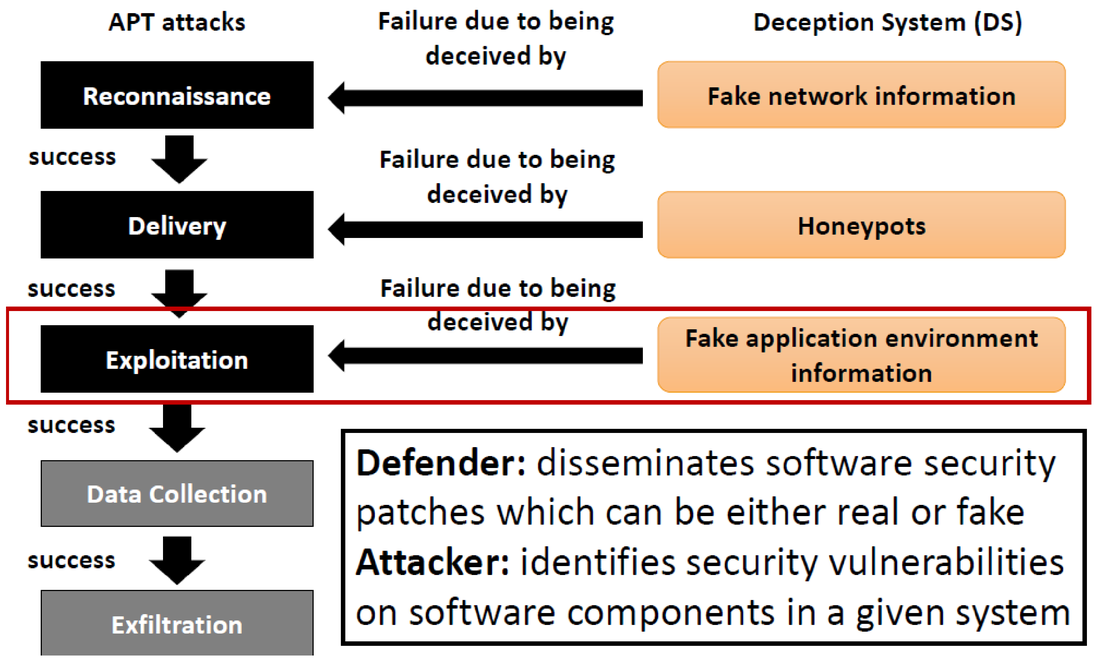
Defensive Deception in a Hypergame

Gaurav Dixit, Jin-Hee Cho, Ing-Ray Chen,
Mu Zhu, Munindar P. Singh, Charles A. Kamhoua

gdixit@vt.edu

Motivation

- Emergence of deception techniques as promising techniques to deal with advanced persistent threat (APT) attacks.
- Highly challenging to consider the behaviors of attackers and defenders with limited knowledge under given uncertain cyberspace.
- Need a realistic game modeling reflecting subjective beliefs of the attacker and defender which affect their choice of strategies to maximize utilities.



Research Goal

- Model an attack-defense game under uncertainty based on hypergame theory by developing a Stochastic Petri Nets model.
- Model defensive deception strategies to deal with APT attacks and to maximize defense utility, leading to maximum system reliability (i.e., mean time to security failure) while minimizing attack success probability.

Attack-Defender Hypergame

Attack Strategies vs. Defense Strategies:

Attacker's strategies	
AS_1	Reconnoiter
AS_2	Deliver
AS_3	Camouflage
AS_4	Exploit

Defender's strategies		
DS_1	Lure	Fake patch, honeypot
DS_2	Protect	Real patch, risk exposure
DS_3	Migrate	Perform MTD
DS_4	Hope	Do nothing

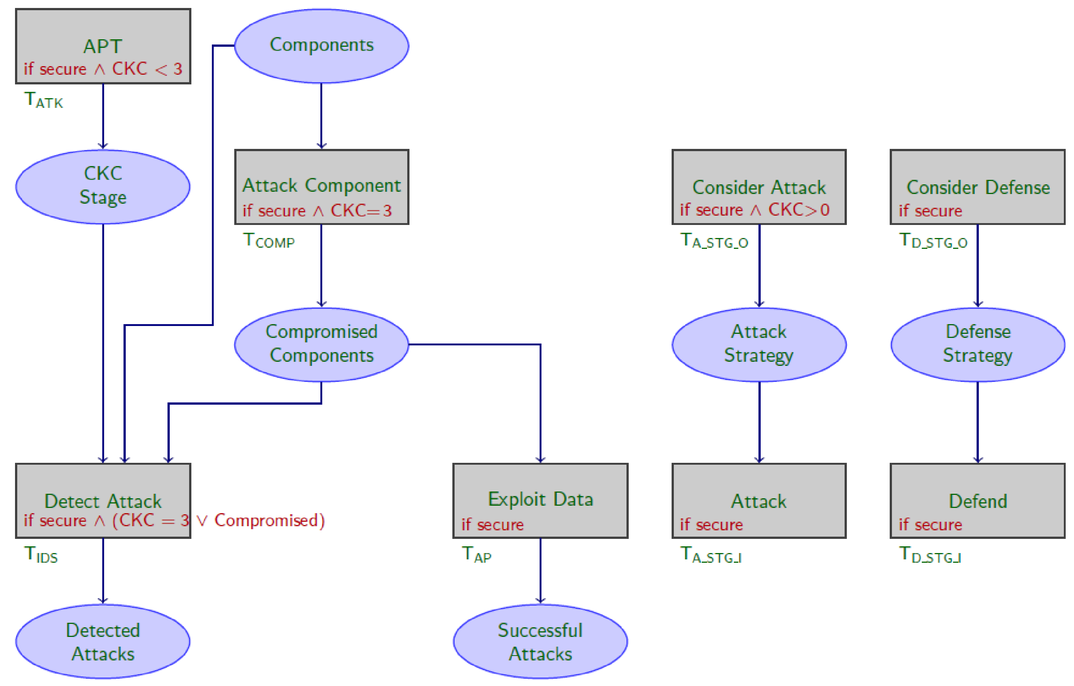
Attacker's subgame depends upon its stage in the CKC	Stage in CKC	Considered Strategies
	Reconnaissance	Reconnoiter, Deliver
	Delivery	Deliver, Camouflage
	Exploitation	Camouflage, Exploit

Defender's subgame depends on its system security status	System Security Status	Considered Strategies
	High: health $[90, 100]\%$	Lure, Hope
	Medium: health $[80, 90)\%$	Lure, Protect, Migrate
	Low: health $[0, 80)\%$	Protect, Migrate

Attack and Defender's Utilities

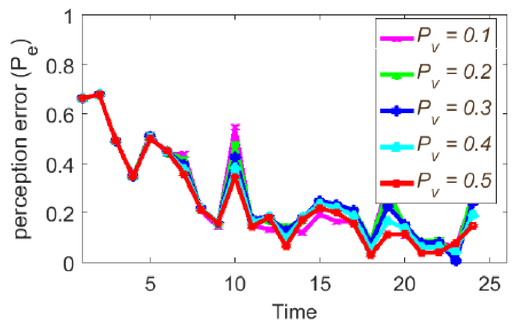
	Attacker	Defender
Payoff	Attack effect - Loss (being detected) - Attack cost	System security - Loss (vulnerabilities) - Defense Cost
Belief	Attacker's subjective belief (ASB) + uncertainty	Defender's subjective belief (DSB) + uncertainty
Utility	Sum of payoff weighted by ASB + worst payoff weighted by uncertainty	Sum of payoff weighted by DSB + worst payoff weighted by uncertainty

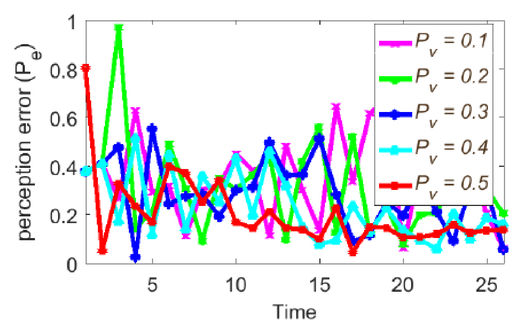
Stochastic Petri Net Model



Preliminary Results

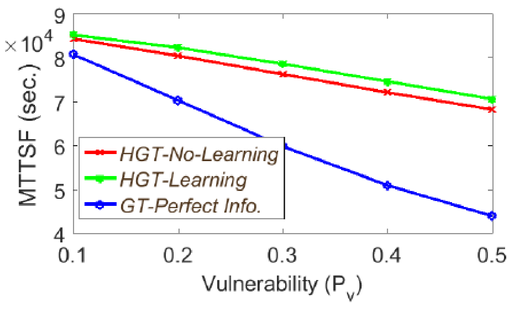
Perception Errors in Hypergame Setting: Perception errors are higher when both parties learn

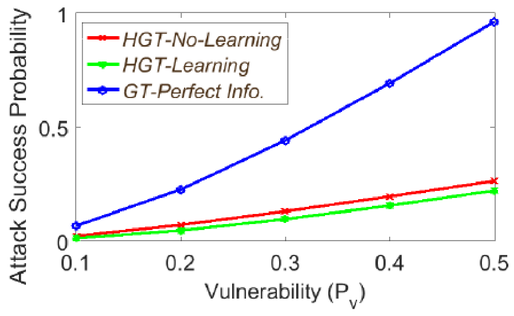




- Hypergame without learning
  - Low error for components with high vulnerability
  - Errors are inverse of component vulnerability
- Hypergame with learning
  - Errors increase with learning
  - High sensitivity to low component vulnerability

Hypergames versus Game with Perfect Information





- Game with perfect information
  - Each knows other's selected strategy
  - Each fully observes the other and the environment
- MTTSF = Mean Time To System Failure
- Perfect information is best for attacker
- Hypergame with learning is worse by a little because of symmetry: the opponent learns too

Conclusions & Future Directions:

- Introduced hypergame model for capturing misperceptions of attackers and defenders.
- Introduced Stochastic Petri Nets, a well-known formalism in reliability engineering, as a representation and analytical tool for deception.
- Introduce dynamic utility calculations based on improved models.
- Improve realism of the system model, especially considering settings such as SDNs, for clarity on the possible moves and incentives of attackers and defenders.