Eduardo B. Fernandez
Dept. of Computer Science and Eng.
Florida Atlantic University
777 Glades Rd., Boca Raton , FL 33431
Tel. (561)297-3466, Fax (561)297-2800
ed@cse.fau.edu http://www.cse.fau.edu/~ed

Security patterns and secure systems design

Tutorial duration
Full day (6 hours). Can be reduced to half day (three hours) if necessary.

Abstract:
Analysis and design patterns are well established to build high-quality software. Patterns combine experience and good practices to develop basic models that can be used for new designs. Security patterns join the extensive knowledge accumulated about security with the structure provided by patterns to provide guidelines for secure system design and evaluation. They are being adopted by companies such as IBM, Sun, and Microsoft. We show the anatomy of a security pattern, a variety of them, and their use in the construction of secure systems. These patterns include Authentication, Authorization, Role-Based Access Control, Firewalls, Web Services Security (XACML, SAML), and others. We apply these patterns through a secure system development method based on a hierarchical architecture whose layers define the scope of each security mechanism. The patterns are shown using UML models and some examples are taken from my book "Security Patterns: Integrating security and systems engineering" (Wiley 2006).

Motivation, audience, and interest to SAC community
Security patterns are valuable to build new systems but also to compare systems. Describing complex standards as patterns makes the standards more understandable and can be used to verify if a system complies with the standard. Finally, we have found security patterns very useful to teach security concepts.

Security researchers and practicioners should find patterns to be a useful tool. As indicated, patterns are useful for students to help their understanding of security mechanisms and architectures. Since all these types of people come to SAC conferences, the tutorial should be of interest to many of them.

Outline (see relevant publications at the end):
Introduction—Motivation, basic concepts. The context for security. Attacks.
The design of secure systems--- Object-oriented design, UML, and patterns, need for good software engineering. Security principles. Security patterns. Standards.
Anatomy of a security pattern.
Security models and their patterns---policies, access matrix, multilevel models, RBAC
Defining authorizations from use cases---nonfunctional aspects of use cases, RBAC and security policies
Firewall, IDS, and operating system patterns
Secure conceptual model
Secure system architectures---Effect of distribution and user interfaces
Patterns for web services: SAML, XACML, Liberty Alliance, WS-Security. Comparing standards through patterns. Application and XML firewalls
Coordination across levels---mapping of authorizations across architectural levels
Conclusions---the future

Learning objectives
Attendees should be able to understand the general concept of security patterns as solutions to security problems. We show how the pattern template focuses on specific aspects of security and on the use of the pattern. We show with several examples how security patterns describe security mechanisms intended to control specific types of attacks. We also see how to use security patterns as guidelines to build secure systems. A complete methodology will be presented with some examples.

Expected background of audience
Basic knowledge of UML and object-oriented design is assumed. Understanding of security concepts is useful.

Audiovisual equipment: computer projector

Biography

Eduardo B. Fernandez
Dept. of Computer Science and Eng.
Florida Atlantic University
777 Glades Rd., Boca Raton , FL 33431
ed@cse.fau.edu http://www.cse.fau.edu/~ed

Eduardo B. Fernandez is a professor in the Department of Computer Science and Engineering at Florida Atlantic University, Boca Raton, Florida. He has published numerous papers on security models, and object-oriented analysis/design, including a book on security patterns. He has lectured all over the world at both academic and industrial meetings. His current interests include object-oriented design and security patterns. He holds a MS degree in Electrical Engineering from Purdue University and a Ph.D. in Computer Science from UCLA. He is a Senior Member of the IEEE, and a Member of ACM. He is an active consultant for industry. More details: http://www.cse.fau.edu/~ed

***Tutorial history*:** This tutorial has been presented at:

- IFIP WCC 1998, Vienna, Austria.
- University of Buenos Aires, Argentina. Escuela de Ciencias Informaticas (ECI), July 2003.
- IEEE Intern. Symp. on Advanced Distributed Systems (ISSADS), Guadalajara, MX, January 2005 and 2006 http://intranet.gdl.cinvestav.mx/issads/
- IEEE Southeastcon, Fort Lauderdale, FL, April, 2005
- Third International Workshop on Security in Information Systems (WOSIS-2005), Miami, May 24-25, 2005
- 5th Latin American Conference on Pattern Languages of Programs, Campos do Jordao, Brazil, August 16-19, 2005 http://sugarloafplop2005.icmc.usp.br/
- IEEE Int. Symposium on Secure Software Engineering (ISSSE.06), Arlington, VA, March 2006. http://www.jmu.edu/iiia/issse/
- IFIP WCC 2006 (Santiago de Chile, August 2006). http://www.wcc-2006.org/program/tc11_security.php?opcion_actual=program

- *Eigth International Symposium on System and Information Security - SSI´2006,* Sao Jose dos Campos, Brazil, November 08-10, 2006.
- *45th ACM Southeast Conference (ACMSE 2007),* March 23-24, 2007, Winston-Salem, North Carolina, http://acmse2007.wfu.edu

The tutorial has been updated each time it has been presented. Aspects that the attendants considered difficult have been clarified in the next version.

Some relevant publications of the presenter:

E. B. Fernandez, M. M. Larrondo-Petrie, and E. Gudes, ``A method-based authorization model for object-oriented databases", in *Security for Object-Oriented Systems*, Springer Verlag, London, 1994.

E. B. Fernandez, E. Gudes, and H. Song, ``A model for evaluation and administration of security in object-oriented databases", *IEEE Trans. on Knowledge and Database Eng.*, vol. 6, no. 2, April 1994, 275--292.

E. B. Fernandez and J. C. Hawkins, "Determining role rights from use cases", *Procs. 2nd ACM Workshop on Role-Based Access Control*, November 1997, 121-125.

E.B.Fernandez, "Building systems using analysis patterns", *Procs. 3rd Int. Software Architecture Workshop* (ISA W3), ACM, November 1998, 37-40.

E.B.Fernandez and X.H.Yuan, "An analysis pattern for reservation and use of entities", *Procs. of Pattern Languages of Programs Conf* (PLoP99), http://st-www.cs.uiuc.edu/~plop/plop99

E.B.Fernandez, "Coordination of security levels for Internet architectures", *Procs. 10th Intl. Workshop on Database and Expert systems Applications*, DEXA99, 837-841.

E.B.Fernandez, "Stock manager: An analysis pattern for inventories, *Procs. of PLoP 2000.* http://jerry.cs.uiuc.edu/~plop/plop2k/proceedings/proceedings.html

E.B. Fernandez and X. Yuan, "Semantic Analysis Patterns", *Procs. of 19th Int. Conf. on Conceptual Modeling, ER2000,* 183-195. http://www.cse.fau.edu/~ed/SAPpaper2.pdf

E B. Fernandez and R.Y. Pan, "A pattern language for security models", *Procs. of PLoP 2001*, http://jerry.cs.uiuc.edu/~plop/plop2001/accepted_submissions/accepted-papers.html

E.B.Fernandez, "Web services security", chapter in *Web Services Business Strategies and Architectures*, P. Fletcher and M. Waterhouse (Eds.), Expert Press, UK, 2002, 290-302.

E.B.Fernandez, "Patterns for operating systems access control", *Procs. of PLoP 2002*, http://jerry.cs.uiuc.edu/~plop/plop2002/proceedings.html

X.Yuan and E.B.Fernandez, "An analysis pattern for course management", *Procs. EuroPLoP 2003*, http://hillside.net/europlop

T. Priebe, E.B.Fernandez, J. Mehlau, and G. Pernul, "A pattern system for access control", *Procs. of the IFIP WG 11.3 Conference on Data and Applications Security*, Sitges, Spain, July 25-28, 2004.

N. Delessy-Gassant, E.B.Fernandez, S. Rajput, and M.M.Larrondo-Petrie, "Patterns for application firewalls", *Procs. of the Pattern Languages of Programs Conference*, 2004, http://hillside.net/patterns

E.B.Fernandez, T. Sorgente, and M.M.Larrondo-Petrie, "A UML-based methodology for secure systems: The design stage", *Procs. of the Third International Workshop on Security in Information Systems (WOSIS-2005), ICEIS*, Miami, May 24-25, 2005, *, 207-216.*

N. Delessy and E. B. Fernandez, "Patterns for the eXtensible Access Control Markup (XACML) Language", *Procs. of the Pattern Languages of Programs Conference* (PLoP 2005).

M.Schumacher, E.B.Fernandez, F. Buschmann, D. Hybertson, and P. Sommerlad, *Security Patterns*: *Integrating security and systems engineering*, Wiley, 2006.

E.B.Fernandez, N.A.Delessy, and M.M. Larrondo-Petrie, "Patterns for web services security", *4th Intl. Workshop on Service-Oriented Architecture and Web Services'*, part of OOPSLA 2006.

E.B.Fernandez, M. VanHilst, M.M.Larrondo-Petrie, and S. Huang, "Defining security requirements through misuse actions" , *Procs. IFIP International Workshop on Advanced Software Engineering (IWASE 2006).* Santiago, Chile, August 2006 (part of WCC) http://www.dcc.uchile.cl/IWASE06 .

E.B. Fernandez, "Security patterns", *Procs. of the Eigth International Symposium on System and Information Security - SSI´2006,Keynote talk*, Sao Jose dos Campos, Brazil, November 08-10, 2006.

E.B. Fernandez, J.C. Pelaez, and M.M. Larrondo-Petrie, "Attack patterns: A new forensic and design tool", *Third Annual IFIP WG 11.9 Int. Conf. on Digital Forensics*, Orlando, FL, Jan. 29-31, 2007. www.cis.utulsa.edu/ifip119

E.B.Fernandez, J. Ballesteros, A. C. Desouza-Doucet, and M.M. Larrondo-Petrie, "Security Patterns for Physical Access Control Systems", in S. Barker and G.J. Ahn (Eds.), *Data and Applications Security XXI*, LNCS 4602, 259-274, Springer 2007. *Procs. of the 21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security*, Redondo Beach, California, U.S.A, July 8-11, 2007 (Acceptance ratio: 40%).