach permits, for the first time, the analysis of risks in each sub-service in authentication, authorisation, and access control deducting formally the factors which are influencing an outsourcing decision. Exclusively motivating AAIs from a technical perspective is not sufficient. It is of high importance to identify the four security sub-services for a system and measure its costs and risks. Accordingly, a service provider can decide on a suitable AAI. Next steps have to comprise the search for empirical data.

References

[1] Castro-Rojo, R., Lopez, D. R.: The PAPI system: point of access to providers of information. In: Computer Networks: The International Journal of Computer and Telecommunications Networking, Volume 37. Elsevier, Amsterdam (2001) 703-710

[2] Cavusoglu, H., Mishra, B., Raghunathan, S.: A Model for Evaluating IT Security Investments. In: Communications of the ACM, Volume 47. ACM Press, New York (2004) 87–92

[3] Chadwick, D., Otenko, A.: The PERMIS X.509 role based privilege management infrastructure. In: Proceedings of the 7th ACM Symposium on Access Control Models and Technologies (SACMAT '02). ACM Press, New York (2002) 135-140

[4] Cremonini, M., Martini, P.: Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA). In: Proceedings of the Fourth Workshop on the Economics of Information Security. Harvard (2005)

[5] Jøsang, A., Pope, S.: User Centric Identity Management. In: Clark, A., Kerr, K., Mohay, G. (eds.): Proceedings of AusCERT Asia Pacific Information Technology Security Conference 2005. Gold Coast (2005) 77-89

[6] Katsikas, S. K., Lopez, J., Pernul, G.: Trust, Privacy and Security in E-business: Requirements and Solutions. In: Proc. of the 10th Panhellenic Conference on Informatics (PCI'2005). Lecture Notes in Computer Science. Springer-Verlag, Berlin Heidelberg New York (2005) 548-558

[7] Kormann, P., Rubin, A.: Risks of the Passport single sign-on protocol. In: Computer Networks: The International Journal of Computer and Telecommunications Networking, Volume 33. Elsevier, Amsterdam (2000) 51-58

[8] Liberty ID-FF Bindings and Profiles Specification, Liberty Alliance Project, 2003. Accessible at http://www.projectliberty.org/specs/liberty-idff-bindings-profiles-v1.2.pdf

[9] Lopez, J., Oppliger, R., Pernul, G.: Authentication and authorization infrastructures (AAIs): a comparative survey. In: Computers & Security, Volume 23. Elsevier, Amsterdam (2004) 578-590

[10] Microsoft Passport Review Guide. Accessible at http://download.microsoft.com/ download/a/f/4/af49b391-086e-4aa2-a84b-ef6d916b2f08/ passport_reviewguide.doc

[11] Nowey, T., Federrath, H., Klein, C., Plössl, K.: Ansätze zur Evaluierung von Sicherheitsinvestitionen. In: Proc. 2. Jahrestagung des GI-Fachbereichs Sicherheit, Lecture Notes in Informatics, P-62, Köllen-Verlag, Bonn (2005) 15-26

[12] Pfleeger, S.L.: Risky Business: what we have yet to learn about risk management. Journal of Systems and Software, Volume 53. Elsevier, New York (2000) 265-273

[13] Pfleeger, C.P., Pfleeger, S.L.: Security in Computing. 3rd edn. Prentice Hall, New Jersey (2002)

[14] Schlaeger, C., Nowey, T., Montenegro, J.A.: A Reference Model for Authentication and Authorisation Infrastructures Respecting Privacy and Flexibility in b2c eCommerce. In: Proc. of the First International Conference on Availability, Reliability and Security (ARES '06). IEEE Computer Society, Los Alamitos (2006) 709-716

[15] Schlaeger, C., Pernul, G.: Authentication and Authorisation Infrastructures in b2c e-commerce. In: Bauknecht, K., Pröll, B., Werthner, H. (eds.): Proc. of the Sixth International Conference on Electronic Commerce and Web Technologies - EC-Web '05. Lecture Notes in Computer Science, Vol. 3590. Springer Verlag, Berlin Heidelberg New York (2005) 306-315

[16] Tanenbaum, A.S., van Stehen, M.: Verteilte Systeme. Grundlagen und Paradigmen. Prentice Hall, München (2003)

[17] Vidalis, S.: A Critical Discussion of Risk and Threat Analysis Methods and Methodologies. School of Computing Technical Report CS-04-03, University of Glamorgan (2004)