Know Your Enemy:
Modeling Hacker Behavior

Natalia Stakhanova *Ali A. Ghorbani*
{natalia, ghorbani@unb.ca}

Problem setting

- Recently emerging new types of cyber threats:
  - – cyberterrorism, politically and socially motivated attacks, raise of organized cyber attacks, etc.
- Who are the attackers?
  - – Myth: cyber attacks are conducted by *teenage genius hackers*, a *revenge seeking employees* or *money hungry criminals*.
  - – FACTS:
    - 43% of insiders have motives different from revenge (e.g., financial gain, reputation boost)
    - Majority of hackers are not technically advanced

Research goals

- develop a **comprehensive classification** of hackers & their organizational structures
- develop an **analysis framework** for profiling potential attackers and their affiliation based on the characteristics of the attack incidents
- build a **computational models** of the adversaries behavior from the attack planning stage to implementation based on the *analysis framework*

How to assess & analyze the cyber threat before the attack starts, during and after the attack?
Application: intrusion prevention, response planning & forensic analysis

Work in progress

Hacker Characteristics

Motives
Demographic profile
Computer knowledge & skills
Attack characteristics

Attack characteristics

Attack result
Attack access
Attack tools

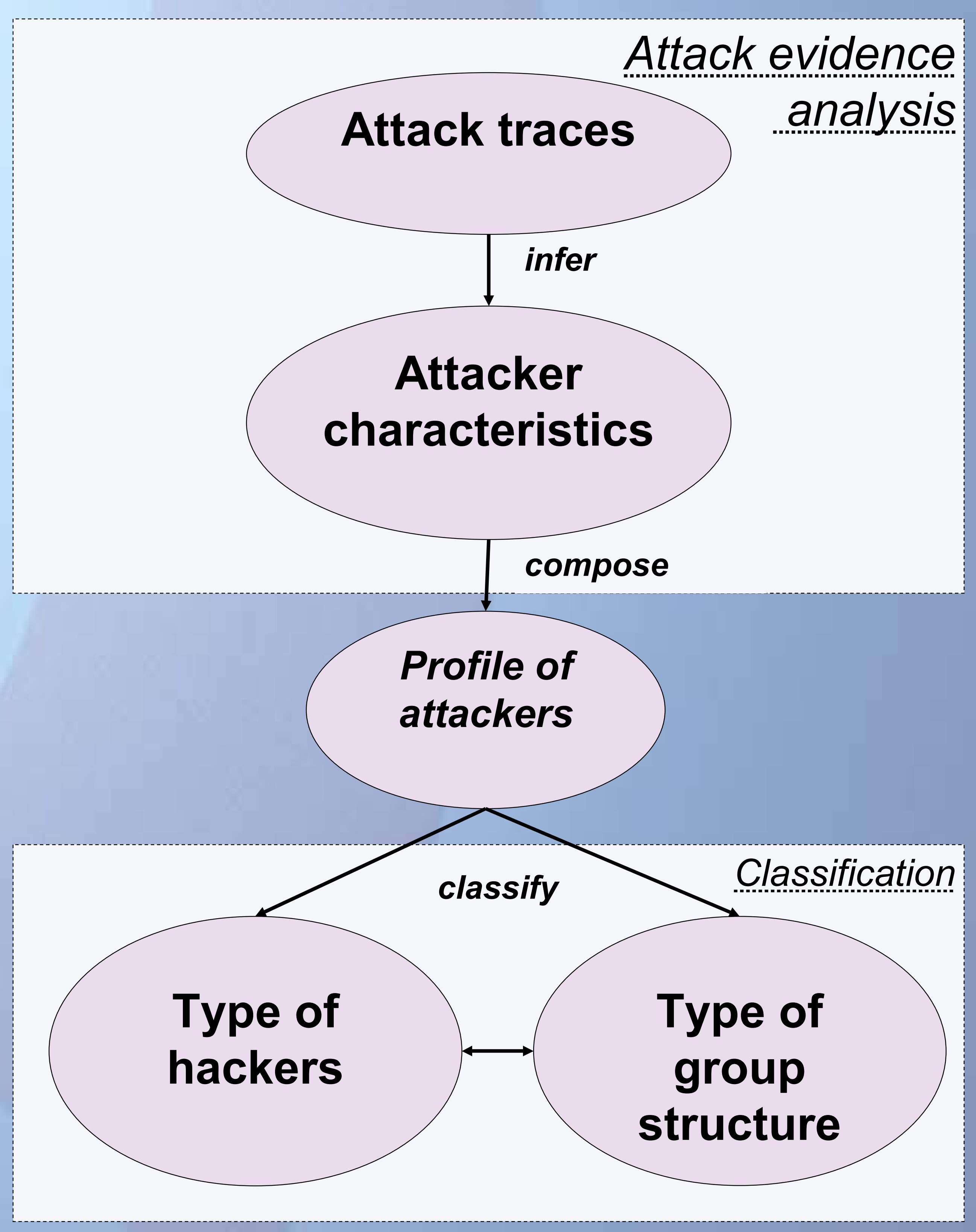
Group structure characteristics

Social interaction
Group participation in attacks
Existence of labor division
Stability of group over time
Patterns of communication
Values shared by group members

Future Work

- Analysis of Honeynet data
- Evaluation of the analysis framework
- Development of computational model of adversaries behavior

Conceptual model of the analysis framework



Faculty of Computer Science
University of New Brunswick