Asymmetric Threat Response and Analysis Program

Michael L. Valenzuela

Jerzy W. Rozenblit

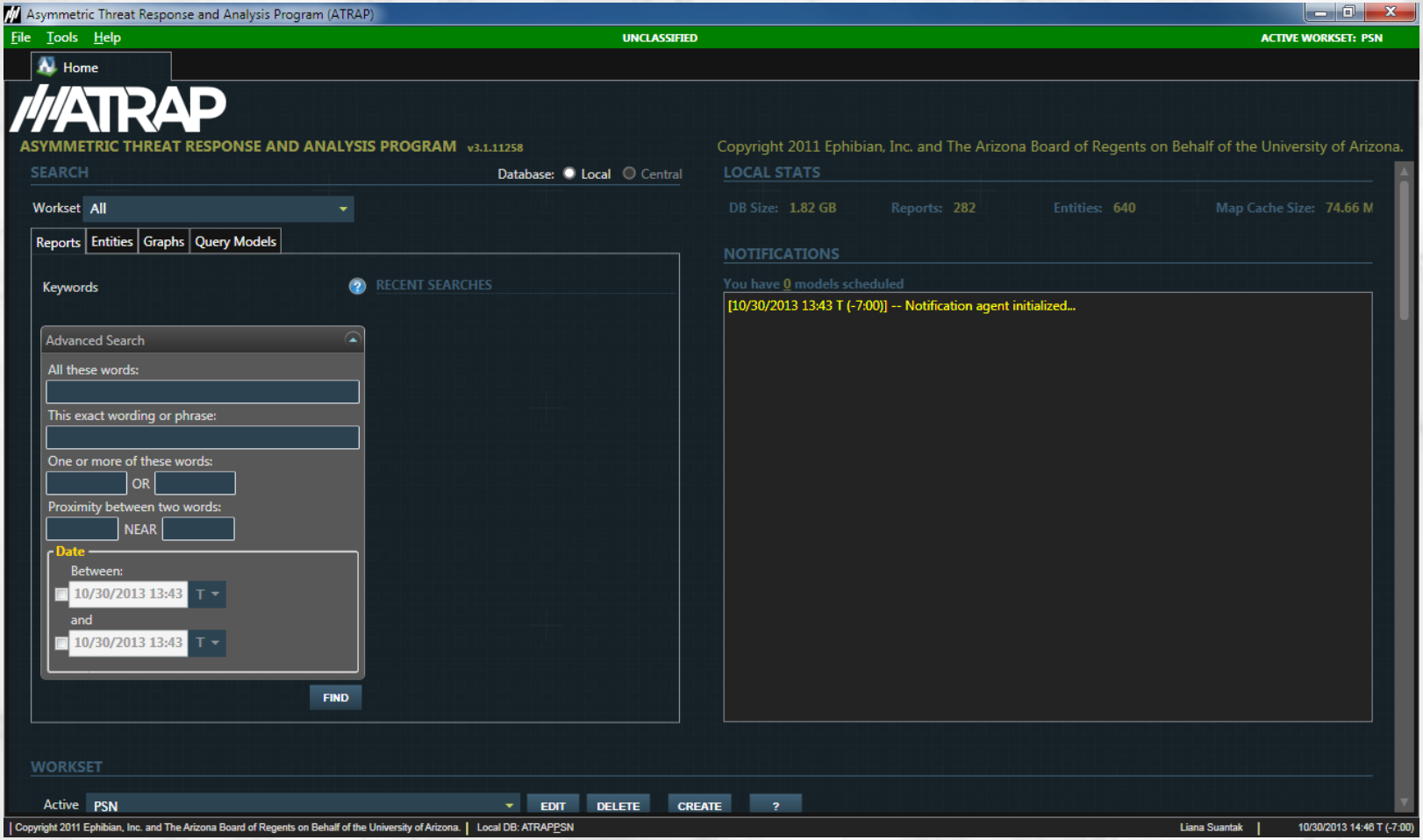
Overview

- 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



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

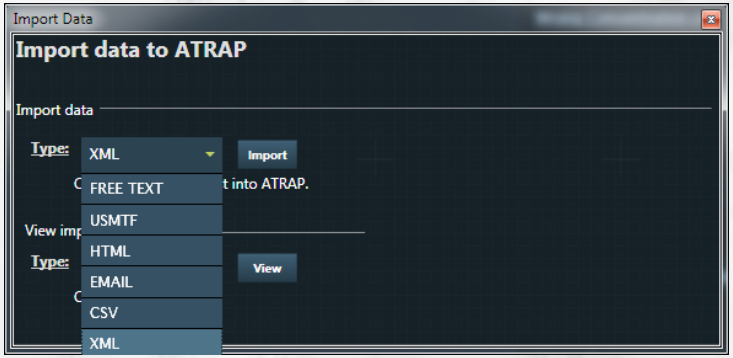
- Think about this
  - Inside jobs cause the majority of damage
  - This tool helps an analyst/detective trace from evidence back to the insider(s)
- Suppose
  - Network traffic is available and events have already been detected via some other tool
  - Some connections between individuals, computers,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

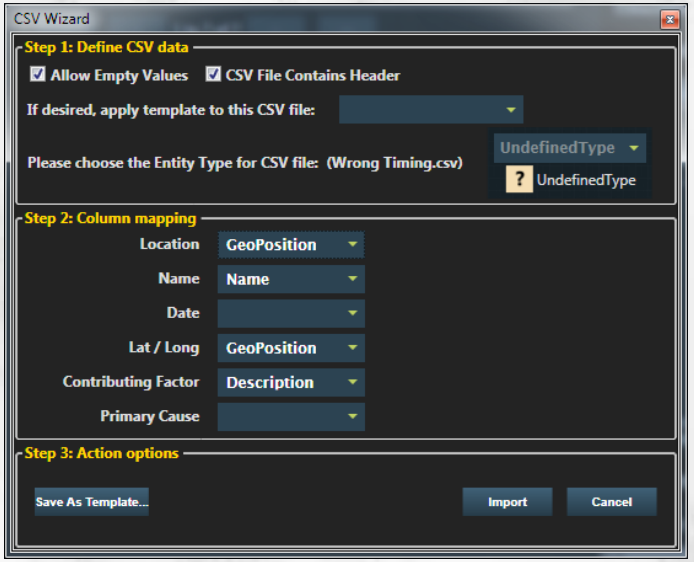
Data Ingestion

- 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

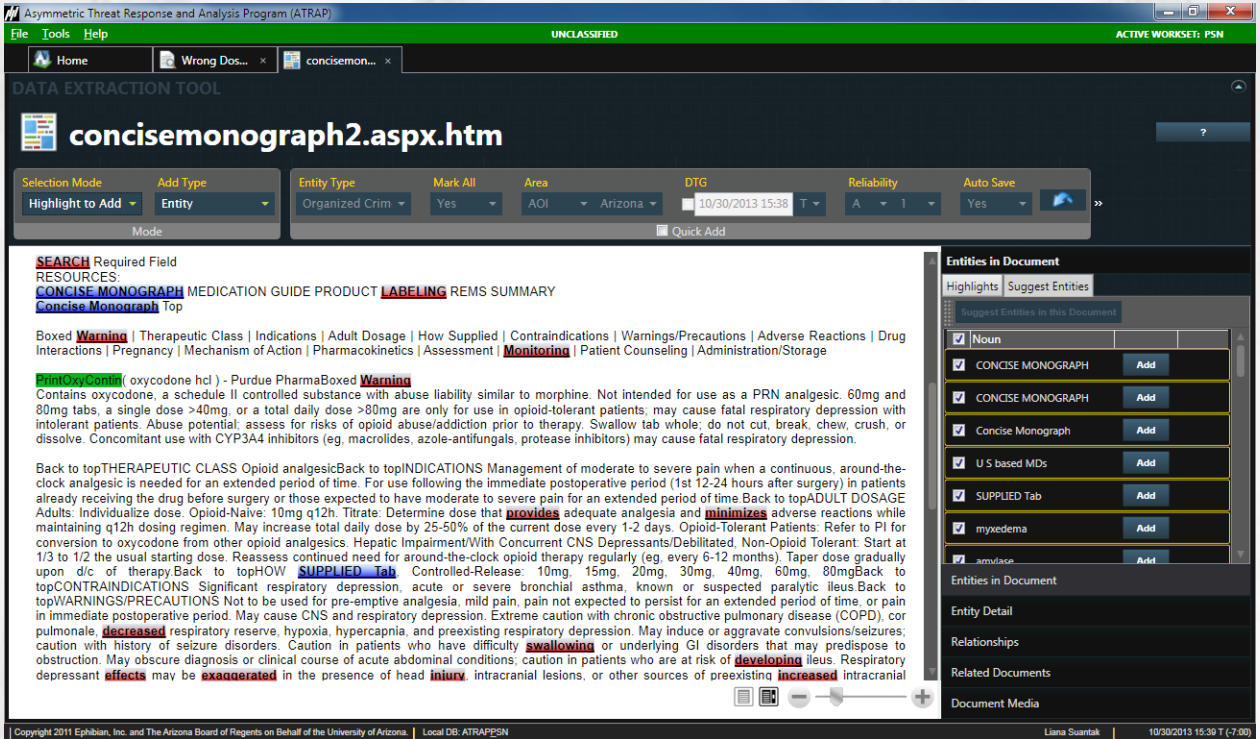
- Structured data can be directly imported as any user defined types.
  - E.g., provided a user defined meta-protocol, each field can be imported from the structured data
  - Nonstandard protocols can be user defined or subtyped





Data Ingestion – free text

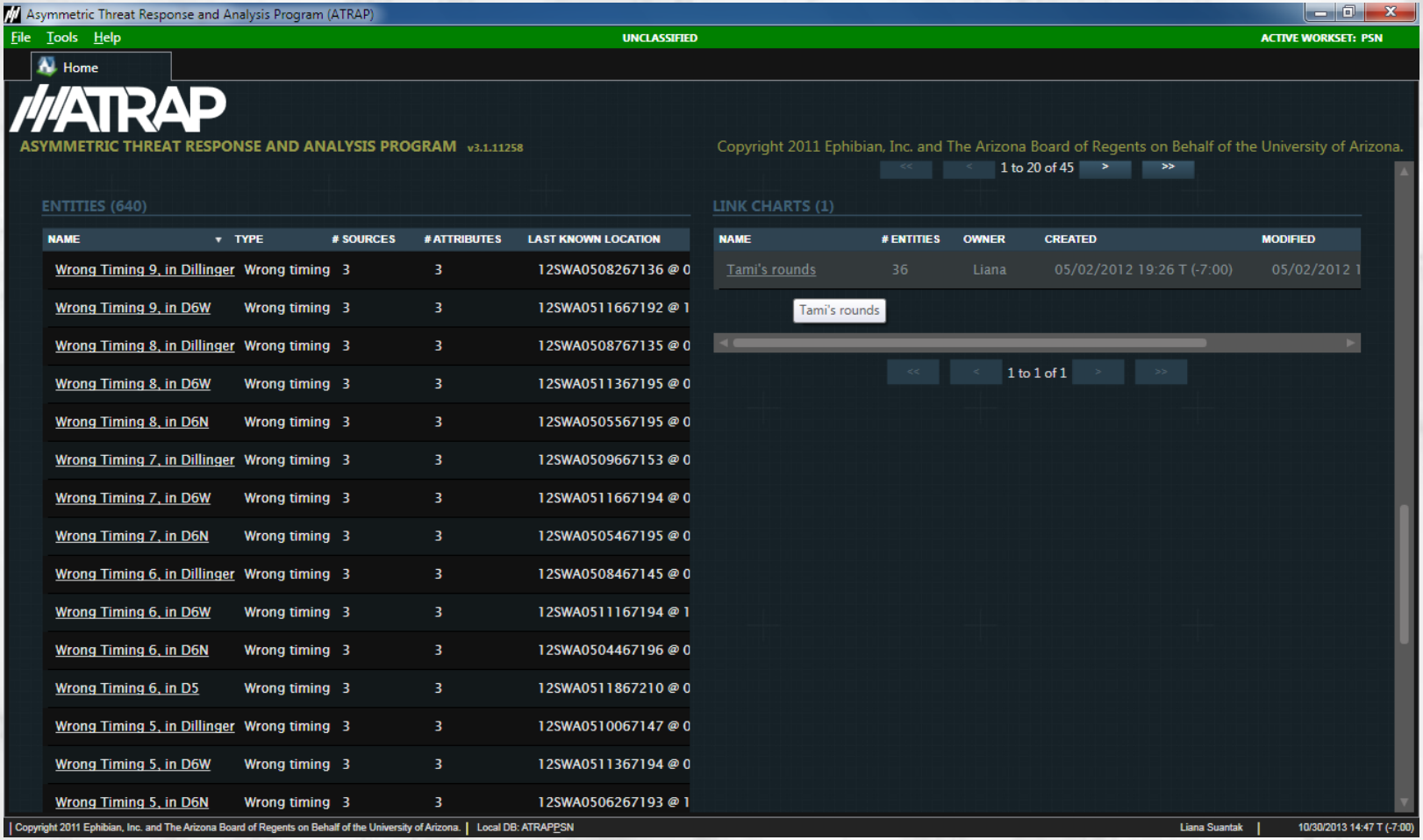
- Entities (structured information) can be extracted from free text
  - ATRAP provides some natural language processing
  - Still requires the use of a person to create a structured piece of information from the text



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

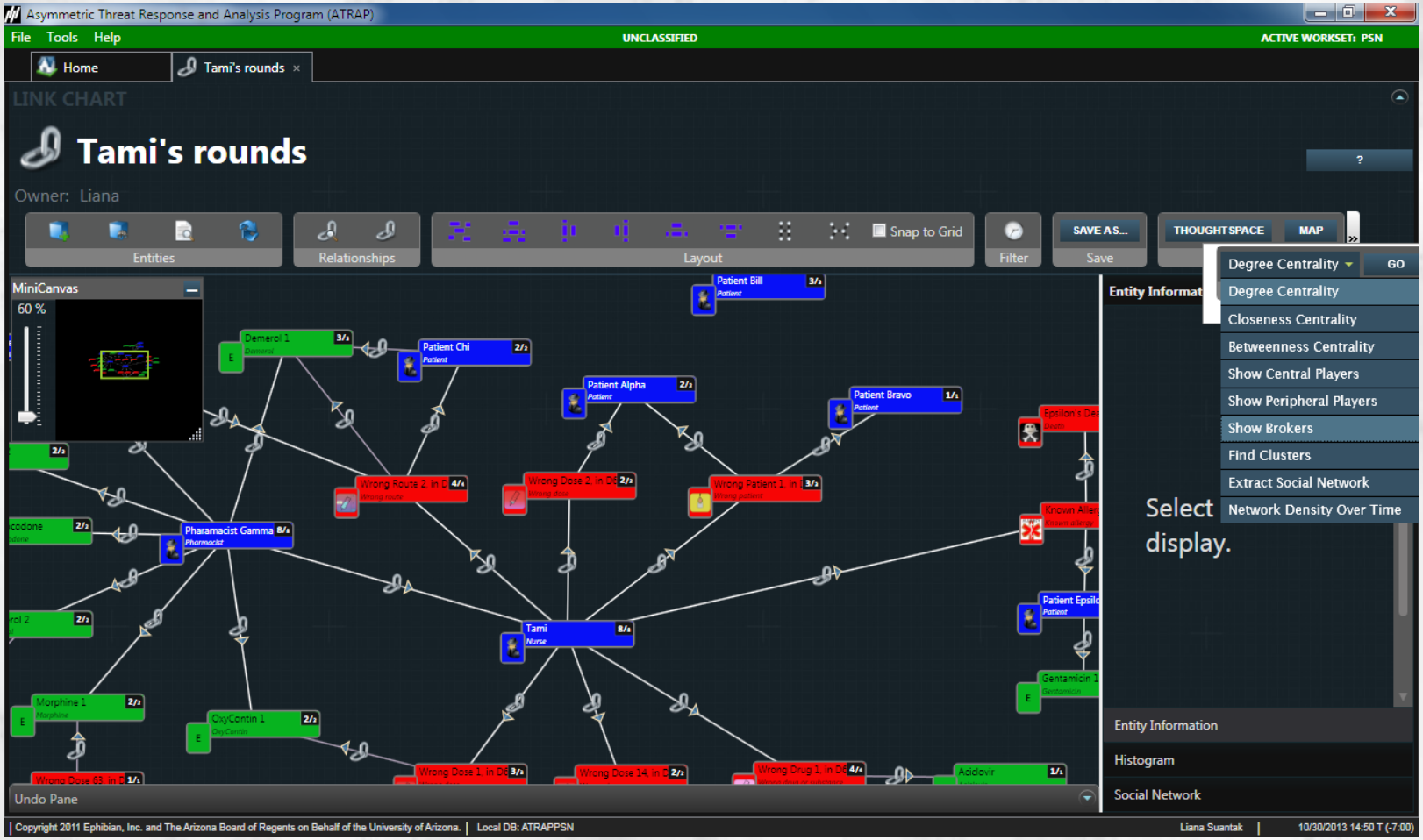
Link Charts


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
Wrong Timing 9, in Dillinger Wrong timing 3 3 12SWA0508267136 @ 0
Wrong Timing 9, in D6W Wrong timing 3 3 12SWA0511667192 @ 1
Wrong Timing 8, in Dillinger Wrong timing 3 3 12SWA0508767135 @ 0
Wrong Timing 8, in D6W Wrong timing 3 3 12SWA0511367195 @ 0
Wrong Timing 8, in D6N Wrong timing 3 3 12SWA0505567195 @ 0
Wrong Timing 7, in Dillinger Wrong timing 3 3 12SWA0509667153 @ 0
Wrong Timing 7, in D6W Wrong timing 3 3 12SWA0511667194 @ 0
Wrong Timing 7, in D6N Wrong timing 3 3 12SWA0505467195 @ 0
Wrong Timing 6, in Dillinger Wrong timing 3 3 12SWA0508467145 @ 0
Wrong Timing 6, in D6W Wrong timing 3 3 12SWA0511167194 @ 1
Wrong Timing 6, in D6N Wrong timing 3 3 12SWA0504467196 @ 0
Wrong Timing 6, in D5 Wrong timing 3 3 12SWA0511867210 @ 0
Wrong Timing 5, in Dillinger Wrong timing 3 3 12SWA0510067147 @ 0
Wrong Timing 5, in D6W Wrong timing 3 3 12SWA0511367194 @ 0
Wrong Timing 5, in D6N Wrong timing 3 3 12SWA0506267193 @ 1
LINK CHARTS (1)
NAME # ENTITIES OWNER CREATED MODIFIED
Tami's rounds 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)

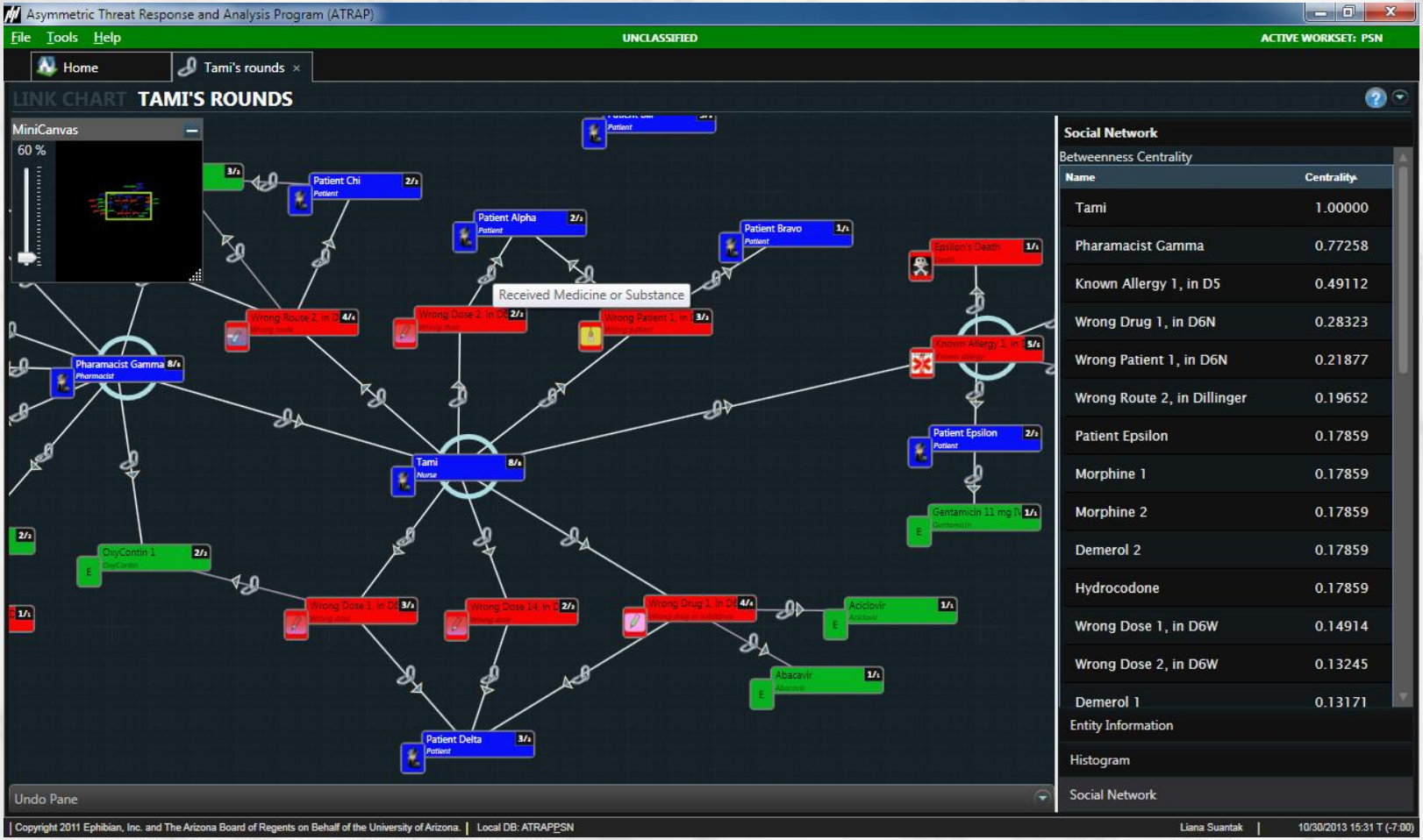
Link Charts

- 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



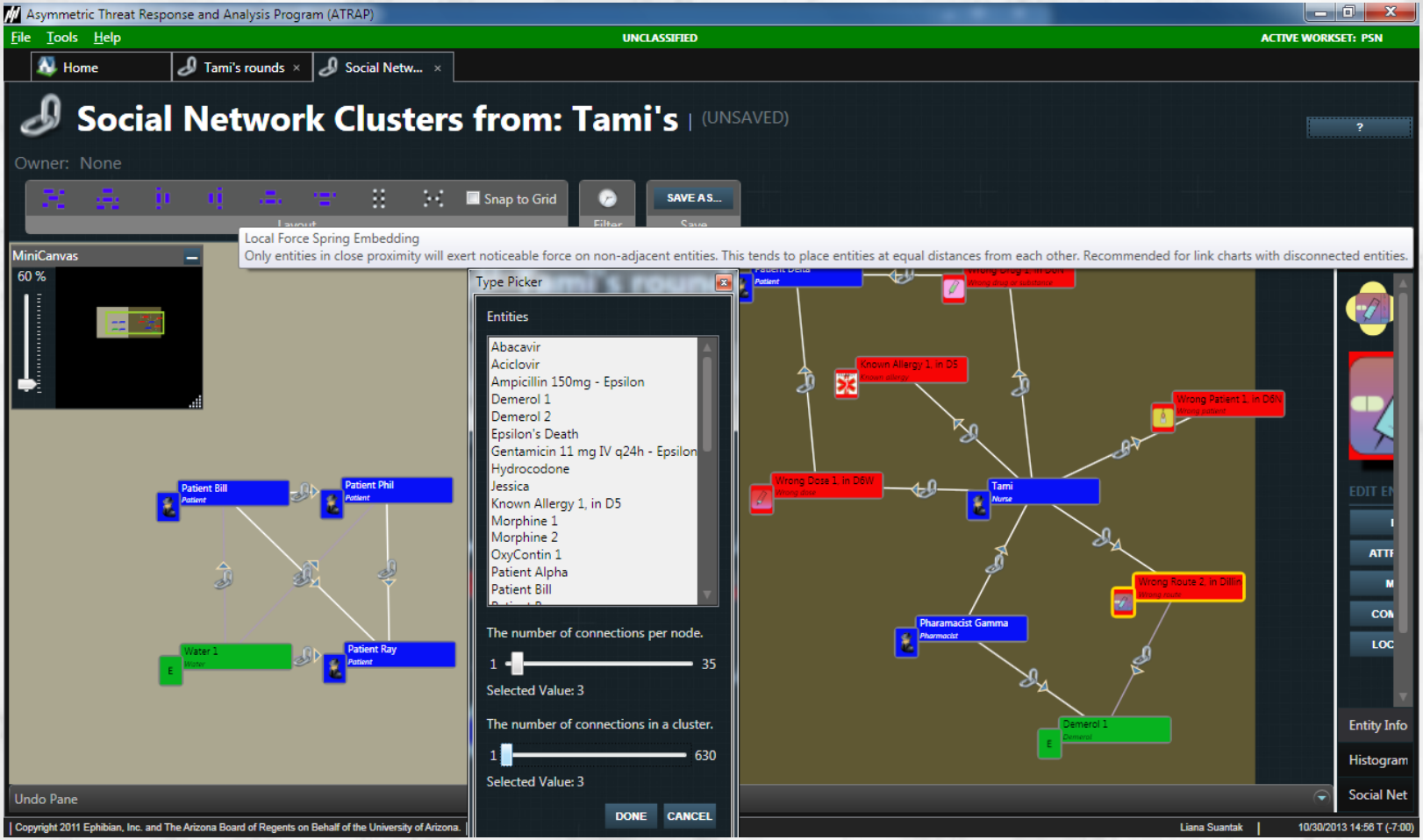
Link Charts – Showing Brokers and Betweenness Centrality



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

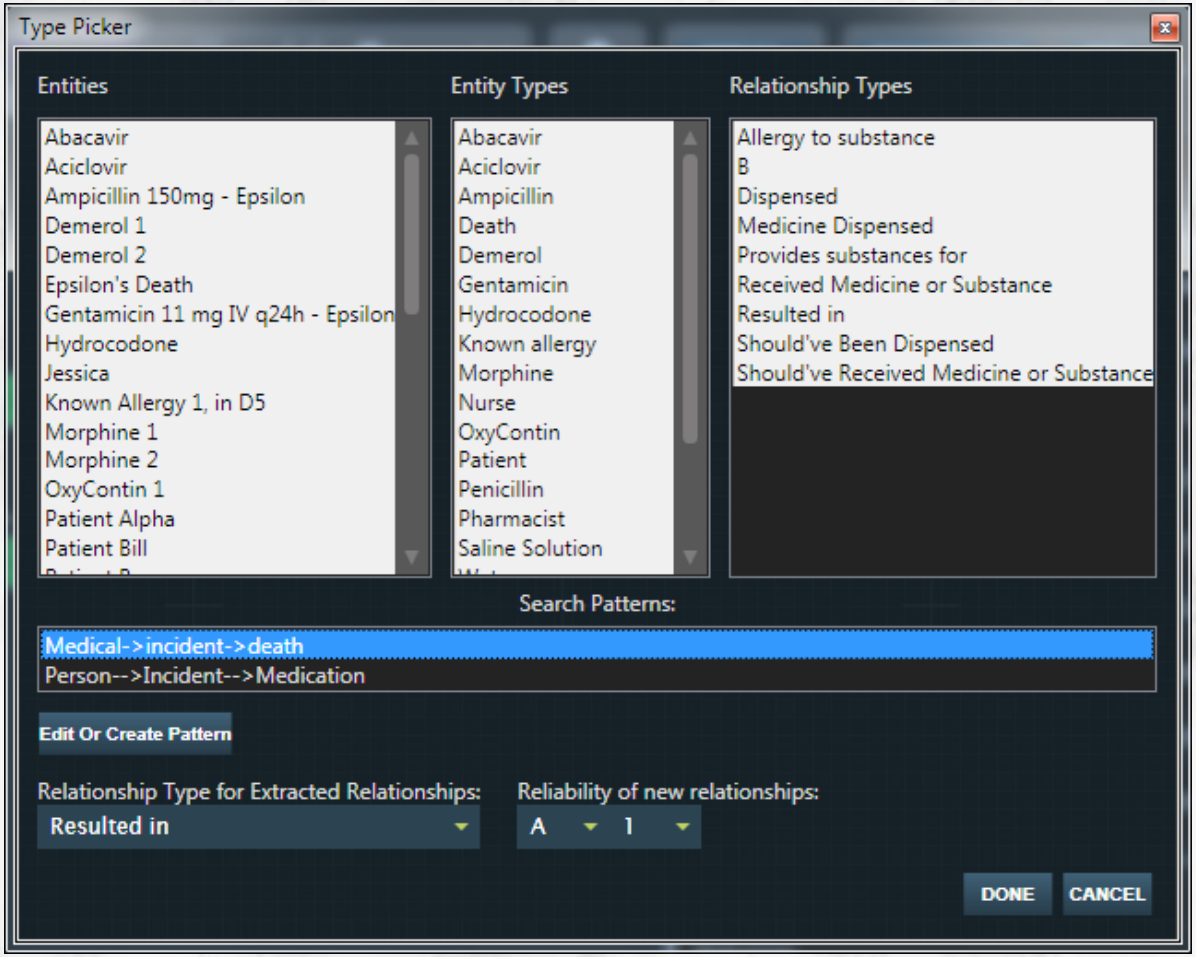
Link Charts – Data Reduction by Clusters



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



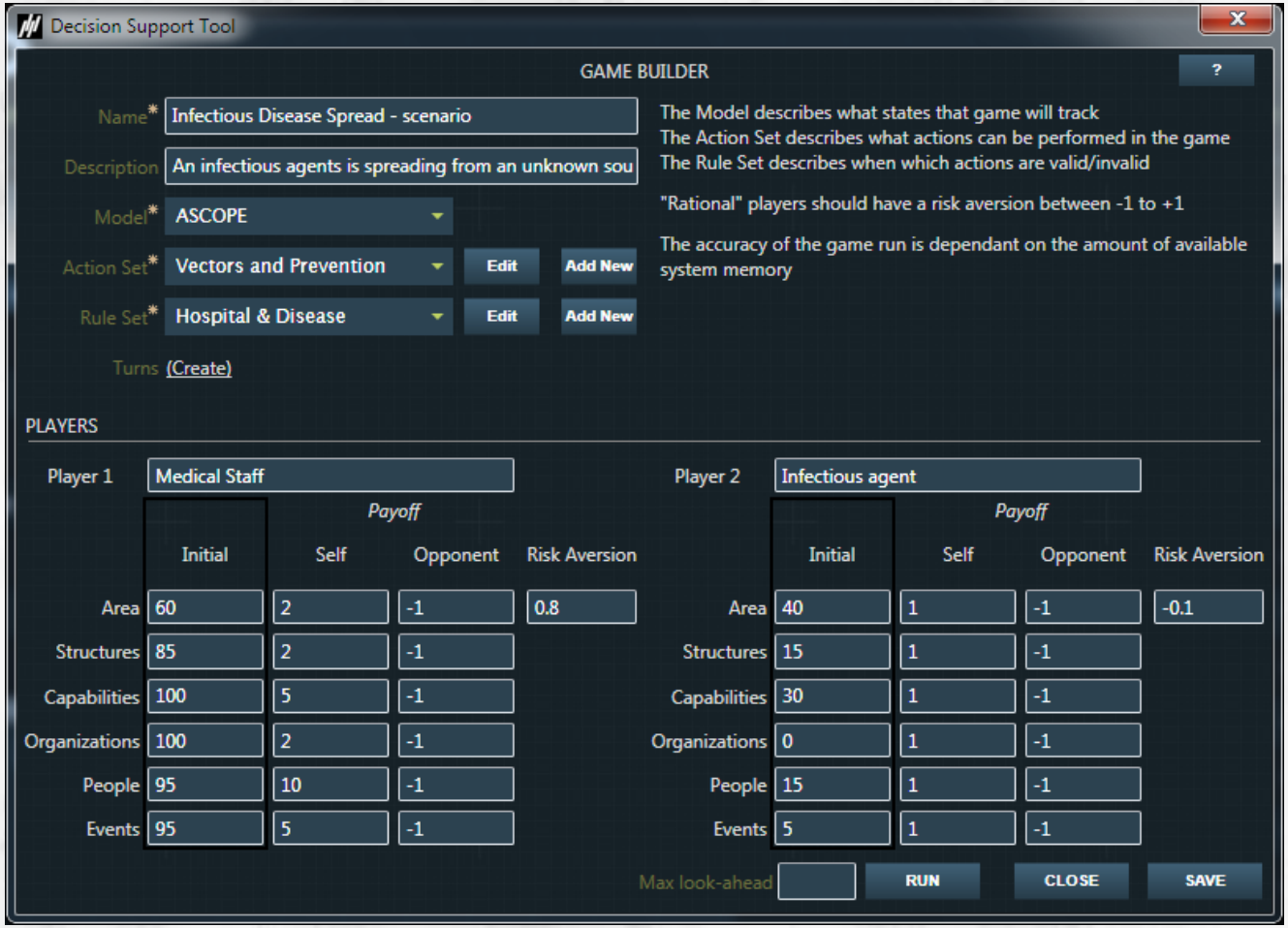
Link Charts – Growing New Connections

- 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



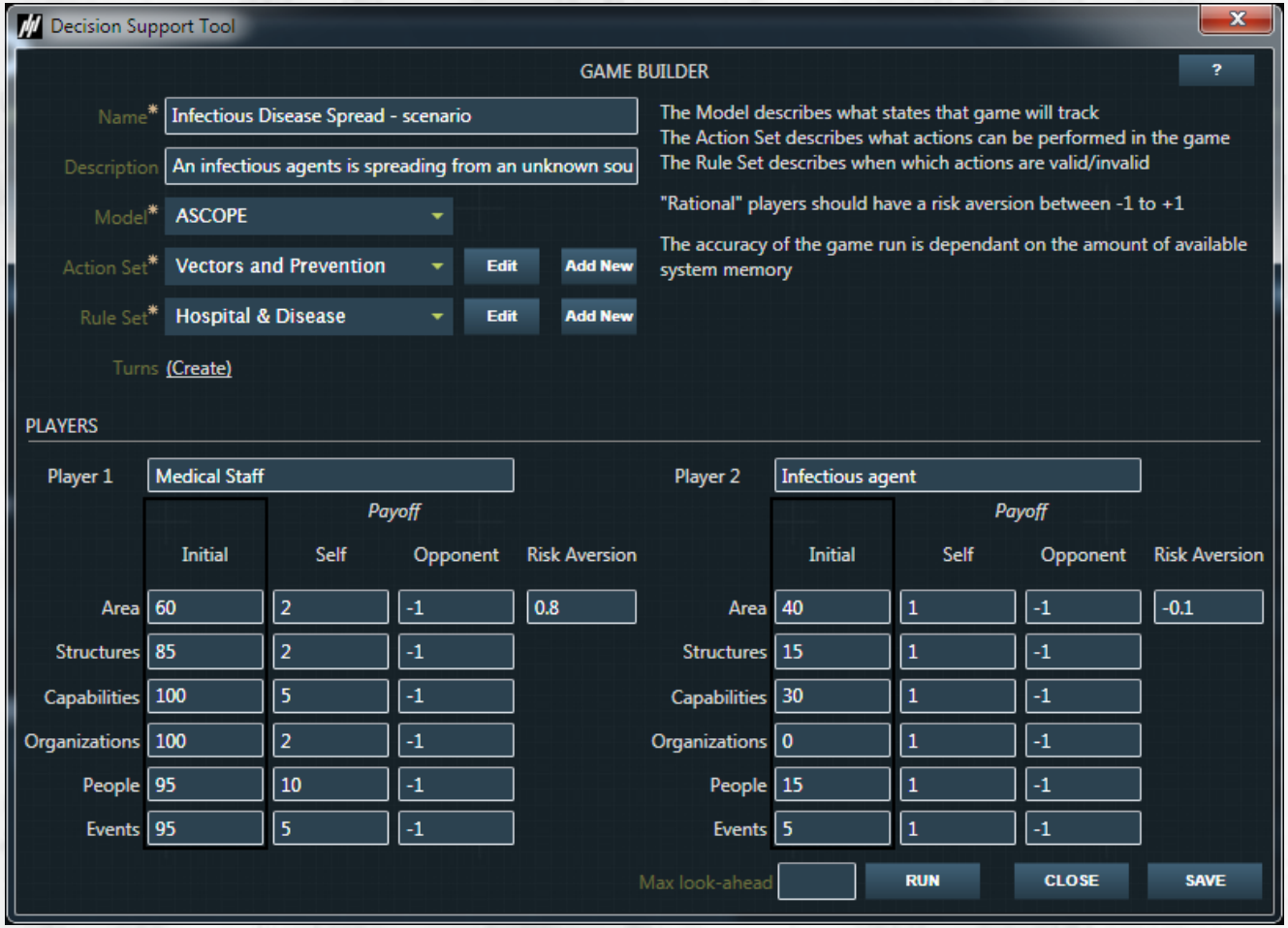
Game Theoretic Decision Support – Stochastic Context

- A play 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

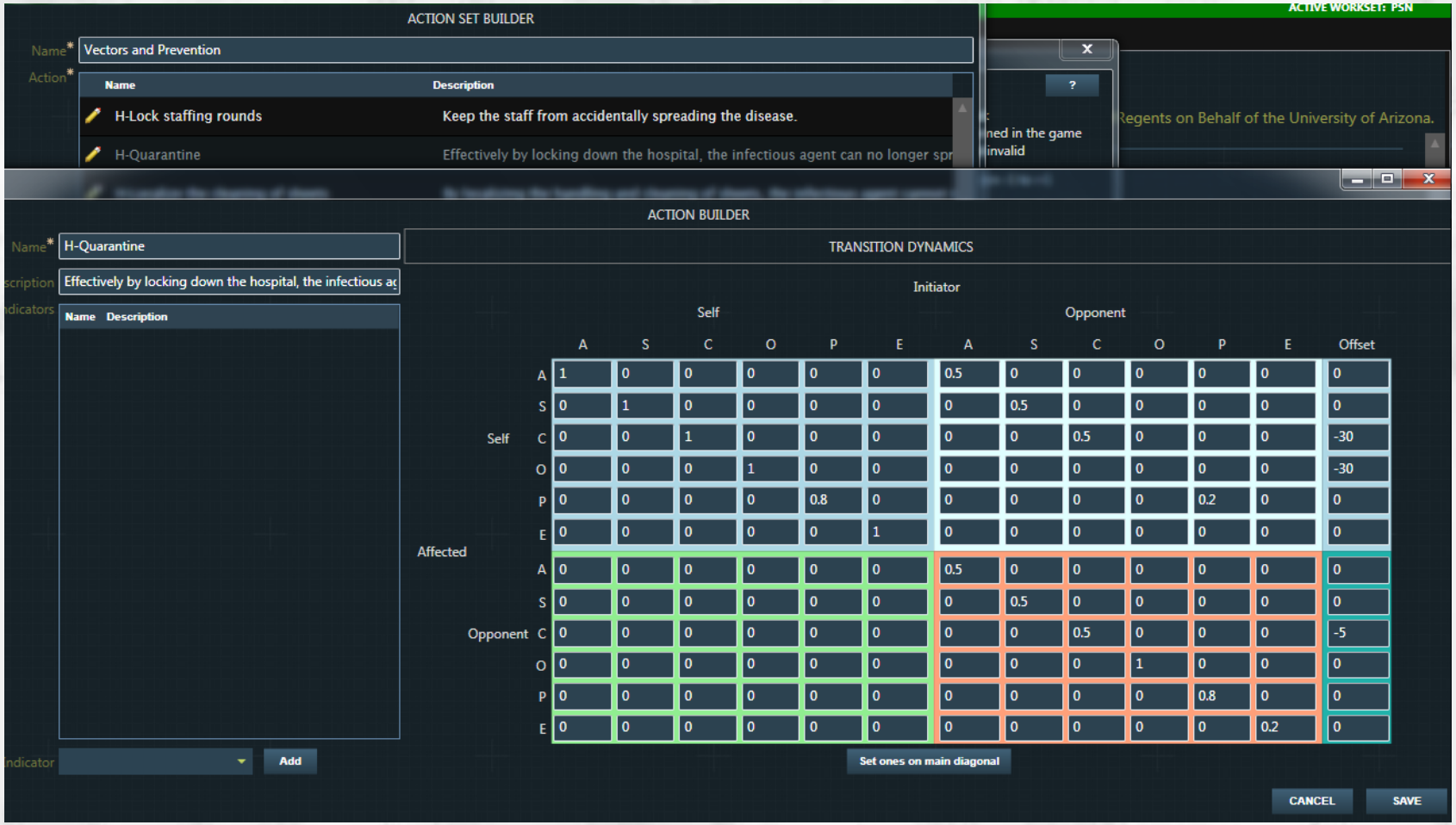
Game Theoretic Decision Support



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.

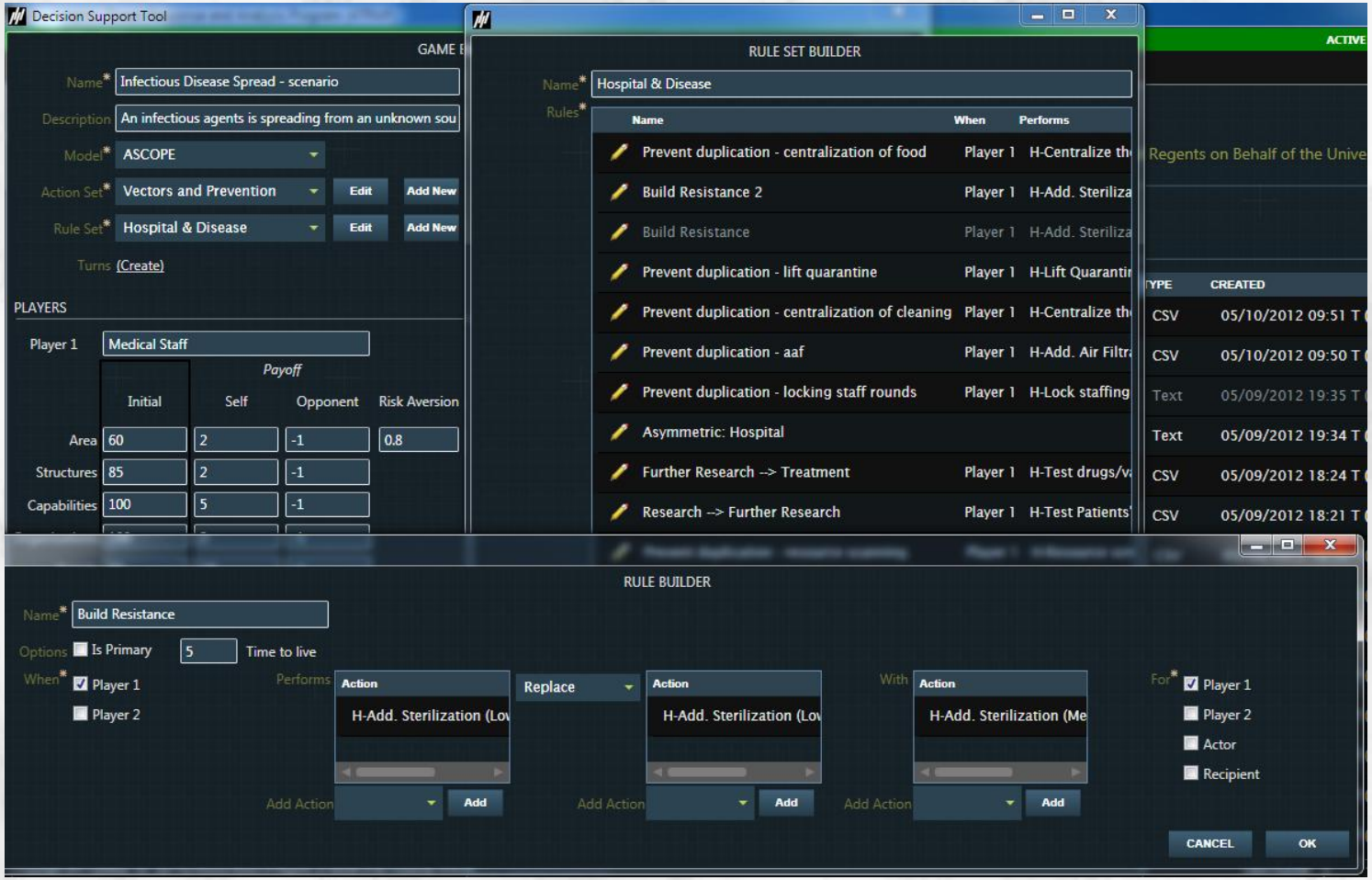
Game Theoretic Decision Support – The Action Set



Game Theoretic Decision Support – The Rule Set

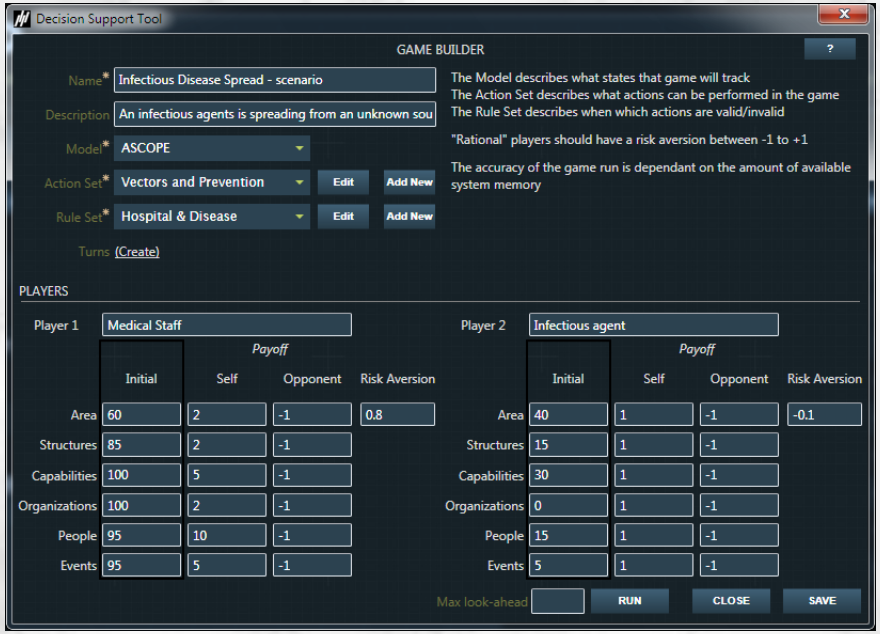
- Not all actions are always valid
  - An action maybe replaced with a more/less effective action provided certain circumstances have been met
- Each action may trigger a rule
  - Allowing/disallowing/replacing one set of actions with another set of actions
  - These may last for any number of turns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

Game Theoretic Decision Support – The Rule Set

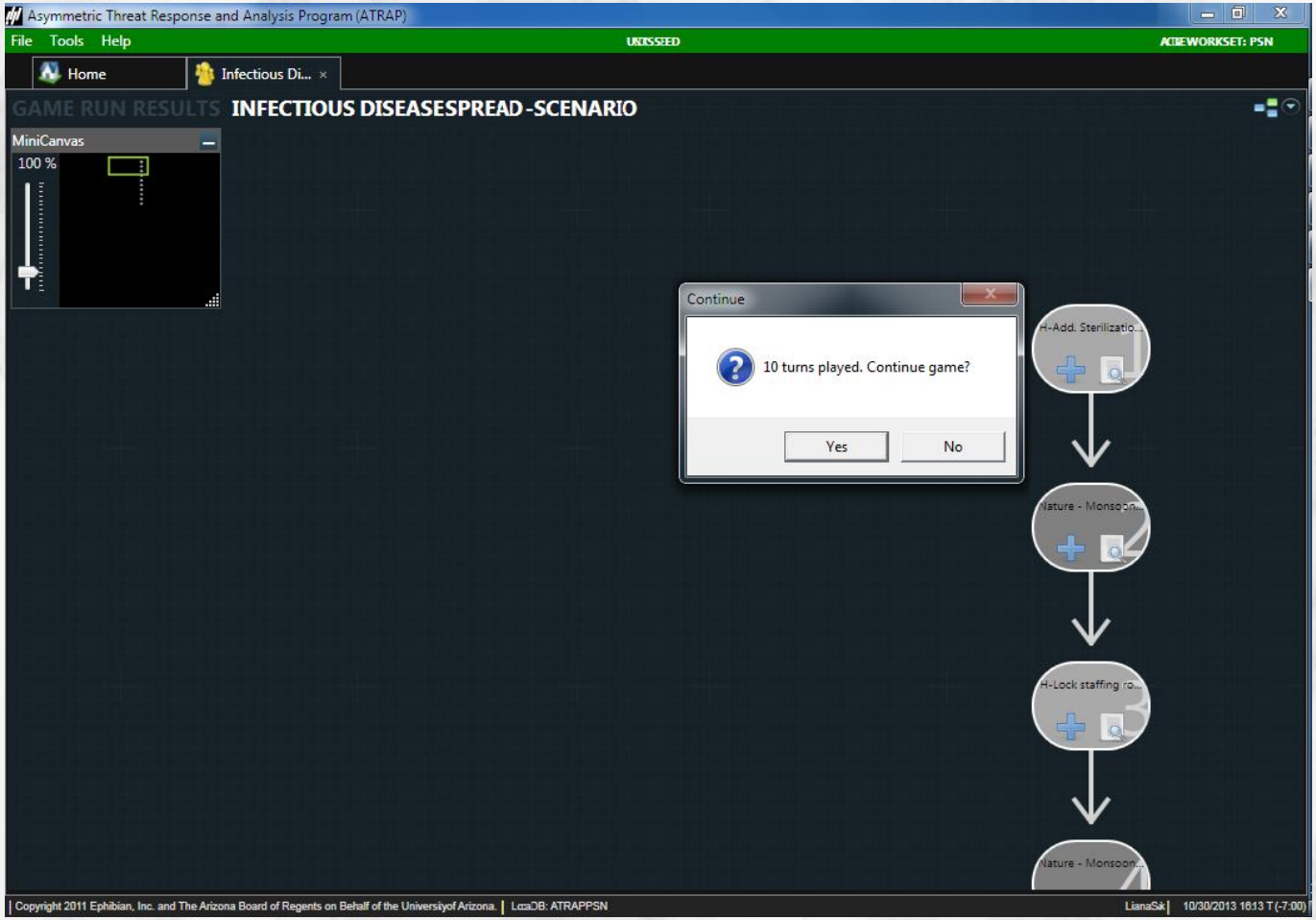


Game Theoretic Decision Support – Running the Game

- 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.



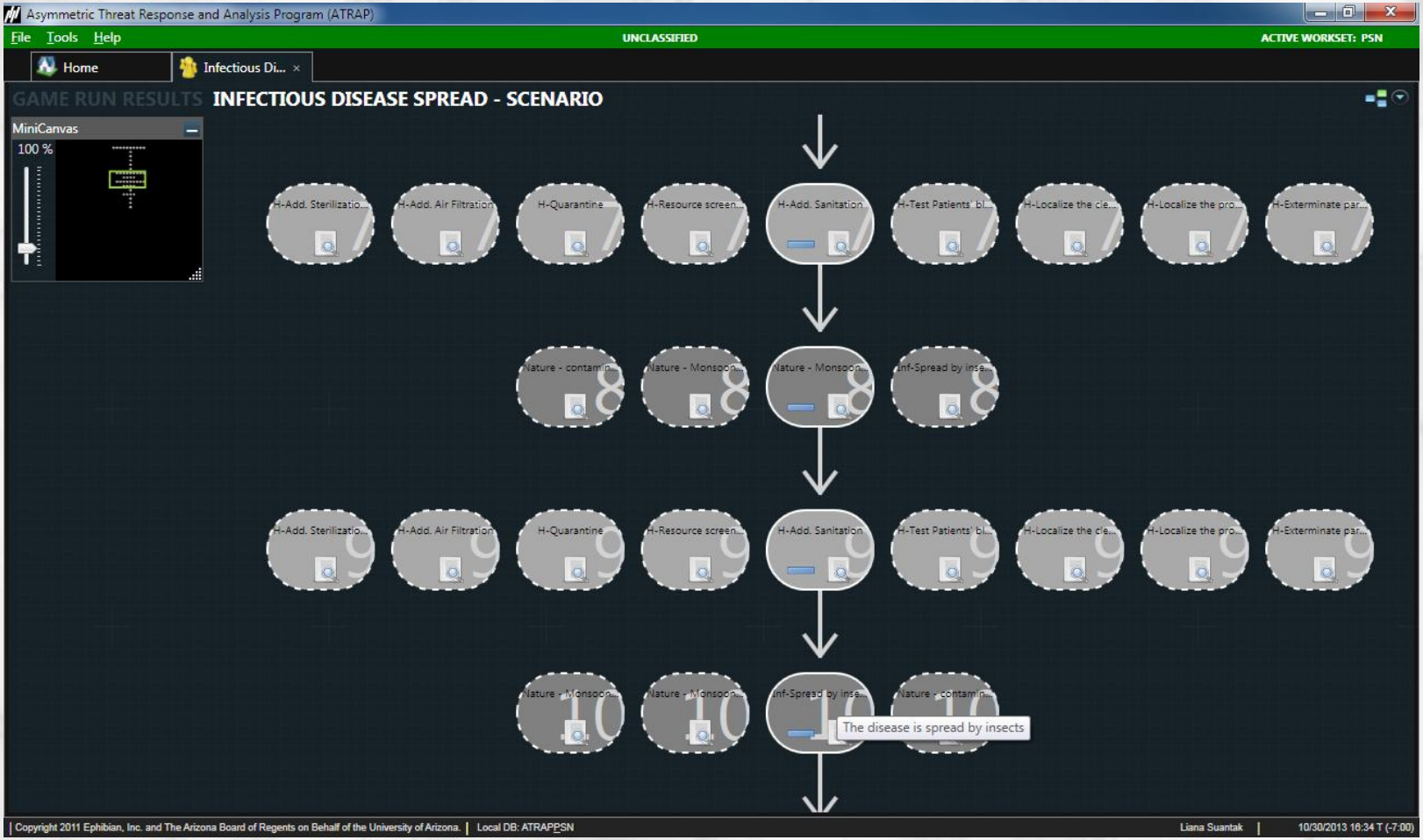
Game Theoretic Decision Support – Running the Game



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

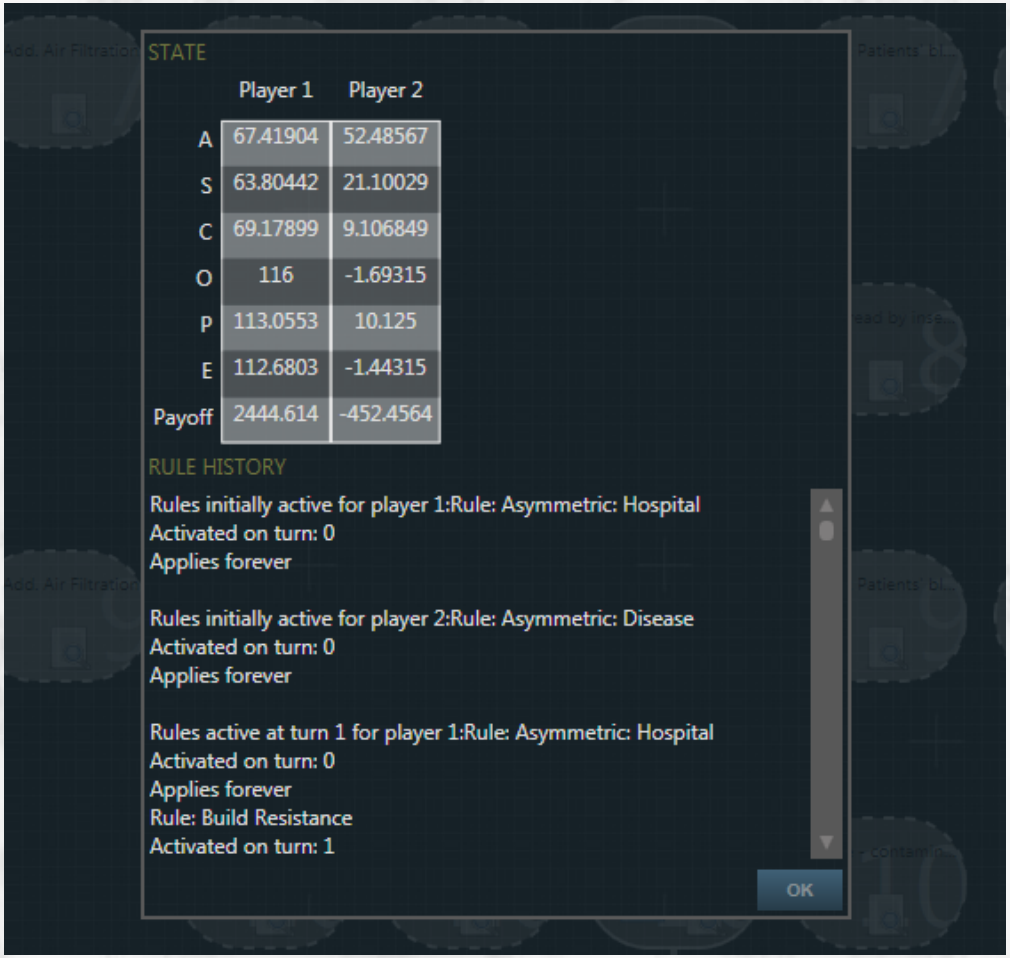
Game Theoretic Decision Support – Introspection



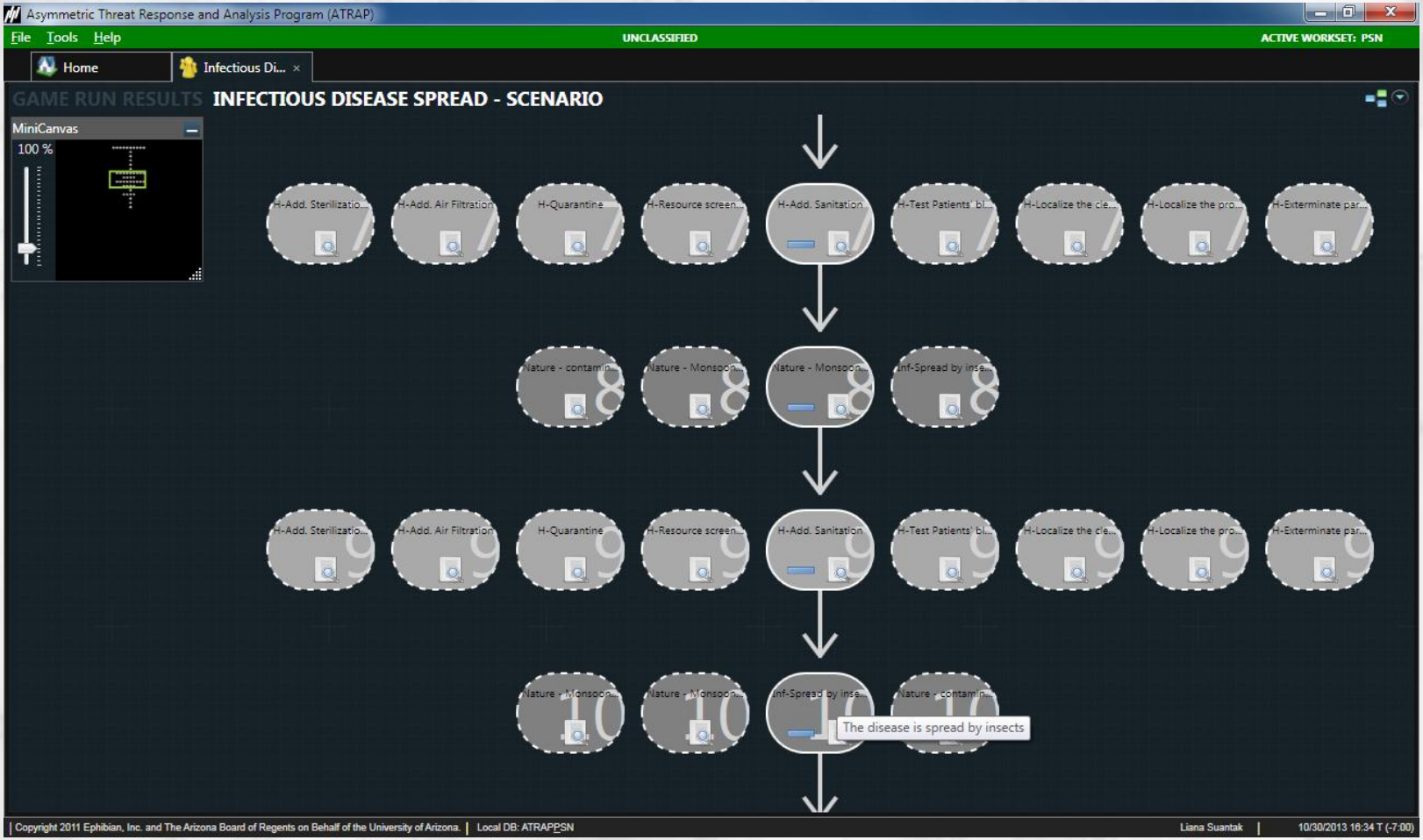
Game Theoretic Decision Support – Introspection

- 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

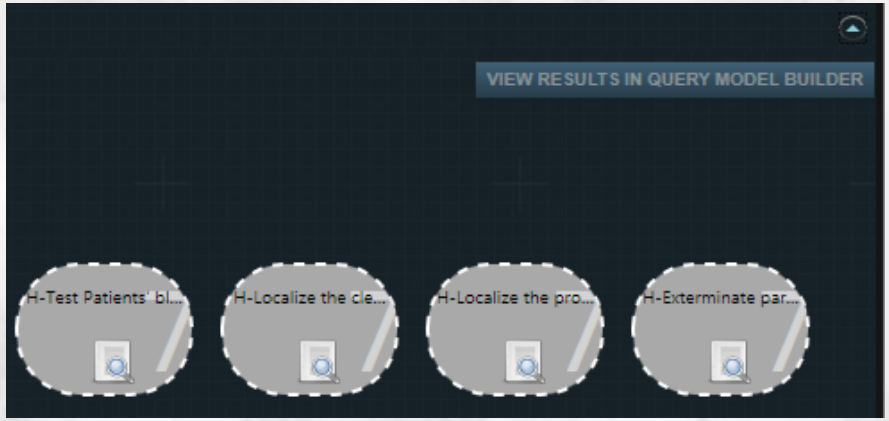


Game Theoretic Decision Support – Converting to a Query

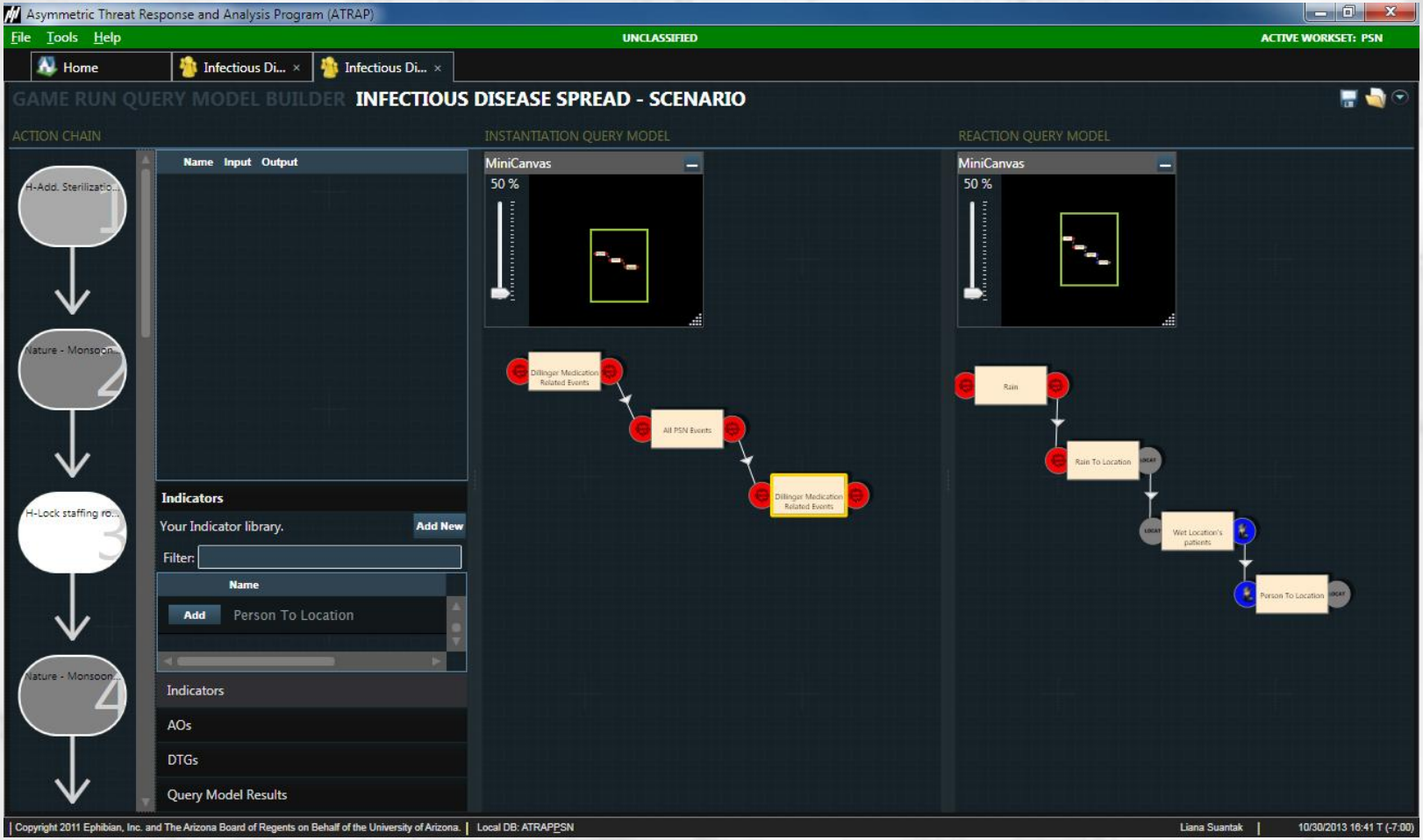


Game Theoretic Decision Support – Converting to a Query

- 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



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

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