Carleton University

Department of Systems and Computer Engineering

SYSC 5807 (ELG 6187) Advanced Topics in Computer Systems: Security and Privacy for E-Services ***Fall 2004***

Course Outline

Instructor: George Yee,
Adjunct Research Professor, Systems and Computer Engineering, Carleton University; Research Officer, Institute for Information Technology, National Research Council Canada (613) 990-4284
gmyee@sce.carleton.ca or george.yee@nrc-cnrc.gc.ca
http://www.sce.carleton.ca/faculty/yee.html

Course Description and Objectives:
The purpose of this course is to present recent advanced methods to add security and privacy to electronic services (e-services) (e.g. e-commerce, e-learning) including web-based services. The course looks at the research literature for new solutions to complement traditional or current security systems. Traditional security systems will be presented as well since not all students will be familiar with them. This is NOT a programming course. Nor is it a detailed protocols course. Protocols will only be examined at a high level. The student who successfully completes this course will:

- Understand the nature of e-services.
- Understand the security, privacy, and trust requirements of e-services.
- Understand how most of these requirements can be met, using traditional and advanced security and privacy methods.
- Understand the research challenges of satisfying the remaining requirements.

Prerequisites:
SYSC 5207 (ELG 6127) or equivalent or permission of the instructor. SYSC 5207 (ELG 6127) may be taken concurrently if available. In addition, a basic knowledge of methods for electronic security would be ideal but not necessary.

Students who have not satisfied the prerequisites for this course must either a) withdraw from the course, or b) obtain a prerequisite waiver from the Registrar's office, or c) will be deregistered from the course after the last day to register for courses in the Fall term.

Textbook: None (no single textbook covers all the different topics in this course). However, substantial traditional material will be taken from reference [1] below.

References: (subject to change - most of the papers will be available online) [1] and [2] should be in the bookstore if you wish to purchase them.

[1] W. Stallings, Cryptography and Network Security, 3rd edition, Prentice Hall, 2003.
[2] M. O'Neil et al, Web Services Security, McGraw-Hill/Osbourne, 2003.
[3] D. Eastlake III and K. Niles, Secure XML, The New Syntax for Signatures and Encryption, Addison Wesley, 2003.
[4] Department of Justice, Privacy provisions highlights, http://canada.justice.gc.ca/en/news/nr/1998/attback2.html

Course Outline

[5] Privacy Technology Review, http://www.health-canada.ca/ohih-bsi/available/tech/tech_e.html
[6] J. Raymond, "Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems", in H. Federrath, editor, Anonymity 2000, Volume 2009 of Lecture Notes in Computer Science, pages 10-29, Springer-Verlag, 2000.
[7] http://www.w3c.org/P3P
[8] Anonymizer web service at: http://www.anonymizer.com/
[9] D.Goldschlag, M.Reed and P.Syverson, "Onion Routing for Anonymous and Private Internet Connections", Communication of the ACM, vol.42, no.2, pages 39-41, 1999.
[10] D. Chaum, "Untraceable Electronic Mail, Return Address, and Digital Pseudonyms", Communications of the ACM, vol.24 no.2, pages 84-88, 1981.
[11] D. Chaum, "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability", *Journal of Cryptology* 1/1 (1988), pp. 65-75.
[12] M. Waidner, "Unconditional Sender and Recipient Untraceability in Spite of Active Attacks", *Eurocrypt'89*, April 1989.
[13] M. K. Reiter and A. D. Rubin, "Crowds: Anonymity for Web Transactions", ACM Transactions on Information and System Security, v. 1, n. 1, pp. 66-92, 1998.
[14] P. Boucher, A. Shostack and I. Goldberg, "Freedom Systems 2.0 Architecture", Dec. 2000.
[15] Thomas Beth, Malte Borcherding, et al, "Valuation of trust in open networks", in Proceedings of Computer Security –ESORICS '94, Brighton, UK, 2-9 Nov. 1994.
[16] Raphael Yahalom, Birgit Klein, et al, "Trust relationships in secure systems: a distributed authentication perspective", in Proc.1993 IEEE Computer Society Symposium on Research in Security and Privacy, pp.150-164, IEEE Computer Society Press, May 1993.
[17] Raphael Yahalom, Birgit Klein, et al, "Trust-based navigation in distributed systems", Computing Systems, pp.45-73, 1994.
[18] Gustavus J.Simmons and Catherine A. Meadows, "The role of trust in information integrity protocols", Journal of Computer Security, 1994.
[19] Pekka Nikander, Kristiina Karvonen, "Users and Trust in Cyberspace", Security Protocols, LNCS 2133, pp.24-35, Springer-Verlag, 2001
[20] Public-Key Infrastructure (X.509) (pkix), last modified: 11-Jan-02, http://www.ietf.org/html.charters/pkix-charter.html
[21] An Open Specification for Pretty Good Privacy (openpgp), last modified: 31-Jul-01, http://www.ietf.org/html.charters/openpgp-charter.html
[22] Matt Blaze, Joan Feigenbaum, John Ioannidis, and Angelos D. Keromytis, "The KeyNote Trust-Management System Version 2, Request For Comments (RFC) 2704", September 1999.
[23] M. Blaze, J. Feigenbaum, J. Lacy, "Decentralized Trust Management", Proceedings of the 17th IEEE Symp. on Security and Privacy, pp 164-173, IEEE Computer Society, 1996.
[24] P. Resnick and J. Miller, "PICS: Internet Access Controls without Censorship", Communications of the ACM, 39 (1996), pp. 87-93. Also available:http://www.w3.org/pub/WWW/PICS/iacwcv2.htm
[25] Y. Chu, "Trust Management for the World Wide Web", 1997, Massachusetts institute of Technology, REFEREE: Trust Management for Web Applications, http://www.w3.org/PICS/TrustMgt/presentation/97-04-08-referee-www6/

Course Outline

[26] C. Ellison, B. Schneier, "Ten risks of PKI: what you're not being told about Public Key Infrastructure", Computer Security Journal, V.XVI, N.1, 2000.
[27] L. Korba, "Privacy in Distributed Electronic Commerce", Proc. 35th Hawaii International Conference on System Science (HICSS), Hawaii, January 7-11, 2002.
[28] L. Korba, R. Song, G. Yee, "Anonymous Communications for Mobile Agents", Proceedings, Fourth International Workshop on Mobile Agents for Telecommunication Applications (MATA'02), Barcelona, Spain, Oct. 23-24, 2002.
[29] G. Yee and L. Korba, "Bilateral E-services Negotiation Under Uncertainty", Proceedings, International Symposium on Applications and the Internet (SAINT 2003), Orlando, Jan 27-31, 2003.
[30] G. Yee and L. Korba, "The Negotiation of Privacy Policies in Distance Education", Proceedings, 14th IRMA International Conference, Philadelphia, Pennsylvania, May 18-21, 2003.
[31] G. Yee and L. Korba, "Feature Interactions in Policy-Driven Privacy Management", Proceedings, Seventh International Workshop on Feature Interactions in Telecommunications and Software Systems, Ottawa, Canada, June 11-13, 2003.
[32] K. El-Khatib, L. Korba, Y. Xu, G. Yee, "Privacy and Security in E-Learning", International Journal of Distance Education Technology, Vol. 1, No. 4, October-December 2003.
[33] L. Korba, G. Yee, Y. Xu, R. Song, A. Patrick, K. El-Khatib, "Privacy and Trust in Agent-Supported Distributed Learning", chapter in book Designing Distributed Learning Environments with Intelligent Software Agents, published by Idea Group Inc., 2004.
[34] G. Yee, K. El-Khatib, L. Korba, A. Patrick, R. Song, Y. Xu, "Privacy and Trust in E-Government", chapter in book Electronic Government Strategies and Implementation, published by Idea Group Inc., 2004.
[35] G. Yee and L. Korba, "Privacy Policies and their Negotiation in Distance Education", chapter in book Instructional Technologies: Cognitive Aspects of Online Programs, published by Idea Group Inc., 2004.
[36] K. El-Khatib, L. Korba, R. Song, G. Yee, "Secure Dynamic Distributed Routing Algorithm for Ad Hoc Wireless Networks", Proceedings, Workshop on Wireless Security and Privacy 2003, The 2003 Conference on Parallel Processing (ICPP 2003), Kaohsiung, Taiwan, Oct 6-9, 2003.
[37] Y. Han, D.C. Petriu, G. Yee, "Towards Better Key Exchange Performance in IPSec-Based VPNs", to be published in Proceedings of IRMA2004, New Orleans, May 2004.
[38] G. Yee and L. Korba, "Semi-Automated Derivation of Personal Privacy Policies", Proceedings, IRMA2004, New Orleans, May 2004.
[39] G. Yee and L. Korba, "Privacy Policy Compliance for Web Services", Proceedings, IEEE International Conference on Web Services (ICWS 2004), San Diego, California, USA, July 6-9, 2004.
[40] G. Yee, L. Korba, N.H. Lin, T.K. Shih, "Context-Aware Privacy and Security Agents for Distance Education", accepted for a special issue of *International Journal of High Performance Computing and Networking*, 2004 or 2005.
[41] L. Korba, R. Song, G. Yee, B. Chen, "Enforcing Privacy: A Rights Management Approach", conference paper, in progress.

Course Outline

Grading Scheme:

- Two assignments (30%):
- Term project (30%): requires oral presentation and final report
- Final exam (40%)

Laboratory Sessions: N/A

Final Exam: 3-hour closed book

Students with Disabilities:
Students with disabilities who require academic accommodations in this course are encouraged to contact the Paul Menton Centre for Students with Disabilities (500 University Centre) to complete the necessary forms. After registering with the Centre, make an appointment to meet with me in order to discuss your needs at least ***two weeks before the first in-class test or CUTV midterm exam.*** This will allow for sufficient time to process your request. Please note the following deadlines for submitting completed forms to the PMC for formally scheduled exam accommodations: ***November 5th, 2004*** for fall and fall/winter term courses, and ***March 11, 2005*** for winter term courses.

Plagiarism:
Plagiarism (copying and handing in for credit someone else's work) is a serious instructional offense that will not be tolerated. Please refer to the section on instructional offenses in the Undergraduate Calendar for additional information.

Week-by-Week Material (subject to change):

1. (Sept 13, 15) Course overview, introduction to e-services

2. (Sept 20, 22) E-service architectures, e-commerce, e-learning, e-government, e-health, web services; the need for security, privacy, and trust

3. (Sept 27, 29) Security and privacy requirements for e-services: e-commerce, e-learning, e-government, e-health, web services; *first assignment issued (Sept 29)*

4. (Oct 4, 6) Fundamental traditional and advanced security and privacy tools for e-services, including encryption, MACs, hash functions, digital signatures, X.509, IPSec, Kerberos, SSL, VPN, firewalls

5. (Oct 11, 13) Oct 11: no class; Oct 13: Fundamental traditional and advanced security and privacy tools for e-services – cont'd

Course Outline

6. (Oct 18, 20) Fundamental traditional and advanced security and privacy tools for e-services – cont'd; *first assignment due (Oct 18); second assignment issued (Oct 20)*

7. (Oct 25, 27) Fundamental traditional and advanced security and privacy tools for e-services – cont'd

8. (Nov 1, 3) Advanced security/privacy techniques for e-services (weaknesses of traditional techniques, onion routing); *term project assigned (Nov 1)*

9. (Nov 8, 10) Advanced security/privacy techniques for e-services (onion routing, privacy policies and their specification); *second assignment due (Nov 8)*

10. (Nov 15, 17) Advanced security/privacy techniques for e-services (Nov 15: privacy policy negotiation; Nov 17: security and privacy for Web Services)

11. (Nov 22, 24) Nov 22: Advanced security/privacy techniques for e-services: security and privacy for Web Services; Nov 24: Application of security and privacy to e-services: e-learning

12. (Nov 29, Dec 1) *term project presentations* (attendance mandatory)

13. (Dec 6) Application of security and privacy to e-services: e-learning; Research challenges; *term project report due*

N.B.: Some adjustment of the Nov and Dec schedule may be necessary depending on the number of students in the course.