Behavioral Analysis for Intrusion Resilience

Ahmed Fawaz
Dec 6, 2016
Recent Cyber Attacks on Private and Public Entities
Traditional Security

- All Possible States
- Good States
- Initial State
- Reachable States

Diverse Monitoring
Secure Monitoring
Monitoring Fusion

Resiliency Approach

Good States

Reachable States

Initial State

All Possible States

Design for Resiliency

Diverse Monitoring

Secure Monitoring

Monitoring Fusion

Conclusion & Future
Cyber resilience is the ability to *identify, prevent, detect* and *respond* to malicious and random process or technology failures and recover—while maintaining an acceptable level of service.

Notional Architecture for Cyber Resiliency

- "World View" System Model
- Diverse System Monitoring
- Monitor Fusion
- Response Selection and Actuation
- Secure Monitoring and Response Infrastructure

OFFLINE/ONLINE COMPUTATION

ONLINE COMPUTATION

RESILIENCY INFRASTRUCTURE
Notional Architecture for Cyber Resiliency

“World View” System Model

Diverse System Monitoring

Monitor Fusion

Response Selection and Actuation

Secure Monitoring and Response Infrastructure

ONLINE COMPUTATION

RESILIENCY INFRASTRUCTURE

The system model represents:
- services
- possible responses
- attacker characteristics
- architecture of a system
Diverse monitors are deployed at all levels of the system to generate a diverse sensor data.

The sensor inputs, alerts, and logs feed into a different set of fusion and correlation algorithms to generate a higher-level alert.

**Notional Architecture for Cyber Resiliency**

- **OFFLINE/ONLINE COMPUTATION**
  - "World View" System Model
  - Diverse System Monitoring
  - Response Selection and Actuation

- **ONLINE COMPUTATION**
  - Monitor Fusion

- **RESILIENCY INFRASTRUCTURE**
  - Secure Monitoring and Response
Notional Architecture for Cyber Resiliency

The decision algorithm decides on learning responses to intensify and focus the monitoring resources, and/or effect a response strategy, e.g.:
- Block an attacker
- Move a target
- Reallocate services
- Recover services
The monitoring and response architecture provides a trustworthy infrastructure on which to implement resiliency services and maintain a trustworthy world view.
Kobra: A Kernel Monitoring Engine

“World View” System Model

Diverse System Monitoring

Monitor Fusion

Response Selection and Actuation

Secure Monitoring and Response Infrastructure

OFFLINE/ONLINE COMPUTATION

ONLINE COMPUTATION

RESILIENCY INFRASTRUCTURE
Problem Description

*How to use diverse data types to model application behavior for anomaly detection?*
Our Approach

Data Sources
- Processes
- File Operations
- Packets

System View

Signal

Learning

[Diagram showing a flow from data sources through system view, signal, and learning stages.]
Kobra’s Architecture

• Kernel-level monitor for Windows kernel

• Cooperative drivers that captures:
  • Network activity
  • Process communications
  • Process creation/termination
  • Objects access
  • File system activity

• Low-overhead
What is the **System View**?

- The intent of the system view is to provide high-level information about host state.

- Reflects the methods by which users and user processes access different resources.
File and Network behaviors

- Filter by Process and Application

- Data is converted to a discrete time signal

- Chromium
- VLC
Map Discrete Events to a Polar Space

• Mapping inspired by digital modulation methods

• Partition space by quadrants according to type of events

• Map each event to a part of the quadrant

• The magnitude is a function of the “size” of event
Exampled
Application Behavior Model

• Learn local patterns in the signal (sliding window)

• Learn the co-occurrence relationships between the patterns

• Model: \(<\text{Local Patterns, Co-occurrence}>\)
Learning Local Patterns

• Learn sparse representation dictionary on the time signals
• Dictionary atoms correspond to the local patterns

\[
y \approx D x
\]

\[
y \in \mathbb{R}^n
\]
\[
D \in \mathbb{R}^{n \times p}
\]
\[
x \in \mathbb{R}^p
\]

\[
D = \arg\min_D \sum_{i=1}^{n} \min \{ \| Dx_i - y_i \|^2 + \lambda \| x_i \|_1 \}
\]
Learning Co-occurrence (LSA)
Anomaly Detection using Model

Introduction
Design for Resiliency
Diverse Monitoring
Secure Monitoring
Monitoring Fusion
Conclusion & Future

Extract subsequence

Dictionary

Sparse Representation

LSA Rep.

Anomaly Score
Reconstruction of MySQL using VLC Model

![Graph showing anomaly score over execution steps with 95th percentile of reconstruction error indicated.]

LSE = 1.8804

95th percentile of reconstruction error
Evaluation Methodology

1. Generate traces of normal behavior of application
   - VLC playing local files
   - Apache + Mysql running wordpress
   - Windows services

2. Learn model of each application
3. Inject traces of shellcode behavior into testing traces
4. Compute anomaly scores
Evaluation Results

False Positive/Negative Rates for Reverse Shell

False Positive/Negative Rates for Drive-by-Download
Lateral Movement Detection Using Distributed Data Fusion

“World View” System Model

Diverse System Monitoring

Secure Monitoring and Response Infrastructure

Response Selection and Actuation

ONLINE COMPUTATION

OFFLINE/ONLINE COMPUTATION

RESILIENCY INFRASTRUCTURE

Monitor Fusion

Secure Monitoring and Response Infrastructure
Problem Description

*How do we fuse diverse data sources using a distributed agent-based system to detect lateral movement in a network while maintaining scalability?*
Lateral Movement Explained

- Starting from the entry point attacker moves to target host
- Uses system services or custom tools
State-of-the-art

• Centrally correlate NetFlows to detect lateral movement

• NetFlow correlation method is not accurate

• Amount of information is too large to be handled centrally
Approach Overview

Cluster Comm. Graph

Host Comm. Graph
(Connection Causation Events)

Process Comm. Graph
(Inter Process Comm. Events)
System Model

Cluster 2

Cluster 1
Lateral Movement

A critical step during APT to move from the entry point to target host
Inside Host 1

**Process Communication View** created by Kobra using timestamped events:

- Processes running
- Process communication (pipes, messages, ...)
- Network connections (with a unique ID across system)
- File access

Connection causation event is generated when the agent find a path between incoming and outgoing connections
Inside Host 1

Local agent infers connection causation using the Process Communication Graph.
Inside Host 1

Local agent infers connection causation using the **Process Communication Graph**

\[ C_1 \rightarrow C_2 \implies t(C_1) < t(C_2) \]
Lateral Movement

A critical step during APT to move from the entry point to target host

C1 ➔ C2
C2 ➔ C3
C3 ➔ C4

Entry Point ➔ C1

Target Host ➔ Host 1 ➔ Host 2 ➔ Host 3 ➔ Host 4 ➔ Host 5 ➔ Target Host

C1 ➔ C2
C2 ➔ C3
C3 ➔ C4

Design for Resiliency
Diverse Monitoring
Secure Monitoring
Monitoring Fusion
Introduction
Conclusion & Future
Inside Cluster Leader 1

Cluster head maintains **Host Communication** Graph

**Agents do not need to synchronize clocks**

\[ C_1 \triangleright C_2 \triangleright C_3 \triangleright C_4 \]

\[ \Rightarrow t(C_1) < t(C_2) < t(C_3) < t(C_4) \]
Lateral Movement

A critical step during APT to move from the entry point to target host
Discussion

• Network level causation inference using host-level calls

• Detection load distributed over all agents via distributed fusion

• Eliminate the need for global clocks by abstracting data using hierarchy
Conclusion

• We designed an “end-to-end solution” that provides cyber resiliency against coordinated threats

  • Kobra generate views of a host and to learn models of applications
  • In a hierarchical manner, we used Kobra’s views to generate a network-wide chain of a coordinated attack
Future Work

• We will formulate a theory for resilient integrity checking when an attacker is attempting evasion
  • PowerAlert
  • Integrity checking of an SDN
  • Rekeying of smart meters

• We plan to develop a response mechanism for lateral movement using adaptive control
  • The attacker model is unknown, to be learned
  • Response actions change network topology and healing rates of machines
Bibliography


