

Protecting Alice from Malice: Protocols, Process Calculi, Proved Programs

Theory Mini-Course
University of Cambridge Computer Laboratory
May 16 and 18, 2006

Andrew D. Gordon, Microsoft Research

Networked computer systems face a range of threats from hostile parties on the network, that may lead to violations of design goals such as confidentiality, privacy, authentication, access control, and availability. Cryptographic protocols are an essential tool for protecting against such attacks. New designs and new implementations of cryptographic protocols are continually appearing, driven, for instance, by new networking technologies and new business requirements. Still, achieving security goals via cryptography is notoriously subtle; many attacks have been discovered on both the abstract designs and concrete implementations of security protocols. Hence, there is a need for effective tools for analyzing protocols and the programs that implement them.

The purpose of this course is to introduce an approach to this problem based on process calculi, and in particular on the π -calculus [Mil99, SW01] and its variants. The syllabus is as follows.

Lecture 1 Design, informal objectives, and potential attacks on cryptographic protocols [NS78]. Formal methods [DY83, BAN89] and informal methods [AN95, AN96] for security protocols. Some recent examples in the setting of XML web services [Vog03, Apa06, IBM06, Mic04].

Lecture 2 Development of formal models of protocols and their security properties within the π -calculus and its variants [AG99, AF01]. Proof techniques, including behavioural equivalences [DH84], and security types for secrecy [Aba99, AB05], authentication [GJ03c, GJ03a, GJ03b] and authorization [FGM05].

Lecture 3 Application of these ideas to recent specifications of security protocols for web services, including the discovery of potential vulnerabilities, and the verification of protocol designs against demanding threat models. We consider formal models for WS-Security [BFG05, BFGP04, KR04], WS-Trust and WS-SecureConversation [BCFG04, KR05], and WS-Policy and WS-SecurityPolicy [BFG04, BFG05].

Lecture 4 Techniques for extracting verifiable models from executable implementation code [BFGT06, GP05].

The application examples illustrate recent progress on narrowing the gap between formal models of protocols and their implementation in code, an area with many remaining research problems.

References

- [AB05] M. Abadi and B. Blanchet. Analyzing security protocols with secrecy types and logic programs. *Journal of the ACM*, 52(1):102–146, 2005.
- [Aba99] M. Abadi. Secrecy by typing in security protocols. *Journal of the ACM*, 46(5):749–786, September 1999.
- [AF01] M. Abadi and C. Fournet. Mobile values, new names, and secure communication. In *Proceedings of the 28th ACM Symposium on Principles of Programming Languages (POPL’01)*, pages 104–115, 2001.
- [AG99] M. Abadi and A. D. Gordon. A calculus for cryptographic protocols: The spi calculus. *Information and Computation*, 148:1–70, 1999.
- [AN95] R. Anderson and R. Needham. Programming Satan’s computer. In J. van Leeuwen, editor, *Computer Science Today: Recent Trends and Developments*, volume 1000 of *LNCS*, pages 426–440. Springer, 1995.
- [AN96] M. Abadi and R. Needham. Prudent engineering practice for cryptographic protocols. *IEEE Transactions on Software Engineering*, 22(1):6–15, 1996.
- [Apa06] Apache Software Foundation. *Apache WSS4J*, 2006. At <http://ws.apache.org/wss4j/>.
- [BAN89] M. Burrows, M. Abadi, and R.M. Needham. A logic of authentication. *Proceedings of the Royal Society of London A*, 426:233–271, 1989.
- [BCFG04] K. Bhargavan, R. Corin, C. Fournet, and A. D. Gordon. Secure sessions for web services. In *2004 ACM Workshop on Secure Web Services (SWS)*, pages 11–22, October 2004.

- [BFG04] K. Bhargavan, C. Fournet, and A. D. Gordon. Verifying policy-based security for web services. In *11th ACM Conference on Computer and Communications Security (CCS'04)*, pages 268–277, October 2004.
- [BFG05] K. Bhargavan, C. Fournet, and A. D. Gordon. A semantics for web services authentication. *Theoretical Computer Science*, 340(1):102–153, June 2005.
- [BFGO05] K. Bhargavan, C. Fournet, A. D. Gordon, and G. O'Shea. An advisor for web services security policies. In *2005 ACM Workshop on Secure Web Services*, pages 1–9. ACM, 2005.
- [BFGP04] K. Bhargavan, C. Fournet, A. D. Gordon, and R. Pucella. TulaFale: A security tool for web services. In *International Symposium on Formal Methods for Components and Objects (FMCO'03)*, volume 3188 of *LNCS*, pages 197–222. Springer, 2004.
- [BFGT06] K. Bhargavan, C. Fournet, A. D. Gordon, and S. Tse. Verified interoperable implementations of security protocols. In *19th IEEE Computer Security Foundations Workshop (CSFW'06)*, 2006. To appear.
- [DH84] R. De Nicola and M. C. B. Hennessy. Testing equivalences for processes. *Theoretical Computer Science*, 34:83–133, 1984.
- [DY83] D. Dolev and A.C. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, IT-29(2):198–208, 1983.
- [FGM05] C. Fournet, A. D. Gordon, and S. Maffei. A type discipline for authorization policies. In *European Symposium on Programming (ESOP'05)*, volume 3444 of *LNCS*, pages 141–156. Springer, 2005.
- [GJ03a] A. D. Gordon and A. Jeffrey. Authenticity by typing for security protocols. *Journal of Computer Security*, 11(4):451–521, 2003.
- [GJ03b] A. D. Gordon and A. Jeffrey. Types and effects for asymmetric cryptographic protocols. *Journal of Computer Security*, 12(3/4):435–484, 2003.

- [GJ03c] A. D. Gordon and A. Jeffrey. Typing correspondence assertions for communication protocols. *Theoretical Computer Science*, 300:379–409, 2003.
- [GP05] J. Goubault-Larrecq and F. Parrennes. Cryptographic protocol analysis on real C code. In *6th International Conference on Verification, Model Checking and Abstract Interpretation (VMCAI'05)*, volume 3385 of *LNCS*, pages 363–379. Springer, January 2005.
- [IBM06] IBM Corporation. *IBM WebSphere Application Server*, 2006. At <http://www.ibm.com/software/websphere/>.
- [KR04] E. Kleiner and A. W. Roscoe. Web services security: A preliminary study using Casper and FDR. In *Proceedings of Automated Reasoning for Security Protocol Analysis (ARSPA 04)*, 2004.
- [KR05] E. Kleiner and A. W. Roscoe. On the relationship between web services security and traditional protocols. In *Mathematical Foundations of Programming Semantics (MFPS XXI)*, 2005.
- [Mic04] Microsoft Corporation. *Web Services Enhancements (WSE) 2.0*, 2004. At <http://msdn.microsoft.com/webservices/building/wse/default.aspx>.
- [Mil99] R. Milner. *Communicating and Mobile Systems: the π -Calculus*. CUP, 1999.
- [NS78] R. Needham and M. Schroeder. Using encryption for authentication in large networks of computers. *Communications of the ACM*, 21(12):993–999, 1978.
- [SW01] D. Sangiorgi and D. Walker. *The π -calculus: A Theory of Mobile Processes*. CUP, 2001.
- [Vog03] W. Vogels. Web services are not distributed objects. *IEEE Internet Computing*, 7(6):59–66, 2003.
- [Wik05] Wikipedia contributors. Alice and Bob. *Wikipedia*, 2005. At http://en.wikipedia.org/wiki/Alice_and_Bob.