On the difficult tradeoff between security and privacy: challenges for the management of digital identities

David Arroyo[1], Jesus Diaz[2], and Víctor Gayoso[3]

Grupo de Neurocomputacion Biologica, Departamento de Ingenieria Informatica,
Escuela Politecnica Superior, Universidad Autonoma de Madrid
[1,2]{david.arroyo,jesus.diaz}@uam.es
Institute of Physical and Information Technologies (ITEFI),
Spanish National Research Council (CSIC), Madrid, Spain
[3]victor.gayoso@iec.csic.es

Abstract. The deployment of security measures can lead in many occasions to an infringement of users' privacy. Indeed, nowadays we have many examples about surveillance programs or personal data breaches in online service providers. In order to avoid the latter problem, we need to establish security measures that do not involve a violation of privacy rights. In this communication we discuss the main challenges when conciliating information security and users' privacy.

1 Introduction

Along the second half of the twentieth century there was a technological revolution that has led to the so-called *information era*. Information technologies have evolved from having a marginal position to being a cornerstone of today's economical activities. Certainly, in these days it is almost impossible to conceive the daily work without the usage of technological means related to information management.

This capital prominence of Information and Communication Technologies (ICT) is consequently endorsed by the digital agenda of the national and transnational organisations. For example, in the digital agenda of the European Union it is underlined that economical progress is currently built upon the proper concretion and management of ICT [1]. In fact, the *health* of modern democracy is heavily dependent on the application of ICT to enlarge and ensure governability. The result of such an effort is oriented to what it is coined as *e-democracy*[26], which cannot be attained unless users trust and use ICT appropriately and respectfully.

According to the cybersecurity strategy of the European Commission [1], it is demanded a supra-national effort to reinterpret the laws in *physical world* in the new coordinates of the *digital world*. The main goal is on shaping Internet as a democratic *agora* for sharing and discussing information on the grounds of free speech, data confidentiality and users' privacy protection. This complex objective

can be only achieved by creating and using adequate access and authorisation rules and, of course, by applying robust and efficient security measures.

On this point, we have to take into account that the performance of security procedures and methods should not imply an erosion of citizens' rights. As it is pointed out by Hanni M. Fakhour (staff attorney of the Electronic Frontier Foundation), any control measure and/or security procedure should not pose a threat to fundamental citizen rights such as confidentiality and privacy [17]. Furthermore, the implementation of technological and normative regulations is not an exclusive responsibility of government institutions and private enterprises: citizens are required to use ICT in a responsible way, and thus we have to be aware that most *cyber attacks* are enabled by the information trace that we leave in the Internet. Indeed, our visits to online social networks [34] and our continuous search for information drop an almost indelible fingerprint of ourselves [25].

In this paper we present a study of the most significant aspects of privacy protection when using cryptographic tools. The concept of privacy is far from being easily captured by a closed definition. In this communication, we have interpreted privacy with respect to the expected requirements in security systems. Thus, we have focused our study in mechanisms to preserve privacy through confidentiality protection (privacy as confidentiality), by means of convenient access control services (privacy as control), and on the grounds of easy-to-use solutions (privacy as practice). Accordingly, we have distinguished six challenges that should be faced to accomplish a fully integration of the previous highlighted domains.

2 Challenge 1: privacy enhanced secure data provenance

Data provenance is required to further protect information systems, since information assets cannot be protected just by assuming that confidentiality, integrity and availability are guaranteed. Certainly, in modern Information Security Management Systems (ISMS) it is not a good option to take for granted any expected behaviour from our systems. It is necessary to design and establish proper defences against information assets such as confidentiality, integrity and availability. After that, a continuous evaluation process is needed in order to confirm the likelihood of our protection measures and the suitability of the authentication and authorisation protocols. For such an examination underlying logging systems must be developed for capturing the different events that appear when using our ICT network to access and manage our information assets. In other words, auditability is another major concern in security engineering.

A critical step when creating audit trails consists in deciding the events to capture and the information needed to characterise each event. This definition is fundamental for intrusion detection, and thus the audit logs should be properly protected [32]. Here we have to consider both efficiency and privacy compliance as the current challenges with respect to data provenance in the scope of auditing. Regarding efficiency, we should bear in mind that the main operation to perform

on audit trails is derived from information search processes. If we are dealing with encrypted files, it implies that we need to decrypt all logs in order to look for events. While this could be a bottleneck, in practice we can solve it by using searchable encrypted logs [4]. Furthermore, since the main concern when encrypting logs is to avoid the threat of non-trusted storage servers and the application of anti-forensics techniques, we could use peer-to-peer (P2P) schemes to create split trust domains in order to reduce the effect of *malicious* individual storage servers [33].

As for privacy-respectful audits, we should consider that anonymisation and proper event coding are not an option but a requirement [7]. In specific, secure data provenance relies on four elements: access control, privacy, integrity, and accountability. As it occurs with the protection of audit logs, conventional encryption and authentication procedures are not the best solution. Aligned with the claim presented in [7], we should adopt solutions coming from the field of the Privacy Enhancing Technologies (PET). This being the case, the challenge of secure data provenance should be tackled by considering homomorphic encryption [18], secure multi party computation [12], multi signatures [8], group signatures [10], ring signatures [11], etc.

3 Challenge 2: client-side encryption

The emergence of *cloud computing* is one of the most relevant novelties in the technological scenario in the last five years. It entails a low cost opportunity to share and store data, which is specially important for Small and Medium Enterprises (SMEs). Actually, platforms such as Dropbox or Google Drive make possible to backup our information assets for free. Nevertheless, we have to take into account that the final storage servers cannot be assumed to be fully trusted.

Certainly, in most situations the adoption of a cloud computing solution implies some form of data outsourcing, so there is not a clear guarantee about the way our data are going to be treated and protected. This is the main reason behind the design of new procedures enabling an active role for the client of cloud computing services. These initiatives are intended to create software products to provide users with the proper encryption tools, so each item of data is encrypted before it is sent to the cloud [20]. As an important effort in client-side encryption, we have to pinpoint all the contributions to solve the main security problems (due to some form of code injection) in web applications [31]. In addition, we can find several meaningful proposals handling the shortcomings of homomorphic encryption to create privacy-respectful web platforms [27].

4 Challenge 3: client-side integrity verification

Client-side encryption is not the only means to manage zero trust models in cloud computing [37]. Indeed, data fragmentation is another important issue that should be considered when pondering the pros and cons of outsourcing data storage. The main problem with data fragmentation is that we need to

have several copies of each data fragment (otherwise we cannot recover the original information), and an exhaustive protocol for data integrity verification is also demanded in order to guarantee data coherence and consistence. Integrity verification is a commitment in all the different schemes of cloud computing where we do not have a complete trust in the service provider [23]. Moreover, if digital signatures are used to carry out integrity validation, then schemes as group signatures could be integrated into our system to protect users' anonymity [9].

5 Challenge 4: anonymity management

Being privacy one of the basic rights in current societies, different approaches have been suggested in order to guarantee it. Anonymity is certainly one of the fundamental alternatives: if the identities of the parties inside a system are not known, it is harder to violate their privacy. However, as it happens with all privacy-respectful techniques, it may be misused for illegitimate purposes, giving institutions and governments a reason to ban it[1]. Accordingly, it would probably also make it harder for companies (who, as stated in [13] also possess private information of value to governments) to decline government requests and, of course, to trust anonymising systems. As matter of fact, this risk has not gone unnoticed to systems providing anonymity[2].

One logical way to address this issue is to incorporate mechanisms that allow the detection and sanction of illegitimate anonymous actions. However, for this to be possible, anonymity management must be somehow included. Efforts in this direction have already been made, which allow to create X.509 anonymous identities based on group signatures [6,10] and subsequently manage and revoke them if necessary [16]. Moreover, specific applications have been proposed for systems such as Tor [15], but also as an additional layer for these anonymising networks [21,22,35,36]. However, this is a concern that needs to be carefully dealt with, since a significant reduction in anonymity would certainly be rejected by the users of anonymous communication systems.

6 Challenge 5: digital content life-cycle management

The definition and implementation of Digital Rights Management (DRM) systems is one of the most difficult tasks in the current technological scenario. Although DRM is usually assumed to be just a mechanism to protect intellectual

[1] A recent example of privacy enhancing technologies being questioned by a government is that of Cameron in the UK who, after the attack on Charlie Hebdo in Paris, stated: "*are we going to allow a means of communications where it simply is not possible to do that [listen in on communications]?*" `http://www.theguardian.com/technology/2015/jan/15/david-cameron-encryption-anti-terror-laws`.

[2] See, for instance, the call made by Tor: `https://blog.torproject.org/blog/call-arms-helping-internet-services-accept-anonymous-users`.

property, it also provides privacy protection as a result of avoiding information leakage in assets with Personal Identifiable Information (PII) [2]. DRM systems can (and, in some cases, should) be extended considering P2P privacy-respectful platforms [29] and Private Information Retrieval protocols (PIR) [3].

7 Challenge 6: usable identity management systems

The claim for assuming the security-by-design and privacy-by-design paradigms is a recurrent chant in recent contributions in cryptography engineering [19]. In this regard, standards and well-known technologies are a basic set to design new security systems, since they are continuous and carefully evaluated by the information security community. This initial selection of technologies should be further complemented with a explicit definition of security assumptions and a correct analysis and validation of the underlying security protocols [14].

However, the success of a security solution is not possible without the acceptance of end users. On this point, we have to bear in mind that the low users' acceptance of encryption [38] is even worse when considering the broader spectrum of PET [30]. Therefore, it is highly advisable to acknowledge and learn from recent contributions on creating usable authentication procedures [24] and enforcing privacy settings online [5]. In fact, this last concern is of paramount importance in online services, since the related providers collect and manage PII whereas the user generally has only partial knowledge about the proper and legitimate use of his or her data [28].

8 Conclusion

In this contribution we have summarised the main open problems in the crossed domain of security and privacy, providing an sketch of the most critical challenges in that field. We have provided a list of the limitations in current systems implementations, and we have also discussed some possible ways to solve those shortcomings.

As the main lesson of our study, we can conclude that an adequate collaboration between the cryptology community and the security engineering collective is necessary. There are plenty of theoretical solutions to handle the problems that we have underlined in this paper. However, in many occasions those theoretical solutions are difficult to implement and tend to incur in excesive computational costs.

Regarding this issue, software engineers could help to adapt theoretical proposals to already deployed infrastructures, taking into account the usability of the final products as a mandatory requisite. Moreover, this help should be built upon a thorough examination of each step of the design, implementation and maintenance phases of the corresponding software products. In this regard, software engineers could call for assistance from formal system analysts and information theory experts in order to better study and characterise data breaches.

Acknowledgements

This work was supported by Comunidad de Madrid (Spain) under the project S2013/ICE-3095-CM (CIBERDINE).

References

1. EU Cybersecurity plan to protect open internet and online freedom and opportunity - Cyber Security strategy and Proposal for a Directive. http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security (February 2013), http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security
2. Aaber, Z.S., Crowder, R.M., Fadhel, N.F., Wills, G.B.: Preventing document leakage through active document. In: Internet Security (WorldCIS), 2014 World Congress on. pp. 53–58 (Dec 2014)
3. Backes, M., Gerling, S., Lorenz, S., Lukas, S.: X-pire 2.0: A user-controlled expiration date and copy protection mechanism. In: Proceedings of the 29th Annual ACM Symposium on Applied Computing. pp. 1633–1640. SAC '14, ACM, New York, NY, USA (2014), http://doi.acm.org/10.1145/2554850.2554856
4. Backes, M., Maffei, M., Pecina, K.: Automated synthesis of privacy-preserving distributed applications. Proc. of ISOC NDSS (2012), http://www.lbs.cs.uni-saarland.de/publications/asosda-long.pdf
5. Balsa, E., Brandimarte, L., Acquisti, A., Diaz, C., Gurses, S.: Spiny CACTOS: OSN Users Attitudes and Perceptions Towards Cryptographic Access Control Tools. Proceedings 2014 Workshop on Usable Security (2014), https://www.internetsociety.org/doc/spiny-cactos-osn-users-attitudes-and-perceptions-towards-cryptographic-access-control-tools
6. Benjumea, V., Choi, S.G., Lopez, J., Yung, M.: Anonymity 2.0 - X.509 extensions supporting privacy-friendly authentication. In: Cryptology and Network Security, 6th International Conference, CANS 2007, Singapore, December 8-10, 2007, Proceedings. pp. 265–281 (2007), http://dx.doi.org/10.1007/978-3-540-76969-9_17
7. Bertino, E., Ghinita, G., Kantarcioglu, M., Nguyen, D., Park, J., Sandhu, R., Sultana, S., Thuraisingham, B., Xu, S.: A roadmap for privacy-enhanced secure data provenance. Journal of Intelligent Information Systems 43(3), 481–501 (2014)
8. Boyd, C.: Digital multisignatures. Cryptography and coding pp. 241–246 (1989)
9. Camenisch, J.: Efficient anonymous fingerprinting with group signatures. In: Advances in Cryptology-ASIACRYPT 2000, pp. 415–428. Springer (2000)
10. Chaum, D., van Heyst, E.: Group signatures. In: Advances in Cryptology - EUROCRYPT '91, Workshop on the Theory and Application of of Cryptographic Techniques, Brighton, UK, April 8-11, 1991, Proceedings. pp. 257–265 (1991), http://dx.doi.org/10.1007/3-540-46416-6_22
11. Chow, S.S., Yiu, S.M., Hui, L.C.: Efficient identity based ring signature. In: Applied Cryptography and Network Security. pp. 499–512. Springer (2005)
12. Damgård, I., Pastro, V., Smart, N., Zakarias, S.: Multiparty computation from somewhat homomorphic encryption. In: Advances in Cryptology–CRYPTO 2012, pp. 643–662. Springer (2012)

13. Díaz, C., Tene, O., Gürses, S.: Hero or Villain: The Data Controller in Privacy Law and Technologies. Ohio State Law Journal 74 (2013)
14. Diaz, J., Arroyo, D., Rodriguez, F.B.: A formal methodology for integral security design and verification of network protocols. The Journal of Systems and Software Accepted: In Press. DOI: http://dx.doi.org/10.1016/j.jss.2013.09.020
15. Diaz, J., Arroyo, D., Rodriguez, F.B.: Fair anonymity for the Tor network. CoRR abs/1412.4707 (2014), http://arxiv.org/abs/1412.4707
16. Diaz, J., Arroyo, D., Rodriguez, F.B.: New x.509-based mechanisms for fair anonymity management. Computers & Security 46, 111–125 (2014), http://dx.doi.org/10.1016/j.cose.2014.06.009
17. Fakhoury, H.M.: Technology and privacy can co-exist. The New York Times (December 12,2012), http://www.nytimes.com/roomfordebate/2012/12/11/privacy-and-the-apps-you-download/privacy-and-technology-can-and-should-co-exist
18. Gentry, C.: A fully homomorphic encryption scheme. Ph.D. thesis, Stanford University (2009)
19. Gurses, S., Troncoso, C., Diaz, C.: Engineering Privacy by design. In: Computers, Privacy & Data Protection. vol. 317, pp. 1178–9 (Aug 2011), http://www.ncbi.nlm.nih.gov/pubmed/17761870
20. He, W., Akhawe, D., Jain, S., Shi, E., Song, D.: Shadowcrypt: Encrypted web applications for everyone. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. pp. 1028–1039. ACM (2014)
21. Henry, R., Henry, K., Goldberg, I.: Making a nymbler nymble using verbs. In: Privacy Enhancing Technologies. pp. 111–129 (2010)
22. Johnson, P.C., Kapadia, A., Tsang, P.P., Smith, S.W.: Nymble: Anonymous ip-address blocking. In: Privacy Enhancing Technologies. pp. 113–133 (2007)
23. Juels, A., Kaliski Jr, B.S.: Pors: Proofs of retrievability for large files. In: Proceedings of the 14th ACM conference on Computer and communications security. pp. 584–597. Acm (2007)
24. Li, S., Sadeghi, A.R., Heisrath, S., Schmitz, R., Ahmad, J.: hpin/htan: A lightweight and low-cost e-banking solution against untrusted computers. In: Danezis, G. (ed.) Financial Cryptography and Data Security, Lecture Notes in Computer Science, vol. 7035, pp. 235–249. Springer Berlin Heidelberg (2012), http://dx.doi.org/10.1007/978-3-642-27576-0_19
25. Long, J., Skoudis, E., Eijkelenborg, A.v.: Google Hacking for Penetration Testers. Syngress Publishing (2004)
26. OECD: The E-Government Imperative (Complete Edition - ISBN 9264101179), E-Government Studies, vol. 2003 (2003)
27. Popa, R.A., Stark, E., Valdez, S., Helfer, J., Zeldovich, N., Balakrishnan, H.: Building web applications on top of encrypted data using mylar. In: Proceedings of the 11th USENIX Symposium on Networked Systems Design and Implementation, NSDI 2014, Seattle, WA, USA, April 2-4, 2014. pp. 157–172 (2014), https://www.usenix.org/conference/nsdi14/technical-sessions/presentation/popa
28. Preibusch, S., Peetz, T., Acar, G., Berendt, B.: Purchase details leaked to PayPal. In: Financial Cryptography (2015), https://lirias.kuleuven.be/handle/123456789/476251
29. Qureshi, A., MegÃas, D., RifÃ -Pous, H.: Framework for preserving security and privacy in peer-to-peer content distribution systems. Expert Systems with Applications 42(3), 1391 – 1408 (2015), http://www.sciencedirect.com/science/article/pii/S0957417414005351

30. Renaud, K., Volkamer, M., Renkema-Padmos, A.: Why doesn't jane protect her privacy? In: Privacy Enhancing Technologies. pp. 244–262. Springer (2014)
31. Ryck, P.D.: Client-Side Web Security: Mitigating Threats against Web Sessions. Ph.D. thesis, University of Leuven (2014), https://lirias.kuleuven.be/bitstream/123456789/471059/1/thesis.pdf
32. Schneier, B., Kelsey, J.: Secure audit logs to support computer forensics. ACM Transactions on Information and System Security (TISSEC) 2(2), 159–176 (1999)
33. Seneviratne, O., Kagal, L.: Enabling privacy through transparency. In: Privacy, Security and Trust (PST), 2014 Twelfth Annual International Conference on. pp. 121–128. IEEE (2014)
34. Thomas, K., McCoy, D., Grier, C., Kolcz, A., Paxson, V.: Trafficking fraudulent accounts: The role of the underground market in twitter spam and abuse. In: Proceedings of the 22nd Usenix Security Symposium (2013)
35. Tsang, P.P., Au, M.H., Kapadia, A., Smith, S.W.: Blacklistable anonymous credentials: blocking misbehaving users without TTPs. In: ACM Conference on Computer and Communications Security. pp. 72–81 (2007)
36. Tsang, P.P., Kapadia, A., Cornelius, C., Smith, S.W.: Nymble: Blocking misbehaving users in anonymizing networks. IEEE Trans. Dependable Sec. Comput. 8(2), 256–269 (2011)
37. De Capitani di Vimercati, S., Erbacher, R., Foresti, S., Jajodia, S., Livraga, G., Samarati, P.: Encryption and fragmentation for data confidentiality in the cloud. In: Aldini, A., Lopez, J., Martinelli, F. (eds.) Foundations of Security Analysis and Design VII, Lecture Notes in Computer Science, vol. 8604, pp. 212–243. Springer International Publishing (2014), http://dx.doi.org/10.1007/978-3-319-10082-1_8
38. Whitten, A., Tygar, J.D.: Why johnny can't encrypt: A usability evaluation of pgp 5.0. In: Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8. pp. 14–14. SSYM'99, USENIX Association, Berkeley, CA, USA (1999), http://dl.acm.org/citation.cfm?id=1251421.1251435