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]
- Approach to track assets even in presence of aliasing [UCB]
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]
Scientific Accomplishments

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]
- Detection of malicious behavior in browser extensions [UCSB]
- Detection of connections used to download malware [UCSB]
Scientific Accomplishments

Actionable cyber-attack forecasts

- Sampled Saddle Point, 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]
- Validated 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]
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]
- Studied effects of different interactive graph manipulation techniques on standard graph analysis tasks [UCSB]
- Mission-specific visualizations using the iCTF data and formal mission models [UCSB]
- Multimodal full surround displays that achieve situation awareness using collaborative interaction [UCSB]
Student Statistics

- Students supported YR 6
  - 8 Graduate
  - 3 Postdocs
  - 6 Faculty
- PhDs awarded
  - 1 year 1
  - 1 year 2
  - 2 year 3
  - 2 year 4
  - 5 year 5
  - 4 year 6
- MS awarded
  - 1 year 2
  - 2 year 3
  - 2 year 4
  - 3 year 5
  - 1 year 6
Technology Transfer (1)

- 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-Study tour, September 2012
- Invited talk at Microsoft Research, August 2012
- Invited talk at UCSB College of Engineering Affiliates Meeting, April 2013
Five talks presented at U.S. Study Tour, 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 continue to attend UCSB hack meetings, March 2013 – August 2015
Technology Transfer (4)

- 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
- Analyzers for enterprise traffic integrated into Bro: MySQL, Kerberos 5, RDP, SIP, Windows PE objects, 2014
- Invited participants, Cybersecurity Workshop, Berkeley Center for Law & Technology, April 2015
- UCSB SecLab invited to qualification round of DARPA Cyber Grand Challenge, site visit conducted 22 June 2015

- Various keynotes, invited talks, and government briefings
  - 22 keynote, 38 invited, 9 plenary (3 keynote, 10 invited this year)
Keynote, Plenary, and Invited Talks

- Hespanha
  - Keynote: 3rd International Workshop on Wireless Networking and Control for Unmanned Autonomous Vehicles (WiUAV’12). WiUAV is collocated with the IEEE International Conference on Global Communications (GLOBECOM 2012).
  - Keynote talk: “Opportunities and Challenges in Control Systems Design Arising from Ubiquitous Computation and Communication.” 2014 IEEE Int. Conf. on Control and Automation (IEEE ICCA), Taichung, Taiwan, June 2014.
  - Plenary speaker: 4th IFAC Workshop on Distributed Estimation and Control in Networked Systems (NECSYS’13).
  - Keynote speaker: 2014 IEEE Int. Conf. on Control and Automation (IEEE ICCA), Taichung, Taiwan.
Höllerer:

- Keynote: “Collaborative Augmentations and Augmented Collaborations,” Taking AR to the next level - CDL Workshop on Tracking Technology for AR, Graz, Austria, September 15-17, 2014.
Keynote, Plenary, and Invited Talks

- **Kemmerer:**
• Kruegel:

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

• Paxson (cont.)

• Shamma:
  – Invited talk: S. Mohammed Dahleh Award and Distinguished Lecture, University of California, Santa Barbara, April 2013
  – Plenary speaker at the 52nd IEEE Conference on Decision and Control, December 2013.

• Vigna
  – Distinguished Lecturer at University of Illinois, Chicago, November 2014.
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
• UC Berkeley EECS Department’s Diane S. McEntyre Award for Excellence in Teaching – Paxson
• Best Paper Award at IEEE/ASE SocialCom 2013 – Höllerer
• ACM Distinguished Scientist in Nov. 2013 – Höllerer
• Best Paper Award at IEEE CogSIMA 2014 – Höllerer
• Recipient of the 2015 IEEE Internet Award – Paxson
• Best paper award at MoST Workshop 2015 – Kruegel and Vigna
Awards (3)

- IEEE senior membership grade, January 2015 – Höllerer
Papers Published (1)

103 refereed conference, 10 journal publications
(19 conference, 2 journal this year)

• "Your Botnet is My Botnet: Analysis of a Botnet Takeover," ACM CCS, November 2009.
• “Botnet Judo: Fighting Spam with Itself,” NDSS, February 2010
Papers Published (2)

• “Network Intrusion Detection: Dead or Alive?,” Annual Computer Security Application Conference (ACSAC), December 2010.
Papers Published (3)

- “Peering Through the iFrame,” IEEE International Conference on Computer Communications, April 2011.
Papers Published (4)

Papers Published (5)

• “Hide-and-Seek with Directional Sensing,” 18th World Congress of the International Federation of Automatic Control, August 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.
Papers Published (6)

Papers Published (7)

- “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 (8)


Papers Published (10)

- “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 (11)

Papers Published (12)


• “Practical Attacks Against The I2P Network,” Research in Attacks, Intrusions and Defenses Symposium (RAID), October 2013.

• “Follow the Green: Growth and Dynamics in Twitter Follower Markets,” ACM Internet Measurement Conference (IMC), October 2013.
Papers Published (13)

Papers Published (14)

Papers Published (15)


“Real-time Pricing Leading to Optimal Operation under Distributed Decision Makings,” American Control Conference (ACC), June 2014.


Papers Published (17)

• “Eyes of a Human, Eyes of a Program: Leveraging different views of the web for analysis and detection,” 17th Symposium on Research in Attacks, Intrusions and Defenses (RAID), Sweden, September 2014.
• “Protecting Web Single Sign-on against Relying party Impersonation Attacks through a Bi-directional Secure Channel with Authentication.” 17th Symposium on Research in Attacks, Intrusions and Defenses (RAID), Sweden, September 2014.
Papers Published (18)

- “Count Me In: Viable Distributed Summary Statistics for Securing High-Speed Networks,” Symposium on Research in Attacks, Intrusions and Defenses (RAID), September 2014.
Papers Published (19)

Papers Published (20)

- “Portrait of a Privacy Invasion - Detecting Relationships Through Large-scale Photo Analysis,” 15th Privacy Enhancing Technologies Symposium (PETS), June 2015.
- “EvilCohort: Detecting Communities of Malicious Accounts on Online Services,” to appear at the 24th USENIX Security Symposium, August 2015.
Papers Published (21)

  Submitted to journal publication in February 2015.
http://seclab.cs.ucsb.edu/academic/projects/topics/cyber-situation-awareness/
Questions?