

Attack Detection

Jonathan Jogenfors

Leonardo Iwaya

2016-09-26

- About us



- Model of information security: Prevention, Detection, Reaction (PRD)
 - Prevention: Difficult because attacker has the advantage.
Large attack surface.
 - Reaction: Too late!
 - Detection: What our papers are all about

When prevention fails

Anomaly detection

Honeypots

Motivation

Attack detection and identification in cyberphysical systems (2013)