Flexible Interactive Information Visualization for a Cybersecurity Situation Room

ARO MURI on Cyber Situation Awareness Year Five Review Meeting
November 19, 2014, University of California, Santa Barbara

Tobias Höllerer
Four Eyes Laboratory (Imaging, Interaction, and Innovative Interfaces), Computer Science Department, Media Arts & Technology Program, UC Santa Barbara
Analysis to get up-to-date view of cyber-assets

Analysis to determine dependencies between assets and missions

Mission Model

Cyber-Assets Model

Sensor Alerts

Correlation Engine

Impact Analysis

Simulation/Live Security Exercises

Data

Analyze and Characterize Attackers

Predict Future Actions

Real World Enterprise Network

Observations: Netflow, Probing, Time analysis

Create semantically-rich view of cyber-mission status
Team

- Charlie Roberts  PhD, 2014
- Christopher Hall  PhD candidate
- James Schaffer  PhD candidate
- Donghao Ren  PhD student

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

Year 1 & 2:
- User / Task Analysis & Platform Evaluation: [Mobile – Desktop – Situation Room]
- Cybaware NSR software framework for immersive situation room (Allosphere)
- 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 & 4:
- Interactive 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)
- Bridging Dimensions in Visualization, User Interface Design for CyMiR (Cyber Mission Range)
- Information Tapestries & Magic Lenses (Surround Sit. Awareness + Mobile)

Year 5:
- Immersive Situation Room: Information Management for Cyber-Security Situational Awareness (Situation Room Improvements, Information Surround Content Management)
- Flexible Interactive Multimodal Information Visualization
- Mission-Based Cybersecurity Response Planning
- Towards Self-Descriptive Data Formats and Platform-Scalable User Interfaces
• Immersive Situation Room: Information Management for Cyber-Security Situational Awareness
  – Situation Room Improvements
  – Information Surround Content Management
• Flexible Interactive Multimodal Information Visualization
  – Two approaches: textual programming vs. visual interaction
  – iVisDesigner, system overview and live demo
• Towards Interoperable Data Formats and Platform-Scalable User Interfaces
• Interactive Mission-Based Cybersecurity Simulation
• <Demo in Allosphere Situation Room>
Overview

• Immersive Situation Room: Information Management for Cyber-Security Situational Awareness
  – Situation Room Improvements
  – Information Surround Content Management

• Flexible Interactive Multimodal Information Visualization
  – Two approaches: textual programming vs. visual interaction
  – iVisDesigner, system overview and live demo

• Towards Interoperable Data Formats and Platform-Scalable User Interfaces

• Interactive Mission-Based Cybersecurity Simulation

• <Demo in Allosphere Situation Room>
Situation Room Improvements

- UCSB Allosphere: A Surround-View Situation Room
  - Completion of full-surround projection
UCSB Allosphere: A Surround-View Situation Room
  - Completion of full-surround projection
Situation Room Improvements

- UCSB Allosphere: A Surround-View Situation Room
  - Completion of full-surround projection
  - Turnkey (re-)calibration (currently just geometric, soon radiometric)
Situation Room Improvements

- UCSB Allosphere: A Surround-View Situation Room
  - Completion of full-surround projection
  - Turnkey (re-)calibration (currently just geometric, soon radiometric)
  - User observation for cognitive HCI studies
Information Surround Content Management

Begins to implement the “Information Tapestries” vision from Y4

Tablet-based controllers allow arrangement of information items
Overview

• Immersive Situation Room: Information Management for Cyber-Security Situational Awareness
  – Situation Room Improvements
  – Information Surround Content Management

• Flexible Interactive Multimodal Information Visualization
  – Two approaches: textual programming vs. visual interaction
  – iVisDesigner, system overview and live demo

• Towards Interoperable Data Formats and Platform-Scalable User Interfaces

• Interactive Mission-Based Cybersecurity Simulation

• <Demo in Allosphere Situation Room>
Cybersituation Room Requirements:
- Need to import/access/review data flexibly
- Scenario needs and urgency may change dramatically
- Expert users may be available, but ease of use is desirable

Two different approaches:

- Textual (Live) Programming
  Gibber (Roberts, Wright, Kuchera-Morin & Höllerer, ACM Multimedia 2014)

- User Interaction
  IVisDesigner (Ren, Höllerer & Yuan, IEEE InfoVis 2014)
• Design information visualizations without the need for textual programming or templates.

• Vector graphics design paradigm with flexible data importation and mappings

• Different focus from: Tableau, Analyst’s Notebook, SketchStory, Lyra.
iVisDesigner  
(Ren, Höllerer & Yuan, InfoVis 2014)

Goals:
- Interactively design information visualizations
- Provision for end-user interactions
- Flexibly react to new information demands

Approach:
- Data-driven Vector Graphics Editing Paradigm.
- Represent designs with
  - Graphical, Guide, Generator and Component objects.
- Web-based (HTML 5 canvas) for multi-platform applicability
iVisDesigner: Video & Demo

Select object.
Object-oriented Framework

Object Classes:

**Graphical Objects**: Map data items to graphical elements.
- Circles, Lines, Arcs, Polylines, etc.

**Guide Objects**: Provide Information for Graphical Objects.
- Axes, Scatters, Maps, Linear Mapping, etc.

**Generator Objects**: Attach derived data back to the dataset.
- Statistics, Range, Expression, Brushing, ForceLayout, etc.

**Components**: Nest objects inside (for example, glyphs).
• **Pros:**
  – Expressive: Able to construct a variety of different designs.
  – Extensible: Templates / New Objects.
  – Web-based: Easily embed designs into websites or web applications.

• **Integrated into Allosphere Situation Room**

• **Open Source:**
  – [https://github.com/donghaoren/iVisDesigner](https://github.com/donghaoren/iVisDesigner)
Overview

• Immersive Situation Room: Information Management for Cyber-Security Situational Awareness
  – Situation Room Improvements
  – Information Surround Content Management
• Flexible Interactive Multimodal Information Visualization
  – Two approaches: textual programming vs. visual interaction
  – iVisDesigner, system overview and live demo
• Towards Interoperable Data Formats and Platform-Scalable User Interfaces
• Interactive Mission-Based Cybersecurity Simulation
• <Demo in Allosphere Situation Room>
User Interfaces are not adaptable:
- users get one prescribed UI design
- no outlets for users to apply gradations of computational literacy to bridge proportional gaps in functionality, for changing needs
Goals of HCI Metacomputing

- Eliminate two classic design tradeoffs
  - expert/novice friendly UI, binary/printable data-format
- Cleanup archaic aspects of computing
  - metadata cap., arbitrary character / content limitations
- Improve learnability and consistency of applications
  - self-describing structure, presentation assignable
- Facilitate unambiguous structural expression / intention
- Enable impromptu interoperability
- Disseminate computation to every corner of computing
- Simplify software development
- Create outlets for applying computational literacy
- Enable constructivist computational literacy acquisition
- Never not have UI support
Interoperable Data Formats and Platform-Scalable User Interfaces

Progress <1>

Implemented:

- Reflection-based synthetic OO-UIs for pre-existing Java programs

- **Universal Metaformat**
  - replacement structural layer of *all* formats / languages
  - ‘parsed’ (quantitative syntax) - suitable for runtime & non-runtime
    - eliminate the need for escaping & byte padding
  - binary (mixed encodings)
  - recursive free-form trees (w/ first-class metadata)
  - indirect logical structure layer - references (graphs), transclusion (symmetric representations - unobfuscated compression)
  - semantics bootstrapping

- **Structured Data Editor**
  - replacement for all text editors / textual widgets
  - edit Universal Binary Metaformat with [graphical syntax](https://example.com) & mixed markup-based visualization
    - render human-readable (as Text Editors do for UTF8)
  - new threshold for computer literacy (2D natural language expression)
Explored benefits of a Universal Binary Metaformat as an alternative backbone for computing:

- everything can be fractal structured human & machine readable
- unambiguous expression of structure at the data level
  - eliminates an entire genre of security vulnerabilities

Agenda/Report won John Vlissides Award for significant promise in applied software research at the ACM SIGPLAN OOPSLA Doctoral Symposium at SPLASH’14
Overview

• Immersive Situation Room: Information Management for Cyber-Security Situational Awareness
  – Situation Room Improvements
  – Information Surround Content Management
• Flexible Interactive Multimodal Information Visualization
  – Two approaches: textual programming vs. visual interaction
  – iVisDesigner, system overview and live demo
• Towards Interoperable Data Formats and Platform-Scalable User Interfaces
• Interactive Mission-Based Cybersecurity Simulation
• <Demo in Allosphere Situation Room>
CybaVis
(Mission-based Cybersituational Awareness)
Petri-nets ‘unrolled’ into gantt-charts
Each mission phase: set of dependencies spanning $n$ ticks

User Interactions:
- **select** between alternative execution paths
  - black phases: paths not currently planned to be taken
- **plan delays** to optimize dependency overlaps
Mission Rendering Modes

as Bars

answers: **how many** services when?

as Glyphs

answers: **which** services when?
Histogram of Unique Dependencies

Total # of unique dependencies per tick
Entirely Green - can be completely defended
Partially Red - requires defense trade-off decisions
Service-Centric View

Groups everything common to each service
Slopes show mission-phase progress over time

User Interaction: strategically place shields for future ticks
Visualizing Attacks and Shields

- Service 1
  - Successful attack
  - Blocked attack
  - Failed attack

- Service 2
  - Successful attack
  - Blocked attack
  - Failed attack

- Service 3
  - Successful attack

was unshielded
was shielded
will be

(can be)

attack band
defense band
mission-phase
execution band

(successful attacks' artifacts interject in this space)
Attack Predictions

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

Applied to iCTF 2011 attack dataset

C,P,R plots

attacker’s cost/payoff/risk
Year 5 Results, Overview

- Immersive Situation Room: Information Management for Cyber-Security Situational Awareness
  - Situation Room Improvements
  - Information Surround Content Management
- Flexible Interactive Multimodal Information Visualization
  - Two approaches: textual programming vs. visual interaction
  - iVisDesigner, system overview and live demo
- Towards Interoperable Data Formats and Platform-Scalable User Interfaces
- Interactive Mission-Based Cybersecurity Simulation

- *<Demo in Allosphere Situation Room>*
Year 5 Metrics

Awards and Honors

- Tobias Höllerer: Program (Co-)Chair for ICAT 2013: 23rd International Conference on Artificial Reality and Teleexistence.
- Tobias Höllerer: Program (Co-)Chair for IEEE VR 2015: 17th Int'l Conference on Virtual Reality.

Synergistic Talks and Tech Transfer:

- Army Research Meeting on Trust, Influence, Modeling, and Enhancing Performance (TIME), March 2014, Aberdeen, MD.
- Joint International Technology Alliance and Network Science Collaborative Technology Alliance Technical Meeting, June 2014, University of Delaware, Newark, DE.

Conference and Journal Papers:


Theses and Technical Reports:

- Charles Roberts, Dissertation, “Immediacy In Creative Coding Environments”, Media Arts and Technology Program, UC Santa Barbara
- Angus Forbes, Dissertation, “Emerging Methodologies for Interdisciplinary Research Practice”, Media Arts and Technology Program, UC Santa Barbara
- Angus Forbes, M.S. project, “Exploring Motion as a Modality for Visualizing Data”, Computer Science Department, UC Santa Barbara
Questions?

Cybaware

UC Santa Barbara