**Challenge**

Determining the *intent* of someone when they access information which they have legitimate rights to access, but which they might then use for purposes that are counter to the organization that owns the data.

**Focus**

This CA Labs research project is focused on determining new approaches to detecting people who are “inside” an organization, but whom might be acting against the organization’s best interests.

**Result**

New insider threat detection approaches and algorithms can help protect organizations against fraud, data exfiltration, and system sabotage.

Employees, contractors, and third-party outsourcers are automatically trusted by an organization and thus are given access to large amounts of information. Often it is too labor-intensive to restrict users to JUST the information they need to perform their job, and so they have access to more data than necessary. Insider threat research aims to detect when someone with such legitimate access is actually acting *against* the best interests of their organization.

Generally, access to resources within an organization is granted based on the role of the individual. This saves the organization effort by (typically) ensuring that the individual has access to all the resources he requires, while at the same time reducing the number of permission sets that need to be maintained to be the number of roles rather than the number of employees. However, providing employees with access to more resources, files and information than they need makes an implicit assumption that the employee can be trusted with this information and will not abuse that access, thus breaking the security policy of least privilege. For the most part, that trust is well-founded, and employees, along with other insiders (e.g., contractors), will not abuse that trust nor do anything that runs counter to the mission of their organization. However, in those instances where an employee does harm their organization, the damage they typically cause is considerable given the nature of their access.
Advancing insider threat capabilities

CA Labs Insider Threat research project advanced the value of insider threat detection activities by:

■ Flagging individuals who are making a suspicious file access.
■ Providing the capability to block access to a file if the activity is too unusual.
■ Warning administrators that an individual has started behaving differently (based on file access).

More information on CA Labs Insider Threat research project

CA Labs is collaborating with researchers from the University of California at Davis (United States) and Carleton University (Canada). The following papers have been published about this research project:


For additional information about this or other CA Labs projects, please contact Dr. Carrie Gates at Carrie.Gates@ca.com.

About CA Labs and innovation

CA Labs is the research arm for CA Technologies and a hub for the company's initiatives for innovation. CA Labs collaborates with the world's foremost researchers in academia, industry and government to perform advanced research to address cloud, software-as-a-service, security, virtualization, automation, mainframe, service assurance, and service and portfolio management challenges. For more information, visit ca.com/calabs.