A Semantic Approach to Situational Awareness for Intrusion Detection

Sumit More, Mary Matthews, Anupam Joshi and Tim Finin
University of Maryland, Baltimore County

Problem Statement

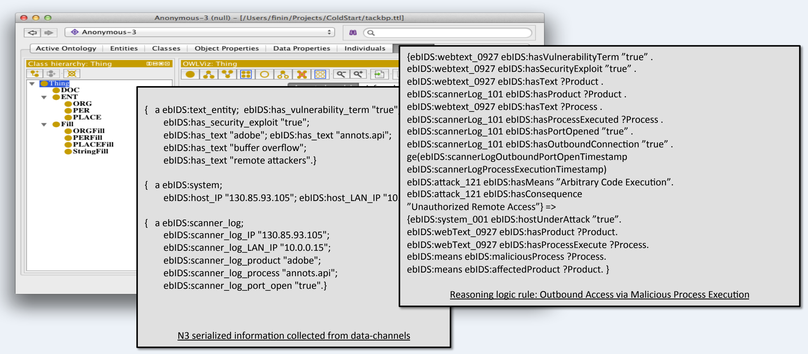
We formulate a semantically rich approach to intrusion detection by gathering data from heterogeneous data channels, integrating it into an information-rich knowledge base, and reasoning over the contents to detect attacks or intrusions whose signatures are not available for comparison.

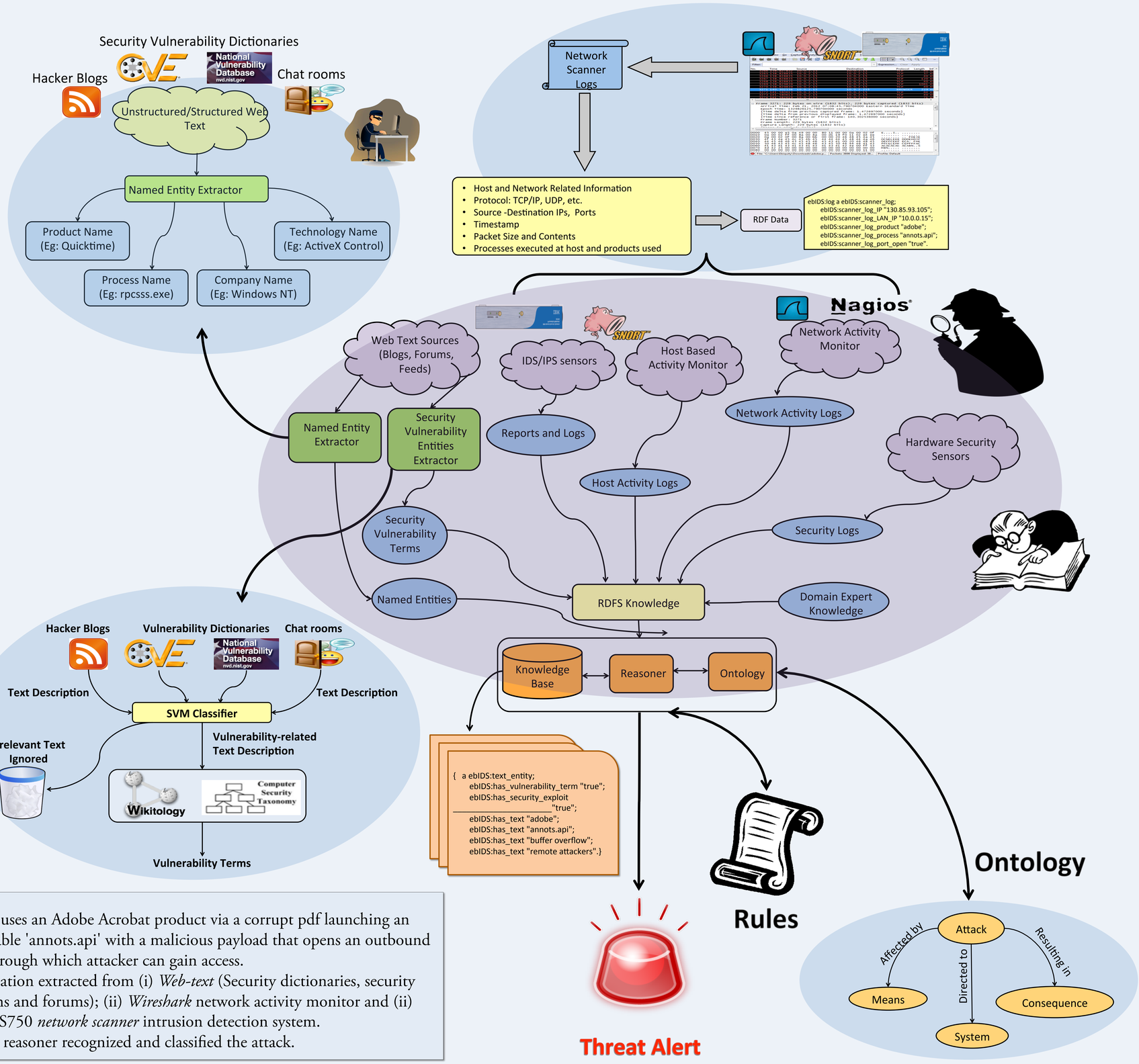
Motivation

Current intrusion detection systems are limited in their ability to handle zero-day attacks and intrusions that follow a low-and-slow intrusion pattern. Heterogeneous data sources can provide useful information even when an attack signature is unavailable and can monitor their temporal and spatial extent.

System Architecture

- Data streams: Web text, host-based and network-based activity monitors, and IDS/IPS logs
- Intrusion detection ontology: Models the intrusion, attack, system and network behaviors
- Knowledge Base: integrates information collected from heterogeneous data-sources
- Reasoner: OWL DL reasoner augmented with rules to infer possibility of an attack





Evaluation Experiments

- We tested the system's effectiveness by executing attacks with unknown signatures and observing if they were detected
- Example: A stack-based buffer overflow in Adobe Reader allows remote attackers to execute arbitrary code via a corrupt pdf file on the infected host (CVE-2009-0927). It is known to have infected over 1200 hosts.

- Attack uses an Adobe Acrobat product via a corrupt pdf launching an executable 'annots.api' with a malicious payload that opens an outbound port through which attacker can gain access.
- Information extracted from (i) *Web-text* (Security dictionaries, security bulletins and forums); (ii) *Wireshark* network activity monitor and (ii) IBM ES750 *network scanner* intrusion detection system.
- Result: reasoner recognized and classified the attack.

UMBC ebiquity
Supported by AFOSR FA9550-08-1-0265 and a gift from Northrop Grumman Corporation
http://ebiq.org/j/98