

# From Malware Pattern-State-Spaces to IDS AttacksFeatureMap

MONAM Panel Presentation

27 September 2006

Tubingen

**Prof. Atta Badii**

**Dept. Computer Science**

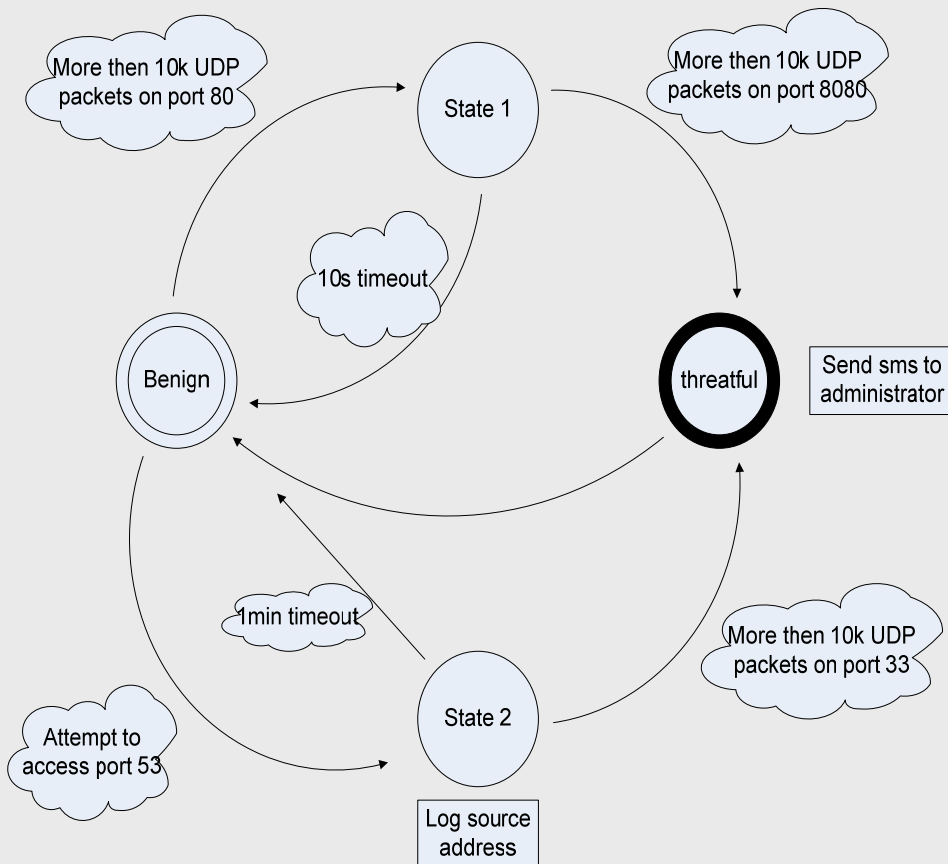
**School of Systems Engineering**

**University of Reading, UK**

# Discussion Summary

- **Conceptualisation of the Behavioural Model**
- **Feature System & Virtual Data Model Framework**
- **Dynamically Optimised Feature Maps**
- **Specification and Design of the Feature Map**
- **Feature Map Ontology and Mark Up Language Design Specification**
- **Topic Map Technology to IDS FeatureMap**
- **The topic map design and implementation: main Objectives**
- **Mapping IDS FS Ontology onto Topic Map**
- **XTM 1.0 syntax for the topic map implementation**
- **The [topicMap](#), [scope](#), and [association](#) element: example Syntax**
- **Classification of IDS attacks on the topic map-enabled FeatureMap**
- **Populating IDS attacks on the topic map-enabled FeatureMap**

# Conception of Behavioral Model

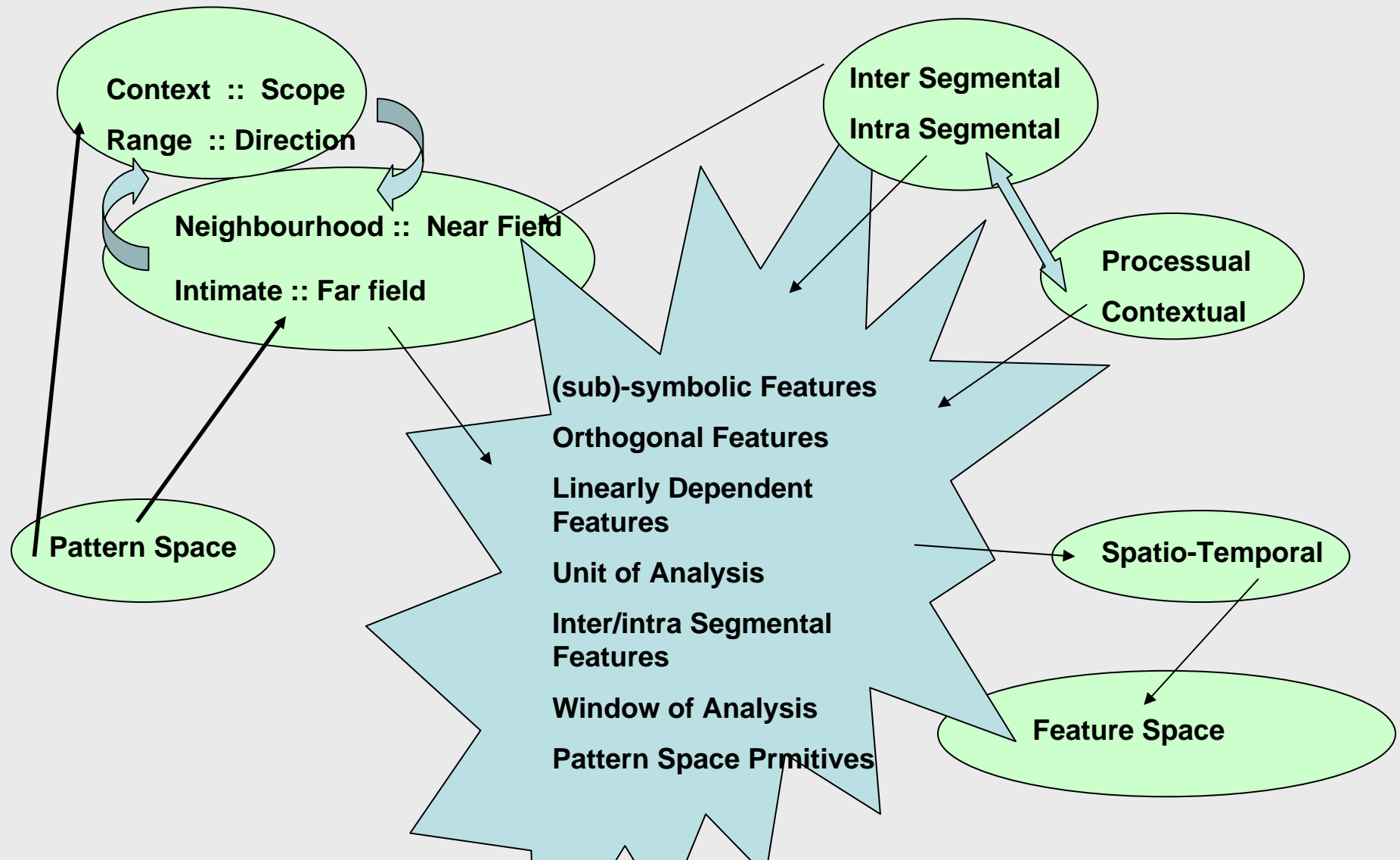


1. Behavioral model in the form of automata allows us to describe the behaviour of the system at every operational level of NSPES.
2. Time events allow going back to idle state of model with some timeouts or to dispersed in time set of features.
3. In the model properties of different features can be combined with logical operators.
4. With each state we can bind set of actions to be taken when model enters that state.
5. Model can be used to detect /prevent single threats as well as multiples.

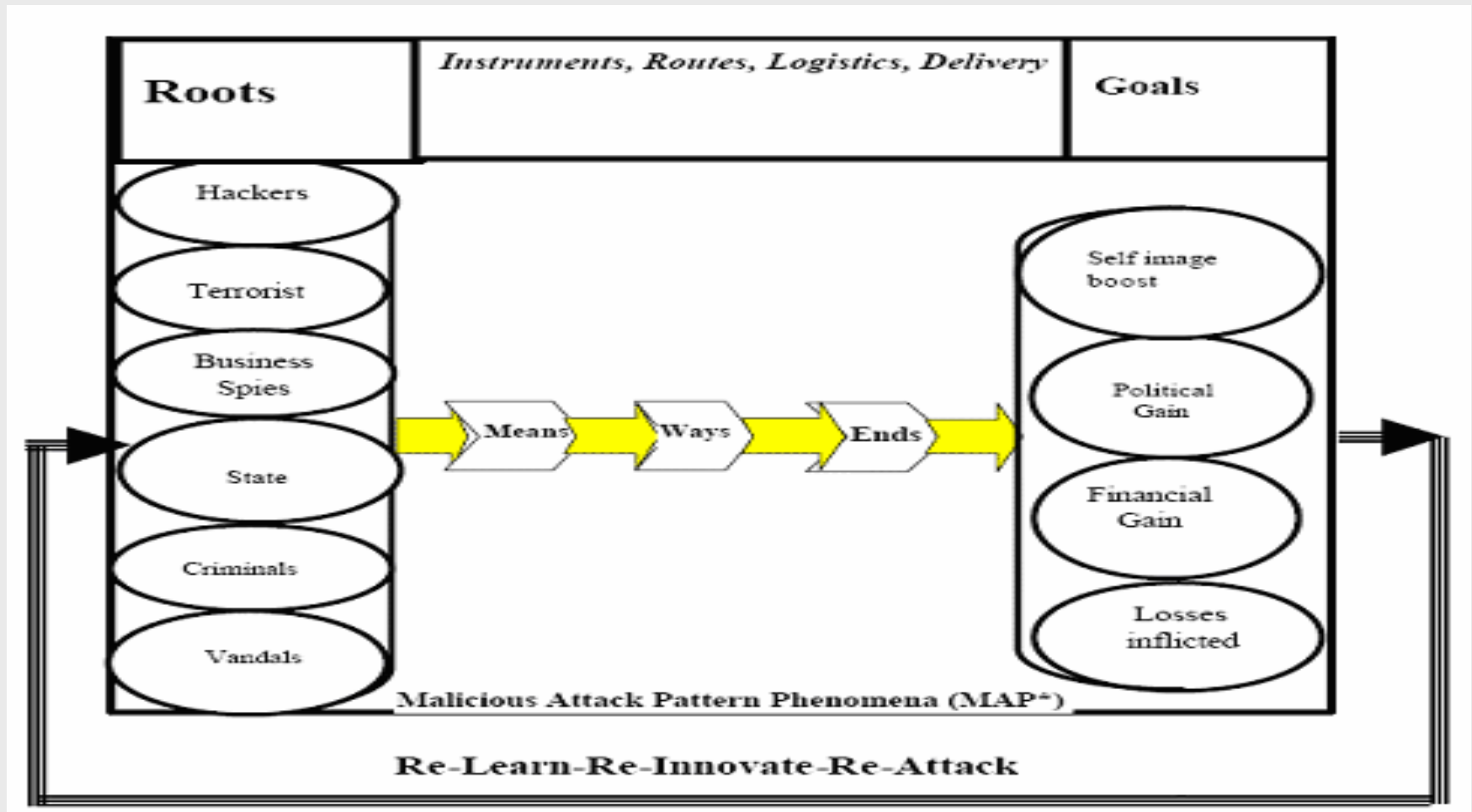
## Feature System & Virtual Data Model Framework

- The semantic bridges that can operate horizontally across different signature models e.g. Snort-vulnerabilities-exploits, Hackers' cookbook reverse engineered signatures, etc.
- Dynamic responsive scoping of operative analysis windows and associated context ranges.
- A semantic scaffolding structure that can permit traversal up and down, and dynamic refinement of, the Feature Map abstraction hierarchy to enable Knowledge Extraction and Knowledge Reporting loops.

# Dynamically Optimised Feature Maps

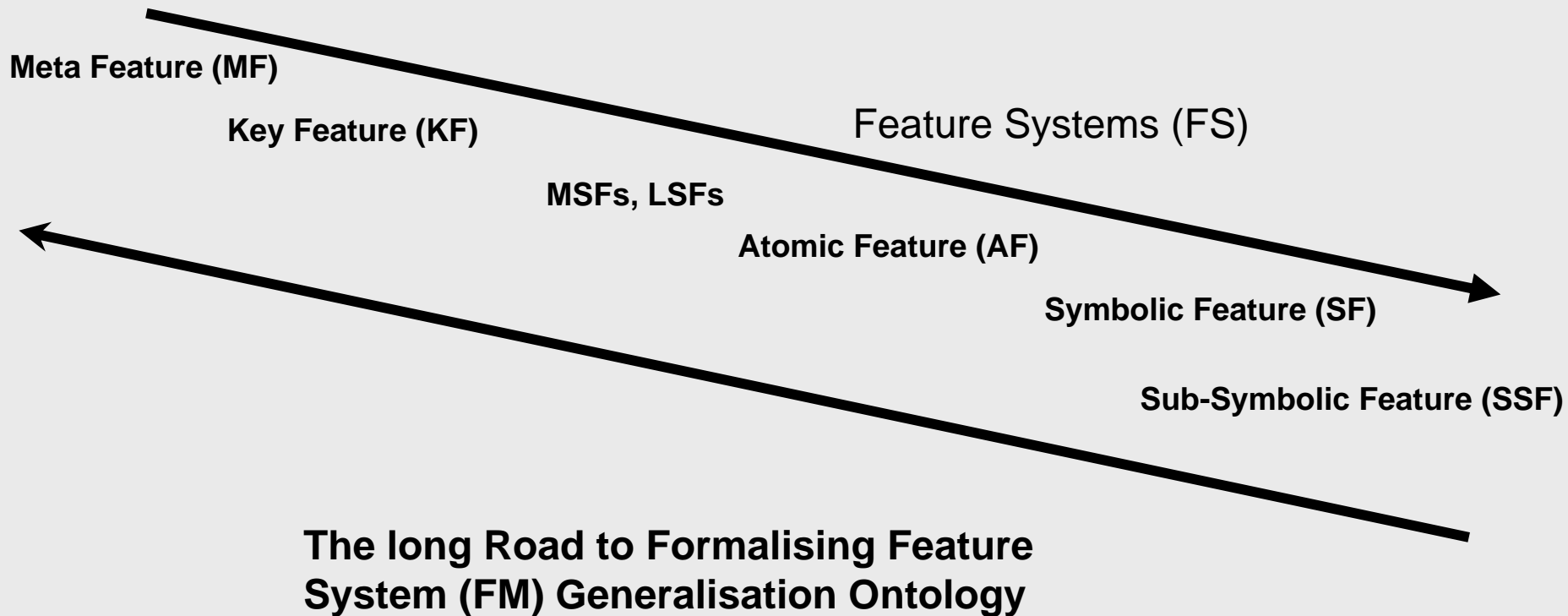


# Specification and Design of the Feature Map



# Feature Map Ontology and Mark Up Language Design Specification

- Topic Map: an XML-based semantic-associative standard that may be formalise the Feature System Representation and deploy its generalisation ontology as single, multiple recombinant FeatureMaps using Topic Maps  
Primary Features, Secondary Features, Composite (Derived) Features



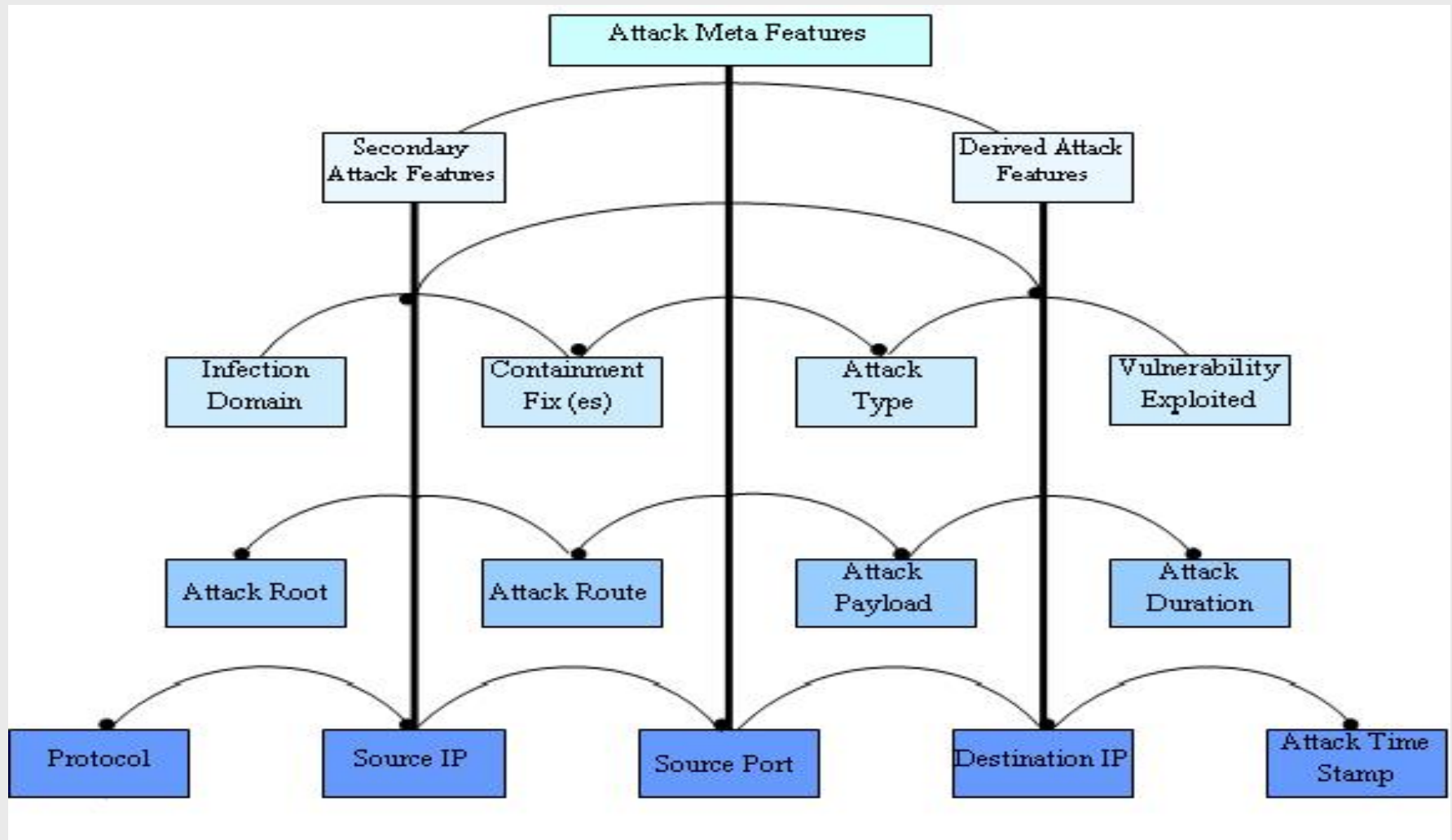
# Topic Map Technology

- According to [ISO/IEC 13250], a topic Map is an SGML or XML document (or set of documents) in which different element types, derived from a base set of architectural forms, are used to represent topics, occurrences of topics, and relationships (or “associations”) between topics.
  - *Topic*
    - *Topic Type*
  - *Topic Occurrence*
  - *Occurrence Role*
  - *Topic Association*
  - *Association Type*
  - *Association roles*
    - *Scope*
  - *Public Subject*
    - *Facets*

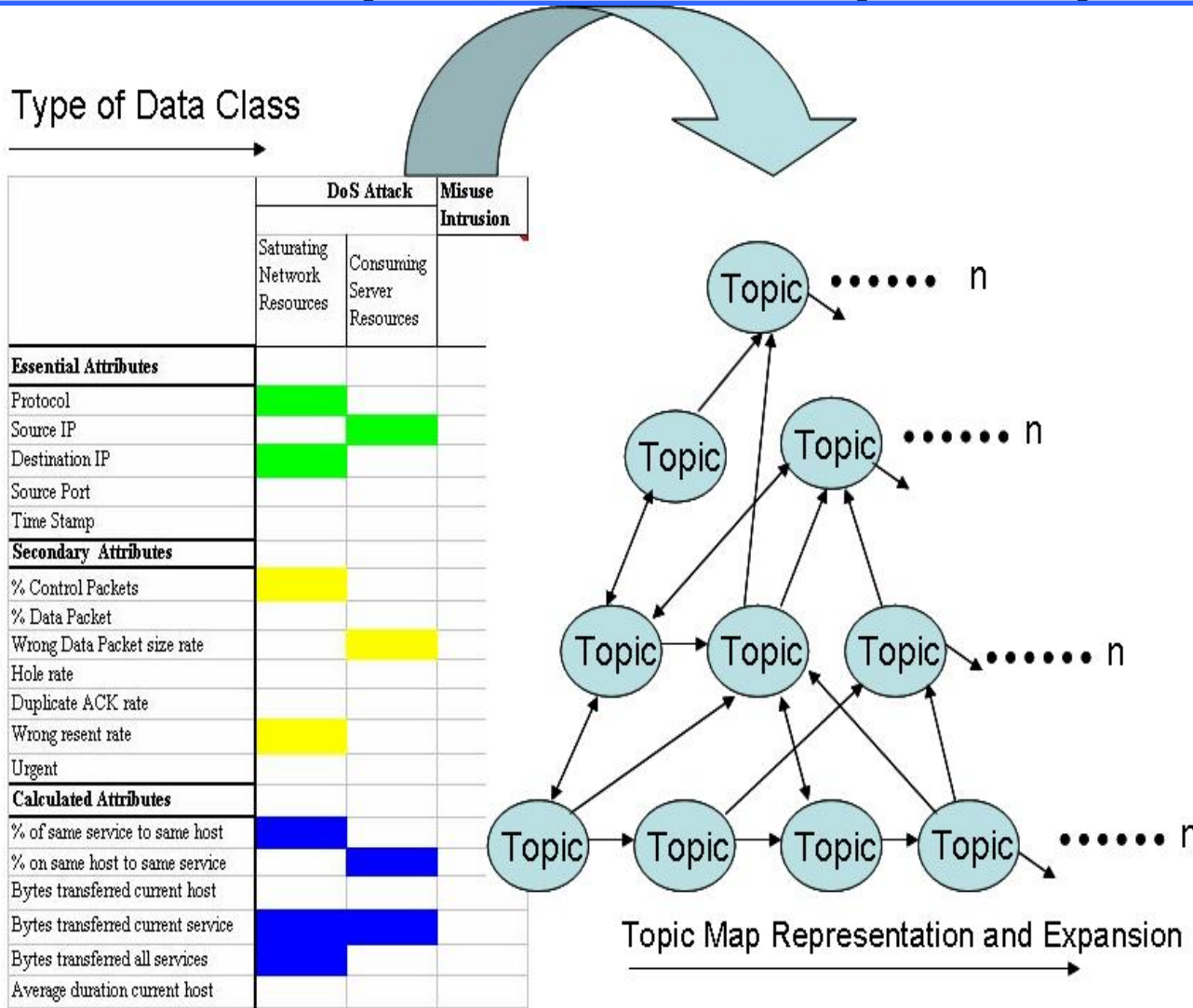
# The topic map design and implementation: main Objectives

- Define the application domain – what will be covered by the topic map.
- Define the functional requirements – who will use the topic map and for which purposes.
- Define the schema – what kind of subjects will be covered and how will they be related; what should a valid and consistent topic map look like.
- Select tool and implement the application – which software and architecture to use to implement the application.
- Populate the topic map – generate instances automatically or manually.

# Mapping IDS FS Ontology onto Topic Map



# XTM 1.0 syntax for the topic map implementation



An **XTM topic map** is a topic map serialized in XTM syntax as a topicMap element with descendants.

An **XTM document** is an **XML document** that contains one or more XTM topic maps. In a process known as deserialization, the XTM topic map is read by a topic map processor, which produces from it some representation of the Standard Application Model, by following a procedure equivalent to the one defined in this specification.

**Conversion of Feature Matrix to Topic Map Representation to arrive at the Feature Map**

# The **topicMap** element: example Syntax

The **topicMap** element is the root element of all XTM topic maps. It acts as a container for the topic map, and can be either the document element of an XML document, or it may be the root of a subtree inside an XML document that contains more than just a single topic map. In both cases, the input to the XTM deserialization process is the subtree contained by the **topicMap** element.

The **topicMap** element type is declared as follows:

```
<!ELEMENT topicMap
( topic | association | mergeMap )*
>
<!ATTLIST topicMap
  id          ID          #IMPLIED
  xmlns      CDATA      #FIXED 'http://www.topicmaps.org/xtm/1.0/'
  xmlns:xlink CDATA      #FIXED 'http://www.w3.org/1999/xlink'
  xml:base   CDATA      #IMPLIED
>
```

# The **scope** element: example Syntax

The scope element type is used throughout XTM to indicate the scope of a topic characteristic assignment.

The scope element type is declared as follows:

```
<!ELEMENT scope
  ( topicRef | resourceRef | subjectIndicatorRef )+
>

<!ATTLIST scope
  id          ID          #IMPLIED
>
```

# The **association** element: example Syntax

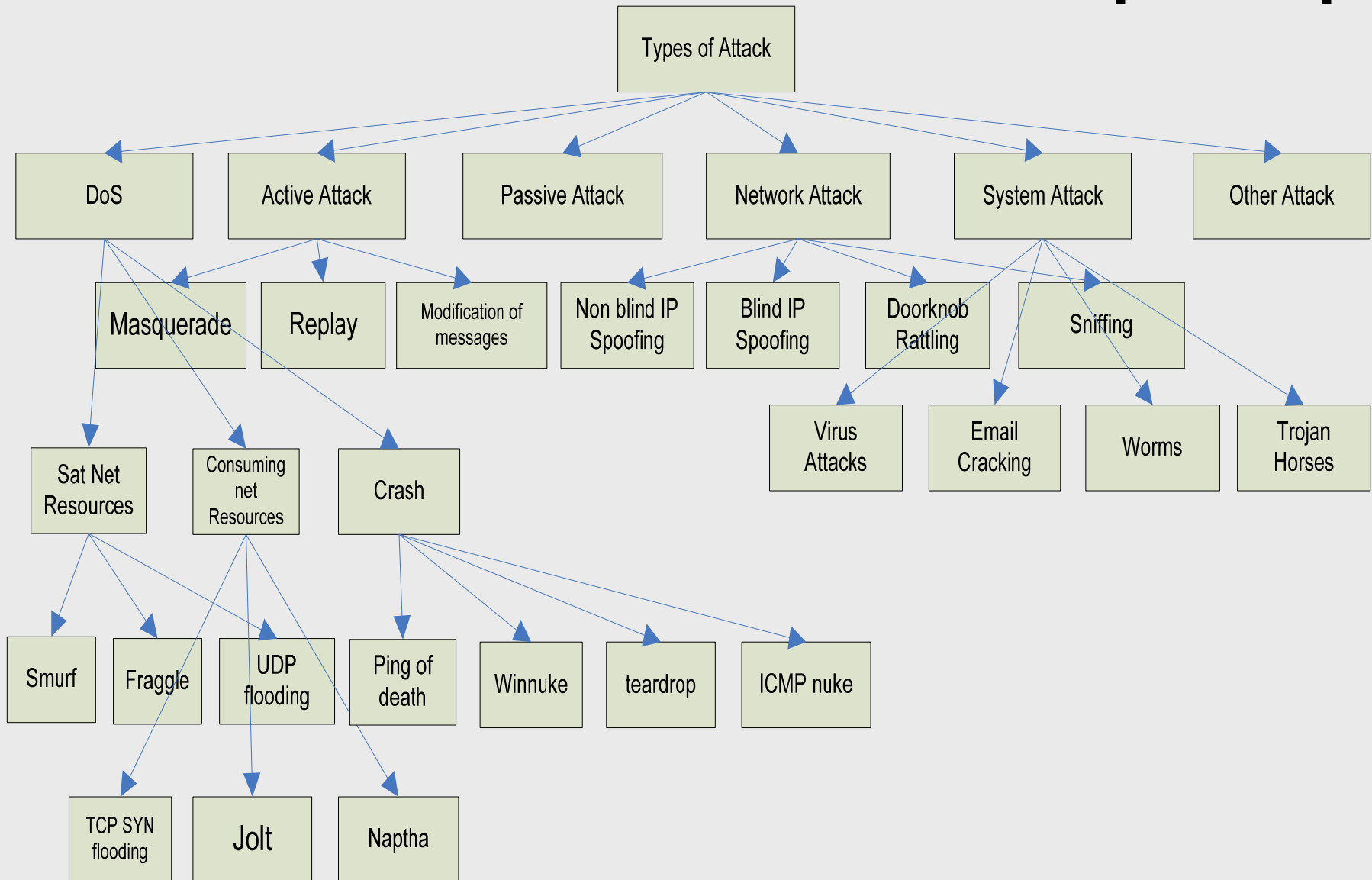
The association element type is used to express associations between topics. The member child elements provide the association role players of the association.

The association element type is declared as follows:

```
<!ELEMENT association
  ( instanceOf?, scope?, member+ )
>

<!ATTLIST association
  id      ID      #IMPLIED
>
```

# Classification IDS attacks on the topic map



# Populating IDS attacks on the topic map

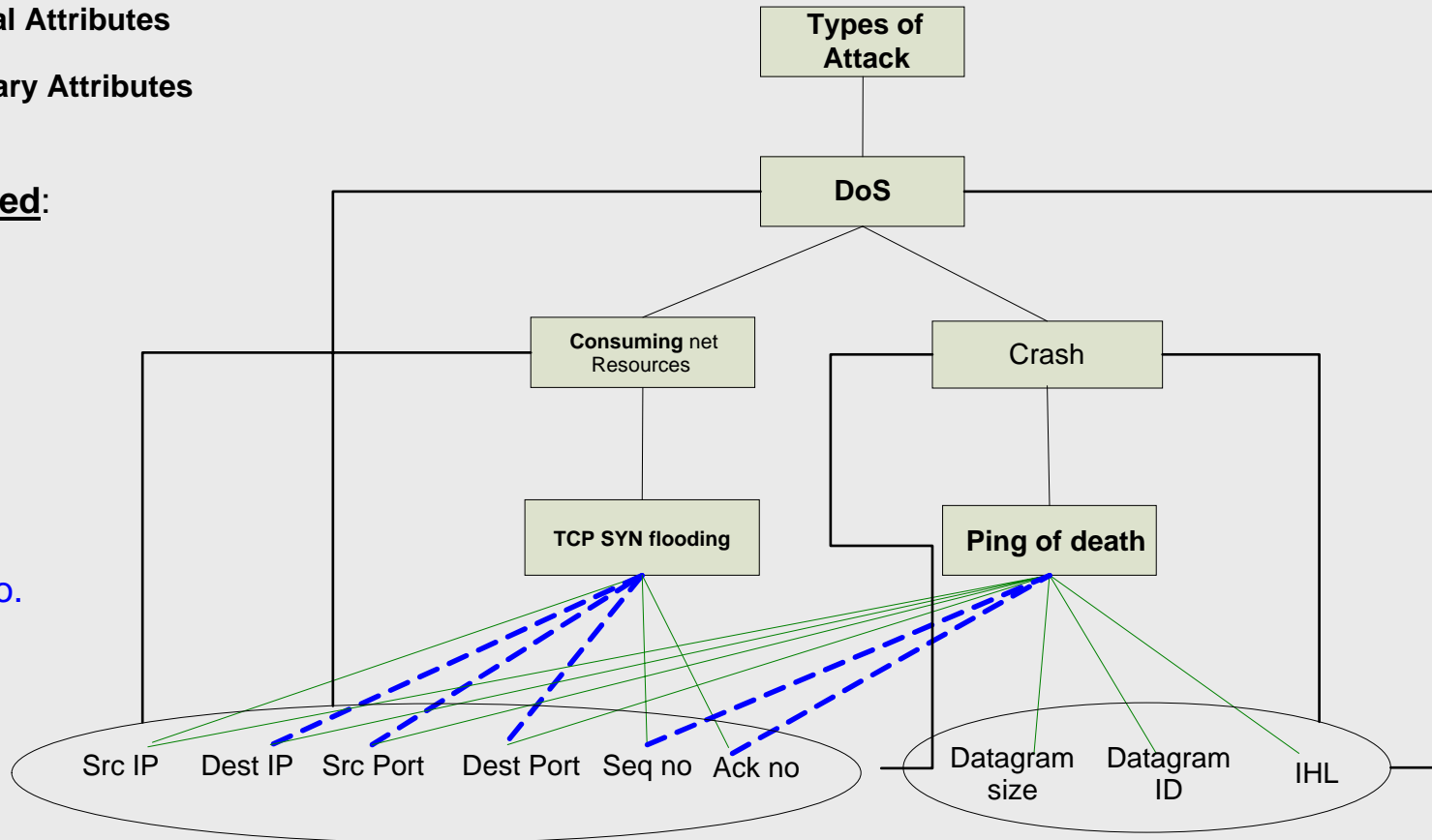
— Association

— Essential Attributes

- - - Secondary Attributes

## •Attributes Considered:

- Source IP
- Destination IP
- Source Port
- Destination Port
- Sequence No.
- Acknowledgement No.
- Datagram Size
- Datagram ID
- IP Header Length





**Thank You**