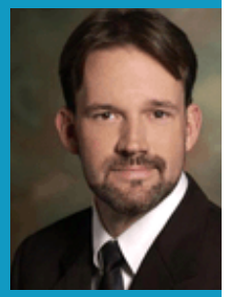
Keynote Speaker



John N. Stewart
Vice President and Chief Security Officer, Corporate Security Programs Organization
Cisco

In his current role, Mr. Stewart provides leadership and direction to multiple corporate security teams throughout Cisco Systems, Inc., strategically aligning with Business Units and the IT organization to generate leading corporate security practices, policies, and processes. He is responsible for overseeing the security for Cisco Connection Online, the infrastructure supporting Cisco's more than $28.5 billion business.

Mr. Stewart's longstanding career in information security has included numerous roles. He was the Chief Security Officer responsible for operational and strategic direction for corporate and customer security at Digital Island. Mr. Stewart has served as a Research Scientist responsible for investigating emerging technologies in the Office of the CTO at Cable & Wireless America. His professional experience also includes software development, systems and network administration, software specialist, author, and instructor. He has given numerous tutorials and presentations at various security forums including SANS, USENIX, and the Java Security Alliance.

Throughout his career, he has been an active member of the security industry community. He served on advisory boards for Akonix, Finjan, Cloudshield, Riverhead, and TripWire, Inc. Currently, Mr. Stewart sits on technical advisory boards for Ingrian Networks and Signacert, Inc.

Conference Sponsors

napatech

NETEZZA
an IBM® Company

SOFTWARE PROCESS TECHNOLOGIES

See the conference matrix for times and locations for breakfast, lunch, the opening reception, birds of a feather sessions, and the off-site event.

CERT

Software Engineering Institute
Carnegie Mellon

www.cert.org

CERT Software Engineering Institute Carnegie Mellon

FloCon®2011

A FORUM FOR SHOWCASING THE NEXT GENERATION OF NETWORK FLOW-BASED ANALYSIS

www.flocon.org

January 10-13, 2011
Salt Lake City, Utah

FloCon Session Schedule

Monday

Morning

An Introduction to Argus, Ballroom ABCD
Carter Bullard, QoSient LLC

This class will introduce Argus, the network Audit Record Generation and Utilization System. It will include Argus's approaches to data generation, collection, and stream processing of large scale flow data, including establishing, maintaining, and using large flow repositories and archives.

iSilk Introduction, Deer Valley
Note: Tim Shimeall teaches the "Advanced Flow Analysis with SiLK" course in the afternoon.

Jonathan Steele, CERT; Ron Bandes, CERT

This class will introduce students to network flow analysis using the iSiLK graphical user interface. This is an optionally hands-on class in which students may follow along on their own laptops if they fulfill the prerequisites.

Prerequisites: Students who wish to follow along on their own MS Windows laptops must install iSiLK in advance.

Afternoon

Advanced Flow Analysis with SiLK, Ballroom ABCD
Dr. Tim Shimeall, CERT

This class picks up after the introductory SiLK class and includes many complex examples of analysis using SiLK.

Prerequisite: introductory SiLK or iSiLK, familiarity with basic UNIX command-line operations

Visualization for NetFlow, Deer Valley
Dr. Paul Krystosek, CERT; Sidney Faber, CERT; Evan Wright, CERT; Rhiannon Weaver, CERT; Phil Groce, CERT

This class will examine the use of readily available graphics software to visualize NetFlow Data. Packages include Excel/OpenOffice, GnuPlot, GraphViz, R, and Rayon. Excel and OpenOffice are not strictly graphics packages but are often used for simple bar charts, histograms, scatterplots and histograms. GnuPlot is a comprehensive graphics program used in many areas of visualization. GraphViz is a special-purpose system for visualizing directed graphs that depict the relationship between communication end points. R is a statistical package with extensive visualization features. Rayon is a graphics toolkit developed specifically to visualize SiLK and related data. Rayon consists of several command-line graphics applications and a Python library.

Prerequisites: introductory SiLK or equivalent, some knowledge of Python recommended

Tuesday

9:00 – 10:00

Keynote, Ballroom ABCD
John Stewart, Cisco Chief Security Officer

10:30 - 12:00

Session 1: Know Your Network, Ballroom ABCD
Chair: Josh Goldfarb

10:30 – Garbage Collection: Using Flow to Understand Private Network Data Leakage, Sidney Faber

11:00 – DLP Detection with Netflow, Christopher Poetzel

11:30 – Detecting Long Flows, John McHugh

1:00 - 3:00

Session 2: Visualization, Ballroom ABCD
Chair: John Gerth

1:00 – Flows as a Network Topology Chart, Hiroshi Asakura

1:30 – FloVis: A Visualization Suite, Carrie Gates

2:00 – Real Time Topology Based Flow Visualization, John Smith

2:30 – The Rayon Visualization Toolkit, Phil Groce

3:00 - 3:30

Demo Panel, Ballroom ABCD
Chair: Tim Shimeall

4:00 - 5:30

Demo Session, Deer Valley
Chair: Tim Shimeall

Wednesday

8:30 - 10:30

Session 3: Malware, Ballroom ABCD
Chair: Michael Jacobs

8:30 – From Data Collection to Action: Achieving Rapid Identification of Cyber Threats and Perpetrators, Joel Ebrahimi

9:10 – Network Profiling of Waladec-Infected IP Space, Rhiannon Weaver

9:50 – Botnet Detection Through Temporal Group Behavior, Kevin Carter

10:00 – Botnet Detection Based on NetFlow, Vojtech Krmicek

11:00 - 12:00, 1:00 - 2:00

Session 4: Collection, Ballroom ABCD
Chair: Bill Orvis

11:00 – Not to Miss Small-Amount But Important Traffic, Kzunori Kamiya

11:30 – Coordinated Non-Intrusive Capturing of Flow Paths, Tanja Zseby

1:00 – Privacy-Preserving Network Flow Recording, Bilal Shebaro

1:30 – Incorporating Dynamic List Structures Into YAF to Enhance Deep Packet Inspection, Emily Sarneso

2:30 - 4:30

Session 5: Blended Analysis, Ballroom ABCD
Chair: Chris Kinnahan

1:30 – Using Flow for Other Things than Just Network Data, Jeroen Massar

3:00 – Leveraging Other Data Sources with Flow to Identify Anomalous Network Behavior, Peter Mullarkey

3:30 – Using Flow as a Full Packet Capture System Index, Randy Heins

4:00 – Exploring the Interactions Between Network Data Analysis and Security Information/Event Management, Tim Shimeall

Thursday

8:30 - 10:00

Session 6: Network Traffic Modeling, Ballroom ABCD
Chair: Rhiannon Weaver

8:30 – Network Flow Data Analysis Using Graph Pattern Search, Josh Goldfarb

9:00 – Protocol Graphs as a Social Network Analysis Tool, Jeff Janies

9:30 – Darkspace Construction and Maintenance – Jeff Jaines

10:30 - 12:00

Session 7: Analysis, Ballroom ABCD
Chairs: Paul Krystosek and Ed Stoner

10:30 – Security Incident Discovery and Correlation on Gov Networks, Cory Mazzola

11:00 – Analysis Pipeline - Streaming Flow Analysis with Alerting, Dan Ruef

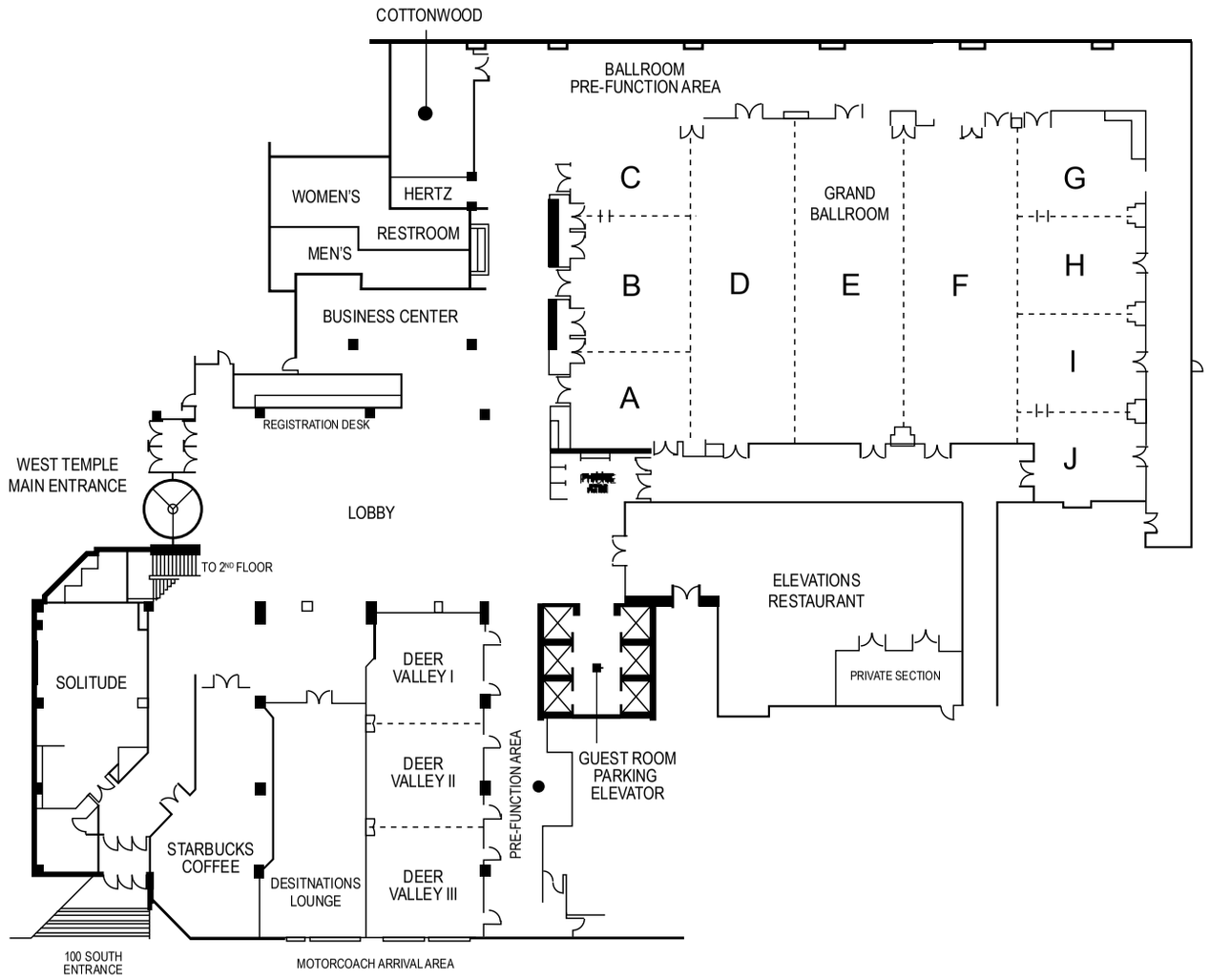
11:30 – What's New in the SiLK Virtual Training Environment, George Warnagiris

FloCon 2011 Program

Monday			Tuesday		Wednesday		Thursday	
	Registration Ballroom Foyer		**Registration** Ballroom Foyer		**Registration** Ballroom Foyer		**Registration** Ballroom Foyer	
7:30	**Breakfast** Ballroom E		7:30	**Breakfast** Ballroom E	7:30	**Breakfast** Ballroom E	7:30	**Breakfast** Ballroom E
8:00			8:00		8:00		8:00	
8:30	**Introduction to Argus** *Carter Bullard* Ballroom ABCD	**iSiLK** *Jon Steele* *Ron Bandes* Deer Valley	8:30	**Welcome**	8:30	**Session 3** Ballroom ABCD	8:30	**Session 6** Ballroom ABCD
9:00			9:00	**Keynote** *John Stewart* Ballroom ABCD	9:00		9:00	
9:30					9:30		9:30	
10:00			10:00	**Break**	10:00	**Break**	10:00	**Break**
10:30			10:30	**Session 1** Ballroom ABCD	10:30	**Session 4** Ballroom ABCD	10:30	**Session 7** Ballroom ABCD
11:00			11:00		11:00		11:00	
11:30			11:30		11:30		11:30	
12:00	**Lunch** Ballroom E		12:00	**Lunch** Ballroom E	12:00	**Lunch** Ballroom E	12:00	**Wrap Up** Ballroom ABCD
12:30			12:30		12:30			
1:00	**Advanced SiLK Analysis** *Tim Shimeall* Ballroom ABCD	**Visualization for NetFlow** *Paul Krystosek* *Sidney Faber* *Evan Wright* *Rhiannon Weaver* *Paul Groce* Deer Valley	1:00	**Session 2** Ballroom ABCD	1:00	**Session 4 (cont.)** Ballroom ABCD		
1:30			1:30		1:30			
2:00			2:00		2:00			
2:30			2:30		2:30	**Break**		
3:00			3:00	**Demonstration Panel** Ballroom ABCD	3:00	**Session 5** Ballroom ABCD		
3:30			3:30	**Break**	3:30			
4:00			4:00	**Demonstration Session** Deer Valley	4:00			
4:30			4:30		4:30	**Adjourn**		
5:00			5:00		5:00			
5:30			5:30	**Adjourn**	5:30	**FloCon Off-Site Event** Clark Planetarium 110 South 400 West Salt Lake City, UT 84101		
6:00	**FloCon Opening Reception** Wasatch Room		6:00	**Birds of a Feather Sessions**	6:00			
6:30			6:30		6:30			
7:00			7:00		7:00			
7:30			7:30		7:30			
24-Hr. Hold	Side Meeting Room - Solitude		24-Hr. Hold	Side Meeting Room - Solitude	24-Hr. Hold	Side Meeting Room - Solitude	12a - 12N	Side Meeting Room - Solitude
24-Hr. Hold	Office - Cottonwood		24-Hr. Hold	Office - Cottonwood	24-Hr. Hold	Office - Cottonwood	12a - 5p	Office - Cottonwood

Salt Lake City Marriott Downtown

First floor



Second Floor