DAI-Labor
TU Berlin

CRITIS‘06

Intelligent Network-Based Early Warning Systems

CRITIS’06 August/September 2006

Karsten Bsufka
karsten.bsufka@dai-labor.de
Olaf Kroll-Peters
olaf.kroll-peters@dai-labor.de
Sahin Albayrak
sahin.albayrak@dai-labor.de

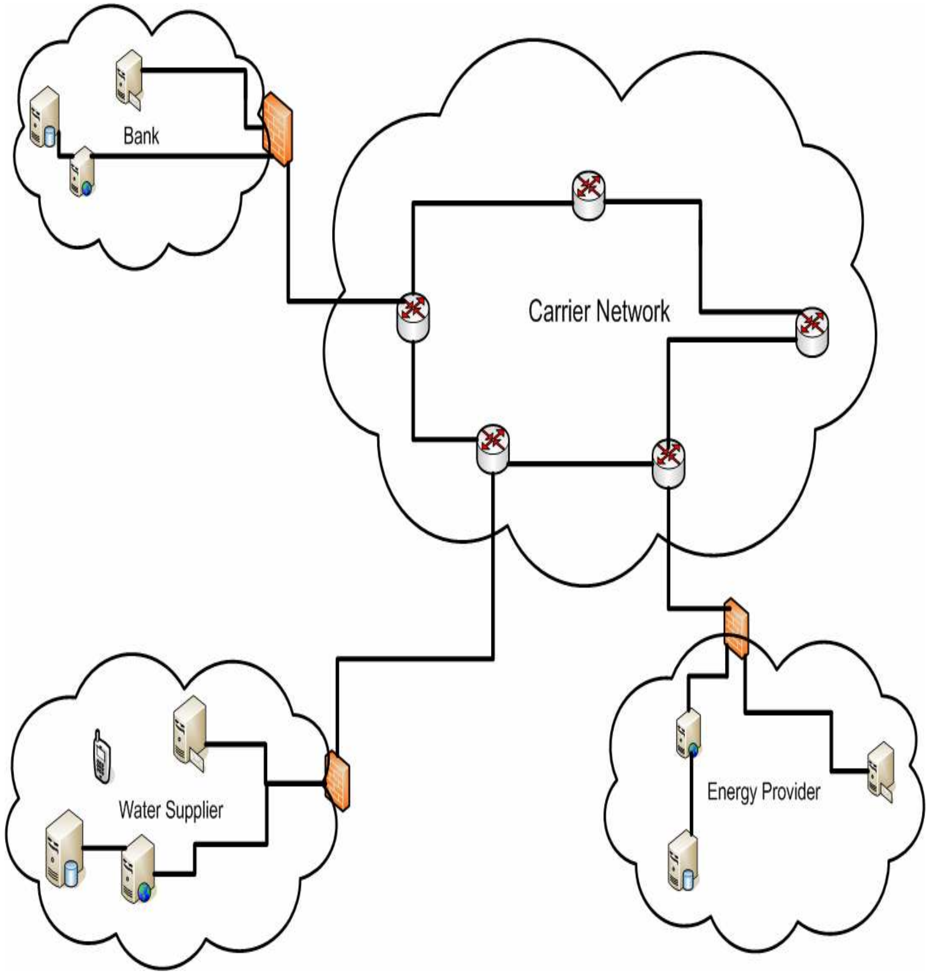
A|O|T
Agententechnologien in
betrieblichen Anwendungen
und der Telekommunikation

Overview

1. Motivation for CRITIS early warning system
2. Elements of an agent-based early warning system (A-EWS)
3. Interaction between agents
4. Important issues and conclusion

Motivation for CRITIS early warning system

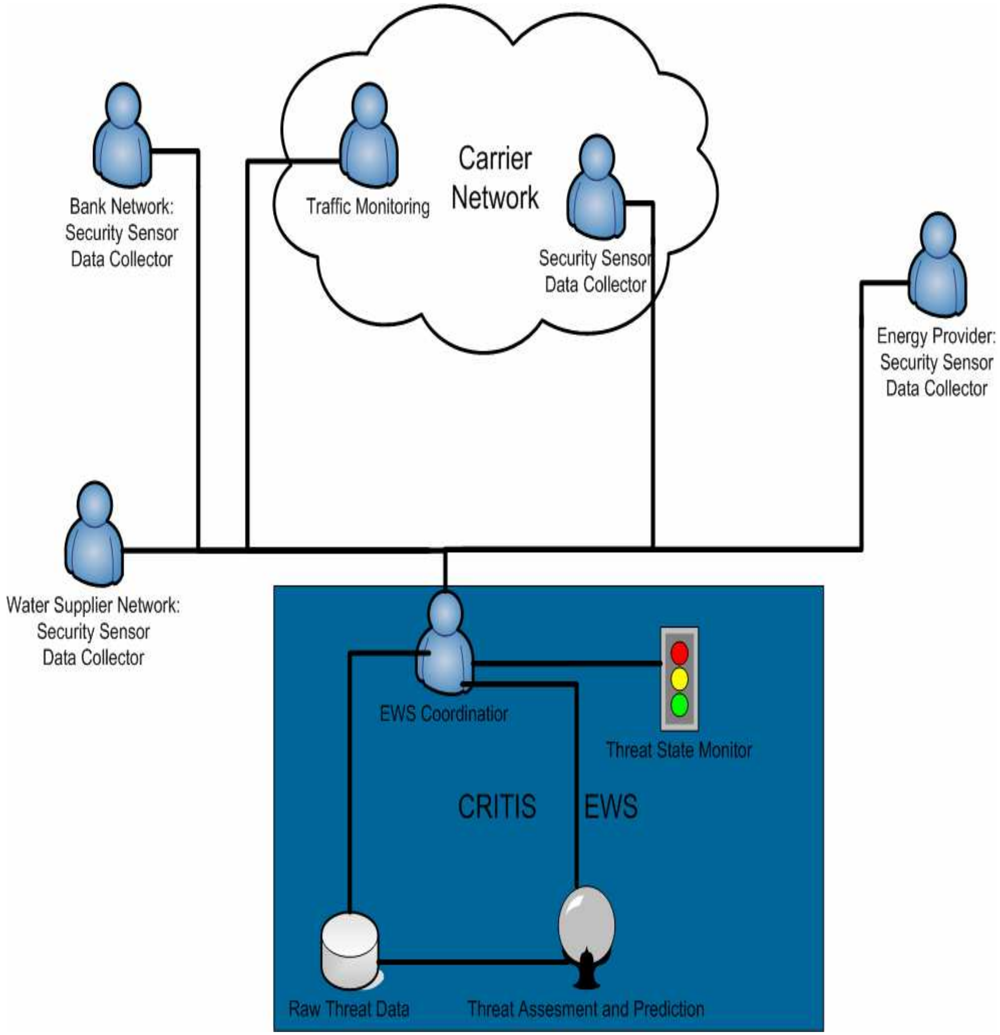
- **Untargeted malware is a threat to every critical infrastructure.**
- **Successful untargeted attacks and targeted attacks can affect other infrastructures due to the interdependencies between infrastructures.**



Elements of an agent-based early warning system (A-EWS)

- **Sensors**
  - **Security appliance (IDS, firewall, …) Sensors**
  - **Network Traffic Sensors**
  - **Anomaly Sensors**
  - **Attack Pattern Sensors**

- **A-EWS Center**
  - **EWS Coordinator (event and indicator collection and pre-processing)**
  - **Raw threat data base**
  - **Threat assessment and prediction (generate warnings and alerts)**
  - **Threat state monitor**


Carrier Network
Bank Network: Security Sensor Data Collector
Traffic Monitoring
Security Sensor Data Collector
Energy Provider: Security Sensor Data Collector
Water Supplier Network: Security Sensor Data Collector
EWS Coordination
Threat State Monitor
CRITIS
EWS
Raw Threat Data
Threat Assesment and Prediction

Sensors

- **Security appliance Sensors**
  - Scan log files and/or receive events directly.
  - Interpret events: Forward relevant events.
- **Network Traffic Sensors**
  - Analyses network traffic flow information.
- **Attack Pattern Sensors**
  - Searches for attack patterns on different network layers.
- **Anomaly Sensors**
  - Detection of non-typical behavior and classification of detection results.

A-EWS Center

- **EWS Coordinator**
  - Receives raw events from sensors and warnings of local attacks, this may include information about attackers.
  - Attaches source information to events and warnings.
  - Attaches a priority to events and warnings.
- **Event and indicator data base**
  - Stores and manages stored events and warnings.

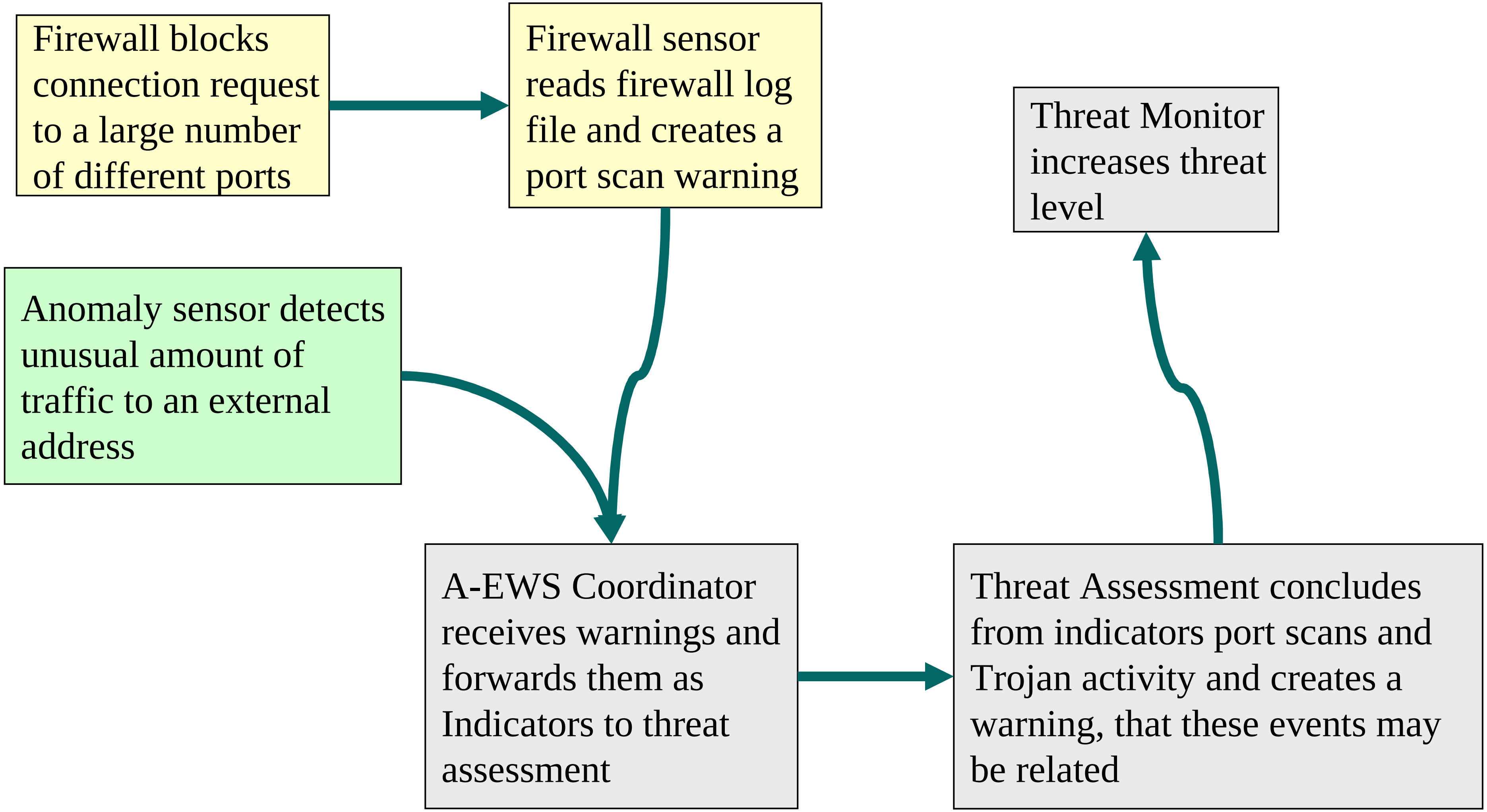
A-EWS Center

- **Threat assessment and prediction**
  - Responsible for creating warnings for humans.
  - Informing security experts about indecisive results.
  - Store information for later analyses, especially for automatic decisions.
- **Threat state monitor**
  - Quick overview of global threat state.
  - Influences assignment of priorities by EWS Coordinator.
  - Influences threat assesment and prediction.
  - Influenced by threat assesment and prediction.

Interaction between agents

- Sensors have only a local view of events.
- On a local scope, e.g. within one critical infrastructure network, sensors may cooperate with each other.
- Sensors must cooperate with an A-EWS Center.
- Cooperation is based on a common set of ontologies and communication protocols.
- Sensor agents act as translators for local and application specific formats and the A-EWS ontologies and protocols.
- Agents should be capable of using different communication techniques, e.g. they use SMS for alerts, when Internet connections have failed.

Example scenario



Firewall blocks connection request to a large number of different ports

Firewall sensor reads firewall log file and creates a port scan warning

Anomaly sensor detects unusual amount of traffic to an external address

A-EWS Coordinator receives warnings and forwards them as Indicators to threat assessment

Threat Assessment concludes from indicators port scans and Trojan activity and creates a warning, that these events may be related

Threat Monitor increases threat level

Important issues and conclusion

- **Described A-EWS architecture is possible, but requires that the following points are addressed:**
  - Detection of unknown attacks.
  - Flexible common ontologies and communication protocols.
  - Sensor agents must also enforce a local and global A-EWS policy.
    - Which deals with privacy aspects of collected personal information.
    - Which deals with secrecy aspects of collected infrastructure (company) data.
  - Scalability and data management aspects of the A-EWS.
  - Quality of generated warnings and alerts.
  - Up-to-dateness of detectable risks and threats.
  - Intelligent combination of IT related events and non-IT related events (e.g. burglar or fire alarms).
  - Cost effective sensor deployment.

The End

Questions?