10 Years of FloCon

Prepared for FloCon 2014

George Warnagiris - CERT/CC

gwarnagi@cert.org

#GeoWarnagiris

CARNEGIE MELLON UNIVERSITY

PITTSBURGH PENNSYLVANIA 1900

Software Engineering Institute

Carnegie Mellon

CERT

CERT

COORDINATION CENTER

CERT

NETWORK SITUATIONAL AWARENESS

CERT

Software Engineering Institute

Carnegie Mellon

FloCon®2014

Disclaimer

Firefox

FloCon 2014 - Charleston, South Carolin...

http://www.FloCon.org

Google

CERT | Software Engineering Institute
Carnegie Mellon University

search GO

HOME | Software Assurance | Secure Systems | Organizational Security | Coordinated Response | Training

HOME COMMITTEE PROCEEDINGS REGISTER SPEAKERS PROGRAM TUTORIALS TRAVEL & VENUE SPONSORSHIP

Call for Participation

This year's conference will focus on *perspectives*. We are accepting abstracts for presentations, posters, and demonstrations. What have we learned in 10 years of flow analysis? What has worked? Where can we do better? We invite submissions that look at flow analysis in *perspective*. Perspectives can be in relation to past work in flow analysis, changes in the threat landscape and operational environment, changes in technologies, or changes in the relative value of flow vs. other data

Important Dates

Newcomers Orientation & Early Registration
Sunday, January 12th
5:30 PM

Training Day

Motivation

Firefox

FloCon 2014 - Charleston, South Carolin...

http://www.FloCon.org

Google

CERT | Software Engineering Institute
Carnegie Mellon University

search GO

HOME | Software Assurance | Secure Systems | Organizational Security | Coordinated Response | Training

HOME COMMITTEE PROCEEDINGS REGISTER SPEAKERS PROGRAM TUTORIALS TRAVEL & VENUE SPONSORSHIP

Conference Overview

FloCon 2014, a network security conference, takes place at the Francis Marion Hotel in Charleston, South Carolina, on January 13-16, 2014. This open conference provides a forum for operational network analysts, tool developers, researchers, and other parties interested in the analysis of large volumes of traffic to showcase the next generation of flow-based analysis techniques.

Important Dates

Newcomers Orientation & Early Registration
Sunday, January 12th
5:30 PM

Training Day

FloCon 2013 | Albuquerque, New Mexico | January 2013

At FloCon 2013, organizers and participants focused on the challenges of "Analysis at Scale." In large network environments, flow data helps to provide a scalable way of seeing the big picture, as well as a streamlined platform for highlighting patterns of malicious behavior over time. More and more commercial tools and platforms are available for collecting and storing not only flow data, but large volumes of other data such as DNS information, packet capture, security logs, and incident reports. At FloCon 2013, participants discussed how to refine "big data" into knowledge, design methods for aggregated analyses at the network edge, and build systems for monitoring thousands or millions of assets at once.

- Proceedings
- Call for Papers

FloCon 2012 | Austin, Texas | January 2012

At FloCon 2012, participants focused on the progression of analytics from ideas, to prototypes, to tools. Since each phase has its own set of successes and raises its own set of challenges, organizers encouraged submissions and discussions across the spectrum, and participants addressed topics such as identifying which incident case studies spark the seed of a new idea, discussing how flow data can help refine a static signature, identifying the costs and benefits of implementing a technique at the large-scale network level versus host level, and discussing how well new flow-based analytical tools integrate into an analysts workflow.

- Proceedings
- Call for Participation

FloCon 2011 | Salt Lake City, Utah, | January 2011

At FloCon 2011, participants focused on learning about their networks and confirming what we know about them. Participants explored a wide range of

Gold Level

Bronze Level

napatech

nPULSE TECHNOLOGIES

Association Sponsor

ISSA, the Information Systems Security Association

Social Media Partner

THE CYBER SECURITY

Firefox

FloCon 2013 - Proceedings

http://www.cert.org/flocon/2013/proceedings-2013.html

Proceedings — FloCon 2013

FloCon 2013 took place in Albuquerque, New Mexico, on January 7-10, 2013. This page lists the keynote presentation, training sessions, presentations, and posters that were presented at the conference. We have also compiled these assets into one **FloCon 2013 proceedings file**. We will update this file as presentations become available, and we will announce updates here and in the FloCon rss feed.

Keynote Presentation

Steven M. Bellovin, Federal Trade Commission/Columbia University
Thinking Security

Training

Ron Bandes
Introduction to SiLK & Advanced SiLK Training

Carter Bullard
Network Flow Metadata Processing with Argus

Doug Burks
Network Monitoring with Security Onion

Presentations

Ron McLeod & Ashraf Abusharekh
Mongoose Flow Collection Tools

Igor Balabine & Sasha Velednitsky
Taming Big Flow Data

Firefox

BibTeX

http://www.bibtex.org/

Google

BIBTEX.org

Home | Convert | Format | Using | Special Symbols | About | Links

Your BibTeX resource

Here you will find everything you need to know about BibTeX

The word ,,BibTeX" stands for a tool and a file format which are used to describe and process lists of references, mostly in conjunction with LaTeX documents.

Here you can learn about the BibTeX File Format, How to use BibTeX and BibTeX Tools which can help you to ease your BibTeX usage.

NEW: Be sure to try the *Bib2x Online Converter* which allows you to **convert your BibTeX bibliographies** into a few target formats. It is meant to serve as a demonstration of Bib2x, a tool that allows arbitrary conversion of BibTeX bibliographies using templates.

```
@inproceedings{Best:2010:FloCon,
        abstract = "Tools and a Pipeline to Provide Defense in Depth Traffic Circle Visualization for situat
ional awareness Correlation Layers for Information Query and Exploration (CLIQUE) Network behavior visualiza
tion using LiveRac interface Middleware for Data-Intensive Computing (MeDiCi) Data pipeline",
        address = "Pittsburgh, PA, USA",
        affiliation = "",
        author = "Best, Daniel",
        booktitle = "{FloCon 2010 Proceedings}",
        keywords = "Visualization; Tools",
        note = "\url{http://www.cert.org/flocon/2010/presentations/Best\_RealTimeFlowVis.pdf}",
        publisher = "CERT",
        title = "{High-Throughput Real-Time Network Flow Visualization}",
        type = "Presentation",
        year = "2010"
}

@inproceedings{Bullard1:2010:FloCon,
        abstract = "Argus • Argus is a network utilization audit system Argus was officially started at the
CERT-CC as a tool in incident analysis and intrusion research. It was recognized very early that Internet te
chnology had very poor usage accountability, and Argus was a prototype project to demonstrate Red Book strat
egies for LAN and CAN network auditing. • Composed of: Real-time Network flow monitor Network flow data coll
ection system Network flow data processing programs Audit data repository tools",
        address = "Pittsburgh, PA, USA",
        affiliation = "",
        author = "Bullard, Carter",
        booktitle = "{FloCon 2010 Proceedings}",
        keywords = "Training; Analysis",
        note = "\url{http://www.cert.org/flocon/2010/presentations/Bullard\_IntroductionToArgus.pdf}",
        publisher = "CERT",
        title = "{Introduction to Argus}",
        type = "Presentation",
        year = "2010"
```

```
foreach $item (@files){
        @doc = `ps2ascii $dirname/$item`;
        foreach $line (@doc){
                @word = split(/\s/,$line);
                foreach $noun (@word){
                        chomp($noun);
                        $noun = lc($noun);
                        $noun =~ s/\.$//;
                        $noun =~ s/\:$//;
                        $noun =~ s/flows/flow/;
                        if (&prepcheck($noun)){
                                @letter = split(undef,$noun);
                                $x = 0;$result = "";
                                foreach $char (@letter){
                                        $x++;
                                        #$tobin = ord($char);
                                        $hex = unpack("H*", $char);
                                        if ($x <= 16){
#                                               print "$hex";
                                                $result = "$result" . "$hex";
                                                if ((($x % 2) == 0) && ($x<16))
{$result = "$result" .  ":";}
                                        }
                                }
                                if (($x % 2) == 0 & ($x<15)){
                                        $result = "$result" . ":";
                                }elsif ($x<15){
                                        $result = "$result" . "::";
                                }
                                if ($result =~ /\w{4}\:\w{4}/){
                                        open OUTPUT,">>z$year.txt" or die "Writ
e fail $!";
                                        print OUTPUT "$result|$date\n";
                                        close OUTPUT;
```

```
/analysis/gwarnagi/data/flocon>ls
2004  2009  2013        z2005.rw   z2008.rw   z2010.rw   z2012.rw
2005  2010  flocon.rw   z2005.txt  z2008.txt  z2010.txt  z2012.txt
2006  2011  z2004.rw    z2006.rw   z2009.rw   z2011.rw   z2013.rw
2008  2012  z2004.txt   z2006.txt  z2009.txt  z2011.txt  z2013.txt
/analysis/gwarnagi/data/flocon>rwfileinfo --field=command *.rw
flocon.rw:
z2004.rw:
  command-lines
                    1  rwtuc --fields=sip,stime --output-path=z2004.rw z2004.tx
z2005.rw:
  command-lines
                    1  rwtuc --fields=sip,stime --output-path=z2005.rw z2005.tx
z2006.rw:
  command-lines
                    1  rwtuc --fields=sip,stime --output-path=z2006.rw z2006.tx
z2008.rw:
  command-lines
                    1  rwtuc --fields=sip,stime --output-path=z2008.rw z2008.tx
z2009.rw:
  command-lines
                    1  rwtuc --fields=sip,stime --output-path=z2009.rw z2009.tx
z2010.rw:
  command-lines
                    1  rwtuc --fields=sip,stime --output-path=z2010.rw z2010.tx
z2011.rw:
  command-lines
                    1  rwtuc --fields=sip,stime --output-path=z2011.rw z2011.tx
z2012.rw:
  command-lines
                    1  rwtuc --fields=sip,stime --output-path=z2012.rw z2012.tx
z2013.rw:
  command-lines
                    1  rwtuc --fields=sip,stime --output-path=z2013.rw z2013.tx
/analysis/gwarnagi/data/flocon>
```

```
/analysis/gwarnagi/data/flocon>rwfilter flocon.rw --stime=2005/1/1-2005/12/1 -
-proto=0- --pass=stdout | rwstats --count=10 --field=sip
```

```
/analysis/gwarnagi/data/flocon>rwfilter flocon.rw --stime=2005/1/1-2005/12/1 -
-proto=0- --pass=stdout | rwstats --count=10 --field=sip
INPUT: 20028 Records for 6297 Bins and 20028 Total Records
OUTPUT: Top 10 Bins by Records
                                      sIP|   Records|  %Records|   cumul_%|
                              6461:7461::|       315|  1.572798|  1.572798|
                              666c:6f77::|       278|  1.388057|  2.960855|
                        7472:6166:6669:63::|       235|  1.173357|  4.134212|
                        6e65:7477:6f72:6b::|       218|  1.088476|  5.222688|
                    616e:616c:7973:6973::|       148|  0.738965|  5.961654|
                              7469:6d65::|       145|  0.723986|  6.685640|
                              706f:7274::|       137|  0.684042|  7.369682|
                        6e65:7466:6c6f:77::|       109|  0.544238|  7.913921|
            696e:666f:726d:6174:696f:6e::|       109|  0.544238|  8.458159|
                          736f:7572:6365::|       100|  0.499301|  8.957460|
/analysis/gwarnagi/data/flocon>
```

```
INPUT: 20028 Records for 6297 Bins and 20028 Total Records
OUTPUT: Top 10 Bins by Records
                                      sIP|   Records|  %Records|   cumul_%|
                                6461:7461::|       315|  1.572798|  1.572798|
                                666c:6f77::|       278|  1.388057|  2.960855|
                          7472:6166:6669:63::|     235|  1.173357|  4.134212|
                          6e65:7477:6f72:6b::|     218|  1.088476|  5.222688|
                      616e:616c:7973:6973::|       148|  0.738965|  5.961654|
                                7469:6d65::|       145|  0.723986|  6.685640|
                                706f:7274::|       137|  0.684042|  7.369682|
                          6e65:7466:6c6f:77::|     109|  0.544238|  7.913921|
              696e:666f:726d:6174:696f:6e::|       109|  0.544238|  8.458159|
                             736f:7572:6365::|     100|  0.499301|  8.957460|
/analysis/gwarnagi/data/flocon>
/analysis/gwarnagi/data/flocon>rwfilter flocon.rw --stime=2005/1/1-2005/12/1 -
-proto=0- --pass=stdout | rwstats --count=10 --field=sip | ~/tools/converthex
INPUT: 20028 Records for 6297 Bins and 20028 Total Records
OUTPUT: Top 10 Bins by Records
sIP|   Records|  %Records|   cumul_%|
data|       315|  1.572798|  1.572798|
flow|       278|  1.388057|  2.960855|
traffic|       235|  1.173357|  4.134212|
network|       218|  1.088476|  5.222688|
analysis|       148|  0.738965|  5.961654|
time|       145|  0.723986|  6.685640|
port|       137|  0.684042|  7.369682|
netflow|       109|  0.544238|  7.913921|
information|       109|  0.544238|  8.458159|
source|       100|  0.499301|  8.957460|
/analysis/gwarnagi/data/flocon>
```

FloCon 2004 - Arlington, Virginia

Theme: The First FloCon

Date: July, 22 2004

Topics:

- Infrastructure Issues
- Analysis
- Data Sharing

Chair:

- Tom Longstaff

SiLK Release 0.4, 2004-Mar-19

Changelog

- Critical Update. Public releases of the SiLK Tool Suite prior to this release (SiLK-0.3 and earlier) contained a bug that affected the packing of web records. This bug caused the source and destination ports for web records to be swapped, e.g., web connections from your network to sourceforge.net would show the sourceforge.net web service on a high port and have your client machine on port 80.
- This SiLK-0.4 release fixes that bug, and we've provided a Perl script, rwpatchwww.pl, that will repair files you've packed with previous versions. The rwpatchwww.pl script will also migrate your all of your packed files to Version 2 of the SiLK file format. Release SiLK-0.4 of the SiLK Tools will read files packed either in Version 1 or Version 2 format.

SiLK Release 0.3, 2004-Feb-6

Changelog

- Added the rwfpd script that was accidentally omitted from the SiLK-0.2 release.
- Other minor fixes.

SiLK Release 0.2, 2004-Jan-28

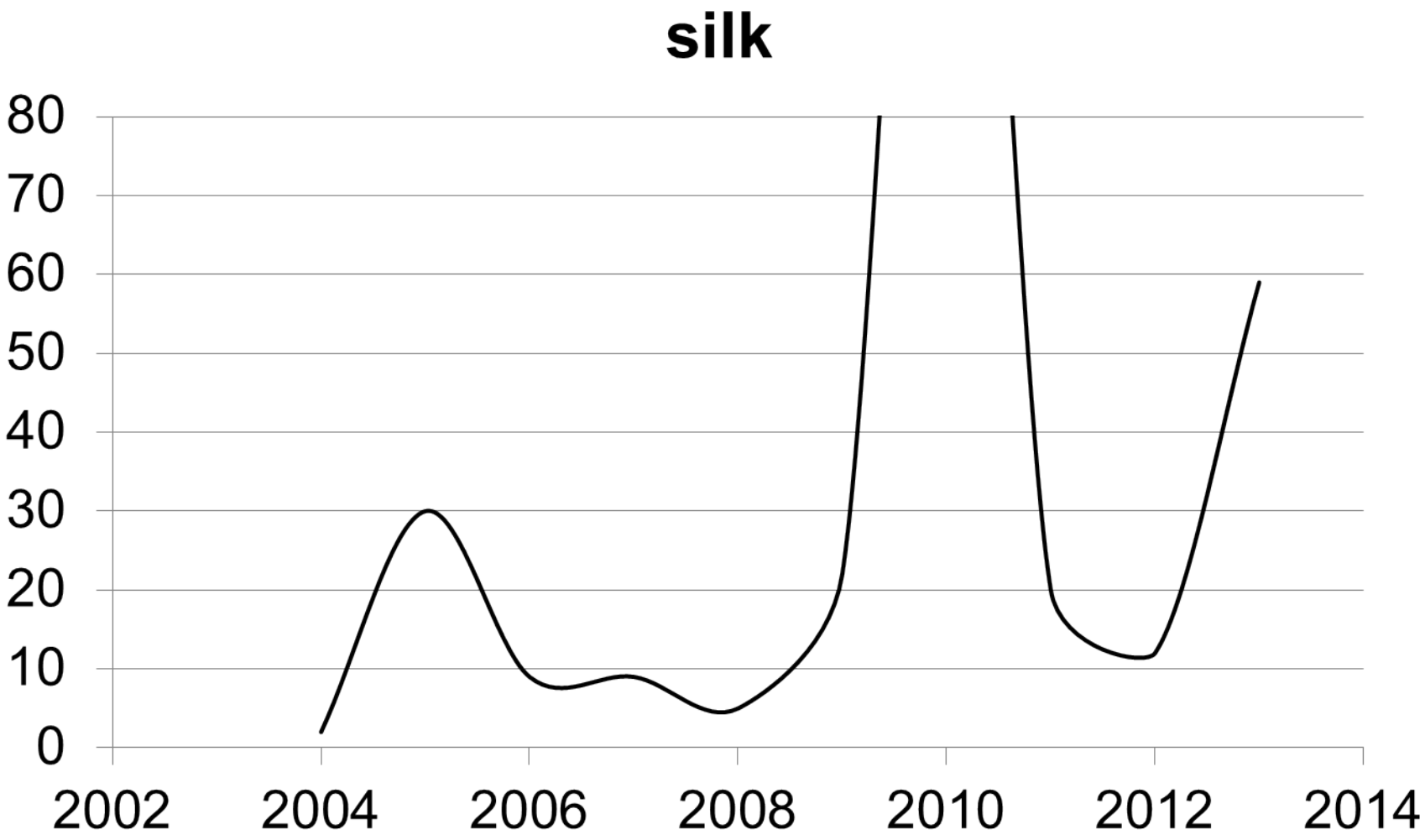
Changelog

- Critical Update. This version fixes major bugs in the initial release of rwflowpack, including a problem that cause the system to produce corrupted packed data files.

SiLK Release 0.1, 2003-Dec-22

Changelog

- Initial public "preview" of the SiLK Analysis Suite and Packing System.


silk
80
70
60
50
40
30
20
10
0
2002
2004
2006
2008
2010
2012
2014

FloCon 2004 - Arlington, Virginia

Carnegie Mellon
Software Engineering Institute

CERT
Situational
Awareness

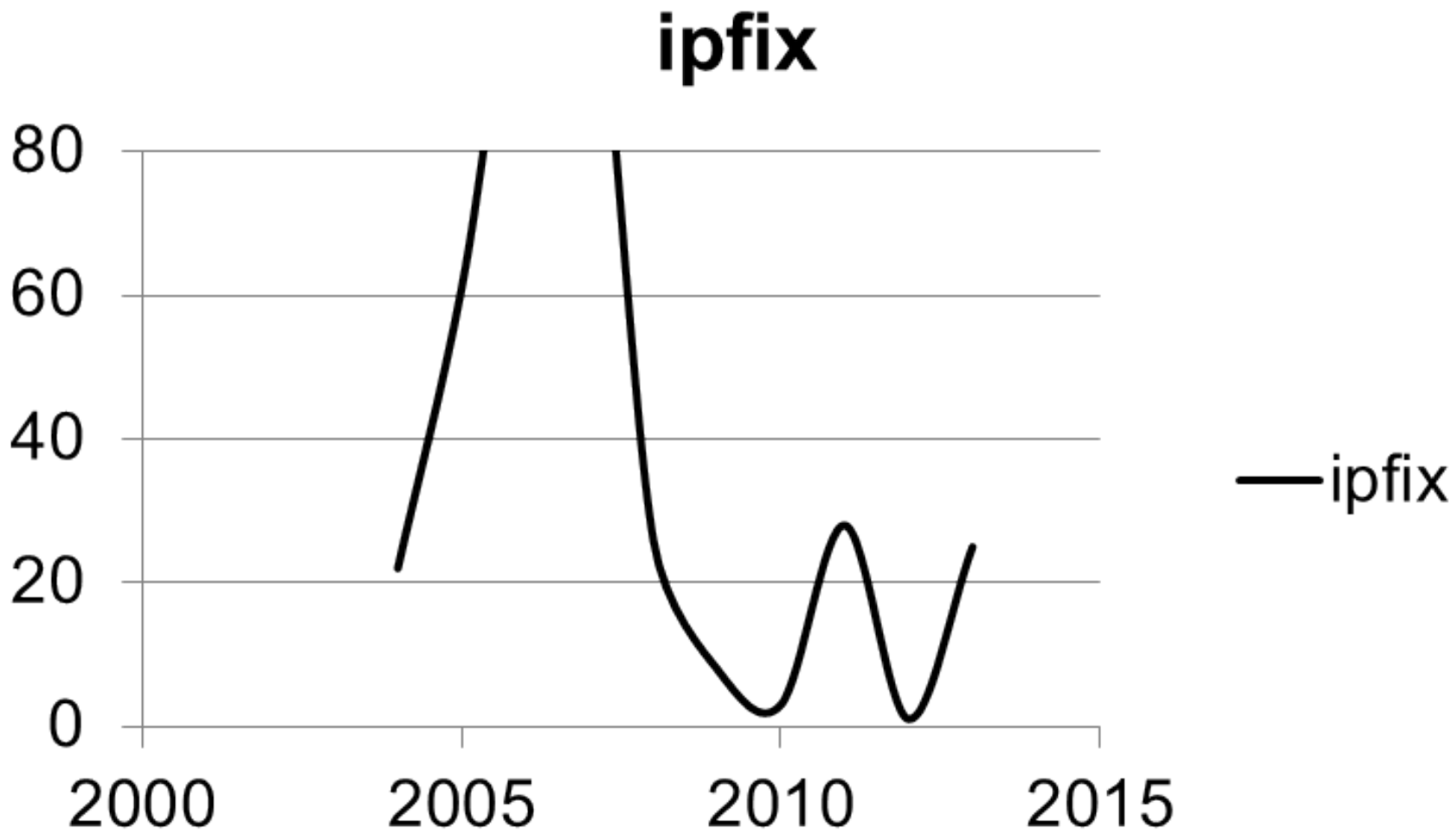
IETF IP Flow Information Export (IPFIX) WG

http://www.ietf.org/html.charters/ipfix-charter.html

- Binary, extensible information model for IP flows exported from a given *observation point* (i.e., router line-card) to a *collector*
  - Based on Cisco Netflow v9
- Designates a mandatory protocol (SCTP) to use in the transport of these flows

(Note: Various text and figures were taken from the IPFIX I-Ds)

6


ipfix
80
60
40
20
0
2000
2005
2010
2015
ipfix

FloCon 2004 - Arlington, Virginia

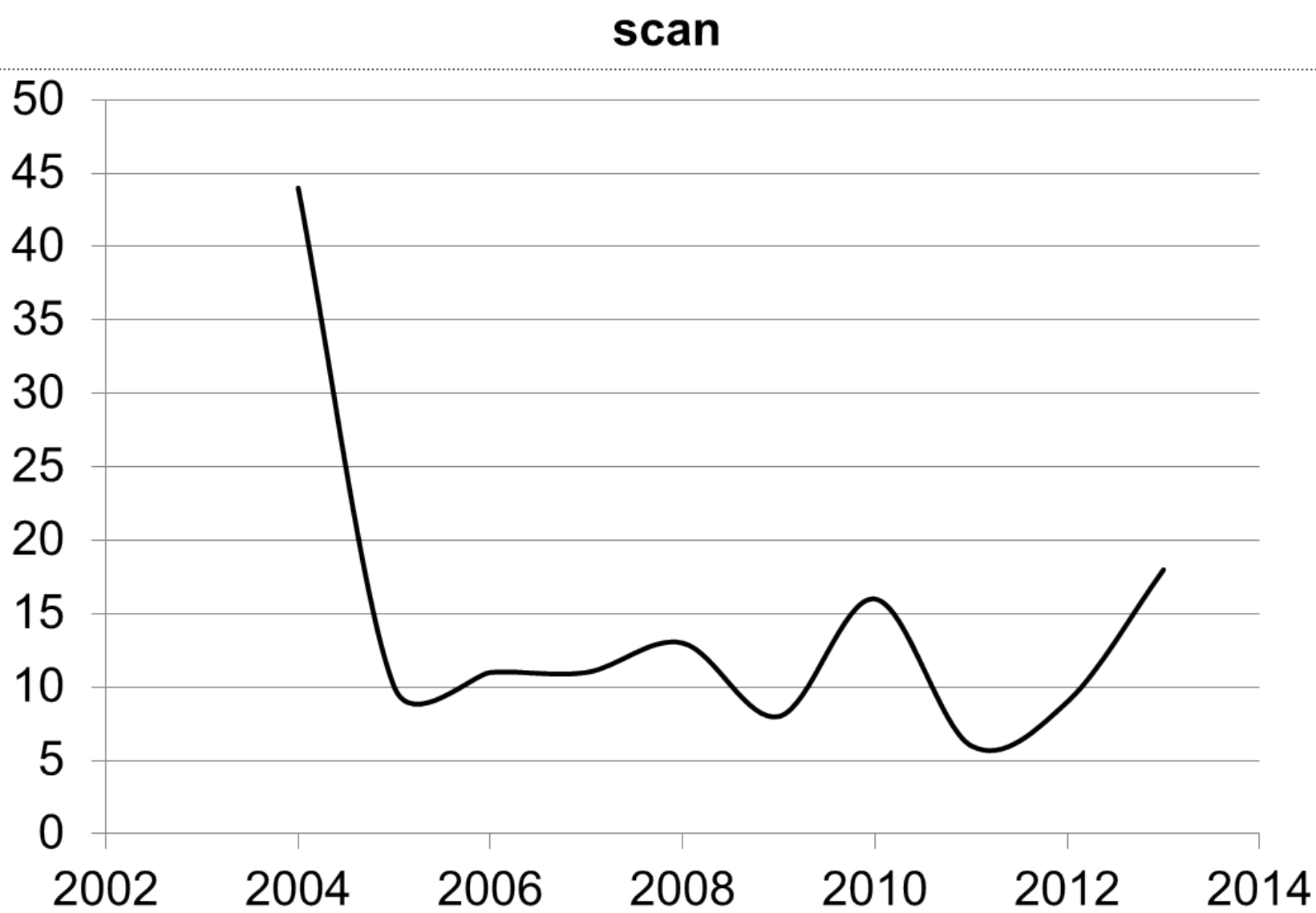
Carnegie Mellon University
Software Engineering Institute

Detection and Analysis of Scans on Very Large Networks

FloCon 2004: Modeling Techniques Panel
July 21, 2004

Marc Kellner
Carrie Gates

CERT® Centers
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890


scan
50
45
40
35
30
25
20
15
10
5
0
2002
2004
2006
2008
2010
2012
2014

FloCon 2004 - Arlington, Virginia

Carnegie Mellon
Software Engineering Institute

CERT
Situational
Awareness

What do you want from Netflow?

- Distribution of flags
- Payload hash
- Start/End packet
- IPV6
- MPLS
- Eval network changes on netflow implementation
- IP packet frags
- Sizing characterization (mean/packets vs packet size)
- Methods of data reduction (sampling, compression, etc)
- ICMP data

3

FloCon 2005 - New Orleans, Louisiana

Theme: Community Building

Date: September 21, 2005

Topics:

- Experience reports in flow analysis
- Operational security analysis using flow
- Advanced flow analysis techniques
- Expanding the flow format for security needs
- Integrating flows into other security analyses
- Facilitating data sharing/public repositories
- Flow collection technologies
- Network traffic modeling for security
- Alternative traffic abstraction approaches
- Traffic summarization of other services

Chair:

- Michael Collins

FloCon 2005

FloCon 2005 - ~~New Orleans, Louisiana~~

Theme: Community Building

Date: September 21, 2005

Topics:

- Experience reports in flow analysis
- Operational security analysis using flow
- Advanced flow analysis techniques
- Expanding the flow format for security needs
- Integrating flows into other security analyses
- Facilitating data sharing/public repositories
- Flow collection technologies
- Network traffic modeling for security
- Alternative traffic abstraction approaches
- Traffic summarization of other services

Chair:

- Michael Collins

FloCon 2005 - Pittsburgh, Pennsylvania

Theme: Community Building

Date: September 21, 2005

Topics:

- Experience reports in flow analysis
- Operational security analysis using flow
- Advanced flow analysis techniques
- Expanding the flow format for security needs
- Integrating flows into other security analyses
- Facilitating data sharing/public repositories
- Flow collection technologies
- Network traffic modeling for security
- Alternative traffic abstraction approaches
- Traffic summarization of other services

Chair:

- Michael Collins


PNC
GATEWAY CLIPPER FLEET
MAJESTIC

FloCon 2005 - Pittsburgh, Pennsylvania

data	315
flow	278
traffic	235
network	218
analysis	148
time	145
port	137
information	109
netflow	109
source	100
detection	89
figure	81
security	80
ports	80
applications	76
user	64
internet	63
ipfix	61

FloCon 2005 - Pittsburgh, Pennsylvania

VisFlowConnect-IP: An Animated Link Analysis Tool For Visualizing Netflows *

Xiaoxin Yin William Yurcik Adam Slagell
National Center for Supercomputing Applications (NCSA)
University of Illinois at Urbana-Champaign
{xiaoxin,byurcik,slagell}@ncsa.uiuc.edu

Abstract

We present VisFlowConnect-IP, a network flow visualization tool that allows operators to detect and investigate anomalous internal and external network traffic. We model the network on a parallel axes graph with hosts as nodes and traffic flows as lines connecting these nodes. We present an overview of this tool's purpose, as well as a detailed description of its functions.

1 Introduction

vides both an overview of traffic as well as drill-down views that allow users to dig out detailed information, and (3) it provides filtering capabilities that enables users to remove mundane traffic details from the visualization.

2 System Architecture

The general system architecture of VisFlowConnect-IP is shown in Figure 1. VisFlowConnect-IP has three main components: (1) an agent that extracts NetFlow records, (2) a NetFlow analyzer that processes the raw data and stores important statistics, and (3) a visualizer that converts the

FloCon 2005 - Pittsburgh, Pennsylvania

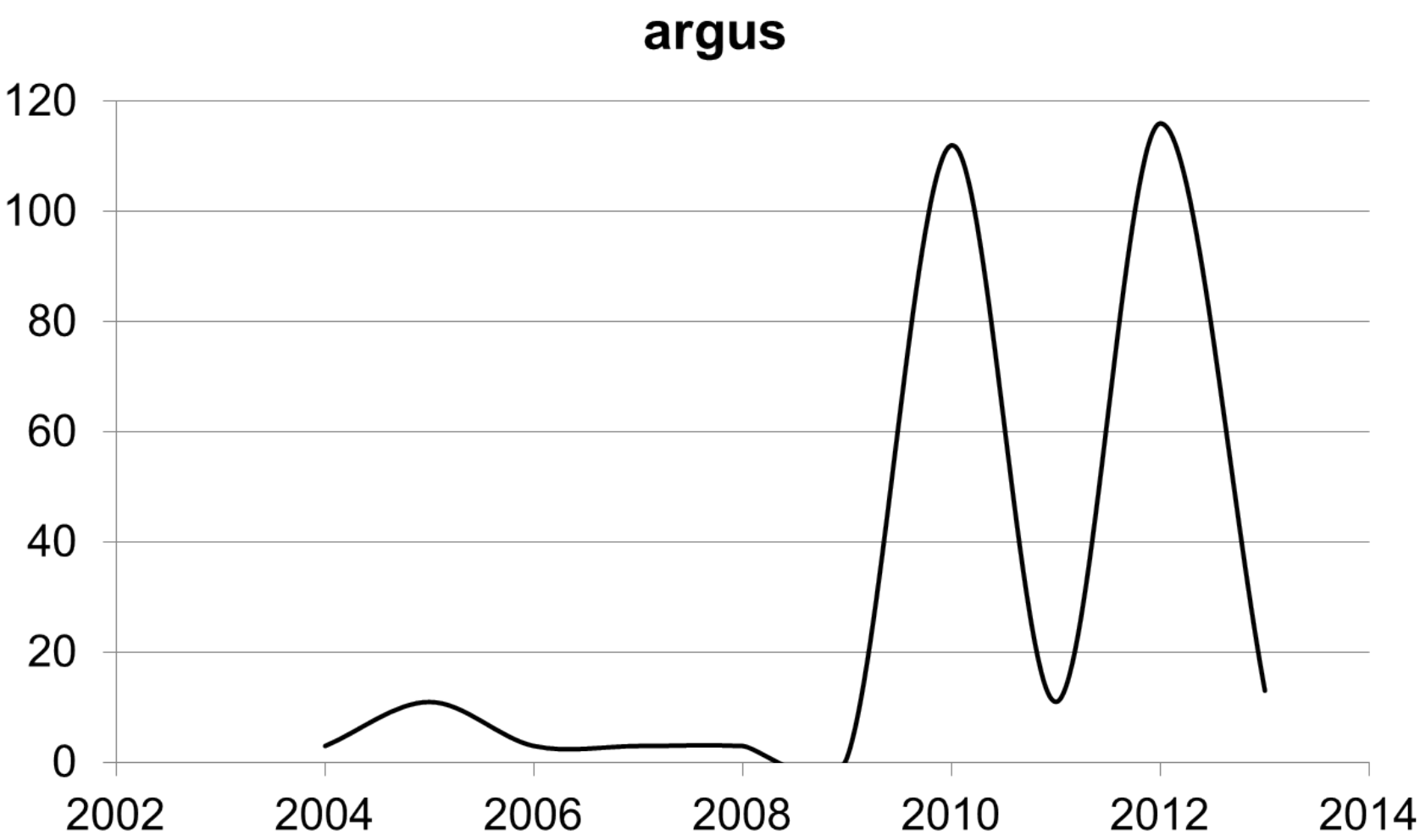
QoSient LLC
Measuring Assessing and Managing QoS

GIGEF
Global Information Grid Evaluation Facilities

Distributed QoS Monitoring
High Performance Network Assurance

Carter Bullard

FloCon 2005 Pittsburgh, PA


argus
120
100
80
60
40
20
0
2002
2004
2006
2008
2010
2012
2014

Pittsburgh, Pennsylvania

2013 - Based on universities, colleges, museums and libraries per person, education level, and public school rank movoto.com names Pittsburgh "Smartest City in America".

Central Connecticut State University names Pittsburgh the 4th most literate city in America based on the culture and resources for reading.

FloCon 2006 - Vancouver, Washington

Theme: Flow as a Study

Date: October 10, 2006

Topics:

- Anomaly detection
- Flow collection and packing
- Visualization techniques
- Standardization

Chair:

- Tim Shimeall

FloCon 2006 - Vancouver, Washington

FloCon 2006 - Vancouver, Washington

DALHOUSIE UNIVERSITY
Inspiring Minds

Faculty of Computer Science
Privacy and Security Lab

The Past and Future of Flow Analysis

John McHugh
Canada Research Chair in Privacy and Security
Faculty of Computer Science
Dalhousie University
Halifax, NS, Canada
My-last-name at cs dot dal dot ca

FloCon 2006 - Vancouver, Washington

FloCon 2006 - Vancouver, Washington

A Traffic Analysis of a Small Private Network Compromised by an On-line Gaming Host

Ron McLeod, BCSc, MCSc.
Director - Corporate Development Telecom Applications Research Alliance
Doctoral Student, Faculty of Computer Science, Dalhousie University

FloCon 2007

FloCon 2008 - Savannah, Georgia

Theme: Beaconing and Distributed Threats

Date: January 7, 2008

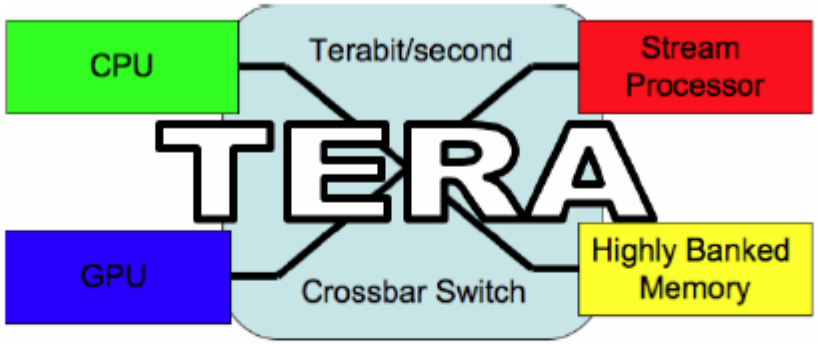
Topics:

- Flow analysis methods
- Experiences in flow analysis
- Innovative security analyses

Chair:

- Tim Shimeall

FloCon 2008 - Savannah, Georgia



On Terabit Flow Analysis

FloCon 2008, Savannah

Jonathan M. Smith

CIS Department, U. Penn

FloCon 2008 - Savannah, Georgia

CERT

YAF

A Case Study in Flow Meter Design

presented at
FloCon 2008 - Savannah, Georgia

Brian Trammell
Technical Lead, Engineering
CERT Network Situational Awareness

Software Engineering Institute | Carnegie Mellon

FloCon 2008 - Savannah, Georgia

STANFORD UNIVERSITY

Regional Visualization and Analytics Center

Incorporating Network Flows in Intrusion Incident Handling and Analysis

John Gerth
Stanford University

gerth@stanford.edu

FloCon 2008

1

FloCon 2009 - Scottsdale, Arizona

Theme: The Practical Use of Flow

Date: January 12, 2009

Topics:

- Flow for network forensics, inventory or incident response
- Visualizations of flow and analytical results
- Multi-stage analysis methods
- Flow collection infrastructure
- Merging flow with other data sources
- Coordination among flow analysis teams
- New or innovative flow methods
- Application detection
- Topology mapping

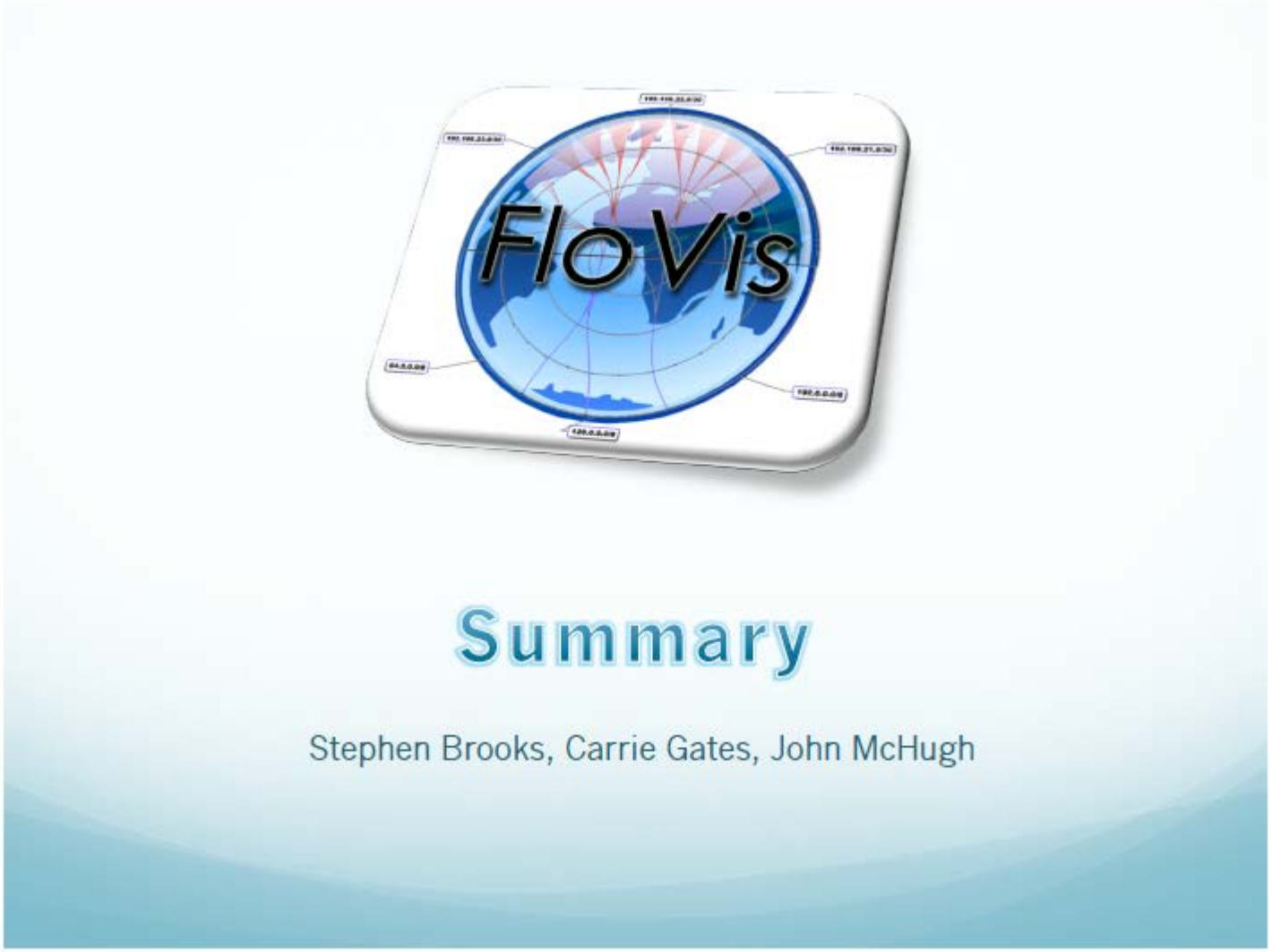
Chair:

- Markus De Shon


DOUBLETREE RESORT
PARADISE VALLEY-SCOTTSDALE

FloCon 2009 - Scottsdale, Arizona

FloCon 2009 - Scottsdale, Arizona



FloCon 2009 - Scottsdale, Arizona

An Analysis of Sampling Effects on Graph Structures Derived from Network Flow Data

Mark Meiss
Advanced Network Management Laboratory
Indiana University

FloCon 2009 - Scottsdale, Arizona

pervasivetechnologylabs
AT INDIANA UNIVERSITY

www.pervasivetechnologylabs.iu.edu

Shared Darknet Development

David A. J. Ripley
daripley@anml.iu.edu

Indiana University Advanced Network Management Laboratory

FloCon 2010 - New Orleans, Louisiana

Theme: Flow in the Context of Other Data

Date: January 11, 2010

Topics:

- Network Operations
- Data Set Sharing
- Network Situational Awareness
- Malicious Behavior
- Flow Collection Technology
- Network Inventory
- Large Scale Modeling
- IPv6 Transition and Analysis
- Network Data Visualization
- Educating on Flow

Chair:

- Sid Faber / Paul Krystosek


Royal Sonesta Hotel
Coca-Cola

FloCon 2010 - New Orleans, Louisiana

FloCon 2010 - New Orleans, Louisiana

FloCon 2010 - New Orleans, Louisiana

Flocon2010 – January 12th, 2010

Introduction to SIE (condensed)

Eric Ziegast
<info@sie.isc.org>

FloCon 2010 - New Orleans, Louisiana

FloCon 2011 - Salt Lake City, Utah

Theme: Learning About Your Network

Date: January 10, 2011

Topics:

- Automated Analysis
- Data Set Sharing
- Educating on Flow
- Flow Analysis with Other Data Sources
- Flow Collection Technology
- IPv6 Transition and Analysis
- Malicious Behavior Detection
- Mathematical and Statistical Modeling
- Network Data Visualization
- Network Inventory, Operations and Situational Awareness

Chair:

- Paul Krystosek / Ed Stoner


Marriott
Marriott
NORDSTROM

FloCon 2011 - Salt Lake City, Utah

FloCon 2011 - Salt Lake City, Utah

FloCon 2011 - Salt Lake City, Utah

REDJACK

Protographs: Graph-Based Approach to NetFlow Analysis

Jeff Janies

RedJack

FloCon 2011

CERT

Analysis Pipeline

Streaming flow analysis with alerting

Dan Ruef - SEI

FloCon 2011 - Salt Lake City, Utah

NTT

NTT Information Sharing Platform Laboratories

Flows as a topology chart

Hiroshi ASAKURA, Kensuke NAKATA,
Shingo KASHIMA, Hiroshi KURAKAMI

NTT Information Sharing Platform Labs.

FloCon 2012 - Austin, Texas

Theme: Progression of analytics from ideas, to prototypes, to tools

Date: January 9, 2012

Topics:

- Automated Analysis
- Adaptive Methods
- Data Set Sharing
- Flow Collection Technology
- Malicious Behavior Detection
- Mathematical and Statistical Modeling
- Network Data Visualization
- Network Inventory and Mapping
- Fusion of Flow Analysis with Other Data Sources

Chair:

- Ed Stoner / Rhiannon Weaver

FloCon 2012 - Austin, Texas

BULLOCK
TEXAS
STATE HISTORY
MUSEUM

TheSTORYofTEXAS.com

FloCon 2012 - Austin, Texas

FloCon 2012 - Austin, Texas

REDJACK

Flow Indexing

Making queries go faster

FloCon
11 January 2012

John McHugh
RedJack LLC

FloCon 2012 - Austin, Texas

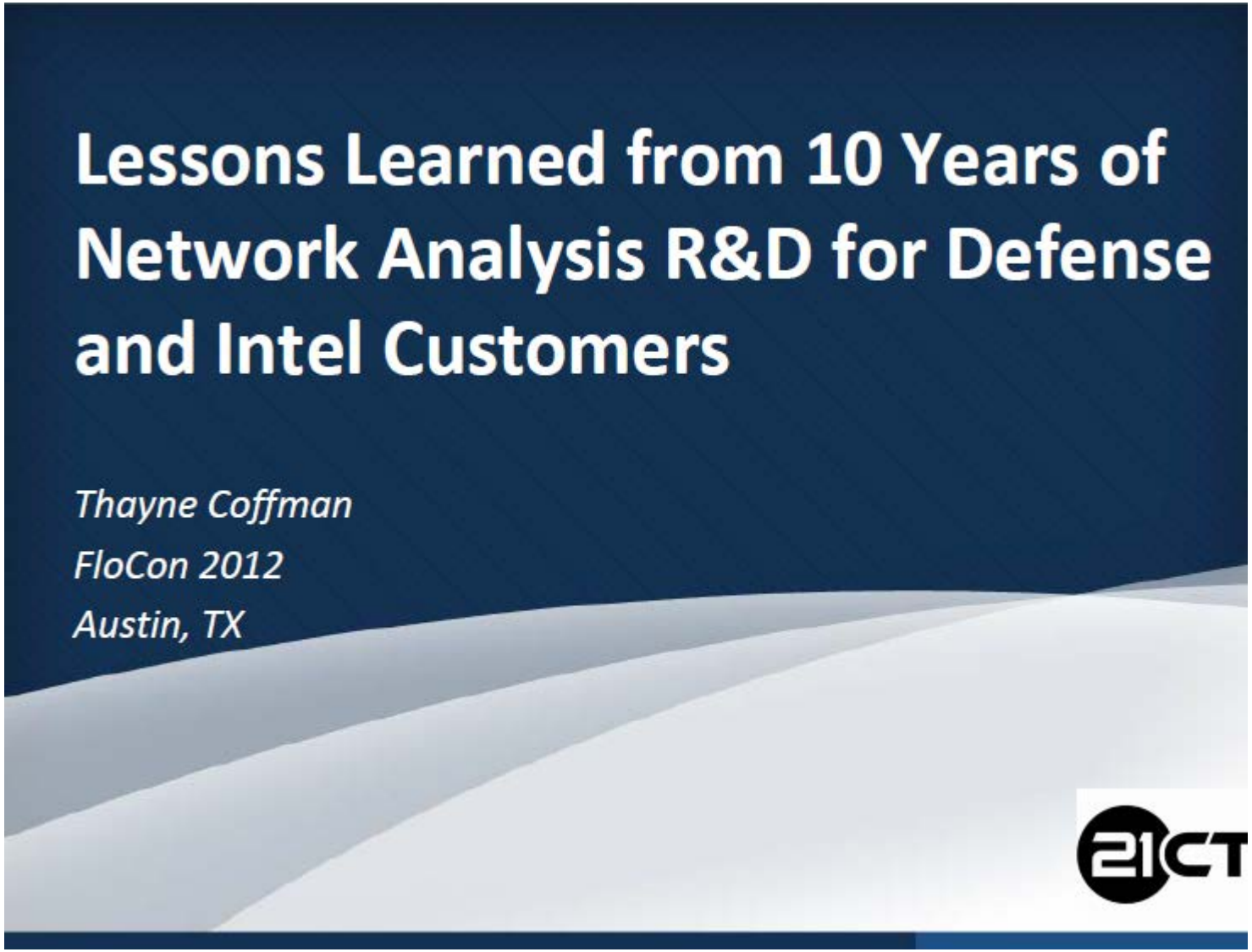
CERT

Network Profiling with SiLK

George Jones, Austin Whisnant
CERT Network Situational Awareness Group

Software Engineering Institute | Carnegie Mellon

FloCon 2012 - Austin, Texas



FloCon 2013 - Albuquerque, NM

Theme: Analysis at Scale

Date: January 7, 2013

Topics:

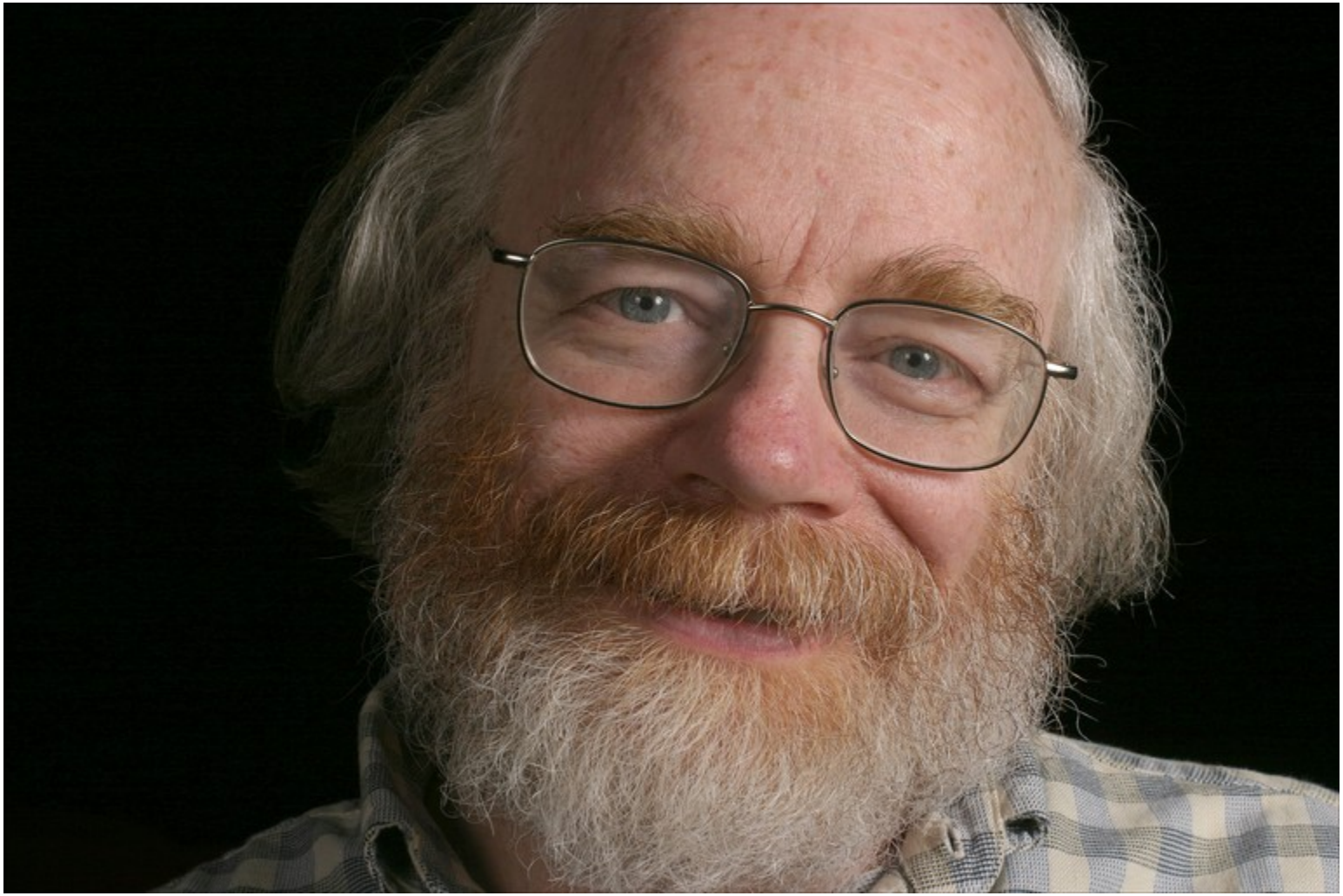
- Automated Analysis
- Data Set Sharing
- Educating on Flow
- Flow Analysis with Other Data Sources
- Flow Collection Technology
- IPv6 Transition and Analysis
- Malicious Behavior Detection
- Mathematical and Statistical Modeling
- Network Data Visualization
- Network Inventory, Operations and Situational Awareness

Chair:

- Rhiannon Weaver / George Jones


HOLIDAYS

FloCon 2013 - Albuquerque, NM



FloCon 2013 - Albuquerque, NM

MS-ISAC CERT

FloCon 2013 - Albuquerque, NM

Bro for Real-Time Large-Scale Understanding

Seth Hall
International Computer Science Institute

FloCon 2013 - Albuquerque, NM

FloCon 2013 - Albuquerque, NM

A Distributed Network Security Analysis System

Based on Apache Hadoop-Related Technologies

Bingdong Li,

Jeff Springer , Mehmet Gunes , George Bebis

University of Nevada Reno

FloCon 2013

January 7-10, Albuquerque, New Mexico

FloCon Top Talkers

Shimeall, Timothy	10
McHugh, John	9
Bullard, Carter	7
McLeod, Ron	7
Zseby, Tanja	7
Collins, Michael	6
Boschi, Elisa	5
Wagner, Arno	5

FloCon 2014 - Charleston, SC

Theme: Perspectives

Date: January 13, 2014

Topics:

- Measurement and metrics
- Discovering and evaluating indicators of malicious behavior
- Automated analysis and augmenting/annotating flow
- Flow collection technology
- Network flow in conjunction with other data sources
- Integrating data sources and data fusion
- Optimizing analyst workflow and scalable statistical techniques
- Data visualization for operational environments and reporting
- Visual perspectives for displaying large data
- Case studies in threat detection and mitigation

Chair:

- George Jones / Jono Spring

10 Years of FloCon

Prepared for FloCon 2014

George Warnagiris - CERT/CC

gwarnagi@cert.org

#GeoWarnagiris