Rational Resilience: ID3AL Process & Communication Games

Spencer Oriot

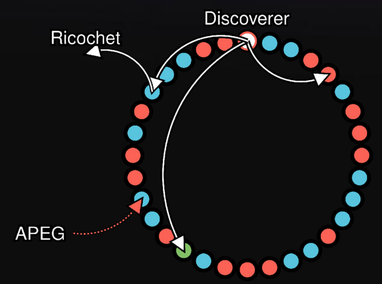
Research Questions

- "Ideal" performance of resilient system?
- System Scope?
- Limitations/Constraints on real performance?
- Relevant measures & definitions?
- Role of AI/ML?
- Strategic value of rationality?
- Implications for resource allocation?

ID3AL Process

ID3 + ALtogether = ID3AL Process

Bug Lifecycle



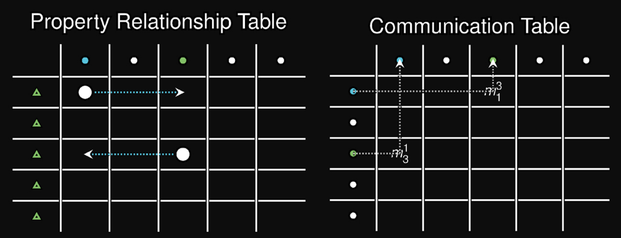
Conclusions

- No "wrong" Tx is primary objective
- "Ideal" performance is technically possible
- Incentive manipulation is critical to winning
- Discoverer economics rule the day
- "Rocky" resilience ≠ "Wolverine" resilience
- Shannon's Maxim holds (w/ slight modification)

Method

- Cybernetics definitions of machines, complex systems, and regulation and control analysis
- Mechanism Design incentive structuring
- Define ideal performance
- Identify mechanical requirements
- Model system's key interactions (context)
- Examine possible game courses (dynamics)

Communication Game



Game Play

Communication is a sequences of messages:

$$s = (m_1, m_2, ...)$$

Transfers are functions of communications:

$$f(s) = \mathsf{Tx}[s, r]$$

Bugs induce "wrong" transfers:

$$f(b) = \mathsf{Tx}^{\star}[s, r]$$

Takeaways

- First discoverer is cheapest path to identify
- Factor incentive effects in compute allocations
- Focus design efforts on discoverer economics
- Force "give or I take" dynamic
- Searching for undiscovered bugs is risky
- Mitigating damage potential (e.g. redundancy) likely a strong incentive strategy

C3E
Computational Cybersecurity in Compromised Environments
2024 Fall Workshop | September 17-19 | SRI International in Menlo Park, CA