SAND2016-11419C

Refining the Foundations for Cyber Zone Defense

Robert Mitchell
rrmitch@sandia.gov
703.597.3730

Sandia National Laboratories

Exceptional service in the national interest

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

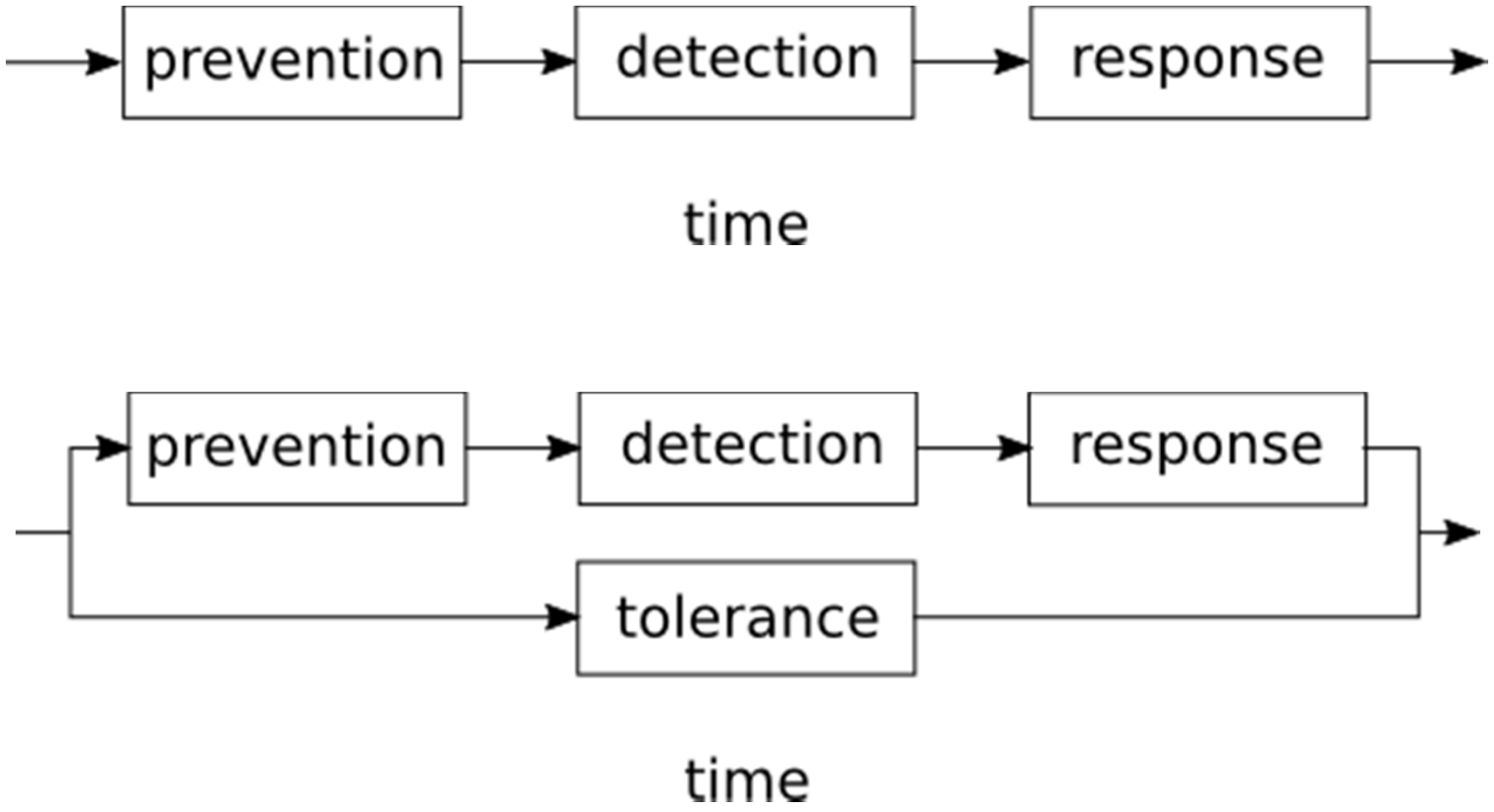
Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

Agenda

Sandia National Laboratories

- Cyber Security Concept of Operations
- Threat Model
- Metrics of Interest
- Closed-Form Mathematical Model
- Simulation
- Results
- Parameter Estimation
- Conclusions

Cyber Security Concept of Operations



Threat Model

Sandia National Laboratories

- Insider Threat
  - Witting: carrot and stick
  - Unwitting: spear phish, watering hole and document exploit
- Lateral Movement
  - File shares
  - RDP
  - SSH
- Exfiltration
  - Beacon
  - Upload sensitive data

Metrics of Interest

- Probability of Compromise
  - Represented by p_c
  - How likely an arbitrary host is to be compromised
- Probability of Reachback
  - Represented by p_r
  - How likely the adversary is to be able to beacon

Closed-Form Mathematical Model

Sandia National Laboratories

- p_e = probability an exploit is available
- z = zone size
- n = network size
- ϕ = interzone porosity
- x = number of externally facing hosts
- $p_c = \frac{1+p_e\left(\frac{z}{n}+\phi\frac{n-z}{n}\right)(n-1)}{n}$
- $p_r = 1 - (1-p_c)^x$

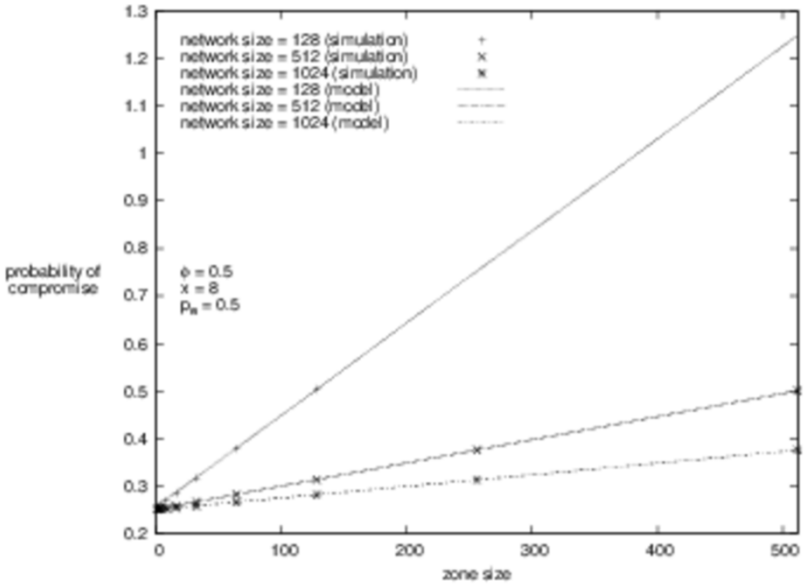
Simulation

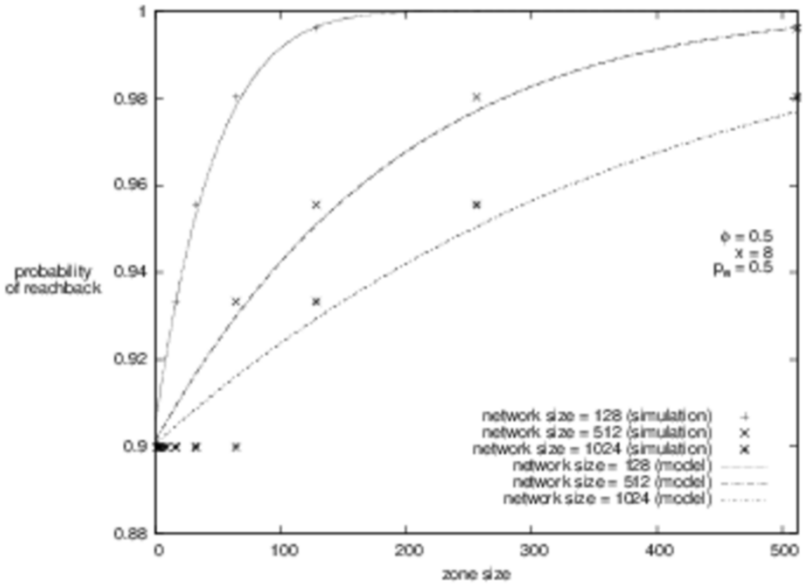
- Instrumented in Python.
- Start with one or more insiders (for whom $p_c = 1$) and legitimate hosts (for whom $p_c = 0$).
- Simulate lateral movement in rounds.
  - Update $\overrightarrow{p_c}$ (per-host probabilities of compromise) based on adjacencies, p_e and prior $\overrightarrow{p_c}$.
- Repeat until $\overrightarrow{p_c}$ converges.
- Calculate $\overline{p_c}$ (average probability of compromise).
- Calculate p_r based on actual p_c for externally-facing nodes.

Results

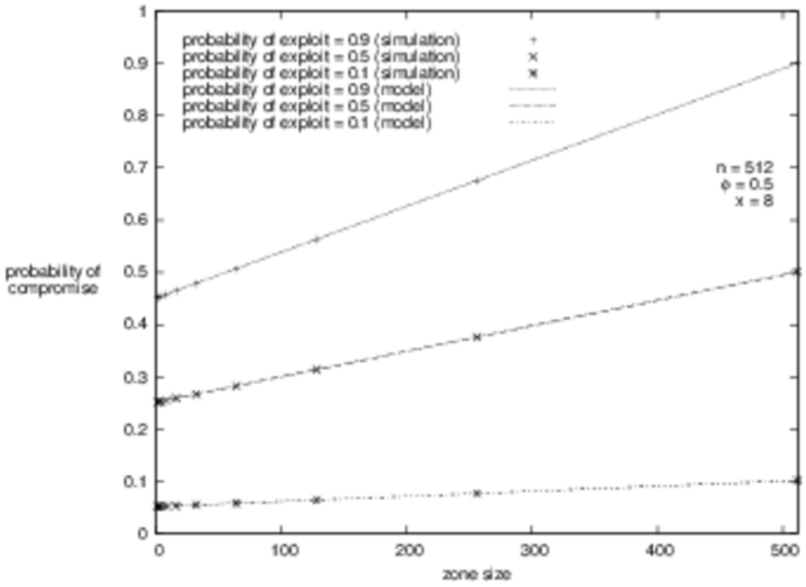
- Two Dependent Variables: p_c and p_r
- Five Independent Variables: z, n, p_e, x and ϕ

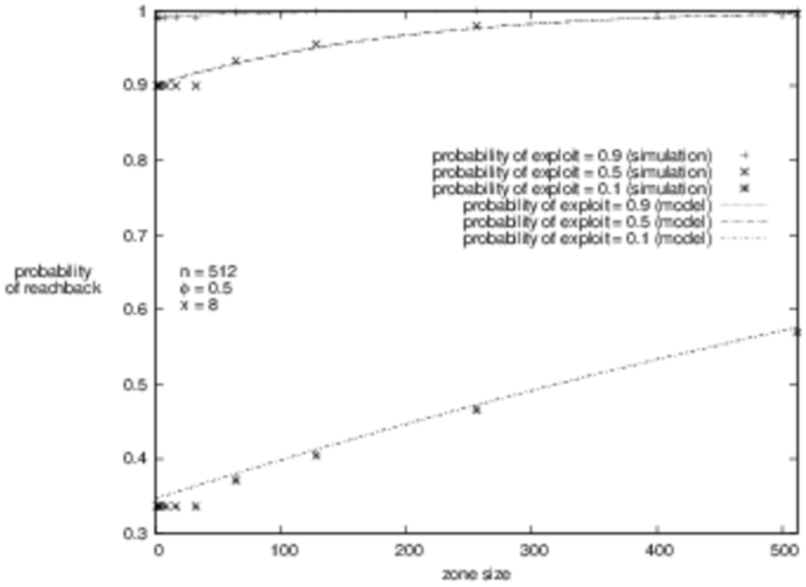
Results: Impact of Zone Size and Network Size



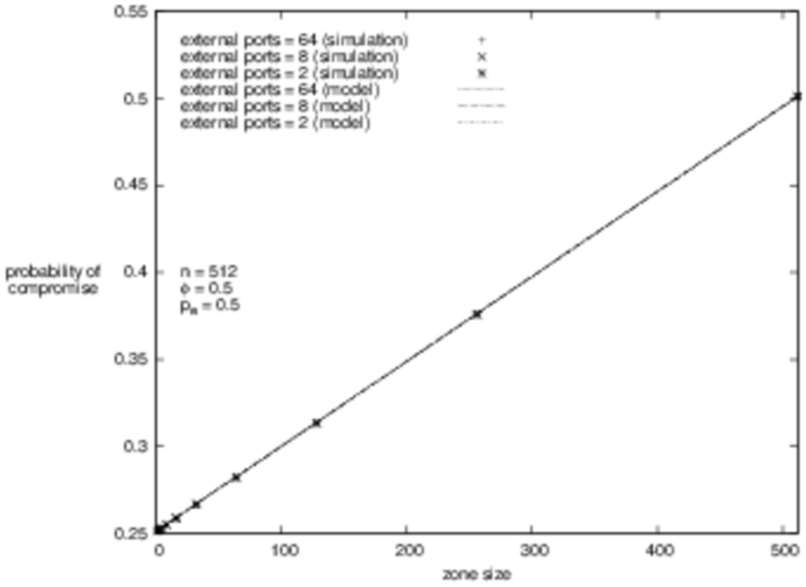


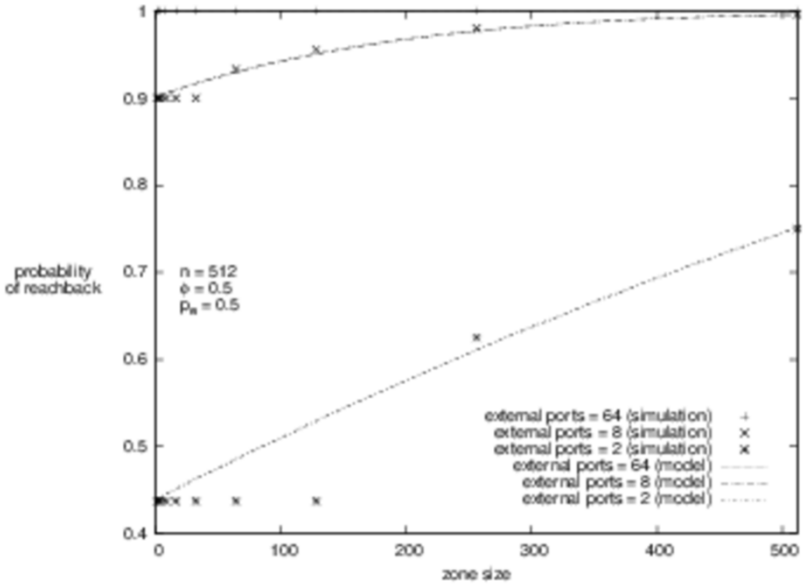
Results: Impact of Zone Size and Exploit Probability



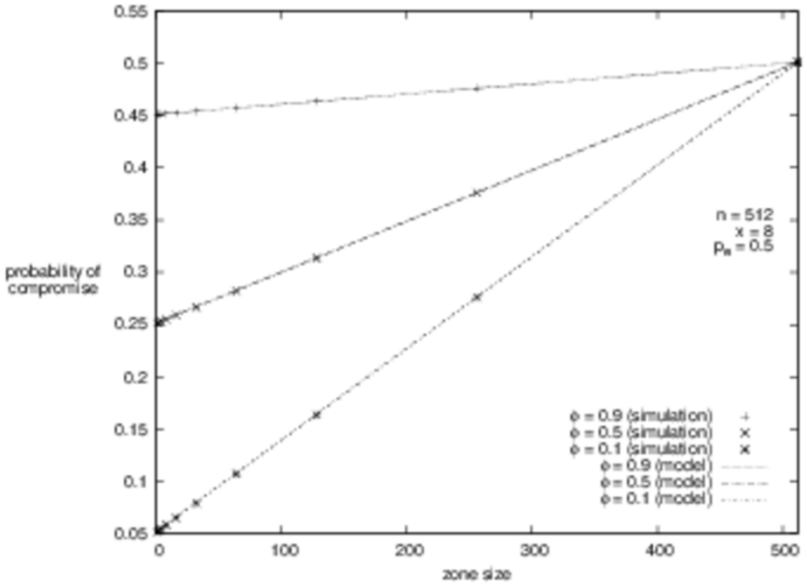


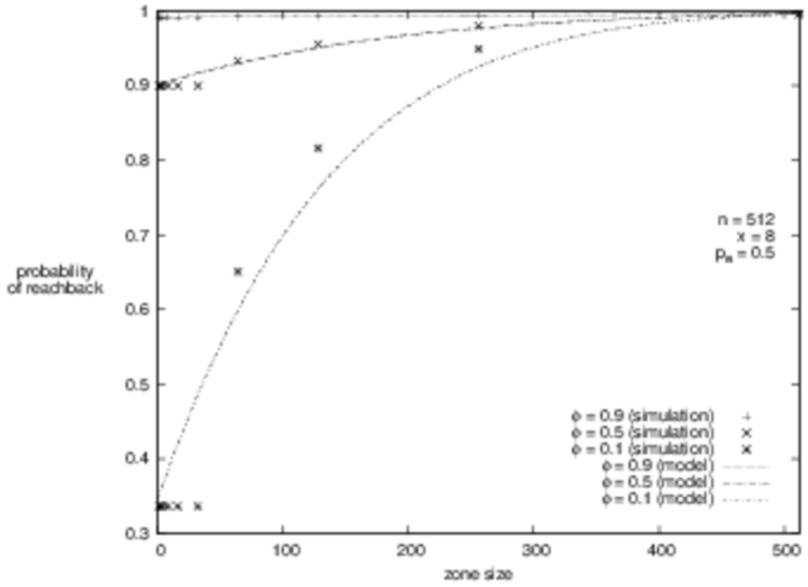
Results: Impact of Zone Size and External Ports





Results: Impact of Zone Size and Porosity





Parameter Estimation

Sandia National Laboratories

- Probability an Exploit Exists
  - Simple
    - $p_e = \frac{\text{vulnerable hosts}}{\text{hosts scanned}}$
  - Weight Host Vulnerabilities
    - $p_e = \sum_i \frac{s_i}{s\text{max}}$
- Porosity
  - Simple
    - $\phi = \frac{\text{ports open}}{\text{total ports}}$
  - Weight by Port's History of Exploitation
    - $\phi = \frac{\sum_i w_i o_i}{\sum_i w_i}$

Conclusions

- Technology Transfer Obstacles are Diminishing
- Future Work
  - Dynamic Zones
  - Intrazone Porosity
  - Per-boundary Porosity
  - Time Impact
  - Host Remediation

Recap

Sandia National Laboratories

- Cyber Security Concept of Operations
- Threat Model
- Metrics of Interest
- Closed-Form Mathematical Model
- Simulation
- Results
- Parameter Estimation
- Conclusions

Refining the Foundations for Cyber Zone Defense

Robert Mitchell
rrmitch@sandia.gov
703.597.3730

Sandia National Laboratories

Exceptional service in the national interest

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP