SAND2017-0030C

Recent Cyber Security Events and Future Research Directions

Robert Mitchell
rrmitch@sandia.gov

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

- Where I Work
- Recent Cyber Security Events
- Future Research Directions

Where I Work

Sandia National Laboratories

Recent Cyber Security Events

Sandia National Laboratories

- Ukraine Power Grid Attack
- United States Democratic National Committee Hack
- Banner Health Private Data Spill
- Dyn Domain Name System Distributed Denial of Service
- San Francisco Municipal Transportation Agency Ransom

Ukraine Power Grid Attack

Sandia National Laboratories

- December 2015
- Computer network attack (CNA)
- State sponsored
- 230,000 customers lose power for up to 6 hours
- Supervisory Control and Data Acquisition (SCADA) target
- BlackEnergy and KillDisk
- Cyber warfare units are the new little green men
- Malware recycling disrupts attribution

United States Democratic National Committee Hack

Sandia National Laboratories

- Two campaigns began in Summer 2015 and April 2016
- Computer network exploitation (CNE)
- State sponsored
- Interfered with the election of the leader of 319M people
- Sea Daddy, X Agent and X-Tunnel
- Sometimes state sponsored actors make mistakes

Banner Health Breach

- June 2016
- Computer network exploitation (CNE)
- Criminal
- Privacy of 3.7M customers compromised
  - Payment data and protected health information spilled
- Lateral movement
- Know your risk ($37M)

Dyn Domain Name System (DNS) Attack

Sandia National Laboratories

- October 2016
- Computer network attack (CNA)
- Ideologue or weapons test
  - Counter-attribution effort
- Many high profile servers had no DNS for 6 hours
- Mirai
- Internet of Things-based Distributed Denial of Service (DDoS)
- Things access our private data

San Francisco Municipal Transportation Agency Attack

- November 2016
- Computer network attack (CNA)
- Criminal
- $1,591,782 loss = 707,459 free rides × $2.25 average fare
- HDDCryptor
- 2112 hosts affected
- Ransomware
- Muni restored from backup instead of paying

Future Research Directions

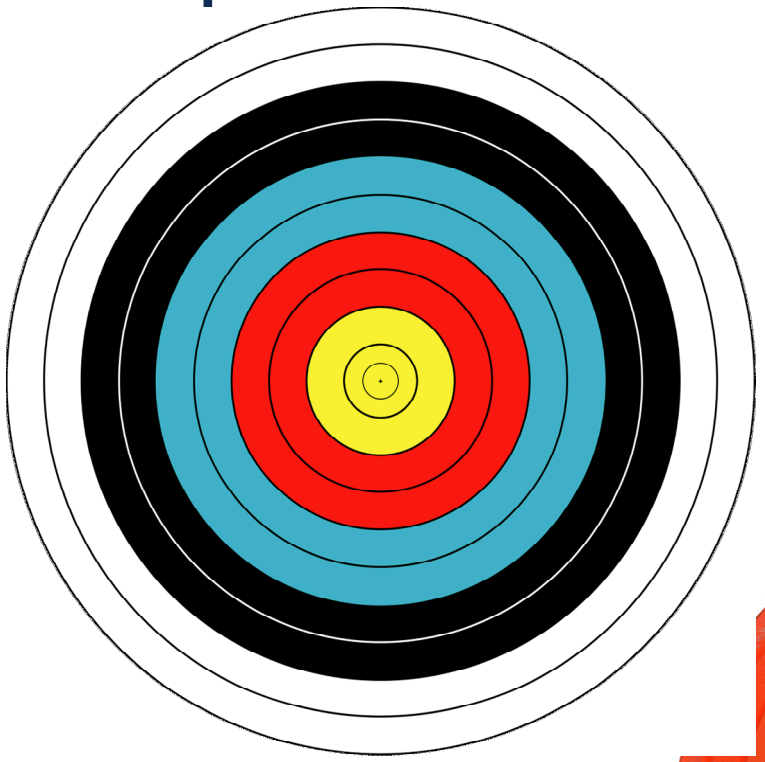
Sandia National Laboratories

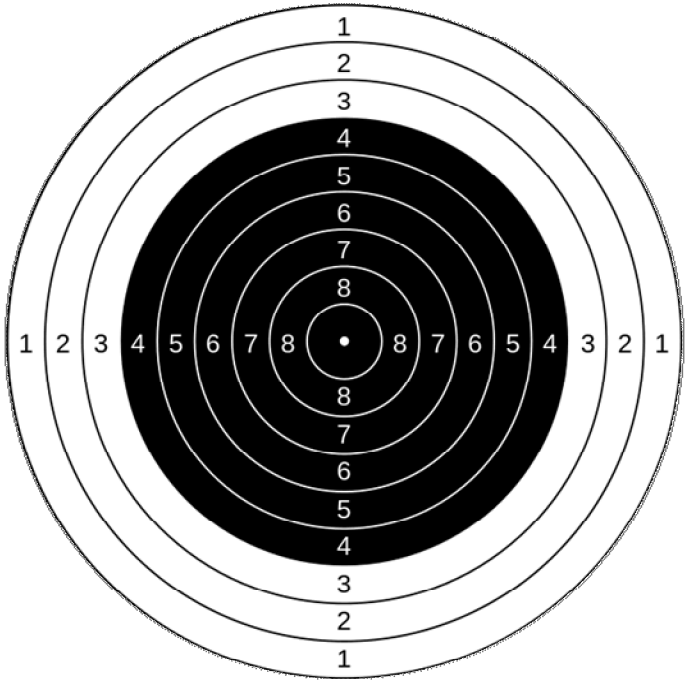
- Adjacent Disciplines
- Topics
  - Ransomware
  - Internet of Things
  - Intrusion Tolerance
  - Attribution
- Methods
  - Real Data Sets
  - Empiricism
  - Canonical, Complete and Orthogonal Metrics
  - Human Subject Research

Adjacent Disciplines

- All research areas are adjacent
  - Security is everyone's business
  - Don't become famous for the wrong reason

Topics




1 2 3 4 5 6 7 8 8 7 6 5 4 3 2 1
1 2 3 4 5 6 7 8 8 7 6 5 4 3 2 1


Remington
125
BLUE ROCK

Topics: Ransomware

Sandia National Laboratories

- Challenges
  - Victims are paying
  - Fast, strong encryption
  - Intuitive solution
- Opportunities
  - 100% recovery
  - Restoring from backup is painful
  - Attribution
  - Related topics
    - Cloud computing
    - Dynamic platform techniques

Topics: Internet of Things

Sandia National Laboratories

- Challenges
  - Can be repurposed
  - Life-critical Things
  - Limited resources
  - Oligoculture
  - Patch rollout
  - Forgotten hosts
  - Privacy
- Opportunities
  - Purpose-built devices are easy to profile
  - Purpose-built devices are easy to lock down
  - Physical access can enhance authentication

Topics: Intrusion Tolerance

- Challenges
  - Optics
  - Increases friction for legitimate users
  - Existing work is mostly intrusion response
- Opportunities
  - Related topics
    - Cyber zone defense
    - Moving target defense
  - Disrupt unseen attacks
  - Establish resilience as a goal

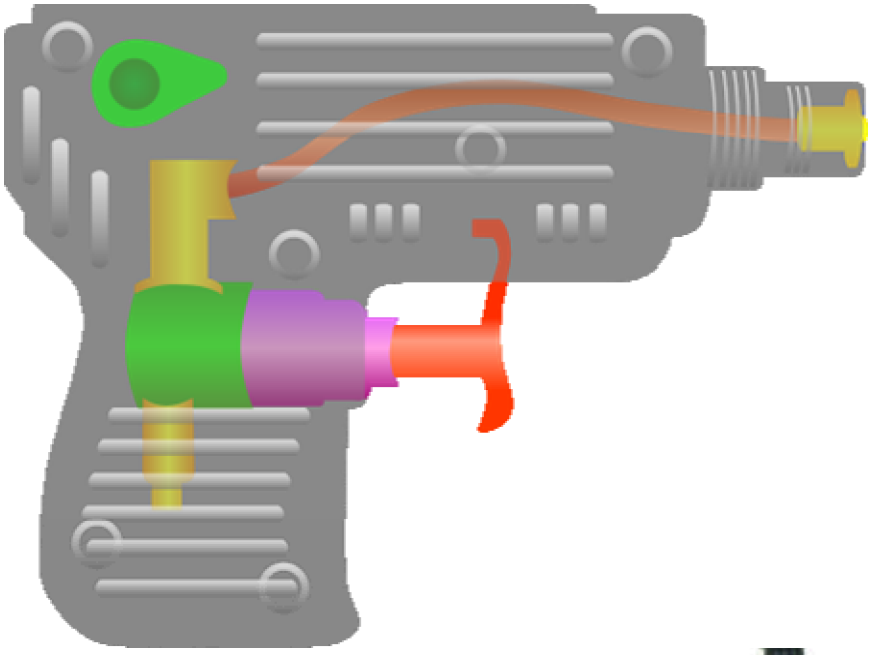
Topics: Attribution

Sandia National Laboratories

- Challenges
  - CNA adversaries
  - Network-based indicators
  - Attackers can tidy up
  - Antagonists can change techniques
  - Recycling programs
- Opportunities
  - CNE adversaries
  - Host-based evidence
  - Snap artifacts before attackers pick them up
  - Extract features from artifacts and tradecraft
  - Reduce asymmetry

Methods

Sandia National Laboratories



Methods: Begin with Real Data

- Challenges
  - Some institutions won't share
    - Publicly-traded companies
    - Governments
  - Professional attackers won't play
- Opportunities
  - Some institutions will share
    - National laboratories
    - Universities
  - Pen testers will play

Methods: Empiricism

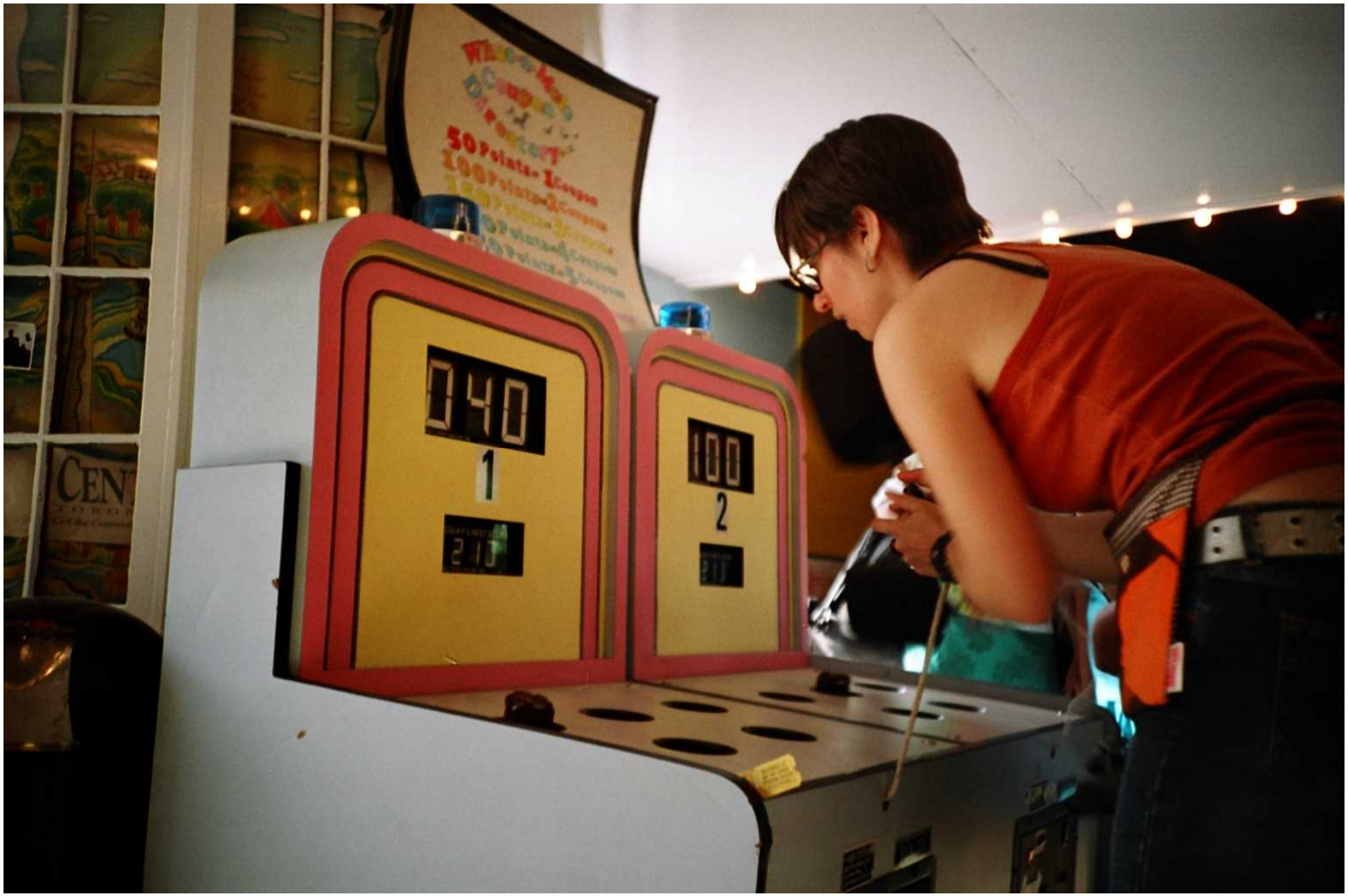
- Challenges
  - Derive models
  - Instrument simulations
  - Carry out experiments
- Opportunities
  - Statistical analysis
  - Compare related studies
  - Visualize relationships

Methods: Canonical Metrics

Sandia National Laboratories

- Challenges
  - Measure the attacker
  - Measure the defender
  - Achieve consensus
- Opportunities
  - Support practitioners
  - Meta-analysis

Methods: Human Subject Research



Methods: Human Subject Research

Sandia National Laboratories

- Challenges
  - Institutional review boards
  - Humans are hard to measure
  - Interdisciplinary research is hard
- Opportunities
  - Bypass Whac-A-Mole
  - External validation and generalizability
  - Linkography
  - Detect cyber rangers who “live off the land”

Outro

Sandia National Laboratories

- Where I Work
- Recent Cyber Security Events
- Future Research Directions

Recent Cyber Security Events and Future Research Directions

Robert Mitchell
rrmitch@sandia.gov

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