Simulation of Workflow and Threat Characteristics for Cyber Security Incident Response Teams

Theodore Reed, Robert G. Abbott, Benjamin Anderson, Kevin Nauer & Chris Forsythe
Cyber threats pose a major risk to business, government and other organizations.
Despite extensive investments in technology, the human remains the last line of defense

- Intrusion detection, firewalls, email filters, anti-virus and other technologies stop most cyber threats
- Yet, criminals still find backdoors and vulnerabilities that provide a foothold onto IT networks
- Humans must fill the gap between the capabilities of technologies and those of adversaries who are sophisticated, enterprising, well-connected, motivated and persistent
Cyber Security Incident Response Teams (CSIRTs) serve as frontline defenders

- Assess alerts and conduct forensic analysis to identify, mitigate and defend against cyber threats
- Priorities, practices and make-up vary across organizations
- Utilize an array of commercial and homegrown software tools for forensic analysis, and archiving and searching past incidents
Existing models have focused on high-demand, as opposed to everyday operations

- ACT-R model incorporated risk aversion and experience with threats, *Dutt, Ahn & Gonzalez (2013)*
- Agent-based model of two-way interaction between attackers and defenders, *Kotenko, 2005*
- Game theory-based simulation of inferences made by attackers and defenders, *Hamilton & Hamilton, 2008*
- Models focused on adversary tactics, *Eom et al., 2008; Lee et al., 2005; Zakrzewska & Ferragut, 2011*

---

Excerpt from ACT-R Model of Cyber Defenders

Model of operations enables comparison of alternative tools, practices, staffing, etc.

CSIRT workflow modeled as a discrete event simulation using MicroSAINT Sharp

NOTE: The objective was to model workflow, as opposed to developing a cognitive model.
Alerts were generated and their characteristics specified

- Overwhelming majority of alerts result from either:
  - Legitimate user behavior,
  - Technical problems unrelated to cyber security, or
  - False alarms generated by automated monitoring

- Likelihood of each alert type was based on actual data

- Simulated daily experience of arriving in the morning with a queue containing alerts either generated overnight or left over from the day before

Alerts were probabilistically identified as one of eight types
Given the type of activity, ground truth level of threat and perceived priority were specified:

- Threat characteristics were specified:
  - Trajectory of the attack
  - Asset targeted
  - Perpetrator

- Based on threat characteristics, a value was derived for the ground truth level of threat

- Perceived priority was calculated as a function of ground truth and characteristics of individual analysts:
  - Related domain knowledge
  - Related experience
Analysts selected alerts for investigation from the queue

- Current model simulated a CSIRT consisting of five analysts

- In parallel, analysts skimmed the queue searching for an alert for which their perceived priority exceeded a pre-specified threshold, taking the first alert that exceeded this threshold

- If no alerts met this criteria, the threshold was lowered and the process repeated
Once an alert was selected from the queue, the investigation began

- Analysts performed one of thirteen forensic analysis tasks
- Forensic analysis tasks corresponded to the use of different software tools
- Based on the type of activity, there was a likelihood based on logs of actual events that each task would be performed
Through tasks, evidence was accumulated toward the resolution of an alert.

- The time to perform a given task was drawn from a random distribution of times for the type of task.
- Analysts sometimes selected to hand off a task to another analyst with superior knowledge or experience.
- Tasks generated evidence and once sufficient evidence was accumulated, the alert was resolved.

Analyst completed tasks accruing time or handed-off to another analyst.

If sufficient evidence was accumulated, the alert was resolved.

If alert was not resolved, based on the task completed, there were probabilities that each task would be the next performed.

In some cases, in completing a task, the threshold for resolving an alert was elevated.

In completing one task, multiple spin-off tasks sometimes needed to be performed.
Validation involved generating alerts equivalent to a set of actual alerts

- A set of 136 alerts and associated records were obtained and an equivalent set of alerts generated with the simulation
- The threat characteristics of each alert were rated using the MITRE Cyber Prep Methodology, Mateski et al. (2012)
  - Trajectory
    - (1) targeting no specific entity,
    - (2) targeting a specific single entity, or
    - (3) targeting multiple entities or high-value entities
  - Targeted asset
    - (1) no asset,
    - (2) a client or set of client assets, or
    - (3) an infrastructure, service, or critical asset
  - Perpetrator
    - (1) a careless or unknown entity,
    - (2) an action associated with criminal activity, or
    - (3) an action associated with an advanced threat

- Two cyber security forensic analysts rated alerts,
  Interrater reliability = 77% ($r = 0.580; p<0.0001$)
Each threat characteristic was correlated with measures of the level of effort

- Records provided three measures of the level of effort required to resolve alerts
  - Total time
  - Number entries
  - Number analysts

- Measures of the level of effort required to resolve alerts were correlated with one another and ratings for each threat characteristic

- Correlations between the ratings for threat characteristics varied

<table>
<thead>
<tr>
<th></th>
<th>Total Time</th>
<th># Entries</th>
<th># Analysts</th>
<th>Trajectory</th>
<th>Asset</th>
</tr>
</thead>
<tbody>
<tr>
<td># Entries</td>
<td>$r=0.513$</td>
<td>$r=0.860$</td>
<td>$r=0.229$</td>
<td>$r=0.326$</td>
<td>$r=0.241$</td>
</tr>
<tr>
<td></td>
<td>$p&lt;0.001$</td>
<td>$p&lt;0.001$</td>
<td>$p&lt;0.008$</td>
<td>$p&lt;0.001$</td>
<td>$p&lt;0.005$</td>
</tr>
<tr>
<td># Analysts</td>
<td>$r=0.524$</td>
<td>$r=0.348$</td>
<td>$r=0.229$</td>
<td>$r=0.311$</td>
<td>$r=0.241$</td>
</tr>
<tr>
<td></td>
<td>$p&lt;0.001$</td>
<td>$p&lt;0.001$</td>
<td>$p&lt;0.008$</td>
<td>$p&lt;0.001$</td>
<td>$p&lt;0.005$</td>
</tr>
<tr>
<td>Trajectory</td>
<td>$r=0.171$</td>
<td>$r=0.348$</td>
<td>$r=0.229$</td>
<td>$r=0.311$</td>
<td>$r=0.241$</td>
</tr>
<tr>
<td></td>
<td>$p&lt;0.048$</td>
<td>$p&lt;0.001$</td>
<td>$p&lt;0.008$</td>
<td>$p&lt;0.001$</td>
<td>$p&lt;0.005$</td>
</tr>
<tr>
<td>Asset</td>
<td>$r=0.326$</td>
<td>$r=0.352$</td>
<td>$r=0.311$</td>
<td>$r=0.241$</td>
<td>$r=0.326$</td>
</tr>
<tr>
<td></td>
<td>$p&lt;0.001$</td>
<td>$p&lt;0.001$</td>
<td>$p&lt;0.001$</td>
<td>$p&lt;0.005$</td>
<td>$p&lt;0.005$</td>
</tr>
<tr>
<td>Perp</td>
<td>$r=0.171$</td>
<td>$r=0.546$</td>
<td>$r=0.498$</td>
<td>$r=0.192$</td>
<td>$r=0.136$</td>
</tr>
<tr>
<td></td>
<td>$p&lt;0.048$</td>
<td>$p&lt;0.001$</td>
<td>$p&lt;0.001$</td>
<td>$p&lt;0.026$</td>
<td>NS</td>
</tr>
</tbody>
</table>
Model predictions for the time to resolve alerts correlated with actual times

- Alerts generated with the same characteristics as actual alerts
- For the simulation, analysts were assigned an intermediate level of expertise
  - (Expertise = 5, on a scale of 1-10)
- NOTE: Simulation did not account for analysts suspending work on an alert and resuming work at a later time

\[ r = 0.185, \ p < 0.03 \]

NOTE: Time units are notional values and do not reflect actual units of time
Conclusions and afterthoughts

- The model appears to capture the basic mechanics that determine the workflow within a CSIRT

- Questions may be raised concerning the differential contribution of threat characteristics, and the knowledge and experience of analysts to the time to resolve alerts

- Knowledge and experience are believed to influence workflow in three ways
  - (1) As analysts gain expertise, they more accurately assess the nature of threats and are better able to calibrate the level of effort devoted to an individual alert to the threat posed by the event
  - (2) A richer understanding of tasks should allow analysts to perform those tasks more efficiently and productively
  - (3) Greater knowledge of the procedures entailed in using software tools combined with a better conceptual knowledge of the application of the software tools should result in superior efficiency and productivity