

Method and Device for In-situ Trainable Intrusion Detection System

Disclosure Number

201202902

Technology Summary

Almost every major computer network is defended by signature-based Intrusion Detection Systems (IDSs) that are designed to alert whenever a pattern that indicates a known exploit is detected. We have developed an advanced, non-signature-based, learning IDS that requires few training samples and can therefore be trained in a cost-effective manner. The approach has demonstrated the ability to catch almost every previously unseen attack (which cannot be detected by signature IDSs) while generating false positive alerts at a much lower rate than signature IDS systems. With this capability, a new machine-learning sensor can be set up in place and trained in an approximately one day with support from a penetration testing team. The resulting sensor offers a very high level of defense against unknown exploits (for which there was previously no proven defense).

Inventor

BEAVER, JUSTIN M

Computational Sciences & Engineering Div

Licensing Contact

SIMS, DAVID L

UT-Battelle, LLC

Oak Ridge National Laboratory

Rm 124C, Bldg 4500N, MS: 6196

1 Bethel Valley Road

Oak Ridge, TN 37831

Office Phone: (865) 241-3808

E-mail: SIMSDL@ORNL.GOV

Note: The technology described above is an early stage opportunity. Licensing rights to this intellectual property may be limited or unavailable. Patent applications directed towards this invention may not have been filed with any patent office.