Cybaware Summary

Richard A. Kemmerer

University of California, Santa Barbara
University of California, Berkeley
Georgia Institute of Technology
**Scientific Objective:**

Development of novel situation awareness theories and techniques to obtain an accurate view of available cyber-assets, mission status, and possible future threats in a semantically rich environment.

An effective approach to cyber situation awareness requires a multi-disciplinary collaboration among security researchers and practitioners, game theoreticians, and visualization and user interface experts.
Scientific Accomplishments

Up-to-date views of the available cyber-assets

- Developed preliminary tools to analyze flow records and distributed logging [UCB, UCSB]
- Models to “fingerprint” specific programs and network services [UCSB]
- Methods for detecting stealthy attacks [UCB]
- Methods to detect highly distributed probing attacks that cannot be found point wise [UCB]
- Methods to integrate external intelligence information into network monitors to better assess the current state of missions [UCB]
- Program analysis technique to find application IDs [UCSB]
Scientific Accomplishments

Dependencies between cyber-missions and cyber-assets

- Petri-net based formalism to describe cyber-missions [UCSB]
- Machine learning techniques to automatically extract mission, activity, and service dependencies from network traffic [UCSB]
- Service dependency model and algorithms for ranking assets and services [UCSB]
- Methods for correlating service ranking, network connectivity, and vulnerability information to refine ranking [UCSB]
- Active component that uses a traffic watermarking to detect dependency relations between services [UCSB]
- Dependency analysis that extracts dependencies based on connection patterns [UCB]
- Infrastructure to enable very large scale archiving of enterprise activity for later use, such as for “what-if” analysis [UCB]
- Investigated how incorporating external information can enhance a purely local network perspective [UCB]
Accurate understanding of the impact of cyber-attacks

- Alert correlation from multiple sources [UCSB]
- Speculative analysis [UCSB]
- Cyber-triaging [UCSB]
- Detection of network “bad neighborhoods” [UCSB]
- Petri-net based formalism to describe cyber-missions [UCSB]
- Machine learning techniques to automatically extract mission, activity, and service dependencies from network traffic [UCSB]
- Service dependency model [UCSB]
- Live security exercises centered on cyber situation awareness (iCTF) [UCSB]
- Framework to support the *ad hoc* selection of assets, user behaviors, and types of attacks, which are used to synthesize specific attacks against a cyber-mission [UCSB]
Scientific Accomplishments

Actionable cyber-attack forecasts

- Sampled Security Policy, and Sampled Security Value algorithms to solve very large static games [UCSB]
- Generalized approach to dynamic games with partial information [UCSB]
- Model reduction for hidden Markov models [GaTech]
- Nexat tool for history based detection of attacks that uses attack traces to determine an adversary’s next move [UCSB]
- Validation of the effectiveness of partial information games methods by applying it to models of the iCTF exercise [UCSB, GaTech]
- Estimation and detection in adversarial environments [UCSB]
- Online optimization techniques for real-time attack prediction [UCSB]
- Computational approaches to derive limited look-ahead policies [GaTech]
- Consensus algorithms to detect misbehaving agents and minimize their influence [UCSB]
Scientific Accomplishments

Developing a semantically-rich, easy-to-grasp view of the cyber-mission status

- Scalable network visualization technology for representing graph-based information [UCSB]
- Interactive cybersecurity analysis frameworks for Allosphere, networked workstations, and ultra-mobile devices [UCSB, UCB]
- Interactive visual recommender systems [UCSB]
- Studied the usefulness of 3D stereoscopic graph display and found benefits for some tasks, but no clear advantage [UCSB]
- Study of the effects of different interactive graph manipulation techniques on standard graph analysis tasks [UCSB]
- Initial evaluation of mission-specific visualizations using the iCTF data and formal mission models [UCSB]
- Initial design of multimodal surround displays that achieve situation awareness using collaborative interaction [UCSB]
Student Statistics

- **Students supported YR 4**
  - 11 Graduate
  - 2 Postdocs
  - 7 Faculty

- **PhDs awarded**
  - 1 year 1
  - 1 year 2
  - 2 year 3
  - 2 year 4

- **MS awarded**
  - 1 year 2
  - 4 year 3
  - 2 year 4

Invited Participants, ISAT Black Cloud Workshop, Berkeley, CA, (DARPA sponsored)

BSD-license OpenSource launch of WiGis platform

One-day Security Symposium for Industry at UCSB, “Next Generation Internet,” May 2011

Invited Participant, Sandia National Laboratory’s University Partners Cyber Open House and Workshop, July 2011

Made iCTF data sets available online for other researchers

CNN interview of UCSB Cyber-Security, July 2011

Invited participant at Technology Exchange Meeting for IARPA KDD program, Arlington, VA, September 2011
Technology Transfer (2)

• Invited participant at ARL Network Science Collaborative Technology Alliance (NS CTA), Cross-Cutting Initiative on 'Trust', Kickoff Meeting, October 2011
• Invited talk at IBM Research, December 2011
• Invited talk at Symantec Systems, February 2012
• Half-day Cyber-Security Consortium at UCSB with researchers and administrators from Northrup-Gruman, March 2012
• Meeting with government representatives, ARL, and NS CTA researchers in the Network Science Collaborative Technology Alliance (NS CTA), April 2012
• Meeting with German MoD to discuss US-Studytour, September 2012
• Invited talk at Microsoft Research, August 2012
• Invited talk at UCSB College of Engineering Affiliates Meeting, April 2013
Technology Transfer (3)

- Five talks presented at U.S. Studytour, a joint meeting with German military and civilian defense, June 2013
- Invited talk at Cisco, June 2013
- UCSB intern at ARL June-September 2013
- Local high school students attending UCSB hack meetings, March-June 2013

- Various keynotes, invited talks, and government briefings
  - 18 keynote, 20 invited, 5 plenary (8, 7, 1 this year)
Keynote, Plenary, and Invited Talks

• Hespanha
  – Keynote: “Stochastic hybrid systems in networks and biology,” 52th Turkish National Symposium on Automatic Control (TOK2010), Gebze, Turkey, September 2010
  – Invited talk: "Networked Control Systems," 5th HYCON2 PhD School on Networked and Large-Scale Systems, European Network of Excellence HYCON2, Lucca, Italy, July 2013
  – Plenary talk: “Stochastic Networked Control Systems,” 4th IFAC Workshop on Distributed Estimation and Control in Networked Systems, Koblenz, Germany, September 2013

• Höllerer:
Keynote, Plenary, and Invited Talks

- Höllerer (cont):
  - Invited talk: "Evaluating the Effects of Immersion on Naval Training Applications," Meeting with ONR representatives, discussing I/ITSEC conference, Orlando, FL, 29 November 2011
  - Keynote: “AR and VR Everywhere? The Quest for Ever-Improving Augmented and Virtual Reality Experiences.” SVR: 15th Symposium on Virtual and Augmented Reality, Cuiaba, Brazil, 28 May 2013

- Kemmerer:
  - Keynote: "How to Steal a Botnet and What Can Happen When You Do," Sixth Conference on Detection of Intrusions and Malware & Vulnerability Assessment, Como, Italy, July 2009
  - Invited talk: “Formal Methods, Concurrent and RealTime Systems,” Matinee with Carlo Ghezzi at ICSE 2012, Zurich, Switzerland, June 2012
• **Kruegel:**
  - Invited talk: “Automated Malware Analysis,” Microsoft Research, Redmond, WA. June 2011

• **Paxson:**
  - Plenary talk: “Perspectives on Countering Internet Attacks and Disrupting Their Ecosystem,” NSF US/Mideast Trustworthy Cyber Workshop, Koc University, Istanbul, Turkey, June 2012

• **Shamma:**
  - Plenary Speaker: 1st IFAC Workshop on Estimation and Control of Networked Systems (NecSys’09), Venice, Italy, September 2009
  - Plenary Speaker: 5th International ICST Conference on Performance Evaluation Methodologies and Tools, Cachan, France, May 2011
  - Invited talk: “From Distributed Control Systems to Game Theory: There and Back Again,” Mohammed Dahleh Award and Distinguished Lecture, University of California, Santa Barbara, April 2013
• **Vigna**
  – Invited Talk: “Network Intrusion Detection: Dead or Alive?,” Annual Computer Security Application Conference (ACSAC), Austin, TX, December 2010
  – Keynote: "Hunt, crack, track, block: Combating today’s and tomorrow’s malware," CODASPY 2012: San Antonio, TX, February 2012
Awards (1)

- Technology Review’s list of top 35 innovators under 35 years old (TR35 Award), 2010 – Kruegel
- IEEE Control Systems Society Ruberti Young Researcher Prize, 2010 – Hespanha
- Santa Barbara Chamber of Commerce Business Star Innovator Award, 2010 – Kemmerer, Kruegel, Vigna
- ACSAC 2010 Classic Paper Award – Kemmerer, Vigna
- ACM SIGCOMM Award for lifetime contribution to the field of communication networks, 2011 – Paxson
- Jim and Donna Gray Faculty Award for Excellence in Undergraduate Teaching, 2011 – Paxson
- USENIX Security 2011 Best Paper Award – Paxson
Awards (2)

• Best Paper Honorable Mention at ACM MobileHCI 2012 – Höllerer
• Best Paper Award at IEEE ISMAR 2012 – Höllerer
• 2007-2013 IEEE Distinguished Lecturer – Hespanha
• Vice Chair of IFAC Technical Committee on Networked Systems, 2009-2011 and 2012-2014 – Hespanha
• IFAC Technical Committee 1.3 on Discrete Event and Hybrid Systems, 2011-2014 – Hespanha
• UC Berkeley EECS Department’s Diane S. McEntyre Award for Excellence in Teaching, 2013 – Paxson
60 refereed conference, 9 journal publications

(25 conference, 3 journal this year)

- “WiGis: A Framework for Scalable Web-based Interactive Graph Visualizations,” GraphDrawing 2009, September 2009
- "Your Botnet is My Botnet: Analysis of a Botnet Takeover," ACM CCS, November 2009
- “On Calibrating Enterprise Switch Measurements,” ACM IMC, November 2009
- “FIRE: Flinding Rogue nEtworks,” ACSAC09, December 2009
- “Learning Approaches to the Witsenhausen Counterexample from a View of Potential Games,” 48th IEEE Conference on Decision and Control, December 2009
- “Botnet Judo: Fighting Spam with Itself,” NDSS, February 2010
- “A Reaction-Diffusion Model for Epidemic Routing in Sparsely Connected MANETs,” IEEE INFOCOM, March 2010
- “On the Potential of Proactive Domain Blacklisting,” USENIX LEET, April 2010
- “Insights from the Inside: A View of Botnet Management from Infiltration,” USENIX LEET, April 2010
Papers Published (2)

- “Network Intrusion Detection: Dead or Alive?,” Annual Computer Security Application Conference (ACSAC), December 2010
- “Toward Automated Detection of Logic Vulnerabilities in Web Applications,” 19th Usenix Security Symposium, August 2010
- “Randomized Sampling for Large Zero-Sum Games,” Conference on Decision and Control, December 2010
Papers Published (3)

- “Peering Through the iFrame,” IEEE International Conference on Computer Communications, April 2011
- “Randomized Solutions to Partial Information Dynamic Zero-Sum Games,” American Control Conference, June 2011
- “MISHIMA: Multilateration of Internet Hosts Hidden Using Malicious Fast-flux Agents (Short Paper),” Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), July 2011
- “An Assessment of Overt Malicious Activity Manifest in Residential Networks,” Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), July 2011
- “BotMagnifier: Locating Spambots on the Internet,” Usenix Security Symposium, August 2011
Papers Published (4)

• “Hide-and-Seek with Directional Sensing,” 18th World Congress of the International Federation of Automatic Control, August 2011
• “Dymo: Tracking Dynamic Code Identity,” Symposium on Recent Advances in Intrusion Detection (RAID), September 2011
• “Understanding Fraudulent Activities in Online Ad Exchanges,” Internet Measurement Conference (IMC), November 2011
• “A Counter Example to Aggregation Based Model Reduction for Hidden Markov Models,” IEEE Conference on Decision and Control, December 2011
• “Stereoscopic Highlighting: 2D Graph Visualization on Stereo Displays,” IEEE Transactions on Visualization and Computer Graphics, December 2011
• “Hit 'em Where it Hurts: A Live Security Exercise on Cyber Situational Awareness,” Annual Computer Security Applications Conference (ACSAC), December 2011
• “Modeling Topic Specific Credibility on Twitter,” 2012 ACM international conference on Intelligent User Interfaces., February 2012
Papers Published (5)

- “Augmented Textual Data Viewing in 3D Visualizations Using Tablets,” 2012 IEEE Symposium on 3D User Interfaces (3DUI), March 2012
- “Robust Detection in the Presence of Integrity Attacks,” 2012 American Control Conference, June 2012
- “B@BEL: Leveraging Email Delivery for Spam Mitigation,” USENIX Security, August 2012
- “Poultry Markets: On the Underground Economy of Twitter Followers,” Workshop on Online Social Networks (WOSN), August 2012
Papers Published (6)

• “A Lone Wolf No More: Supporting Network Intrusion Detection with Real-Time Intelligence,” Symposium on Research in Attacks, Intrusions and Defenses (RAID), September 2012
• “A Fundamental Limitation to the Reduction of Markov Chains via Aggregation,” 50th Annual Allerton Conference on Communication, Control, and Computing, October 2012
• “Adversarial Detection as a Zero-Sum Game,” 51st IEEE Conference on Decision and Control, December 2012
• “Policy Improvement for Repeated Zero-Sum Games with Asymmetric Information,” 51st IEEE Conference on Decision and Control, December 2012
Papers Published (7)

- “COMPA: Detecting Compromised Accounts on Social Networks,” ISOC Network and Distributed System Security Symposium (NDSS 2013), February 2013
- “Trust and Situation Awareness in a 3-Player Diner's Dilemma Game,” 3rd IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA 2013), February 2013
- “Interactive Interfaces for Complex Network Analysis: An Information Credibility Perspective,” IQ2S 2013: 5th International Workshop on Information Quality and Quality of Service for Pervasive Computing, @ IEEE PERCOM, March 2013
Papers Published (8)

- “Randomized Sampling for Large Zero-Sum Games,” *Automatica*, May 2013
- “A Model-based Evaluation of Trust and Situation Awareness in the Diner’s Dilemma Game,” 22nd Behavior Representation in Modeling & Simulation (BRIMS) Conference, July 2013
- “Practical Comprehensive Bounds on Surreptitious Communication Over DNS,” USENIX Security Symposium, August 2013
- “Shady Paths: Leveraging Surfing Crowds to Detect Malicious Web Pages,” ACM Conference on Computer and Communications Security (CCS), November 2013
- “Detecting Stealthy, Distributed SSH Brute-Forcing,” ACM Conference on Computer and Communications Security (CCS), 2013
- “Gossip Average Consensus in a Byzantine Environment Using Stochastic Set-Valued Observers,” 52nd IEEE Conference on Decision and Control (ICDC), December 2013
http://seclab.cs.ucsb.edu/academic/projects/topics/cyber-situation-awareness/
Questions?

Cybaware