Zeitplanung Arbeitsgruppe 4: Applied Cryptography and Security Engineering

Montag, 21.9.2009: Plenum, Lectures

Zeit	Titel	Vortragende
09:00–10:30	Plenum	
11:00–12:30	Introduction to Applied Cryptography	Torsten Schütze, Susanne Wetzel

Dienstag, 22.9.2009: Lectures

Zeit	Titel	Vortragende
09:00–10:30	Introduction to Applied Cryptography	Torsten Schütze, Susanne Wetzel
11:00–12:30	Introduction to Applied Cryptography	Torsten Schütze, Susanne Wetzel

Mittwoch, 23.9.2009: Lectures

Zeit	Titel	Vortragende
09:00–10:30	Introduction to Applied Cryptography	Torsten Schütze, Susanne Wetzel
11:00–12:30	Introduction to Applied Cryptography	Torsten Schütze, Susanne Wetzel

Donnerstag, 24.9.2009: Ausflug

Zeit	Paper	Vortragender	Betreuer
ganztägig	Ausflug nach Nizza		

Freitag, 25.9.2009: Practical Recommendations for Crypto; Secret Sharing and Visual Cryptography; Wireless Security

Zeit	Paper	Vortragender	Betreuer
09:00–09:45	Selecting Cryptographic Key Sizes by A.K. Lenstra and E.R. Verheul [LV01]	Fabian Steiner	Wetzel
09:45–10:30	Geeignete Algorithmen für qualifizierte elektronische Signaturen [BSI09b]; Kryptographische Verfahren: Empfehlungen und Schlüssellängen [BSI08b]	Julian Schiele	Wetzel
11:00–11:45	Intercepting Mobile Communications: The Insecurity of 802.11 by N. Borisov, I. Goldberg, and D. Wagner [BGW01]; Attacks on the WEP protocol by Erik Tews [Tew07]	Jonathan von Schroeder	Wetzel
11:45–12:30	Security Weaknesses in Bluetooth by M. Jakobsson and S. Wetzel [JW01], Bluetooth 3.0 Security Specification [Blu09, pages 149–154; 1113–1164]	Sebastian Hanschke	Wetzel
14:00–14:45	How to share a secret by A. Shamir [Sha79]; Secret sharing made short by H. Krawczyk [Kra94]	Frauke Tabert	Wetzel
14:45–15:30	Visual Cryptography by M. Naor and A. Shamir [NS94]	Christopher Grob	Wetzel
16:00–17:30	How Cryptosystems Fail: Security Nightmares from 25C3 + Diskussion	alle	

Montag, 28.9.2009: Side Channel Analysis

Zeit	Paper	Vortragender	Betreuer
09:00–10:30	Introduction to Side Channel Analysis	Torsten Schütze	
11:00–11:45	An Implementation of DES and AES, Secure against Some Attacks by M.L. Akkar and C. Giraud [AG01]; Master Thesis [Hoh09]	Samuel Hetterich	Schütze
11:45–12:30	On the Importance of Checking Cryptographic Protocols for Faults by D. Boneh, R.A. DeMillo, and R. J. Lipton [BDL97]; Shamir US Patent 5991415, 1999 [Sha99]; Infineon Gegenmaßnahme [ABF+02]	Christian Tiedt	Schütze

Dienstag, 29.9.2009: Automotive Security

Zeit	Paper	Vortragender	Betreuer
09:00–09:45	A Practical Attack on KeeLoq [IKD+08]	Damaris Schindler	Schütze
09:45–10:30	On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme [EKM+08]	Andreas Gross	Schütze
11:00–11:45	A Review of the Digital Tachograph System [FL06, Lie07]	Matthias Hüser	Schütze
11:45–12:30	Automotive Security Engineering [Wol09, And08]	Martin Maas	Schütze

Mittwoch, 30.9.2009: Test + Diskussion

Zeit	Paper	Vortragender	Betreuer
09:00–13:00	Aufnahmetest der Studienstiftung		
21:00–22:00	Diskussion Security Engineering	alle	

Donnerstag, 1.10.2009: RFID – Security and Privacy; Machine Readable Travel Documents and Electronic Passports

Zeit	Paper	Vortragender	Betreuer
09:00–09:30	RFID Security and Privacy: A Research Survey by A. Juels [Jue06]	Lena Riediger	Wetzel
09:30–10:30	Unidirectional Key Distribution Across Time and Space with Applications to RFID Security [JPP08]	Sandro Bauer	Wetzel
11:00–11:45	Basic Access Control (BAC) and Extended Access Control (EAC) bei RFID-Reisepässen [Ngu07, Küg06]	Bernd Waschneck	Schütze
11:45–12:30	Advanced Security Mechanisms for Machine Readable Travel Documents – Password Authenticated Connection Establishment (PACE), elektronischer Personalausweis [UKN+08, BSI08a, BSI09a]	Matthias Ohst	Schütze

Freitag, 2.10.2009: Cryptographic Primitives – IPSec, Security Economics

Zeit	Paper	Vortragender	Betreuer
09:00–09:45	Cryptography in Theory and Praxis: The Case of Encryption in IPSec [PY05]	André Hong Lam Dau	Schütze
09:45–10:30	Attacking the IPsec Standards in Encryption-only Configurations [DP07a]	Martin Skrodzki	Schütze
11:00–11:45	Economics, Psychology, and Sociology of Security by A. Odlyzko [Odl03a, Odl03b]	Katja Rösch	Wetzel
11:45–12:30	Abschlußdiskussion	alle	

Literatur

[ABF+02] C. Aumüller, P. Bier, W. Fischer, P. Hofreiter, and J.-P. Seifert. Fault attacks on RSA with CRT: Concrete results and practical countermeasures. In B. S. Kaliski, C. K. Koç, and Chr. Paar, editors, *Proceedings of CHES 2002*, Lecture Notes in Computer Science, pages 261–276. Springer-Verlag, 2002. pre-proceedings.

[AG01] M. L. Akkar and Chr. Giraud. An implementation of DES and AES, secure against some attacks. In C. K. Koç, D. Naccache, and Chr. Paar, editors, *Proceedings of CHES '2001*, volume 2162 of *Lecture Notes in Computer Science*, pages 309–318. Springer-Verlag, 2001.

[And08] Ross Anderson. *Security Engineering. A Guide to Building Dependable Distributed Systems.* Wiley Computer Publishing, second edition, 2008.

[BDL97] D. Boneh, R. A. DeMillo, and R. J. Lipton. On the importance of checking cryptographic protocols for faults. In W. Fumy, editor, *Proceedings of EUROCRYPT '97*, volume 1233 of *Lecture Notes in Computer Science*, pages 37–51. Springer-Verlag, 1997.

[BGW01] Nikita Borisov, Ian Goldberg, and David Wagner. Intercepting mobile communications: The insecurity of 802.11. In *Proceedings of 7th ACM Conference on Mobile Computing and Networking (MOBICOM 2001)*, 2001.

[Blu09] Bluetooth SIG. *Specification of the Bluetooth system*, 2009. Core Specification Version 3.0 + HS, 21 April 2009, see `http://www.bluetooth.com/NR/rdonlyres/298BE70B-4353-4492-9A91-160549463612/10885/Core_V30__HS.zip`.

[BSI08a] Bundesamt für Sicherheit in der Informationstechnik BSI. Advanced security mechanisms for machine readable travel documents – Extended Access Control (EAC). Technical Guideline TR-03110, BSI, 2008. Version 1.11, 2008-02-21.

[BSI08b] Bundesamt für Sicherheit in der Informationstechnik BSI. Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Technical Guideline TR-02102, BSI, 2008. Version 1.0, 2008-06-20.

[BSI09a] Bundesamt für Sicherheit in der Informationstechnik BSI. Advanced security mechanisms for machine readable travel documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI). Technical Guideline TR-03110, BSI, 2009. Version 2.01, 2009-05-05.

[BSI09b] Bundesamt für Sicherheit in der Informationstechnik BSI. Geeignete Algorithmen zur Erfüllung der Anforderungen nach § 17 Abs. 1 bis 3 SigG in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV. *Bundesanzeiger*, 13:346, 2009. 27. Januar 2009.

[DP07a] Jean Paul Degabriele and Kenneth G. Paterson. Attacking the IPsec Standards in Encryption-only Configurations. In *IEEE Symposium on Privacy and Security*, pages 335–349. IEEE Computer Society, 2007.

[DP07b] Jean Paul Degabriele and Kenneth G. Paterson. Attacking the IPsec Standards in Encryption-only Configurations. Cryptology eprint archive, report 2007/125, Royal Holloway, University of London, 2007. Available at `http://eprint.iacr.org/2007/125`.

[EKM+08] Thomas Eisenbarth, Timo Kasper, Amir Moradi, Christof Paar, Mahmoud Salmasizadeh, and Mohammad T. Manzuri Shalmani. On the power of power analysis in the real world: A complete break of the KeeLoq code hopping scheme. In D. Wagner, editor, *Proceedings of CRYPTO 2008*, volume 5157 of *Lecture Notes in Computer Science*, pages 203–220. Springer-Verlag, 2008.

[FL06] I. Furgl and K. Lemke. A review of the digital tachograph system. In K. Lemke, C. Paar, and M. Wolf, editors, *Embedded Security in Cars*, pages 69–94. Springer, 2006.

[Hoh09] A. Hoheisel. Side-Channel Analysis resistant implementation of AES on automotive processors. Master's thesis, Ruhr-Universität Bochum, Chair Embedded Security, Prof. Dr.-Ing. Christof Paar, June 2009.

[IKD+08] S. Indesteege, N. Keller, O. Dunkelman, E. Biham, and B. Preneel. A practical attack on KeeLoq. In N. Smart, editor, *Proceedings of EUROCRYPT 2008*, volume 4965 of *Lecture Notes in Computer Science*. Springer-Verlag, 2008.

[JPP08] Ari Juels, Ravikanth Pappu, and Bryan Parno. Unidirectional key distribution across time and space with applications to RFID security. In Paul C. van Oorschot, editor, *Proceedings of the 17th USENIX Security Symposium*, pages 75–90. USENIX Association, 2008.

[Jue06] Ari Juels. RFID security and privacy: a research survey. *IEEE Journal on Selected Areas in Communications*, 24(2):381–394, 2006.

[JW01] Markus Jakobsson and Susanne Wetzel. Security weaknesses in Bluetooth. In David Naccache, editor, *Topics in Cryptology, CT-RSA 2001: The Cryptographers' Track at RSA Conference 2001*, volume 2020 of *Lecture Notes in Computer Science*, pages 176–191. Springer-Verlag, 2001.

[Kra94] Hugo Krawczyk. Secret sharing made short. In D. R. Stinson, editor, *Advances in Cryptology – CRYPTO '93*, volume 773 of *Lecture Note in Computer Science*, pages 136–146. Springer-Verlag, 1994.

[Küg06] Dennis Kügler. Extended access control: Infrastructure and protocol. Talk at Interop-Test Berlin, 2006-06-01, Slides, 2006.

[Lie07] Nora Lieberknecht. Seitenkanalresistente symmetrische Verschlüsselung für digitale Tachographen. Diplomarbeit, Universität Karlsruhe, 2007.

[LV01] Arjen K. Lenstra and Eric R. Verheul. Selecting cryptographic key sizes. *Journal of Cryptology*, 14(4):255–293, 2001. Preprint version available at `http://www.cryptosavy.com/Joc.pdf`.

[Ngu07] Kim Nguyen. Contactless authentication protocols for machine readable travel documents (MRTDs). Invited talk at CHES 2007 in Vienna, Slides, 2007.

[NS94] Moni Naor and Adi Shamir. Visual cryptography. In Alfredo De Santis, editor, *Advances in Cryptology – EUROCRYPT '94*, number 950 in Lecture Notes in Computer Science, pages 1–12. Springer-Verlag, 1994.

[Odl03a] Andrew M. Odlyzko. Economics, psychology, and sociology of security. In Rebecca N. Wright, editor, *Financial Cryptography, 7th International Conference*, volume 2742 of *Lecture Notes in Computer Science*, pages 182–189. Springer, 2003.

[Odl03b] Andrew M. Odlyzko. Privacy, economics, and price discrimination on the internet. In Norman M. Sadeh, Mary Jo Dively, Robert J. Kauffman, Yannis Labrou, Onn Shehory, Rahul Telang, and Lorrie Faith Cranor, editors, *Proceedings of the 5th International Conference on Electronic Commerce, ICEC 2003*, volume 50 of *ACM International Conference Proceeding Series*, pages 355–366. ACM, 2003.

[PY05] Kenneth G. Paterson and Arnold K. L. Yau. Cryptography in Theory and Praxis: The Case of Encryption in IPSec. Cryptology eprint archive, report 2005/416, Information Security Group, Royal Holloway, University of London, 2005. Extended version of [PY06], Available at `http://eprint.iacr.org/2005/416`.

[PY06] Kenneth G. Paterson and Arnold K. L. Yau. Cryptography in Theory and Praxis: The Case of Encryption in IPSec. In S. Vaudenay, editor, *Proceedings of EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Computer Science*, pages 12–29. Springer-Verlag, 2006.

[Sha79] A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–612, 1979.

[Sha99] A. Shamir. Method and apparatus for protecting public key schemes from timing and fault attacks. United States Patent 5991415, November 23, 1999.

[TB09] Erik Tews and Martin Beck. Practical attacks against WEP and WPA. In David A. Basin, Srdjan Capkun, and Wenke Lee, editors, *Proceedings of the Second ACM Conference on Wireless Network Security, WISEC 2009, Zurich, Switzerland, March 16-19, 2009*, pages 79–86. ACM, 2009.

[Tew07] Erik Tews. Attacks on the WEP protocol. Diplomarbeit, TU Darmstadt, FB Informatik, December 2007. see also Cryptology ePrint Archive, Report 2007/471.

[UKN+08] Markus Ullmann, Dennis Kügler, Heike Neumann, Sebastian Stappert, and Matthias Vögeler. Password authenticated key agreement for contactless smart cards. In *Workshop on RFID Security 2008, July 9th-11th, 2008, Budapest*, 2008. 22 pages.

[Wol09] M. Wolf. *Security Engineering for Vehicular IT Systems*. Vieweg + Teubner, 2009.