Haruspex: ICT risk analysis with Monte Carlo method

Claudio Telmon
claudio@di.unipi.it

Trento, 12 March 2012

Harúspex

The simulator has been developed by the ICT risk and management research group at the Dipartimento di Informatica of the University of Pisa

- Prof. Fabrizio Baiardi
- Daniele Sgandurra*, Claudio Telmon, Gabriele Piga**

* IIT – CNR – Pisa

** Worked on the project for his thesis

Haruspex: Etruscan man practising a form of divination based on the inspection of the entrails of sacrificed animals.

haruspex@di.unipi.it

The problem

ICT security is a tool for operational risk management

- Focus is on intelligent threats (agents)

Risk is a function of impact and probability of adverse events

- With some simplifications, impact x probability

Impact can be estimated

- Or at least, estimation is inside the organization

What about the probability that a threat agent can successfully attack the system and cause that impact?

Too complex for a mathematical model

haruspex@di.unipi.it

Decomposing the problem

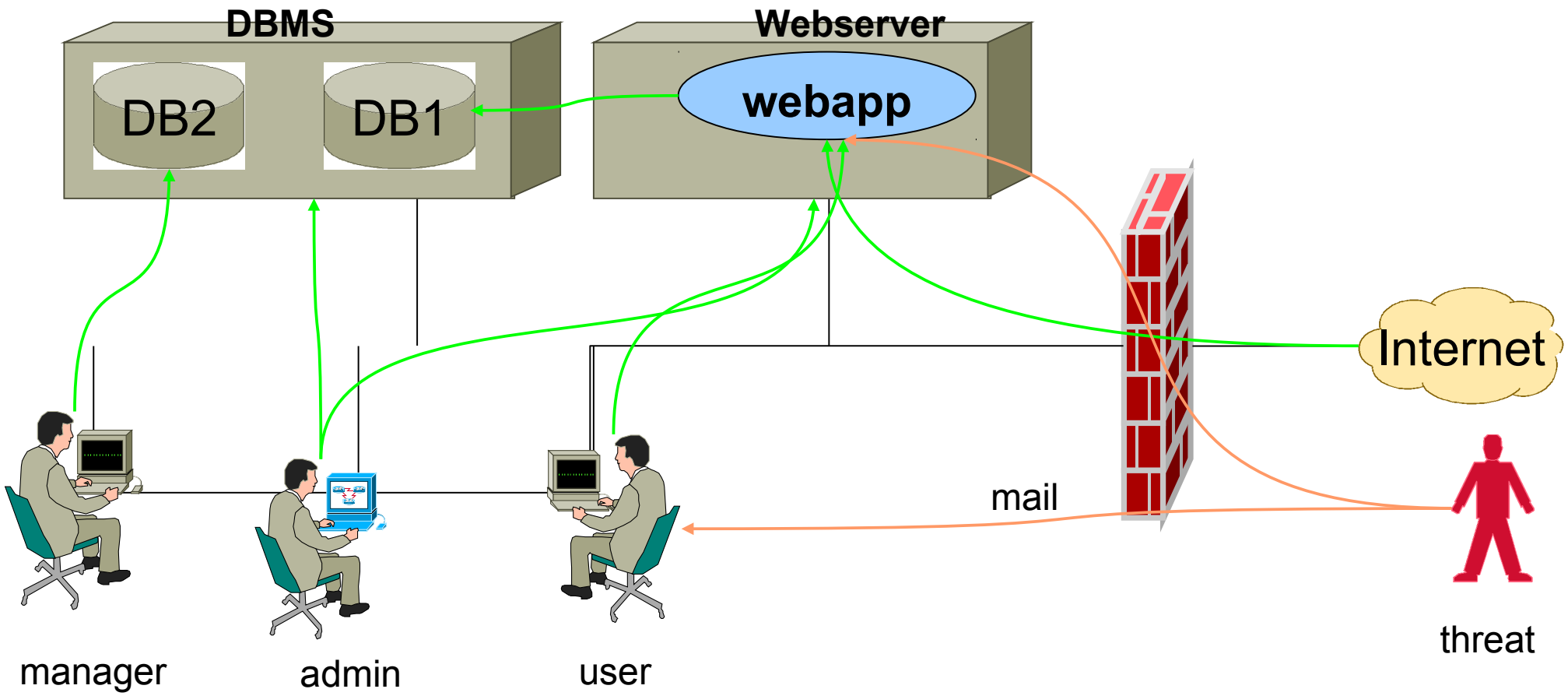
Probability of a complex (multi-step) attack:

- Threat (agent) properties
- Probability that the agent actually attempts the attack
- Discovery probability of every single vulnerability
- Ability of the threat to detect its goals in the system
- Ability of the threat to perform attacks
- Success probability of elementary attacks

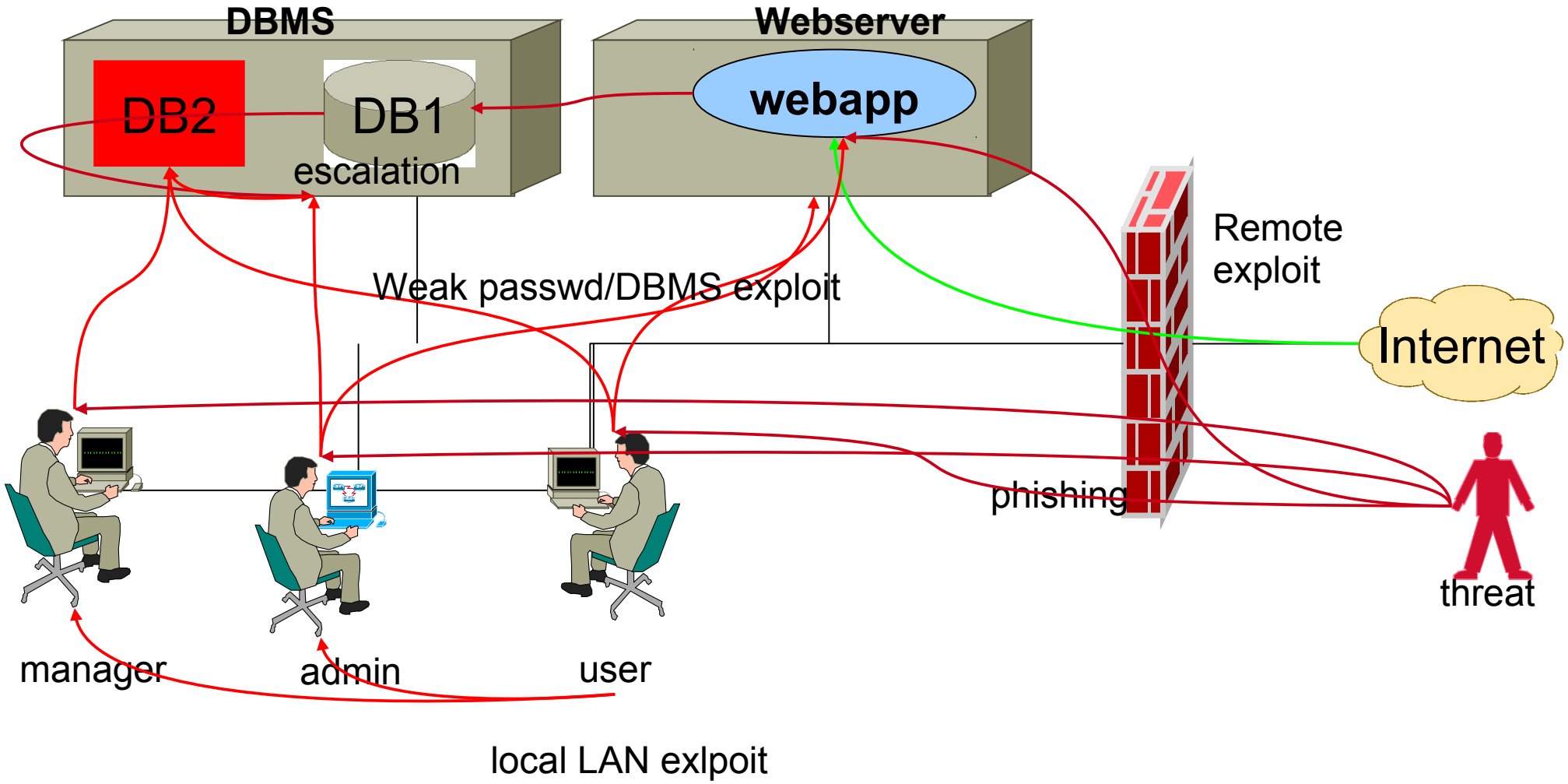
Can we deal with each of them separately?

haruspex@di.unipi.it

A simple system



Attacks


DBMS
Webserver
DB2
DB1
webapp
escalation
Weak passwd/DBMS exploit
Remote
exploit
Internet
phishing
threat
manager
admin
user
local LAN exlpoit

System representation

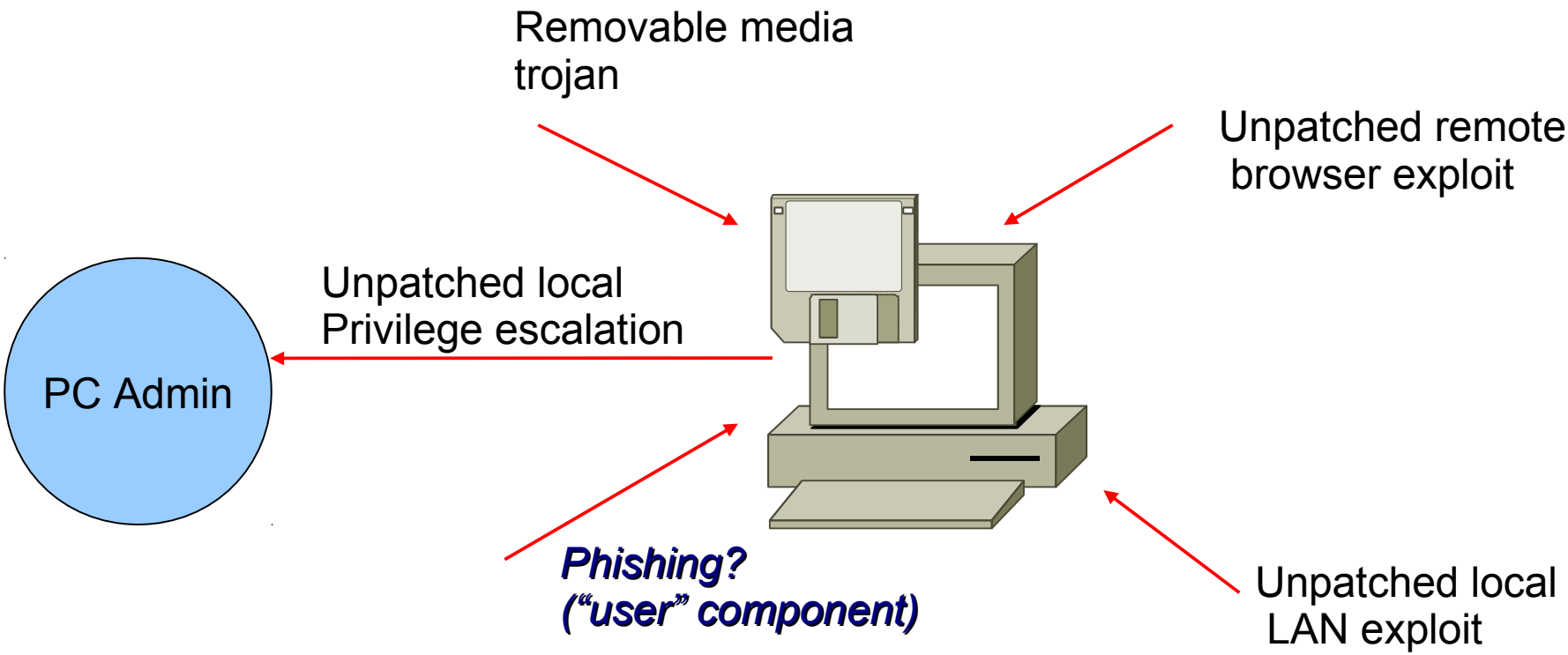
The system is represented as a set of interacting components

The analyst decides the detail level for the components

- Some subsystems may be represented as a single component, others may be very detailed
- We can start with a “high level” representation, and then detail the most critical/interesting subsystems

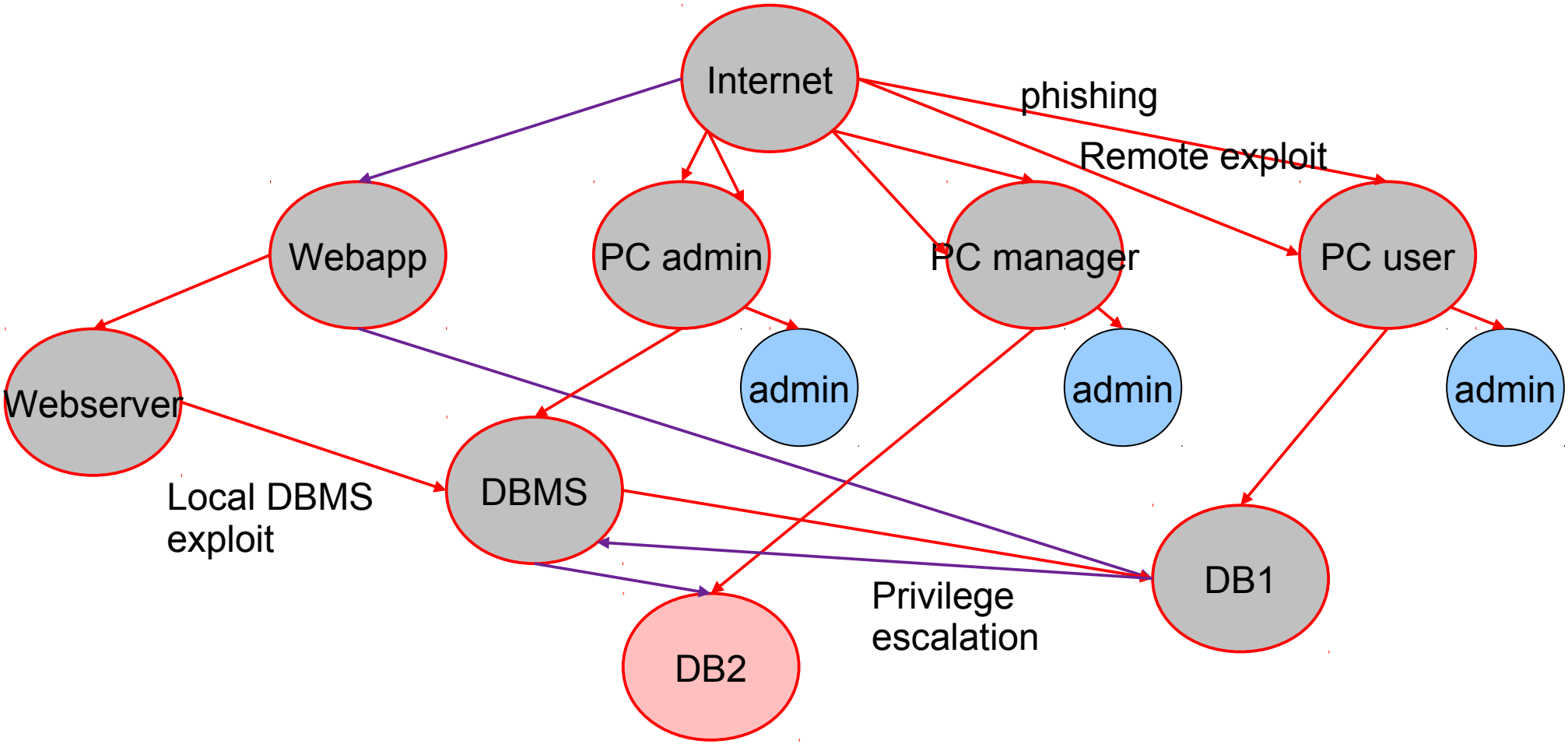
haruspex@di.unipi.it

Components, an example: a PC



e.g. every component connected to the LAN can be connected to "unpatched local LAN exploit"

Attack graph



haruspex@di.unipi.it

Use and limits of the attack graph

An attack graph shows everything that “can be done”

Including highly-improbable (non high-impact) attacks... we won't waste our money on them!

- … and we don't have all that money anyway

We associate probabilities:

- To the presence/discovery of vulnerabilities
- To attack success (e.g. password guessing, race conditions, version-dependant exploits...)

Probability: a “local” problem?

What is the probability that a vulnerability of a component is discovered **in a given time frame**?

- What is the probability (frequency) that a remote vulnerability is discovered in a Windows pc in the next six months? What is the “exposure window” before patching?
- Answer: statistics based on Microsoft security bulletins

There are answers to these (simpler) questions!

haruspex@di.unipi.it

Probabilities

Independent probabilities?

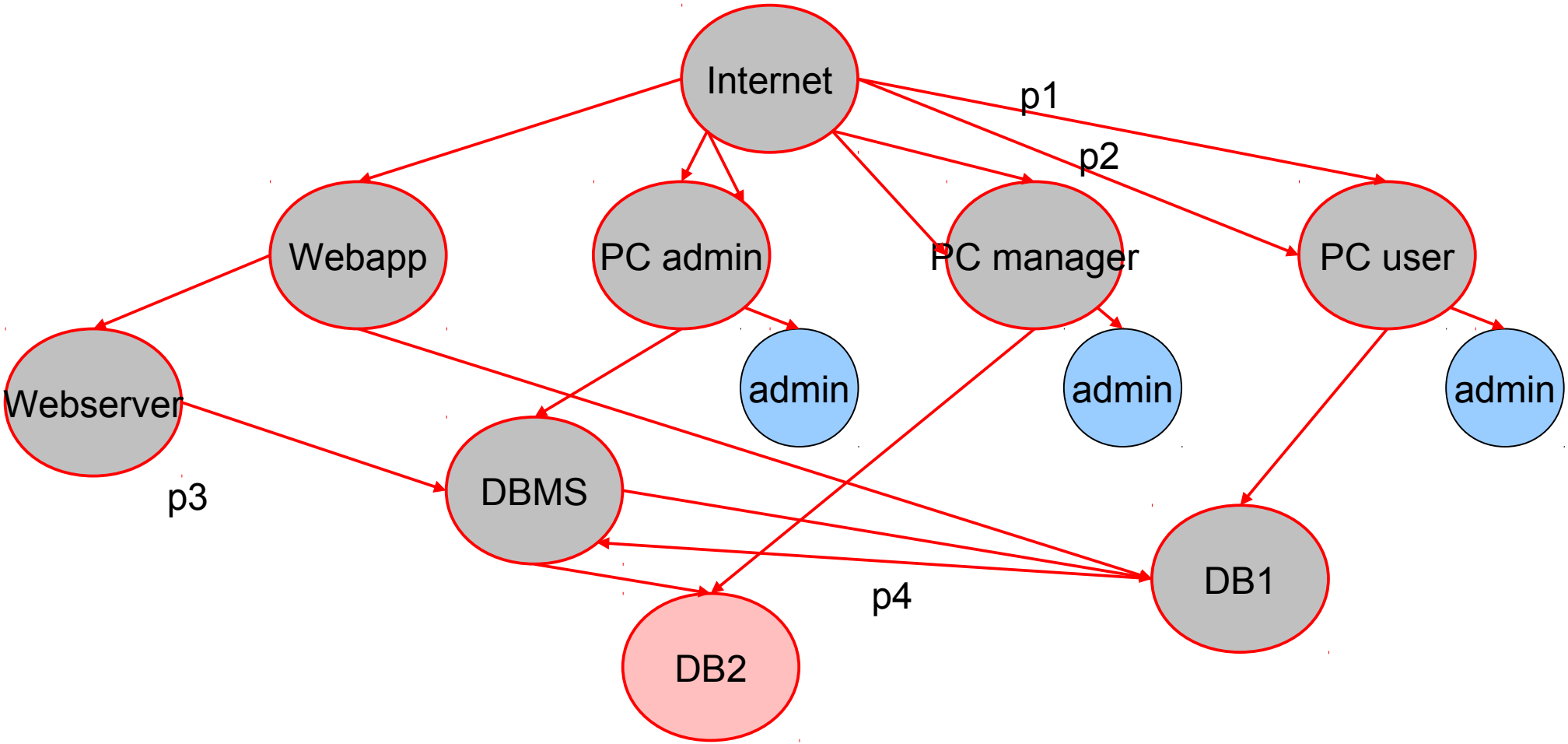
- Case 1: probability that a remote vulnerability is discovered in a Windows pc within the next six months
  - Evaluated through Microsoft bulletins
  - What if we have 1000 PCs? Not that much difference, probabilities are not independent!
- Case2: probability that a user is fooled by a phishing e-mail
  - Evaluated through in-house probing (e.g. during awareness rising programs)
  - What if we have 1000 users? A lot of difference... probabilities are mostly independent (however, users have usually the same awareness level)

Attacks:

- Probability for an attack to be successful, given the required competences and resources... depends on the threat and on the countermeasures

haruspex@di.unipi.it

With probabilities the attack graph gets more complicated...



No easy analytical solution

Threats have their own goals and strategies:

- Threats don't “see” the whole system, so they need a strategy
  - To suppose that threats know everything is a “worst case” that lets us spend more and worse
  - Threats goals are not (necessarily) the ones with the highest impact for the system

State transitions cannot be represented as a Markov chain, since the way a given status is reached influences the future behavior of the threat

Threats react to countermeasures by changing their plans

haruspex@di.unipi.it

Haruspex: let's enter the simulator

Monte Carlo method: several independent simulations of the system being attacked by threat agents

Input:

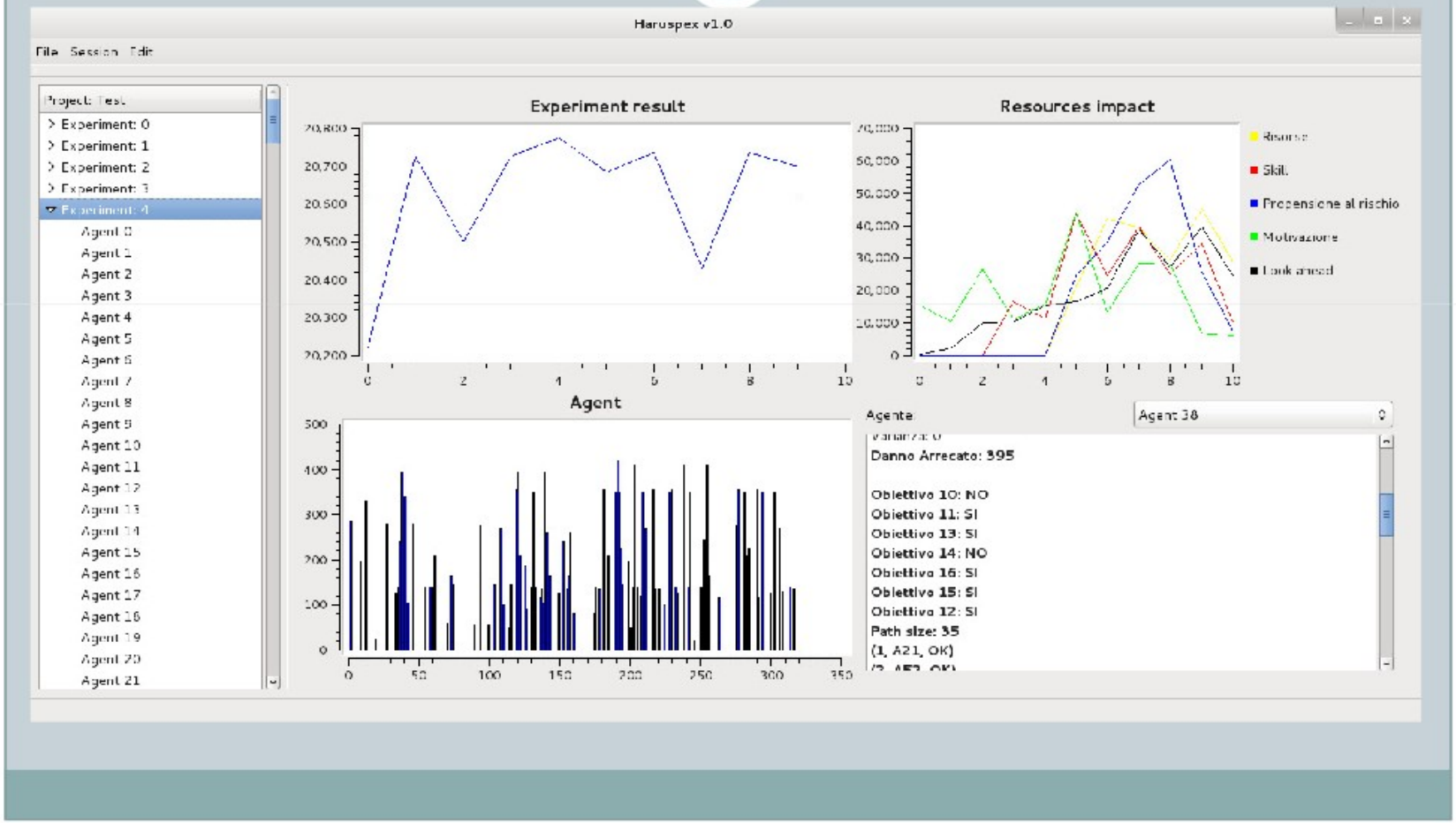
- A threat description (goals, starting privileges, resources...)
- A system decomposition
  - Components, rights...
  - Vulnerabilities and their probabilities
- Attacks
  - Vulnerabilities
  - Rights: preconditions and postconditions
  - Required resources
  - Success probability

A simulation

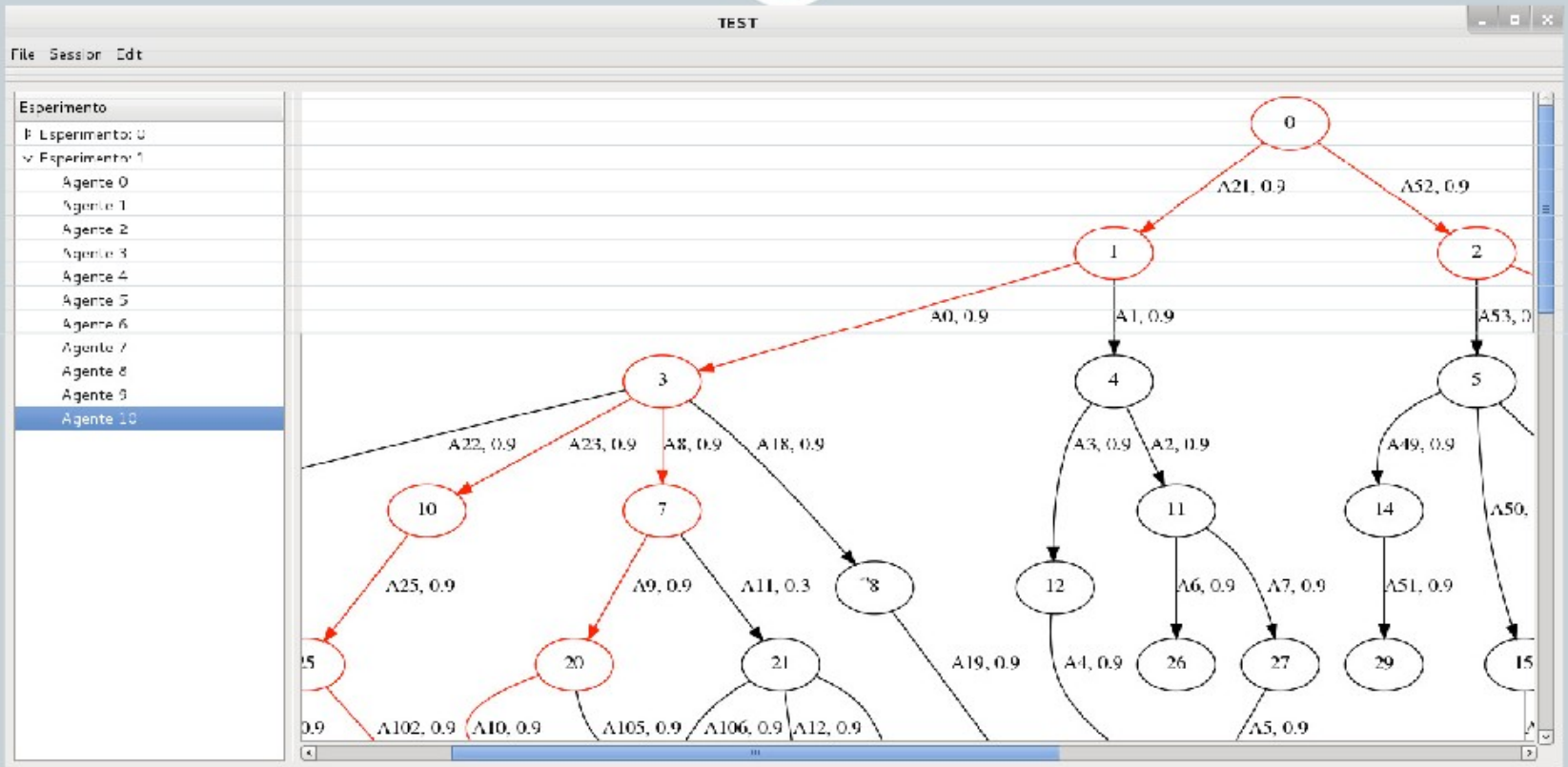
At every simulation step:

- Vulnerabilities can be discovered
- Threat agents can attempt some attacks
  - If they have the required resources and competences, and the required vulnerabilities have been discovered; attacks selection is based on strategies for reaching threat goals
  - If they succeed, threat agents gain new access rights that can be used in subsequent attacks
  - Whenever a threat reaches a goal, it causes an impact

Haruspex – Output



Haruspex - Output



Countermeasures

The ultimate goal of Haruspex is to help in the selection of countermeasures

A (technical) countermeasure can:

- decrease the existence/discovery probability for a vulnerability
  - e.g. better patch management or coding practices
- decrease the success probability for an attack
  - e.g. increase password quality, personnel training against phishing
- modify the system architecture
  - Introducing new security components, e.g. an IDS
  - Actually modifying the architecture, e.g. separating services on dedicated virtual machines

Selecting countermeasures

Haruspex provides the most probable attack paths in the system for a given set of strategies

We can use it for

- Selecting countermeasures, within budget constrains
- Prioritizing countermeasures, if we hope that we will have enough budget for a cut set of the attack graph (yeah, sure...)

After planning some countermeasures, a new simulation can be used to evaluate the effectiveness of the set

- Before actually spending the money
- Because threats adapt to countermeasures
- Countermeasures usually don't remove vulnerabilities, they decrease probabilities
- Adding countermeasures could increase the risk...

Other uses and issues

Sensibility analysis

- How relevant is a given parameter for the overall risk?
- How relevant is the evaluation of the probability of an attack for the overall risk?

Definition of “robustness” metrics for a system, both for design and for audit

Attack strategies evaluation

Evaluation of information availability for the threat

- Strategies may be more effective with a better knowledge of the system
- Insider vs. outsider, security trough obscurity

… and much more

- Output is collected in a database, so data mining and other types of analysis are possible

haruspex@di.unipi.it

Practical issues

Definition of component libraries

- Components with their vulnerabilities and typical probabilities for them

Vulnerabilities probability sharing within communities

- Easier than sharing information on the overall attack, easier to anonymize
- Less bound to specific properties (e.g. size, market) of an organization
    - More useful for different organizations
    - Easier definition of benchmarks

haruspex@di.unipi.it

Did we solve our problem?

Probability of a complex attack:

- Threat (agent) properties
- Probability that the agent actually attempts the attack
- Discovery probability of every single vulnerability
- Ability for the threat to detect its goals in the system
- Ability for the threat to perform attacks
- Success probability of elementary attacks

We can answer with a given confidence level to the question:

"If a threat with given strategy and resources attacks the system, what is the probability for it to reach its goals, and cause an impact?"

haruspex@di.unipi.it

Thank you!

haruspex@di.unipi.it