Visualization and Interaction for Multi-platform Cybersecurity Awareness

ARO MURI on Cyber Situation Awareness
Year Four Review Meeting
November 28, 2013, Arizona State University

Tobias Höllerer
Four Eyes Laboratory (Imaging, Interaction, and Innovative Interfaces), Computer Science Department, Media Arts & Technology Program, UC Santa Barbara
Mission Cyber-Assets

- **Analysis to get up-to-date view of cyber-assets**
- **Analysis to determine dependencies between assets and missions**

**Real World Enterprise Network**

- **Observations:** Netflow, Probing, Time analysis
- **Sensor Alerts**
- **Correlation Engine**
- **Data**
- **Impact Analysis**
- **Data**

- **Mission Model**
- **Cyber-Assets Model**

- **Simulation/Live Security Exercises**
  - **Data**
  - **COAs**
  - **Analyze and Characterize Attackers**
  - **Predict Future Actions**

- **Create semantically-rich view of cyber-mission status**
Team

- Basak Alper – PhD, 2013
- Devdeep Choudhury – M.S. 2013
- Christopher Hall – PhD student
- Mathieu Rodrigue – PhD student

Four Eyes Laboratory, Computer Science Department and Media Arts and Technology Program, UC Santa Barbara
Accomplishments

UC Santa Barbara

• Year 1 & 2:
  – User Experience & Platform Evaluation: Mobile / Desktop / Situation Room
  – Cybaware NSR software framework for immersive situation room (Allosphere), including plugins for various data/simulations (LBL logs, simple game theoretic analysis)
  – Mission-based Visualizations (Attacks, Compromised Services, Mission SA)
  – Studies: Graph analysis in 3D / 2D & Effects of graph manipulation on analysis tasks
  – Early explorations of interactive visual recommender systems

• Year 3:
  – Interactive visual recommendation
  – Collaborative Data Exploration (Allosphere and Mobile Devices)
  – Mission-Centric Exploration Tool for Cybersecurity Situation Awareness (Desktop)
  – Mobile Exploration Tool for Cybersecurity Situation Awareness (Android)

• Year 4:
  – Mission-Centric Scenario Simulation & Evaluation
  – User Interface Design for CyMiR (Cyber Mission Range)
  – Immersive Situation Room: Updates and Improvements
  – Information Tapestries & Magic Lenses (Surround Sit. Awareness + Mobile)
  – Bridging Dimensions in Visualization
Year 4 Results, Overview

- Mission-Centric Scenario Simulation & Evaluation
Year 4 Results, Overview

- Mission-Centric Scenario Simulation & Evaluation
- User Interface Design for CyMiR (Cyber Mission Range)
Year 4 Results, Overview

- Mission-Centric Scenario Simulation & Evaluation
- User Interface Design for CyMiR (Cyber Mission Range)
- Immersive Situation Room, updates and improvements
Year 4 Results,

- Mission-Centric Scenario Simulation & Evaluation
- User Interface Design for CyMiR
- Immersive Situation Room, updates and improvements
Year 4 Results, Overview

- Mission-Centric Scenario Simulation & Evaluation
- User Interface Design for CyMiR (Cyber Mission Range)
- Immersive Situation Room, updates and improvements

Additional UI Designs and User Studies:
- Contour Maps (bridging 2D/3D in visualization)
- Situation awareness and trust in game-theoretic simulations
Mission-Centric Scenario Simulation & Evaluation

• The high-level scenario, simplified to a quantifiable evaluation task:
  – **Missions:** Petri Nets / FSMs with an end goal and a series of steps to accomplish the goal.
  – **Services:** Entities required at the steps for the missions to progress. An attack on a service when it is required would cause the mission to compromise.
  – **Attacker:** A single attacker launches attacks at the services over time in order to get one or more missions compromised.
  – **Defender:** This is the perspective of the user of our work. The user is in charge of defending the services using shields and preventing the missions from getting compromised.

• **Objective:** **Visualize the steps of the missions, aid the analyst to defend the services from potential attacks using further visualizations and prevent missions from getting compromised.**
Previous Work

- Based on 2010 iCTF data
- Missions represented as trees showing possible decisions
- Attacks on a service would cause the mission to delay
- Services could be repaired for the mission to progress
Previous Work

- Based on 2011 iCTF data
- Missions represented as trees
- Provided overview of the 2011 iCTF competition
- Introduced concept of an optimal attacker
- Helps the analyst answer perceptive, comprehensive and projective questions such as:
  - What is the current state of our missions?
  - Which services have been targeted the most?
  - Which services will it be most effective to concentrate defense on?
• Mission: Each mission repeats for several iterations, using different state branches each time.
• Dataset (ICTF 2011) determined the path taken in the Petri-nets.
• We decided against using branching as an active decision in this game.
• Zero or more services required at every state.
• All missions progress at the same rate → unified timeline
• A mission gets compromised for all of its current iteration if a required service is attacked.
Simplified Mission Control

- Mission display linearized. Each mission repeats for several iterations, using different state branches each time.
- Dataset (ICTF 2011) determined the path taken in the Petrinets. We decided against using branching as an active decision in this game.
- Zero or more services required at every state.
- All missions progress at the same rate → unified timeline
- A mission gets compromised for all of its current iteration if a required service is attacked.
New CybaViz UI
Shielding services

- Services can be shielded proactively to prevent them from getting compromised due to an attack.
- Shields have a finite life (10 ticks) and they take time to regenerate (10 ticks).
- Active Shields defend all attacks on a service.
- Visualization shows successful and defended attacks, as well as shield status.
- One or more shields may be used on the same service. (Shield extension)
Aiding the analyst

- **Attack History**
- Services that have been attacked the most may be attacked again (vulnerabilities)
- Graphs for number of attacks on every service are provided.
- The two most attacked services are outlined by dashes in the services panel.
Aiding the analyst

- **Next crucial service**
- Services that are required in upcoming mission states should be shielded.
- Mission Panel by default focuses on these services. *(Toggling overview can view all services.)*
- Next services also shown alongside the mission panel.
- Two most-used upcoming services are highlighted in the services panel with dotted outlines.
Aiding the analyst

• **Predictions based on optimal attacker**
• The optimal attacker uses an optimization based on the Cut-Payoff-Risk values to decide attacking which services is most valuable.
• Predictions for the next 3 time steps are shown.
• They are sorted in decreasing order of value to attacker.

Joint work with J. Hespanha and K. Vamvoudakis
maximize
\[ TD = \sum_t \sum_s f^s_t(AR^s_t)g(AR^s_t) \]
constrained by:
\[ \sum_s AR^s_t \leq TR_t, \quad \forall t \quad \sum_t \sum_s AR^s_t \leq TR \]

- Plausibility of next attack prediction for service \( s \) (based on historical data)
- Integrated measure of threat to different services

\[ PL^s(t + 1) := \frac{SP^s(0 \cdots t)}{SP^s(0 \cdots t) + FP^s(0 \cdots t)} \in [0, 1] \]

# of successful attack predictions on service \( s \) up to time \( t \)

# of false-positives on service \( s \) up to time \( t \)

Joint work with J. Hespanha and K. Vamvoudakis
Simple scoring function: One point per time step for each non-compromised mission. If mission is compromised, no points will be received until the next iteration of the mission starts.

- Recorded points received for automated strategies and human operators
- User Study: 10 users (eight novice users, two with previous shorter experience with the system)
- Users had 10 seconds per tick and they could use the *step* button to make the missions go faster if needed.
- Average play time was 15 minutes.
- Post-study questionnaires, and other observations:
  - Experience can improve score.
  - All users said they used the ‘most attacked’, ‘most used’ indicators.
  - Two users said they used the game-theoretic predictions
  - Four novice users would not use shields even when they were available.
  - Two users said that the rules were too complex.
Evaluation

Points received by automated strategies and Human Operators

- U6
- Prediction sorted by points to attacker
- U3
- Random with shield extension (20 runs)
- U8
- U5
- Random (20 runs)
- U2
- Prediction over next 3 ticks sorted by points to attacker
- Prediction sorted by service number
- U1
- Look-ahead next tick sorted by service usage
- Prediction based on attack history
- U7
- U9 (Extra Practice)
- U10 (Extra Practice)
- U4
- Complete knowledge of human attacker

Points range from 516 to 766.
Year 4 Results, Overview

- Mission-Centric Scenario Simulation & Evaluation
- User Interface Design for CyMiR (Cyber Mission Range)
- Immersive Situation Room, updates and improvements

Additional UI Designs and User Studies:
- Contour Maps (bridging 2D/3D in visualization)
- Situation awareness and trust in game-theoretic simulations
CyMiR developed from the 2012/2013 iCTF
Main advantage for human-in-the-loop experiments: Dynamic simulation instead of logged data playback; much more flexible scenario development

New evaluation scenario:
- Shields (scarce resource) can be placed on services (as before)
- Compromised services can be repaired
- Branches in mission execution are important choice points (weighing safe but longer paths against short but vulnerable ones)
Hypothetical Futures Interaction Model

Situational Awareness Interface (on multiple platforms)

- An environment for playing out attacker/defender models in simulation
- Make and evaluate decisions in advance
  - against all available adversary models simultaneously
  - reduce cognitive load (focus only on changes in expectation)
- Adjust as real-time information is accumulated
  - converge confidence on most predictive models
- Present aggregated statistics as the countless combinatorial scenarios are played out
- Use informed human understanding to prioritize and prune exploration tree

Applied to CybaViz evaluation scenario

- Arrange/Adjust pre-placed shields (service centric)
- Steer and evaluate mission execution paths (mission centric)
- Provide an optimized view for each task, coordinated by time markers
Example mission:

- Gantt format derived by petri net expansion (previous work)
- Example above:
  - initial phase depends on 6 services (14 ticks long)
    - one of which is highly vulnerable - red
    - one vulnerable to lesser degree - mustard yellow
  - two execution paths - one choice point
    - the lower of which has been taken - black outline
  - 4 states/phases in its upper path
    - shorter possible overall execution time
  - 3 states/phases in its lower path
    - finishing with 1 vulnerable and 3 protected service dependencies
Service-Centric View

Each service has its own band on the timeline. Mission executions appear within:

e.g. gold & blue missions running:

Vulnerability varies over time:

- Low
- Mid
- High

Special conditions:

- Shielded
- COMPROMISED

Transition lines detail dependency changes over time:

executing purple mission on service 3 currently, service 1 and 4 next, service 2 eventually

This line bundling indicates that teal mission is transitioning to:

- 4 services above
- plus remaining on the current service
- will stop making progress (white hatching) due to an expected attack on a dependent service
Initial Testing in AlloSphere
Year 4 Results, Overview

- Mission-Centric Scenario Simulation & Evaluation
- User Interface Design for CyMiR (Cyber Mission Range)
- Immersive Situation Room, updates and improvements

Additional UI Designs and User Studies:
- Contour Maps (bridging 2D/3D in visualization)
- Situation awareness and trust in game-theoretic simulations
Situation Room

UCSB Allosphere:
2013 ONR DURIP: “A High-Fidelity Mixed Reality Simulator” (PI Hollerer)

- This grant mentioned as one of two additional DoD funded projects directly benefiting
- Grant pays for projectors and computers completing surround-view 2D/3D graphics projection as well as eye-tracking and neuromonitoring equipment for user studies within the instrument.
### Information Tapestries: Immersive Surround Situation Rooms

<table>
<thead>
<tr>
<th>Category</th>
<th>Type of Information</th>
<th>Application Domains</th>
<th>Presentation Format</th>
<th>Typical Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Worlds</td>
<td>3D Environments &amp; Volumetric Data</td>
<td>Entertainment, Architecture, CAD/CAM, Medicine, Sciences, ...</td>
<td>Immersive 3D stereoscopic scenes that the user navigates through</td>
<td>3D user interfaces [22] incl. head tracking, hand tracking, tracked VR wands, etc.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Tapestries</td>
<td>Stretched Tapestries</td>
<td>Geography (Earth), Astronomy (Planets &amp; Star Systems) [84], Remote Presence (Scene Panoramas), ...</td>
<td>Minimally distorted continuous wall projections that surround the user; stereoscopy optional</td>
<td>Pan/Zoom interaction via tablets or gestures; tracking optional</td>
</tr>
<tr>
<td></td>
<td>Collage Tapestries</td>
<td>General Information Analysis, Productivity, Planning, ...</td>
<td>Minimally distorted wall projections of disjoint elements (Images, Text, Spreadsheets, Databases, Calendars, ...)</td>
<td>Content arranged by user, supported by intelligent UIs; Pan/Zoom interaction via tablets or gestures</td>
</tr>
</tbody>
</table>
Year 4 Results, Overview

- Mission-Centric Scenario Simulation & Evaluation
- User Interface Design for CyMiR (Cyber Mission Range)
- Immersive Situation Room, updates and improvements

Additional UI Designs and User Studies:
- Contour Maps (bridging 2D/3D in visualization)
- Situation awareness and trust in game-theoretic simulations
Contour Maps
Bridging 2D / 3D in Visualization

Figure 4.2: Contour Maps generated with different data properties: (left) degree of graph nodes, (middle) betweenness coefficient of graph nodes and (right) point density in scatter plots.

Figure 4.3: Stages of contour map generation: (a) original node-link diagram, (b) triangulation of the background area, (c) threshold surface, (d) resulting contour paths.
Three different user experiments:

- **Task 1:** low-level **readability** task on graph topology—find common connections between two nodes.
- **Task 2:** **comparison** task—determine if and how two graphs differ.
- **Task 3:** **revisitation** task—revisit previously highlighted nodes.

**Results:**

- **Task 1:** No significant effects. Plain Node-Link diagram preferred.
- **Task 2:** Contour Maps significantly outperform Plain N-L and Grid.
- **Task 3:** Contour Maps significantly outperform Plain N-L and Grid.
Army Mission Command Distributed Decision making with uncertain information

- Team experiment: 2-person distributed teams
- Understanding of Trust and SA emergence aids in the development of future MC systems and training
- SAGAT and MARS Evaluations

Cognitive Models of Trust:
- Trust Game (Diner’s Dilemma)
- Model Participant Behavior
- Explore Trust/SA Relationship
Year 4 Metrics

Invited Talks and Tech Transfer:
- **01/10/2013**  
  “Cognitive Models of Trust,” Presentation at Network Science Collaborative Technology Alliance: Trust CCRI (Cross-cutting Research Initiative) Kickoff Meeting, Cambridge, MA
- **04/02/2013**  
  “Analysis of Information Credibility in Networks,” Presentation and breakout session at ARL Network Science Collaborative Technology Alliance, Technical Meeting, University of Delaware, Newark, DE
- **05/28/2013**  
  “AR and VR Everywhere? The Quest for Ever-Improving Augmented and Virtual Reality Experiences,” *Keynote talk*, SBC SVR: 15th Symposium on Virtual and Augmented Reality, Cuiaba, Brazil
- **06/18/2013**  
  “The Quest for Ever-Improving Augmented and Virtual Reality Experiences,” Max-Planck-Institute Tuebingen, Germany
- **06/24/2013**  
  “AR and VR Everywhere?,” Qualcomm Inc., Vienna, Austria

Conference and Workshop Papers:

Theses and Technical Reports:
- Devdeep Choudhury (now at Qualcomm): M.S. in Computer Science, “Cybavis: an interactive tool to promote situational awareness in a mission centric cybersecurity scenario,”
- Basak Alper (now visiting Professor at Sabanci University, Turkey): PhD in Media Arts and Technology, 2013, " Bridging Dimensions in Visualization,”
Future Work

- Evaluation of mission-specific visualizations using iterative usability design <cont.> [Hollerer w. Kemmerer, Hespanha]

- Scalability across and automatic adaptation to presentation platforms, screen estate, and implied user context [Hollerer w. Kemmerer]

- Design, development, and evaluation of interfaces for active exploration of game theoretic what-if analyses [Hollerer w. Hespanha, input from Shamma]

- Deployment of interactive visualization framework for real-world scenarios [Hollerer w. input from Kemmerer, Kruegel, Vigna, Paxson, Hespanha]
Questions?

Cybaware