Context-Aware Systems and Adaptive User Authentication

Kimmo Halunen and Antti Evesti

VTT Technical Research Centre of Finland, Oulu, Finland
{kimmo.halunen,antti.evesti}@vtt.fi

Abstract. In this paper we discuss the possibilities of context-aware systems in providing more secure user authentication. We describe some approaches in using context information in adaptive security systems, especially in adaptive user authentication. In addition, we discuss some recent results in applying the context itself as an authentication factor. Recent advances in cryptographic protocol design and adaptive, context-aware systems enable the linking of the context information to the cryptographic keys and authentication. Furthermore, new protocols make adaptive user authentication easier as it is possible to combine several different factors in a single protocol. We give some examples of this and discuss the further potential of these methods.

1 Introduction

Reliable user authentication is crucial for many services that are provided over networks. In many cases, the devices that the users apply to gain access to the services provide a context that the context-aware services utilise. Furthermore, the service providers and devices have profile information on the users. The combination of these two information sources can be used in many different ways. One application area is the user authentication mentioned earlier.

Context-aware systems have become more prominent in recent years and there are many different ways that these systems can be designed and utilised [1]. From security perspective these systems offer both increased risks as well as benefits. Risks come from the fact that more and more different types of devices and sensors are networked and thus are subject to possible abuse by remote attackers. One benefit of these systems is the possibility to adapt the security of the system based on the context information.

Adaptive security systems utilise some form of security monitoring and modify the system behaviour according to the monitored security state of the system. Thus, adaptive security systems use various forms of contextual information. With the help of this information, the system provides self-protection, which defends the system against incidents and also anticipates problems [27].

Many of the adaptive security approaches use authentication as an example of a security process that can benefit from the adaptive system. However, the two domains remain separated in the sense, that although there is an adaptive process controlling the authentication, it is not utilised in or tied into the actual

M.J. O'Grady et al. (Eds.): AmI 2013 Workshops, CCIS 413, pp. 240–251, 2013.

authentication protocol. The adaptive process is used in setting the limits on what factors are used and how often the authentication is initiated. The authentication protocol that is used is then a separate process. In some cases this is acceptable, but it may enable the clever attacker with a way to compromise the security of the underlying authentication protocol(s) and thus undermine the security of the system as a whole.

In cryptography, authenticated key exchange (AKE) protocols are used to establish a common, secret key that is used to encrypt the communications and to authenticate the messages and their origin between two (or more) parties. Furthermore, these protocols can be usually utilised to authenticate the users or devices, even if the secret key material is not needed in the communications.

There are different ways for users and devices to authenticate themselves. These are usually called *factors* of authentication. These factors are traditionally divided into three categories. The first is *something you know* such as a password or a secret handshake. The second is *something you have* such as a key, a token or a device. The third is *something you are* or *a biometric* such as a fingerprint, DNA or some behavioral trait. Also other categories have been discussed in recent years. One is *someone you know* or someone who knows you as in e.g. [6]. Others include such ideas as proximity to friends [13] and *something you process* [32].

Several protocols have been designed to provide AKE between two parties based on one or several of the above mentioned factors. As passwords have been the dominant method of authentication there are several protocols that provide password authenticated key exchange (PAKE) such as [14] and many others. There are also authenticated key exchange protocols based on biometrics such as [5] and based on secret keys (usually stored on smart cards or other devices) and an associated PKI scheme [15,2].

The various transactions and processes that take place in the networked environment require different levels of security and different levels of authentication. As it is possible to use several different factors of authentication to gain more trust on the authenticity of the transaction, user or device, it is also important to have adaptive systems that utilise these possibilities.

1.1 Contributions and Organisation of This Paper

In this paper we discuss some possibilities of context-aware user authentication in adaptive security systems. We show that with current cryptographic protocols it is possible to link the context to the cryptographic authentication process and also to use the context in making the adaptive security decisions. We also describe and discuss the potential of some recent proposals that consider the context (or some part of it) as a separate authentication factor.

The paper is organised in the following way. In the next section we present some previous results on context-aware adaptive systems and cryptographic authentication protocols. In the third section we present different ways in which the context can be utilised in the adaptive user authentication. We illustrate some of these concepts with small examples. The fourth section briefly discusses

the privacy implications of context-aware adaptive user authentication. The fifth section contains discussion and future research topics and the sixth section gives our conclusions.

2 Previous Work

In this section we present some of the most relevant previous results in context-aware systems, adaptive security and authentication.

2.1 Context-Aware and Pervasive Systems

Pervasive computing is applied in various domains to improve the life experience of people, e.g. smart spaces, healthcare and transportation. Due to these varying domains, the security requirements for different applications vary greatly together with other quality and functional requirements. Context information can be applied to deduce these requirements for the pervasive applications [25]. Moreover, context information supports the adaptive behaviour in pervasive computing. It has been stated in [8] that the adaptive behaviour is one major challenge related to pervasive environments.

It is possible to utilise the context-awareness of applications in several ways and, depending on the application, the required context information also changes. Taxonomy of security related context information for smart space purposes is presented in [10]. This taxonomy divides security related context information to three levels as follows: The bottom level consists of the physical context that describes an execution platform, e.g. operating system, utilised network connection etc. The second level constitutes of the digital context, which is intended to describe the role of the environment. For instance, the smart space can be either private or public. The highest context level is the situational context, which describes the role of the exchanged data and the user's role in the environment. For example, the user could be a healthcare professional, who is trying to retrieve work related documents from her home environment.

2.2 Adaptive Security

In an adaptive security system, the system selects the course of action among the existing security mechanisms and/or tuning parameters of these mechanisms. These modifications to the system behaviour are based on the monitored security level and the perceived context of the system. Thus, adaptive security can be seen as the capability of the system to offer self-protection. Self-protection defends the system against malicious attacks and anticipates problems [27].

Achieving adaptive security requires that the system is able to monitor its own behaviour and environment. This monitoring can be realised, for instance, by security measuring, an Intrusion Detection System (IDS) or by some other means. The monitored data is analysed further in order to recognise security

breaches or other incidents, which in turn cause an adaptation need. Examples of these analyses are the calculation of security indicators [28], the calculation of authentication confidence [17] and the calculation of user's suspiciousness level [26]. Lastly, when the adaptation need is recognised, the system has to decide what parts of the system will be adapted and how. The survey in [35] reveals that this decision making part is the most uncovered area in the current security adaptation approaches.

In [9], the authors compare four security adaptation approaches from the application layer viewpoint. The compared adaptation approaches act as described above, i.e. existing security mechanisms and their parameters are adapted. Consequently, security mechanisms themselves are not made adaptive but their utilisation is adapted based on the monitored security level and context. In [35] the authors list and compare over 30 self-protection approaches in a tabular form. However, these approaches also concentrate on adapting existing security mechanisms and security policies.

2.3 Authenticated Key Exchange

In [2], Bellare and Rogaway present a framework in which they can achieve provable security for several AKE protocols that they describe and it is one of the first designs for authenticated key exchange with a proof of security. This has provided the basis on which many of the subsequent AKE protocols rely.

There has been a great amount of work done on provably secure authentication protocols with one or many factors. Single factor schemes have traditionally been password-based, as in [14], biometrics based, as in [5] or based on some public key setting as in [15]. Two-factor authenticated key exchange has been proposed for example in [22,20]. In [23] a multi-factor authenticated key exchange protocol has been introduced. Thus it can be seen that there exist many protocols, that can be used with different factors of authentication either separately or in a single protocol.

In [12] the authors describe MFAKE, a new multi-factor authentication protocol, that can be used with any number of passwords, client secret keys and biometrics. The security of MFAKE is based on sub-protocols that utilise tag-based authentication [18] for each authentication factor. This modular approach enables a security proof for the MFAKE protocol. MFAKE facilitates also mutual authentication between the client and the server.

Some form of contextual information has been proposed as a factor of authentication in several publications [29,6,13]. In [13] the authors propose using mobile devices users' proximity to their friends mobile devices as a suitable factor for authentication. In [6], the authors describe a system for vouching for legitimate users if they forget their security tokens. Also the authors of [29] propose a social approach to authentication. One could also argue that the proposal of [32] is a case of contextual information being applied to authentication.

It is worth noting that the above protocols provide examples of two different ways of using contextual information in authentication. The first, demonstrated in [13], means that the context itself becomes one factor in the authentication.

On the other hand, as in for example [6], the context can dictate how and when the user should authenticate herself to the system. This is also the case in some adaptive security systems such as in [17].

3 Combining Authentication and Context-Awareness

As user authentication is currently an important topic in information security and on the other hand different context-aware systems and middleware are emerging, it is important to examine the possible benefits and threats that this combination offers. In this section, we will discuss different ways to combine context-awareness provided by pervasive systems with adaptive security and entity authentication. In the next section we will discuss some of the privacy implications of these technologies.

First of all, we will give some definitions of concepts that are used later in this paper. *Context* is a set of environmental states and settings that either determines an application behaviour or in which the application even occurs and is interesting to the user [7]. From security perspective, this set can be assumed to be public.

3.1 Context as a Separate Authentication Factor

As mentioned in the previous section, there have been some recent proposals that use some contextual information as an authentication factor. For example, in [13] the authors propose to use the proximity of users friends as a possible factor for authentication. The proximity could be measured with many different methods such as GPS or some wireless connectivity. In [13] Bluetooth is proposed as the measure of users proximity with friends. However, this method does not generate enough entropy to be utilised in authenticated key generation.

In [32] the authors propose to add into the security of passwords by requiring the password to be a mathematical formula that is applied and the result used as the secret. There is very little indication that this would gain popular acceptance or that this approach would be immune to the same weaknesses that the normal passwords face.

There are some proposals ([29,6]), where the social context of the user is used in some authentication scenario. These proposals offer a very limited use of the context and do not rely on any autonomously working context-aware application.

The above examples are very interesting first steps in providing new authentication factors. It is also worth noting, that utilising contextual authentication factors could require very little user interaction and would thus be fairly easy to use from user's perspective. However, there is a need for further research on the most usable factors, as the recent proposals do not provide secure enough authentication or are not really related to context-aware systems.

3.2 Context-Awareness as an Adaptation Mechanism

Many attributes that the context-aware systems provide are by themselves insufficient for reliable authentication. For example GPS coordinates and IP address may be easily available, but are fairly useless as separate authentication factors. However, these can be used in adapting the authentication process.

Thus, in contextual authentication the client context defines the different factors and channels that the client must utilise to perform authentication to the server. For example, this context can be the time, the physical location (GPS), virtual location (IP address) or the different applications that the client is running.

As a small example we give the environmental variable provided by many web browsers. This variable contains a lot of information on the context, where the browser is running (e.g. operating system) as well as on the browser itself (browser name, version number etc.) and can be easily accessed by programmers. This information could be used to adapt the user authentication. For example, if the user has an outdated version of a browser, which is known to contain security vulnerabilities, the system might require two-factor authentication.

We made a small proof of concept application that recognises the name of the browser and, based on user preferences on trusted browsers, decides whether the user needs to provide just a password or a password and insert a valid USB token to the computer. The authentication was performed using the MFAKE protocol [12].

In our opinion, it would be beneficial to link the contextual information with the authentication and the possible keys generated in the process. In many adaptive authentication systems, the authentication process is completely separated from the underlying context-aware application except from some triggering functionality. This is of course sensible from development perspective as these two may then be developed independently.

However, with recent tag-based authentication methods, such as MFAKE [12], it is possible to link the contextual information either partly or completely to the authentication process. This could be included in the adaptive security process. Thus it would be harder to use successful (partial) authentications in different contexts.

In [11] the authors present an adaptive security architecture in a smart space. Their adaptive security solution is based on the Smart-M3 smart space architecture [16]. As an example of this adaptive security they give an authentication use case where user communicates via a smart phone with the established smart space and uses the smart space to open and close the lock on her apartment's front door. As the environment recognises the different actions in different contexts the user needs to authenticate and re-authenticate herself in order to be allowed to perform some tasks. The system is based on several predefined authentication levels that are enforced for certain actions of the user.

In [11] the authors do not delve deep into the authentication mechanisms that are invoked by the smart space. They only mention the usage of passwords, but do not specify a protocol for this password authentication. This is reasonable as

the adaptive security system should work with any such protocol. However, with existing protocols, the contextual information that guides the adaptive security process is left out of the final authentication. With the help of MFAKE the information could be included in the user authentication. The context could be used at least in the computation of the tag and thus be linked to the end result of the authentication.

By realising the proposed scenario with the help of the MFAKE protocol, we could improve the adaptive security system. As the smart space already provides a rich contextual environment, one could include all of that or only the security related context to the MFAKE protocol. For example, when unlocking the door, the system requires a new authentication as the previous authentication level does not allow for this action. When re-authenticating the user, the MFAKE includes the context information (time, previous authentication level, required authentication level, etc.) to the computation of the tag used in the protocol. The system also makes the decision on the necessary authentication factors and proceeds with the necessary sub-protocols. After successful authentication, the adaptive security system updates the authentication level and allows the unlocking operation. This could also improve the user experience of the system, if the contextual information would be used to require less user interaction in the authentication.

4 Privacy Issues

Pervasive computing and monitoring of user context and behaviour raises some privacy issues. Many service providers already collect a lot of information on their users and profile them accordingly. Although these profiles may help in user authentication they also pose a risk to privacy.

There are methods that allow for anonymous authentication (e.g. [3,34]) and that allow for example attribute based authentication (or signatures) [21,30]. However, these only solve the problem partially for authentication. The problem with pervasive systems and possible cross matching of different contexts and profiles over several service providers is not solved by these authentication solutions.

There have been efforts to quantify and model the privacy issues related to context-aware systems. For example [19] presents a model for controlling users privacy. In [33] the authors propose to use metadata related to the quality of the context information to control the privacy.

However, as can be seen from [1], many systems do not facilitate security and privacy controls. This is fairly troubling, as in the light of recent news, the users cannot be certain that their context information is not misused by the different service providers or some governmental agencies or even blackhat hackers.

5 Discussion and Future Work

Because there are many areas of improvement both in user authentication and in context-aware systems and middleware, we discuss some of the more interesting future directions.

As seen in previous sections there are cryptographic protocols which can utilise context information and link it into the actual authentication and the shared secret between communicating parties. There are also some proposals that use the context information itself as an authentication factor. However, there are still many open questions on which context attributes are best suited to be used as authentication factors and how we can minimise the impact on privacy.

Especially with biometric authentication factors it is important to consider both improving the accuracy of different methods and to ensure that the original biometrics are not leaked in possible database breaches as the replacement of these is usually quite impossible. Some work towards this end has been done (e.g. fuzzy extractors, fuzzy vaults and fingerprint hashes), but some of these are very specific to a certain type of biometric or otherwise impractical to combine with existing biometrics. A good survey on the topic can be found in [24].

It is widely known that the username-password based authentication mechanisms start to show many signs of weakness. With a provably secure protocol as a backbone, we may start to devise authentication systems that employ the MFAKE protocol or some other protocol that enables the use of multiple different authentication factors. Thus, we could move from the username-password based authentication to more advanced and hopefully more secure and reliable authentication.

With context-aware applications the context information could be used in real-time fashion and thus it is very well suited for continuous authentication. This means that the authentication is performed continuously relating the user's actions to the level of security of the data and actions. Usually, authentication is a one-time action that grants access to different services for some period of time. It is also very much a binary decision of accept or reject. In continuous authentication the decision can be based on the context that is monitored frequently. Even if continuous authentication cannot be realised, with the use of adaptive security systems we may at least amplify the authentication mechanisms if the context of the user changes.

Furthermore, we could employ a more risk-based and probabilistic approach to authentication by using the context information. In these types of scenarios the authentication is not a clear cut accept or reject but a level of confidence on the legitimacy of the action performed by the user. For example in [17] the adaptive authentication system gives a trust score on the level of authentication. This trust score could be reflected against the security policy of the service provider.

The above discussion links authentication to trust. For example in [31], Schneier writes extensively about the different levels of trust we as individuals place on other individuals, different institutions and even processes and systems

that we interact with . One possible direction of development in authentication systems could be systems that allow for these nuances of trust to be present even in online activities. Context-aware, adaptive authentication could help in developing systems to this end. By linking contextual information and adaptive mechanisms to provably secure authentication and key exchange protocols, we can provide more tools for building secure environments and applications on modern smart spaces.

However, there are many issues that the cryptographic protocols still leave open. One major issue is the enrollment of the different factors used in the protocol. One of the reasons passwords and usernames have become so popular is that enrolling to a new service is extremely easy. With other factors such as tokens, biometrics and even the new social factor, the enrollment process is usually more complicated or very hard to do in a secure manner over untrusted systems and networks. Solutions to this problem need to be devised in order to have access to the security features of MFAKE or other multi-factor authentication protocols. In [4] the authors present a very good framework for evaluating new methods of authentication. This methodology should be used to evaluate the possible benefits of adding different factors to authentication and the feasibility of new, possibly context-based, authentication factors.

One solution could be to have different trust levels for different types of enrollment and maybe to have an algorithm learn the trustworthiness of the different factors. This would make the process of authentication closer to the interactions we have in real life with other people. We have a different amount of trust for different people and we require more rigorous proofs of identity for some people than for others and in different contexts. This kind of system could be more secure than a system based only on a binary trust/no trust decisions, but it would also be more open to different attacks and prone to human-like errors of judgment over the trustworthiness of some entities. This type of approach is discussed for example in [36].

6 Conclusion

In this paper we presented some possibilities of utilising context aware systems in adaptive user authentication. Recent advances in both adaptive security systems and in cryptography show that it is possible to combine the context information gathered from modern pervasive systems with cryptographic authentication schemes. This information can be first used to control an adaptive security system and then linked to the authentication scheme via tags.

Furthermore, we discussed some proposals for utilising the context information itself as an authentication factor. However, this direction requires more research as the proposed methods do not achieve satisfactory security for authentication.

We have made some motivational proof of concept work in combining context information with the MFAKE [12] protocol. The next step is to include this in some pervasive computing system with adaptive security mechanisms. In this way we could improve and further validate our approach.

References

1. Baldauf, M., Dustdar, S., Rosenberg, F.: A survey on context-aware systems. International Journal of Ad Hoc and Ubiquitous Computing 2(4), 263–277 (2007)
2. Bellare, M., Rogaway, P.: Entity authentication and key distribution. In: Stinson, D.R. (ed.) CRYPTO 1993. LNCS, vol. 773, pp. 232–249. Springer, Heidelberg (1994)
3. Boneh, D., Franklin, M.: Anonymous authentication with subset queries. In: Proceedings of the 6th ACM Conference on Computer and Communications Security, pp. 113–119. ACM (1999)
4. Bonneau, J., Herley, C., van Oorschot, P., Stajano, F.: The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In: 2012 IEEE Symposium on Security and Privacy (SP), pp. 553–567 (May 2012)
5. Boyen, X., Dodis, Y., Katz, J., Ostrovsky, R., Smith, A.: Secure remote authentication using biometric data. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 147–163. Springer, Heidelberg (2005)
6. Brainard, J., Juels, A., Rivest, R.L., Szydlo, M., Yung, M.: Fourth-factor authentication: somebody you know. In: Conference on Computer and Communications Security: Proceedings of the 13th ACM Conference on Computer and Communications Security, vol. 30, pp. 168–178 (2006)
7. Chen, G., Kotz, D.: et al.: A survey of context-aware mobile computing research. Tech. rep., Technical Report TR2000-381, Dept. of Computer Science, Dartmouth College (2000)
8. Conti, M., Das, S.K., Bisdikian, C., Kumar, M., Ni, L.M., Passarella, A., Roussos, G., Tröster, G., Tsudik, G., Zambonelli, F.: Looking ahead in pervasive computing: Challenges and opportunities in the era of cyber–physical convergence. Pervasive and Mobile Computing 8(1), 2–21 (2012)
9. Elkhodary, A., Whittle, J.: A survey of approaches to adaptive application security. In: International Workshop on Software Engineering for Adaptive and Self-Managing Systems, ICSE Workshops SEAMS 2007, p. 16. IEEE (2007)
10. Evesti, A., Pantsar-Syväniemi, S.: Towards micro architecture for security adaptation. In: Proceedings of the Fourth European Conference on Software Architecture: Companion, pp. 181–188. ACM (2010)
11. Evesti, A., Suomalainen, J., Ovaska, E.: Architecture and knowledge-driven self-adaptive security in smart space. Computers 2(1), 34–66 (2013)
12. Fleischhacker, N., Manulis, M., Sadr-Azodi, A.: Modular design and analysis framework for multi-factor authentication and key exchange. Cryptology ePrint Archive, Report 2012/181 (2012), `http://eprint.iacr.org/`
13. Frankel, A., Maheswaran, M.: Feasibility of a socially aware authentication scheme. In: 6th IEEE Consumer Communications and Networking Conference, CCNC 2009, pp. 1–6 (January 2009)
14. Gentry, C., Mackenzie, P., Ramzan, Z.: Password authenticated key exchange using hidden smooth subgroups. In: Proceedings of the 12th ACM Conference on Computer and Communications Security, pp. 299–309. ACM (2005)
15. Hao, F.: On robust key agreement based on public key authentication. Security and Communication Networks (2012)

16. Honkola, J., Laine, H., Brown, R., Tyrkko, O.: Smart-m3 information sharing platform. In: 2010 IEEE Symposium on Computers and Communications (ISCC), pp. 1041–1046. IEEE (2010)
17. Hulsebosch, R., Bargh, M., Lenzini, G., Ebben, P., Iacob, S.: Context sensitive adaptive authentication. In: Kortuem, G., Finney, J., Lea, R., Sundramoorthy, V. (eds.) EuroSSC 2007. LNCS, vol. 4793, pp. 93–109. Springer, Heidelberg (2007)
18. Jager, T., Kohlar, F., Schäge, S., Schwenk, J.: Generic compilers for authenticated key exchange. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 232–249. Springer, Heidelberg (2010)
19. Jiang, X., Landay, J.: Modeling privacy control in context-aware systems. IEEE Pervasive Computing 1(3), 59–63 (2002)
20. Lee, Y., Kim, S., Won, D.: Enhancement of two-factor authenticated key exchange protocols in public wireless LANs. Computers & Electrical Engineering 36(1), 213–223 (2010)
21. Maji, H.K., Prabhakaran, M., Rosulek, M.: Attribute-based signatures. In: Kiayias, A. (ed.) CT-RSA 2011. LNCS, vol. 6558, pp. 376–392. Springer, Heidelberg (2011)
22. Park, Y.M., Park, S.K.: Two factor authenticated key exchange (take) protocol in public wireless LANs. IEICE Transactions on Communications 87(5), 1382–1385 (2004)
23. Pointcheval, D., Zimmer, S.: Multi-factor authenticated key exchange. In: Bellovin, S.M., Gennaro, R., Keromytis, A.D., Yung, M. (eds.) ACNS 2008. LNCS, vol. 5037, pp. 277–295. Springer, Heidelberg (2008)
24. Rathgeb, C., Uhl, A.: A survey on biometric cryptosystems and cancelable biometrics. EURASIP Journal on Information Security 2011(1), 1–25 (2011)
25. Raychoudhury, V., Cao, J., Kumar, M., Zhang, D.: Middleware for pervasive computing: A survey. In: Pervasive and Mobile Computing (2012)
26. Ryutov, T., Zhou, L., Neuman, C., Leithead, T., Seamons, K.E.: Adaptive trust negotiation and access control. In: Proceedings of the Tenth ACM Symposium on Access Control Models and Technologies, pp. 139–146. ACM (2005)
27. Salehie, M., Tahvildari, L.: Self-adaptive software: Landscape and research challenges. ACM Transactions on Autonomous and Adaptive Systems (TAAS) 4(2), 14 (2009)
28. Savola, R.M., Abie, H.: Development of measurable security for a distributed messaging system. International Journal on Advances in Security 2(4), 358–380 (2010)
29. Schechter, S., Egelman, S., Reeder, R.: It's not what you know, but who you know: a social approach to last-resort authentication. In: Proceedings of the 27th International Conference on Human Factors in Computing Systems, pp. 1983–1992. ACM (2009)
30. Schläger, C., Sojer, M., Muschall, B., Pernul, G.: Attribute-based authentication and authorisation infrastructures for e-commerce providers. In: Bauknecht, K., Pröll, B., Werthner, H. (eds.) EC-Web 2006. LNCS, vol. 4082, pp. 132–141. Springer, Heidelberg (2006)
31. Schneier, B.: Liars and outliers: enabling the trust that society needs to thrive. Wiley (2012)
32. Shah, S., Minhas, A., et al.: New factor of authentication: Something you process. In: International Conference on Future Computer and Communication, ICFCC 2009, pp. 102–106. IEEE (2009)

33. Sheikh, K., Wegdam, M., Sinderen, M.V.: Quality-of-context and its use for protecting privacy in context aware systems. Journal of Software 3(3), 83–93 (2008)
34. Tsang, P.P., Au, M.H., Kapadia, A., Smith, S.W.: Perea: Towards practical ttp-free revocation in anonymous authentication. In: Proceedings of the 15th ACM Conference on Computer and Communications Security, pp. 333–344. ACM (2008)
35. Yuan, E., Malek, S.: A taxonomy and survey of self-protecting software systems. In: 2012 ICSE Workshop on Software Engineering for Adaptive and Self-Managing Systems (SEAMS), pp. 109–118. IEEE (2012)
36. Yung, M.: On the evolution of user authentication: Non-bilateral factors. In: Pei, D., Yung, M., Lin, D., Wu, C. (eds.) Inscrypt 2007. LNCS, vol. 4990, pp. 5–10. Springer, Heidelberg (2008)