Test of Time Award

ACSAC 2022

Test of Time Paper Awards

- Recognize and honor selected papers from the first 20+ years (1985-2006) that have had a significant impact
  - Led to a major change in the field
  - Are used commercially
  - Have been well cited
  - Are well known as strong papers

https://www.wabisabilearning.com/blog/13-educational-tools-test-time

Test of Time Committee

Juan Caballero, IMDEA Software Institute

Wouter Joosen, KU Leuven

Evangelos Markatos, University of Crete & FORTH

Robin Sommer, CoreLight

Dongyan Xu, Purdue University

Selection Process

- Committee examined all papers from 1985 through 2006 (inclusive)
- Papers with more than 15 years since publication in ACSAC
- Committee could nominate any (non-conflicted) paper
- Meeting to discuss nominations
- All awarded papers had at least 3 nominations

ACSAC 1998

- **Title:** Detecting Anomalous and Unknown Intrusions Against Programs
- **Authors:** Anup K. Ghosh, James Wanken, Frank Charron
- **Summary of Nomination:** One of the first applications of machine learning (more specifically neural networks) to intrusion detection. The authors focus on anomaly detection by building profiles of computer programs, as opposed to previous work that builds user profiles. Expectations of normal program behavior are created by dynamic analysis of the process under normal operational conditions. The committee found this to be a hidden gem that reminds us how techniques widely used by our community today like neural networks, dynamic execution, and program profiling were introduced nearly 25 years ago.

ACSAC 2002

- **Title:** Throttling Viruses: Restricting propagation to defeat malicious mobile code

- **Author:** Matthew Williamson

- **Summary of Nomination:** Highly cited, single-author, paper that presents the property that under normal activity a machine will make a low rate of outgoing connections to new or different machines, and that connections are locally correlated, e.g., it is more likely to connect to the same machine regularly than to different machines. This intuition has been the basis for follow-up work on scan detection, worm detection, and peer-to-peer protocols.

ACSAC 2006

- **Title:** PolyUnpack: Automating the Hidden-Code Extraction of Unpack-Executing Malware.

- **Authors:** Paul Royal, Mitch Halpin, David Dagon, Robert Edmonds, Wenke Lee

- **Summary of Nomination:** Arguably, the first generic malware unpacking system. It proposes the widely used unpack and execute (or write-and-execute) property that serves as basis for generic malware unpackers. Made their implementation available as a great example of early open science. The committee appreciated that this work brings a solid base for investigating and studying malware, i.e., delivering an enabler for practical work and thus, potentially a high and significant impact to researchers and practitioners.