Towards Adaptive Process Confinement Mechanisms

COMP5900I Literature Review

William Findlay

October 14, 2020

Abstract

[Come back hither when done.]

References

[1] AppArmor authors, *aa-easyprof*, Linux user's manual. [Online]. Available: https://manpages.ubuntu.com/manpages/precise/man8/aa-easyprof.8.html.

[2] A. Berman, V. Bourassa, and E. Selberg, "TRON: Process-Specific File Protection for the UNIX Operating System," in *Proceedings of the USENIX 1995 Technical Conference*, 1995, pp. 165–175. [Online]. Available: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.56.9149&rep=rep1&type=pdf.

[3] H. Chen, N. Li, and Z. Mao, "Analyzing and Comparing the Protection Quality of Security Enhanced Operating Systems," in *Proceedings of the Network and Distributed Systems Security Symposium (NDSS)*, 2009. [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/2017/09/Chen.pdf.

[4] L. Deshotels *et al.*, "iOracle: Automated Evaluation of Access Control Policies in iOS," in *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, ser. ASIACCS '18, Incheon, Republic of Korea: Association for Computing Machinery, 2018, pp. 117–131, ISBN: 9781450355766. DOI: 10.1145/3196494.3196527.

[5] W. Findlay, "Host-Based Anomaly Detection with Extended BPF," Honours Thesis, Carleton University, Apr. 2020. [Online]. Available: https://williamfindlay.com/written/thesis.pdf.

[6] W. Findlay, A. B. Somayaji, and D. Barrera, "bpfbox: Simple Precise Process Confinement with eBPF," in *Proceedings of the 2020 ACM Cloud Computing Security Workshop (CCSW'2020)*, To appear, Nov. 2020. DOI: 10.1145/3411495.3421358.

[7] M. Fleming, "A thorough introduction to eBPF," *LWN.net*, Dec. 2017. [Online]. Available: https://lwn.net/Articles/740157 (visited on 09/26/2020).

[8] S. Forrest, S. A. Hofmeyr, A. Somayaji, and T. A. Longstaff, "A Sense of Self for Unix Processes," in *Proceedings 1996 IEEE Symposium on Security and Privacy*, May 1996, pp. 120–128. DOI: 10.1109/SECPRI.1996.502675.

[9] G. Gheorghe and B. Crispo, "A Survey of Runtime Policy Enforcement Techniques and Implementations," University of Trento, Tech. Rep., 2011. [Online]. Available: http://eprints.biblio.unitn.it/2268/1/techRep477.pdf.

[10] I. Goldberg, D. Wagner, R. Thomas, and E. Brewer, "A Secure Environment for Untrusted Helper Applications (Confining the Wily Hacker)," in *Proceedings of the Sixth USENIX UNIX Security Symposium*, 1996. [Online]. Available: https://www.usenix.org/legacy/publications/library/proceedings/sec96/full_papers/goldberg/goldberg.pdf.

[11] B. Gregg, *BPF Performance Tools*. Addison-Wesley Professional, 2019, ISBN: 0-13-655482-2.

[12] H. Inoue, "Anomaly detection in dynamic execution environments," Ph.D. dissertation, University of New Mexico, 2005. [Online]. Available: https://www.cs.unm.edu/~forrest/dissertations/inoue-dissertation.pdf.

[13] H. Inoue and S. Forrest, "Inferring Java Security Policies through Dynamic Sandboxing," in *International Conference on Programming Languages and Compilers (PLC'05)*, 2005. [Online]. Available: https://www.cs.unm.edu/~forrest/publications/inoue-plc-05.pdf.

[14] K. Jain and R. Sekar, "User-level infrastructure for system call interposition: A platform for intrusion detection and confinement," in *Proceedings of the Network and Distributed Systems Security Symposium (NDSS)*, 2005.

[15] K. MacMillan, "Madison: A new approach to policy generation," in *SELinux Symposium*, vol. 7, 2007. [Online]. Available: http://selinuxsymposium.org/2007/papers/08-polgen.pdf.

[16] N. Provos, "Improving Host Security with System Call Policies," in *Proceedings of the 13th USENIX UNIX Security Symposium*, 2003. [Online]. Available: https://www.usenix.org/legacy/events/sec03/tech/full_papers/provos/provos_html.

[17] Z. C. Schreuders, T. J. McGill, and C. Payne, "Towards Usable Application-Oriented Access Controls," in *International Journal of Information Security and Privacy*, vol. 6, 2012, pp. 57–76. DOI: 10.4018/jisp.2012010104.

[18] J. R. Smith, Y. Nakamura, and D. Walsh, *audit2allow*, Linux user's manual. [Online]. Available: http://linux.die.net/man/1/audit2allow.

[19] B. T. Sniffen, D. R. Harris, and J. D. Ramsdell, "Guided policy generation for application authors," in *SELinux Symposium*, 2006. [Online]. Available: http://gelit.ch/td/SELinux/Publications/Mitre_Tools.pdf.

[20] A. B. Somayaji, "Operating System Stability and Security through Process Homeostasis," Ph.D. dissertation, University of New Mexico, 2002. [Online]. Available: https://people.scs.carleton.ca/~soma/pubs/soma-diss.pdf.

[21] A. B. Somayaji and H. Inoue, "Lookahead Pairs and Full Sequences: A Tale of Two Anomaly Detection Methods," in *Proceedings of the 2nd Annual Symposium on Information Assurance Academic track of the 10th Annual 2007 NYS Cyber Security Conference*, NYS Cyber Security Conference, 2007, pp. 9–19. [Online]. Available: http://people.scs.carleton.ca/~soma/pubs/inoue-albany2007.pdf.

[22] D. A. Wagner, "Janus: An Approach for Confinement of Untrusted Applications," M.S. thesis, University of California, Berkeley, 1999. [Online]. Available: https://www2.eecs.berkeley.edu/Pubs/TechRpts/1999/CSD-99-1056.pdf.