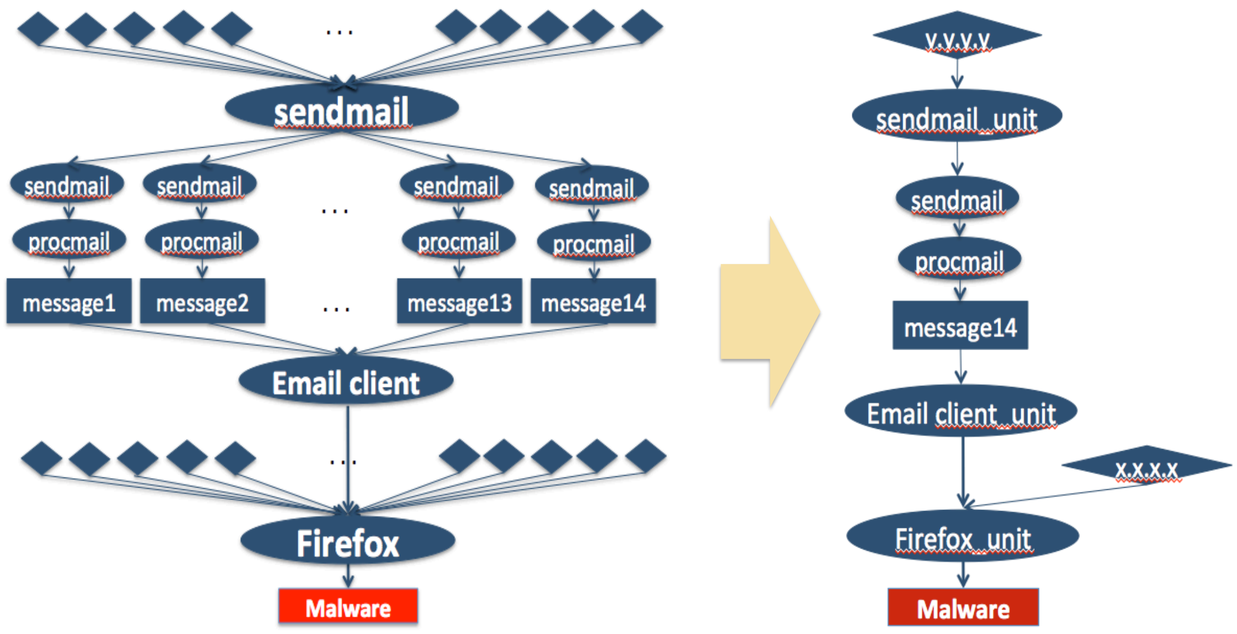
# Binary-Centric Forensic Analysis of Advanced Cyber Attacks Against Enterprise Environments

Dongyan Xu (PI)*, Xiangyu Zhang*, Golden G. Richard III**
*Purdue University, **University of New Orleans

Emerging cyber attacks such as **Advanced Persistent Threats (APTs)** pose significant threat to enterprises. Such attacks are often stealthy, low-and-slow, and disguised via deceptive campaigns. This research focuses on developing advanced **binary analysis and instrumentation** techniques for **holistic forensics** of advanced cyber attacks against enterprise infrastructures and assets.

## Temporal Forensics

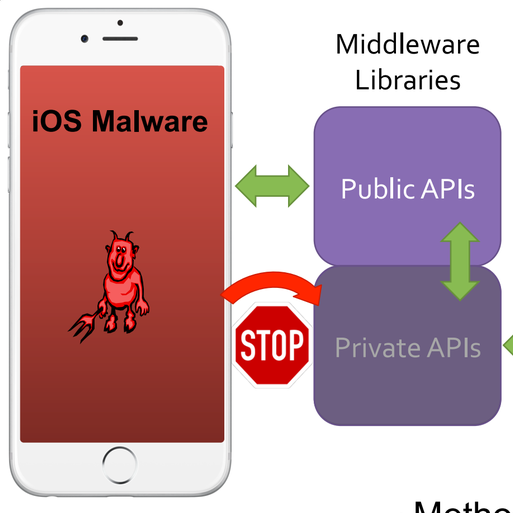



**Goal**: Reveal an Attack's Initial Entry and Ramifications via Log-Based Causal Analysis

**Challenge**: Traditional System-Level Causality Tracking Causes *Dependence Explosion*

**Solution**: Partition Program *Execution* and *Data* into Fine-Grain *Units* to Enable *Efficient, High-Accuracy Causality Tracking* (publications at NDSS'16 and ACSAC'16)

## Malware Forensics




Privacy-Critical Resources

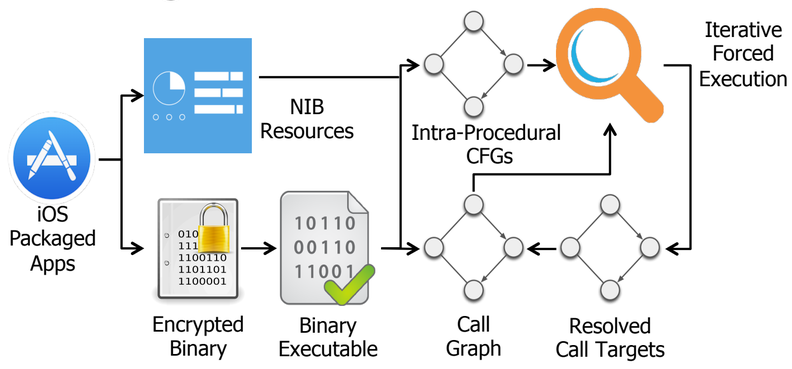
- Serial Number
- IMEI
- Installed Apps
- Battery ID
- Camera ID

Method Selector = String

```
objc_msgSend ( obj, "access", param );
```

```
char sel[3];   strcpy ( sel, "acc" );   strcat ( sel, "ess" );
objc_msgSend ( objc, sel, param );          + Encryption
                                            + Obfuscation
```

**Observation:** Stealthy iOS Malware Construct Attacks Though Obfuscated Private APIs



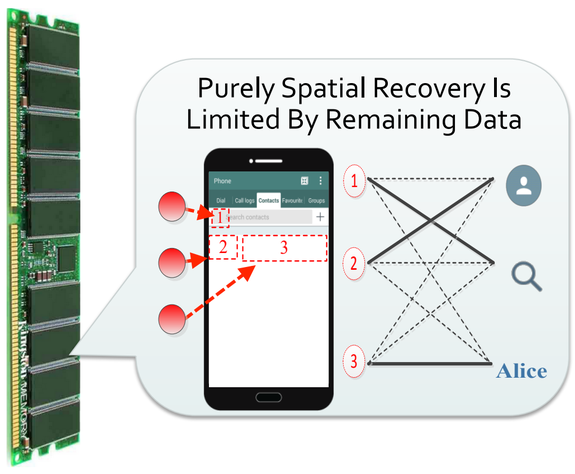

**Impact:** Lead To The Removal Of Hundreds Of Privacy-Violating Apps From Apple's App Store

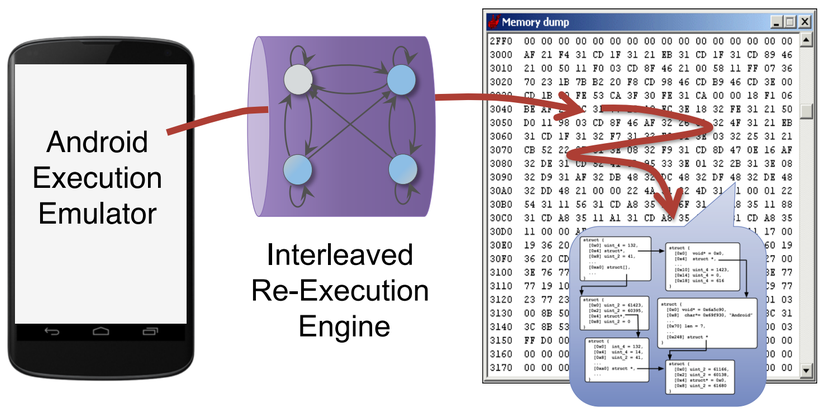
**Goal**: Efficiently Expose Private API Abuse During Automated App-Review

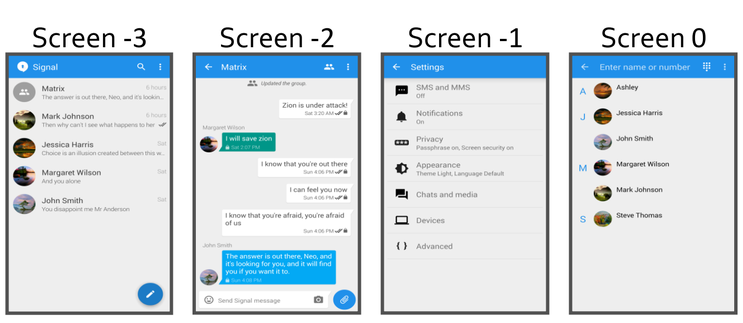
**Challenge**: Existing Analysis Techniques Have Limitations In Efficiency Or Complexity

**Solution**: Apply Iterative Forced Execution To Derive Private Method Selector Outcomes (publication at CCS'15)

## Spatial Forensics




**Goal**: Bridge The Recovery Of Purely Spatial And Spatial-Temporal In-Memory Evidence

**Challenge**: Application-Specific Data (e.g., chat strings, bank balances) Lack Semantic Ties

**Solution**: Retarget The Execution Of A Live Android App To Historic Temporal Data In A Memory Image (publications at CCS'15, USENIX Sec'16)

Interested in meeting the PIs? Attach post-it note below!

NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
Jan. 9-11th 2017
Arlington, VA

National Science Foundation
WHERE DISCOVERIES BEGIN

PURDUE UNIVERSITY
THE UNIVERSITY of NEW ORLEANS