A Reference Model of Passive Network Origin Identification

Thomas E. Daniels
Fall 2002

Information Assurance Center
Department of Electrical and Computer Engineering
Iowa State University
What am I talking about?!

- Origin Identification Systems
  - Where did that network traffic come from?
  - Not just IP spoofing and island hopping
  - We’re concerned with causality here.
- Active – Mark or redirect traffic to assist in finding its origin
- Passive – Just listen to collect evidence of the origin
- Passive is what we’re talking about here
Outline

- Some introductory material
- Reference Models
- Our Reference Model
- Implications of the model
- What does this mean for network forensics?
Past Work in NOIS

Passive
- Host-based (CISIE, Carrier’s STOP)
- Network-based (Traffic Thumbprinting, IDIP, DoSTracker)

Active
- Traffic Marking (Authentication, Probabilistic Packet Marking, embedding watermarks)
- Route Modifying (Centertrack, Deciduous)
Some Intro Material

Network Assumptions

\[ G = (V, E, IM, XM) \text{ where } IM \subset V \text{ and } XM \subset E \]

Messages follow an unbounded path through \( G \) to some destination

Observables

- Content
- Headers
- Timing and Location
- Signal Characteristics
Reference Models

- Structured construct that defines a class of mechanisms
- Describes the member’s of the class in a structured way
- Defines the interaction
- Compare to the ISO OSI 7 layer reference model
- Why are reference models important?
  - Assists understanding components,
  - their interactions,
  - education,
  - generalizations about systems, and
  - build terminology.
Our Reference Model

- Network Monitors
  - Collect and process data for online or later use
  - Internal
  - External

- Analysis Program(s)
  - Collect data from Monitors
  - Make/support decisions about tracing traffic to origin
  - Direct tracing procedure
Network Monitors

External Monitors are arguably less powerful than internal

Capabilities of Internal monitors are optimistic

Edge Observed Networks

Observer
- An abstraction of one or more monitors
- Merges observations of many distinct monitors

Edge Observed Networks
- Reduce a network topology to a simplified one
- such that all edges in new network are monitored.

What are EOG’s good for?

- Allow merging internal and external monitors in one NOI System
- Abstracts away enough detail that general statements can be made.
Components of a Passive NOIS

- Data Available
- Selection
- Data Reduction
- Storage
- Control
- Reporting
- Analysis Program
- Commands
- Query Responses
Conditions for Passive NOI

- Necessary Conditions
  - Network Separation
  - Enough Storage
    \[ \text{history} > \frac{\text{storage}}{\text{obsfreq} \times \text{obssize}} \]

- Mutually Sufficient Conditions (in addition to above)
  - Analysis Program
  - Trusted Communication Paths
  - Correlation of an input to any given output across all nodes in EOG

- Sufficient because these together allow a step by step trace to succeed.
Forensic Implications

- Passive NOIS’s will be limited to initial investigation
  - Data reduction is key to success of NOI, but at odds with corroborating evidence or integrity.
  - Future research needs to consider this tradeoff

- Current NOIS proposals’ utility for investigation is limited
  - Most non-host-based NOISs trace a single type of network traffic
    - Hence, complex attacks can only be traced so far by these systems.
  - Host-based solutions (e.g. Carrier’s STOP) are useful, but require widespread deployment
  - Future research should address the problem of deployable systems that trace multiple types of traffic and how to take advantage of different types of NOISs
Conclusions

- We hope this model and future refinements will prove useful in education, research, and development of network forensics tools.

- There are forensics objectives that conflict with objectives of current passive NOISs.

- This reference model has motivated our current work in Divide and Trace methods for tracing traffic.
Questions?

- Thanks for the wonderful workshop experience!
- Rock Out, Jam Out
- More info can be found in my dissertation at
  http://www.eng.iastate.edu/~daniels/diss.pdf