Intelligent Agents – The New perspective Enhancing Network Security

Krystian Baniak

24 October 2007

Agenda

- Introduction
- Intelligent Agent Based Systems
- Agent Reinforced Reasoning
- Research description
- Law & ethics concerns
- Conclusions

Introduction

Internet is insecure environment that gives us false notion of anonymity

- Growing amount of global spam email
- New types of sophisticated threats
- Increasing number of users with low perception of Internet dangers
- Cyber terrorism and cyber crime

Cyber crime prevention in the Internet is not perfect

- Legislation discrepancies across country boundaries
- Standards as the only way to tackle cyber crime globally
- Developing countries do not have resources

Successful prevention requires global systematic approach!

Agent frameworks have proven its usability in data exploration and classification what can be leveraged in wider scope

Introduction:: Research motives

- Penetration testing and security posture assessments experience signals need for faster and more sophisticated reporting
- Knowledge mining techniques provide more adequate results when applied to the results of network penetration tests

Goal of the research

Design and implement agent based framework that leverages knowledge exploration techniques for network activity comprehension and artificial intelligence for detection and elimination of misusage.

1. Intelligent Agents

introduction into world of artificial agents

Intelligent Agent Based Systems

Why intelligent agents?

Agent: hardware or (more usually) software-based computer system

Intelligent Agent systems, as in the society, form a group and operate cooperatively in order to realize complex and distributed tasks.

- **Agents are meant to constantly perceive the surrounding environment, analyze it and react on it in order to satisfy its goals.**
- **Agents actively interact with the environment to pursue its goals**
- **Agents use reasoning techniques to represent and analyze the world in which they operate**
- **Artificial Intelligence is a science that studies the art of creating and designing intelligent agents systems in general.**

Intelligent Agent Based Systems

Intelligent Agent properties

Wooldridge and Jennings 1995

- Autonomous - mission oriented approach
- Social ability – works in groups, cooperatively
- Reactive – agents perceive and analyze the environment
- Proactive – can influence the environment

Agent types in terms of code migration

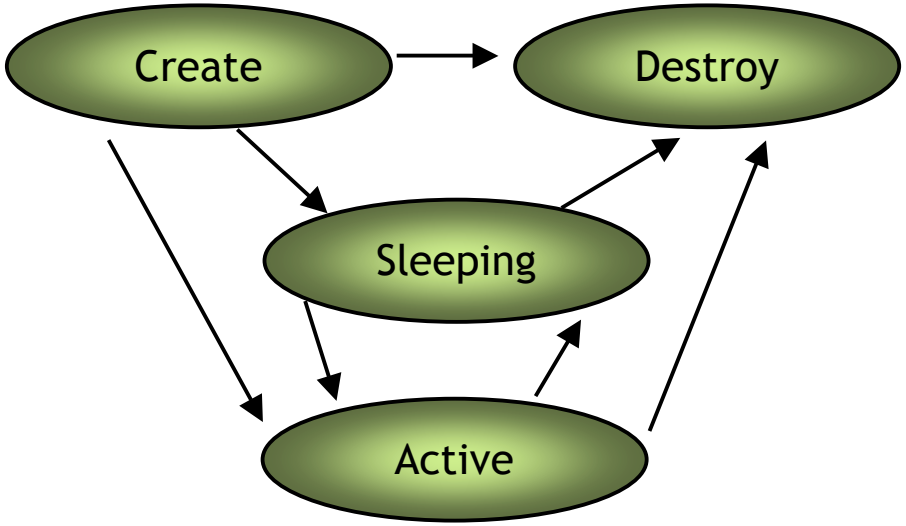
- Stationary – does not change execution environment
- Mobile – migrates across execution platforms

Agent depending on requirements can form hierarchical or flat structures

Agents can be unique or work in large sets

- MAS: Multiple Agent Systems

Agent's Life Cycle



- The transition between sleep and active state depends on environment
- Agent can be created on demand or perform long term action

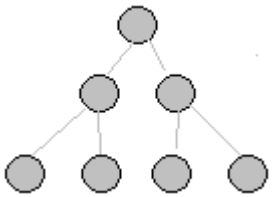
Intelligent Agent Based Systems

Types of problems that can be solved with help of intelligent agents

- Analysis of mass amounts of information
- Massively distributed environments
- Continual simple tasks on large number of data sets

EX Agents can filter information of our interest out of massive amount of false knowledge (like in IPS/IDS systems for example)

EX Agents can form hierarchical structures that enable use of different abstraction layers and methods of reasoning.



Intelligent Agent Based Systems

Properties of Intelligent Agent System: IAS

- Domain of exploration $\sum$
- Knowledge exploration technique $\Diamond$
- Knowledge representation ∂
- Reasoning method Δ
- Set of goals $\bullet$
- Accumulated knowledge Ω

$$IAS: < \sum, \Diamond, \partial, \Delta, \Omega, \bullet >$$

System uses reasoning on Ω to decide upon its actions in order to achieve goals $\bullet$

In particular system can manipulate the reasoning ruleset as the result of the learning process

Intelligent Agent Based Systems :: Problems

Problems and challenges for agents based systems

General class

- Representation of surrounding environment in symbolic logical notation aka ontology
- Selection of knowledge representation
- Reasoning technique

Prolog rule, term example:

```
man(Frank).
man(John).
parent(Fran,John).
father(X,Y):- parent(X,Y), man(Y).
```

Security class

- Security of communication
- Integrity of acquired knowledge and information
- Trust and reliability of agent

Examples of applications of the intelligent agent systems

- IDS/IPS systems with ability to adapt to given environment (monitoring agents)
- Creating profiles of users using information systems
  - Web query monitoring agents that create preference profiles (data mining agents)
- Distributed data mining to profile and correlate suspects in police databases
- Data mining systems that deliver knowledge about statistical parameters of various systems like library, e-bookstore, bank accounts usage, physical access control usage (biometrics, door locks)
- Agent systems that help tailor the system response according to your preference (personal agent)

Agents are applicable in transportation, logistics, graphics, GIS systems as well as in many other fields. It is widely being advocated to be used in networking and mobile technologies, to achieve automatic and dynamic load balancing, high scalability, and self healing networks.

(based on Wikipedia Multi-Agent Systems MAS definition)

2. Reasoning Methods

selecting agent reasoning method adequate for network

environments

Agent Reinforced Reasoning

Reasoning definition

Is a task that allows, in coherent way, prove newly acquired knowledge basing on so far accumulated knowledge.

Can be realized in many forms …

- Logical reasoning
  - Deduction
  - induction
- Via analogy, similarity
- Via examples
- other

What the knowledge really is?

Data → Information → Knowledge → Wisdom

Wisdom is not amenable to computer representation as it is strictly connected with human intelligence

We need knowledge representation to apply computer reinforced reasoning…

Agent Reinforced Reasoning

Knowledge Representation [J. Sowa]

Is a multidisciplinary subject that applies theories and techniques from three other fields:

1. Logic provides the formal structure and rules of inference
2. Ontology of application domain
3. Computation, which provides a concrete basis for applying philosophical precepts

Knowledge representation = < **DEFINITION_LANGUAGE, MANIPULATION_RULES**>

Agent Reinforced Reasoning

Why in the end we need knowledge representation?

- It is the surrogate of the real observed environment and enables resolving problem via reasoning not just via acting on input.
- It forms a set of rules of how to perceive the real world and how to deal with it
- It is essential for application of artificial intelligence

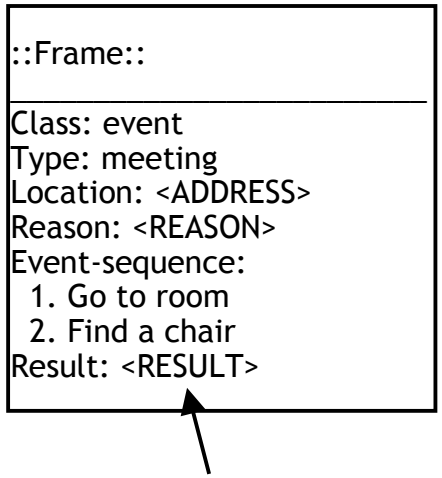
Problems and challenges

- Completeness, veracity and accuracy of representation model
- Quality
- Achievable effectiveness of reasoning
- Representation of dynamics (time, change, process)

Introducing the concept of "Frames"

First introduced by Marvin Minsky, MIT in 1975

- A "data structure" for representing a stereotyped situation.
- Part of frame describes the use case
- Other part describes the sequence of events.
- Frames are hierarchical and use inherence
- They contain slots which constitute the declarative part of the associated information
- Frames include inference mechanisms in their structure
- Frames van be easily applied to classify and represent behavioral models of analyzed individuals
  - Individual, whose actions comply with set of frames can be bound to the certain class
- Frames use similar concept as in Object Oriented languages



3. Research insights

Overview of the research details

Research description

Goals

Create agent based systems that will be able to:

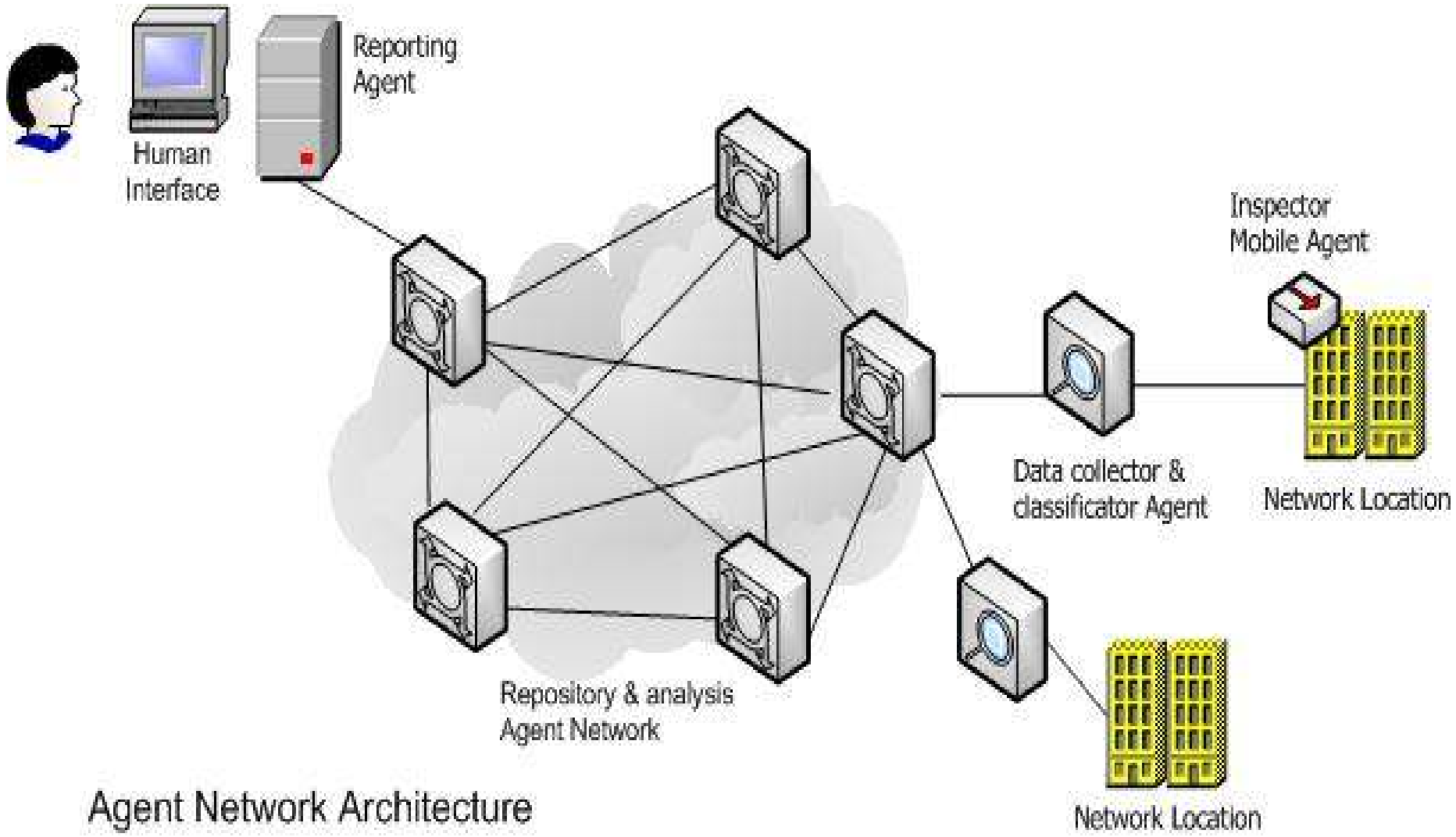
- Analyze network activity in order to create ontology of network behaviors
  - Create repository of network relater frames that will help classify network users into categories.
- Select and test knowledge representation methods
- Define good and bad behaviors and its patterns
- Profile network users as well as filter and trace wrongdoers
- Safeguard individual’s privacy and anonymity

Research description

Elements of the puzzle :: the architecture

- Three layers of abstraction and event aggregation
  - Network monitoring probes
  - Knowledge mining layer
  - Human interface and reporting layer
- Revocable anonymity system to conform to legal objectives
- Distributed architecture of sentinels enables for rudimentary filtering and tracking complex network scenarios

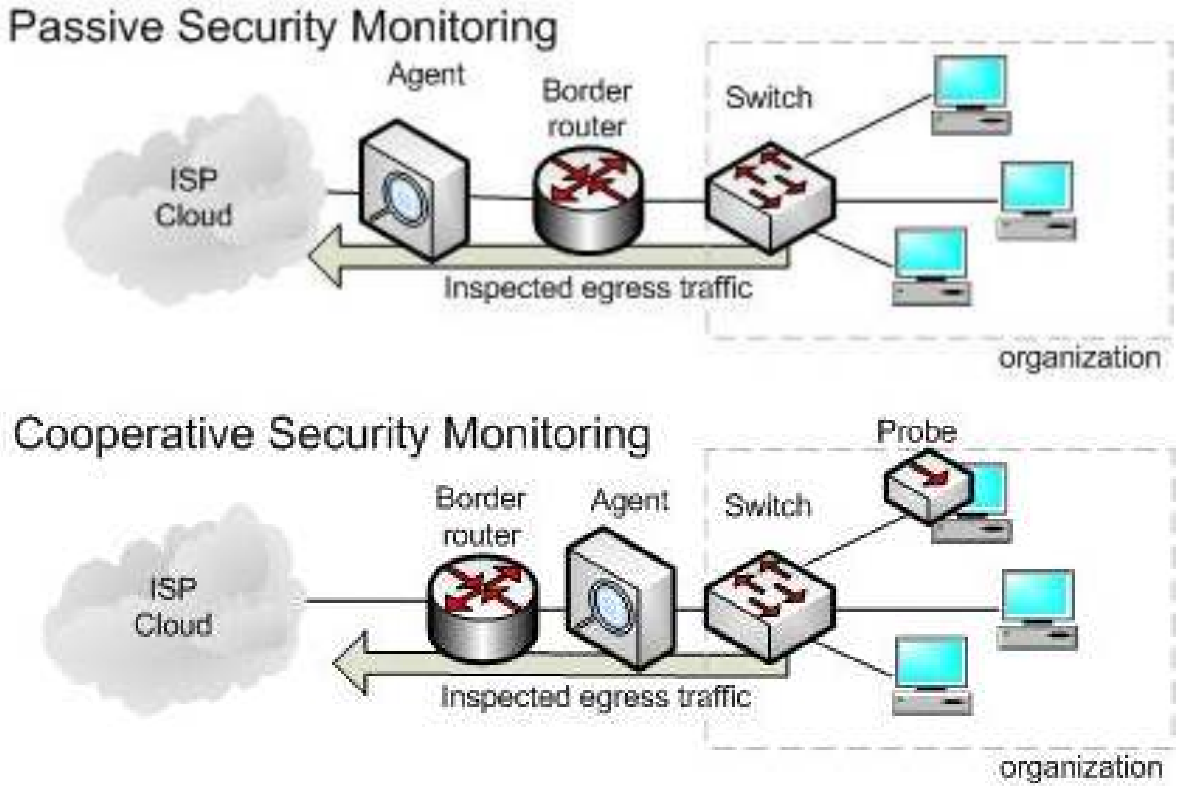
Research description



Agent Network Architecture

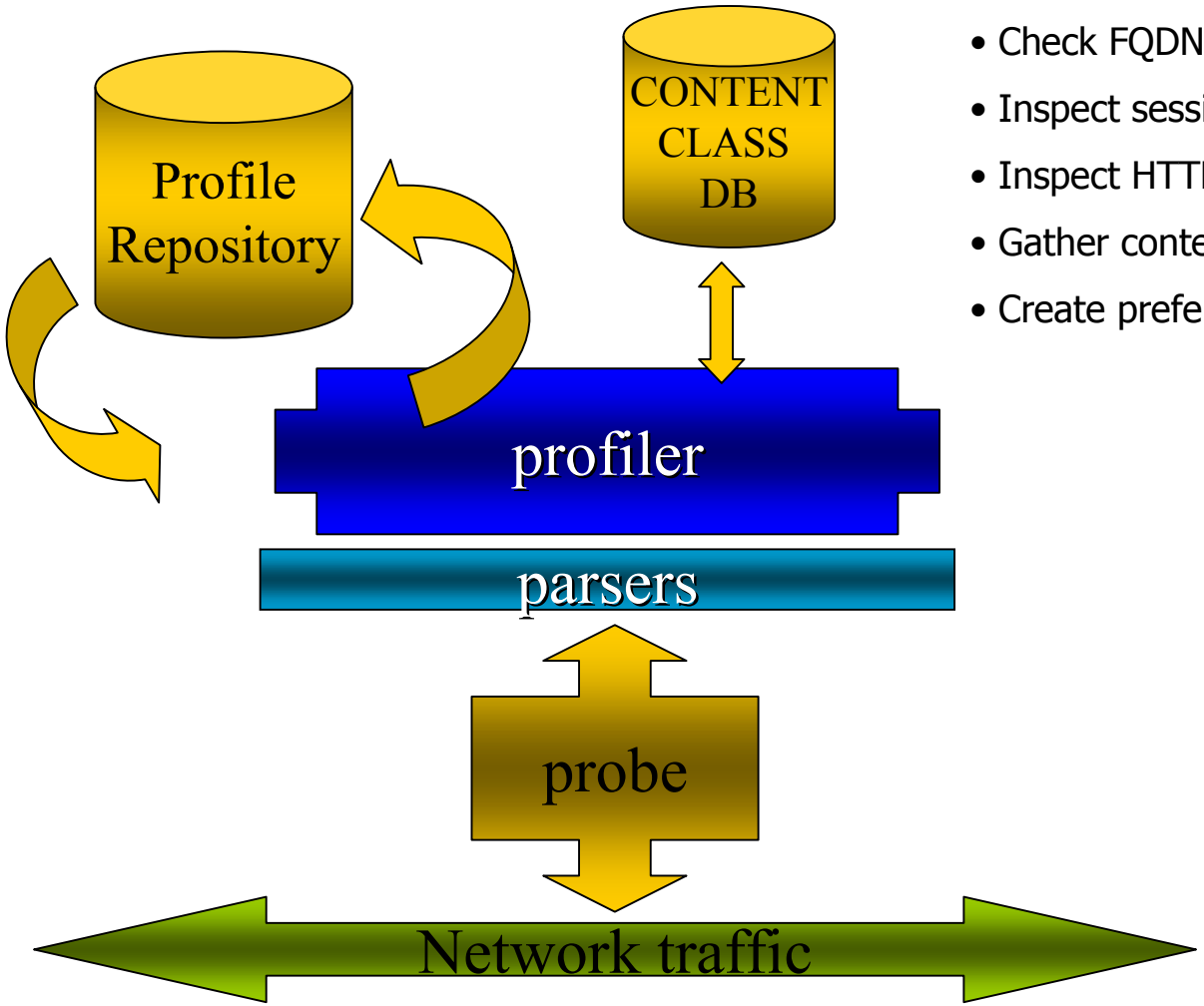
Research description

→ Modes of security probe operation depending on trust model



Research description

Data collector agent diagram



- Check IP address, Nationality
- Check FQDN, time of occurrence
- Inspect sessions, protocols
- Inspect HTTP queries and search engine sessions
- Gather content classification
- Create preference profile

Research description

Brief description of operational model

- Agent collector observes network traffic and produces profiles of all internal network nodes/users
- Profiles are compared against security behavior classes based on frame applicability analysis
- When user is considered to be a suspect agent collector starts gathering details about the user and evidence of the suspicious activity
- Both profiles and details are send for abstract layer for further analysis and correlation with data sent by other agent collectors.
- Abstract layer uses concepts of social nets analysis to find potential clique of users and analyze its properties.

Profiles are produced with help of set of classification tools that help to establish such parameters as:

- Distribution of destination's nationality, location, category, security level
- Time of occurrence and frequency

Research description

Security Aspects of the system

Security of inter-agent communication

- Based on Public Key Infrastructure and digital certificates.
- Confidentiality and integrity protected by use of Secure Sockets Layer (SSL) v3 and mutual certificate validation.

Security of agent's execution environment

- Secure and trusted platform is required – dedicated appliance

Research description

Achievements so far:

- Network probe is implemented with basic functionality that enables tracking TCP sessions and HTTP protocol usage. Probe does not gather PII for the moment.
- Abstraction layer agent is currently placed on the same platform as human interface module. It gathers and stores most important profiles and generates initial set of frames.
- Two networks (including part of university campus) are currently monitored (cooperative model)
- Security of inter-agent communication is implemented together with authorization model for system operators

4. Law & Ethics

Privacy and anonymity concern as encountered during the research

Law & ethics concerns

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks

Universal Declaration of Human Rights , December 1948, UN

- Growing system and network's complexity leads to more spending on monitoring and security analysis
- Global terrorism introduces dangerous precedents into controlling techniques
- Do public networks guarantee us our civil rights?
- How can we enhance monitoring tools?

Law & ethics concerns

Observation cannot affect Internet user's privacy

- US Electronic Communication Privacy Act ECPA
- EU OECD Guidelines (Organization for Economic Cooperation and Development)

International efforts toward cyber crime

- Mutual Legal Assistance Treaties (MLAT)
- Interpol (EU border control)
- UN Agreements

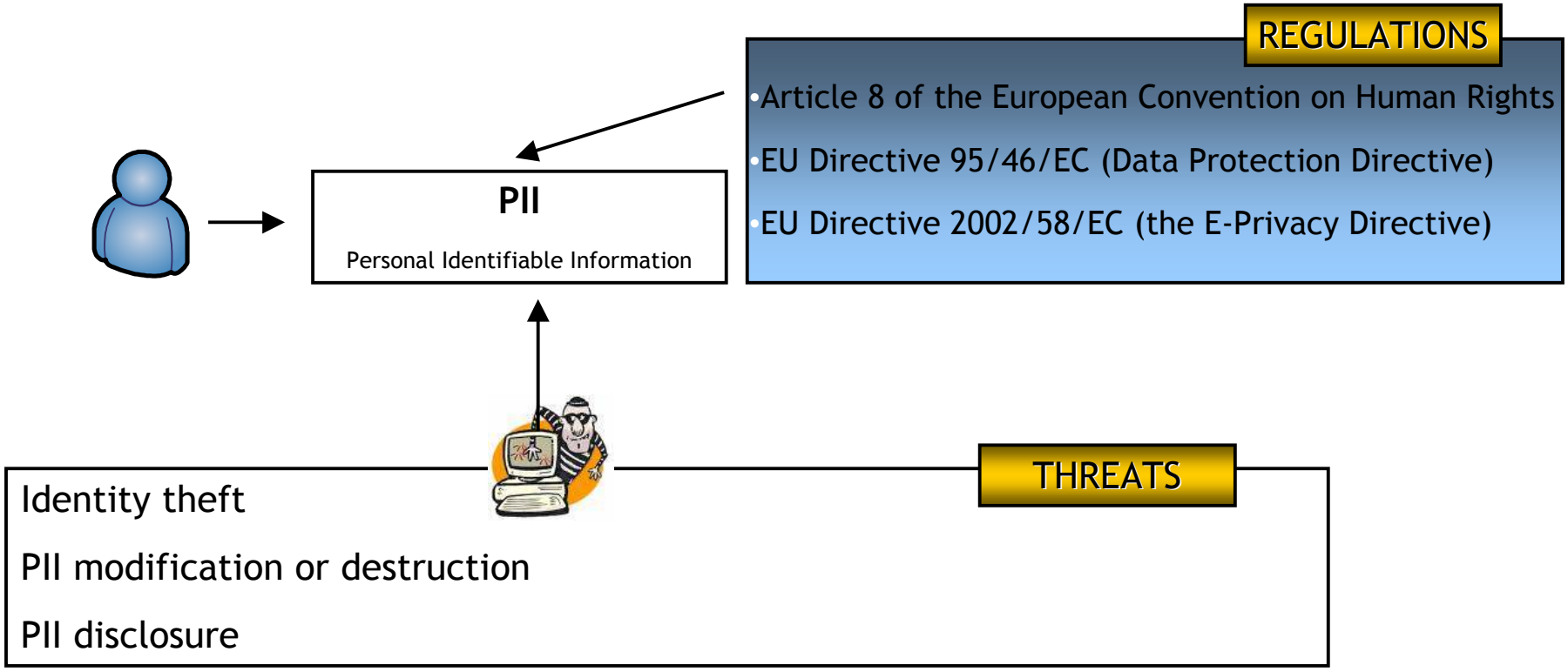
Agent platform requires global coverage to be successful – it has to be supported by law

- Acceptable evidence – hearsay rule
- Appropriate regulations – permit to gather information

Law & ethics concerns

Privacy – ability to keep our sensitive information secret and control time and extent of its disclosure.

Anonymity – state in which given element remains undistinguished among the set members

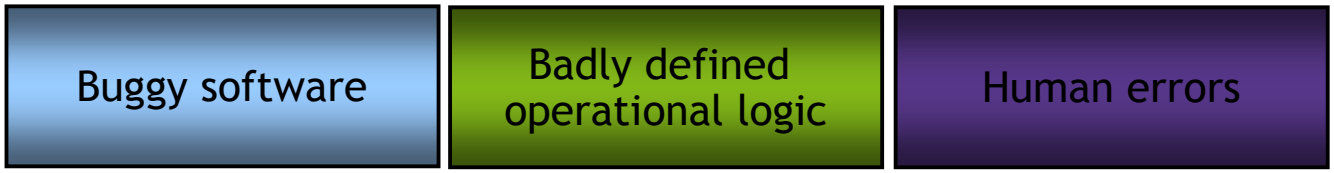


Law & ethics concerns

Technology poses a threat to privacy

- Technological means of payment and identification
- Personal data databases and repositories
- Access control system and fraud detection systems

Areas of the privacy threats



- Profiling systems manipulate PII to create models which are sets of sensitive information

Law & ethics concerns

What are the good properties of secure monitoring system?

- Anonymity of the individual is retain as long as possible. The revocation conditions must be connected with illegal aspects of individual behavior.
- Data acquired via monitoring systems has to be sufficient for correct indication of responsible individual. False positives can affect benevolent users!

Answer: revocable anonymity

Conclusions

→ Intelligent agents are advocated method of enhancing network security nowadays

→ Intelligent agents easily can offload humans from tedious inspection and analysis of complex network security problems

The key success factor is selection of appropriate knowledge representation and inference model that is the system that autonomously would learn and protect the network security.

This Is the subject of the research and space of growth of similar systems that unquestionably must appear in future to encompass rising complexity of security threats.

Thank you