INFORMATION OPERATIONS & SECURITY

5 MAR 2012

DR. ROBERT HERKLOTZ
PROGRAM MANAGER
AFOSR/RSL
Air Force Research Laboratory
**Report Title:** Information Operations & Security

**Performing Organization:** Air Force Research Laboratory, Wright-Patterson AFB, OH, 45433

**Report Date:** 05 MAR 2012

**Dates Covered:** 00-00-2012 to 00-00-2012

**Distribution/Availability Statement:** Approved for public release; distribution unlimited

**Supplementary Notes:** Presented at the Air Force Office of Scientific Research (AFOSR) Spring Review Arlington, VA 5 through 9 March, 2012

**Security Classification:**
- a. Report: unclassified
- b. Abstract: unclassified
- c. This Page: unclassified

**Number of Pages:** 40

**Limitation of Abstract:** Same as Report (SAR)

**Sponsor/Monitor’s ACRONYM(S):**

**Sponsor/Monitor’s Report Number:**

**SPONSOR/MONITOR’S REPORT NUMBER(S):**

**STANDARD FORM 298 (Rev. 8-98)**

Prescribed by ANSI Std Z39-18
NAME: DR. ROBERT HERKLOTZ

BRIEF DESCRIPTION OF PORTFOLIO:
Fund science that will enable the AF and DOD to dominate cyberspace: Science to develop secure information systems for our warfighters and to deny the enemy such systems.

LIST SUB-AREAS IN PORTFOLIO:
1: SOS-Science of Security
2: Secure Humans
3: Secure Networks
4: Secure Hardware
5: Covert Channels
6: Execute on Insecure Systems
7: Secure Data
8: Secure Systems-Security Policy
### MOTIVATION

- Cyber Security basic research has the potential to change the current balance that favors the attackers.
- Discovery and development of a Science of Cyber Security (SOS) should be vigorously pursued.
- Develop methods to execute mission while under attack.

### TECHNICAL IDEAS

- Science of Security: formally model relationships between attacks, defenses and policies and invent good metrics.
- Develop a theory of Covert Channels.
- Pursue methods to execute mission on insecure components.

### PICTURE

![Diagram showing relationships between attacks, defenses, and policies.](image)

### PAYOFF

- Inherently secure software and hardware systems can be deployed in the future.
- Covert channels can be anticipated and denied or used.
- Insecure, distributed systems can be used to execute the mission.
SOS Laws: Analysis and Synthesis

• Science:
  – Laws or theories that are predictive

• Analysis: Given an artifact, predict its properties…
  – Qualitative properties: What it does?
  – Quantitative properties: How well?

• Synthesis: Compose artifacts with given properties to obtain a new one with predictable properties.
SOS: Laws about What?

• Features:
  • Classes of policies
  • Classes of attacks
  • Classes of defenses

• Relationships (\(= \text{SoS}\))
  • Defense class D enforces policy class P despite attacks from class A.
Anupam Datta (CMU)
Joe Halpern (Cornell)
John Mitchell (Stanford, PI)
Andrew Myers (Cornell)
Andre Scedrov (U Penn)
Fred Schneider (Cornell)
David Wagner (UC Berkeley)
Jeannette Wing (CMU)
Ittai Abraham (Microsoft Research, unfunded collaborator)

Stanford, Berkeley, Carnegie-Mellon, Cornell, U Penn
SOS MURI Goals

• Scientific objective
  – Advance the science base for trustworthiness by developing concepts, relationships, and laws with predictive value.

• Technical approach
  – Security modeling: characterize system, threats, and desired properties. Leverage game-theoretic concepts to model incentives for the defender and attacker.
  – Composition: develop principles for explaining when security schemes compose, and how to achieve compositionality.
  – Security Measurement: goals include determining relative strengths of defense mechanisms, evaluating design improvements, and calculating whether additional mechanism is warranted based on attacker and defender incentives.
Science Base for Evaluation and Characterization of System Trustworthiness-SOS Metrics

Fred B. Schneider
Department of Computer Science
Cornell University
Ithaca, New York
Kinds of Analysis Laws

• **Analysis**: Given an artifact, predict its properties…
  – Qualitative properties: What it does.
  – Quantitative properties: How well it works.

• **Synthesis**: Compose artifacts with given properties to obtain a new one with predictable properties.
The Promise of Security Metrics

• **Users**: Purchasing decisions
  – Which system is the better value?

• **Builders**: Engineering trade-offs
  – Select among different designs?

• **Researchers**: Evaluating new ideas
  – Basis for declaring success!

Fred B. Schneider, Cornell
“\( \mu \) is a security metric” should mean...

- \( \mu \): Systems \( \rightarrow \) Vals, where:
  - \( < \) is a partial order on Vals
    - … so theory applies to more “metrics”. E.g.,
      \( \mu(S) = \{ \text{all attacks that compromise } S \} \)
  - \( \mu(S) \) is efficiently computable
  - \( x < y \) is efficiently computable

Intent: \( < \) reflects “actual security”, so

\( \mu(S) < \mu(S') \) means S is less secure than S’
Properties of Security Metrics

Define: \( S \ll S' \) – \( S \) is “less secure than” \( S' \)

**Soundness of \( \mu \):** (Useful for users)
\[ \mu(S) < \mu(S') \quad \text{implies} \quad S \ll S' \]

**Completeness of \( \mu \):** (Useful for engineers)
\[ S \ll S' \quad \text{implies} \quad \mu(S) < \mu(S') \]
If \( S \ll S' \) holds then …

\( S, S' \) must implement “same” specification:

- Specification defines an interface.
  - All interactions with the system involve actions in this interface.
    E.g., Includes side-channels.
- Specification describes expected effects of actions at the interface.

An attack is an input that causes the specification to be violated.
The $64,000 Question!

For what classes of specifications do there exist sound (and complete?) security metrics?

Conjecture:

- Expressive specs IMPLY security metric $\mu$ must be undecidable or $\mu$ incomplete.
- Security metric $\mu$ decidable and soundness IMPLY $F$ expressiveness is bounded by static type checking.
Non-Intrusive Media Forensics Framework

K. J. Ray Liu and Min Wu

Department of Electrical and Computer Engineering
University of Maryland, College Park
Digital Multimedia Anti-Forensics

- Very little consideration has been given to **anti-forensic operations**
  - Designed to remove/falsify intrinsic fingerprints
  - Create undetectable forgeries

- **The study of anti-forensics is**
  - Identifies weaknesses in existing forensic techniques
  - Important for the development of tools to detect the use of anti-forensic operations
ENF: A Ubiquitous and Natural Fingerprint

- **ENF**: Electrical Network Frequency
  - 60 Hz in North America, 50 Hz elsewhere (50/60 Hz in Japan)
  - Electro-magnetic (EM) field from power grid interferes with electronic recording mechanisms (Sensors)

- ENF varies slightly from 50/60 Hz over time
  - Deviations depends on regulations: ~ on the order of 0.05-0.1Hz
  - Main trends are the same over the power grid [1]

- ENF can be “heard” and “seen”
  - Present in audio recordings near power sources
  - We showed luminance of indoor lightings fluctuates based on ENF
    - Captured by optical sensors: photo diode, CCD camera sensors, etc.
  - Random deviations can be used as fingerprints for multimedia content:
    - Determine the time and place of recordings
    - Detect tampering in the multimedia content; bind video and audio

---

Verify Time of Recording

- **Video ENF signal**
- **Power ENF signal**
- **Normalized correlation**

ENF matching result demonstrating similar variations in the ENF signal extracted from video and from power signal recorded in India

- **Aliasing Challenge with video:** temporal sampling rate lower than ENF
- **Our recent results from US, China, and India power grids**
  - Exploit signal processing to harvest from aliasing
  - **Highest correlation between power ENF and video ENF signal corresponds to the time at which recording took place**
Tampering Detection

ENF matching result demonstrating the detection of video tampering based on the ENF traces

- Adding a clip between the original video leads to discontinuity in the ENF signal extracted from video
- Clip insertion can also be detected by comparing the video ENF signal with the power ENF signal at corresponding time
Forensic Binding of Audio and Visual Tracks

- ENFs in audio and video tracks captured at the same time have high correlation

Research questions ahead:
(1) How to accurately estimate and match weak and noisy ENF?
(2) Can ENF be removed? Tampered?
(3) How to prevent anti-forensics on ENF? ……
High Performance Semantic Cloud Auditing

Keesook J. Han, Ph.D
Keesook.Han@rl.af.mil

Develop High Performance Semantic Cloud Auditing Technologies and Applications that includes Comprehensive Cloud Auditing Data Capturing, Analysis and Rapid Response to Improve Cloud Quality of Services.

Approved for Public Release; Distribution Unlimited: 88ABW-2011-4496, 16-Aug 2011
Cloud Research Facilities

University of Texas at San Antonio
- FlexFarm (Honeyfarm) & FlexCloud: Institute for Cyber Security

Texas A&M University
- Cisco Test Engineering Center
- Cisco Cloud Testing Lab

University of South Carolina
- Router Testbed: Center for Information Assurance Engineering

University of Texas at Dallas
- UTD Secure Cloud Repository: Hadoop File System

SUNY Binghamton University
- GPGPU Cluster: Real-Time Embedded Systems Lab

University of Illinois at Urbana Champaign
- Coordinated Science Lab Assured Assured Cloud Computing Center

Tennessee State University
- Center of Excellence in Information Systems and Engineering Management

Rochester Institute of Technology
- Networking, Security, and Systems Administration Labs

University of Pittsburgh
- Swanson Institute for Technical Excellence

University of Missouri Kansas City
- Networking & Multimedia System Lab

AFRL RI
- GPGPU Cluster: CONDOR Supercomputer

Georgia Institute of Technology
- Foundations of Data and Visual Analytics Center
Conclusion

- **Semantic Cloud Auditing:**
  - **Develop Efficient Information Theoretic Metadata and Aggregation:** Fast Information Exploitation of Massive Cloud Auditing Data for Rapid Response

- **Semantic Cloud Auditing will benefit to the following projects:**
  - **Access Control:** “Advanced Access Control for Assured Clouds”
  - **Cloud Security:** “Honeyfarm Data Capturing, Rapid Sharing and Exploitation of Malicious Traffic for Cloud Security”
  - **Customized Hadoop:** “Massive Cloud Auditing Using Data Mining on Hadoop”
  - **Secure Hadoop:** “Assured Information Storage and Sharing on Hadoop”
  - **GPGPU Computing:** “High Performance Processing of Cloud Auditing Data Using GPGPU Many-Core Parallelism”
  - **SLA-based Cloud Service Workloads:** “Dynamic Mapping of Cloud Resources to Meet Service Level Agreement (SLA)-based Cloud Service Workloads”
  - **Traffic Control:** “Router-Based Filtering and Rerouting to Traffic Control in Cloud Computing”
  - **Outage Management:** “Router-Initiated Network Outage Management for Multitenant Clouds”
  - **File Transfer:** “Bandwidth Intensive Multimedia Data Transfer for Smartphone-Friendly Cloud Services”
Detection of Covertly Embedded Hardware in Digital Systems

Douglas H. Summerville
Associate Professor
Electrical and Computer Engineering
State University of New York at Binghamton
Covertly Embedded Trojan

- Malicious circuit embedded in “implementation space” of its host
  - Neither functional nor parametric
- Trojan uses *existing resources* that are artifacts of the host’s implementation
- No alteration of functional characteristics of host, therefore not testable
- Can be combinational or sequential circuits
The Embedding

- Covert Hardware alters the circuit’s behavior in the “don’t care” space
- In effect, two circuits co-exist in the same physical hardware
  - The original circuit, only exercised during normal operation
  - The malicious circuit, exercised by special trigger
Motivating Assumption

- Assume general case is unsolvable
- In practice, standard design approaches generate a small fraction of possible implementations
- We focus on securing few practical cases
Structural Circuit Analysis

- Can’t look at circuit’s function, so look at its structure
- Exploits how design approaches optimize for speed, area, power, etc. in deterministic ways
  - Contributing regularity to circuit structure
- Identify structural characteristics of circuits that
  - Result from standard design approaches
  - Are removed or altered by tampering
- Restrict optimization to solutions in that space
  - tradeoff
Detecting Hidden Communications Protocols

R. R. Brooks
Associate Professor
Holcombe Department of Electrical and Computer Engineering
Clemson University
Clemson, SC 29634-0915
Tel. 864-656-0920
Fax. 864-656-1347
email: rrb@acm.org
Objective
Detect use of tunneled communications protocols and infer their current internal state
- Private communications often tunneled through virtual private networks (VPNs)
- Mix networks tunnel connections for anonymity
- Tunneling tools (ex. ssh, ssl, TOR) have timing vulnerabilities
- Hidden Markov models (HMM) and probabilistic grammars will detect protocol use, infer network flows, partially decipher content

DoD Benefit:
- Detection of tunneled communications protocols
- In some cases (ex. interactive ssh), partially decipher message contents
- Determination of communications patterns in mix networks, such as TOR
- Detection of timing side channel attack vulnerabilities in DoD networks

Technical Approach:
- Collect inter-packet timing information from tunneled sessions
- Zero-knowledge HMM model inference
- Determination of HMM statistical significance
- Tracking HMM transitions driven by network flow inter-packet timing data detects protocol use
- Viterbi algorithm finds maximum likelihood Markov state sequence
- Two point-to-point connections with same Markov state sequences (Viterbi paths) are likely data source and sink

Detection of Hidden Communications Protocols
Richard Brooks: rrb@acm.org, Clemson University

DISTRIBUTION A: Approved for public release; distribution is unlimited
Active Defense: Reactively Adaptive Malware: Attacks & Defenses

Kevin W. Hamlen & Latifur Khan
University of Texas at Dallas

AFOSR Contract FA9550-10-1-0088
September 2011
Attacks Upon Signature-matchers

• Randomize features during propagation
  – Polymorphism
    • encrypt payload with randomly chosen key
  – Oligomorphism
    • randomly re-assemble decryptor
  – Metamorphism
    • non-deterministically recompile decryptor and/or payload

• Weakness: Undirected mutation
Reactively Adaptive MALware (RAMAL)

• Three challenges:
  1. Covertly harvest data about victim defenses (malware signature databases)
  2. Mine harvested data effectively
  3. Derive new mutation strategy from inferred model
Hardware, Languages, & Architectures for Defense Against Hostile Operating Systems (DHOSA)

V. Adve, UIUC
K. Asanović, UC Berkeley
D. Evans, UVA
S. King, UIUC
G. Morrisett, Harvard
R. Sekar, U Stony Brook
D. Song, UC Berkeley
D. Wagner (PI), UC Berkeley

http://www.dhosa.org/
The Approaches

Advances that cut across traditional disciplines:

• new OS and software architectures
• new hardware architectures
• new policy enforcement techniques
• new techniques for trustworthiness
• new coding techniques
TRANSFORMATION

SVA

Binary translation and emulation

Formal methods

HARDWARE

Hardware support for isolation

Dealing with malicious hardware

WEB-BASED ARCHITECTURES

Cryptographic secure computation

Data-centric security

Secure browser appliance

Secure servers

SYSTEM ARCHITECTURES

e.g., Enforce properties on a malicious OS

e.g., Prevent data exfiltration

e.g., Enable complex distributed systems, with resilience to hostile OS’s

DISTRIBUTION A: Approved for public release; distribution is unlimited

John Knight
University of Virginia

AFOSR PI Meeting 9/21/2011
Helix Team Members

- University of Virginia
  - John C. Knight (PI) - Software engineering, dependability
  - Jack W. Davidson - Languages, security, virtual machine
  - David Evans - Security, applied cryptography
  - Westley Weimer - Program analysis
  - Anh Nguyen-Tuong - Security, grid computing

- University of New Mexico
  - Stephanie Forrest - Biological inspired computing
  - Jared Saia - Computational & game theory

- University of California at Davis
  - Hao Chen - Security, Web applications
  - Zhendong Su - Program analysis, software engineering
  - S. Felix Wu - System fault tolerance
  - Jeff Rowe - Operating systems
  - Karl Levitt - Security

- University of California at Santa Barbara
  - Frederic Chong - Secure hardware, hardware acceleration for program/system analysis

DISTRIBUTION A: Approved for public release; distribution is unlimited.
Research Highlights

• Security for mobile devices:
  – Static analysis framework for detecting information leaks (Android)

• Security for web applications:
  – Static analysis to detect access control vulnerabilities

• Security for applications:
  – Detection of unsafe component loading

• Automated repairs via genetic programming:
  – Demonstrated on assembly code
  – Proactive diversity/variant generation

• Hardware/architecture for security:
  – Hardware description language (compiler released)
  – Provably leak-free hardware

See web site: http://helix.cs.virginia.edu