

Using Rule-Based Activity Descriptions to Evaluate Intrusion-Detection Systems

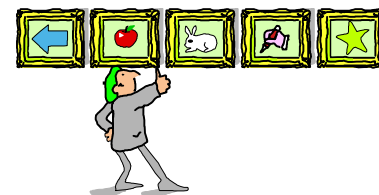
An Approach

Dominique Alessandri
IBM Research Laboratory Zurich, Switzerland

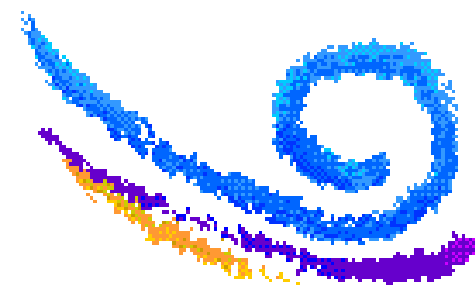
`dal@zurich.ibm.com`

October 2000

Overview



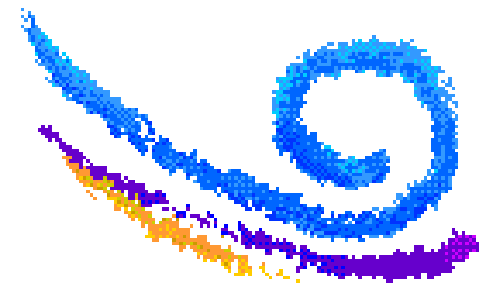
- ▶ Introduction
 - Motivation, Goals and Approach
- ▶ Description of IDSes (capabilities)
 - IDS engine, Information source, IDS configuration
- ▶ Activities
 - Malicious vs. non-malicious
 - Activity Groups, Activity Variations
- ▶ Conclusion



Motivation



- ▶ **IDS failures (False positives and false negatives)**
Generic sensors generate many false positives
 - Similarities between attacks and normal activities
 - Implementation faults
 - Tradeoff functionality vs. performance
- ▶ **Limitations of testing (High diversity of IDSes, Influence of test environment / static setup, Difficulty of IDS testing)**
- ▶ **Combining (lightweight) sensors**
 - Strengths and weaknesses of a sensor
 - Characteristics of a sensor

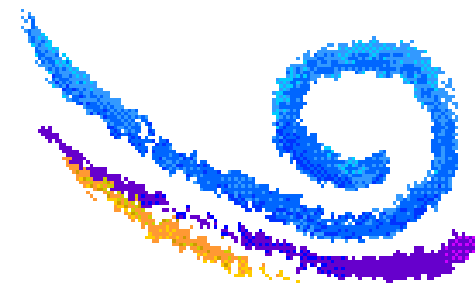


Goals



- ▶ Evaluate IDSes with respect to false positives and false negatives based on a representative set of activities.
- ▶ Evaluate how IDSes can be combined to reduce the overall rate of false positives and false negatives.

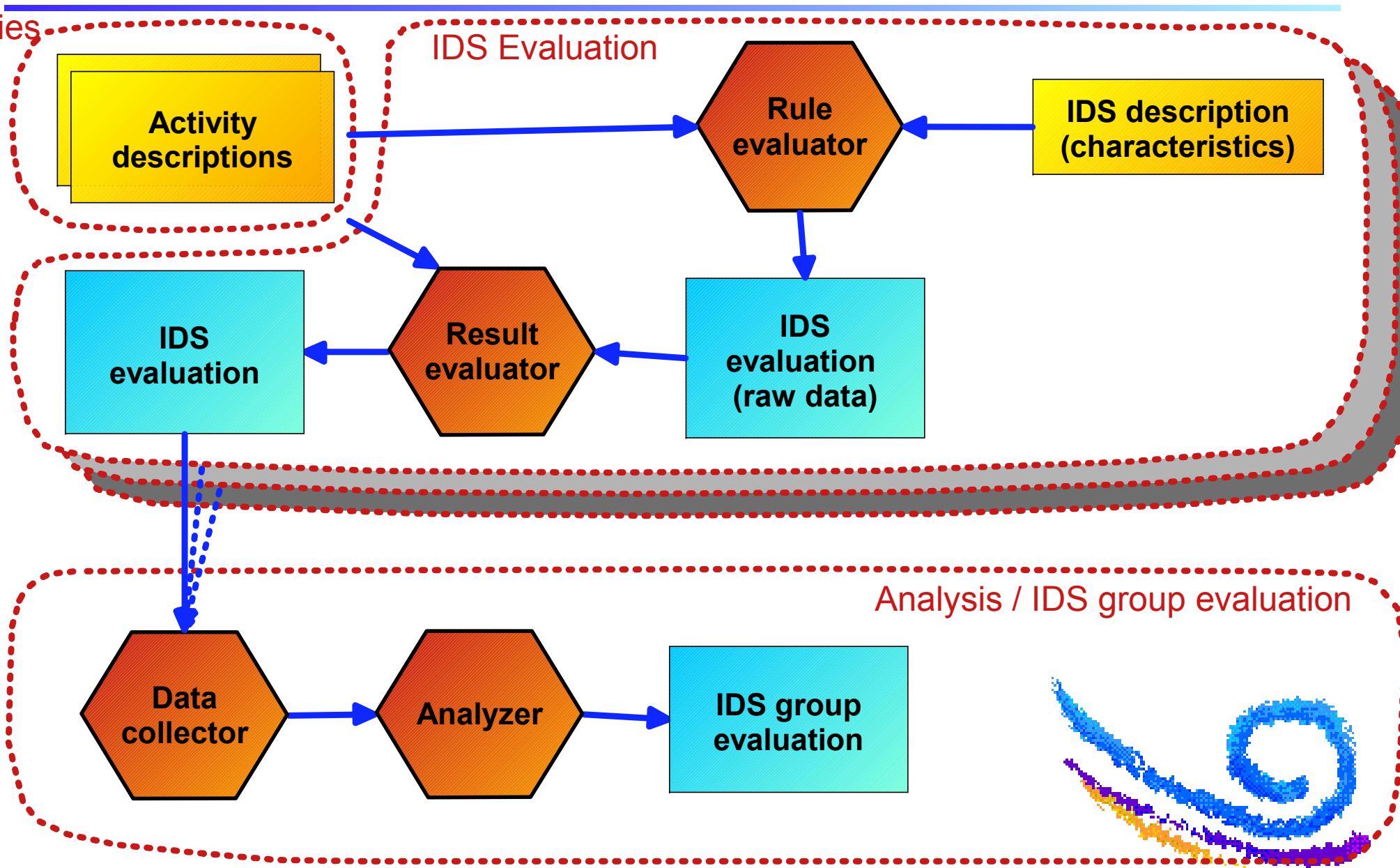
Evaluation of an IDS: Reproducible analysis of the results generated by an IDS for a given set of input data (i.e. activities) with respect to failure (i.e. false positives and false negatives).



Approach



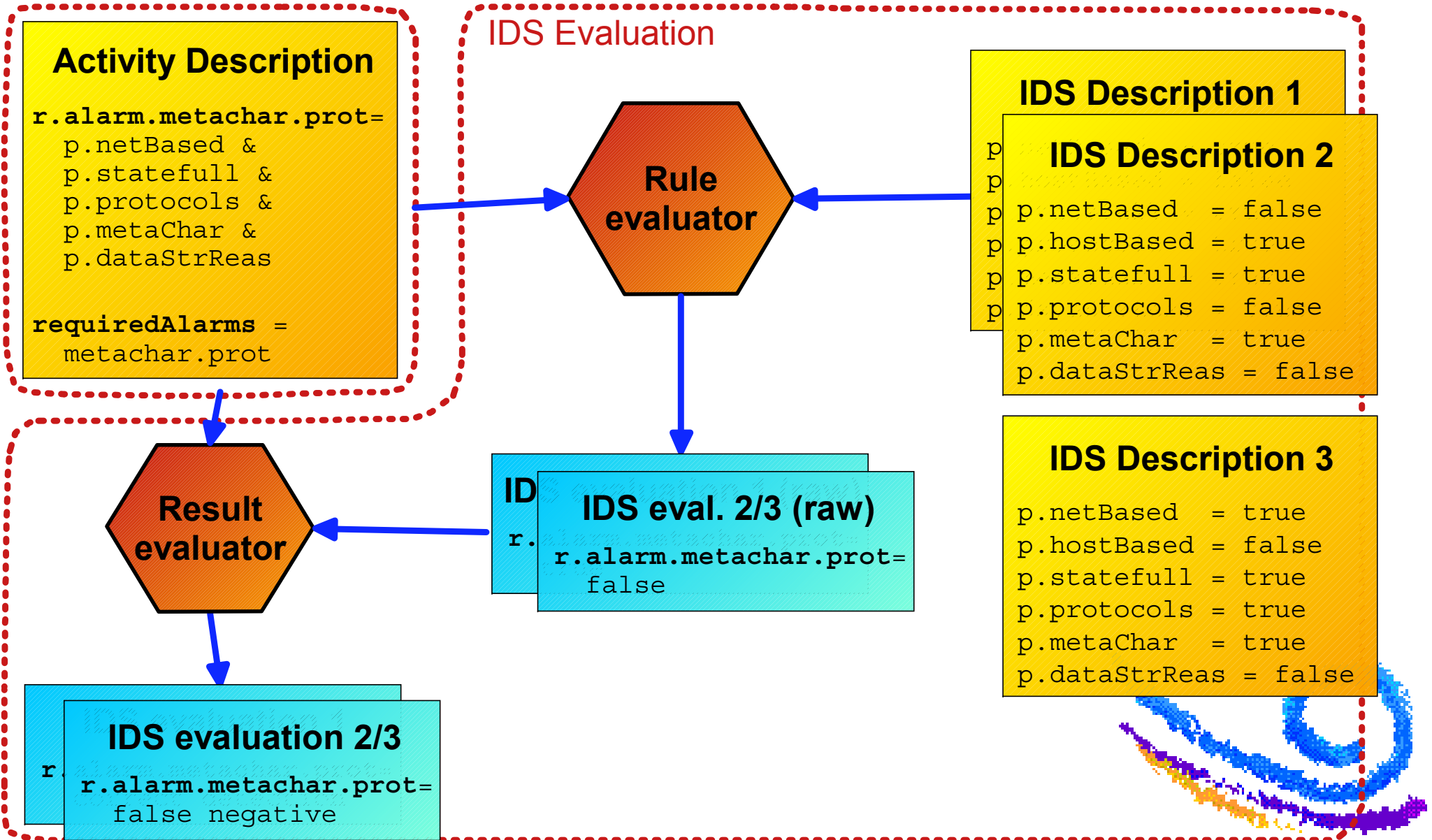
activities



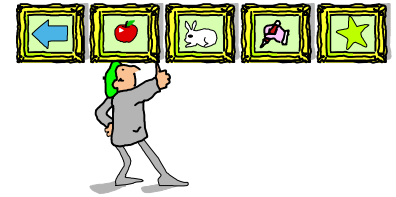
Approach



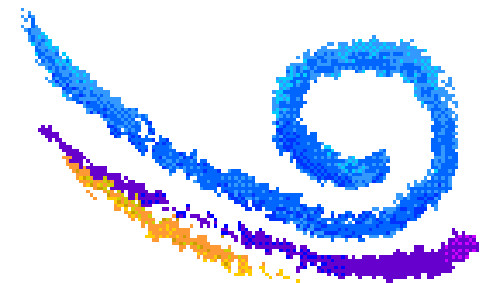
Activities



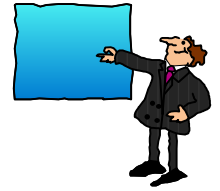
Overview



- ▶ Introduction
 - Motivation, Goals and Approach
- ▶ Description of IDSes (capabilities)
 - IDS engine, Information source, IDS configuration
- ▶ Activities
 - Malicious vs. non-malicious
 - Activity Groups, Activity Variations
- ▶ Conclusion



Description



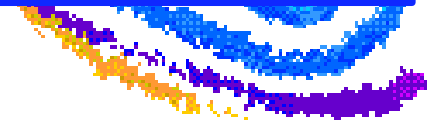
| Example (subset) | Proc. | App. Layer | Trsp. Layer (cnx) | Trsp. Layer (no cnx) |
|---------------------------------------|-------|------------|-------------------|----------------------|
| Multi-instance (aware) | Green | Blue | | |
| Multi-instance (inter-instance logic) | | | | |
| Multi-part (first) | Green | Blue | Blue | Blue |
| Multi-part (all) | Green | Blue | Blue | Blue |
| Multi-part (inter-part aware) | | | Blue | Blue |
| Multi-part (inter-part logic) | | | Blue | Blue |
| Pattern recognition (string matching) | | Blue | | |
| Pattern recognition (regexp) | | Blue | | |

IDS Description

ID Engine Capabilities

Properties


IDS Configuration



IDS Description - Capabilities

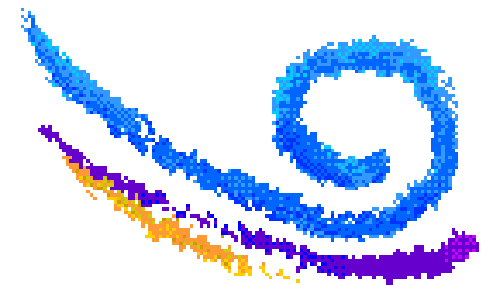
| | Host | User | OS core | Dev. | File sys. | Proc. | MW | App. Layer | Trsp. Layer (cnx) | Trsp. Layer (no cnx) | Netw. Layer (cnx) | Netw. Layer (no cnx) | Link Layer (LLC) | Link Layer (MAC) |
|---------------------------------------|---|---|---------|------|-----------|----------------|----|-------------------|-------------------|----------------------|-------------------|----------------------|------------------|-------------------|
| Logic verification (awareness) | Not applicable | Not applicable | | | | | | Network based IDS | Network based IDS | Network based IDS | | Network based IDS | | Network based IDS |
| Logic verification (control only) | Not applicable | Not applicable | | | | | | Network based IDS | Network based IDS | Network based IDS | | Network based IDS | | Network based IDS |
| Logic verification (complete) | Not applicable | Not applicable | | | | | | Network based IDS | Network based IDS | Network based IDS | | Network based IDS | | Network based IDS |
| Multi-instance (aware) | Host-based IDS | Host-based IDS | | | | Host-based IDS | | Network based IDS | | | | | | |
| Multi-instance (inter-instance logic) | | | | | | | | | | | | | | |
| Multi-part (first) | Host-based IDS | Overlap of network based and host-based IDS | | | | | | Network based IDS | Network based IDS | Network based IDS | | Network based IDS | | |
| Multi-part (all) | Host-based IDS | Overlap of network based and host-based IDS | | | | | | Network based IDS | Network based IDS | Network based IDS | | Network based IDS | | |
| Multi-part (inter-part aware) | | | | | | | | | Network based IDS | Network based IDS | | Network based IDS | | |
| Multi-part (inter-part logic) | | | | | | | | | Network based IDS | Network based IDS | | Network based IDS | | |
| Bi-directional (aware) | | | | | | | | Network based IDS | Network based IDS | Network based IDS | | | | |
| Bi-directional (logic) | | | | | | | | Network based IDS | Network based IDS | Network based IDS | | | | |
| Bi-directional (fully statefull) | | | | | | | | | | | | | | |
| Statistics (periodicity) | | | | | | | | Network based IDS | Network based IDS | Network based IDS | | | | |
| Statistics (intensity) | Overlap of network based and host-based IDS | Host-based IDS | | | | | | Network based IDS | Network based IDS | Network based IDS | | | | |
| Statistics (categorical) | Host-based IDS | Host-based IDS | | | | | | | | | | | | |
| Statistics (ordinal) | Host-based IDS | Host-based IDS | | | | | | | | | | | | |
| Learning (statistics) | | | | | | | | | | | | | | |
| Learning (sequence) | | | | | | | | | | | | | | |
| Data normalization | | | | | | | | Network based IDS | | | | | | |
| Pattern recognition (string matching) | | | | | | | | Network based IDS | | | | | | |
| Pattern recognition (regexp) | | | | | | | | Network based IDS | | | | | | |
| Length | | | | | | | | Network based IDS | | | | | | |
| Decryption | Not applicable | Not applicable | | | | | | | | | | | | |

 Network based IDS

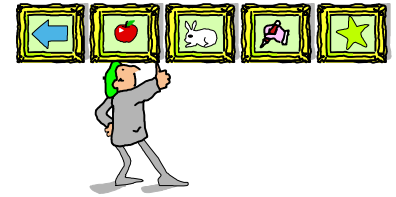
 Not appliciple

 Host-based IDS

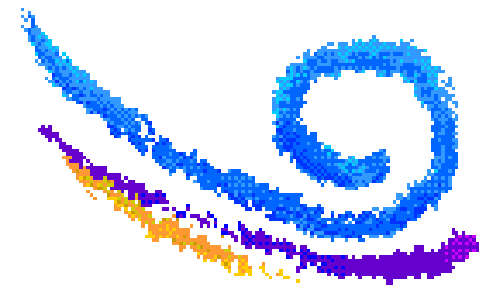
 Overlap of network based and host-based IDS



Overview



- ▶ Introduction
 - Motivation, Goals and Approach
- ▶ Description of IDSes (capabilities)
 - IDS engine, Information source, IDS configuration
- ▶ **Activities**
 - **Malicious vs. non-malicious**
 - **Activity Groups, Activity Variations**
- ▶ Conclusion



Activities (malicious vs. non-malicious)



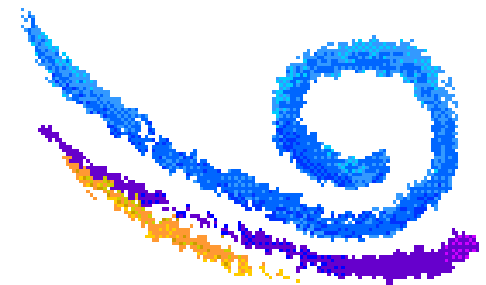
Classification of attacks

Non-malicious, but potential causes for false positives

Activities (non-malicious)

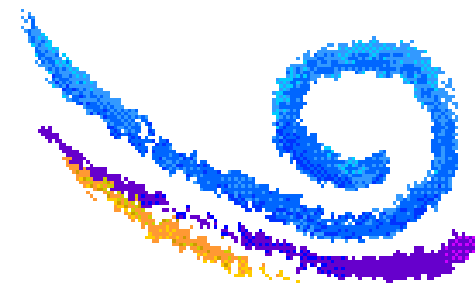
Attacks (malicious)

Non-Attacks

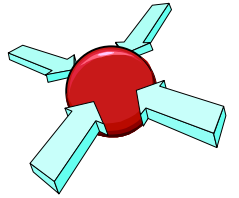


Attack Classification

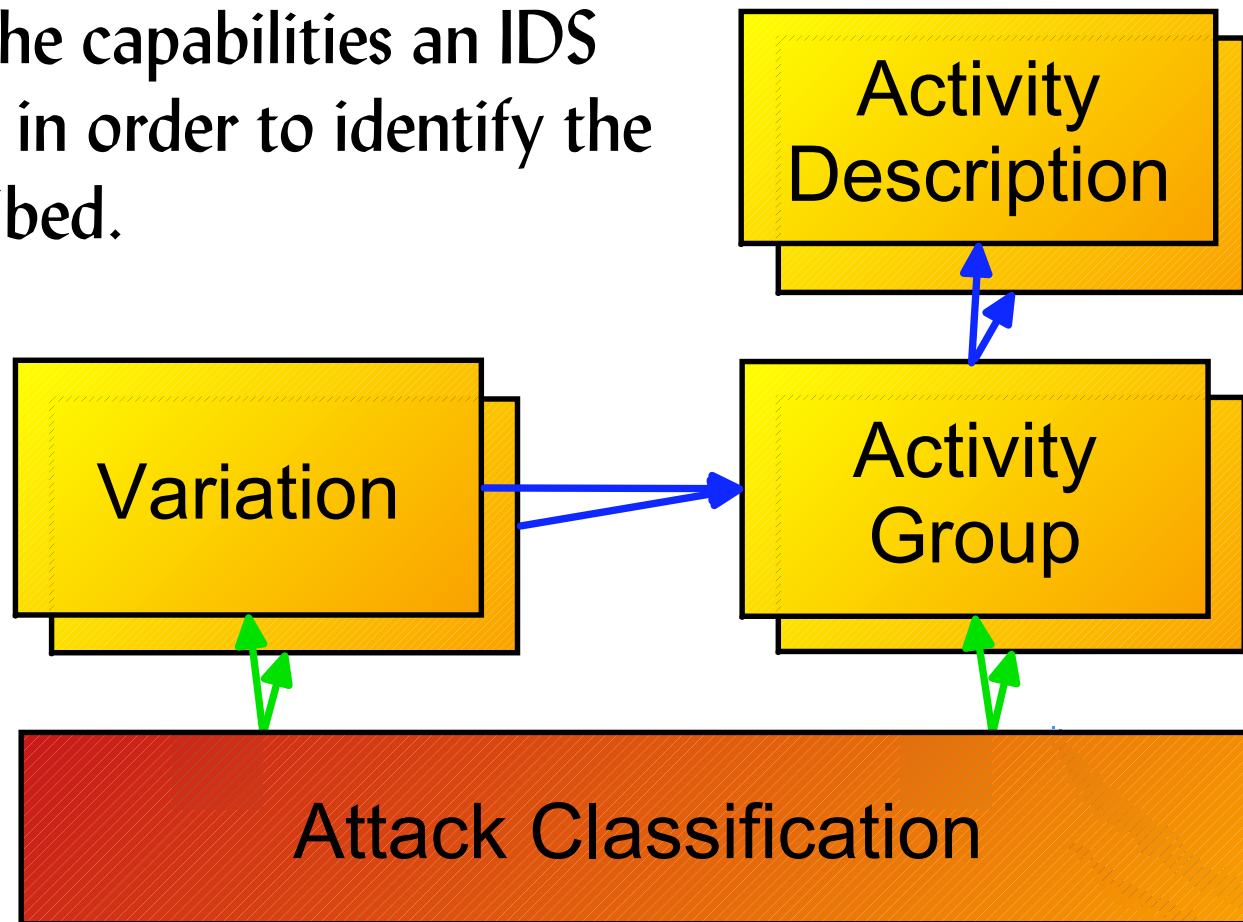
- ▶ Attack described by 4 parameters
 - Attack characteristics (9 characteristics + 4 attributes)
 - Attacked object type (12 object types)
 - Attack interface used (26 interfaces)
 - Vulnerability (10 fault characteristics)
- ▶ ~250 Classified attacks

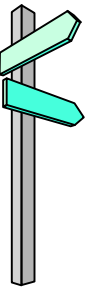


Activities (Activity groups and variations)



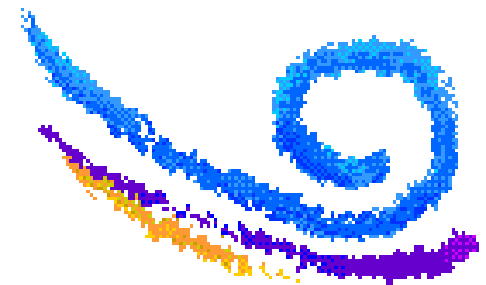
- ▶ An activity-description describes an activity with a set of rules. These rules specify the capabilities an IDS needs to have in order to identify the activity described.

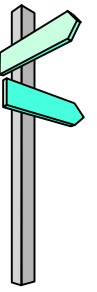




Outlook

- ▶ Attack classification
- ▶ Implementation of (prolog) rules describing activities
- ▶ Analysis of evaluation results
- ▶ Refine IDS characteristics





Conclusion

- ▶ A systematic approach to evaluate IDSeS
- ▶ A systematic approach to describe activities (although non-trivial)
- ▶ A simple way to describe IDSeS
- ▶ Implementation is ongoing

Contact: dal@zurich.ibm.com

