Towards Adaptive Process Confinement Mechanisms

COMP5900I Literature Review

William Findlay

October 23, 2020

Abstract
[Come back hither when done.]

1 Introduction

Restricting unprivileged access to system resources has been a key focus of operating systems security research since the inception of the earliest timesharing computers in the late 1960s and early 1970s [12, 17]. With the advent of the Internet and multi-tenant cloud computing, the problem of protecting hosts from their own applications has been further exacerbated.

Despite decades of work, the process confinement problem remains largely unsolved. Traditionally access to security-sensitive resources was controlled by the reference monitor mechanisms built into the operating system.

1.1 The Process Confinement Threat Model

[Threat Vectors]

T1. Malicious software.

T2. Semi-honest software.

T3. Compromised processes.

[Attack Goals]

A1. Installation of backdoors/rootkits.

A2. Compromise of trusted computing base.

A3. Unauthorized access to files.

A4. Denial of service.

A5. Theft of computational resources.

1.2 Outline

The rest of this paper proceeds as follows. **[List sections and what is in them.]**

2 Traditional Process Confinement Approaches

3 Automating Policy Generation

4 Automating Policy Audit

5 Integrating System State into Process Confinement

5.1 Anomaly Detection

5.2 Extended BPF

6 Conclusion

References

[1] J. Anderson, "A Comparison of Unix Sandboxing Techniques," *FreeBSD Journal*, 2017. [Online]. Available: http://www.engr.mun.ca/~anderson/publications/2017/sandbox-comparison.pdf.

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

[3] 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.

[4] 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.

[5] L. Deshotels, R. Deaconescu, C. Carabas, I. Manda, W. Enck, M. Chiroiu, N. Li, and A.-R. Sadeghi, "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.

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

[7] 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.

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

[9] 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.

[10] 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.

[11] 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.

[12] R. M. Graham, "Protection in an information processing utility," vol. 11, no. 5, pp. 365–369, 1968, ISSN: 0001-0782. DOI: 10.1145/363095.363146.

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

[14] 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.

[15] 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.

[16] 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.

[17] B. W. Lampson, "A Note on the Confinement Problem," in *Communications of the ACM*, vol. 16, New York, NY, USA: Association for Computing Machinery, 1973, pp. 613–615. DOI: 10.1145/362375.362389.

[18] 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.

[19] 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.

[20] 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.

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

[22] 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.

[23] 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.

[24] 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.

[25] 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.