

The IPID project aims to provide tools for narrowing the gap between the operational and the strategic levels of security management in organizations. We tackle this challenge by addressing both the proactive (vulnerability assessment) and the reactive (intrusion detection) aspects of security, providing feedback that supports decision making.

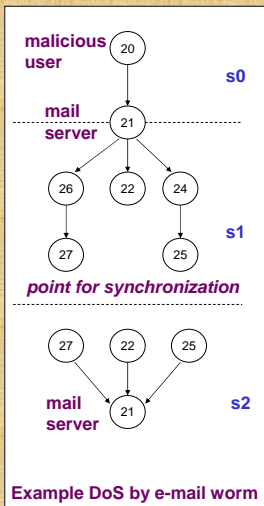
<http://ipid.ewi.utwente.nl>

## Proactive security

### Problem:

- Network vulnerabilities which involve synchronism, concurrency and simultaneity are hard to simulate and model. Thus, it is difficult to determine proactively if a network is subject to these risks.
- In this category of vulnerabilities are several types of Denial of Service (DoS), coordinated distributed attacks, distributed phishing attacks, cyber 9-11 attack, among others.
- A network may involve a Local Area Network, the Internet, a social network, or a computer grid.

```
CSP = Seq [
  s0 Arc(20,21),
  s1 Par [ Seq [ Arc(21,26),Arc(26,27) ],
           Arc(21,22),
           Seq [ Arc(21,24),Arc(24,25) ] ],
  s2 Par [ Arc(27,21),
           Arc(22,21),
           Arc(25,21) ] ]
```



Example DoS by e-mail worm

DoS characteristics: parallelism, synchronization and target sharing  
[franqueirav@ewi.utwente.nl](mailto:franqueirav@ewi.utwente.nl)

DoS by e-mail worm attack specification

## CSP attack specifications

### Solution:

- An algorithm that learns attack specifications from a network graph by minimizing the cost attached to arcs and maximizing the added value of a set of nodes.
- The output attack specifications are represented in a fragment of Hoare's CSP (Communicating Sequential Processes) language, used for the specification of parallel programming.

### Results:

- The approach is currently under evaluation for known attacks.

## Reactive security

### Problem:

- False positives (i.e. false alerts) form an universal problem for both signature and anomaly-based Network Intrusion Detection Systems.
- Current solutions support only signature-based systems and rely either on the human expertise or on semi-automatic assessments, which are not feasible approaches.

### Solution:

- A successful attack often causes an anomaly in the normal output of the attacked system (e.g. SQL Injection, Cross-site Scripting).
- Detecting anomalies in the outgoing traffic and correlating them with the alerts produced by a NIDS (be it signature or anomaly-based) monitoring incoming traffic improves the detection accuracy.

### Results:

- Improves significantly (50% - 100%) the accuracy of both signature and anomaly-based NIDSs analyzing incoming traffic, operating in a completely automatic way.

[damiano.bolzoni@utwente.nl](mailto:damiano.bolzoni@utwente.nl)

## APHRODITE: an Architecture for False Positive Reduction

