



Multiple Classifier Systems for Network Security

from data collection to attack detection

Claudio Mazzariello
Università degli Studi di Napoli Federico II

Tutori: prof. Carlo Sansone, prof. Simon Pietro Romano



Contesto applicativo

➤ Rilevazione delle intrusioni nelle reti di calcolatori

- Individuare comportamenti anomali
- Distinguere, fra i comportamenti anomali, quelli incidentali da quelli legati a specifici intenti malevoli

➤ Ambiente operativo *ostile*

- Scenari applicativi dinamici ed eterogenei
- Gli attaccanti tentano di eludere i meccanismi di controllo
- Gli attacchi subiscono mutazioni che possono renderli indistinguibili dai comportamenti ammissibili

Approccio proposto

- **Utilizzo di tecniche di pattern recognition nella rilevazione delle intrusioni**
 - Capacità di adattamento
 - Capacità di apprendimento

- **Sistemi multiclassificatore**
 - Molteplici punti di osservazione del problema
 - Molteplici tecniche con differenti caratteristiche
 - Molteplici tipologie di dati da analizzare

Implementazione e sperimentazione

➤ Etichettatura automatica del traffico

- Definizione automatica della ground truth
- Combinazione delle indicazioni fornite da molteplici tecniche di pattern recognition
 - Metodo non supervisionato per garantire l'indipendenza dai dati analizzati

➤ Multiclassificatori per la rilevazione *online* di intrusioni

- Utilizzo di metodi di combinazione supervisionati
 - Behavior Knowledge Space + informazioni sull'evoluzione temporale dei comportamenti analizzati
- Utilizzo di metodi di combinazione non supervisionati
 - Majority voting
 - Criterio di Dempster-Shafer

➤ Architetture distribuite per intrusion detection



GRAZIE PER L'ATTENZIONE