A Common Process Model for Incident Response and Digital Forensics


Felix C. Freiling
Laboratory for Dependable Distributed Systems
University of Mannheim, Germany

Bastian Schwittay
Symantec (Deutschland) GmbH, Germany
Motivation

- Analysis of digital evidence can put people into jail
- Only generally accepted, scientific methods should be applied in the analysis
- Frameworks for performing this analysis are called **process models**
- Different process models have emerged for different areas
- Can they be unified?
Examples: Incident Response and Digital Forensics

• Incident Response (IR): detect and contain computer security incidents
• Digital Forensics (DF): obtain valid evidence for (cyber)crime
• Highly related disciplines with a lot of overlap
• Aim: unified view of IR and DF using a Common Process Model
Agenda

• Background
  – Incident Response
  – Computer Forensics
• Common Model: Unifying IR and CF
• Summary and Discussion
Background: Incident Response (IR)

- **Computer Security Incident** is a „violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.“ [NIST, Computer Security Incident Handling Guide]

- **Incident Response**: Detection and containment of computer security incidents
- Focus on quick remediation and return to day-to-day business
- Root cause analysis may be skipped to prevent costs, interruption of business, etc.
- Structured approach to IR process
IR Process Model

- Process model structures the investigation so that investigators make less errors
- Standard reference:
- Process model of Mandia et al.
  - 7 phases ...
IR Process Model (Mandia et al.)
Background: Digital Forensics (DF)

- Part of forensic science: Obtain, analyze and present **digital evidence**
- Evidence handling suitable for a court of law
- Reliable, repeatable and well-documented methods for analysis
- Process model of Casey: **Investigative Process**
  - General model for digital investigations
  - Includes tasks of first responders
  - De facto standard
- 11 phases ...
Comparison: IR vs. DF

• IR puts focus on:
  – Management and quick containment of the security incident
  – Integration of investigation into the business processes of an organization
  – Usually quick return to service

• DF puts focus on:
  – Detailed and careful handling of digital evidence and analysis
  – Scientific approach

• Orthogonal aspects
Agenda

• Background
  – Incident Response
  – Computer Forensics

• **Common Model: Unifying IR and DF**

• Summary and Discussion
The Common Model (CM)

- Combine IR and DF processes:
  - Adds a management aspect to DF
  - Adds choice of suitable response strategy to DF
  - Adds option to conduct full-scale forensic analysis to IR

- Three phases to structure the response to a computer security incident
  - Pre-analysis phase
  - Analysis phase
  - Post-analysis phase

- Each phase divided into multiple steps
- Pre-Analysis phase determines depth of analysis phase
Common Model: Overview

Pre-Incident Preparation

Pre-Analysis Phase
- Detection of Incidents
- Initial Response
- Formulation of Response Strategy

Analysis Phase
- Live Response
- Forensic Duplication
- Data Recovery
- Harvesting
- Reduction and Organization

Analysis

Post-Analysis Phase
- Report
- Resolution
Pre-Analysis Phase

Pre-Analysis Phase

Pre-Incident Preparation

Incident Occurs

Detection of Incidents → Initial Response → Formulation of Response Strategy

full-scale forensic analysis?

Analysis Phase

....
Analysis Phase

Pre-Analysis Phase

....

Analysis Phase

Live Response → Forensic Duplication → Data Recovery → Harvesting → Reduction and Organization

Analysis

Post-Analysis Phase

....
Post-Analysis Phase

Analysis Phase

....

Post-Analysis Phase

Report

Resolution
Discussion (1/2)

• Unified view of IR and DF
• Flexible approach:
  – Takes organisational issues into account
  – Enforces scientific rigor where appropriate

• When to do a full-scale forensic analysis?
  – Hard factors:
    • Response posture: Does the organization follow a “zero tolerance“ policy?
    • Legal constraints: Must the incident be communicated to the police?
  – Soft factors:
    • Attacker threat level: Does the attacker represent a great threat?
    • Potential damage: Is the expected damage large?
• Formalized criterion for soft factors:
  Attacker Threat Level x Potential Damage > X

• Similar to risk equation:
  Risk = Threat x Vulnerability x Cost
  – AttackerThreatLevel ~ Threat
  – Potential Damage ~ Cost
  – „Vulnerability = 1“: incident has already occurred
References

  • http://pi1.informatik.uni-mannheim.de/filepool/teaching/forensik-2007

• Bastian Schwittay: Towards automating analysis in computer forensics. Diplomarbeit, RWTH Aachen, Department of Computer Science, 2006, Chapters 2 and 3.