2J-08

ソフトウェアセキュリティ知識ベースを活用したセキュリティ要求分析からセキュリティ設計を支援するシステムの提案

櫨山淳雄† 宮原光† 田中昂文†† 橋浦弘明§
鷲崎弘宜‡ 吉岡信和‡‡ 海谷治彦* 大久保隆夫**

†東京学芸大学 ††東京農工大学 §日本工業大学 ‡早稲田大学
‡‡国立情報学研究所 *神奈川大学 **情報セキュリティ大学院大学

1. はじめに

インターネットが社会に浸透している現在，様々なサービスがソフトウェアで実現されており，ソフトウェアセキュリティ[5]の重要性が認識されている．一方で，ソフトウェア開発者は必ずしもセキュリティの専門家ではないため，セキュアなソフトウェアの開発は困難であることが指摘されている[1]．特に，セキュリティ設計の困難さ，セキュリティ要求分析の結果に基づいた適切な設計の困難さが指摘されている[4]．著者らはソフトウェアセキュリティ分野で研究開発されてきたさまざまな既存知識を関連付けたセキュリティ知識ベースの構築を進めている[3]．そして，知識ベースを活用してセキュリティ要求分析，設計作業を支援することを目指している．

セキュリティ要求分析の知識が設計以降の知識と関連付けられているならば，セキュリティ要求分析で使用された知識に関連付けられた設計工程で考慮すべき知識を提示することが可能になる．本論文では，このコンセプトに基づいてセキュリティ要求分析から設計作業を支援するシステムを提案する．

2. 関連研究

本節では，セキュリティ要求分析から設計をつなぐ支援を目指している研究について述べる．

Xu と Pauli はセキュリティ要求分析の結果であるミスユースケース図からソフトウェアアーキテクチャの一種であるモジュール構成図を作成し，モジュールとミスユースケースの対応表を作成することを提案している[13]．

Rosado らはセキュリティ要求からセキュリティパターン，セキュリティ標準の間の追跡可能性を管理するという問題意識の下，セキュリティ要求，セキュリティパターン，セキュリティ標準を関連づけることを提案している[8]．この考え方は，我々と同じものである．

我々は，次節で述べるように，セキュアなソフトウェア開発ライフサイクル全体を扱う知識体系を知識ベースシステム上に構築し，その知識ベース中の分析工程で使用した知識に関連付けられた設計工程で考慮すべき知識を開発者に提示しながらセキュリティ要求分析から設計作業をシームレスに行うことが可能な開発環境の構築を目指している．

Proposal of a System Supporting Security Design from Security Requirements Analysis using a Software Security Knowledge Base, Atsuo Hazeyama, Hikaru Miyahara, Takafumi Tanaka, Hiroaki Hashiura, Hironori Washizaki, Nobukazu Yoshioka, Haruhiko Kaiya and Takao Okubo, Tokyo Gakugei University, Tokyo University of Agriculture and Technology, Nippon Institute of Technology, Waseda University, National Institute of Informatics, Kanagawa University and Institute of Information Security.

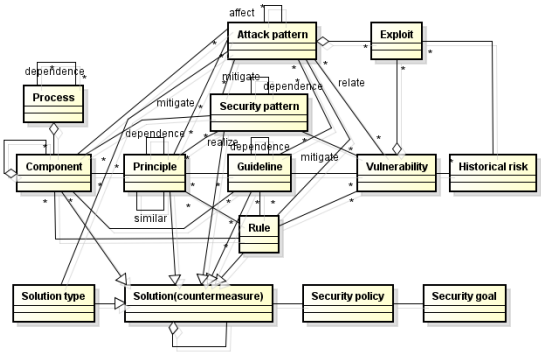

図 1. セキュリティ知識ベースのためのメタモデル

3. ソフトウェアセキュリティ知識ベース

鷲崎らはセキュリティとプライバシーの知識を扱うことができるメタモデルの開発を進めている[12]．図 1 はこのうち，セキュリティに関する知識に関わる部分を抽出して示したものである．知識ベースに登録されている知識はメタモデル中の各クラスのインスタンスである．

4. セキュリティ要求分析支援システム

著者らはセキュアなソフトウェア開発における分析・設計作業を支援するシステムの開発を目指している．その基本的なコンセプトとして，成果物の構成要素に，それを抽出するに至った知識ベース中の知識を関連付けて設計根拠を記録することを提案している．これまでにミスユースケース図[10]を拡張したダイアグラム[7]によりセキュリティ要求分析を行うシステムを開発した (図 2)[11]．

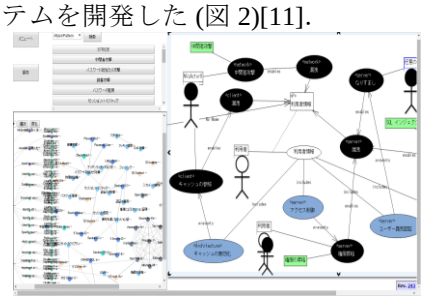

図 2. セキュリティ要求分析支援システム

Copyright ©2017 Information Processing Society of Japan.
All Rights Reserved.

5. 知識ベースを用いたセキュリティ要求分析から設計へのシームレスな支援

提案する開発環境のイメージを図 3 に示す.

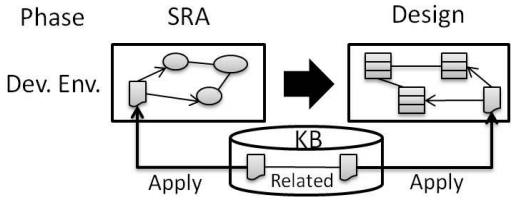

図 3. 工程を跨いだシームレスな知識提供のイメージ

設計 (Design)において，開発者が要求分析 (SRA)の成果物を閲覧し，成果物に関連付けられている知識を選択すると，それに関連付けられている設計で考慮すべき知識が提示される．この時，設計で適用されるべき知識を抽出できる必要がある．我々の知識ベースでは，各知識の適用工程を識別するため，Yskout [14]の方法を応用して各知識に適用工程をメタデータとして付加する．

セキュリティ要求分析から設計へのシームレスな支援について，認証を例に説明する．[6]では「なりすまし」という脅威に対する対応策として「認証」が示されている．この抽象度の知識はセキュリティ要求分析で利用することを想定する．Hafiz はセキュリティパターンを体系化している[2]．その中に認証に関わるパターンとして Authenticator Enforcer (以下 Authenticator と記す)がある．我々の知識ベースでは，「認証」は Solution type のインスタンスとして管理し，それをセキュリティパターン Authenticator と関連づける(このパターンの適用工程として「設計」をメタデータに付与する)(図 4)．Hafiz の論文では Authenticator は文献[9]を参照しており，そこには，Authenticator の構造がクラス図として提供されている．また，[6]では設計ガイドラインとして認証に関する知識が提供されている．これらの情報を提案システムで参照できるようにすることで，認証をどのように実現すればよいのかという知識を開発者に提供することができる．

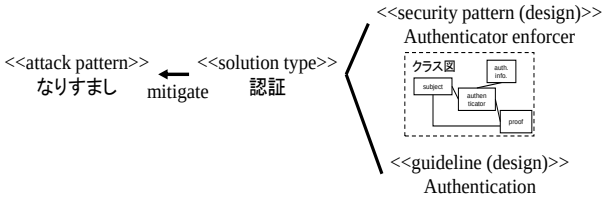

図 4. 認証に関する知識間の関連

6. おわりに

本稿では，知識ベースを活用したセキュリティ要求分析から設計作業を支援するシステムを提案した．セキュリティ要求分析の成果物の構成要素に知識を関連付けることは単に設計根拠を記録するのみでなく，知識間の関連を積極的に活用して設計作業を効果的に支援できる可能性を示唆している．今後は提案したシステムを実装していく予定である．

謝辞

本研究の一部は科学研究費補助金基盤研究 (C) 26330394 並びに科学研究費補助金基盤研究 (B) 15H02686 の助成の下で行われた．知識ベースのメタモデル開発は 2015 年度並びに 2016 年度 SSR 産学戦略的研究フォーラムの助成を受けた．記して謝意を表す.

参考文献

[1] Axelle Apvrille and Makan Pourzandi, Secure Software Development by Example, IEEE Security & Privacy, Vol. 3, No. 4, pp. 10-17, 2005.
[2] Munawar Hafiz, Paul Adamczyk, and Ralph Johnson, Growing a Pattern Language (for Security), Proceedings of the ACM International Symposium on New ideas, new paradigms, and reflections on programming and software, pp. 139-158, ACM Press, 2012.
[3] 櫨山淳雄, Web アプリケーション開発のためのソフトウェアセキュリティ知識ベース KBSSD の提案, 電子情報通信学会技術研究報告知能ソフトウェア工学 KBSE2012-72, pp. 19-24, 2013.
[4] 小橋孝紀, 大久保隆夫, 海谷治彦, 吉岡信和, 伊永祥太, 鷲崎弘宜, 深澤良彰, モデルテストによるセキュリティ分析・設計パターンの適用支援, 情報処理学会コンピュータセキュリティシンポジウム 2012 論文集, pp. 655-662, 2012.
[5] Gary McGraw, Software Security, IEEE Security & Privacy, Vol. 2, No. 2, pp. 80-83, 2004.
[6] マイクロソフト，脅威とその対策，https://msdn.microsoft.com/ja-jp/library/ff648641.aspx, 2004.
[7] 大久保隆夫, 田中英彦, 効率的なセキュリティ要求分析手法の提案, 情報処理学会論文誌, Vol. 50, No. 10, pp. 2484-2499, 2009.
[8] David G. Rosado, Carlos Gutiérrez, Eduardo Fernández-Medina, and Mario Piattini, Security patterns and requirements for internet-based applications, Internet Research, Vol. 16, No. 5, pp. 519-536, 2006.
[9] Markus Schumacher, Eduardo Fernandez-Buglioni, Duane Hybertson, Frank Buschmann, and Peter Sommerlad, Security Patterns: Integrating Security and Systems Engineering, John Wiley & Sons, 2013.
[10] Guttorm Sindre and Andreas L. Opdahl, Eliciting security requirements with misuse cases, Requirements Engineering, Vol. 10, pp. 34-44, Springer, 2005.
[11] 田中俊一, 田中昂文, 沓澤脩, 櫨山淳雄, 宗藤誠治, ソフトウェアセキュリティ知識ベースを活用したセキュアなソフトウェア開発のためのモデリングツールの開発, 電子情報通信学会技術研究報告知能ソフトウェア工学 KBSE2015-53, pp. 31-36, 2016.
[12] Hironori Washizaki, et al., A Metamodel for Security and Privacy Knowledge in Cloud Services, Proceedings of the 2016 IEEE World Congress on Services, pp. 142-143, IEEE, 2016.
[13] Dianxiang Xu, and Joshua Pauli, Threat-driven design and analysis of secure software architectures, Journal of Information Assurance and Security, Vol. 1, No. 3, pp. 171-180, Dynamic Publishers Inc., 2006.
[14] Koen Yskout, Riccardo Scandariato, and Wouter Joosen, Does Organizing Security Patterns Focus Architectural Choices?, Proceedings of the 34th International Conference on Software Engineering, pp. 617-627, IEEE, 2012.

Copyright ©2017 Information Processing Society of Japan.
All Rights Reserved.