EAGER: Exploring the Use of Deception to Enhance Cyber Security

CERIAS **PURDUE** UNIVERSITY

Challenge:

- 🔴 In everyday lives, deception plays a prominent role in our physical world security, e.g., fake "Beware of Dog" sign.
- 🔴 We are investigating how deception can be strategically inserted to improve the security of computers and networks

Solution:

- 🟢 A framework where deception can be planned and integrated into computer defenses
- 🟢 Mechanism to detect in real-time attempts to destroy forensic evidence and deceive adversary
- 🟢 "Ghost patches" to deceive adversary trying to exploit unpatched system
- 🟢 Game-theoretic investment of defense budget in a multi-stakeholder system
- 🟢 "Ersatz password" scheme to exploit hacked password database
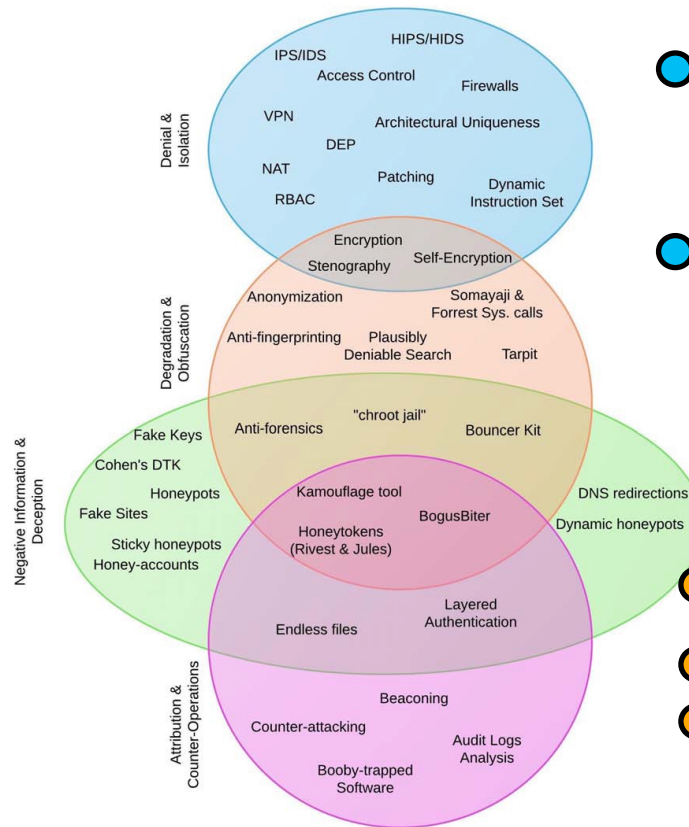
Scientific Impact:

- 🔵 Map deception to the digital world to improve security, turning the tables on its typical usage
- 🔵 Exemplars are shown for common security use cases — patching, password hacking, anti-forensics

Broader Impact:

- 🟠 Society can place higher confidence in security of *existing* systems
- 🟠 Analogies to security in physical world
- 🟠 Publications in book, conferences, journals plus presentations in professional societies, including non-academic forums
- 🟠 Graduate and undergraduate students involved
- 🟠 Partners at other institutions – government labs and companies

Diagram

Denial & Isolation
- HIPS/HIDS
- IPS/IDS
- Access Control
- Firewalls
- VPN
- Architectural Uniqueness
- DEP
- NAT
- Patching
- Dynamic Instruction Set
- RBAC

Degradation & Obfuscation
- Encryption
- Self-Encryption
- Stenography
- Anonymization
- Somayaji & Forrest Sys. calls
- Anti-fingerprinting
- Plausibly Deniable Search
- Tarpit

Negative Information & Deception
- Fake Keys
- Cohen's DTK
- Honeypots
- Fake Sites
- Sticky honeypots
- Honey-accounts
- Anti-forensics
- "chroot jail"
- Bouncer Kit
- Kamouflage tool
- BogusBiter
- DNS redirections
- Dynamic honeypots
- Honeytokens (Rivest & Jules)

Attribution & Counter-Operations
- Endless files
- Layered Authentication
- Beaconing
- Counter-attacking
- Audit Logs Analysis
- Booby-trapped Software