Fachhochschule Gelsenkirchen

Internet Early Warning Systems

Overview and Architecture

Mathias Deml
Sebastian Schmidt
Sascha Bastke

{deml,schmidt,bastke} (at) internet-sicherheit.de

Institute for Internet-Security
https://www.internet-sicherheit.de/en
University of Applied Sciences Gelsenkirchen

Agenda

- Introduction
- Threat Scenarios
- Definition of an IEWS
- Technical Components
- Architecture
- Conclusion

Agenda

- **Introduction**
- Threat Scenarios
- Definition of an IEWS
- Technical Components
- Architecture
- Conclusion

Introduction (1/2)

- Protection of critical infrastructure is necessary
- Internet is part of the critical infrastructure
- For protection of the Internet we need Internet Early Warning Systems (IEWS)
- Goal
  - Protect and uphold the functionality of the internet

    => Protect and uphold the systems that are part of this infrastructure
- Relevant aspects
  - Early detection of threats and initiation of countermeasures
  - Improvement of the infrastructure to deal with future requirements

Introduction (2/2)

- Definition early warning for natural catastrophe:

  “Early Warning is the warning of menacing natural phenomenon which occurs so early that the potentially concerned persons have the possibility to react so that personal injury can be avoided or reduced” [1]

- Basically the same for internet early warning
- Different types of early warning
  - Type 1: Before the start of an attack
  - Type 2: With beginning of/During the attack
  - Type 3: Before a possible threat
- How early can be warned?

Agenda

- Introduction
- **Thread Scenarios**
- Definition of an IEWS
- Technical Components
- Architecture
- Conclusion

Thread Scenarios (1/4)

- (D)DoS
  - Early warning problematical, because pakets reach the target to fast
  - Early warning time: seconds
- Exploits
  - Early warning of actual executed Exploit problematical because pakets reach the target to fast
  - Early warning time: seconds
  - Early Warning of potential imperiling Exploit possible, because not all vulnerable Systems attacked in parallel
    - Early warning time dependent on exploitation (e.g. Malware Spreading)

Thread Scenarios (2/4)

- Malware Spreading
  - Spreading needs a period of time
  - Period of time is dependent on the malware design (without taking countermeasures into account)
  - Spreading time to infect all potential infectable systems: minutes up to days
  - Spreading is exponential
  - Reaction must be initialized as early as possible
  - Early warning time: minutes up to days

Thread Scenarios (3/4)

- Botnet Communication
  - Idea: Eavesdrop the communication to react to actual threats
  - Early warning time is dependent on the communication speed of the botnet
  - Early warning time: Dependent on the botnet structure. Based on research results a few minutes
- Routing
  - Distribution of wrong prefixes in the routing system
  - Example: youtube route captured by Pakistani Telecom
  - Route information distributed in a few minutes in big part of the routing infrastructure

Thread Scenarios (4/4)

- Conclusions
  - In general very short early warning times
  - A warning before an started attack is impossible in most cases
  - Warning before potential threats is possible
  - Sometimes also problematical

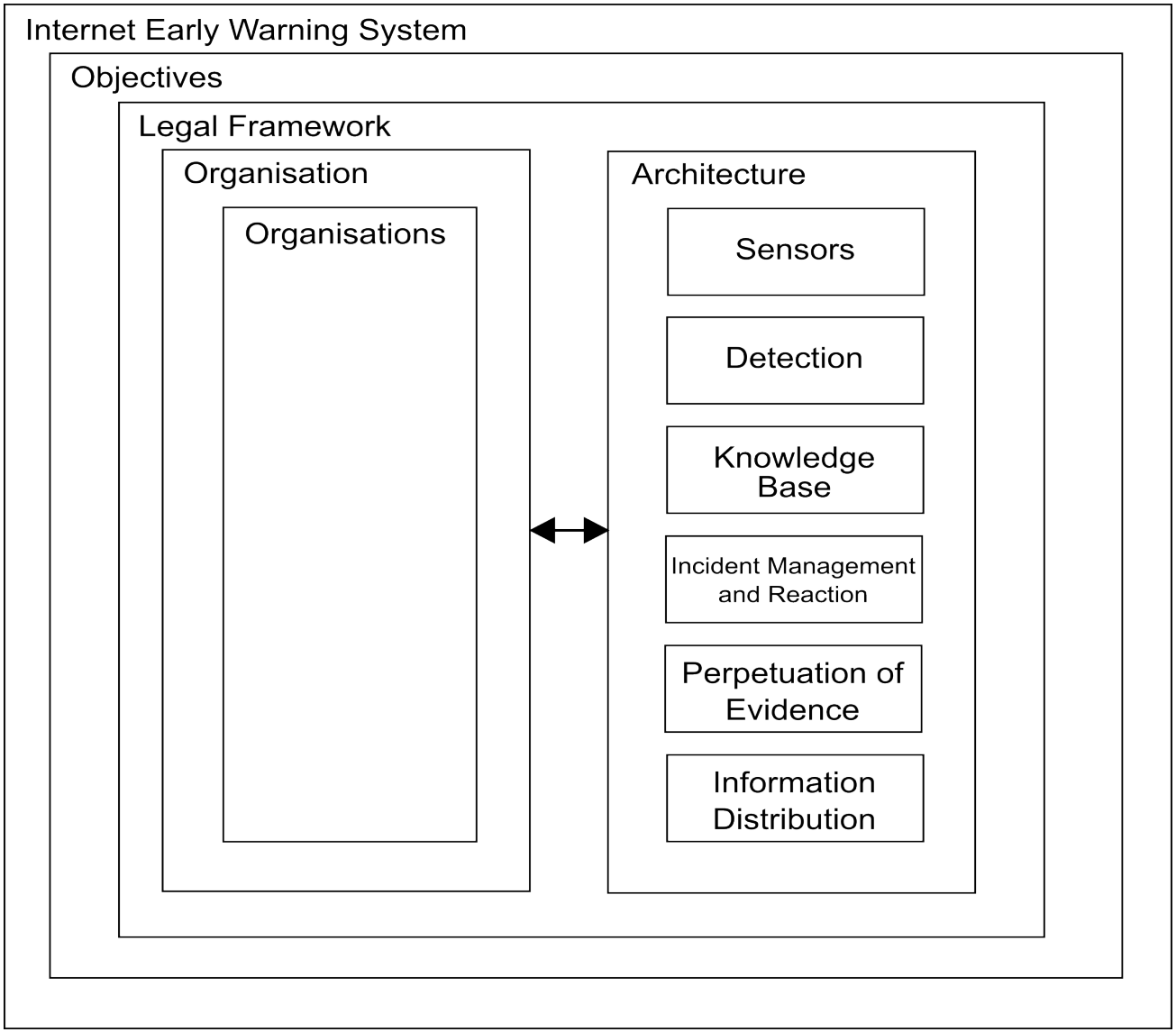
Agenda

- Introduction
- Thread Scenarios
- **Definition of an IEWS**
- Technical Components
- Architecture
- Conclusion

Definition of an IEWS (1/3)

- F = (N,P,O,L,G,C)
  - N := Network, that should be monitored
  - P := Organisations, that are part of the early warning system
  - O := Definition of the organisational structures and processes necessary to operate an early warning system
  - L := Legal framework, necessary for the operation of an early warning system
  - G := Objectives, that should be achieved by an early warning system
  - C := Technical components of an early warning system

Definition of an IEWS (2/3)



Definition of an IEWS (3/3)

- Not only technical components are relevant for the operation of an Internet Early Warning System
- The legal framework must allow the operation of an early warning system
- In most cases fast reaction is necessary, so the organisation must support fast reaction
  - Short decision making process
  - Efficient information distribution
  - Clearly defined responsibilities
- For an effective Internet Early Warning you need the right partners for
  - Sensor placement, reaction, ...

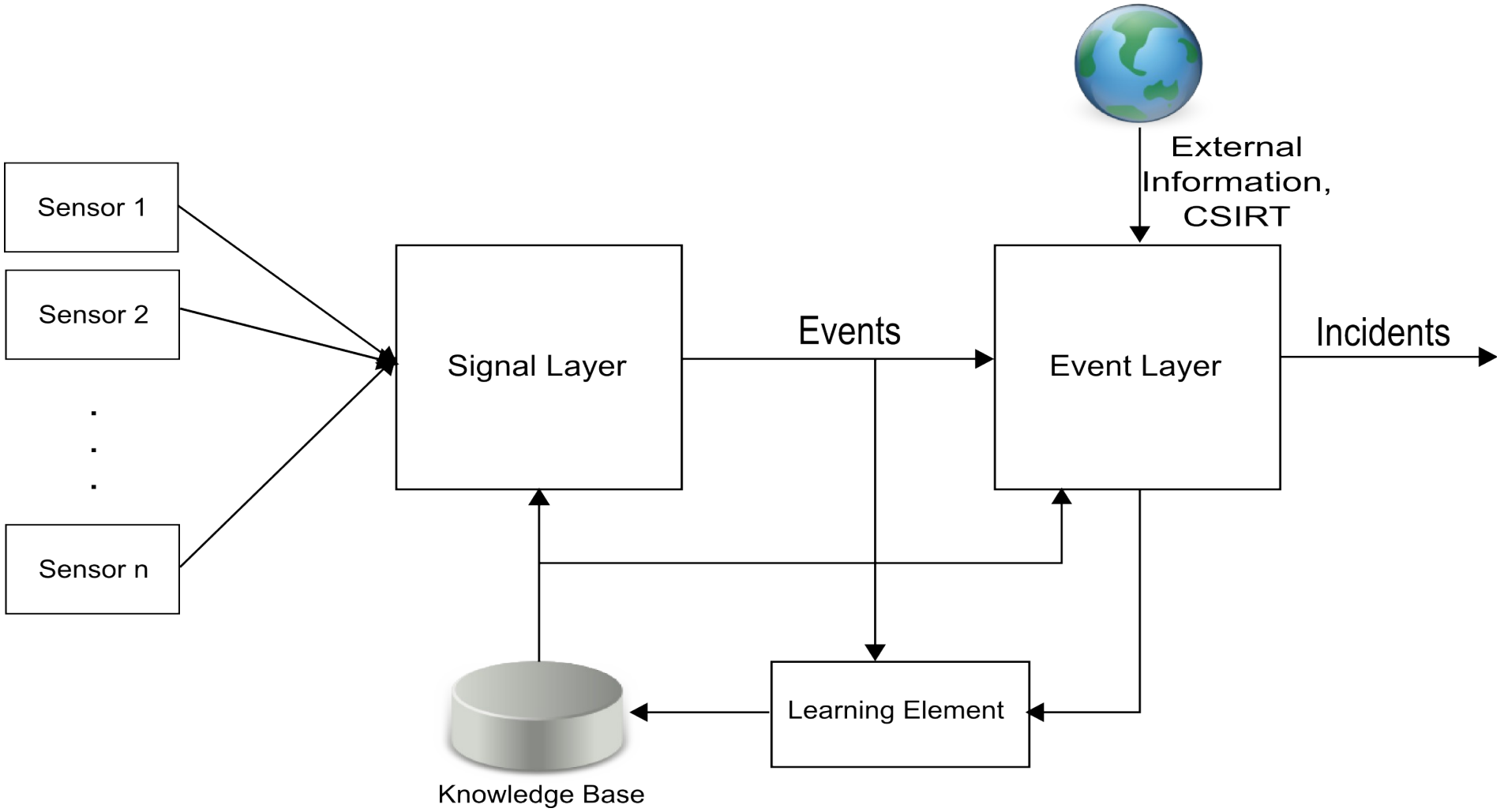
Agenda

- Introduction
- Thread Scenarios
- Definition of an IEWS
- **Technical Components**
- Architecture
- Conclusion

Technical Components (1/4)

- Sensor
  - Generate an overview of the actual situation
  - Identify new threats, e.g. malware spreading
  - Identify concrete attacks actual running
- Detection Component
  - Core of an early warning system
  - Detection of attacks, threats and prediction of incidents
  - Consists of a signal layer and an event layer
  - Uses external information and information taken from a knowledge base to identify threats or anormal behaviour

Technical Components (2/4)



Technical Components (3/4)

- Knowledge Base
  - Store different kind of knowledge, e.g. normal behaviour of the network, threat signatures, network structure, incidents and countermeasures
  - Must be updated on a regular basis
- Incident Management and Reaction
  - Expert system
  - Support of the user during processing of incidents
    - e.g. suggesting steps for further analysis, suggesting countermeasures
  - Connected to the Knowledge Base
  - Should react in most cases automatically

Technical Components (4/4)

- Perpetuation of Evidence
  - Needed for the criminal prosecution
  - Take evidence that an attack happened and who has started the attack
  - Access to data must be limited and should occur only in reasonable cases
- Information Distribution
  - Distribute information between the users of the Internet Early Warning System
  - e.g. warning/alerts, countermeasures, threat description, …
  - Must be fast and resilient

Agenda

- Introduction
- Thread Scenarios
- Definition of an IEWS
- Technical Components
- **Architecture**
- Conclusion

Architecture (1/5)
→ Important Aspects

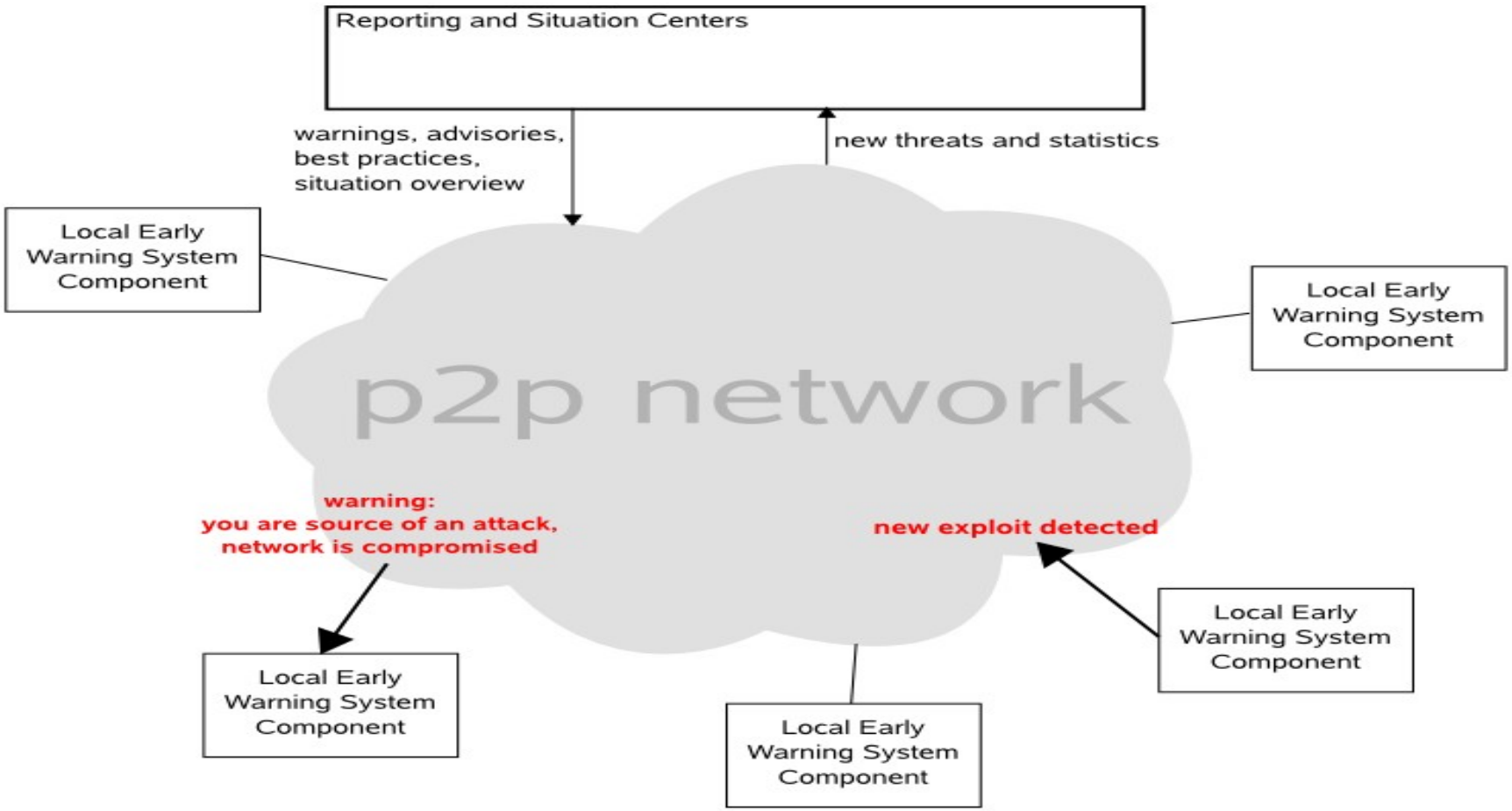
- Different policies at the local system for incident handling and initiation of countermeasures
- Different environmental conditions, so that not every countermeasure could be applied to every network
- Fast distribution of threat descriptions
- In future more use of cryptography, so that deep packet inspection is only usable at the endpoints of communication
- Different legal conditions at different countries
- An Internet Early Warning System should be resilient

=> Distributed architecture

Architecture (2/5)
→ Basic Components

- Core of the system are strong local security components
- These components are connected by an efficient information sharing network
  - Sharing information of threats and countermeasures
  - At the moment we analyse P2P-Structures for this purpose
- Situation center is a node in this network
  - Can build a global Situation Awareness
  - Can help by coordinating countermeasures

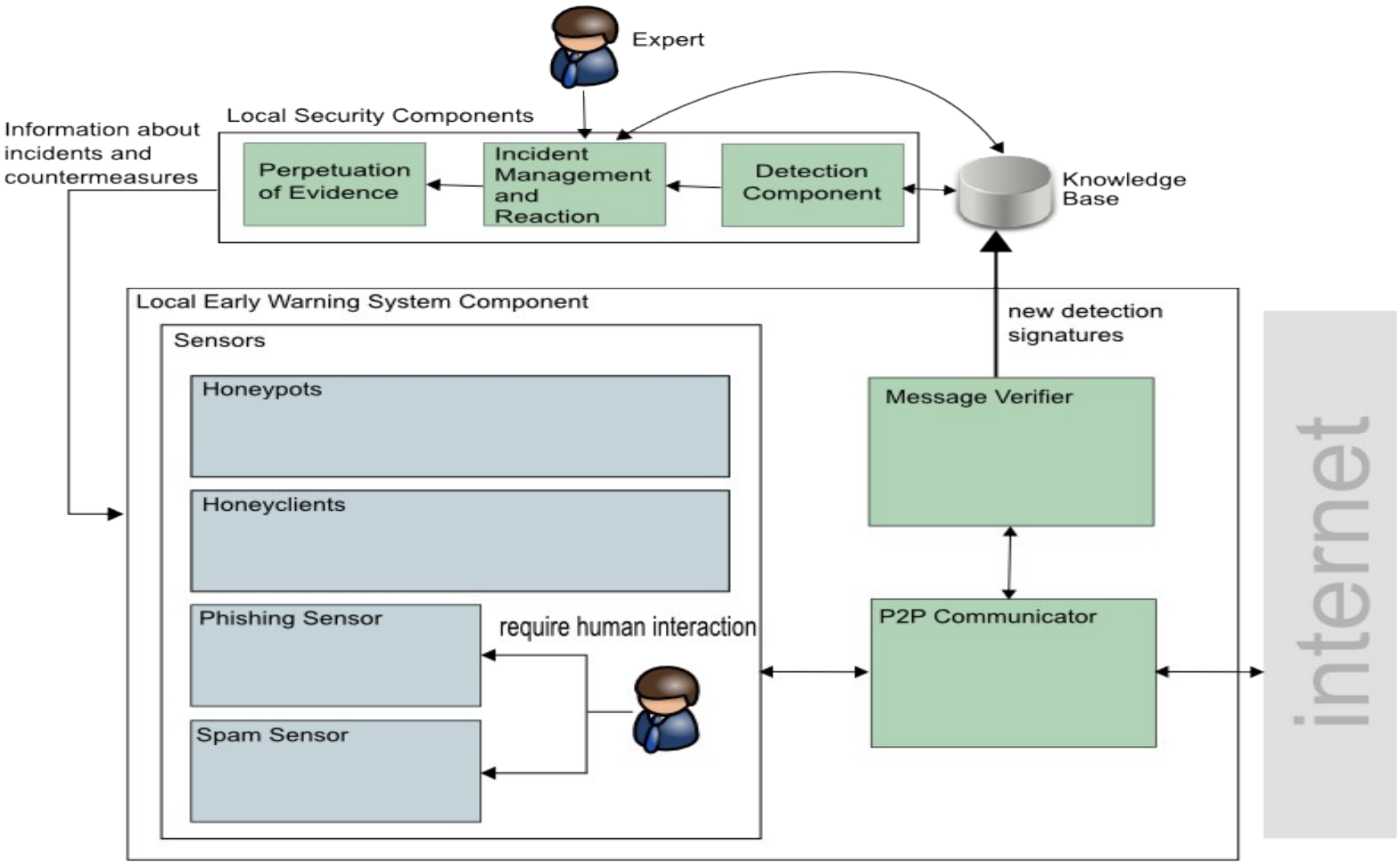
Architecture (3/5)
→ Information Sharing Network



Architecture (4/5)
→ Local Security Component

- Consists of the components mentioned before
  - Sensors, Detection, Knowledge Base, Pepetuation of evidence, Incident Management and Reaction
- Responsible for
  - Detection of attacks/anomalies
  - Generation of countermeasures
  - Identification of new threats
  - Distribution of information to other nodes of the Internet Early Warning System
- For this it uses
  - The local sensor information
  - The information of the Knowledge Base
  - The information from the Internet Early Warning System

Architecture (5/5)
→ Local Security Component



Agenda

- Introduction
- Threat Scenarios
- Definition of an IEWS
- Technical Components
- Architecture
- **Conclusion**

Conclusion (1/2)

- We proposed a definition for the terms Early Warning and Internet Early Warning System
- We have discussed different threat scenarios and analysed the possible early warning times
- In most cases an early warning before an attack is not possible
- We can only distribute warnings of possible threats
- An Internet Early Warning System is more than just its technical components
  - Organisational and legal aspects are also very important
  - To build an operational system the partners are also very important

Conclusion (2/2)

- Key components of an Internet Early Warning System are:
  - Local Security Components
  - Information Sharing Network
- Situation Center is a client of this network
- Next Steps
  - Analyse the usage of P2P-Structures for Information Sharing
  - Analyse the types of information that must be distributed in the network
  - Automatic generation of countermeasures

Fachhochschule Gelsenkirchen

Internet Early Warning Systems – Overview and Architecture

Thank you for your attention!

Questions ?

Mathias Deml
Sebastian Schmidt
Sascha Bastke

{deml,schmidt,bastke} (at) internet-sicherheit.de

Institute for Internet-Security
https://www.internet-sicherheit.de/en
University of Applied Sciences Gelsenkirchen

if(is) internet security.