

# Asymmetric Threat Response and Analysis Program

Michael L. Valenzuela

Jerzy W. Rozenblit

# Overview

- What is the Asymmetric Threat Response and Analysis Program (ATRAP)?
- Data Ingestion
  - Structured vs. unstructured
- Link Charts
- Game Theoretic Decision Support Tool

# Note

- We apologize in advance
  - The original security data has ITAR restrictions
  - Thus we cannot show this data publically
- Instead we have medical data
  - Statically correct, but sanitized
  - Can still be used to show ATRAP's features

# Asymmetric Threat Response and Analysis Program

The screenshot shows the ATRAP web application interface. At the top, the title bar reads "Asymmetric Threat Response and Analysis Program (ATRAP)". Below it is a green navigation bar with "File", "Tools", and "Help" menus, and a status bar showing "UNCLASSIFIED" and "ACTIVE WORKSET: PSN". The main content area features the ATRAP logo and version "v3.1.11258". A search bar is present with a "Database:" selector set to "Local". Below the search bar are tabs for "Reports", "Entities", "Graphs", and "Query Models". The "Keywords" section includes an "Advanced Search" dialog with fields for "All these words:", "This exact wording or phrase:", "One or more of these words:" (with an "OR" operator), and "Proximity between two words:" (with a "NEAR" operator). A "Date" section is also visible, showing a range from "10/30/2013 13:43" to "10/30/2013 13:43". A "FIND" button is located at the bottom of the search area. On the right side, there are sections for "LOCAL STATS" (DB Size: 1.82 GB, Reports: 282, Entities: 640, Map Cache Size: 74.66 M) and "NOTIFICATIONS" (You have 0 models scheduled, with a notification from [10/30/2013 13:43 T (-7:00)] -- Notification agent initialized...). At the bottom, a "WORKSET" section shows "Active PSN" with buttons for "EDIT", "DELETE", "CREATE", and "?". The footer contains copyright information for Ephibian, Inc. and The Arizona Board of Regents, along with the user "Liana Suantak" and the timestamp "10/30/2013 14:46 T (-7:00)".

# ATRAP

- Originally a tool for military intelligence analysts
- Built upon a “human-in-the-loop” philosophy
  - Avoids a fully automated tool making mistakes
  - Provides transparency and introspection into data processing
- Much like a toolbox of individual tools
  - Like Matlab, except for security
  - Due to the number of tools, we will only show a few tools
- Now encompasses many security domains

# ATRAP – Motivation

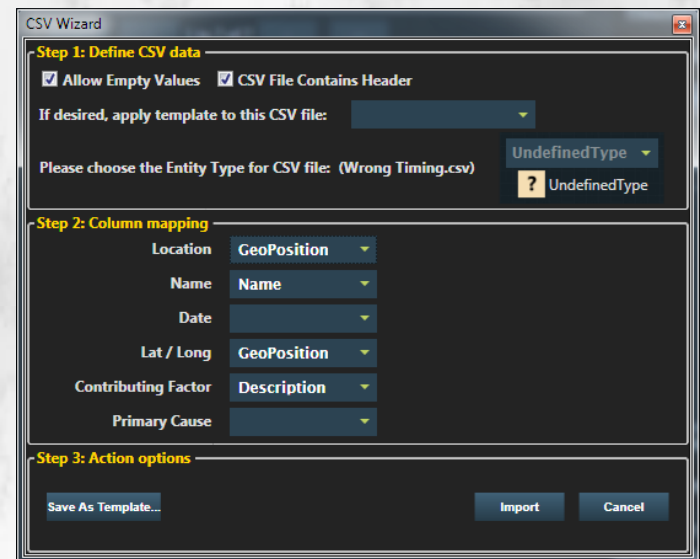
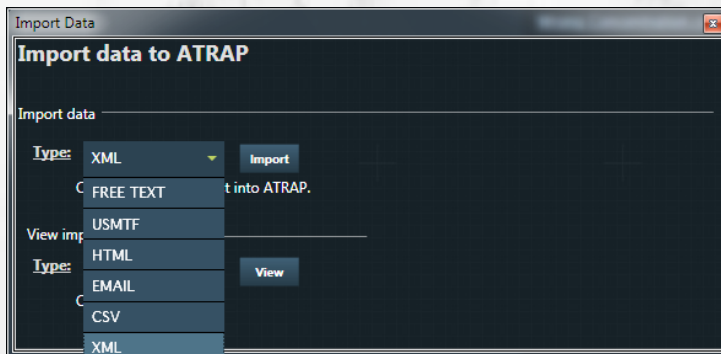
- Think about this
  - Inside jobs cause the majority of damage
  - This tool helps an analyst/detective trace from evidence back to the insider(s)
- Suppose
  - Network traffic is available and events have already been detected via some other tool
  - Some connections between individuals, computers, and events are known

# Data Ingestion

- ATRAP operates on databases (Microsoft or Oracle)
- Data can be structured (xml, csv, html, etc.)
- Data can be unstructured (free text)
  - Free text data can be structured with a text-processing tool which includes some basic natural language processing

# Data Ingestion

- Structured data can be directly imported as any user defined types.
  - E.g., provided a user defined meta-protocol, each field can be imported from the structured data
  - Nonstandard protocols can be user defined or subtyped





# Data Ingestion – free text

- Entities (structured information) can be extracted from free text
  - ATRAP provides some natural language processing
  - Still requires the use of a person to create a structured piece of information from the text

The screenshot displays the ATRAP software interface. At the top, the title bar reads "Asymmetric Threat Response and Analysis Program (ATRAP)" and "UNCLASSIFIED". The main window shows a document titled "concisemonograph2.aspx.htm". The interface includes a menu bar (File, Tools, Help) and a toolbar with options like Home, Wrong Dos..., and concisemon... The main content area displays a document with various sections and highlighted text. A sidebar on the right, titled "Entities in Document", lists extracted entities such as "Noun", "CONCISE MONOGRAPH", "U S based MDs", "SUPPLIED Tab", "myxedema", and "amylase". The document text includes sections like "SEARCH Required Field", "RESOURCES", "CONCISE MONOGRAPH MEDICATION GUIDE PRODUCT LABELING REMS SUMMARY", "Boxed Warning", "PrintOxyContin", and "THERAPEUTIC CLASS Opioid analgesic".

# Entities (structured data)

- Entities (any structured data) may have
  - Meta-data
  - Data-time information
  - Attributes
  - Associated files (multimedia, reports, etc.)
  - Relationships with other entities
- ATRAP has tools to perform queries on any of these properties

# Link Charts

Asymmetric Threat Response and Analysis Program (ATRAP)

File Tools Help UNCLASSIFIED ACTIVE WORKSET: PSN

Home

## ATRAP

ASYMMETRIC THREAT RESPONSE AND ANALYSIS PROGRAM v3.1.11258

Copyright 2011 Ephibian, Inc. and The Arizona Board of Regents on Behalf of the University of Arizona.

<< < 1 to 20 of 45 > >>

### ENTITIES (640)

| NAME   | TYPE         | # SOURCES | # ATTRIBUTES | LAST KNOWN LOCATION |
|--|--------------|-----------|--------------|---------------------|
| <a href="#">Wrong Timing 9, in Dillinger</a> | Wrong timing | 3         | 3            | 12SWA0508267136 @ 0 |
| <a href="#">Wrong Timing 9, in D6W</a>       | Wrong timing | 3         | 3            | 12SWA0511667192 @ 1 |
| <a href="#">Wrong Timing 8, in Dillinger</a> | Wrong timing | 3         | 3            | 12SWA0508767135 @ 0 |
| <a href="#">Wrong Timing 8, in D6W</a>       | Wrong timing | 3         | 3            | 12SWA0511367195 @ 0 |
| <a href="#">Wrong Timing 8, in D6N</a>       | Wrong timing | 3         | 3            | 12SWA0505567195 @ 0 |
| <a href="#">Wrong Timing 7, in Dillinger</a> | Wrong timing | 3         | 3            | 12SWA0509667153 @ 0 |
| <a href="#">Wrong Timing 7, in D6W</a>       | Wrong timing | 3         | 3            | 12SWA0511667194 @ 0 |
| <a href="#">Wrong Timing 7, in D6N</a>       | Wrong timing | 3         | 3            | 12SWA0505467195 @ 0 |
| <a href="#">Wrong Timing 6, in Dillinger</a> | Wrong timing | 3         | 3            | 12SWA0508467145 @ 0 |
| <a href="#">Wrong Timing 6, in D6W</a>       | Wrong timing | 3         | 3            | 12SWA0511167194 @ 1 |
| <a href="#">Wrong Timing 6, in D6N</a>       | Wrong timing | 3         | 3            | 12SWA0504467196 @ 0 |
| <a href="#">Wrong Timing 6, in D5</a>        | Wrong timing | 3         | 3            | 12SWA0511867210 @ 0 |
| <a href="#">Wrong Timing 5, in Dillinger</a> | Wrong timing | 3         | 3            | 12SWA0510067147 @ 0 |
| <a href="#">Wrong Timing 5, in D6W</a>       | Wrong timing | 3         | 3            | 12SWA0511367194 @ 0 |
| <a href="#">Wrong Timing 5, in D6N</a>       | Wrong timing | 3         | 3            | 12SWA0506267193 @ 1 |

### LINK CHARTS (1)

| NAME                          | # ENTITIES | OWNER | CREATED                    | MODIFIED     |
|-------------------------------|------------|-------|----------------------------|--------------|
| <a href="#">Tami's rounds</a> | 36         | Liana | 05/02/2012 19:26 T (-7:00) | 05/02/2012 1 |

Tami's rounds

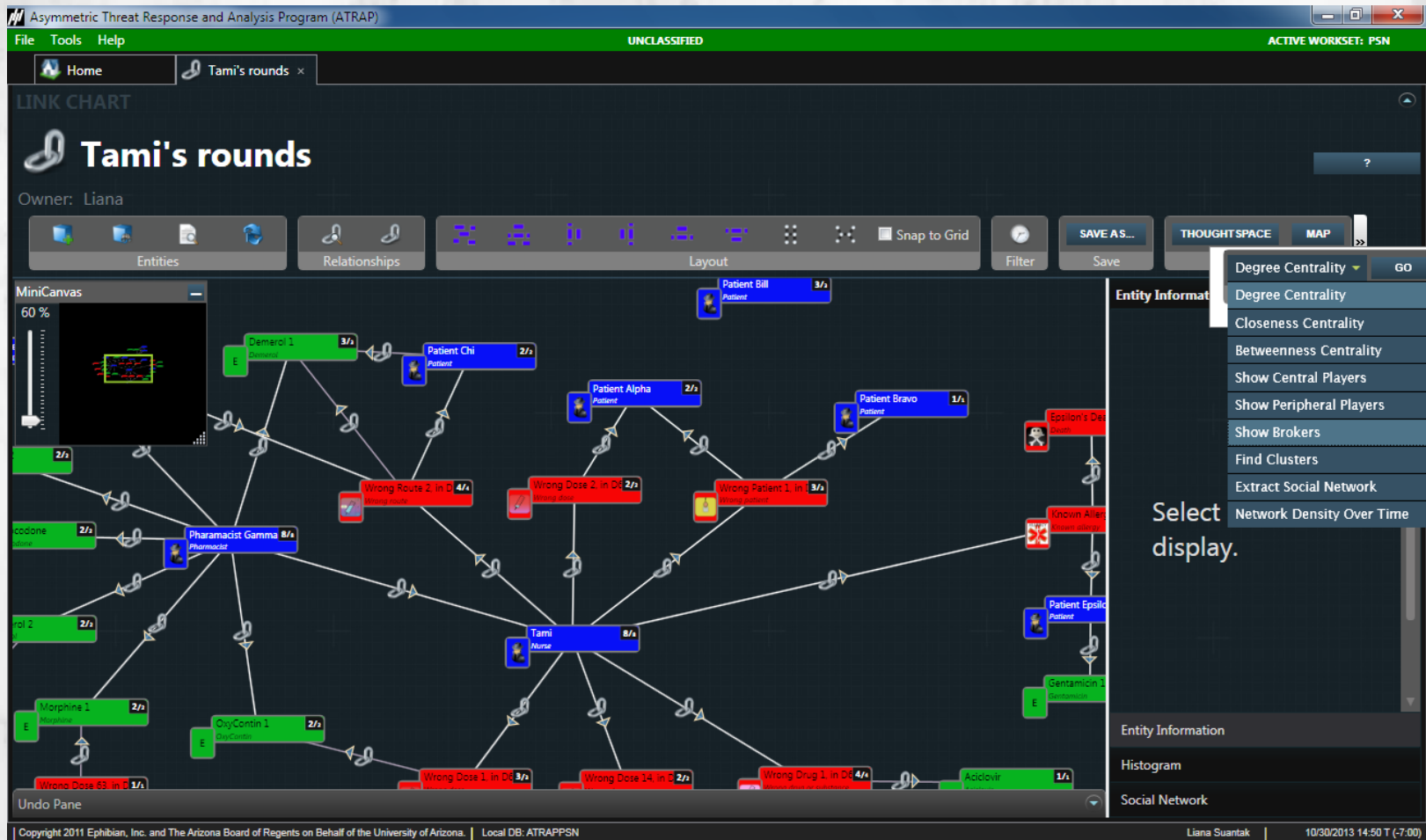
<< < 1 to 1 of 1 > >>

Copyright 2011 Ephibian, Inc. and The Arizona Board of Regents on Behalf of the University of Arizona. | Local DB: ATRAPPSN | Liana Suantak | 10/30/2013 14:47 T (-7:00)

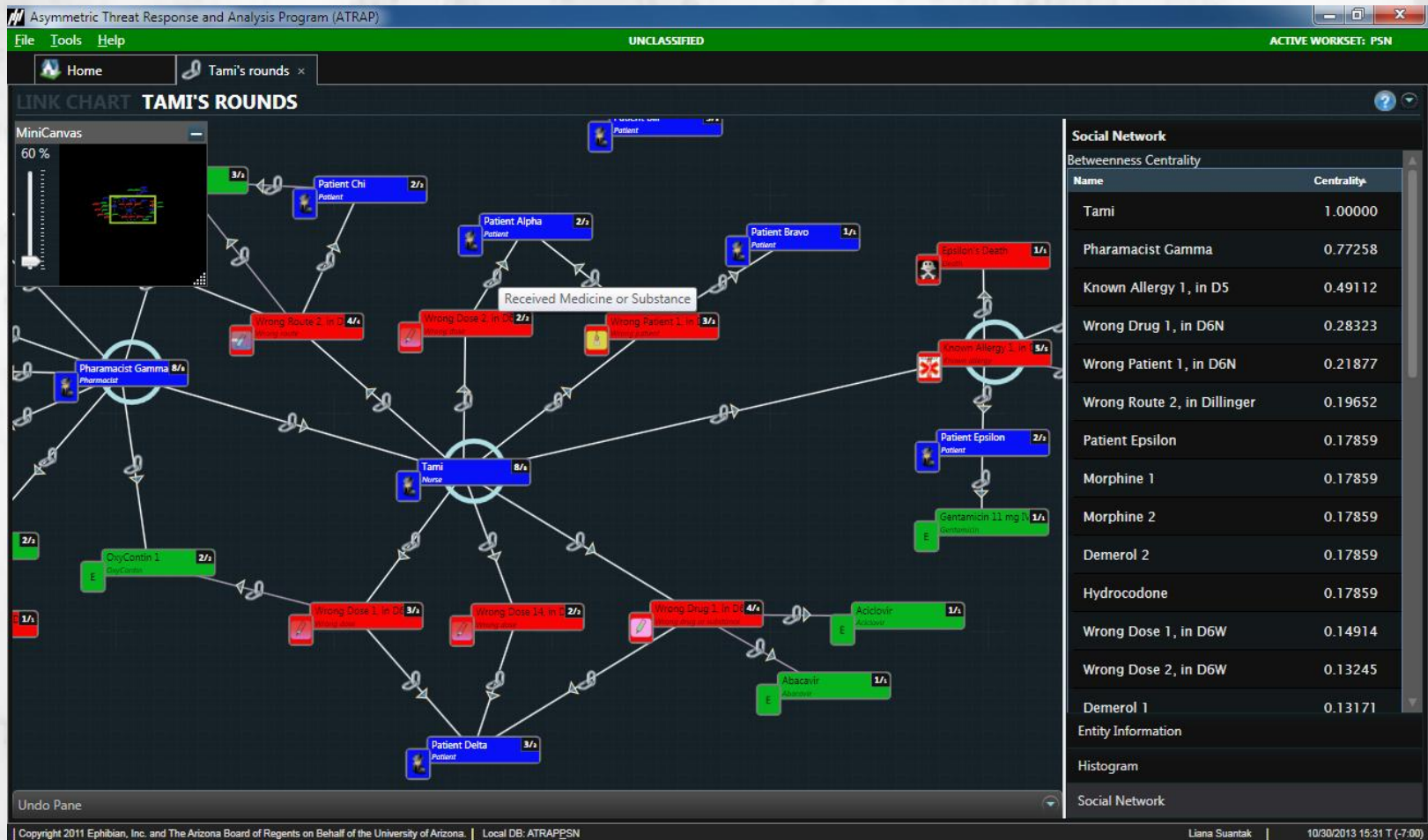
# Link Charts

- Link charts are used to display and explore relationships between entities
  - Color represents a type of entity
    - Icons are used to distinguish between subtypes
  - Relationships are directional and typed
  - Many common graph tools including
    - Clustering
    - Searching by connection patterns
    - Displaying central and broker nodes
    - Extracting subgraphs

# Link Charts – Several Tools



# Link Charts – Showing Brokers and Betweenness Centrality



# Link Charts

- No limits on the size of the link charts
  - Except those that storage and memory impose
- Sometimes it is better to work with smaller groups of entities
- ATRAP allows this through extracting clusters
- Entities can be organized neatly through the use of spring embedders

# Link Charts – Data Reduction by Clusters

The screenshot displays the Asymmetric Threat Response and Analysis Program (ATRAP) interface. The main window is titled "Social Network Clusters from: Tami's | (UNSAVED)". The interface includes a menu bar (File, Tools, Help), a toolbar with icons for Home, Tami's rounds, and Social Netw..., and a status bar at the bottom showing "UNCLASSIFIED" and "ACTIVE WORKSET: PSN".

The central area shows a network graph with nodes representing entities and edges representing connections. A tooltip titled "Local Force Spring Embedding" is visible, stating: "Only entities in close proximity will exert noticeable force on non-adjacent entities. This tends to place entities at equal distances from each other. Recommended for link charts with disconnected entities." A "Type Picker" dialog is open, listing various entities such as Abacavir, Aciclovir, Ampicillin 150mg - Epsilon, Demerol 1, Demerol 2, Epsilon's Death, Gentamicin 11 mg IV q24h - Epsilon, Hydrocodone, Jessica, Known Allergy 1, in D5, Morphine 1, Morphine 2, OxyContin 1, Patient Alpha, Patient Bill, Patient Phil, Patient Ray, Patient, Pharmacist Gamma, Tami, Water 1, Wrong Dose 1, in D&W, Wrong Allergy 1, in D5, Wrong Patient 1, in D&N, and Wrong Route 2, in Dilin. The dialog also includes sliders for "The number of connections per node" (Selected Value: 3) and "The number of connections in a cluster" (Selected Value: 3).

On the left, a "MiniCanvas" window shows a smaller version of the network graph at 60% zoom. The main graph shows nodes for "Patient Bill", "Patient Phil", "Patient Ray", "Water 1", "Tami", "Pharmacist Gamma", "Demerol 1", "Wrong Dose 1, in D&W", "Wrong Allergy 1, in D5", "Wrong Patient 1, in D&N", and "Wrong Route 2, in Dilin".

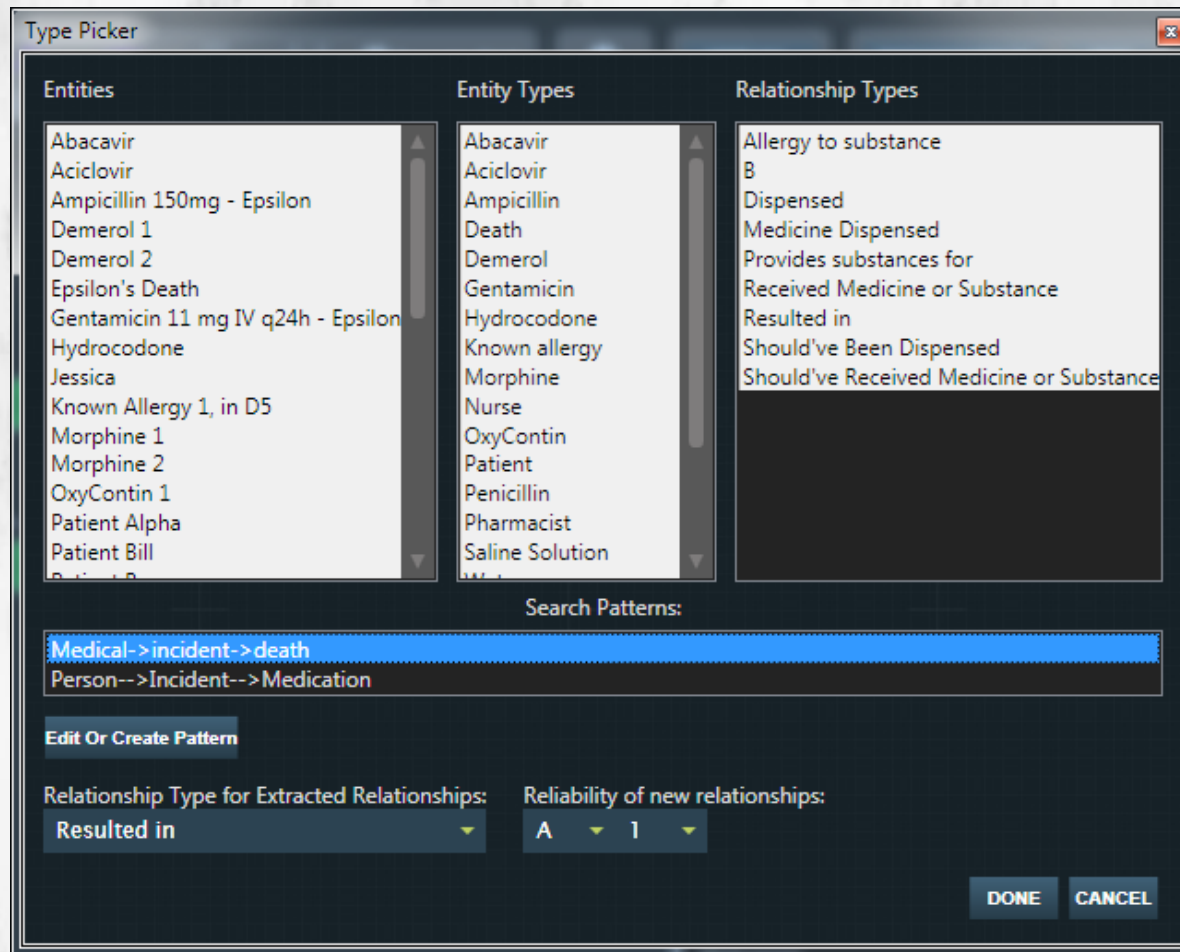
The bottom status bar indicates "Copyright 2011 Ephibian, Inc. and The Arizona Board of Regents on Behalf of the University of Arizona.", "Liana Suantak", and "10/30/2013 14:58 T (-7:00)".



# Link Charts – Growing New Connections

- Suppose the investigator has a hunch as to how entities may be related
- Assuming this can be codified based on the
  - Entities,
  - Types of entities,
  - Types of relationships, and
  - A relationship pattern
- New suspected connections can be made

# Link Charts – Growing New Connections



# Link Charts – Growing New Connections

- Suppose a network administrator want to generate a list of insider suspects
- The administrator could create suspect-links using:  
AttackEvent → Computers → Users → Coworkers
- The results could be further processed with additional filters and queries

# Game Theoretic Decision Support

- Game theory has been applied to cyber-security to
  - Resource allocation [1-4]
  - Countermeasures or responses to an attack [5-11]
- We present a tool for determining optimal responses to an attacker
  - Grounded in stochastic game theoretic context

# Game Theoretic Decision Support

**Decision Support Tool** X

**GAME BUILDER** ?

Name\*

Description

Model\*

Action Set\*

Rule Set\*

Turns

The Model describes what states that game will track  
 The Action Set describes what actions can be performed in the game  
 The Rule Set describes when which actions are valid/invalid  
 "Rational" players should have a risk aversion between -1 to +1  
 The accuracy of the game run is dependant on the amount of available system memory

---

**PLAYERS**

|               | Player 1 <input type="text" value="Medical Staff"/> |                                 |                                 |                                  | Player 2 <input type="text" value="Infectious agent"/> |                                 |                                |                                 |                                   |
|---------------|---|---------------------------------|---------------------------------|----------------------------------|--|---------------------------------|--------------------------------|---------------------------------|-----------------------------------|
|               | Initial   | Payoff                          |                                 | Risk Aversion                    | Initial  | Payoff                          |                                | Risk Aversion                   |                                   |
| Area          | <input type="text" value="60"/>                     | <input type="text" value="2"/>  | <input type="text" value="-1"/> | <input type="text" value="0.8"/> | Area   | <input type="text" value="40"/> | <input type="text" value="1"/> | <input type="text" value="-1"/> | <input type="text" value="-0.1"/> |
| Structures    | <input type="text" value="85"/>                     | <input type="text" value="2"/>  | <input type="text" value="-1"/> |                                  | Structures   | <input type="text" value="15"/> | <input type="text" value="1"/> | <input type="text" value="-1"/> |                                   |
| Capabilities  | <input type="text" value="100"/>                    | <input type="text" value="5"/>  | <input type="text" value="-1"/> |                                  | Capabilities   | <input type="text" value="30"/> | <input type="text" value="1"/> | <input type="text" value="-1"/> |                                   |
| Organizations | <input type="text" value="100"/>                    | <input type="text" value="2"/>  | <input type="text" value="-1"/> |                                  | Organizations  | <input type="text" value="0"/>  | <input type="text" value="1"/> | <input type="text" value="-1"/> |                                   |
| People        | <input type="text" value="95"/>                     | <input type="text" value="10"/> | <input type="text" value="-1"/> |                                  | People   | <input type="text" value="15"/> | <input type="text" value="1"/> | <input type="text" value="-1"/> |                                   |
| Events        | <input type="text" value="95"/>                     | <input type="text" value="5"/>  | <input type="text" value="-1"/> |                                  | Events   | <input type="text" value="5"/>  | <input type="text" value="1"/> | <input type="text" value="-1"/> |                                   |

Max look-ahead

# Game Theoretic Decision Support – Stochastic Context

- A player may not take the optimal action, only probabilistically
- This results in outcome/payoff distributions
  - Need a certainty equivalent to recover a payoff
  - A second-order model takes the expected value and variance into account
  - The relative importance of the variance is determined by the player's risk aversion

# Game Theoretic Decision Support – The Components

- Two players
  - Initial state, payoff function, and risk aversion
- State
  - Defined by user-defined model (*e.g.*, ASCOPE)
    - Area, structures, capabilities, organizations, people, events
- Actions
- Rules
  - Determines when actions are valid and for whom

# Game Theoretic Decision Support

Decision Support Tool

**GAME BUILDER**

Name\* Infectious Disease Spread - scenario

Description An infectious agents is spreading from an unknown sou

Model\* ASCOPE

Action Set\* Vectors and Prevention

Rule Set\* Hospital & Disease

Turns (Create)

The Model describes what states that game will track  
 The Action Set describes what actions can be performed in the game  
 The Rule Set describes when which actions are valid/invalid

"Rational" players should have a risk aversion between -1 to +1

The accuracy of the game run is dependant on the amount of available system memory

**PLAYERS**

|               | Player 1: Medical Staff |      |          |               | Player 2: Infectious agent |      |          |               |
|---------------|-------------------------|------|----------|---------------|----------------------------|------|----------|---------------|
|               | Initial                 | Self | Opponent | Risk Aversion | Initial                    | Self | Opponent | Risk Aversion |
| Area          | 60                      | 2    | -1       | 0.8           | 40                         | 1    | -1       | -0.1          |
| Structures    | 85                      | 2    | -1       |               | 15                         | 1    | -1       |               |
| Capabilities  | 100                     | 5    | -1       |               | 30                         | 1    | -1       |               |
| Organizations | 100                     | 2    | -1       |               | 0                          | 1    | -1       |               |
| People        | 95                      | 10   | -1       |               | 15                         | 1    | -1       |               |
| Events        | 95                      | 5    | -1       |               | 5                          | 1    | -1       |               |

Max look-ahead



# Game Theoretic Decision Support – The Action Set

- The most costly part of game theoretic analysis comes from the construction of the actions in a game
- ATRAP allows the user to recycle actions from other games and to create new actions
- Each action invokes an affine transformation on the game state
  - For an  $n$ -dimensional model, each action has an  $2n \times 2n+1$  transformation matrix.



# Game Theoretic Decision Support – The Rule Set

- Not all actions are always valid
  - An action maybe replaced with a more/less effective action provided certain circumstances have been met
- Each action may trigger a rule
  - Allowing/disallowing/replacing one set of actions with another set of actions
  - These may last for any number of turns
  - May affect either player

# Game Theoretic Decision Support – The Rule Set

The screenshot displays three overlapping windows from a 'Decision Support Tool'.

**GAME EDITOR (Top Left):**

- Name: Infectious Disease Spread - scenario
- Description: An infectious agents is spreading from an unknown sou
- Model: ASCOPE
- Action Set: Vectors and Prevention
- Rule Set: Hospital & Disease
- Turns: (Create)

**PLAYERS (Middle Left):**

Player 1: Medical Staff

| Area         | Payoff  |      |          |               |
|--------------|---------|------|----------|---------------|
|              | Initial | Self | Opponent | Risk Aversion |
| Area         | 60      | 2    | -1       | 0.8           |
| Structures   | 85      | 2    | -1       |               |
| Capabilities | 100     | 5    | -1       |               |

**RULE SET BUILDER (Top Right):**

Name: Hospital & Disease

| Name   | When     | Performs         |
|--|----------|------------------|
| Prevent duplication - centralization of food     | Player 1 | H-Centralize th  |
| Build Resistance 2                               | Player 1 | H-Add. Steriliza |
| Build Resistance                                 | Player 1 | H-Add. Steriliza |
| Prevent duplication - lift quarantine            | Player 1 | H-Lift Quarantin |
| Prevent duplication - centralization of cleaning | Player 1 | H-Centralize th  |
| Prevent duplication - aaf                        | Player 1 | H-Add. Air Filtr |
| Prevent duplication - locking staff rounds       | Player 1 | H-Lock staffing  |
| Asymmetric: Hospital                             |          |                  |
| Further Research -> Treatment                    | Player 1 | H-Test drugs/v   |
| Research -> Further Research                     | Player 1 | H-Test Patients' |

**RULE BUILDER (Bottom):**

Name: Build Resistance

Options:  Is Primary, 5 Time to live

When:  Player 1,  Player 2

Performs: Action: H-Add. Sterilization (Low) [Replace] Action: H-Add. Sterilization (Low)

With: Action: H-Add. Sterilization (Me)

For:  Player 1,  Player 2,  Actor,  Recipient

Buttons: Add Action, Add, Add Action, Add, Add Action, Add, CANCEL, OK

# Game Theoretic Decision Support – Running the Game

- The user may optionally enter a look-ahead amount for the game
  - Otherwise the system takes its best guess at how far it can look ahead without exhausting memory.

Decision Support Tool

GAME BUILDER

Name: Infectious Disease Spread - scenario

Description: An infectious agents is spreading from an unknown sou

Model: ASCOPE

Action Set: Vectors and Prevention

Rule Set: Hospital & Disease

Turns: (Create)

PLAYERS

Player 1: Medical Staff

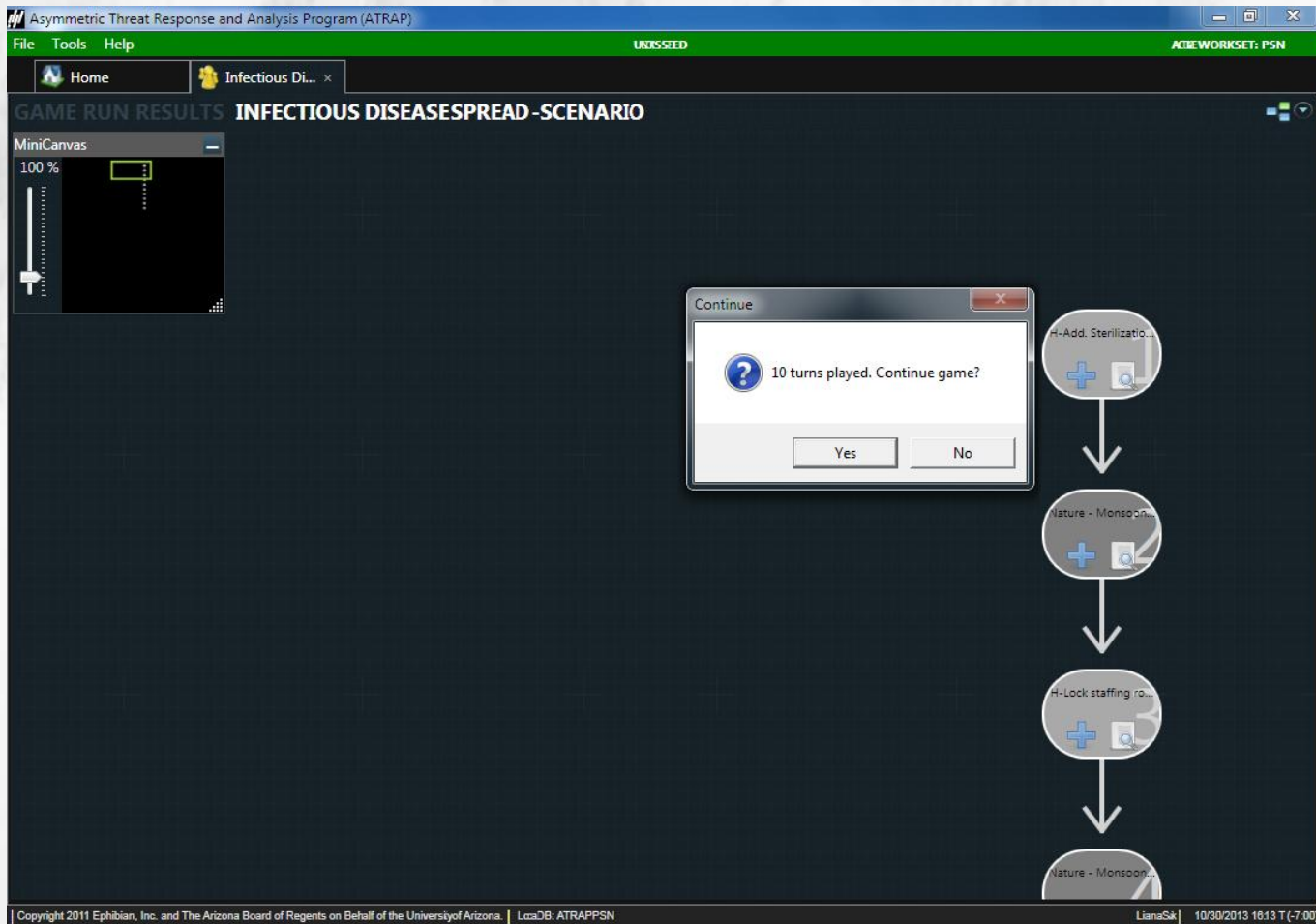
|               | Payoff  |      |          |               |
|---------------|---------|------|----------|---------------|
|               | Initial | Self | Opponent | Risk Aversion |
| Area          | 60      | 2    | -1       | 0.8           |
| Structures    | 85      | 2    | -1       |               |
| Capabilities  | 100     | 5    | -1       |               |
| Organizations | 100     | 2    | -1       |               |
| People        | 95      | 10   | -1       |               |
| Events        | 95      | 5    | -1       |               |

Player 2: Infectious agent

|               | Payoff  |      |          |               |
|---------------|---------|------|----------|---------------|
|               | Initial | Self | Opponent | Risk Aversion |
| Area          | 40      | 1    | -1       | -0.1          |
| Structures    | 15      | 1    | -1       |               |
| Capabilities  | 30      | 1    | -1       |               |
| Organizations | 0       | 1    | -1       |               |
| People        | 15      | 1    | -1       |               |
| Events        | 5       | 1    | -1       |               |

Max look-ahead: [ ] RUN CLOSE SAVE

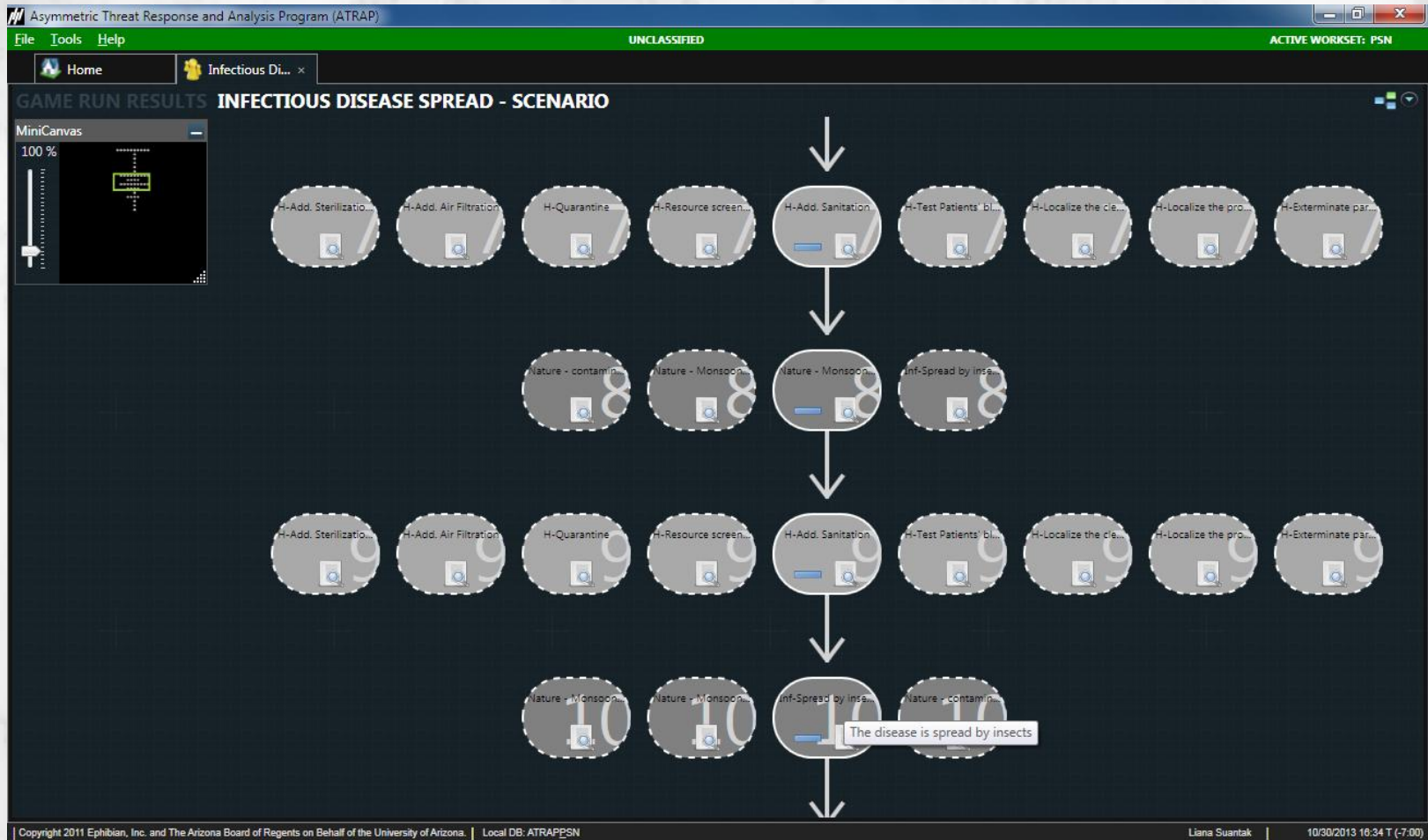
# Game Theoretic Decision Support – Running the Game



# Game Theoretic Decision Support – Running the Game

- Our game avoids artifacts by technically having no end
  - Even the last move shown is still looking as far ahead as the look-ahead permits
  - Actions remain valid until a rule disallows them
- The light (dark) gray boxes represent the first (second) player's actions
- The resulting path through the game tree is the one each player thinks is optimal under uncertainty

# Game Theoretic Decision Support – Introspection

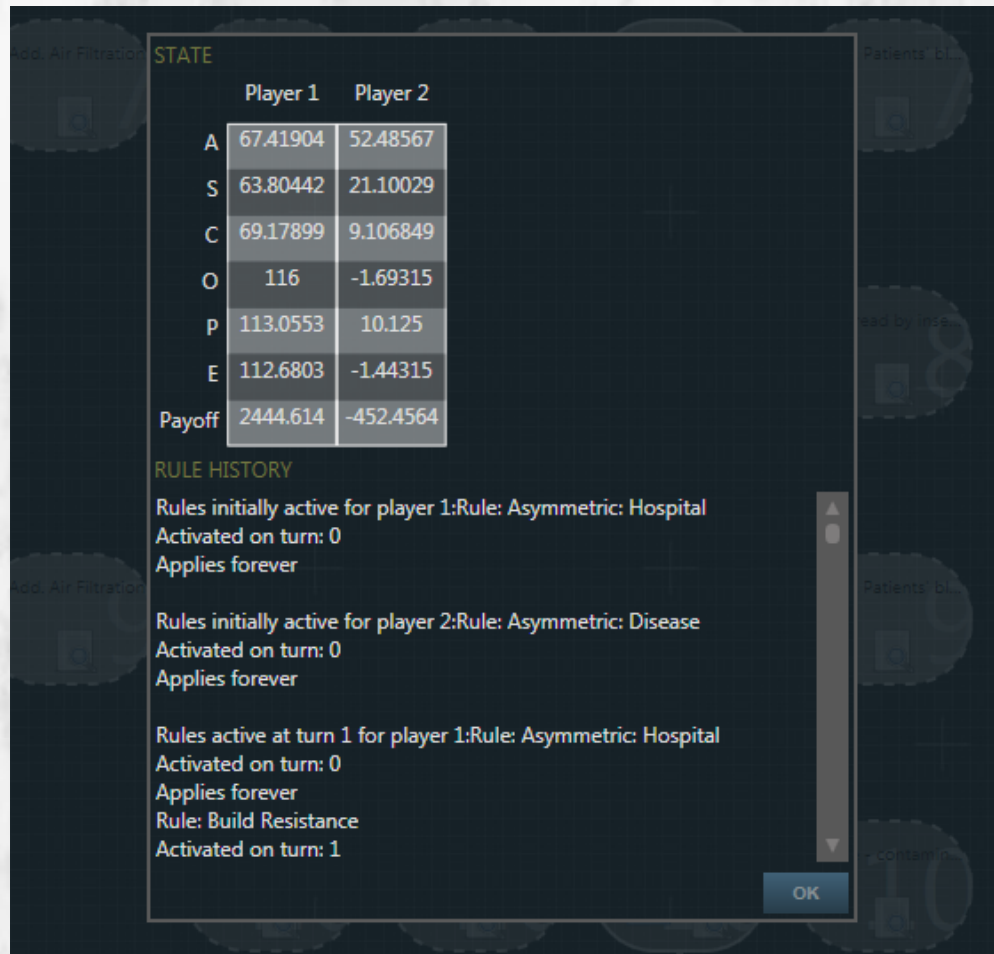




# Game Theoretic Decision Support – Introspection

- Each action can be expanded to show alternatives at that point in time
- Each alternative can have its state inspected
- When inspecting an action or its alternative, a description of the rules that triggered are also provided
  - Much like code, complex games may require debugging

# Game Theoretic Decision Support – Introspection



The screenshot displays a game decision support interface. At the top, it shows a payoff matrix for two players, Player 1 and Player 2, across six strategies: A, S, C, O, P, and E. Below the matrix is a 'RULE HISTORY' section detailing the activation of various rules for both players over time.

|        | Player 1 | Player 2  |
|--------|----------|-----------|
| A      | 67.41904 | 52.48567  |
| S      | 63.80442 | 21.10029  |
| C      | 69.17899 | 9.106849  |
| O      | 116      | -1.69315  |
| P      | 113.0553 | 10.125    |
| E      | 112.6803 | -1.44315  |
| Payoff | 2444.614 | -452.4564 |

**RULE HISTORY**

Rules initially active for player 1: Rule: Asymmetric: Hospital  
Activated on turn: 0  
Applies forever

Rules initially active for player 2: Rule: Asymmetric: Disease  
Activated on turn: 0  
Applies forever

Rules active at turn 1 for player 1: Rule: Asymmetric: Hospital  
Activated on turn: 0  
Applies forever  
Rule: Build Resistance  
Activated on turn: 1

OK

# Game Theoretic Decision Support – Converting to a Query

The screenshot displays the Asymmetric Threat Response and Analysis Program (ATRAP) interface. The title bar reads "Asymmetric Threat Response and Analysis Program (ATRAP)". The menu bar includes "File", "Tools", and "Help". The status bar shows "UNCLASSIFIED" and "ACTIVE WORKSET: PSN". The main window title is "Infectious Di...".

The central area is titled "GAME RUN RESULTS INFECTIOUS DISEASE SPREAD - SCENARIO". It features a "MiniCanvas" on the left with a zoom level of "100 %". The main display is a decision tree with four levels of nodes, each represented by a circular icon with a magnifying glass. The nodes are arranged in a grid-like structure with arrows indicating the flow from top to bottom.

The nodes in the first level are: "H-Add. Sterilization...", "H-Add. Air Filtration", "H-Quarantine", "H-Resource screen...", "H-Add. Sanitation", "H-Test Patients' bl...", "H-Localize the cie...", "H-Localize the pro...", and "H-Exterminate par...".

The nodes in the second level are: "Nature - contamin...", "Nature - Monsoon...", "Nature - Monsoon...", and "Inf-Spread by ins...".

The nodes in the third level are: "H-Add. Sterilization...", "H-Add. Air Filtration", "H-Quarantine", "H-Resource screen...", "H-Add. Sanitation", "H-Test Patients' bl...", "H-Localize the cie...", "H-Localize the pro...", and "H-Exterminate par...".

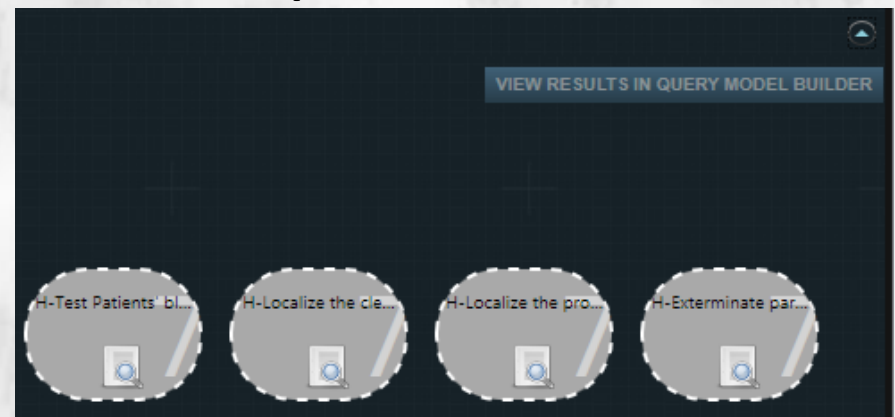
The nodes in the fourth level are: "Nature - Monsoon...", "Nature - Monsoon...", "Inf-Spread by ins...", and "Nature - contamin...".

A tooltip is visible over the "Inf-Spread by ins..." node in the fourth level, containing the text: "The disease is spread by insects".

The footer contains the following information: "Copyright 2011 Ephibian, Inc. and The Arizona Board of Regents on Behalf of the University of Arizona. | Local DB: ATRAPPSN | Liana Suantak | 10/30/2013 16:34 T (-7:00)".

# Game Theoretic Decision Support – Converting to a Query

- In the top right corner there is an option to send the resulting path through the game tree to another tool
- This query model builder allows the game to be instantiated as a series of queries
  - Allows for the search of empirical evidence supporting such an outcome



# Game Theoretic Decision Support – Converting to a Query

The screenshot displays the Asymmetric Threat Response and Analysis Program (ATRAP) interface. The title bar reads "Asymmetric Threat Response and Analysis Program (ATRAP)" and the status bar shows "UNCLASSIFIED" and "ACTIVE WORKSET: PSN". The main window title is "GAME RUN QUERY MODEL BUILDER INFECTIOUS DISEASE SPREAD - SCENARIO".

The interface is divided into several panels:

- ACTION CHAIN:** A vertical sequence of four nodes: "H-Add. Sterilizatio...", "Nature - Monsoon...", "H-Lock staffing rou...", and "Nature - Monsoon...".
- INSTANTIATION QUERY MODEL:** A "MiniCanvas" showing a 50% progress bar and a graph with a downward-sloping line. Below it is a flowchart with nodes: "Dillinger Medication Related Events", "All PSN Events", and "Dillinger Medication Related Events".
- REACTION QUERY MODEL:** A "MiniCanvas" showing a 50% progress bar and a graph with a downward-sloping line. Below it is a flowchart with nodes: "Rain", "Rain To Location", "Wet Location's patients", and "Person To Locations".
- Indicators:** A section titled "Your Indicator library." with a filter and a table containing one entry: "Person To Location".

The bottom status bar contains the following text: "Copyright 2011 Epihbian, Inc. and The Arizona Board of Regents on Behalf of the University of Arizona. | Local DB: ATRAPPSN | Liana Suantak | 10/30/2013 16:41 T (-7:00)".

# Game Theoretic Decision Support – Converting to a Query

- Queries have an input and output type
- Queries can search any entity data
- Queries may be chained together
- Queries may be modified by soft-factors (skillfulness or organization size)
  - Allows for better sorting of suspects

# Conclusions

- ATRAP is a toolbox full of human-in-the-loop data analysis tools
  - Analysis of relationships between entities
  - Game Theory to help predict potential outcomes and how to best respond
- Geared toward security data mining

# References

- [1] Hausken, K.: Strategic defense and attack of series systems when agents move sequentially. IIE Trans. 43(7), 483–504 (2011). DOI 10.1080/0740817X.2010. 541178. URL <http://www.tandfonline.com/doi/abs/10.1080/0740817X.2010.541178>
- [2] Hausken, K., Bier, V.M., Azaiez, M.N.: Defending against terrorism, natural disaster, and all hazards. In: Bier, V.M., Azaiez, M.N. (eds.) Game Theoretic Risk Analysis of Security Threats, International Series in Operations Research & Management Science, vol. 128, chap. 4, pp. 1–33. Springer, New York (2009). DOI 10. 1007/978-0-387-87767-9\_4. URL [http://dx.doi.org/10.1007/978-0-387-87767-9\\_4](http://dx.doi.org/10.1007/978-0-387-87767-9_4)



# References

- [3] Hausken, K., Zhuang, J.: The timing and deterrence of terrorist attacks due to exogenous dynamics. *Journal of Operations Research Society* 63(6), 726–735 (2012). URL <http://dx.doi.org/10.1057/jors.2011.79>
- [4] Hausken, K., Zhuang, J.: Governments' and terrorists' defense and attack in a t-period game. *Decis. Anal.* 8(1), 46–70 (2011). DOI 10.1287/deca.1100.0194

# References

- [5] Luo, Y., Szidarovszky, F., Al-Nashif, Y., Hariri, S.: A game theory based risk and impact analysis method for intrusion defense systems. In: 2009 IEEE/ACS International Conference on Computer Systems and Applications (AICCSA), pp. 975–982. IEEE (2009)
- [6] Luo, Y., Szidarovszky, F., Al-Nashif, Y., Hariri, S.: Game theory based network security. *J. Inf. Secur.* 1, 41–44 (2010)
- [7] Luo, Y., Szidarovszky, F., Al-Nashif, Y., Hariri, S.: A fictitious play approach for multi-stage intrusion defense systems. *Int. J. Inf. Secur.* (2011). In press

# References

- [8] Shen, D., Chen, G., Blasch, E., Tadda, G.: Adaptive markov game theoretic data fusion approach for cyber network defense. In: Military Communications Conference, 2007. MILCOM 2007. IEEE, pp. 1–7. Orlando, FL, USA (2007). DOI 10.1109/MILCOM.2007.4454758
- [9] Szidarovszky, F., Luo, Y.: Optimal protection against random attacks. Reliab. Eng. Syst. Saf. (2013). Submitted for publication

# References

- [10] Valenzuela, M., Rozenblit, J., Suantak, L.: Decision support using deterministic equivalents of probabilistic game trees. In: Proceedings of the 2012 19th IEEE International Conference and Workshops on the Engineering of Computer Based Systems (ECBS), pp. 142–149. Novi Sad, Serbia, Europe (2012). DOI 10.1109/ECBS.2012.22
- [11] Zonouz, S., Khurana, H., Sanders, W., Yardley, T.: RRE: A game-theoretic intrusion response and recovery engine. In: 2009 DSN IEEE/IFIP International Conference on Dependable Systems Networks, pp. 439–448. Lisbon (2009). DOI 10.1109/DSN.2009.5270307