# Specifying Digital Forensics: A Forensics Policy Approach

*By*

**Carol Taylor, Barbara Endicott-Popovsky, and Deborah Frincke**

*Presented At*

The Digital Forensic Research Conference

**DFRWS 2007 USA** Pittsburgh, PA (Aug 13th - 15th)

# Specifying Digital Forensics: A Forensics Policy Approach

Carol Taylor, Barbara Endicott-Popovsky
and Deborah Frincke

# Overview

- Motivation
- Forensics Policy
- Forensics System Properties
  - Forensic Readiness
- Forensics Policy Example
- Conclusion and Future Directions

# Motivation

- Digital forensics has become a critical component of both civil and criminal cases
- Slowly being recognized as important by non-technical groups
  - Judges and lawyers
  - Law enforcement
  - Business entities

# Motivation

- Has been some progress in defining recognized good practices in forensics application
- Most, aimed at collection of evidence from typical systems
- There is still a lack of widely accepted theoretical models or principles
- Creates problems in specifying or designing systems capable of capturing digital forensics evidence

# Motivation

- Without standard methods for specifying system forensics capabilities
  - Measuring or comparing systems is not possible
  - Implementing forensics capable systems is hit and miss with low probability of success

# Motivation

- **Our Solution**
  - Forensics policy approach
    - Assist with forensics system specification and most importantly verification
- **Why this approach?**
  - Clear statement of forensics policy allows design of system to meet the policy
  - Formalizing policy allows formal verification of system capabilities
  - Borrow from large body of security policy literature

# Forensics Policy vs. Security Policy

- Security Policy
  - Statement that clearly specifies what **is** allowed and what is disallowed with regards to security
  - Partitions system states into secure and unauthorized
  - Implement mechanisms to enforce system security policy

# Forensics Policy vs. Security Policy

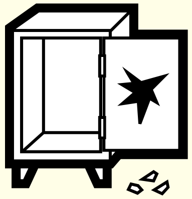
- Forensics policy
  - Statement
    - Clearly states which assets are forensically important
    - Specify data needed for investigation into breach of those assets

# Forensics Policy vs. Security Policy

- Forensics policy
  - Partitions space of all possible breaches or criminal activity into sets of events that are forensically noteworthy and those that are not
  - Allows for mechanisms or design decisions to enforce the policy

# Forensics Policy vs. Security Policy

- Another way to view differences …
  - Violate security policy → Insecure System
    - Consequences of break-in or insider misuse



  - Violate forensics policy → Lack of Evidence
    - Can’t show or prove guilt

# Security Policies

- Security policies
  - Policies viewed as high level goals for the system
  - Dictate system behavior to meet the goals
  - Example: Military Security policy
    - Unclassified, classified, secret, top secret

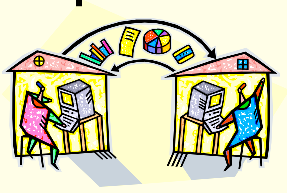
# Security Policies

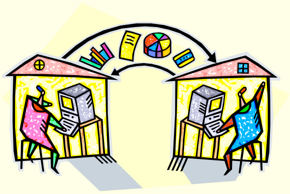
- Example: Military Security policy
  - Goal:
    - System should prevent unauthorized disclosure of information
  - Policy states:
    - All classified information must be protected from unauthorized disclosure or declassification
      - Classified, secret, top secret

# Security Policies

- Example: Military Security policy continued
  - Enforcement mechanisms:
    - Mandatory labeling of documents for classification level
    - Assignment of user access categories based on person’s clearance
    - Physical separation of data at highest classifications

Top Secret





Classified

# Forensics Policies

- Forensics policies define different goals
  - Deal with assets, data and possible storage issues
    - Capture digital evidence so forensic integrity of data preserved
    - Capture enough data to insure prosecution is possible

# Forensics Policies

- Forensics policies define different goals
  - Deal with assets, data and possible storage issues
  - Specify events that must be handled and data that must be preserved
  - Events not included in the policy will not need associated data

# Forensics Policy Example

- Example: Network intrusion policy commercial system Internet based
  - Goal:
    - Capture data from network intrusions for possible prosecution
  - Policy states:
    - All events identified as intrusions will have their associated data captured and preserved

# Forensics Policy Example

- Example: Network intrusion policy commercial system continued
  - Enforcement mechanisms:
    - Routine preservation of IDS, firewall, router and Web server logs for some configurable length of time

# Forensics Properties

# Policies Enable Properties

- Security policies,  specify system behavior, contribute to security properties
  - Confidentiality, Integrity and availability
  - Widely recognized security properties
- Similarly …
- Forensics policies, specify forensics system behavior, contribute to forensics properties
  - What are commonly recognized forensics properties?

# Forensics Systems Properties

- There doesn’t appear to be any widely acknowledged forensics system properties, except one …
  - Forensic Readiness
- Yet, concept not well defined in forensics literature and many would argue its not a property at all !!!

# Forensic Readiness Definitions

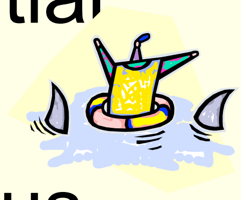
- Tan – 2001
  - Maximize environment’s ability to collect creditable digital evidence
  - Minimize cost of forensics in incident response
- Rowlinson – 2004
  - Expanded definition for enterprise systems and defined 10 steps for forensic readiness
- Endicott-Popovsky
  - Defined forensic readiness in terms of hardware devices and their capacity for dropping packets

# Forensic Policy Example

- For  purposes of discussion,
  - Forensic readiness is a property
  - Enabled through a forensics policy
  - Enforced through system design mechanisms

# Forensic Policy Example

- Define a Forensics policy to ensure the property of Forensic Readiness
- Steps:
  - Identify digital assets of value
  - Perform risk assessment for potential loss and threats to assets
  - Identify associated data needed plus storage and collection needs



# Forensics Policy Example

- Define a Forensics policy to ensure the property of forensic readiness
- Steps continued:

4. Write the forensic policy in terms of assets, forensic events, data collection and storage
5. Ensure there are forensic policy enforcement mechanisms

# Forensics Policy Example

- Using above approach,
  - Hypothetical forensics policy for corporation
    - High value Oracle database,
    - Lower value Apache web server,
    - Various routers, several firewalls
    - Snort IDS

# Forensic Policy Example

1 **All access to Oracle DB must be monitored.**

2 **Access logs and Administration logs to Oracle DB will be preserved for no less than one year**

3 **Access and activity to Web server is monitored**

4 **Apache Web server logs will be preserved for one year months**

5 **Firewall and Snort logs will be preserved for one year**

6 **Router logs will be preserved for 6 months**

7 **Network will be tested every 6 months for congestion situation by overloading it until it begins to drop traffic**

8 **Network capacity will be increased before traffic hits the level where packets will be dropped**

# Conclusion

- Forensics policies can help by clearly stating which events and associated data important
  - Leading to systems capable of capturing and preserving only data needed as opposed to all potential data
- Mechanisms can then be identified for policy enforcement
- Result will likely be systems more capable of supporting digital investigations without unnecessary cost

# Future

- Ideas in this paper were preliminary
- Write and implement forensic policies for actual systems. See them as complimentary to existing security policies
- Define forensics properties for systems
  - Capturability, System Integrity  (valid logs, accurate time stamps, authenticated users)
  - Availability, Data integrity

# Future

- Formal definition of policies
  - Reason about forensics capabilities
  - Discover inconsistencies and incomplete specification of forensic capabilities prior to system design

# Thank you

Questions