Title
Synthesis of Obfuscation Policies to Ensure Privacy and Utility

Journal
Journal of Automated Reasoning, 60(1)

ISSN
0168-7433

Authors
Wu, Yi-Chin
Raman, Vasumathi
Rawlings, Blake C
et al.

Publication Date
2018

DOI
10.1007/s10817-017-9420-x

Peer reviewed

Published: 22 July 2017

Synthesis of Obfuscation Policies to Ensure Privacy and Utility

Yi-Chin Wu, Vasumathi Raman, Blake C. Rawlings, Stéphane Lafortune & Sanjit A. Seshia

Journal of Automated Reasoning **60**, 107–131(2018)

Abstract

We consider the problem of privacy enforcement for dynamic systems using the technique of obfuscation. Our approach captures the trade-off between privacy and utility, in a formal reactive framework. Specifically, we model a dynamic system as an automaton or labeled transition system with predefined *secret* behaviors. The system generates event strings for some useful computation (utility). At the same time, it must hide its secret behaviors from any outside observer of its behavior (privacy). We formally capture both privacy and utility specifications within the model of the system. We propose as obfuscation mechanism for privacy enforcement the use of *edit functions* that suitably alter the output behavior of the system by inserting, deleting, or replacing

events in its output strings. The edit function must hide secret behaviors by making them observationally equivalent to non-secret behaviors, while at the same time satisfying the utility requirement on the output strings. We develop algorithmic procedures that synthesize a correct-by-construction edit function satisfying both privacy and utility specifications. The synthesis procedure is based on the solution of a game where the edit function must react to the system moves by suitable output editing. After presenting an explicit algorithm for solving for the winning strategies of the game, we present two complementary symbolic implementations to address scalability of our methodology. The first symbolic implementation uses a direct encoding of the explicit algorithm using binary decision diagrams (BDDs). The second symbolic implementation reframes the synthesis of edit functions as a *supervisory control* problem and then applies a recently-developed tool for solving supervisory control problems using BDDs. Experimental results comparing the two symbolic implementations are provided.

Notes

1. This could be defined equivalently in terms of controllable events (as is more common in the supervisory control literature) by modifying the set of events and the set of transitions. Specifically, for each event e that can occur in multiple different states $\{x_1, x_2, \ldots\}$, replace e with a set of events $\{e_{x_1}, e_{x_2}, \ldots\}$ such that e_{x_1}

only occurs when the system is in state x_1, etc., and define the controllable events such that e_{x_1} is a controllable event if and only if (x_1, e) is a controllable (state, event) pair, etc.

2. EdiSyn is available at https://gitlab.eecs.umich.edu/M-DES-tools/EdiSyn/.

3. SynthSMV is available at https://bitbucket.org/blakecraw/synthsmv/.

4. dd is available at https://github.com/johnyf/dd.

References

1. Badouel, E., Bednarczyk, M., Borzyszkowski, A., Caillaud, B., Darondeau, P.: Concurrent secrets. Discrete Event Dyn. Syst. **17**(4), 425–446 (2007). doi:10.1007/s10626-007-0020-5

2. Bryant, R.E.: Graph-based algorithms for Boolean function manipulation. IEEE Trans. Comput. **C–35**(8), 677–691 (1986)

3. Burch, J.R., Clarke, E.M., McMillan, K.L., Dill, D.L., Hwang, L.J.: Symbolic model checking:

10^{20} states and beyond. Inf. Comput. **98**(2), 142–170 (1992)

4. Cassandras, C.G., Lafortune, S.: Introduction to Discrete Event Systems. Springer, Berlin (2008). doi:10.1007/978-0-387-68612-7

5. Cimatti, A., Clarke, E., Giunchiglia, E., Giunchiglia, F., Pistore M., Roveri, M., Sebastiani, R., Tacchella, A.: NuSMV 2: an OpenSource tool for symbolic model checking. In: Computer Aided Verification, Lecture Notes in Computer Science, pp. 359–364. doi:10.1007/3-540-45657-0_29 (2002)

6. Clarke, E.M., Emerson, E.A., Sistla, A.P.: Automatic verification of finite-state concurrent systems using temporal logic specifications. Assoc. Comput. Mach. Trans. Program. Lang. Syst. **8**(2), 244–263 (1986). doi:10.1145/5397.5399

7. Dubreil, J., Darondeau, P., Marchand, H.: Supervisory control for opacity. IEEE Trans. Autom. Control **55**(5), 1089–1100 (2010). doi:10.1109/tac.2010.2042008

8. Dwork, C.: Differential privacy. In: International Conference on Automata, Languages and

Programming, pp. 1–12 (2006)

9. Ehlers, R., Lafortune, S., Tripakis, S., Vardi, M.Y.: Supervisory control and reactive synthesis: a comparative introduction. Discrete Event Dyn. Syst. (2016). doi:10.1007/s10626-015-0223-0

10. Emerson, E.A.: Model checking and the mu-calculus. DIMACS Ser. Discrete Math. **31**, 185–214 (1997)

11. Falcone, Y., Marchand, H.: Runtime enforcement of K-step opacity. In: 52nd IEEE Conference on Decision and Control (2013)

12. Huth, M., Ryan, M.: Logic in Computer Science. Cambridge University Press, Cambridge (2004). doi:10.1017/cbo9780511810275

13. Jacob, R., Lesage, J.J., Faure, J.M.: Overview of discrete event systems opacity: models, validation, and quantification. Annu. Rev. Control **41**, 135–146 (2016). doi:10.1016/j.arcontrol.2016.04.015

14. Kozen, D.: Results on the propositional

μ-calculus. Theor. Comput. Sci. **27**(3), 333–354 (1983)

15. Kupferman, O., Tamir, T.: Coping with selfish on-going behaviors. Log. Program. Artif. Intell. Reason. **6355**, 501–516 (2010)

16. Ligatti, J., Bauer, L., Walker, D.: Edit automata: enforcement mechanisms for run-time security policies. Int. J. Inf. Secur. **4**(1–2), 2–16 (2005). doi:10.1007/s10207-004-0046-8

17. O'Kane, J.M., Shell, D.A.: Automatic design of discreet discrete filters. In: IEEE International Conference on Robotics and Automation (ICRA), pp. 353–360 (2015)

18. Ramadge, P.J., Wonham, W.M.: Supervisory control of a class of discrete event processes. SIAM J. Control Optim. **25**(1), 206–230 (1987)

19. Rawlings, B.C.: Discrete dynamics in chemical process control and automation. Ph.D. thesis, Carnegie Mellon University (2016)

20. Rawlings, B.C., Christenson, B., Wassick, J., Ydstie, B.E.: Supervisor synthesis to satisfy

safety and reachability requirements in chemical process control. In: 12th International Workshop on Discrete Event Systems, pp. 195–200, (2014). doi:10.3182/20140514-3-FR-4046.00127

21. Saboori, A., Hadjicostis, C.N.: Opacity-enforcing supervisory strategies via state estimator constructions. IEEE Trans. Autom. Control **57**(5), 1155–1165 (2012)

22. Schneider, F.B.: Enforceable security policies. ACM Trans. Inf. Syst. Secur. **3**(1), 30–50 (2000). doi:10.1145/353323.353382

23. Somenzi, F.: CUDD: CU decision diagram package release 2.3.0. University of Colorado at Boulder (1998)

24. Wu, Y.C., Lafortune, S.: Synthesis of insertion functions for enforcement of opacity security properties. Automatica **50**(5), 1336–1348 (2014)

25. Wu, Y.C., Raman, V., Lafortune, S., Seshia, S.A.: Obfuscator synthesis for privacy and utility. In: NASA Formal Methods, Lecture Notes in Computer Science, pp. 133–149,

(2016). doi:10.1007/978-3-319-40648-0_11

Author information

Yi-Chin Wu

Present address: Pure Storage, Inc., Mountain View, CA, USA

Affiliations

Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI, USA
Yi-Chin Wu, Blake C. Rawlings & Stéphane Lafortune

Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, Berkeley, CA, USA
Yi-Chin Wu & Sanjit A. Seshia

Zoox, Inc., Menlo Park, CA, USA
Vasumathi Raman

Corresponding author

Correspondence to Stéphane Lafortune.

Additional information

This work was supported in part by TerraSwarm, one of six centers of STARnet, a Semiconductor Research Corporation program sponsored by

MARCO and DARPA, in part by the National Science Foundation under Grants CCF-1138860 and CCF-1139138 (NSF Expeditions in Computing Project ExCAPE: Expeditions in Computer Augmented Program Engineering) and CNS-1421122, and in part by Industrial Learning Systems, Inc.

Rights and permissions

About this article

Cite this article

Wu, YC., Raman, V., Rawlings, B.C. *et al.* Synthesis of Obfuscation Policies to Ensure Privacy and Utility. *J Autom Reasoning* **60,** 107–131 (2018). https://doi.org/10.1007/s10817-017-9420-x

Received	Accepted	Published
05 December 2016	12 July 2017	22 July 2017

Issue Date
January 2018

DOI
https://doi.org/10.1007/s10817-017-9420-x

Keywords

Privacy **Formal synthesis**

Supervisory control **Edit functions**

Obfuscation