

# Defense from Cyber-Attack Using Deception

Neil C. Rowe, U.S. Naval Postgraduate School

<http://www.cs.nps.navy.mil/people/faculty/rowe>



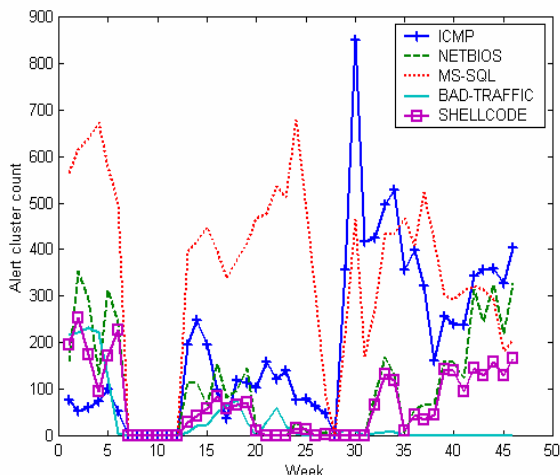
## Theory and Software for Defensive Deceptions

We are developing a set of deception methods and their implementations. Our goal is to provide more variety of attack responses than just delaying and dropping packets.

We have developed a taxonomy of 23 basic deceptive defenses for cyberspace, with subcategories for each defense.

Deception is an unexpected defense in cyberspace and (unlike most defenses) works best against smart attackers.

The graph at the right plots Snort alerts per week on our honeypot, showing a predominant overall decrease in attacks on the (apparently) new machine, plus provoking effects of deliberate disconnection from the Internet.



Results of deceptions on our honeypot

### Approach

- Systematically enumerate possible defensive deceptions.
- Implement some on a honeypot, study attacker reactions pro and con.

### Research Impact

- Techniques for better honeypots
- New methods for confusing attackers
- New challenges for attackers to worry about

### Current areas of research:

- Perform particular deceptions on a honeypot, then statistically analyze attacker reactions.
- Develop methods for analyzing “last packets” (or near-to-last) to find specific clues that make attackers go away.
- Develop methods for mimicry of honeypots (“fake honeypots”), using last-packet analysis, to scare away intelligent attackers.
- Find methods that cause attackers to redouble attack efforts.
- Investigate quantitative decision-theoretic and game-theoretic models of deceptions, plus of deceptions in response to deceptions.
- Study social engineering techniques (especially phishing) to learn tricks we can use defensively.