CERIAS
The Center for Education and Research in Information Assurance and Security

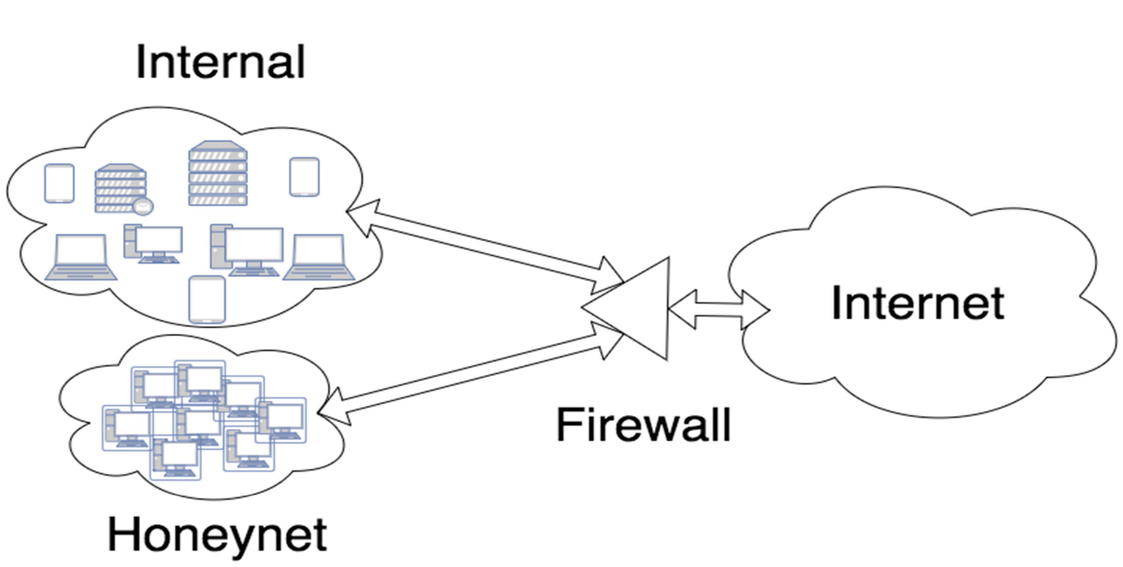
The Cost of Deception

Jeffrey Avery, Christopher N. Gutierrez, Eugene H. Spafford

Limited research has been done to incorporate deception into software where it executes and exists alongside legitimate programs and data In 2015, MITRE published a model representing the deceptive development process. We propose an analysis of the cost of deception using this model and Microsoft's Security Development Lifecycle to show the effect of integrating deception, identify cost heuristics at each stage of the deceptive lifecycle and provide insight to the feasibility of injecting deception into the software development. Portions of this research are funded by National Science Foundation Grants CPS-1329979, Science and Technology Center CCF-0939370, and EAGER-1548114.

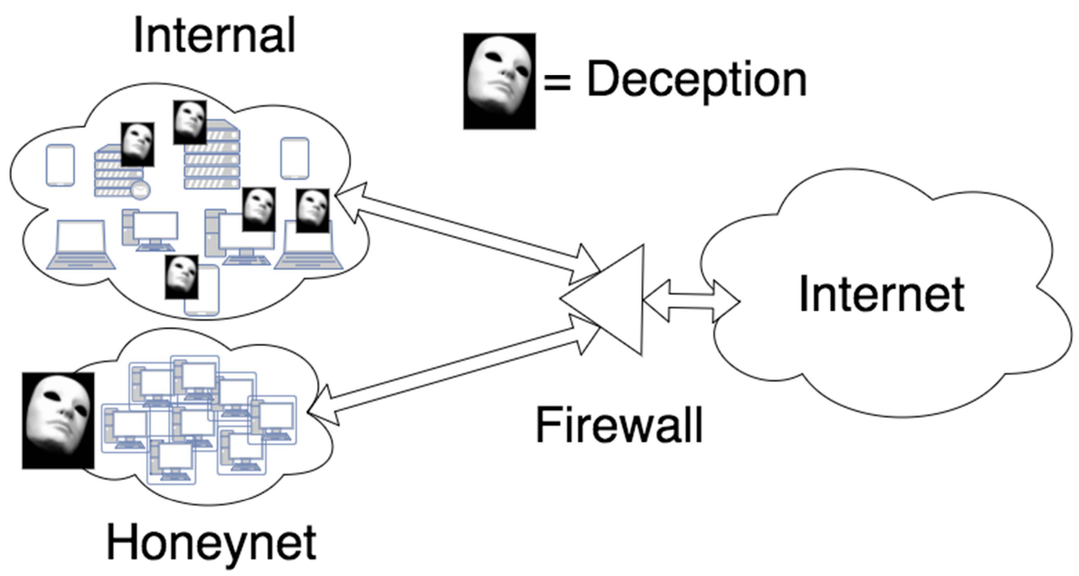
Traditional Deception

- Positioned externally to corporate network
- Identify intrusion attempts missed by firewall
- Must be populated with bait
- Bypassing deception can lead to compromise of authentic network/machines/data without alert



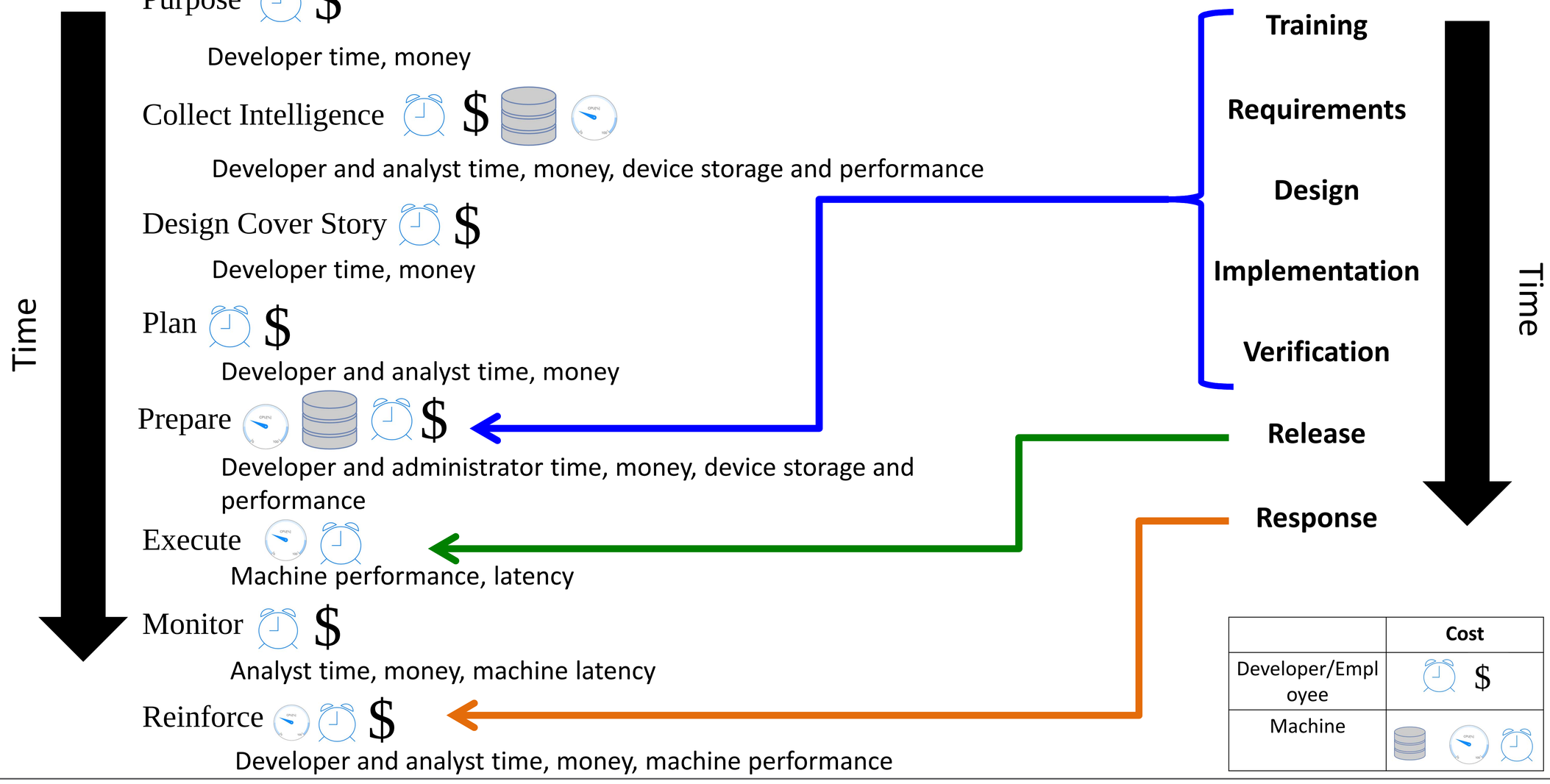
Integrated Deception

- Positioned externally as well as internally to corporate network
- Increase the depth of defense
- Can cause more confusion, time wasting by and exposure of attackers
- False positives due to legitimate programs executing



Deceptive Development Lifecycle Cost Analysis

Deceptive Development Lifecycle *Security Development Lifecycle*



	Cost
Developer/Employee	$
Machine	