SAND2012-7253C

Machine-Oriented Biometrics and Cocooning for Dynamic Network Defense

Late-Start LDRD

September 5, 2012

Jason Haas

PI: J.D. Doak

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.

Failures of Current Defenses

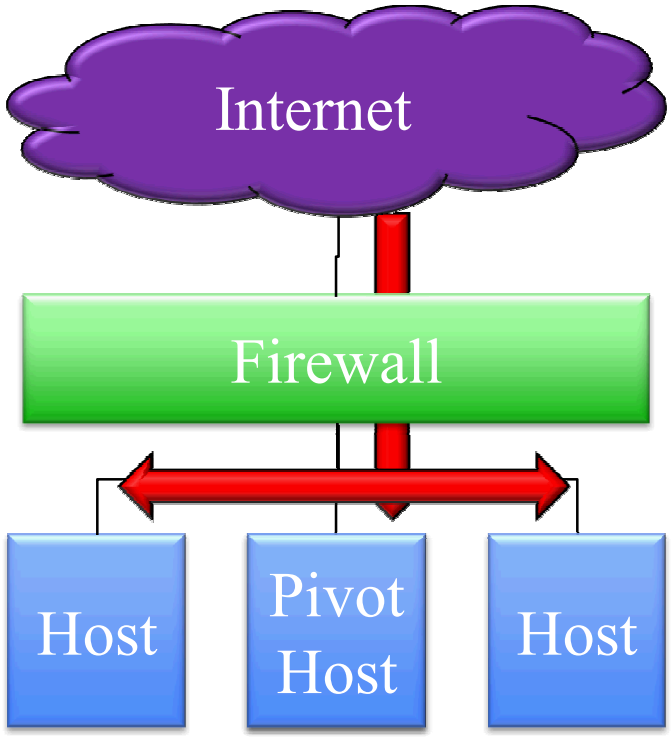
- Defense-in-depth – shallow
- Perimeter focus
  - Firewalls, intrusion detection/prevention systems
  - Spam filters
  - **Static**
- Binary reaction – fully connected or disconnected
  - More evidence required
  - Human time scales
  - Large variance in calculation of expected cost
- Honeypots
  - Low fidelity
  - Different threat focus

Focus – Dynamics

- Automation
  - React faster than human analysts
  - Incremental evidence leads to non-binary decisions
- Anomaly detection – machine-oriented biometrics
- Deception
  - Hide sensitive information
  - Delay attacker progress
- Introspection
  - Observe attackers tools, techniques, and procedures
  - Captive environment to reduce risk to production environment

Threat Model

- Longitudinal movement (agnostic) – entry mechanism (e.g., spearphishing, drive-by download)
- Lateral movement (focus) – moving from one host to another on a network, attacker gaining a greater foothold
- Attacker goals
  - Stealing information
  - Establishing a greater presence on target network



Motivating Scenario

- Windows
  - Remote procedure call (RPC)
  - Server message block (SMB) – file and printer sharing

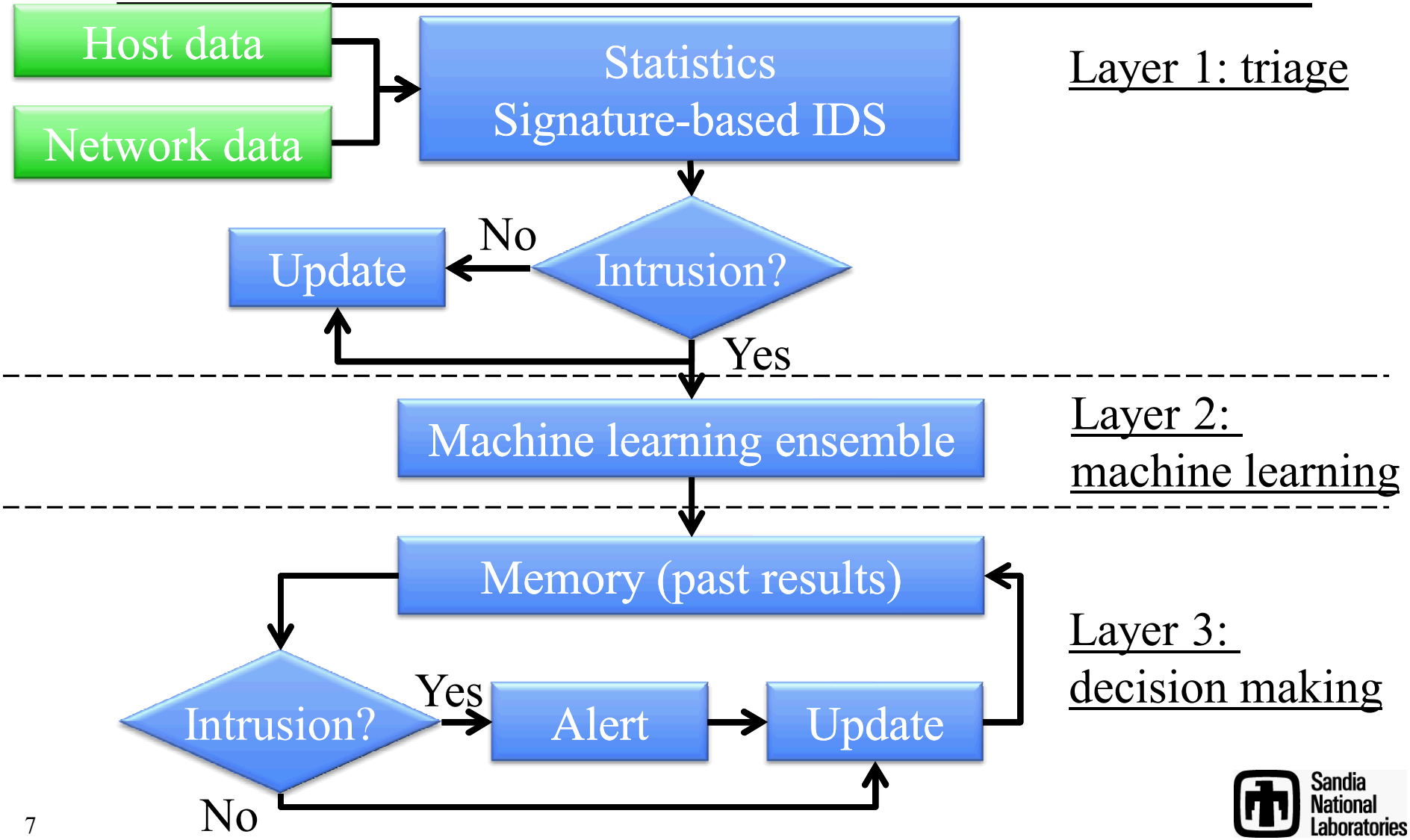
- Stuxnet
  - Lateral movement mechanism
  - Communication mechanism

Approach

- Machine-oriented biometrics – anomaly detection
  - Machines have normal patterns separate from users
  - Malicious behavior distinguishable from benign

- Cocooning
  - Use software-defined networking to switch service access
  - Per-service switching
  - Real versus emulated services
  - Introspection
    - Instrument emulated service
    - Observe attackers

Machine-Oriented Biometrics – Architecture



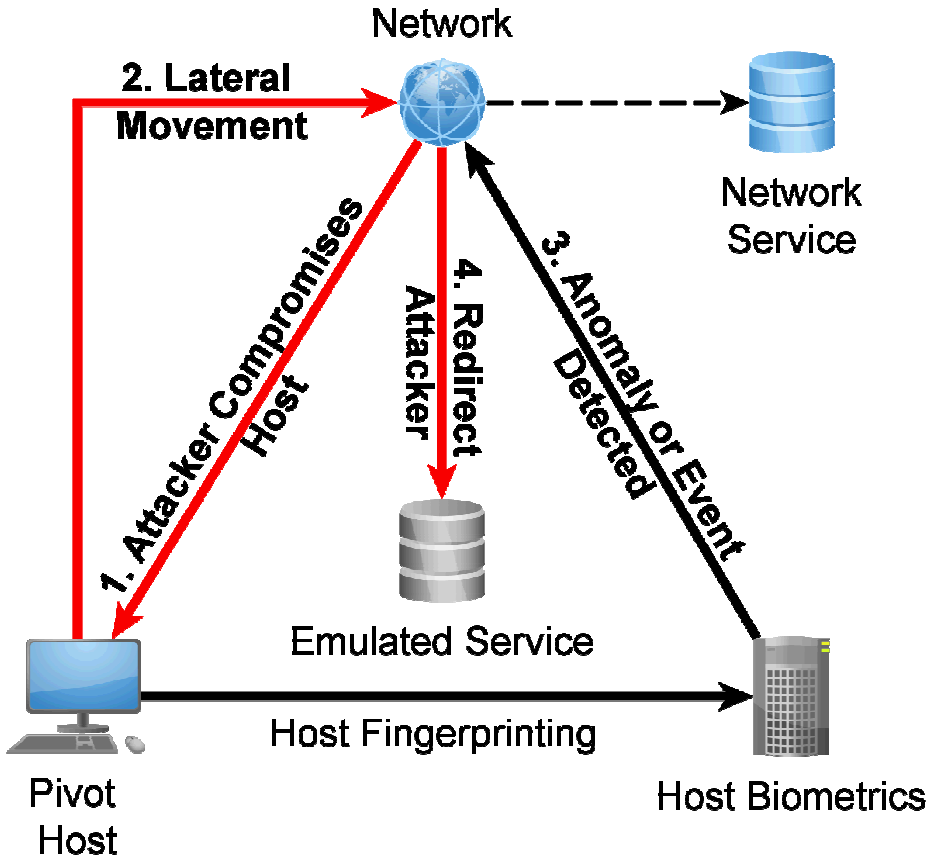
Sandia National Laboratories

Machine-Oriented Biometrics – Implementation

- Layer 1 – triage – Bloom filters, custom analysis
- Layer 2 – machine learning (ML)
  - Artificial neural network, support vector machine, density-based clustering, decision tree
  - Training data – normal and malicious
    - Wireshark, ProcMon
    - Metasploit
- Layer 3 – decision making
  - Evolutionary algorithm
  - Incorporates ML ensemble and signature based results
  - Initiates switch

Cocooning – Architecture

- Host biometrics initiates trigger
- Emulate real network service
  - Indistinguishable to attacker
  - **Must not be exact copy**
- Emulated service instrumented
  - Separate from real network
  - Observe attacker's tool and behavior



Cocooning – Implementation

- Trigger – client/server python script
- Switching – OpenFlow using built-in flow controller
- Services
  - Real – Bare-metal Ubuntu, Windows 7
  - Emulated – Xen Ubuntu, Windows 7 VMs on Ubuntu
- Introspection
  - LibVMI – access to Xen VMs
  - Volatility – provides higher-level access/understanding

Demonstration

- Tested services
  - Apache HTTP on Ubuntu
  - File sharing (SMB) on Windows 7

- Systems issues – lessons learned
  - ARP
  - NetBIOS, RPC

Evaluation

- Metrics development
  - Machine-oriented biometrics
    - Performance – latency, memory requirements
    - Accuracy – false positive/negative rates
  - Cocooning
    - Effectiveness – how effectively is an adversary deceived?
    - Similarity – how indistinguishable are the two services?

Evaluation – Effectiveness Metrics

- Goals – deceive, delay
- How long does an adversary spend in the cocoon?
- How many tools do we observe per time period or attack?
- How much less information is lost per time period or attack?
- Experimentation or deployment required

Evaluation – Similarity Metrics

- Observation – services must not be exactly the same just indistinguishable
- Network stack similarity
  - Some required for switching operation (e.g., MAC/IP address, TCP port)
  - Application type and version number
  - Side-channel information (e.g., TCP round-trip time, throughput, network stack fingerprinting)
- Destination
  - Attacker expects to land on a machine
  - Host content must not be sensitive but interesting

Summary

- Implemented a tool to delay, deceive attackers moving laterally on a network
- Demonstrated ability to switch commonly attacked services
- In progress
  - Full implementation of machine-oriented biometrics
  - Instrumentation
  - Metrics development and evaluation
- Future work
  - Deployment for testing
  - Integration with other tools for better fidelity

Thanks – Questions?

Sandia National Laboratories