SAND2016-11417C

Parameterizing Moving Target Defenses

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

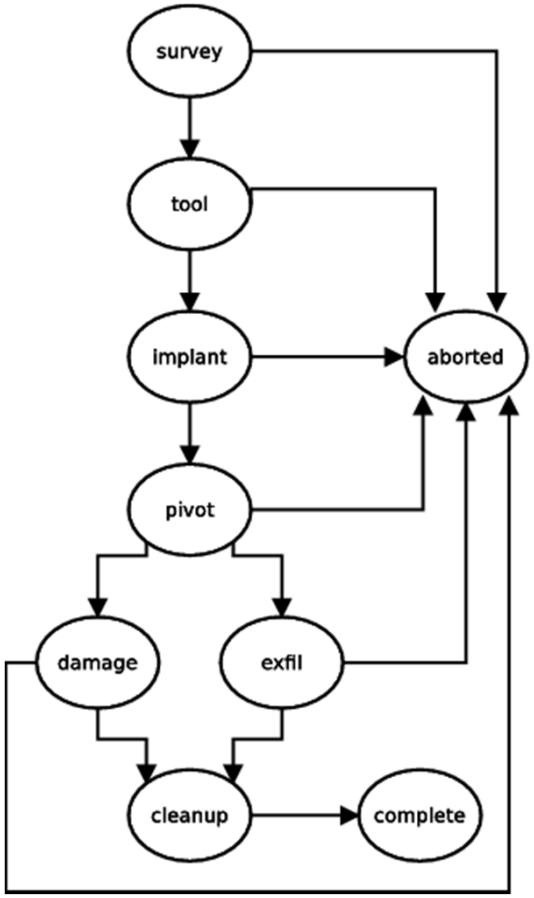
Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

Agenda

Sandia National Laboratories

- Phases of a Cyber Attack
- Threat Model
- Parameters
- Closed-Form Mathematical Model
- Stochastic Petri Net
- Results
- Conclusions

Phases of a Cyber Attack



Threat Model

Sandia National Laboratories

- Persistent Attacker
- Attacks Can Pause and Resume
- Attacker Must Implant Malware
- Detection and Attribution will Deter Attacker

Parameters

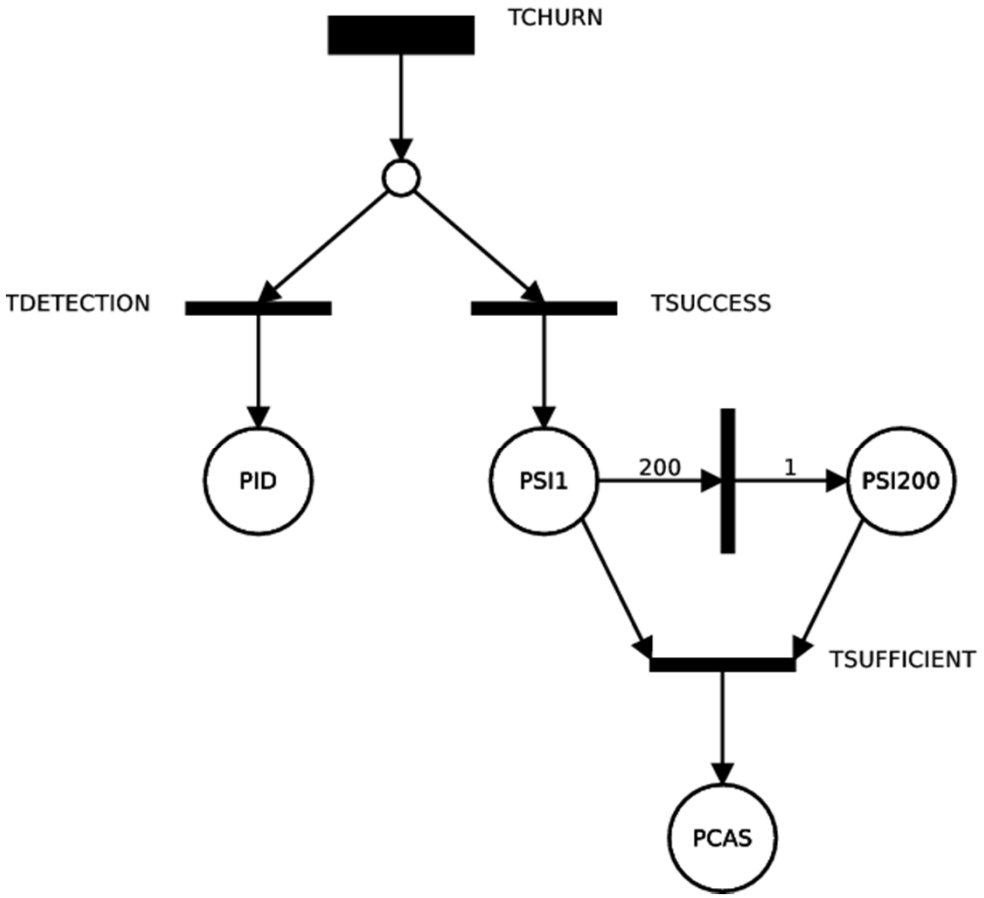
- Metric of Interest
  - a = probability of cyber attack success
- Input Parameters
  - e = probability an exploit is available for a configuration
  - o = number of configurations
  - p = probability of implant detection
  - c = cyber attack length
  - h = moving target defense churn time

Closed-Form Mathematical Model

Sandia National Laboratories

- a = P(exploit is available ∩ all implants are successful)
  = P(exploit is available)
  · P(all implants are successful)
  $= (1 - (1 - e)^o)(1 - p)^i$
- i = number of implants required
  = total number of churns
  · expected churns before exploitable platform
  $= \left(\frac{c}{h}\right)\left(\frac{o}{2}\right)$

Stochastic Petri Net



SPN Transitions

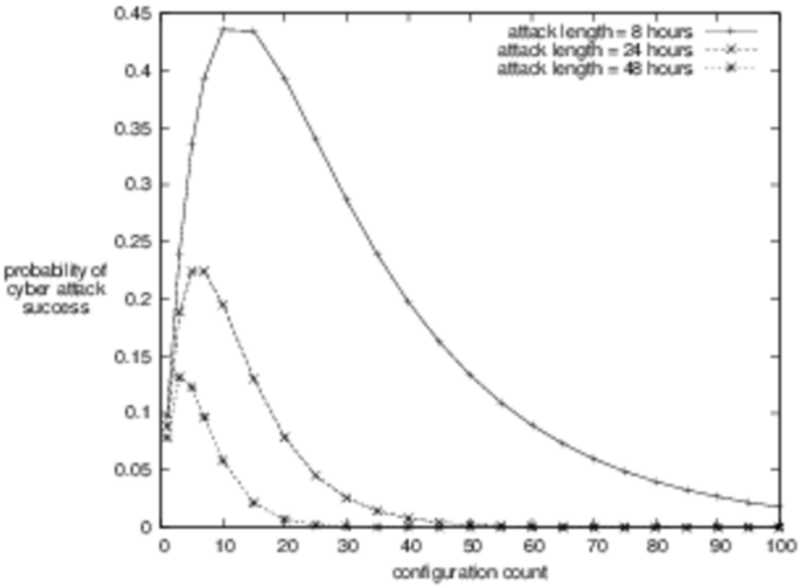
Sandia National Laboratories

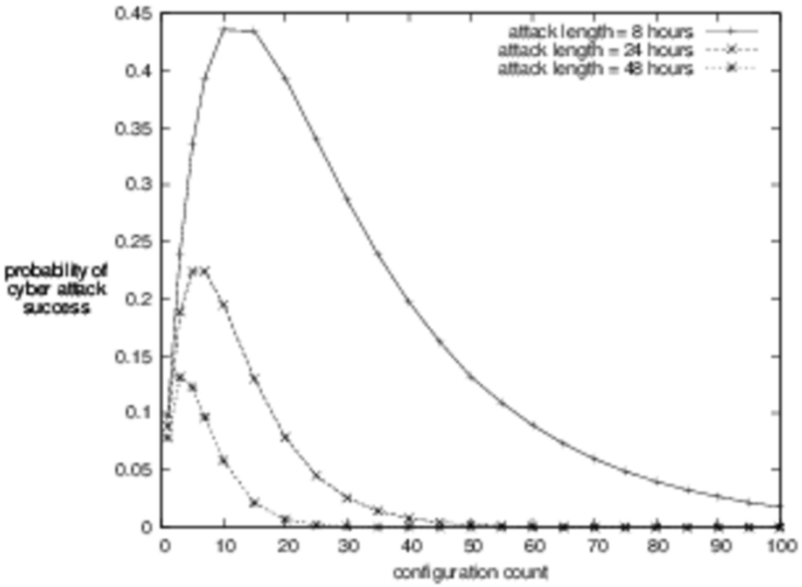
Name	Type	Description	Value
TCHURN	rate	MTD churn rate	$\lambda = 1/h$
TDETECTION	probability	probability implant is detected	p
TSUCCESS	probability	probability implant is not detected	$1 - p$
TSUFFICIENT	multi-immediate	successful implants required to complete mission	$\left(\frac{c}{h}\right)\left(\frac{o}{2}\right)$

Results

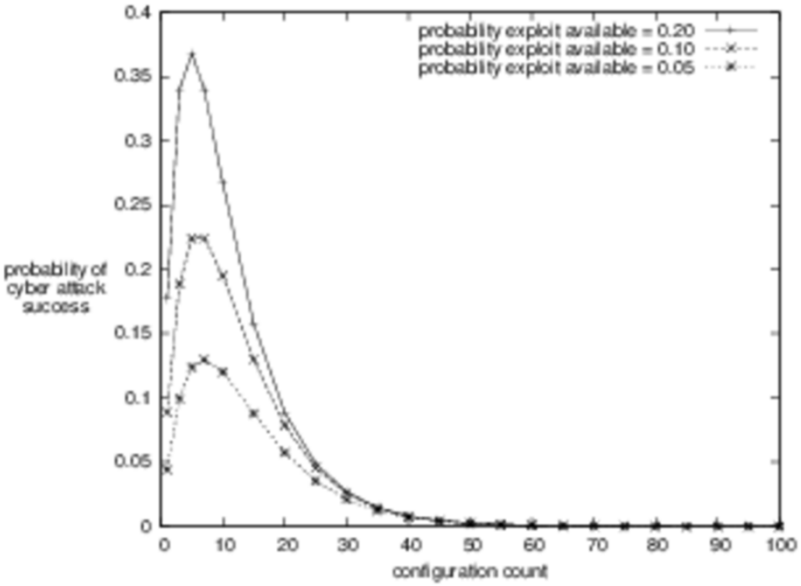
- One Dependent Variable: a
- Five Independent Variables: o, c, e, h and p

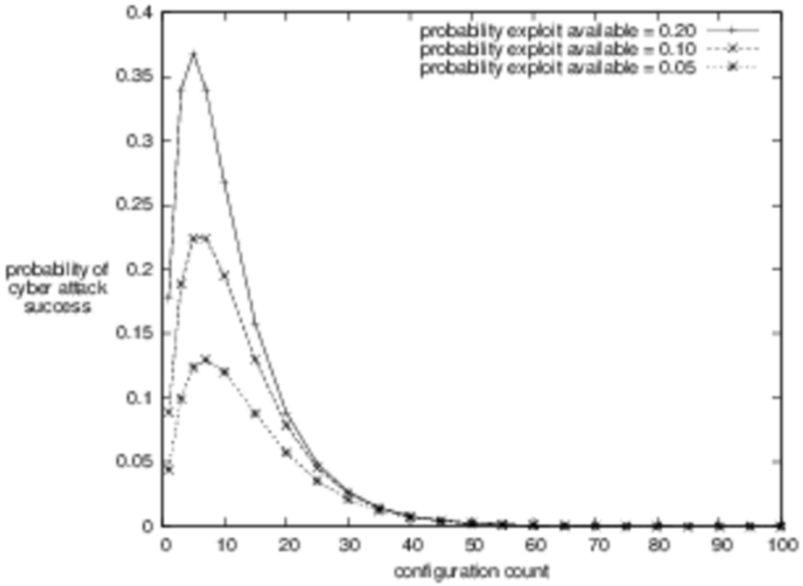
Results: Impact of Configuration Count and Attack Length



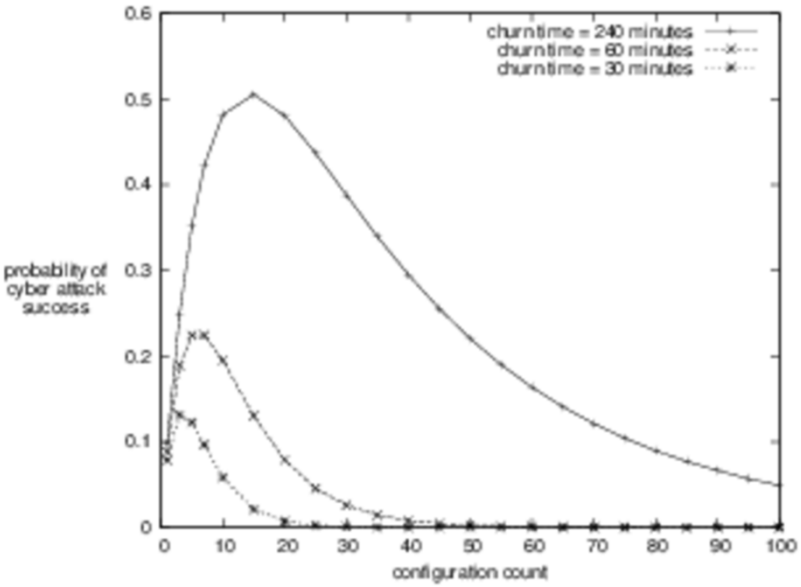


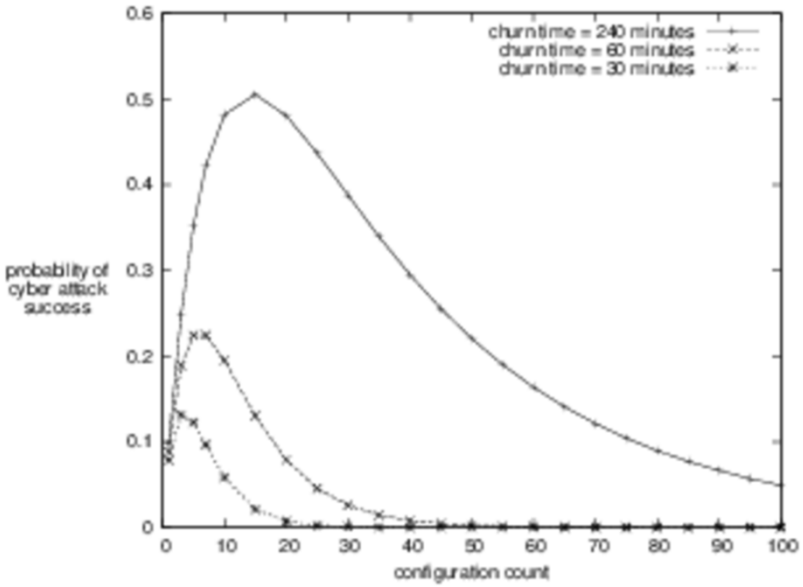
Results: Impact of Configuration Count and Exploit Availability



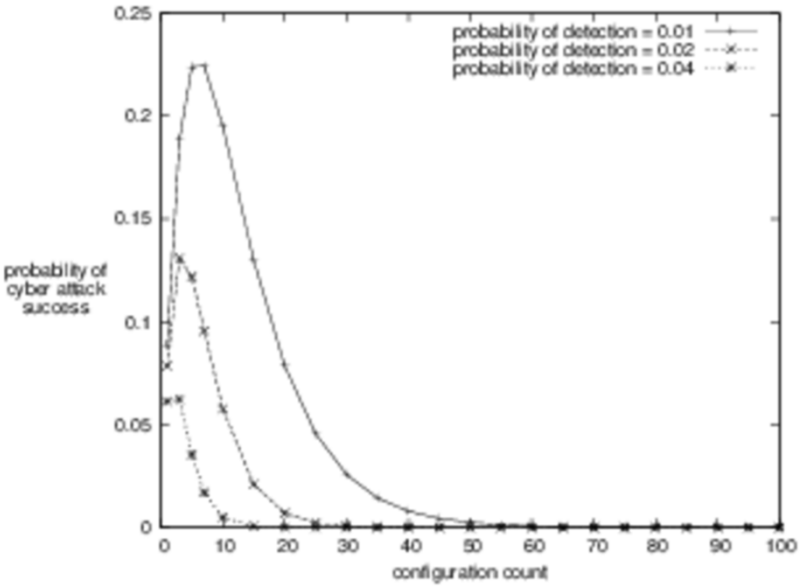


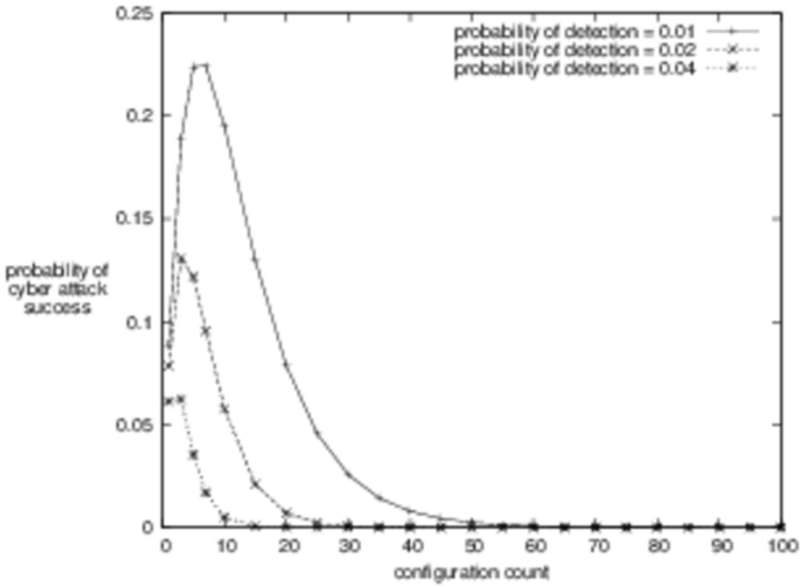
Results: Impact of Configuration Count and Churn Time





Results: Impact of Configuration Count and Implant Detectability





Conclusions

Sandia National Laboratories

- Candidate Models for One Brand of MTD
- Future Work
  - Simulate or Emulate Actual Dynamic Platform Techniques
  - Relax Assumptions:
    - Non-uniform Distributions of Configurations
    - Different e For Each Configuration
    - Implant Not Required
    - Detection and Attribution May Not Deter Attacker
  - Derive Models for non-DPT MTDs

Recap

Sandia National Laboratories

- Phases of a Cyber Attack
- Threat Model
- Parameters
- Closed-Form Mathematical Model
- Stochastic Petri Net
- Results
- Conclusions

Parameterizing Moving Target Defenses

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