Inside the Insider Threat
(Introduction)

Matt Bishop
Department of Computer Science
University of California at Davis
Davis, CA, USA
mabishop@ucdavis.edu

Kara Nance
Hume Center
Virginia Tech
Arlington, VA, USA
knance@vt.edu

Jason Clark
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA, USA
jwclark@cert.org

The insider threat problem has historically been
one of the most important problems in security; as the
ancient Roman satirist Juvenal wrote, “Who will
guard the guards themselves?” The situation is no
different in the Digital Age. Some insider threats
come from those with the greatest access to organiza-
tional resources, and thus the greatest ability to cause
devastating consequences. Other threats come from
unwitting insiders duped into assisting outside enti-
ties in carrying out attacks. Some insiders act alone,
while others collaborate to create failures from sabo-
tage, loss of revenue from fraud and theft, and loss of
information from espionage. Insider attacks may be
accidental or arise from conflicting policies that con-
fuse the putative attacker. In many cases, uninten-
tional insider attacks are as dangerous as deliberate
insider attacks; preventing them adds more complexi-
ty to an already, difficult problem. Any approach
therefore must have not only a technical aspect (de-
tecting the attack), but also a non-technical aspect
detecting the problem), which includes consideration
of social, political, legal, and cultural influences,
among others.

Analyzing and detecting insider threats involve
both technical and non-technical approaches across
many different disciplines, including human-oriented
ones. This mini-track solicited papers emphasizing
this cross-cutting work as well as papers that present
case studies and experiences in coping with insider
attacks or preventing them.

In their contribution Graph Based Framework
for Malicious Insider Threat Detection, Anagi
Gamachchi, Li Sun, and Serdar Boztas combine
graphical analysis and anomaly-based intrusion de-
tection approaches to find malicious insiders. They
first generate a graph and various subgraphs showing
the relationships between various resources, and cal-
culate graph-based parameters for each user. Then
they apply anomaly-based intrusion detection meth-
ods to identify users with anomalous parameters.
These users can then be monitored.

The second paper, Insider Threat Detection in
PRODIGAL by Henry Goldberg, William Young,
Matthew Reardon, Brian Phillips, and Ted Senator,
reports on research leading to the development of
using a prototype system, PRODIGAL, to examine a
variety of detection methods. They describe the ar-
chitecture of the system, and report on a series of
experiments to test how accurately PRODIGAL de-
tects insider behaviors. They also present an analysis
of factors that influence the accuracy of the detector.

In the paper Insider Threats in Emerging Mobili-
ty-as-a-Service Scenarios, Andreas Melis, Marco
Prandini, Saverio Giallorenzo, and Franco Callegati
examine a paradigm called Mobility-as-a-Service,
which applies the cloud computing paradigm to
transportation. Their model is that of a federation of
providers trading resources as needed. This leads to a
number of security and privacy threats, of which the
insider problem is a major component. Their layered
structure leads to a classification of threats and sug-
gested countermeasures.

These papers examine three very different aspects
of the insider problem. Each focuses on the technolo-
gies and the people who use the technologies. The
first reports on a framework that combines techniques
to detect and isolate insiders. The second reports on a
prototype insider detection and analysis system to test
various combinations of insider detection and analy-
sis methods. The third looks at a particular applica-
tion, namely that of a federation of transportation
services, and uses the Mobility-as-a-Service model to
understand the insider threats and countermeasures in
that market. These papers represent not only the cut-
ting edge of research in this area, but also the breadth
of the areas in which this problem arises. Their con-
tributions advance the study of this critical, complex
problem.