FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

Diplomarbeitspräsentationen der Fakultät für Informatik

XIDS - An XVSM-Based Collaborative Intrusion Detection System

Masterstudium:
Software Engineering & Internet Computing

Markus Winkler

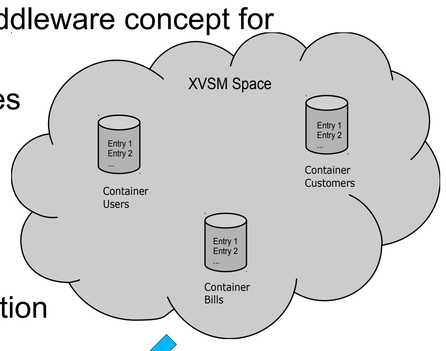
Technische Universität Wien
Institut für Computersprachen
Arbeitsbereich: Programmiersprachen und Übersetzerbau
Betreuerin: A.o. Univ. Prof. Dr. Dipl.-Ing. eva Kühn

Context

- Conventional Intrusion Detection Systems (IDS) are unable to detect certain types of attacks (eg Slow-Scan attacks)
- Collaborative IDS (CIDS) can detect such attacks
- Several CIDS exist, all with different approaches
- Biggest challenge → Collaboration !
- XVSM is a middleware designed for applications with high collaboration needs

XVSM

- XVSM (e**X**tensible **V**irtual **S**hared **M**emory) is a middleware concept for highly collaborative applications
- Efficient coordination between distributed processes
- Supports platform interoperability using an XML protocol for communication
- XVSM space consists of containers, holding data entries
- MozartSpaces is a Java-Based XVSM implementation

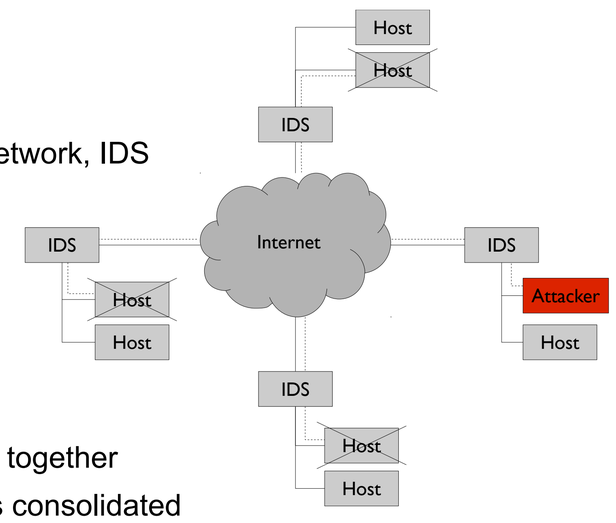


Collaborative Intrusion Detection

Example Slow-scan

regular IDS:

- Attacker attacks ONE host in each network, IDS detects only one scan
- **Result**: Slow-Scan is not detected

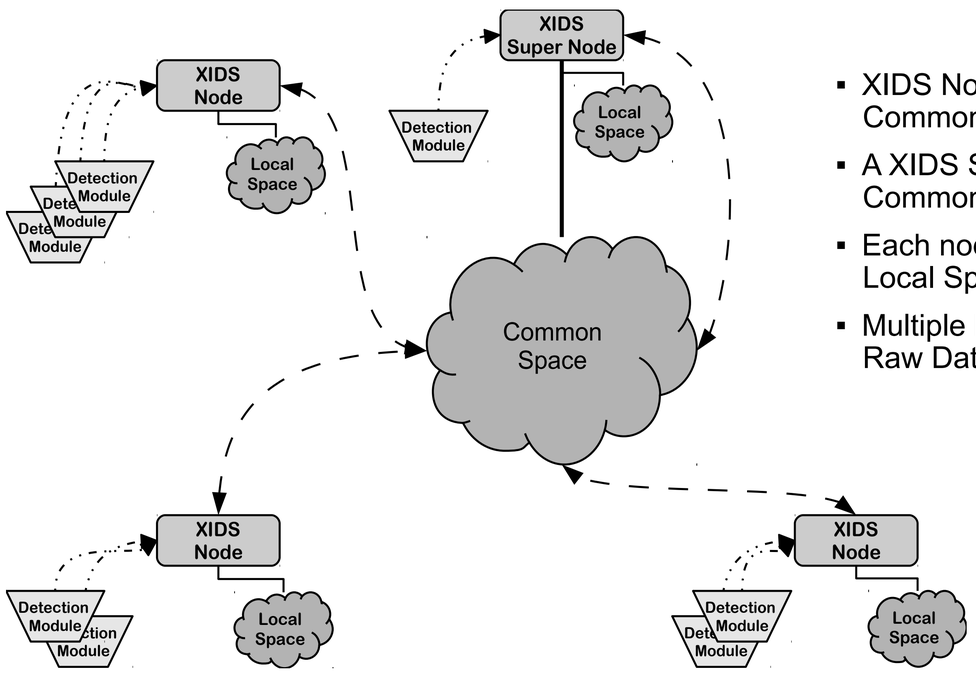


Collaborative IDS:

- Each Detection Instance detects one scan in their network
- The Detection Instances are working together
- The data of all Detection Instances is consolidated
- Due to collaboration, the system knows about 3 incidents
- **Result**: Slow-Scan is detected

Collaborative Intrusion Detection Systems are more or less multiple IDS working together and share information about their locally collected incidents.

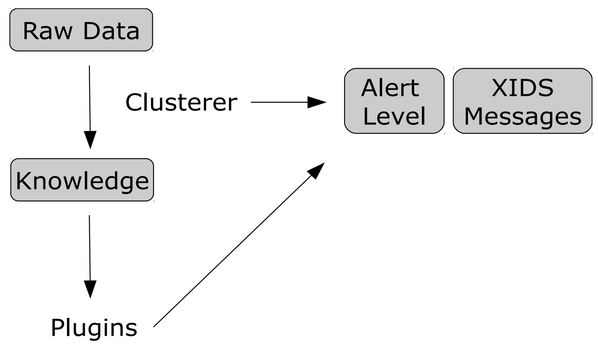
System Architecture



- XIDS Nodes share XVSM Common Space
- A XIDS SuperNode provides Common Space
- Each node stores local data in Local Space
- Multiple Detection Modules provide Raw Data / Alerts to a XIDS Node

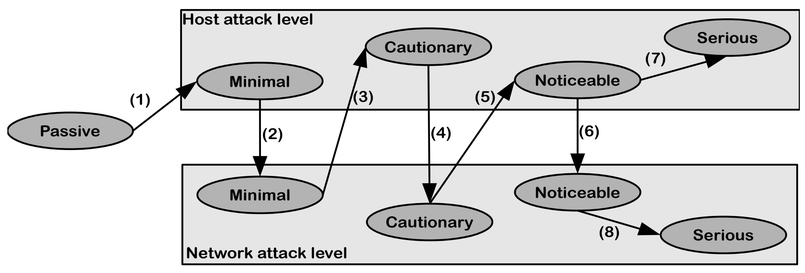
Prototype

Data aggregation (Clustering)



- Raw data is collected in local Raw Data Container
- Clusterer module aggregates RawAlerts into Knowledge
- Clusterer module also generates XIDS Messages indicating detection of threads/alerts
- Clusterer module increase/decreases Alert Level
- Additional detection plugins can also detect threads/alerts
- Plugins can also issue XIDS Messages and alter the Alert Level

Alert Level Escalation



- Alert Level is increased/decreased with number of detected significant threats / alerts
- Host Alert Level on each XIDS Node to indicate the threat on the node itself
- Network Alert Level to indicate the threat on the whole network (global view)
- Expire mechanism allows to decrease Alert Level if alerts are expired
- Each Alert Level change triggers the creation of a XIDS Message
- Each Alert Level shows a certain threat level
- The Alert Level subsystem allows to take specific actions on certain levels
  This could be a simple notification and might also trigger the complete lockdown of the firewall to prevent serious damage on the system

Contributions

- XVSM middleware provides a good and stable base for a fully productive Collaborative Intrusion Detection System
- Modular based solution important due to extensibility
- Plugin subsystem to extend XIDS functionality on runtime
- MozartSpaces (XVSM) allows easy implementation
- XIDS can be extended with plugins to deal with new threads
- Lookup mechanism to minimize local configuration of nodes
- XIDS supports different reports/charts
- Fully working prototype was tested in a small environment of about 3 to 4 nodes and up to 5 detection modules

Contact: e0225272@student.tuwien.ac.at