**1. LEARNING THE APPLICATION DOMAIN**

Billy Goat overview: the basic idea
- **Network**: Summary data
- **Analysis data**: Raw data
- **Explained threats**: Explained threats

- **Defense and Detection Strategies against Internet Worms**
  - Building and Deploying Billy Goat: a Worm-Detection System
  - Mining a Worm Detection System Data

- Billy Goat has a very low false positive rate, but, what about the false negatives?

**2. CREATING A TARGET DATASET**

- **External Billy Goat**
- **Internal Billy Goat**

- Billy Goat has been deployed on the Internet.
- Billy Goat sensors on Internet (Internal Billy Goat)
- Billy Goat sensor on Internal (External Billy Goat)

- Billy Goat overview: data models
  - For each IP address, a data model of:
  - Iptables
  - Summary data
  - Summary data
  - Application layer

- Billy Goat overview: the basic idea

**3. PRE-PROCESSING OF DATA**

- Billy Goat has been deployed on the Internet.
- Billy Goat sensors on Internet (Internal Billy Goat)
- Billy Goat sensor on Internal (External Billy Goat)

- Billy Goat overview: data models
  - For each IP address, a data model of:
  - Iptables
  - Summary data
  - Summary data
  - Application layer

- Billy Goat overview: the basic idea

**4. DATA MINING**

**5. PATTERN INTERPRETATION AND EVALUATION**

**6. CONCLUSIONS**

**References**

- J. Riordan and Y. Duponchel: "Mining a Worm Detection System Data"
- K. Julisch, "Volumes of Data"