Towards Impact Assessment Automation for Multi-Stage Cyber Attacks

Adam Stotz
Moises Sudit
Jared Holsopple

September 2007
Agenda

• Introduction/Motivation
• Cyber Attack Background
• Challenges
• Overall Impact/Situation Assessment Framework
  • Virtual Terrain
  • INFERD*
  • TANDI
  • VTAC
Introduction and Motivation

• Computer networks
  • Can contain sensitive information
  • Can perform critical missions
  • Are constantly targeted by hackers
  • Contain vulnerabilities

• Hackers
  • Think “outside the box”
  • Constantly find new ways to attack
  • Vary widely in skill, but even inexperienced hackers can cause damage

• Many speculate that the next major terrorist attack will be executed via the Internet
  • At a minimum, critical information and/or missions would be compromised
“Typical” Execution of Cyber Attacks

Originate from one or more computers outside of network

- Attacks originating internal to the network are “insider threats”
- Web servers, FTP servers, VPN servers usually most vulnerable to initial attack

Compromised computers can be used as “stepping stones”
Combating Cyber Attacks

• Detecting attacks
  • Intrusion Detection Sensors (IDS)
    • Analyze network traffic for attack signatures
    • Generate alerts for suspicious traffic
    • Placed throughout network
  • System logs
    • Size can make them unmanageable
  • In-house tools
Analyzing incoming attacks

- IDS Alerts/Log messages typically presented in spreadsheet format


- **Information Overload**
- Automated tool would allow analyst to quickly assess the location and severity of threat
Challenges for Automated Impact Assessment

- No “common” representation of a computer network
  - Contextual information (services, operating systems) is valuable for automation

- Lack of Public Data
  - Companies/agencies will not release Cyber Attack data

- Current data
  - Is usually simulated
  - Does not contain important contextual information
    - (Near) complete list of services, operating systems
    - Firewall rules
    - Mission information
Overall Architectural Vision

Components of Virtual Terrain
- Topology: Hardware and Software Infrastructure
- Vulnerabilities
- Information
- Cyber Sensors

A Priori Cyber Sensor Management

Sensed Virtual Terrain

Cyber Traffic

Situation Awareness and Impact Assessment
- Perception (Current Situation) INFERD
- Comprehension (Current Impact) VTAC
- Projection (Future Situation) TANDI
- Anticipation (Future Impact) TANDI+VTAC

Visualization

Decision Maker
- Action
- Forensics

On-Line Cyber Sensor Management

Service-Oriented-Architecture
INFERD Design

- **Hierarchical Fusion Framework**
  - Allows for bottom-up and top-down information analysis
  - Multiple levels of aggregation
- **Operational and Computational Efficiencies**
  - Minimize *a priori* knowledge
  - Distributed Architecture makes System Scalable to Varying Size Networks
  - System performs streaming on-line processing
  - Exact amount of information (no more and no less) at each stage of decision-making
- **Human-in-the-loop drives Fusion Process**
  - Avoid the overflow of raw data and maximize relevant information/knowledge
  - Situational Assessment (what is happening?) - ECCARS
  - Impact Assessment (what could happen?) – Future Programs
- **Interoperability with other Systems**
  - General Visualization Interface
  - Input interface for multiple sensor types & formats
  - Connectivity to Forensics for Adaptive Learning
Introduction and Motivation

- Sensor Location and Settings
  - Efficient Deployment
- Initial Knowledge of Domain and Objectives
- Physical/Virtual Domain of Interest
  - Sensors Type 1
  - Sensors Type 2
  - Sensors Type n
- Cleansing, Filtering and Homogenizing Data
- Hypothesis Generation
- Automatic SME
- Target Graphs Database
- Corpus of Evidence
- Discovery
- Decision Maker
- Impact & Threat
- Adaptive Learning
- Minimize Apriori Knowledge
- INFERD
- Detection & Tracking
- SA/IA Visualization
- Multiple Formats
- Completeness
Concept of Operations

Cyber Kill Chain

Detection vs. Prevention
• Designed for stream-based tracking of *non-traditional* sensed events
  - non-traditional = sensor observations other than position/velocity on physical moving targets
  - *Context* plays an important role
• Accomplished by 6 main processing modules
  - Data Alignment
  - Connotation Elicitation
  - Data Association
  - Track Update + Reporting
  - Ambiguity Detection and Resolution
  - Track Archival

New tracking process stage necessitated by non-traditional data
Present in traditional tracking systems
Information Flow within INFERD

- **Sensing**
  - Input: Network / host activity
  - Process: Cyber IDS(s) calculate anomalous or malicious patterns/signatures
  - Output: Alerts in their own heterogeneous formats in distributed network locations

- **Data Alignment**
  - Input: Heterogeneous / distributed alert data bases
  - Process: Ingests the heterogeneous / distributed alerts via network messaging services and provides a common access language for the INFERD fusion models to leverage
  - Output: Sensor Message = the alert with homogenized data access layer

- **Connotation Elicitation**
  - Input: Sensor Message
  - Process: Fusion model applies a contextual model-based understanding to the Sensor Message
  - Output: Elicited Message = Sensor Message with added model-based meaning

- **Data Association**
  - Input: Elicited Message
  - Process: Uses elicited information to associate the Elicited Message with information track(s) of relevance. Relevance determination is model defined.
  - Output: Information Track(s) of relevance

- **Track Update + Reporting**
  - Input: Elicited Message + Relevant Information Tracks
  - Process: Updates track structure with newly associated information. This update is model based.
  - Output: Report updates to publish to INFERD clients.
Sample Cyber Model

1. Multi-layer definition tying fusion process to specific fusion problem environments.
2. Defines how dynamic hypotheses are generated from data stream and what their content will be.

- **Events of Interest (EoI)**
  - Events INFERD will elicit from input data stream
  - Each EoI is composed by a set of *Features*
  - E.g. EoI’s:
    - Recon Scan DMZ
    - Recon Footprint DMZ
    - ...

- **Features**
  - Define *constraints* which when satisfied by the input data stream, assert the hypothesis that an EoI has occurred
  - E.g. Features:
    - Feature 1
    - Feature 2
    - ...

- **Constraints**
  - Static or dynamic
  - Can reference values within or between Sensor Messages and Information Tracks
Sample Association

- Model defines relation between Intrusion Root DMZ and Recon Scan Internal
  - “If target IP of hypothesized attack in DMZ = source IP of hypothesized attack in internal network than the 2 events are related”

- Model also defines Feature constraints which instruct Connotation Elicitation module to see the alert as a Recon Scan Internal (Feature and constraints not shown)
  - “If Attack Signature = sig1 and Target IP = ip2 Then event is a Recon Scan Internal”

- Data Association module sees that the newly hypothesized Recon Scan Internal attack satisfies the relation constraint defined above so reports the track as relevant
  - “Since source IP of Recon Scan Internal attack = target IP of Intrusion Root DMZ attack, the attacks are related.”
Track Update Example

- Dynamic variables take on values during track update
Benefits of INFERD to the Analyst

- Near “real-time” detection of cyber attacks
  - System runs at real-time for the AFRL DIW network
  - Scalable to larger networks
- Perception and Comprehension of complex coordinated attacks
  - INFERD fuses alerts into dynamic attack tracks
  - Attack tracks provides Situational Awareness (SA) to analyst
  - Ranking measurements filters hypotheses of interest (Depth, Abnormality, Others)
  - Abnormality and Defragmentation Handlers aid in Comprehension of SA
- Minimize requirement of a-priori knowledge
  - Guidance Templates (models) guide dynamic attack track creation
  - Model flexibility enables new hacker behavior and sensor accommodation
- Interoperability with third-party providers
  - DAO allows for interoperability without sacrificing real-time performance
  - Easy to interface with visualization (Flexviewer) or forensics (TMODS)
- Designed to be extendable for growth of capabilities and applications
  - Automatic Knowledge Reasoning: Pedigree, Discovery and/or Conflict Resolution
  - System Need NOT BE IDS-Centric
  - Impact Assessment or Prediction of Adversary Behavior
  - Process Refinement or Sensor Management
  - Other domains: Asymmetric warfare, Disease Surveillance, IED Detection, etc.
Implementation

- Skaion generated data sets
  - Used in Blind Test evaluation
- Alion Corporate Network
- DTO, AFRL, DIW
- Other Sites
Performance Evaluation and Metrics

- **Confidence:** correctly identify the situation(s)
- **Recall:** Activities detected in relation to the “total known”
- **Precision:** Activities detected in relation to number of detections
- **Fragmentation:** Activities reported as multiple s that should have been singleton
- **Mis-Association:** Activities reported as a singleton that should have been multiple

- **Purity** – characterizes the quality of the detections
- **Mis-Association Rate:** Evidence incorrectly assigned to a given activity
- **Evidence Recall:** Evidence detected in relation to the “total known”

- **Cost Utility** – measure of the system in identifying “important” situations
- **Weighted Cost:** Total available cost achieved savings by the system
- **Attack Score:** Attacks identified and where they appear in the proposed list

- **Timeliness** – measures the ability of the system to respond within time requirements of a particular domain
**Conclusions**

- Does not require network information
  - Robust to changing network configurations
  - Prone to false positives from sensors
  - Easy to configure and install on networks of any size/shape
- Can provide network assessment in real-time
  - Gives security analyst a chance to react to critical multi-stage attacks
  - Does not perform complex relationship analysis

**Future Work**

- Add subsequent layered processing to include detailed network information when available (Comprehension)
- Predict future attack vectors (Anticipation)
Virtual Terrain (Network Representation)

- **Infrastructure Topology**
  - Hardware
  - Software
  - Connectivity
- **Information**
  - Privileges
  - Location
  - Criticality
  - User, etc.
- **Cyber Sensors**
  - Type,
  - Location,
  - Pedigree, etc.
Virtual Terrain (VT) Definition

<table>
<thead>
<tr>
<th>Allowed from</th>
<th>Port #</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>12.1</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>11.x</td>
<td>SMTP</td>
</tr>
<tr>
<td>0</td>
<td>20.x</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>XXX</td>
<td>-</td>
</tr>
</tbody>
</table>

firewall rules

Routers/switches

Hosts/Host-clusters

Users & Accounts

service exposures

S. Jay Yang, RIT

Fusion 2007
The Use of VT

Hosts/Host-clusters

Routers/switches

Users & Accounts

Capability

Opportunity

Hosts containing similar service vulnerability are exposed:

- Firewall and permission rules define a dynamic neighbor list for each attacked host
- User accounts and privilege levels define potentially threatened hosts

UNCLASSIFIED
• Domain independent implementation
• Data structures provide contextual information
• Algorithms provide different perspectives of analysis
• Multiple threat scores on an entity are fused using Dempster-Shafer
VTAC: Virtual Terrain Assisted Impact Assessment for Cyber Attacks

- Can calculate impact for hosts, services, users, network
Insider Attack

Initial IU to peak is not administrator

Inside machines affected before external server subnets being impacted
• Can see the progression of different attack tracks at specific times
• For illustrative purposes, assumed that scenarios happened at the same time w/ same inter-step times
Future Work

- Refine INFERD
- Refine TANDI algorithms
- Integrate TANDI/VTAC for current and future impact

Automated impact assessment

- Is necessary to improve an analyst’s view of the situations
- Should allow the analyst to be the final decision-maker
- Requires better network service technology to be truly effective