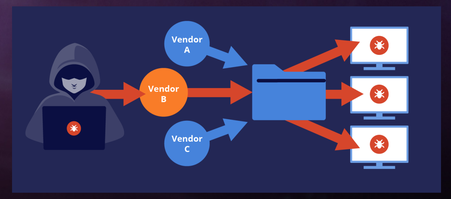
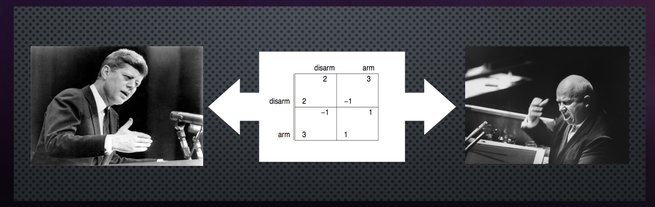
Updating economic methods for strategic reasoning in cybersecurity:
When Advanced Persistent Treat (APT) became Mutual Assured Destruction (MAD)

Dusko Pavlovic, University of Hawaii

dusko.org





Security = Economy

- **Security ⊇ Economy**
  - Only a resource that can be secured is an economic asset.
- **Security ⊆ Economy**
  - The cost of security must not be greater than the value of the asset

Security ≠ Gaming

- **Gaming is based on given rules and payoffs**
  - It is assumed that the rules are enforced and the players must follow them.
- **Security is tasked with enforcing rules and payoffs**
  - ***Gaming problems start where Security problems end***

mutual APT* = *cyber MAD

- Adversary has penetrated our systems
  - We cannot be certain how deep
- We have penetrated their systems
  - They cannot be certain how deep

Either side can strike. The other can retaliate. Both lose posture.

TASK 1. MAD protocol science

- model and analyze MAD protocol interactions
- system security through threat of retaliation
- design protocols for defense-by-offense

TASK 2. APT decision and game theory

- model and analyze APT incentives and utility
- incomplete info*: "Gaming Security by Obscurity"*
- case studies: *Attack Vectors, FlipIt*

GUIDANCE from the past

- FDR: *Unfettered selfishness is bad for economy*
  - and for security
- Eisenhower: *Wars are not won by weapons*
  - *but by strategy*

C3E
Computational Cybersecurity in Compromised Environments
2021 Fall Workshop | October 27-28 | Virtual