Toward Normative Threat Models to Prevent Misuse

Özgür Kafalı, Munindar P. Singh, and Laurie Williams
NC State University

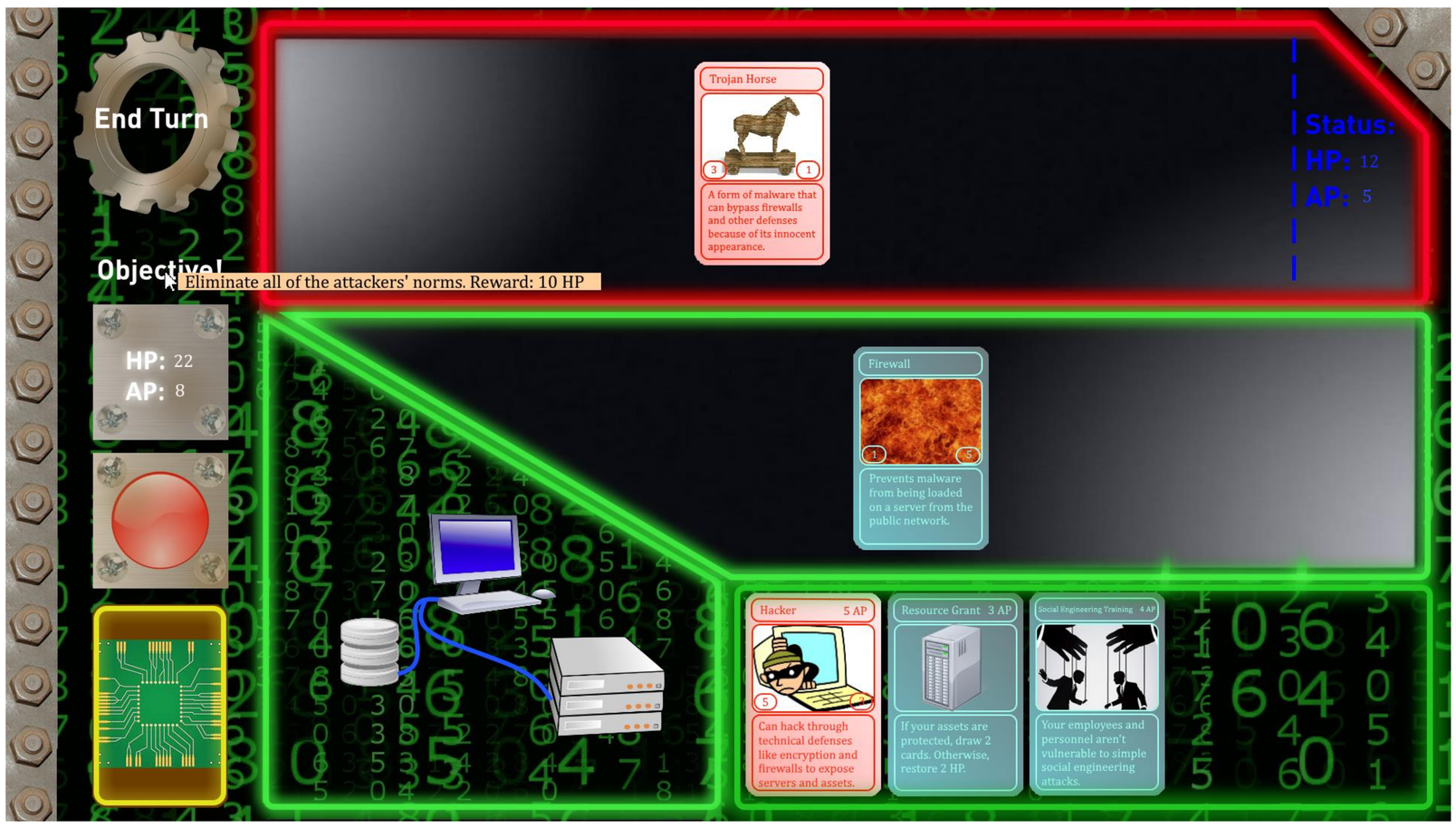
- Accidental misuses are quite prevalent among breaches [DoD Report, 2016]
- Developing comprehensive threat models (e.g., Attack/Defense trees) is hard
- Challenges and Opportunities:

1. Categorization or automatic generation of mitigation techniques
2. Testbed for researchers to develop and test hypotheses
3. Tool for cybersecurity education and training

- Goal: Understand how people make security choices
- Research Questions:

1. What priorities and assumptions people have in making security choices, what strategies they use?
2. What are potential mitigation techniques for various attack types?

- Methodology: Design a card game that players can customize
- Metrics: Compare game outcome to A/D tree



We thank Samuel Rappl for his help with our security card game.

Ongoing Work

- Extend attacker cards based on STRIDE
- Develop defender cards based on Mechanisms, Norms, Assumptions
- Design sample runs based on real settings
- Conduct pilot studies with human subjects

Future Work

- Develop automated agent strategies using the game API
- Extend the game to enable collaboration among defenders and attackers
- Conduct games with human players (via Amazon mTurk)

HoTSoS Symposium and Bootcamp
HOT TOPICS *in the* **SCIENCE OF SECURITY**
APRIL 4-5, 2017 | HANOVER, MARYLAND