Identifying a Shared Mental Model Among Incident Responders

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Robert Floodeen, Software Engineering Institute
John Haller, Software Engineering Institute
Brett Tjaden, James Madison University

March 12, 2013

Introduction

- Typically, there is a direct correlation between the time to resolve an incident and the damage sustained by an organization
  - The faster and incident is resolved, the less damage is done to the organization
- Coordination among organizations experiencing the same or related incidents can speed resolution (and decrease damage)
- **Question**: Can we improve the way incident response teams work together for the first time during a cybersecurity incident by identifying a shared mental model?
- We will describe the results of an exercise we conducted to explore:
  - Whether an ad-hoc group of incident responders share a schema for decision making
  - What some of the decision criteria (questions) and types of values (answers) might be

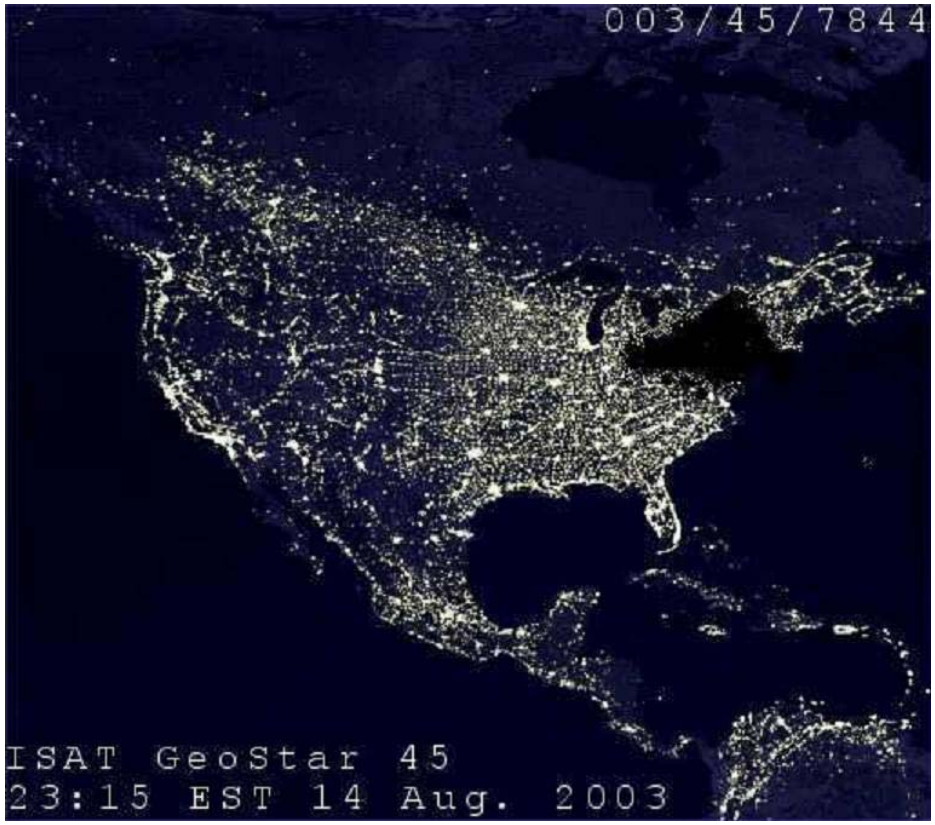
Why should we care?

Critical infrastructure

- Disbursed providers of critical infrastructure

Defense

- Military CSIRT teams
- Cooperating nations



. . . but really any group of distributed response teams.

The Exercise

- Conducted in June, 2012:
  - 90 participants - all members of different computer security incident response teams (CSIRTs)
  - Two 1-hour information-gathering sessions
  - A hypothetical scenario was used to elicit information from the participants about what types of information they would need to decide how to respond

The Exercise – Session #1

Management Concern: Transmittal of Stolen Information

Your organization is infected with a botnet and attacking others; others are attacking you (major DDoS). Senior leadership is demanding to know:

- Is information being stolen from our systems?
- Is stolen information being downloaded to our systems?

The Exercise – Session #1 - Results

After presenting the scenario, we held a chat session and asked the participants what questions they would ask in order to be able to address Management Concern #1. Their questions focused on the following areas:

- Other signatures
- Points of contact
- Who is involved
- Timeliness/Verify report
- Data protection
- Targeted
- Who is aware
- Publicly known
- Integrity of logs

The Exercise – Session #2

Management Concern: Stopping the Botnet

Your organization has all the information it needs on the botnet. There are now forty countries involved in the incident.

What information do you think those forty countries need in order to help them stop the botnet from attacking your country?

The Exercise – Session #2 - Results

We held another chat session and asked the participants what questions they would ask in order to be able to address Management Concern #2. Their questions focused on the following areas:

- Port(s) and associated service(s)
- Detection method
- Audience
- Vulnerability type
- Coordination lead
- Malware removal
- IP(s) involved
- IP(s) of attackers
- Behavior samples
- Possible impact

Gathering More Data

Having completed the two chat sessions and summarized the responses for all to see, we polled the participants and asked them to rank the relative importance of each item.

Table 1: Items Sorted by Importance

Value	Importance
Event, Log, MSG	4.45
Process/Service	4.06
IP address	4.03
Port	3.87
OS	3.87
MD5	3.82
URI, Link, Web Query	3.77
File, Directory	3.77
Content Strings	3.75
Domain	3.74
Hive	3.70
Proto Header	3.69
Key/ Key Group	3.69
Proto Field	3.20
Environment Variable	3.15
Session Token	3.10

Gathering More Data (cont)

Having completed the two chat sessions and summarized the responses for all to see, we polled the participants and asked them to rank the relative difficulty of obtaining each item.

Table 2: Items Sorted by Difficulty

Value	Difficulty
Key/ Key Group	3.40
Hive	3.33
Session Token	3.28
Proto Field	2.98
Environment Variable	2.88
Content Strings	2.81
Process/Service	2.80
File, Directory	2.77
MD5	2.69
Event, Log, MSG	2.65
Proto Header	2.61
OS	2.40
URI, Link, Web Query	2.34
Domain	2.22
IP address	2.20
Port	1.95

Results

This particular group of technicians did not exhibit a shared mental model for decision making:

- The items proposed by the participants did not overlap much
- The items proposed by the participants were general in nature and not specific to the task they had been given
  - Were they trying to fill in the typically fields in the ticketing systems they use?
  - Is it a good strategy to collect general information about an incident before focusing on more specific information?

Results (cont)

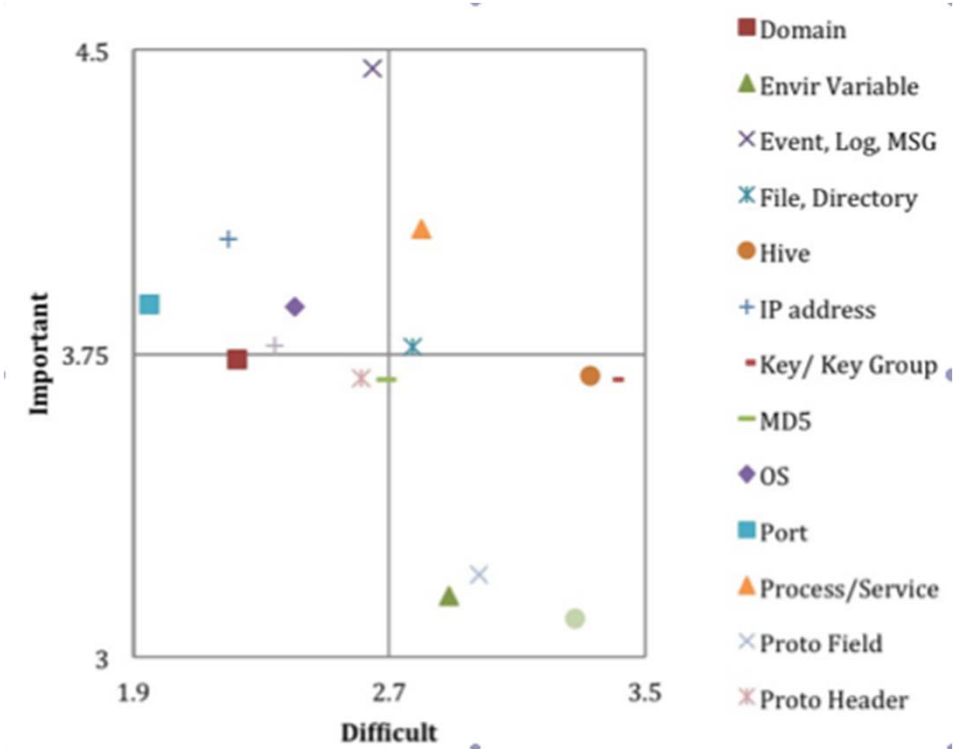
By subtracting the participants' difficulty ranking (Table 2) from their importance ranking (Table 1) we identified a priority order for information

Table 3: Prioritized Order

Value	Importance minus Difficulty	Sample Message Group
Port	1.92	Initial
IP address	1.84	Initial
Event, Log, MSG	1.80	Initial
Domain	1.51	Secondary
OS	1.46	Secondary
URI, Link, Web Query	1.43	Secondary
Process/Service	1.26	Detailed
MD5	1.13	Detailed
Proto Header	1.08	Detailed
File, Directory	1.00	Detailed
Content Strings	0.93	Detailed
Hive	0.37	In an Advisory
Key/ Key Group	0.28	In an Advisory
Environment Variable	0.27	In an Advisory
Proto Field	0.22	In an Advisory
Session Token	-0.18	In an Advisory

Results (cont)

A scatter chart plotting each item's importance and difficulty:



Results (cont)

The data that we gathered from the participants suggests that the following general questions may be a good starting point for developing a shared mental model for incident responders:

- What types of activity should we be looking for on our network? Specifically:
  - What ports?
  - What IP addresses?
  - What domains?
  - What URLs or web queries?
- What should we be looking for on compromised hosts? Specifically:
  - Are there logs to be reviewed (event, system messages, etc.)?
  - Is there a specific type of operating system (and version)?
  - Is there a process or service associated with the infection?
  - Is there an MD5 of the malware that we could use for detection?

Conclusions

Several interesting questions arose as a result of our exercise:

- What is the impact of the incident ticketing system (or cybersecurity advisory format) used on the mental model of incident responders?
- How much time is spent collecting information that is not relevant to an incident?
- How much time is spent disseminating or reading information that is not relevant to an incident?
- What should the mental models look like for incident response? Is it something that we could create, or can we collect it form incident responders?
- How do we create and convey a shared mental model between teams that may not ordinarily work together?
- What are the differences in the schemata of various types of incidents?
- What are the similarities among the majority of cybersecurity incidents?

Conclusions (cont)

Several interesting questions arose as a result of our exercise:

- What information should be collected relevant to a particular incident? For example:
  - What is the timeliness associated with specific values and decision criteria?
  - What is the importance of the incident?
  - How difficult is it to get the information needed?
  - How difficult is it to use the information for verification?
  - What is the best way to distribute (all at once, as it is learned, etc.) the information?

Conclusions (cont)

The correlation of importance to difficulty of the information that incident responders deal with should be better understood:

- Is some information easy to obtain because it is important (i.e. constant exposure has made it routine to deal with)?
- Is some information naturally easy to obtain and so we prefer to deal with it and have found the ability to get every possible use out of it?

What might an incident mental model look like?

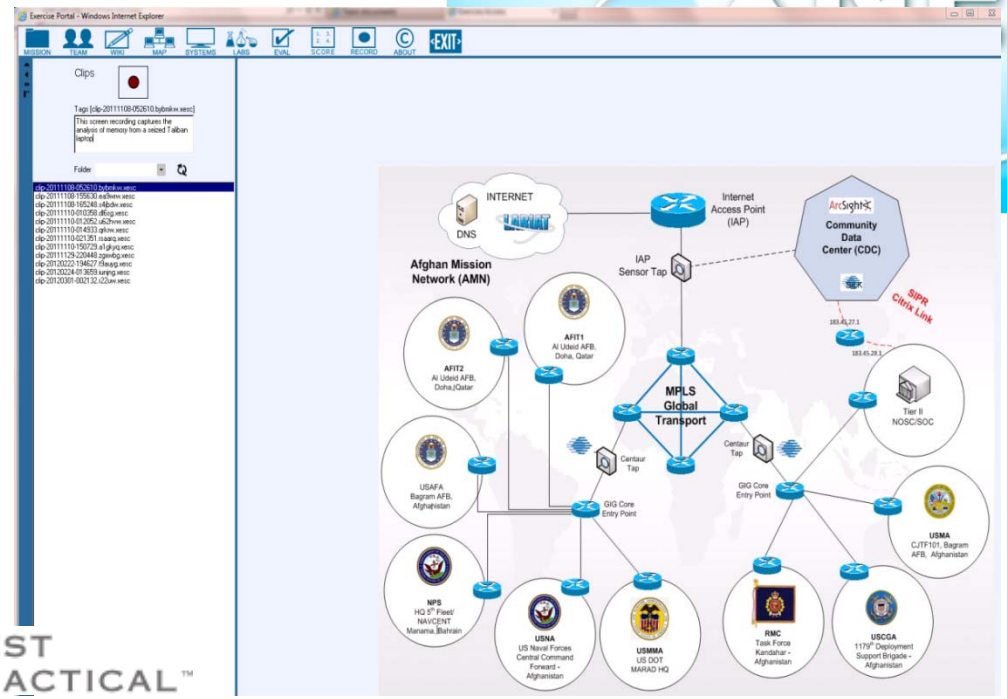
Indicator type	Incident information received	Organization affected	Organization not affected	Inconclusive
IP address	62.123.20.22			62.123.20.xx netblock
Port	21	21		
Specific log event	Registry key change	key change detected		

Indicator type	Incident information received	Sensor input one	Sensor input two	Sensor input *n*
IP address	62.123.20.22	62.123.20.22		62.123.20.xx . . .
Port	21	positive		. . .
Specific log event	Registry key change		positive	. . .

Some possible tools and next steps

Instrumented ticketing systems

Virtual training environments



BEST PRACTICAL™

Final Thoughts

- Incident handling activities and training that share the same mental model might increase ad-hoc performance by allowing teams to coordinate without frequent communication before an incident and with limited, efficient communication during an incident.

- A shared mental model would allow cooperating teams to:

  - Know where their partners are in the incident handling process
  - Predict the next steps both they and their partners need to take
  - Identify the information required to complete the handling of the incident

- We have identified the first steps in developing a shared mental model for incident responders

Contact Information

John Haller

Functional Manager

Cyber Resilience Center CERT
Infrastructure Resilience Team

Telephone: +1 412-268-6648

Email: jhaller@cert.org

U.S. Mail

Software Engineering Institute

Customer Relations

4500 Fifth Avenue

Pittsburgh, PA 15213-2612

USA

Web

www.sei.cmu.edu

www.sei.cmu.edu/contact.cfm

Customer Relations

Email: info@sei.cmu.edu

Telephone: +1 412-268-5800

SEI Phone: +1 412-268-5800

SEI Fax: +1 412-268-6257

This material is based upon work supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.