Overview of publications

Jerry den Hartog

2013

This text gives an overview of my research activities and associated publications. This consists of two main lines of work. Recent work is within the area of security while earlier work focusses on formal methods for probabilistic systems.

1 Security

The overall goal of this research is to create a trustworthy and trusted (i.e. perceived to be trustworthy) architecture for (large scale) distributed systems (such as internet, rfid systems, cloud based systems, etc.) applicable to different key areas (health care, smart energy and mobility, etc.) The different sub-lines mentioned below all contribute to this overall line; establishing the basic requirements for trust in a system, in communication and hardware and addressing key contributing factors such as security and privacy protection.

1.1 Trust and Privacy

In this research activity we look at the management and user perception of trust and factors that contribute to these such as privacy protection, security, reputation systems, etc. Related projects (see `http://www.win.tue.nl/sec/research.html`) are Trusted Architecture for Securely Shared Services (TAS3), Trusted Healthcare Services (THeCS), POSEIDON: System Evolvability and Reliability of Systems of Systems, PEARL: Privacy Enhanced security Architecture for RFID Labels, Mobiman: Identity Management for Mobile Devices, Trust in the Cloud and Secure and privacy-aware mobile identity management.

Publications In [11] trust management techniques applies to the e-business setting are described and a model for trust and trust perceptions in this setting is developed. In [9] the factors contributing to trust perception are identified and their importance shown to be dependent on the knowledge of the user. One conclusion from this work is that, though people find privacy important, they do not read privacy policies. In [10, 12] we aim at quantifying one of the factors contributing to trust perception namely privacy and at supporting the user in assessing privacy policies.

In [1] and [23] we describe a flexible trust management architecture for service-oriented systems which integrates different types of trust management systems into a standard XACML style authentication framework. In [6] we apply this in an overall security and privacy architecture for cloud systems.

In [38] effects of trust delegation in the credential based decentralized trust management (DTM) are studied. To be able to maintain safety goals in the presence of trust delegation we compute minimal restrictions for a set of principles to achieve their goals using the object capability system Scoll. In this way collaborating principles can maintain safety in the presence of delegations (potentially including delegations to non-collaborating principles).

In [24] different trust management techniques are described and their effectiveness linked to the accountability in the form of ability to cause regret when a trusted party misuses the trust placed in it.

In [13] we introduce a trust management language RT- which adds a restricted form of negation to the standard RT trust management language thus admitting a controlled form of non-monotonicity. The semantics of RT- is presented in terms of the well-founded semantics for Logic Programs. An implementation of RT- is given using XSB.

1.2 Information Flow Analysis

In this research activity we look at protecting flows of information rather than single data items at a fixed location. Declassification, an important concept to make information flow practical, was a key subject of study in the S-Mobile project. IN4STARS: INformation INteroperability & INtelligence INteroperability by STatistics, Agents, Reasoning and Semantics also address declassification through information sanitiation.

Publications In [37] a system is introduced for declassification policies which are decoupled from the programs that use them. Declassification is needed as the well-known notion of non-interference is often too restrictive. In most approaches for declassification the declassification policies are embedded in the program itself or heavily tied to the variables in the program being analyzed, thereby providing little separation between the code and the policy. This essentially require that the code be trusted, since to trust that the correct policy is being enforced, we need to trust the source code. In this paper we propose a framework in which declassification policies are related to the source code being analyzed via its I/O channels. The analysis works by constructing a conservative approximation of expressions over input channel values that could be output by the program, and by determining whether all such expressions satisfy the declassification requirements stated in the policy. We prove that if a program is considered safe according to our analysis then it satisfies a property we call Policy Controlled Release, which formalizes information-flow correctness according to our notion of declassification policy.

1.3 Formal analysis of Protocols

In this research activity we model and validate security and privacy properties of protocols and algorithms, ranging from cryptographic primitives to mobile and RFID identification and communication protocols. Related project are PEARL and Mobiman, uCAN and Secure and privacy-aware mobile identity management.

Publications Systems dealing with personal information are legally required to satisfy the principle of data minimisation. However understanding the privacy implications of running multiple protocols each using personal data can be a challenging task. In [41] we present TRIPLEX, a framework for the analysis of data minimisation in privacy-enhancing protocols.

There is no agreement in literature on the exact definition of unlinkability. In [2] different notions of unlinkability from literature are compared and shown to have subtle differences. Conditions, which are reasonable to expect in an RFID setting, are then introduced and proven to be sufficient to link different notions, i.e. under a set of conditions different unlinkability notions coincide.

In [3] a formal model for privacy guarantees of RFID tag protocols is introduces. The notions unlinkability and forward privacy are expressed and related in a formal model based on the applied pi calculus. For a generic class of simple privacy protocols sufficient and necessary conditions for unlinkability and forward privacy are given. These conditions are based on the concept of frame independence that we develop in this paper. Finally, we apply our techniques to two identification protocols, formally proving their privacy guarantees.

In [7] we introduce a Probabilistic Hoare-style logic for Game-based Cryptographic Proofs by extending a Probabilistic Hoare-style logic [25, 29, 26] to formalize game-based cryptographic proofs. Our approach provides a systematic and rigorous framework, thus preventing errors from being introduced. We illustrate our technique by proving semantic security of ElGamal.

The paper [27] is a move towards mechanized correctness proofs for cryptographic algorithms using the method introduced in [7]. The probabilistic Hoare logic includes a standard weakening rule which uses implication between predicates which so far only has a semantical definition. By providing a partial axiomatization of this implication purely syntactic reasoning is enabled, which is illustrated on the results of [7].

The paper [31] treats denial-of-service (DoS) attacks by link-layer jamming in wireless sensor networks. By exploiting the semantics of the link-layer protocol (aka MAC protocol), an attacker can achieve better efficiency than blindly jamming the radio signals alone. We investigate some jamming attacks of S-MAC, what level of effectiveness and efficiency the attack can potentially achieve, and what countermeasures can be implemented against these attacks.

The paper [39] defines functional Principles of Service Discovery for robust, registry-based service discovery. The Service Discovery Protocol FRODO is then formally verified and shown to satisfy these principles. (This paper does not specifically address security.)

1.4 A-posteriori compliance Control: The audit logic

In this research activity we propose a different approach to protecting data addressing some inherent drawbacks of preventative access control. User are held accountable for their actions after they have performed them, allowing checking of purpose and use of data rather than only access to data. Note that this does require a setting (i.e. a trust model) in which you can hold users accountable.

Publications Audit-based compliance control [5, 8] is a framework for a-posteriori policy compliance control. A formal audit procedure is defined in which users may be asked to justify that actions they performed were in compliance with policies. We also define a logging mechanism that allow honest users to gather the information needed to perform this justification. The framework is shown to be tractable and an implementation in form of a proof checker and prove finder are provided. We argue that in a number of settings, such as collaborative work environments, where a small group of users create and manage document in a decentralized way, our framework is a more flexible approach for controlling the compliance to policies than standard a-priory access control mechanisms.

In [4] the framework is applied in the setting of agents.

In [16, 15] the use of the audit-based compliance control for privacy is described and compared to other privacy languages and systems such as P3P and EPAL.

In the report [14] audit-based compliance control is applied in the setting of electronic health record systems.

1.5 Side channel analysis of smartcards

In this research activity we look at the trustworthiness of cryptographic hardware, focussing on the vulnerability of such devices to side channel analysis. Recent projects on this topic are Pinpas JC and ASCA.

Publications In [36] a method for optimizing differential power analysis (DPA) attacks is presented which in addition to looking for a peak indicating the correct key hypothesis also considers expected peak heights for other key candidates. Significant peaks for other key candidates, so called ghost peaks, are normally a problem in DPA but here they are actually used to strengthen the attack.

In [32] it shown that first and second-order DPA attacks can exploit intermediate results further into the inner rounds of computation than generally believed by using partially fixed plain/cypher texts. This is demonstrated with attacks on AES and on AES with specific DPA countermeasures.

In [35] a power analysis attack is given against an S-Box implementation scheme which is provably secure against first and second order differential power analysis. The scheme includes While not technically a first order DPA attack, the attack should be feasible in any setting where a first order DPA attack is feasible.

In [34] a simple yet effective metric is developed to rank the intrinsic vulnerable to DPA attacks of individual operations. The metric is validated with simulations and experiments on hardware.

In [33] the results of a comparative study of some popular Java Cards on the market are presented. Eight different cards from four manufacturers are analyzed at two levels; (i) a documentation-based comparison, also taking other publicly available resources into account, (ii) an actual hands-on testing with software developed specifically for this purpose. The investigations focus on basic functionality, secure channels, the transaction mechanism, support symmetric and asymmetric cryptography, Global Platform and Open Platform compliance, and garbage and memory management.

The PINPAS tool [22, 19, 30] is an instruction-level interpreter for smartcard assembler languages, augmented with facilities to study side-channel vulnerabilities, such as simulating power consumption and performing DPA on the simulated power traces. The PINPAS tool supports the testing of algorithms for vulnerability to SPA, DPA, etc. at the software level.

In [30] the results from a power analysis of the AES and RSA algorithms by simulation using the PINPAS tool are presented. Using the Hitachi H8/300 assembler simulation in the PINPAS tool, the vulnerability for power analysis attacks of straightforward AES and RSA implementations is examined. In case a vulnerability is found countermeasures are added to the implementation that attempt to counter power analysis attacks. After these modifications the analysis is performed again and the new results are compared to the original results.

In [19] applications of the PINPAS tool are discussed. The usage of the tool is illustrated using the common AES and RSA algorithms. Vulnerabilities of the implementations are identified and protective measures added. It is argued, that the tool can be instrumental for the design and realization of secure smartcard implementations in a systematic way.

In [22] the PINPAS tool is introduced. Exploitation of the PINPAS tool allows for the identification of weaknesses in the implementation in an early stage of development. A toy algorithm is discussed to illustrate the usage of the tool.

2 Probabilistic systems

Earlier work focusses on formal methods for the modeling and reasoning about probabilistic systems.

2.1 Semantics

This work focusses on comparative semantics in a metric setting. Comparative semantics provides an operational a denotational model and the relation between the two. In the metric setting, the domains user are metric spaces guaranteeing the existence of unique fixed points.

In [40] a comparative semantics for or-parallel Prolog with commit is given.

In [18] builds different operational semantics for the combination of concurrency, nondeterministic and probabilistic choice.

In [17] a comparative semantics is given for the combination of probabilistic and non-deterministic choice, distinguishing local and global interpretations of these operations.

In [20] gives a comparative semantics to action refinement and synchronization in an interleaving setting. The trace based operational model uses a transition system with syntactical refinement sequences. The denotational model equates statements under all (semantical) refinements and is shown to be fully abstract w.r.t. the operational model.

In [21] shows that the model for action refinement can be applied in a probabilistic setting by extending the language and the fully abstract comparative semantics with probabilistic choice.

In [28] a functor to build metric spaces of probability measures is described.

In [26] describes different semantical models which have been extended with some form of probabilistic choice.

2.2 Logic

In [25, 29, 26] a Hoare-style logic for reasoning about probabilistic programs is given. It is shown to be sound with respect to the denotational semantics of the programs. (Use of this logic in the setting of security is described in Section 1.3.)

References

[1] K. Böhm, S. Etalle, J. I. den Hartog, C. Hütter, S. Trabelsi, D. Trivellato, and N. Zannone. A flexible architecture for privacy-aware trust management. *Journal of Theoretical and Applied Electronic Commerce Research*, 5(2):77–96, August 2010.

[2] M. Bruso, K. Chatzikokolakis, S. Etalle, and J.I. den Hartog. Linking unlinkability. In C. Palamidessi and M.D. Ryan, editors, *Proceedings of the 7th International Symposium on Trustworthy Global Computing (TGC 2012). Revised Selected Papers.*, volume LNCS 8191.

[3] M. Bruso, K. Chatzikokolakis, and J.I. den Hartog. Formal verification of privacy for rfid systems. In *Proceedings of the 23rd IEEE Computer Security Foundations Symposium (CSF'10, Edinburgh, UK, July 17-19, 2010)*, pages 75–88. IEEE Computer Society, 2010.

[4] J. G. Cederquist, R. J. Corin, M. A. C. Dekker, S. Etalle, and J. I. den Hartog. An audit logic for accountability. In A. Sahai and W. H. Winsborough, editors, *6th Int. Workshop on Policies for Distributed Systems*

& Networks (POLICY), Stockholm, Sweden, pages 34–43, Los Alamitos, California, June 2005. IEEE Computer Society.

[5] J. G. Cederquist, R. J. Corin, M. A. C. Dekker, S. Etalle, J. I. den Hartog, and G. Lenzini. Audit-based compliance control. *International Journal of Information Security*, 6(2-3):133–151, 2007.

[6] D.W. Chadwick, S.F. Lievens, J.I. den Hartog, A. Pashalidis, and J. Alhadeff. My private cloud overview : a trust, privacy and security infrastructure for the cloud. In *Proceedings of the 4th IEEE International Conference on Cloud Computing (CLOUD 2011)*, pages 752–753. IEEE Computer Society, 2011.

[7] R. J. Corin and J. I. den Hartog. A probabilistic hoare-style logic for game-based cryptographic proofs. In M. Bugliesi, B. Preneel, and V. Sassone, editors, *ICALP 2006 track C, Venice, Italy*, volume 4052 of *Lecture Notes in Computer Science*, pages 252–263, Berlin, July 2006. Springer-Verlag.

[8] R. J. Corin, S. Etalle, J. I. den Hartog, G. Lenzini, and I. S. Staicu. A logic for auditing accountability in decentralized systems. In T. Dimitrakos and F. Martinelli, editors, *2nd Int. Workshop on Formal Aspect of Security and Trust (FAST), Toulouse, France*, volume IFIP 173, pages 187–201, Berlin, August 2004. Springer-Verlag.

[9] E. Costante, J.den Hartog, and M. Petkovic. On-line trust perception: What really matters. In *Proceedings of the 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST'11)*, pages 52–59. IEEE Computer Society, 2011.

[10] E. Costante, J.I. den Hartog, and M. Petkovic. What websites know about you - privacy policy analysis using information extraction. In *Proceedings of the 7th DPM International Workshop on Data Privacy Management and Autonomous Spontaneous Security. (Revised Selected Papers)*, volume LNCS 7731.

[11] E. Costante, J.I. den Hartog, and M. Petkovic. Trust management and user's trust perception in e-business (chapter 14). In E. Kajan, F.D. Dorloff, and I. Bedini, editors, *Handbook of research on e-business standards and protocols : documents, data and advanced web technologies*, pages 321–341. IGI Global, 2012.

[12] E. Costante, Y. Sun, M. Petkovic, and J.I. den Hartog. A machine learning solution to assess privacy policy completeness. In *Proceedings of the 2012 ACM Workshop on Privacy in the Electronic Society (WPES co-located with CCS 2012)*, pages 91–96. ACM, 2012.

[13] M. Czenko, H. Tran, J.M. Doumen, S. Etalle, P.H. Hartel, and J.I. den Hartog. Nonmonotonic trust management for p2p applications. In S. Mauw, V. Isarny, and C. Cremers, editors, *Proceedings of the First International*

Workshop on Security and Trust Management (STM'05), Milan, Italy, volume Vol. 157(3) of *Electronic Notes in Theoretical Computer Science*, pages 113–130. Elsevier Science, 2005.

[14] M. A. C. Dekker, J. I. den Hartog, and S. Etalle. Audit-based compliance control (ac2) for ehr systems. Technical Report TR-CTIT-07-46, Centre for Telematics and Information Technology University of Twente, Enschede, 2007.

[15] M. A. C. Dekker, S. Etalle, and J. I. den Hartog. Privacy in an ambient world. Technical Report TR-CTIT-06-16, Centre for Telematics and Information Technology University of Twente, Enschede, April 2006.

[16] M. A. C. Dekker, S. Etalle, and J. I. den Hartog. Privacy policies. In M. Petkovic and W. Jonker, editors, *Security, Privacy and Trust in Modern Data Management*, volume XVIII of *Data-Centric Systems and Applications*, pages 383–397. Springer Verlag, Berlin, 2007.

[17] J. I. den Hartog. Comparative semantics for a process language with probabilistic choice and non-determinism. Technical Report IR-445, Vrije Universiteit, Amsterdam, 1998.

[18] J. I. den Hartog and E. P. de Vink. Mixing up nondeterminism and probability: A preliminary report. In *PROBMIV'98, First International Workshop on Probabilistic Methods in Verification, Indianapolis, Indiana*, volume 22 of *Electronic Notes in Theoretical Computer Science*, pages 88–110, Amsterdam, June 1998. Elsevier.

[19] J. I. den Hartog and E. P. de Vink. Virtual analysis and reduction of side-channel vulnerabilities of smartcards. In T. Dimitrakos and F. Martinelli, editors, *2nd Int. Workshop on Formal Aspect of Security and Trust (FAST), Toulouse, France*, volume IFIP 173, pages 85–98, Boston, Massachusetts, August 2004. Kluwer Academic Publishers.

[20] J. I. den Hartog, E. P. de Vink, and J. W. de Bakker. Full abstractness of a metric semantics for action refinement. *Fundamenta Informaticae*, 40:335–382, 1999.

[21] J. I. den Hartog, E. P. de Vink, and J. W. de Bakker. Metric semantics and full abstractness for action refinement and probabilistic choice. In T. Hurley, M. Mac an Airchinnigh, M. Schellekens, and A. Seda, editors, *MFCSIT2000, The First Irish Conference on the Mathematical Foundations of Computer Science and Information, Cork, Ireland*, volume 40 of *Electronic Notes in Theoretical Computer Science*, pages 72–99, Amsterdam, March 2001. Elsevier.

[22] J. I. den Hartog, J. Verschuren, E. P. de Vink, J. Vos, and W. Wiersma. Pinpas: A tool for power analysis of smartcards. In D. Gritzalis, S. De Capitani di Vimercati, P. Samarati, and S. K. Katsikas, editors, *18th IFIP*

TC11 Int. Conf. on Information Security and Privacy in the Age of Uncertainty (SEC), Athens, Greece, pages 453–457, Boston, Massachusetts, 2003. Kluwer Academic Publishers.

[23] J.I. den Hartog, C. Hütter, and S. Trabelsi. Combined trust managemeent architecture (extended abstract). `http://www.eife-l.org/publications/eportfolio/proceedings2/lfl2010/lfl2010proceedings.pdf`, 2010.

[24] S. Etalle, J. I. den Hartog, and S. Marsh. Trust and punishment (invited paper). In *Proceedings of the 1st International Conference on Autonomic Computing and Communication Systems, Autonomics, Rome, Italy*, number 302 in ACM International Conference Proceeding Series. ACM: Association for Computing Machinery, December 2007.

[25] J.I. den Hartog. Verifying probabilistic programs using a Hoare like logic. In P.S. Thiagarajan and R. Yap, editors, *LNCS 1742 (ASIAN'99)*, pages 113–125. Springer, 1999.

[26] J.I. den Hartog. *Probabilistic Extensions of Semantical Models.* PhD thesis, Vrije Universiteit Amsterdam, 2002.

[27] J.I. den Hartog. Towards mechanized correctness proofs for cryptographic algorithms: Axiomatization of a probabilistic hoare style logic. *Science of Computer Programming*, 74(1-2):52–63, 2008.

[28] J.I. den Hartog and E.P. de Vink. Building metric structures with the maes-factor. In F.S. de Boer, M. van der Heijden, and P. Klint, editors, *Liber amicorum Jaco de Bakker*, pages 93–107. CWI, Amsterdam, 2002.

[29] J.I. den Hartog and E.P. de Vink. Verifying probabilistic programs using a Hoare like logic. *International Journal of Foundations of Computer Science*, 13(3):315–340, 2002.

[30] G. Hollestelle, W. Burgers, and J. I. den Hartog. Power analysis on smartcard algorithms using simulation. Technical report CSR 04-22, Eindhoven University of Technology, Eindhoven, 2004.

[31] Y. W. Law, P. H. Hartel, J. I. den Hartog, and P. J. M. Havinga. Link-layer jamming attacks on s-mac. In *2nd European Workshop on Wireless Sensor Networks (EWSN), Istanbul, Turkey*, pages 217–225, Los Alamitos, California, January 2005. IEEE Computer Society.

[32] J. Lu, J. Pan, and J. den Hartog. Principles on the security of aes against first and second-order differential power analysis. In Jianying Zhou and Moti Yung, editors, *Proceedings of the 8th International Conference on Applied Cryptography and Network Security (ACNS'10)*, volume 6123 of *Lecture Notes in Computer Science*, pages 168–185. Springer-Verlag, 2010.

[33] W. Mostowski, J. Pan, S. Akkiraju, E.P. de Vink, E. Poll, and J.I. den Hartog. A comparison of java cards : state-of-affairs 2006. Technical Report CSR 07-06, Eindhoven University of Technology, Eindhoven, 2006.

[34] J. Pan, J.I. den Hartog, and E.P. de Vink. An operation-based metric for dpa resistance. In *Proc. IFIP 23rd International Information Security Conferenfce (SEC08)*, IFIP Conference Proceedigns, Vol. 278, pages 429–443. Springer-Verlag, 2008.

[35] J. Pan, J. Lu, and J.I. den Hartog. You cannot hide behind the mask: Power analysis on a provably secure s-box implementation. In H.Y. Youm and M. Yung, editors, *Information Security Applications (10th International Workshop, WISA 2009, Busan, Korea, August 25-27, 2009, Revised Selected Papers)*, Lecture Notes in Computer Science, Vol. 5932, pages 178–192. Springer, 2009.

[36] J. Pan, J.G.J. van Woudenberg, J.I. den Hartog, and M.F. Witteman. Improving dpa by peak distribution analysis.

[37] B. Pontes Soares Rocha, S. Bandhakavi, J. I. den Hartog, W. H. Winsborough, and S. Etalle. Towards static flow-based declassification for legacy and untrusted programs. In *IEEE Symposium on Security and Privacy, Oakland, California*, pages 93–108, USA, May 2010. IEEE Society press.

[38] A.O.D. Spiessens, J.I. den Hartog, and S. Etalle. Know what you trust: Analyzing and designing trust policies with scoll. In P. Degano, J. Guttma, and F. Martinelli, editors, *Formal Aspects in Security and Trust 2008. Revised Selected Papers, LNCS 5491*, pages 129–142. Springer-Verlag, 2009.

[39] V. Sundramoorthy, C. Tan, P. H. Hartel, J. I. den Hartog, and J. Scholten. Functional principles of registry-based service discovery. In *30th Annual IEEE Conf. on Local Computer Networks (LCN), Sydney, Australia*, pages 209–217, Los Alamitos, California, November 2005. IEEE Computer Society.

[40] E. Todoran, J. I. den Hartog, E. P. de Vink, and J. Maluszynski. Comparative metric semantics for commit in or-parallel logic programming. In *Int. Symp. on Logic Programming (ILPS), Long Island, New York*, pages 101–115, Boston, Massachusetts, October 1997. The MIT Press.

[41] M. Veeningen, M. Bruso, J.I. den Hartog, and N. Zannone. Triplex: Verifying data minimisation in communication systems. In *Proceedings of ACM SIGSAC CCS 2013*, 2013. to appear.