The Base Rate Fallacy and its Implications for the Difficulty of Intrusion Detection

Stefan Axelsson

Presented by Kiran Kashalkar

Agenda

1. General Overview of IDS

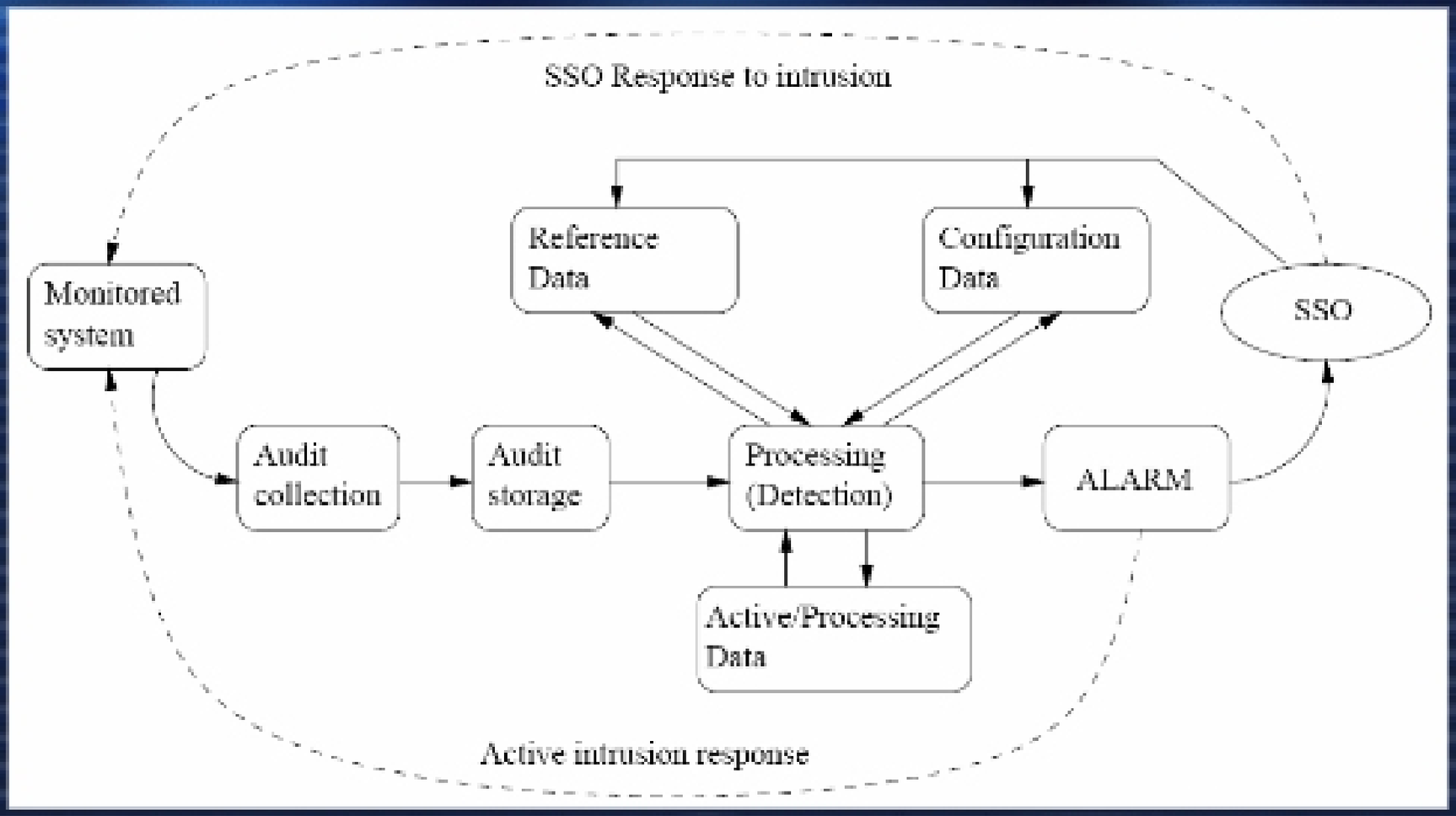
2. Bayes' Theorem and Base-Rate Fallacy

3. Base-Rate Fallacy in Intrusion Detection

4. Impact on Intrusion Detection Systems

5. Conclusion

Intrusion Detection Systems



Organization of a generalized IDS

- Intends to detect security violations from:
  - **Outsiders using prepacked exploit scripts**
  - **Impersonators (outsiders as well as insiders)**
  - **Insiders abusing legitimate privileges**
- Fundamental questions:
  - **Effectiveness, Efficiency, Ease of use, Security, Inter-Operability, Transparency**
- This paper focuses on **"Effectiveness"**