

# COMP5900I Literature Review (Working Title)

William Findlay

October 2, 2020

## 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: <http://www.cip.ifi.lmu.de/~langeh/test/1995%20-%20Berman%20-%20TRON%20-%20Process-Specific%20File%20Protection%20for%20the%20UNIX%20Operating%20System.pdf>.
- [3] W. Findlay, "Host-Based Anomaly Detection with Extended BPF," Honours Thesis, Carleton University, Apr. 2020. [Online]. Available: <https://williamfindlay.com/written/thesis.pdf>.
- [4] 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](https://doi.org/10.1145/3411495.3421358).
- [5] M. Fleming, "A thorough introduction to eBPF," *LWN.net*, Dec. 2017. [Online]. Available: <https://lwn.net/Articles/740157> (visited on 09/26/2020).
- [6] 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](https://doi.org/10.1109/SECPRI.1996.502675).
- [7] 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>.
- [8] B. Gregg, *BPF Performance Tools*. Addison-Wesley Professional, 2019, ISBN: 0-13-655482-2.
- [9] 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>.
- [10] 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](https://doi.org/10.4018/jisp.2012010104).
- [11] J. R. Smith, Y. Nakamura, and D. Walsh, *audit2allow*, Linux user's manual. [Online]. Available: <http://linux.die.net/man/1/audit2allow>.
- [12] 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](http://gelit.ch/td/SELinux/Publications/Mitre_Tools.pdf).
- [13] 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>.
- [14] 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>.
- [15] 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>.