DHS Science and Technology Directorate

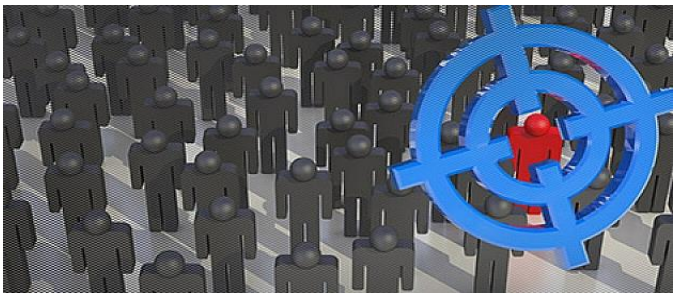
Cyber Security Division - Insider Threat

The real threats posed by trusted insiders

Cybersecurity measures are frequently focused on threats outside an organization, rather than threats posed by untrustworthy individuals inside an organization. In fact, well-publicized insiders have caused irreparable harm to their organizations, as well as national security interests. An insider threat can be defined as the potential violation of system security policy by an authorized user. Although policy violations can be the result of carelessness or accident, the core concern is deliberate and intended actions such as malicious exploitation, theft, or destruction of data; or the compromise of networks, or other information technology (IT) resources.

A research portfolio to aggressively curtail elements of Insider Threat

The U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Cyber Security Division's (CSD) Insider Threat project is developing solutions that compliment and expand the capabilities of existing commercial insider threat tools. In many systems, the integrity, availability, and total system survivability are of the highest priority and can be compromised by insiders. S&T CSD's research includes a project with Northrop Grumman focusing on the exfiltration of data residing in a database management system. CSD is working with Carnegie Mellon University/Software Engineering Institute to develop insider threat case studies based on investigative casework.



Given the universal challenges presented by insiders, this research area considers the global problem and is partnering with the United Kingdom (UK) Centre for the Protection of National Infrastructure to complement ongoing research programs and allow collaboration among researchers.

Another important element of the Insider Threat project is the development of a freely available research dataset for researchers to test their tools. Generating test data in this space is time consuming for academics and small companies, so S&T is developing a collection of insider threat data that will be made available for use by the entire community.

In fiscal year 2015, DHS S&T participated within the Enduring Security Framework Insider Threat Working Group, a DHS/NSA-led partnership between the private sector and government agencies to develop a comprehensive insider threat program using technology and analytics within modern, cloud-based architectures.

Organizations will have a more complete approach to the insider threat problem

Current, widely implemented insider threat detection tools provide capabilities to inform operational use, however they are not considered to be a complete solution. The research conducted through this project will focus on elements that are not currently available via commercial tools. In doing so, S&T's work in this space will benefit a wide range of potential customers including national security bodies, government officials who need controlled unclassified information, healthcare, finance, and many other critical infrastructure sectors where sensitive and valuable information is managed.

Performers

- Northrop Grumman/Purdue University
- Carnegie Mellon University/Software Engineering Institute
- Massachusetts Institute of Technology – Lincoln Labs

Homeland Security
Science and Technology

To learn more about Insider Threat, contact Megan Mahle, Program Manager, at SandT-Cyber-Liaison@HQ.DHS.GOV.

03-03-2016