# ADFA IDS DataSets Version 2.0

# License Agreement

# 23/03/2017

ADFA IDS Datasets consist of following individual IDS datasets:

(1) network and Linux host IDS datasets: ADFA-LD-dataset, netflow-IDS-dataset, and NGIDS-DS IDS Dataset.

Download link:

https://research.unsw.edu.au/people/professor-jiankun-hu,

(2) Windows based IDS dataset ADFA-WD

Download link:
https://cloudstor.aarnet.edu.au/plus/index.php/s/IMWyBMBGOEgdliH).

This License Agreement applies to all of above-mentioned IDS datasets. Redistribution and use of these software/data are permitted if the following General Conditions (GC) and Specific Conditions (SC) are met:

General Condition (GC):

The use of these data/codes is for the purpose of research only. Anyone downloading the data/code must agree the following: (i) The website host and the contributors have the right not to answer any queries. (ii) No any liability whatsoever could be imposed on the website host and contributors.

Specific Conditions (SC):

(1) Following references [1][2][3][4][5][6][7][8][9] must be cited in any paper/report that makes any use of the relevant data/code. Some details of these datasets, and how to use them can be found in these references.
(2) Redistributions must reproduce the License agreement in this document.

[1] W. Haider, J. Hu, S. Slay, B. P. Turnbull and Y. Xie, "Generating Realistic Intrusion Detection System Dataset based on Fuzzy Qualitative Modeling," *Journal of Network and Computer Applications (JNCA), 2017*, DOI: 10.1016/j.jnca.2017.03.018.

[2] G. Creech, J. Hu, “A semantic approach to host-based intrusion detection systems using contiguous and discontiguous system call patterns,” IEEE Transactions on Computers, vol. 63, issue 4, April 2014, pp. 807-819.
[3] G. Creech, and J. Hu, “Generation of a new IDS test dataset: Time to retire the KDD collection,” 2013 IEEE Wireless Communications and Networking Conference, WCNC 2013, pp.4487-4492.
[4] M. Xie, and J. Hu, “Evaluating host-based anomaly detection systems: A preliminary analysis of ADFA-LD,” Proc. Of the 6th International Congress on Image and Signal Processing, CISP 2013, pp. 1711-1716.
[5] M. Xie, J. Hu, X. Yu, and E. Chang, “Evaluating host-based anomaly detection systems: Applications of the frequency-based algorithms to ADFA-LD,” LNCS, vol. 8792, 2014, pp.542-549.
[6] W. Haider, J. Hu, and M. Xie, “Towards reliable data feature retrieval and decision engine in host-based anomaly detection systems,” Proc. Of the 2015 10th IEEE Conference on Industrial Electronics and Applications, ICIEA 2015, pp. 513-517.
[7] W. Haider, G. Creech, Y. Xie, and J. Hu "Windows Based Data Sets for Evaluation of Robustness of Host Based Intrusion Detection Systems (IDS) to Zero-Day and Stealth Attacks." Future Internet 8.3 (2016): 29.
[8] W. Haider, J. Hu, X. Yu, and Y. Xie, “Integer data zero-watermark assisted system calls abstraction and normalization for host based anomaly detection systems,” Proc. Of the 2nd IEEE International Conference on Cyber Security and Cloud Computing, 2016, pp. 349-355.
[9] Q.A. Tran, F. Jiang, and J. Hu, “A real-time NetFlow-based intrusion detection system with improved BBNN and high-frequency field programmable gate arrays,” Proc. Of the 11th IEEE International Conference on trust, Security and Privacy in Computing and Communications, TurstCom 2012, 2012, pp. 201-208.

Other useful references for IDS research

[10] E. Kabir, J. Hu, H. Wang, G. Zhuo, “A novel statistical technique for intrusion detection systems,” Future Generation Computer Systems, 2017
[11] M. Xie, J, Hu, S. Guo, and A. Y. Zomaya, “Distributed segment-based anomaly detection with kullback–leibler divergence in wireless sensor networks,” IEEE Transactions on Information Forensics and Security, vol. 17, issue 1, 2017, pp. 101-110.
[12] M. Ahmed, A.N. Mahmood, and J. Hu, “A survey of network anomaly detection techniques,” Journal of Network and Computer Applications, vol. 60, 2016, pp. 19-31.
[13] Z. Tan, A. Jamdagni, X. He, P. Nanda, R.P. Liu, and J. Hu, “Detection of Denial-of-Service Attacks Based on Computer Vision Techniques ,” IEEE Transactions on Computers, vol. 64, issue 9, 2015, pp. 2519-2533.
[14] M. Xie, J. Hu, and S. Guo, "Segment-based anomaly detection with approximated sample covariance matrix in wireless sensor networks," IEEE Transactions on Parallel and Distributed Systems (TPDS), vo. 26, no.2, 2015, pp.574-583.
[15] Y. Feng, F. Han, X. Yu, Z. Tari, L. Li, and J. Hu, “Terminal sliding mode observer for anomaly detection in TCP/IP networks,” Proc. of 2011 International Conference on Computer Science and Network Technology, 2011, pp. 617-620.
[16] X.D. Hoang, J. Hu, and P. Bertok, “A program based anomaly intrusion detection scheme using multiple detection engines and fuzzy inference,” Journal of Network and Computer Applications, Elsevier, vol.32, Issue 6, 2009, pp.1219-1228.
[17] J. Hu, D. Qiu, H.H. Chen and X. Yu, “A simple and efficient data processing scheme for HMM based anomaly intrusion detection.” IEEE Network, 2009, pp.42-47.

[18] X.D. Hoang, J. Hu, and P. Bertok, “A multi-layer model for anomaly intrusion detection using program sequences of system calls,” The 11th IEEE International Conference on Networks, 2003, pp.531-536