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

CERIAS

Challenge:

- Stealthy cyber attacks (e.g., APTs) hard to investigate
- Attack evidence in multiple forms/aspects (e.g., logs, code, memory/disk images)
- No effective tools to correlate logs, analyze binary code and data

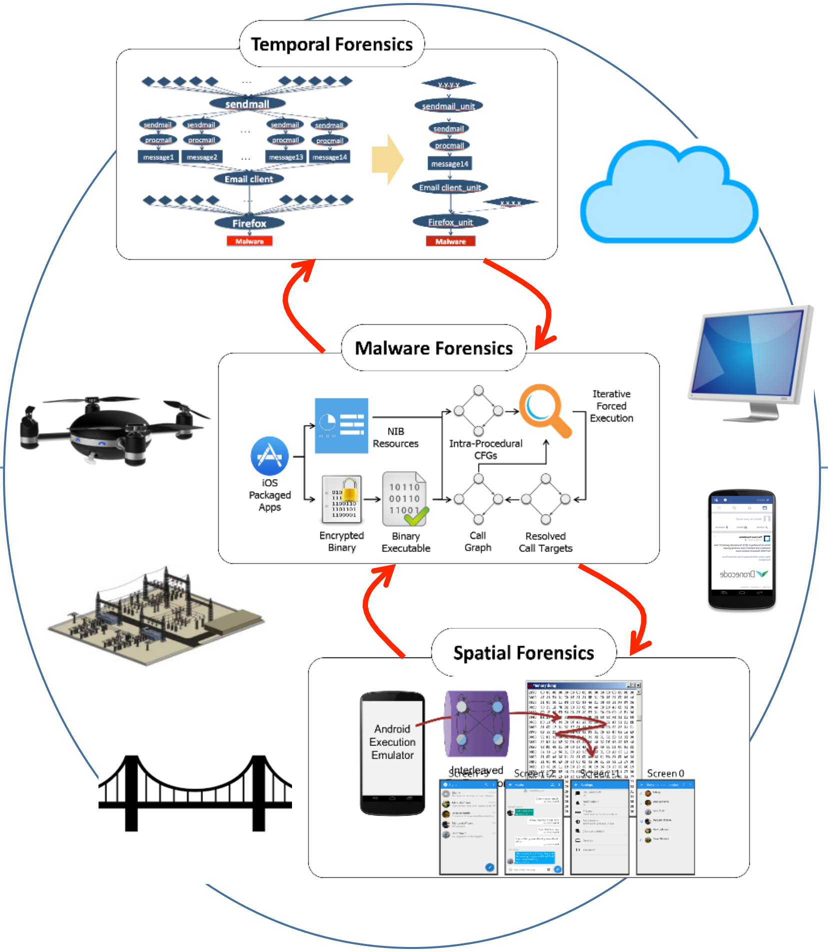
Solution:

- A framework of multi-aspect (temporal, spatial, and malware behavioral) cyber attack forensics
- A suite of advanced techniques for binary code analysis, instrumentation, and extraction

Purdue University (1409668)

University of New Orleans (1409534)

PI: Dongyan Xu (dxu@cs.purdue.edu)



Scientific Impact:

- A new, program analysis-driven paradigm for cyber forensics
- High-accuracy, low-overhead causal logging
- Forced-execution for hidden malicious logic discovery
- In-memory data re-rendering via binary code re-use/steering

Broader Impact:

- Help investigate (and prevent) cyber attacks or crimes
- Offer new digital forensics tools to law enforcement community
- Raise public (including K-12) awareness of cyber crimes and impacts
- Renovate cybersecurity and forensics curriculum