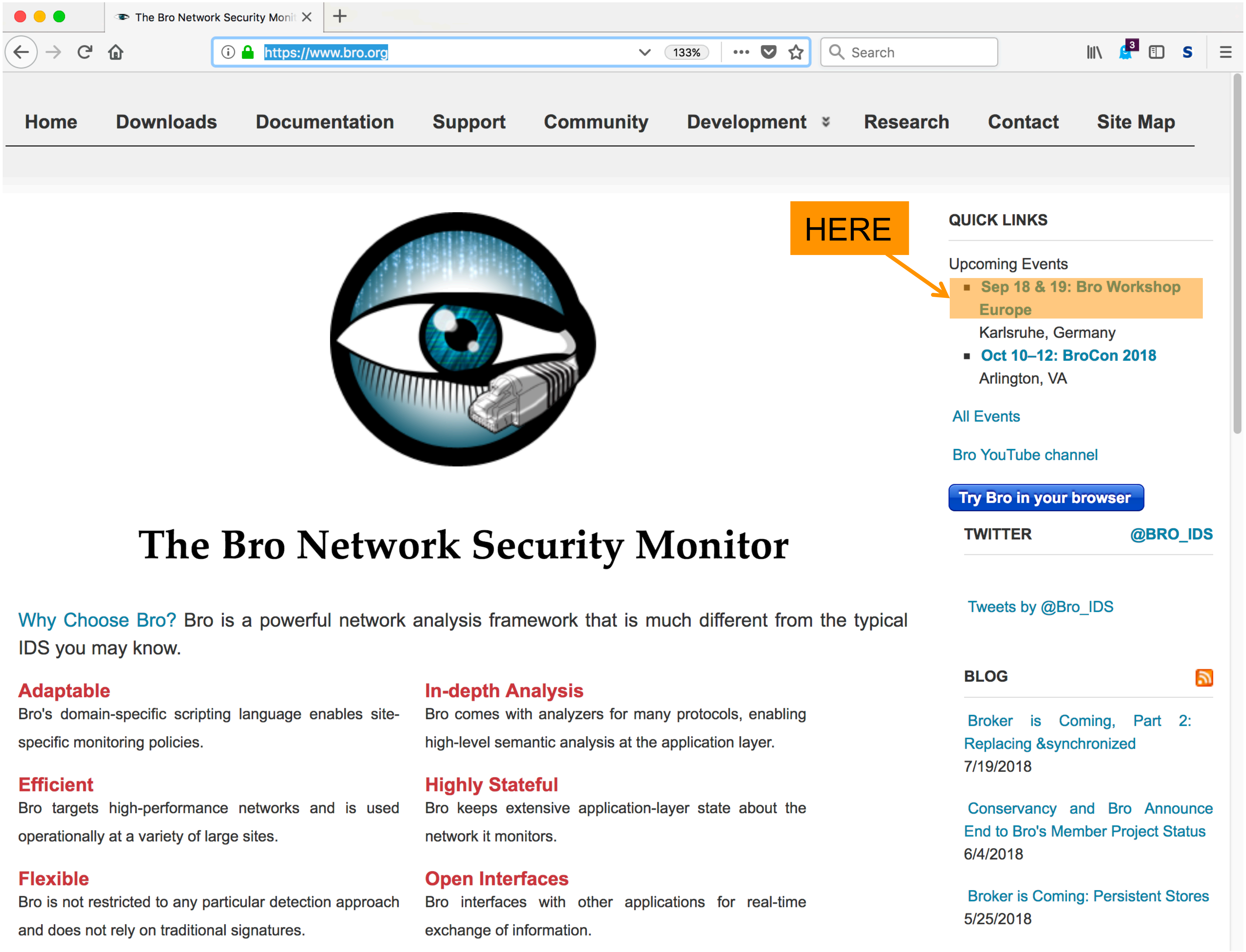
How Did We Get Here?

Vern Paxson

International Computer Science Institute
EECS Department, University of California, Berkeley
Corelight, Inc.

vern@icsi.berkeley.edu
vern@corelight.com

September 18, 2018



The Bro Network Security Monitor

Why Choose Bro? Bro is a powerful network analysis framework that is much different from the typical IDS you may know.

Adaptable
Bro's domain-specific scripting language enables site-specific monitoring policies.

In-depth Analysis
Bro comes with analyzers for many protocols, enabling high-level semantic analysis at the application layer.

Efficient
Bro targets high-performance networks and is used operationally at a variety of large sites.

Highly Stateful
Bro keeps extensive application-layer state about the network it monitors.

Flexible
Bro is not restricted to any particular detection approach and does not rely on traditional signatures.

Open Interfaces
Bro interfaces with other applications for real-time exchange of information.

QUICK LINKS

Upcoming Events

- **Sep 18 & 19: Bro Workshop Europe**
  Karlsruhe, Germany
- **Oct 10–12: BroCon 2018**
  Arlington, VA

All Events

Bro YouTube channel

Try Bro in your browser

TWITTER **@BRO_IDS**

Tweets by @Bro_IDS

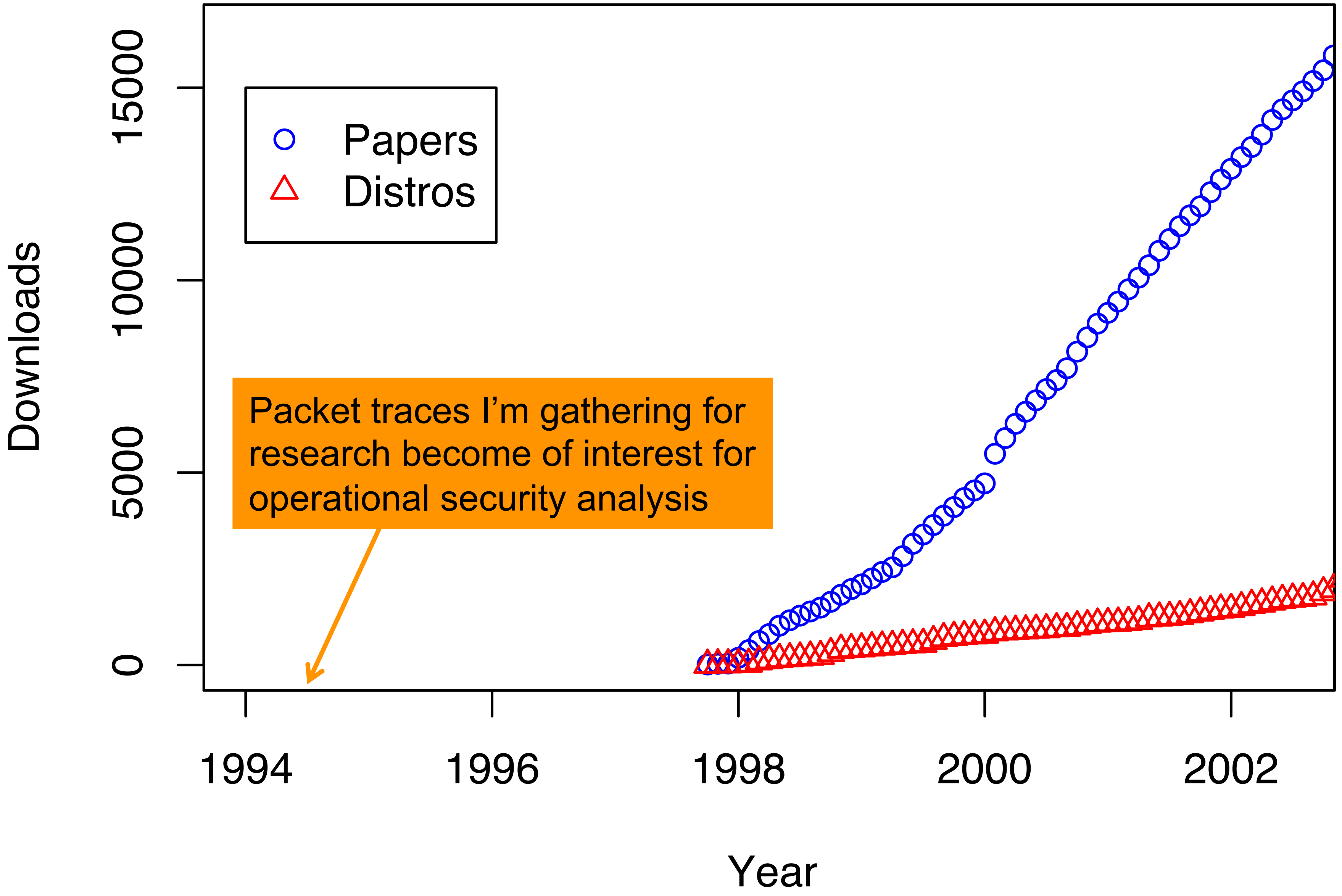
BLOG

Broker is Coming, Part 2: Replacing &synchronized
7/19/2018

Conservancy and Bro Announce End to Bro's Member Project Status
6/4/2018

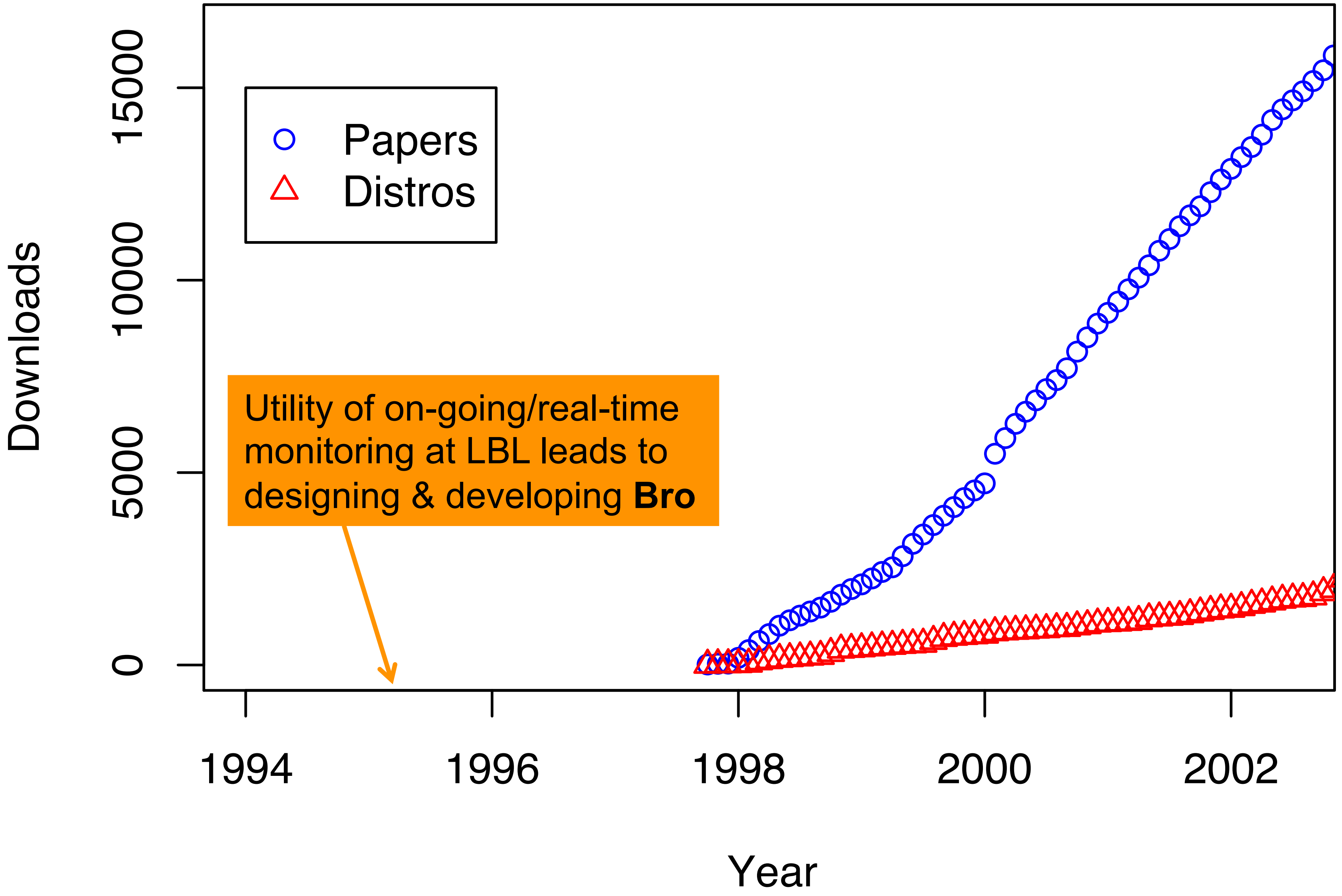
Broker is Coming: Persistent Stores
5/25/2018

Interest in Bro



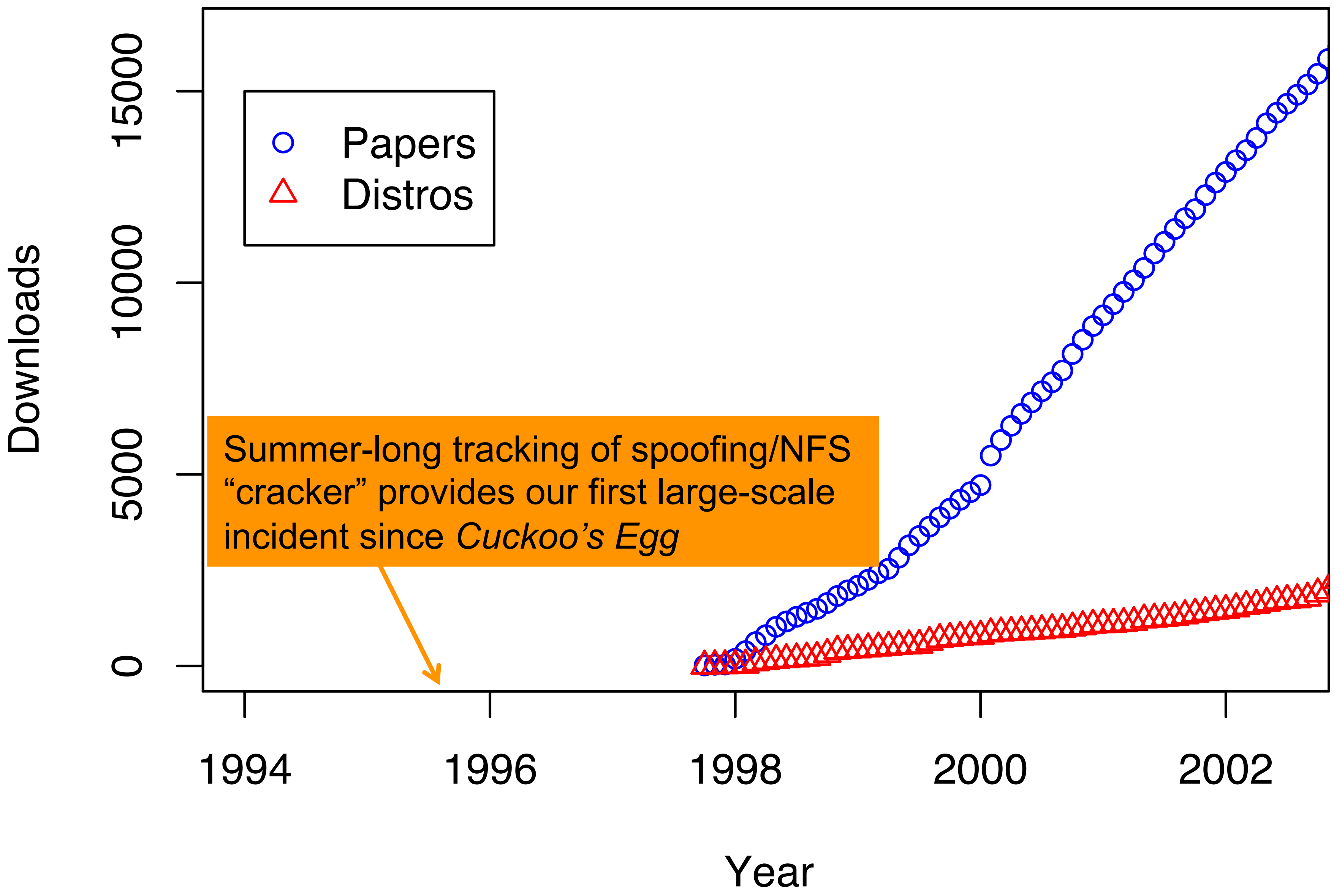
Packet traces I’m gathering for research become of interest for operational security analysis

Interest in Bro



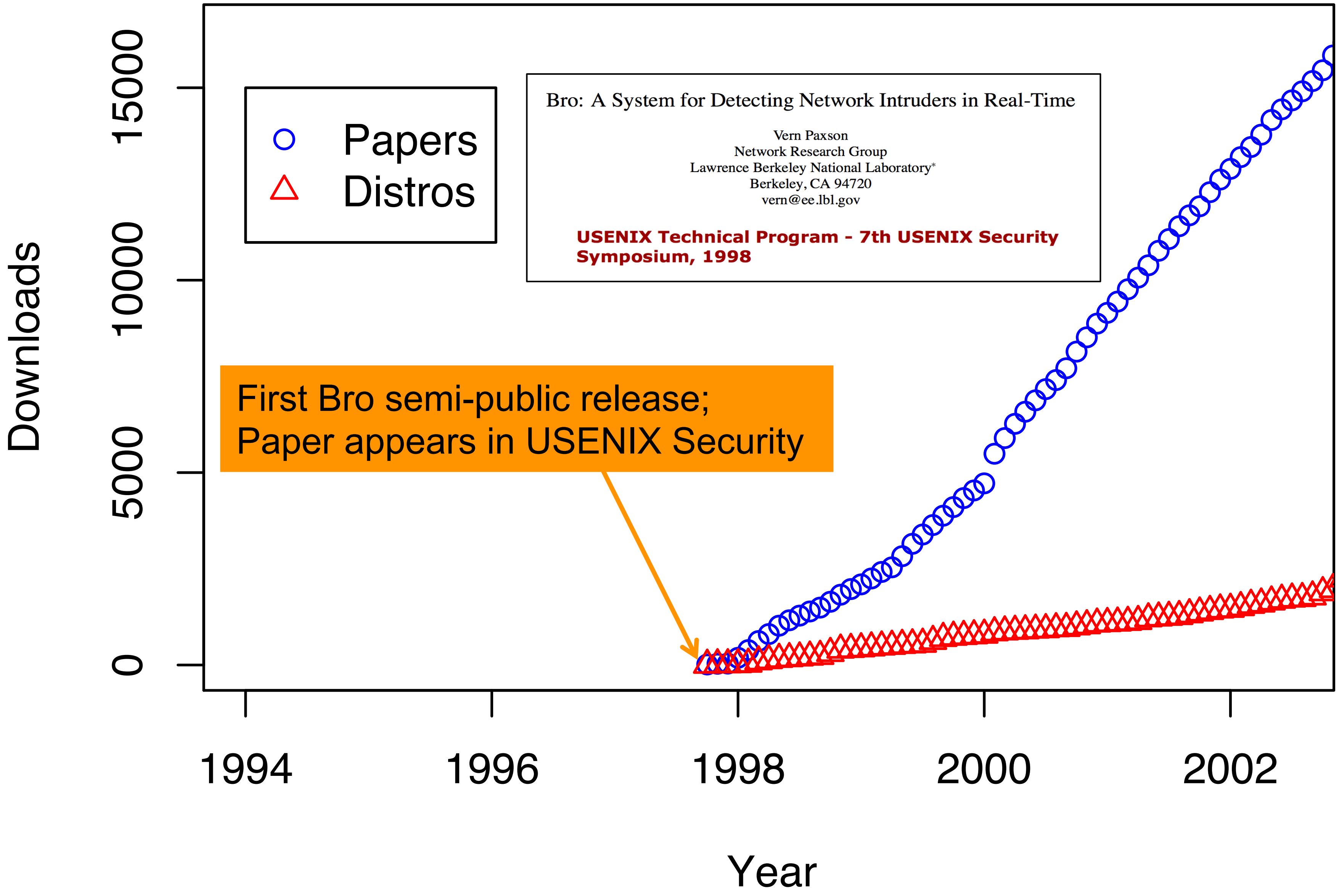
Utility of on-going/real-time monitoring at LBL leads to designing & developing **Bro**

Interest in Bro



Summer-long tracking of spoofing/NFS “cracker” provides our first large-scale incident since *Cuckoo’s Egg*

Interest in Bro

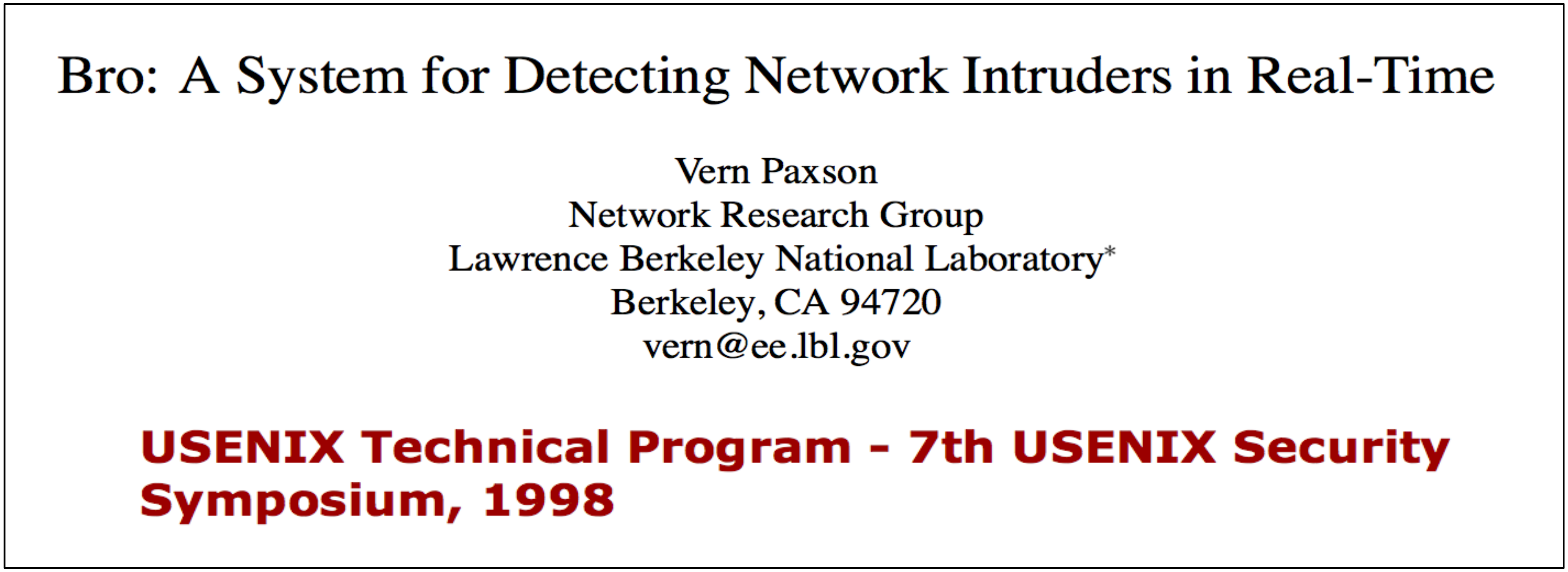


Bro: A System for Detecting Network Intruders in Real-Time

Vern Paxson
Network Research Group
Lawrence Berkeley National Laboratory*
Berkeley, CA 94720
vern@ee.lbl.gov

USENIX Technical Program - 7th USENIX Security Symposium, 1998

First Bro semi-public release;
Paper appears in USENIX Security



Bro: A System for Detecting Network Intruders in Real-Time

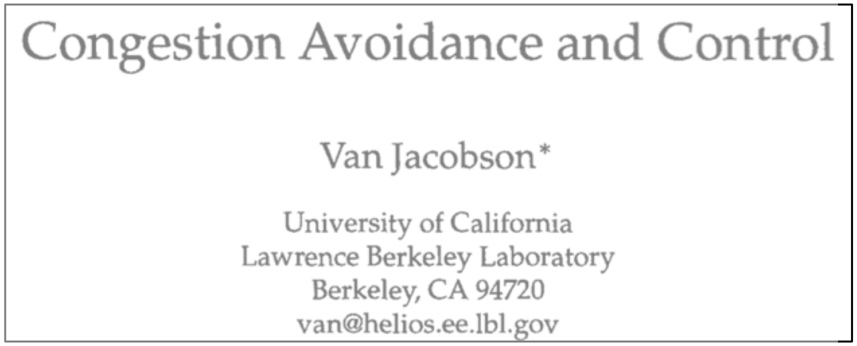
Vern Paxson
Network Research Group
Lawrence Berkeley National Laboratory*
Berkeley, CA 94720
vern@ee.lbl.gov

USENIX Technical Program - 7th USENIX Security Symposium, 1998

Prior to developing Bro, we had significant operational experience with a simpler system based on off-line analysis of `tcpdump` [JLM89] trace files. Out of this experience we formulated a number of design goals and requirements:

BERKELEY LAB

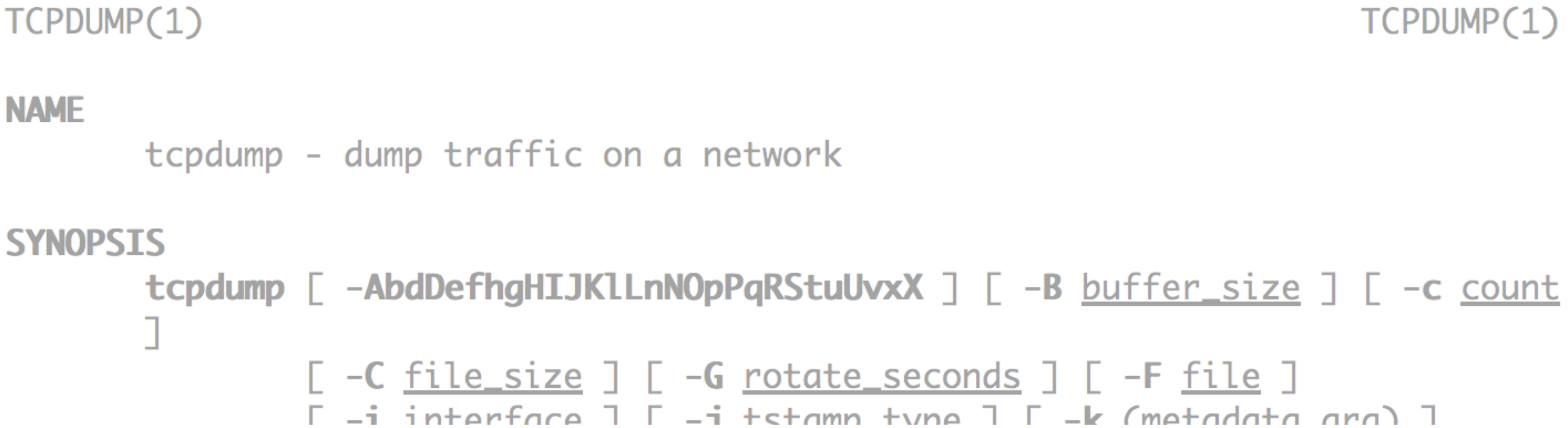
Bringing Science Solutions to the World



Congestion Avoidance and Control

Van Jacobson*

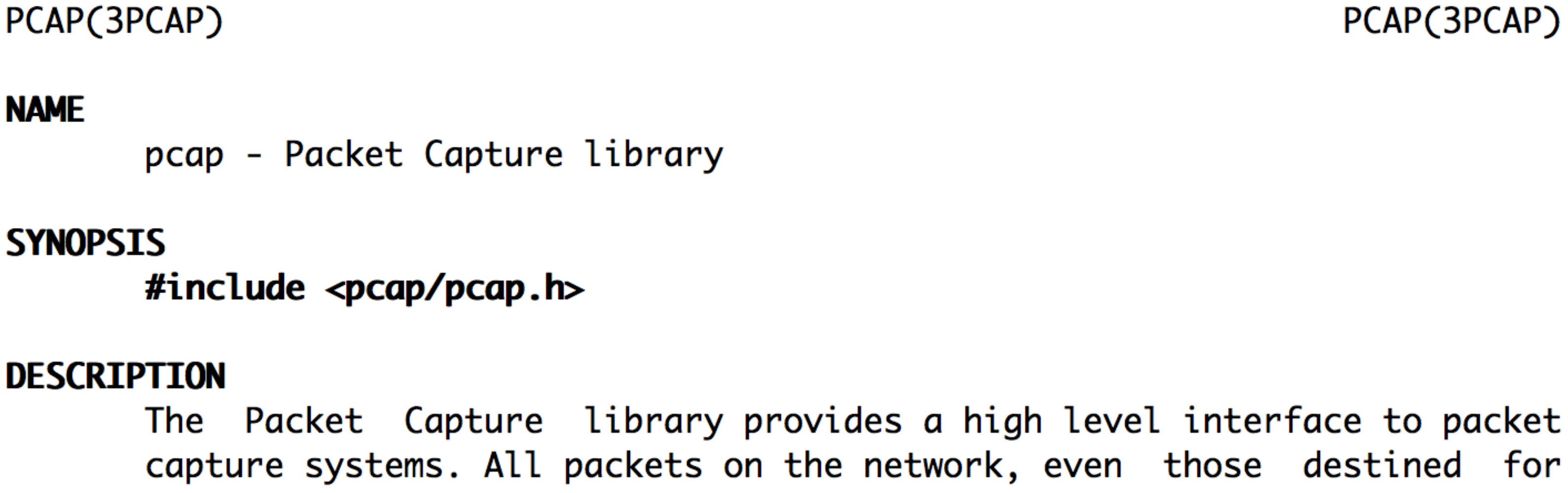
University of California
Lawrence Berkeley Laboratory
Berkeley, CA 94720
van@helios.ee.lbl.gov



```
TCPDUMP(1)                                              TCPDUMP(1)

NAME
       tcpdump - dump traffic on a network

SYNOPSIS
       tcpdump [ -AbdDefhgHIJKlLnNOpPqRStuUvxX ] [ -B buffer_size ] [ -c count
       ]
               [ -C file_size ] [ -G rotate_seconds ] [ -F file ]
               [ -i interface ] [ -j tstamp_type ] [ -k (metadata_arg) ]
```

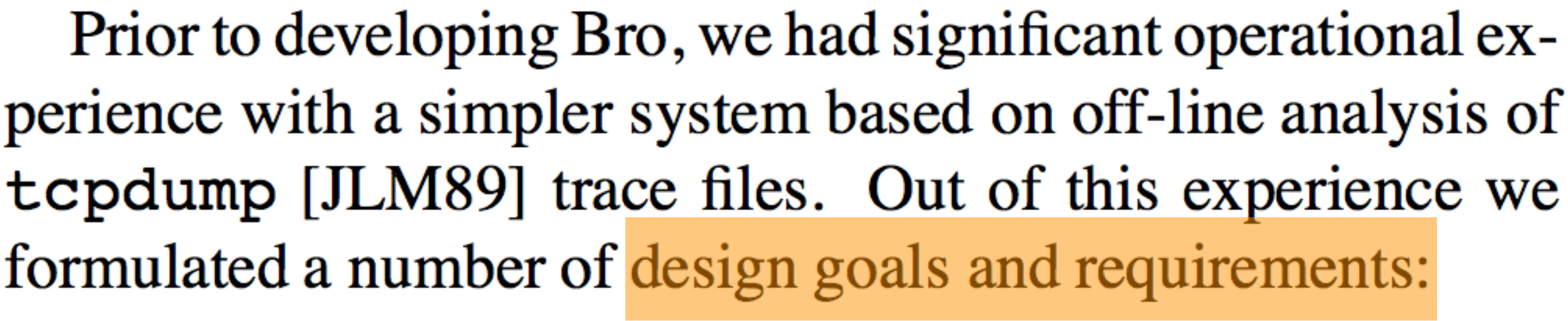


```
PCAP(3PCAP)                                              PCAP(3PCAP)

NAME
       pcap - Packet Capture library

SYNOPSIS
       #include <pcap/pcap.h>

DESCRIPTION
       The  Packet  Capture  library provides a high level interface to packet
       capture systems. All packets on the network, even  those  destined  for
```



Prior to developing Bro, we had significant operational experience with a simpler system based on off-line analysis of `tcpdump` [JLM89] trace files. Out of this experience we formulated a number of design goals and requirements:

High-speed, large volume monitoring

No packet filter drops

Real-time notification

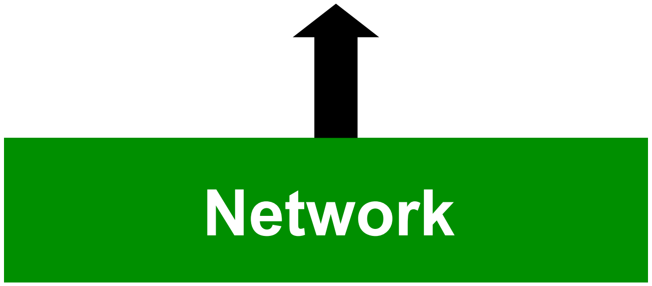
Mechanism separate from policy

Extensible

Avoid simple mistakes

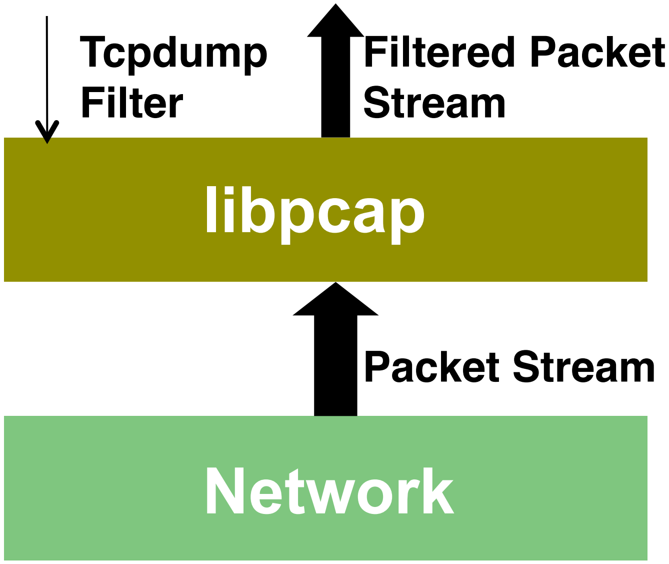
The monitor will be attacked

Original Architecture



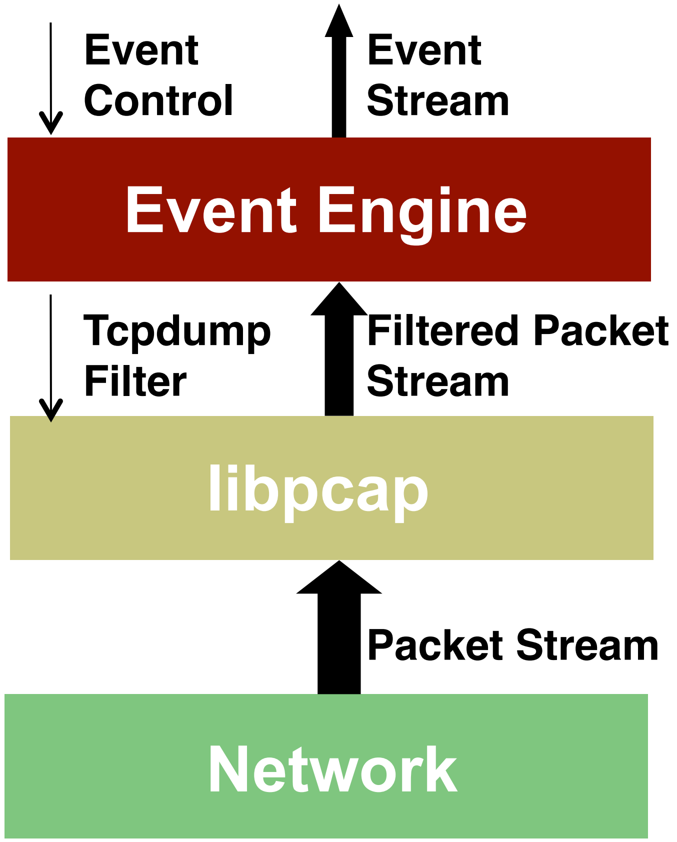
- Taps network link passively, sends up a copy of all network traffic.

Original Architecture



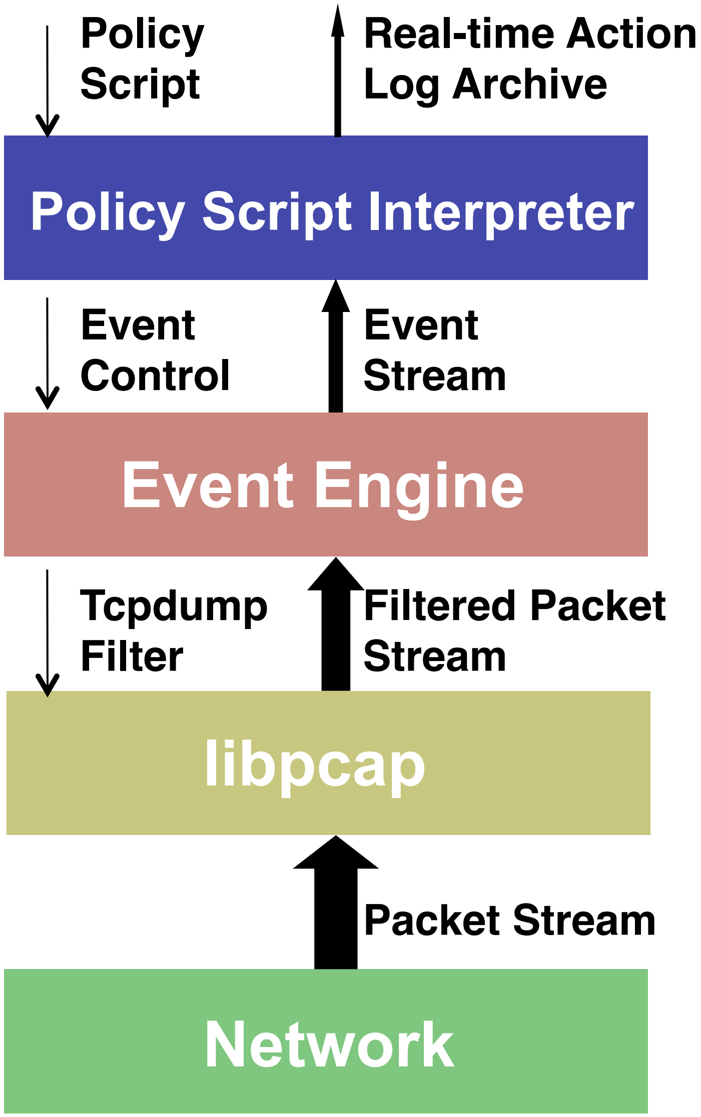
- Kernel filters down high-volume stream via standard *libpcap* packet capture library.

Original Architecture



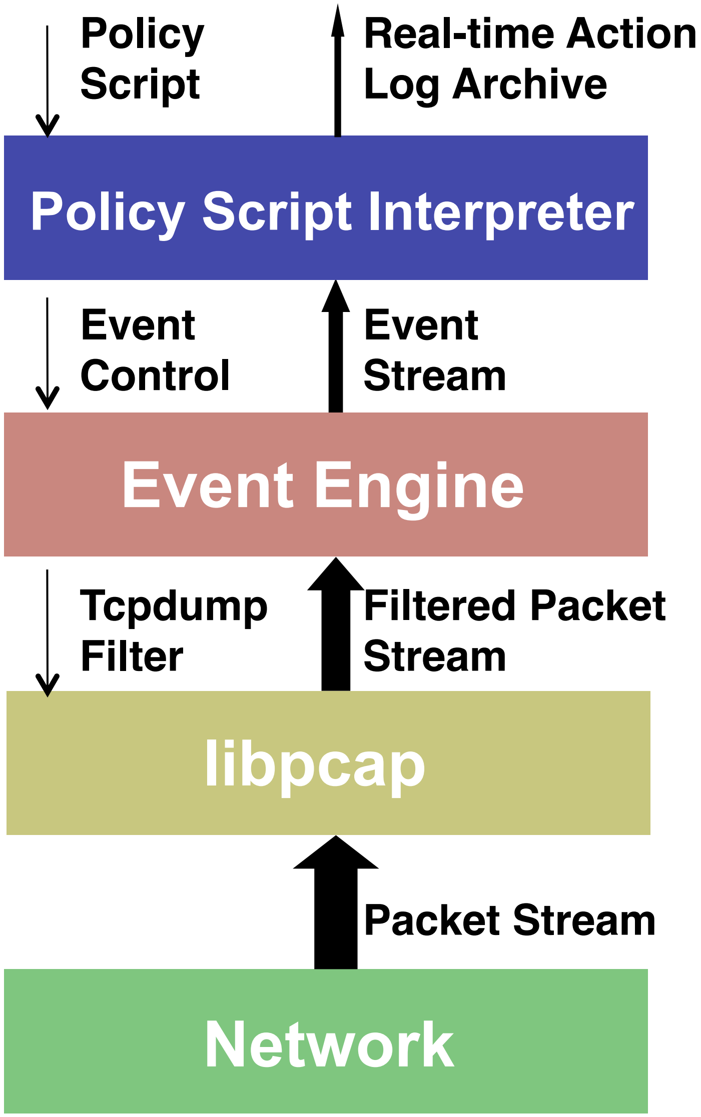
- “Event engine” decodes protocols, distills filtered stream into high-level, *policy-neutral* events reflecting underlying network activity
  - E.g., connection_attempt, http_reply, teredo_authentication
  - These span a range of semantic levels
  - Currently ~700+ different types

Original Architecture



- Script written in Domain Specific Language processes event stream, incorporates:
  - Context/state from past events
  - Additional input sources
  - Site's particular policies

Original Architecture

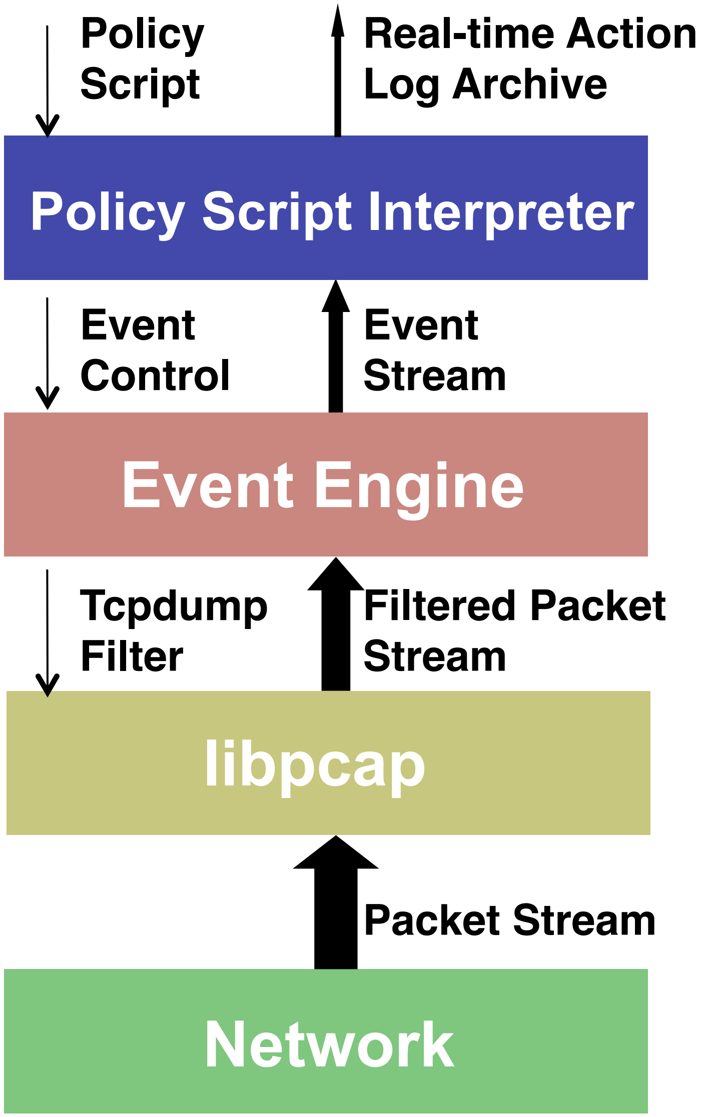


- Script written in Domain Specific Language processes event stream, incorporates:
  - Context/state from past events
  - Additional input sources
  - Site's particular policies

… and *takes action*:

Records to disk - **extensive** logs
Generates real-time alerts
Executes programs as a form of **response**

Original Architecture



- Script written in Domain Specific Language processes event stream, incorporates:
  - Context/state from past events
  - Additional input sources
  - Site's particular policies

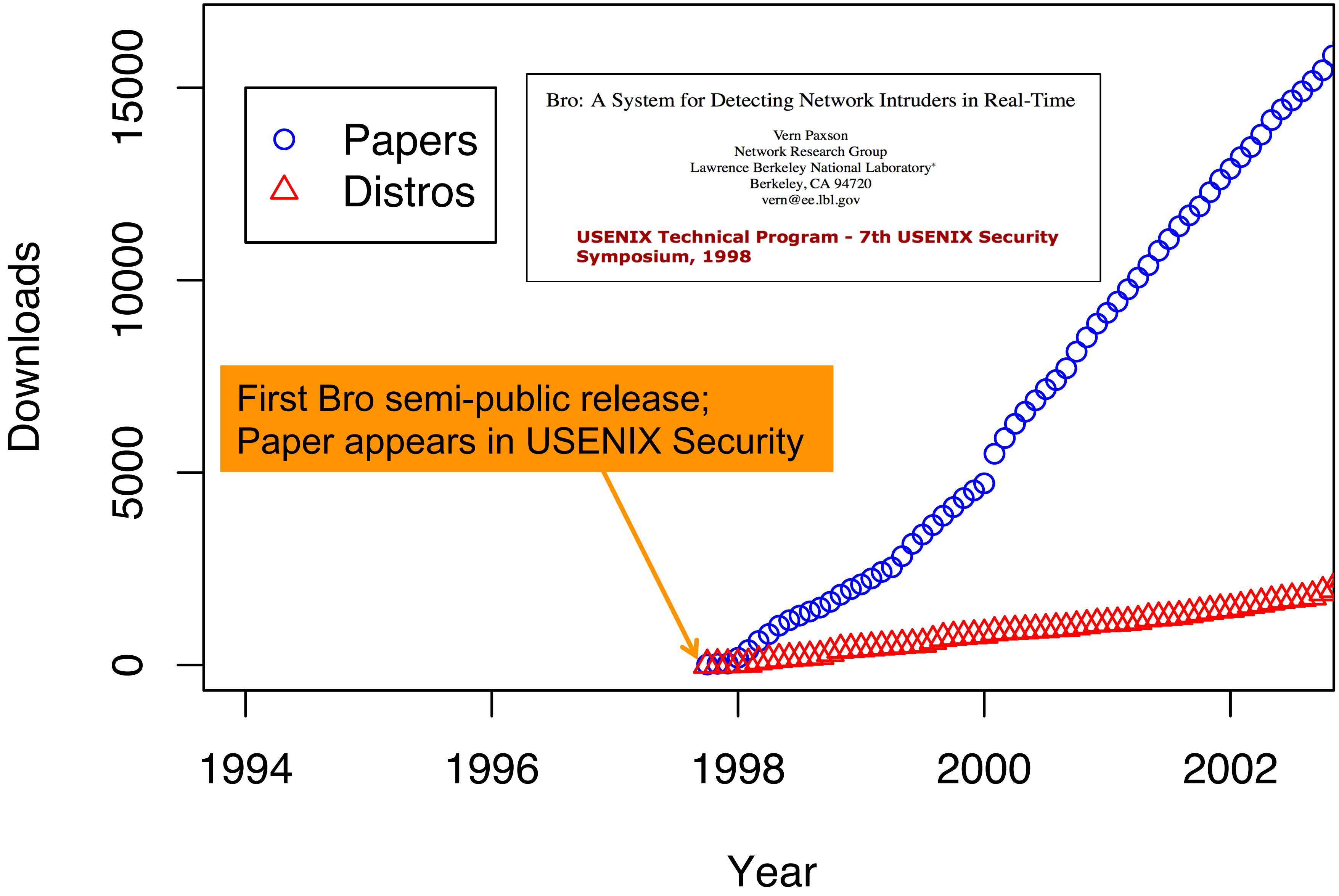
… and *takes action*:

Records to disk - **extensive** logs

Generates real-time alerts

Executes programs as a form of **response**

Interest in Bro



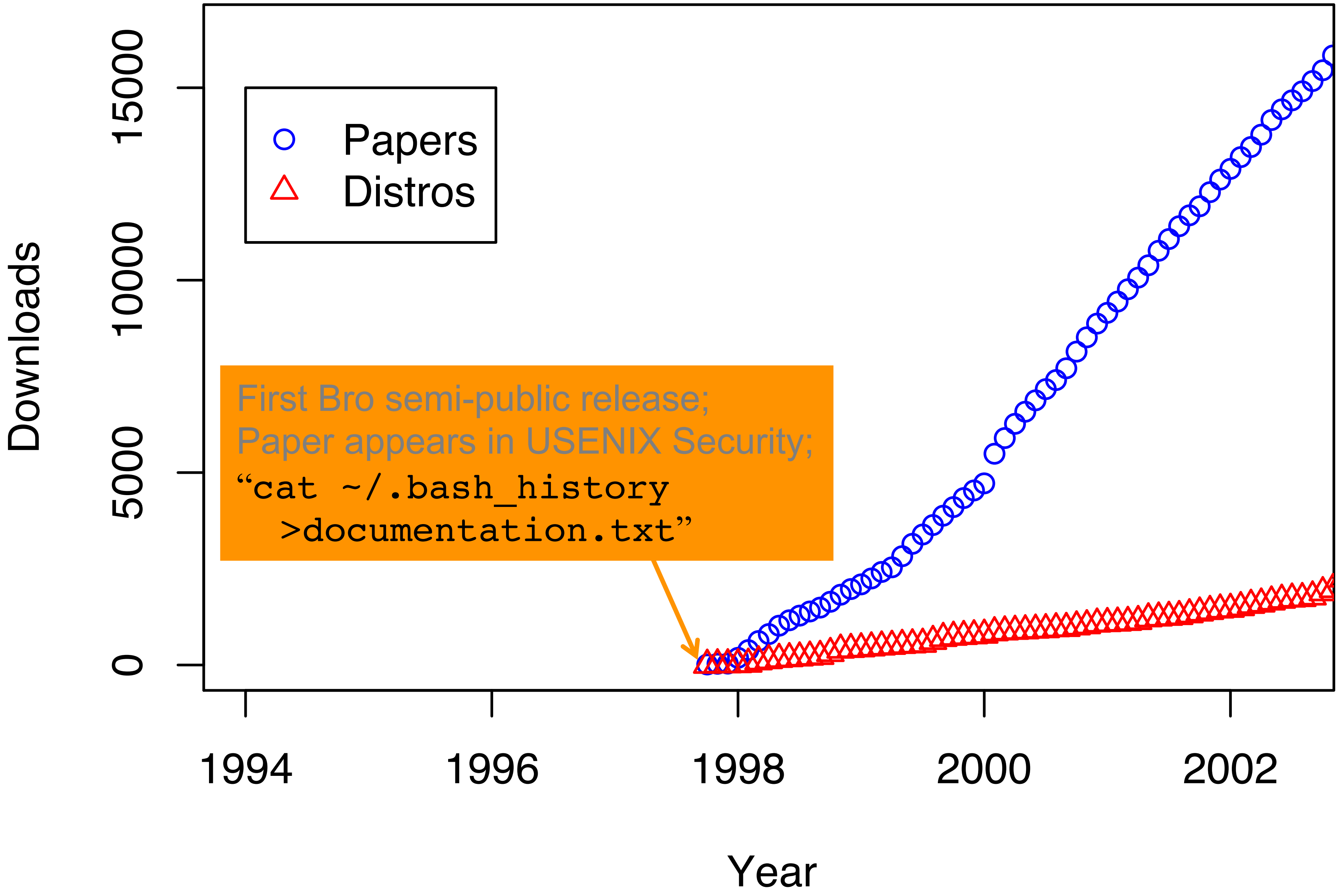
Bro: A System for Detecting Network Intruders in Real-Time

Vern Paxson
Network Research Group
Lawrence Berkeley National Laboratory*
Berkeley, CA 94720
vern@ee.lbl.gov

USENIX Technical Program - 7th USENIX Security Symposium, 1998

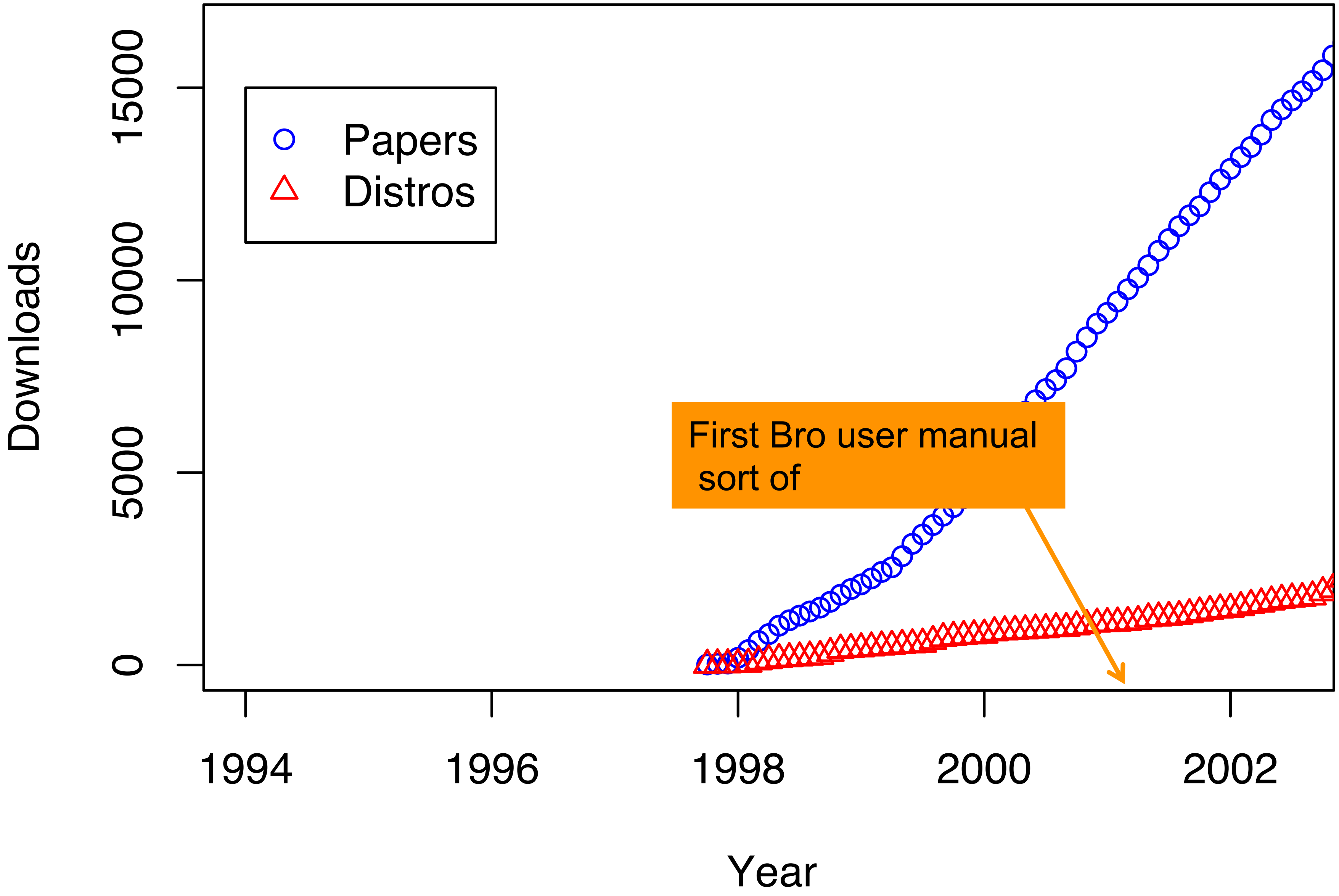
First Bro semi-public release;
Paper appears in USENIX Security

Interest in Bro

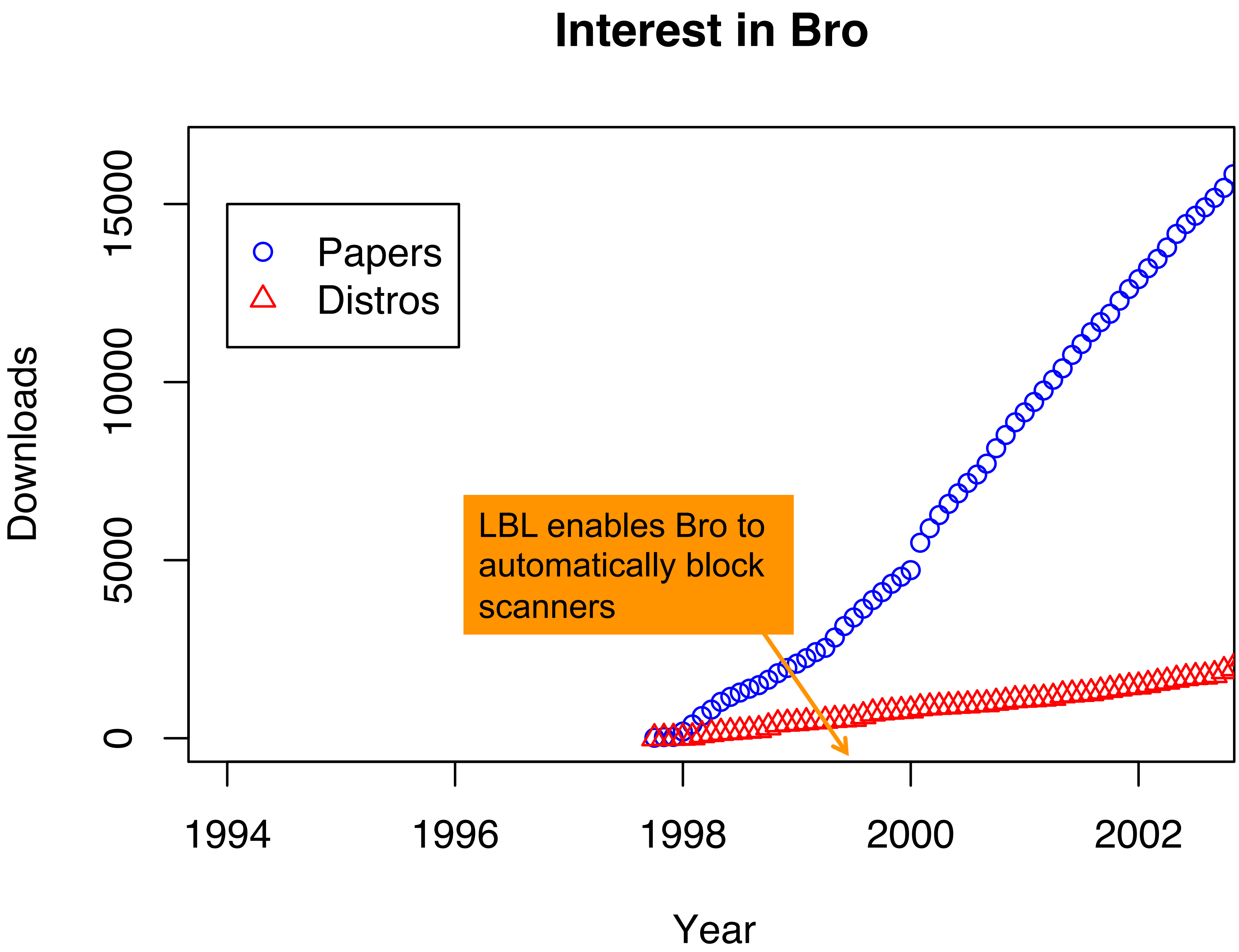


First Bro semi-public release;
Paper appears in USENIX Security;
“cat ~/.bash_history
  >documentation.txt”

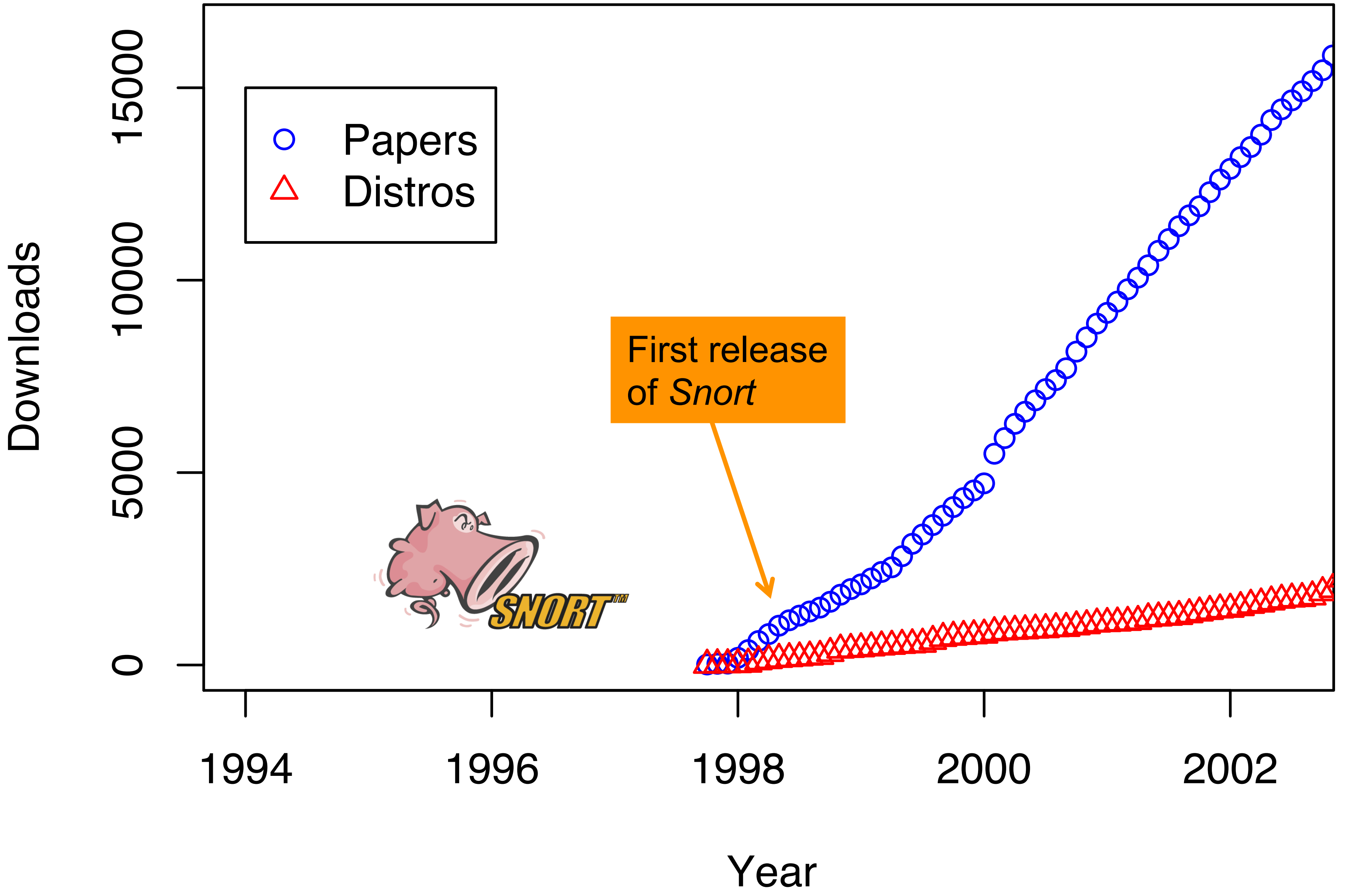
Interest in Bro



First Bro user manual
 sort of

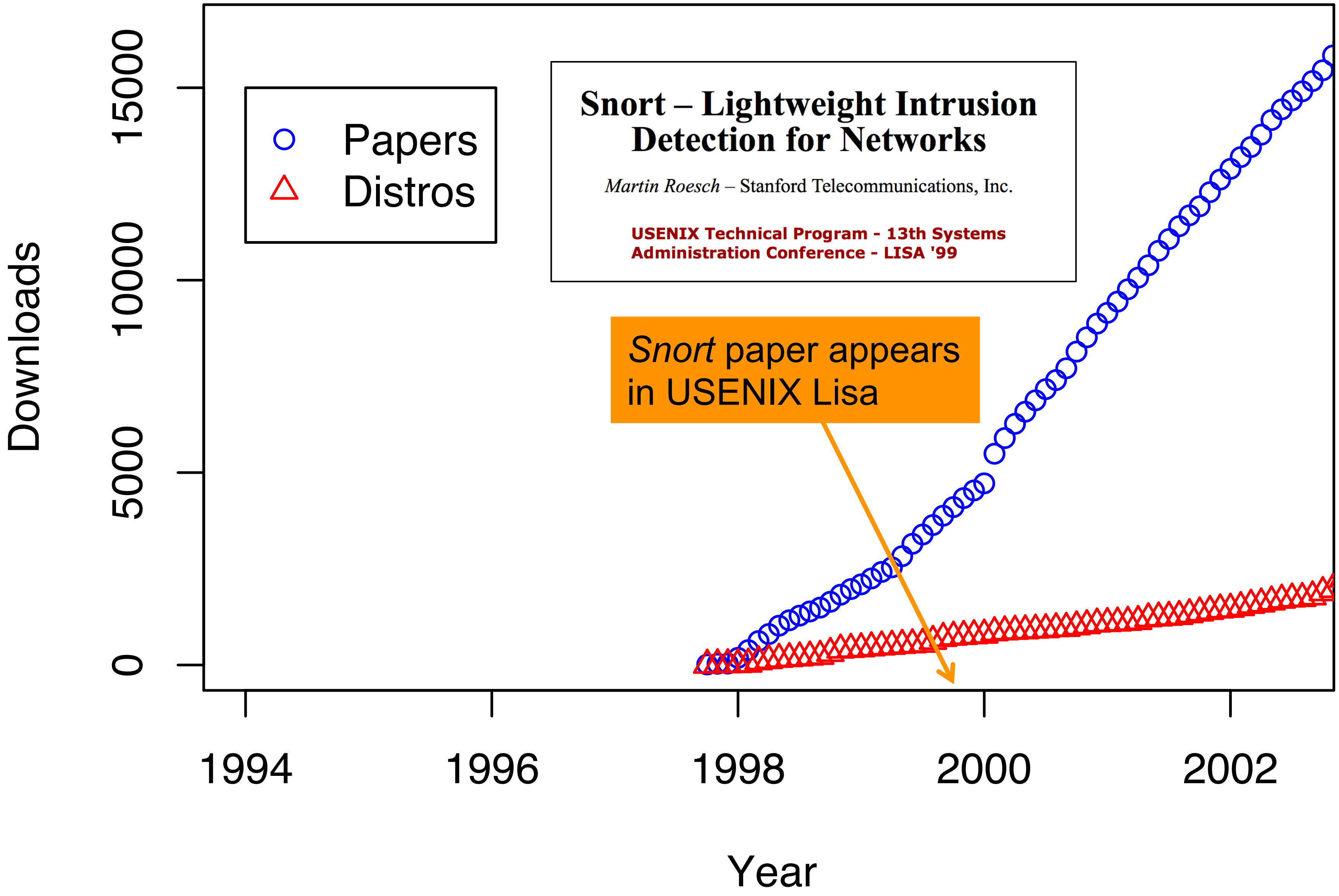

Interest in Bro
Downloads
0
5000
10000
15000
1994
1996
1998
2000
2002
Year
○ Papers
△ Distros
LBL enables Bro to automatically block scanners

Interest in Bro



First release of *Snort*

Interest in Bro



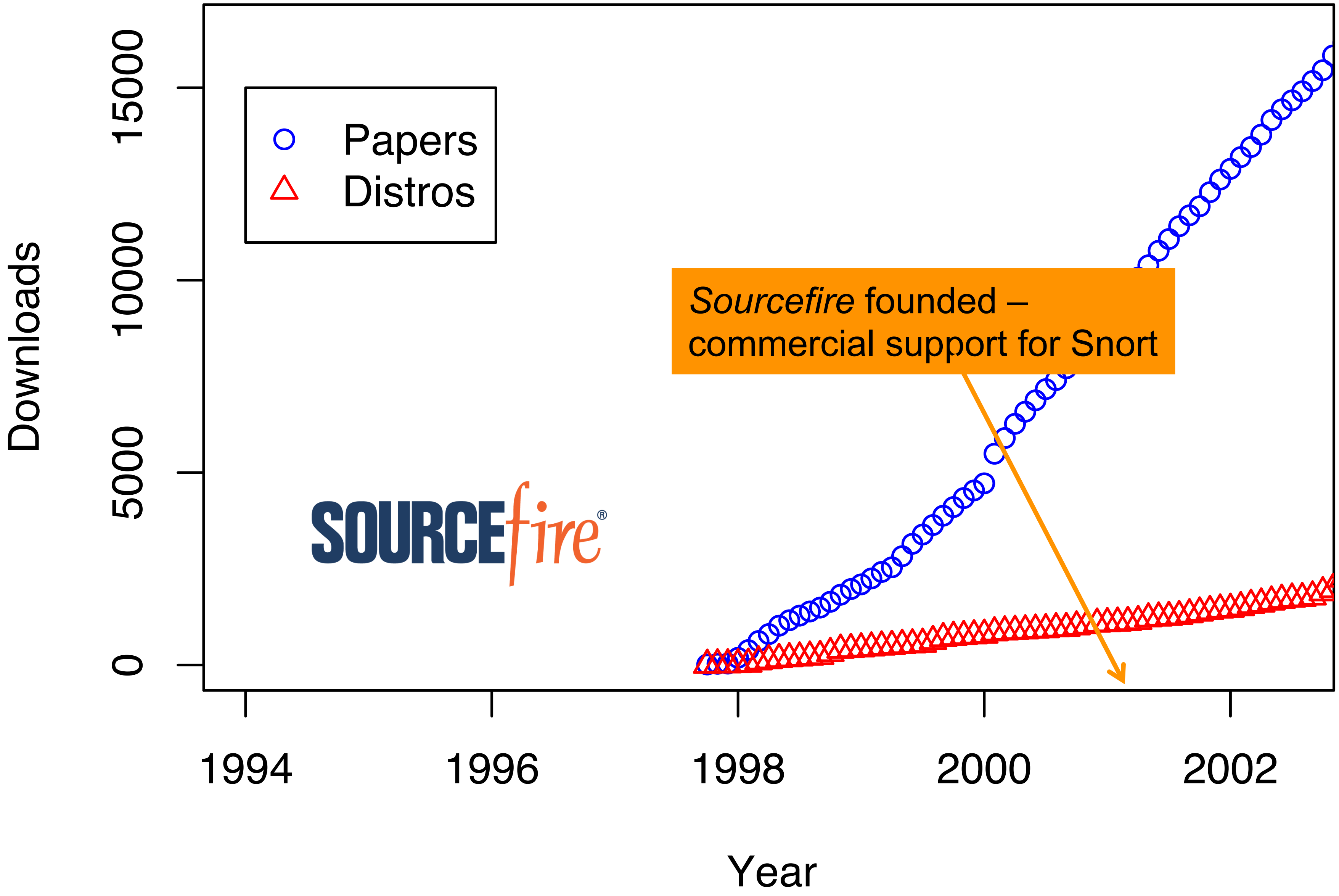
Snort – Lightweight Intrusion Detection for Networks

Martin Roesch – Stanford Telecommunications, Inc.

USENIX Technical Program - 13th Systems Administration Conference - LISA '99

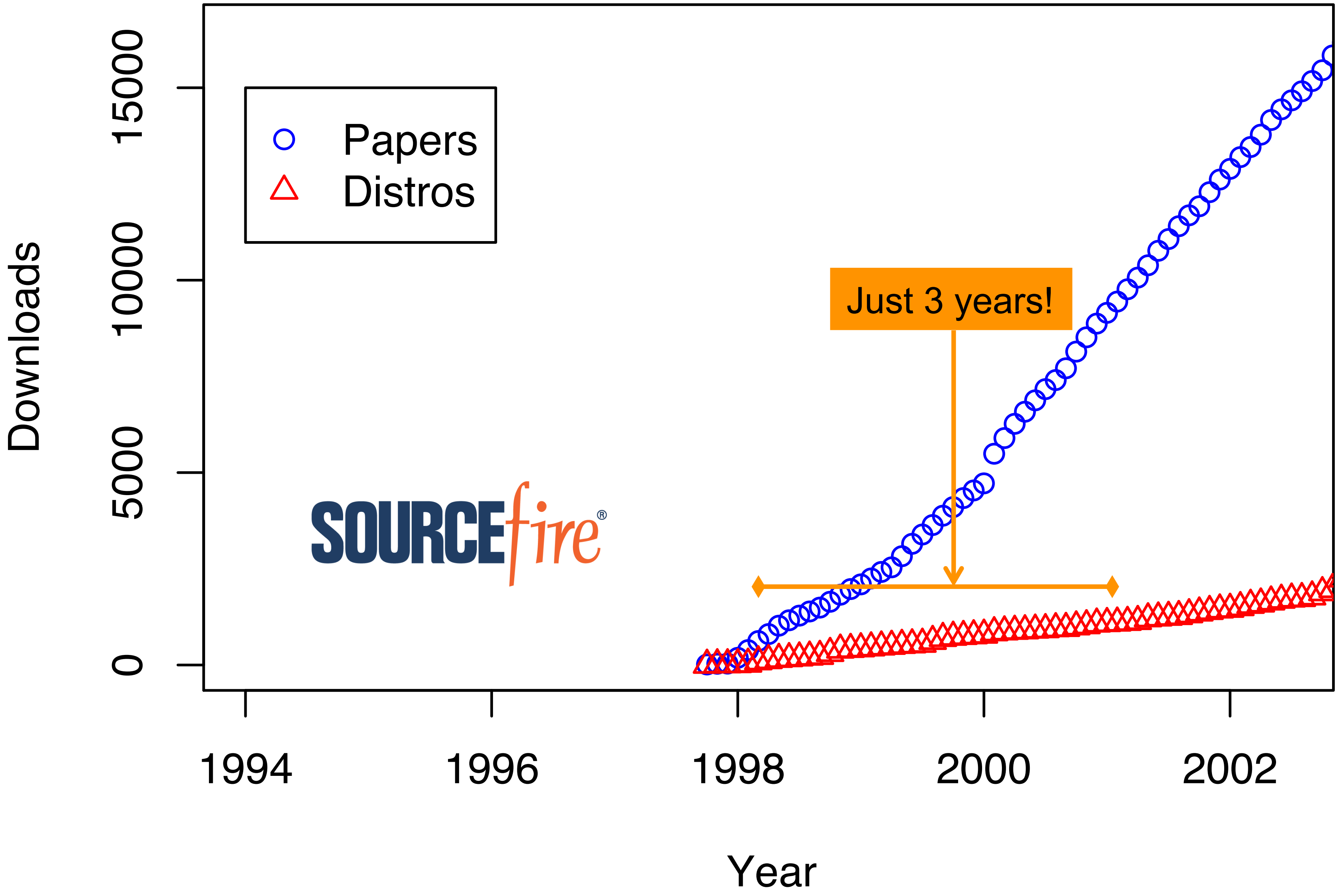
Snort paper appears in USENIX Lisa

Interest in Bro



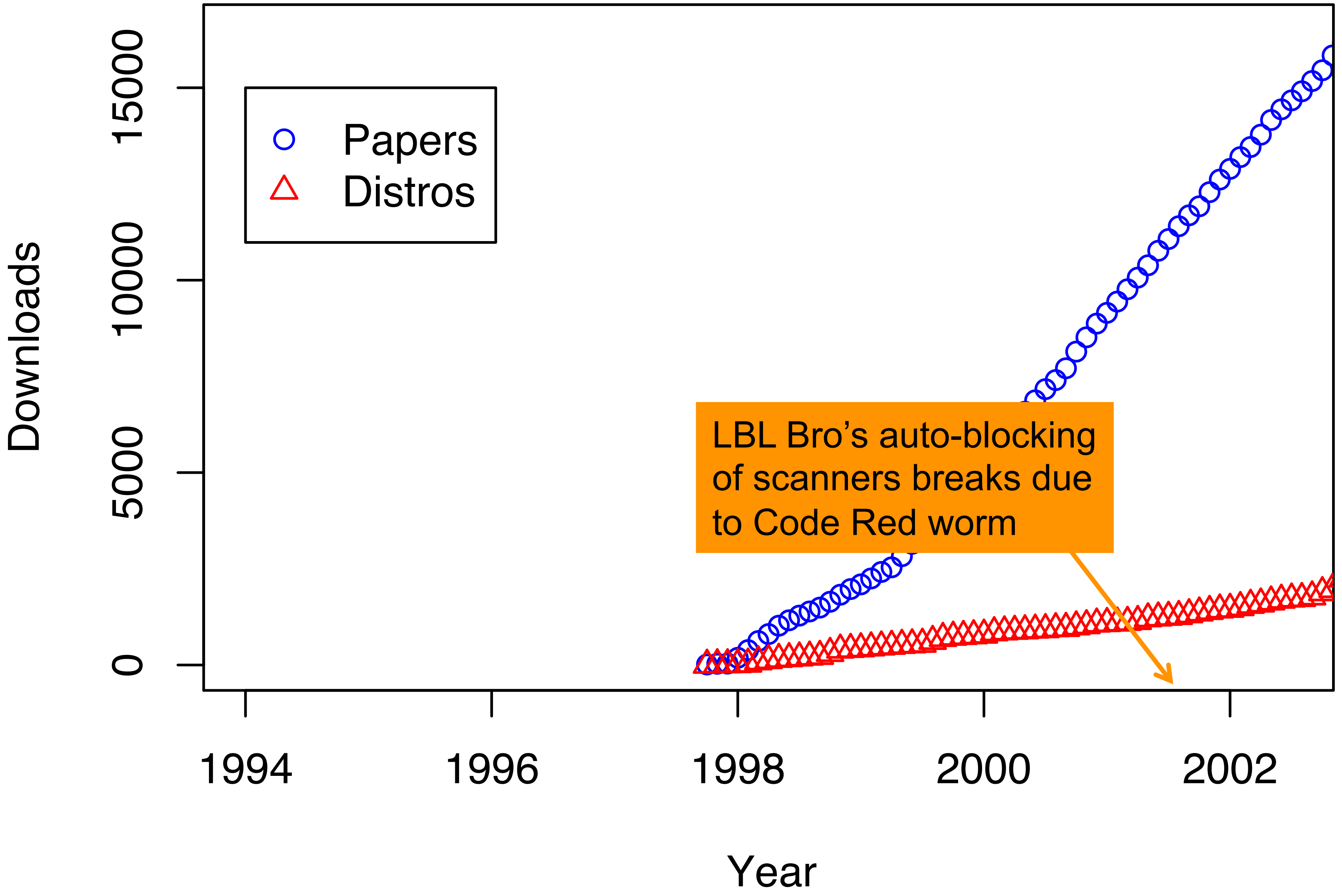
Sourcefire founded –
commercial support for Snort

Interest in Bro



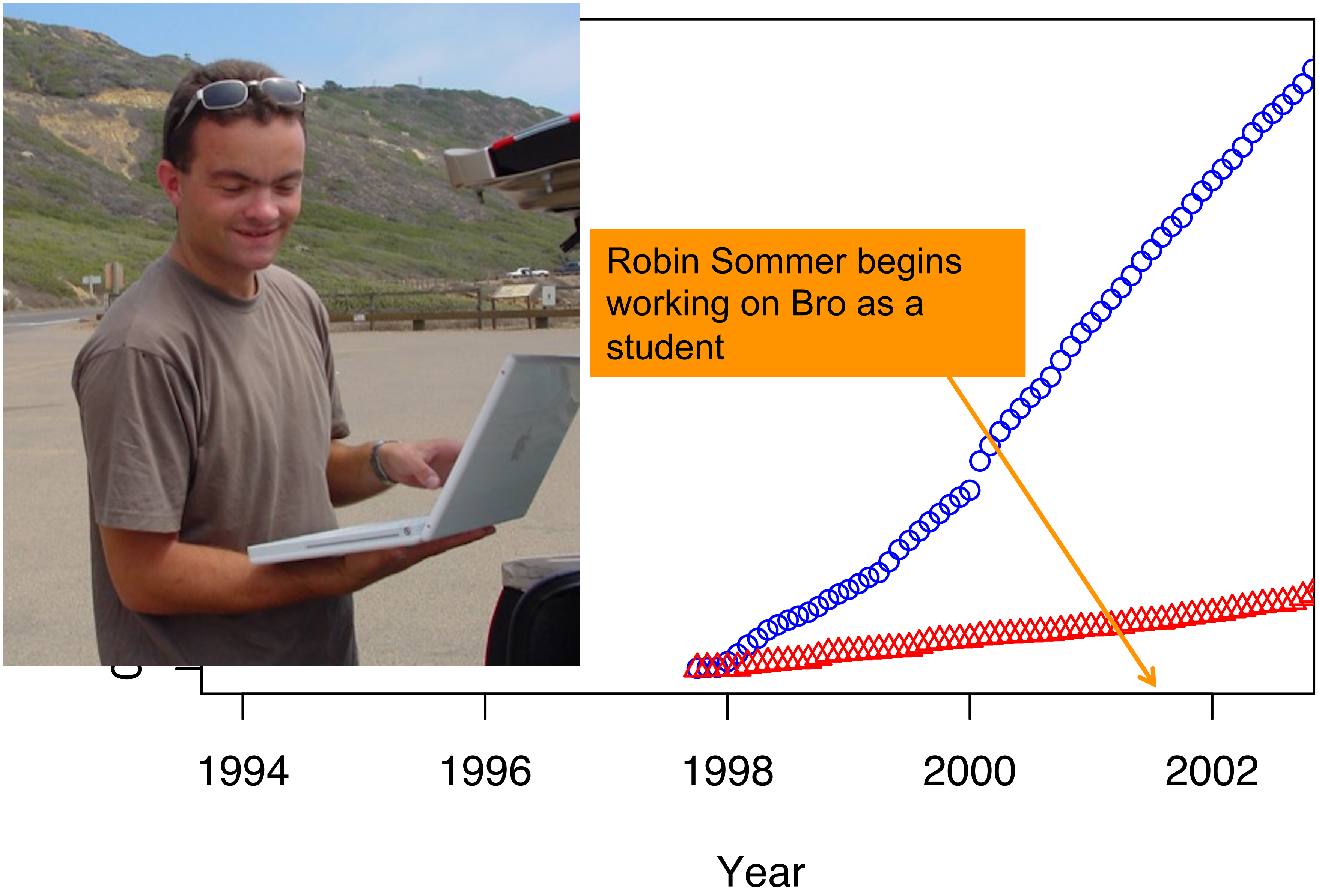
Just 3 years!

Interest in Bro



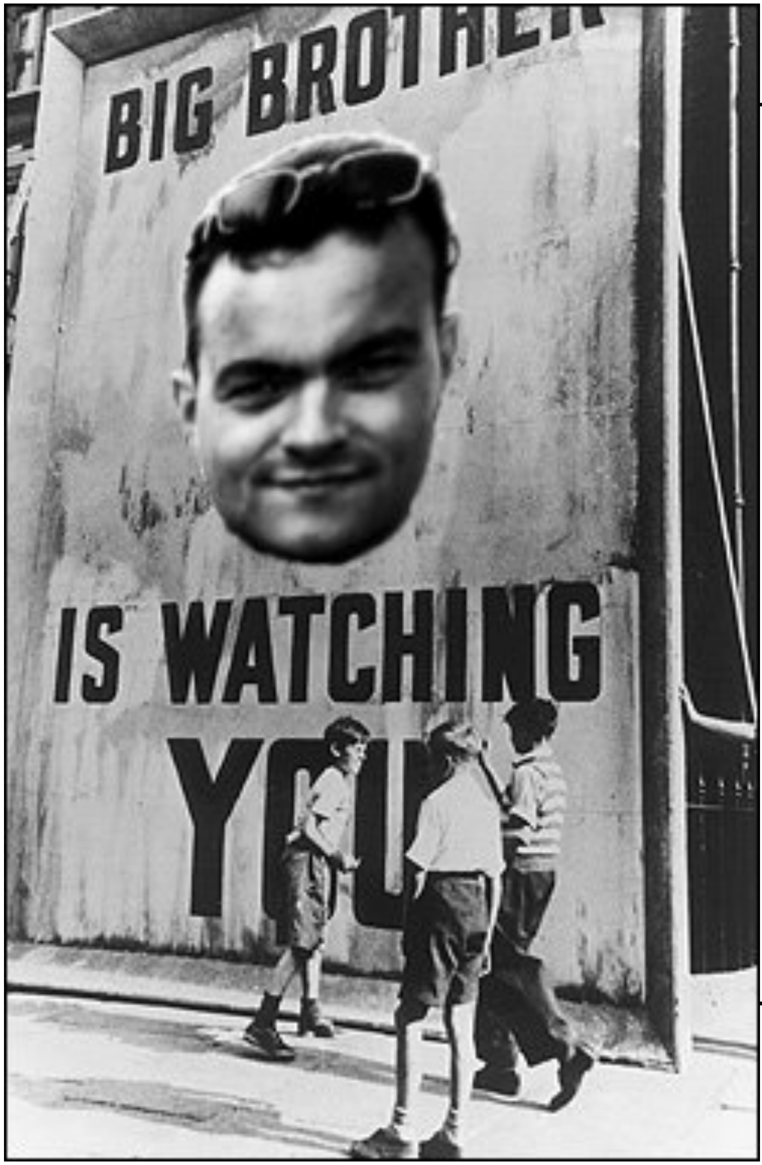
LBL Bro’s auto-blocking of scanners breaks due to Code Red worm

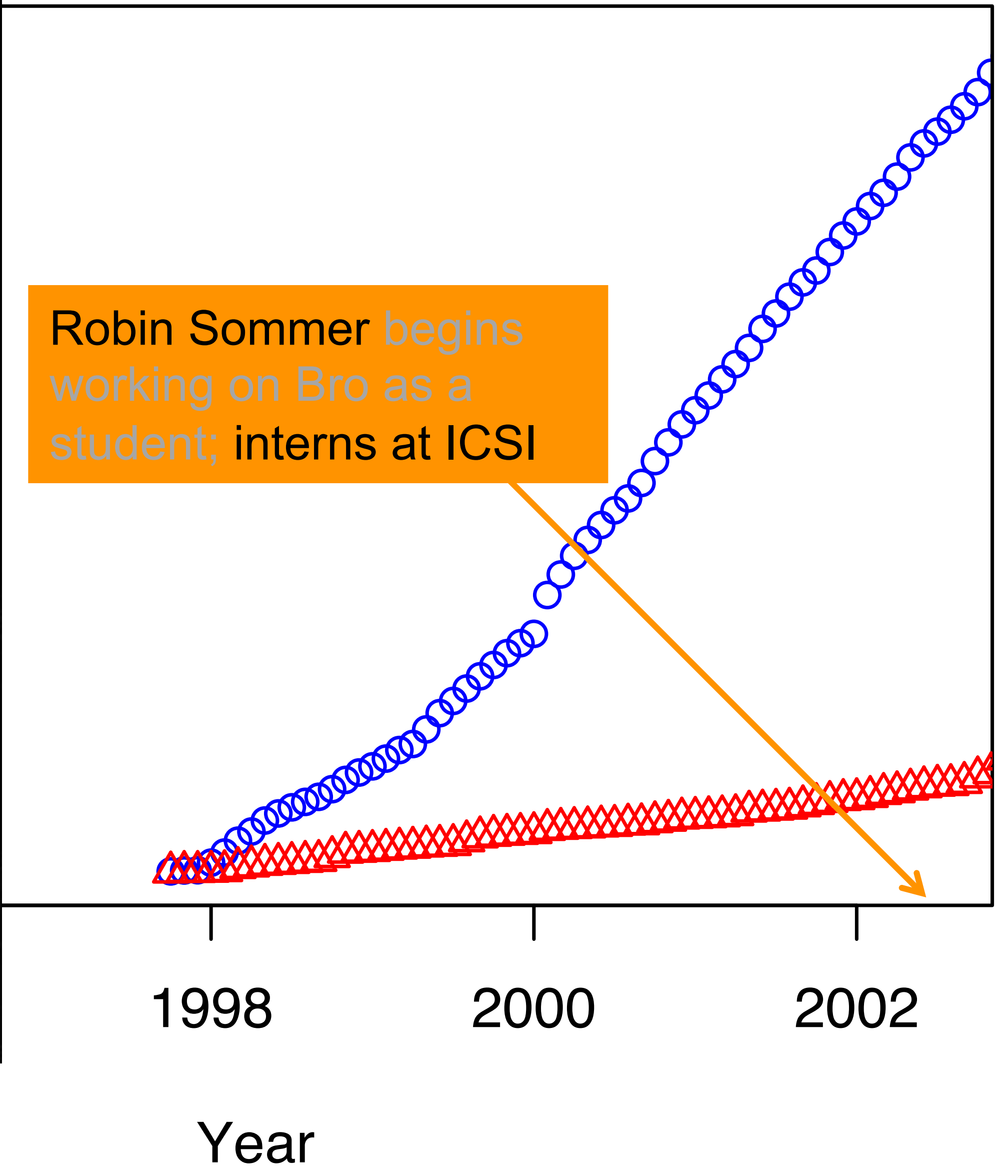
Interest in Bro



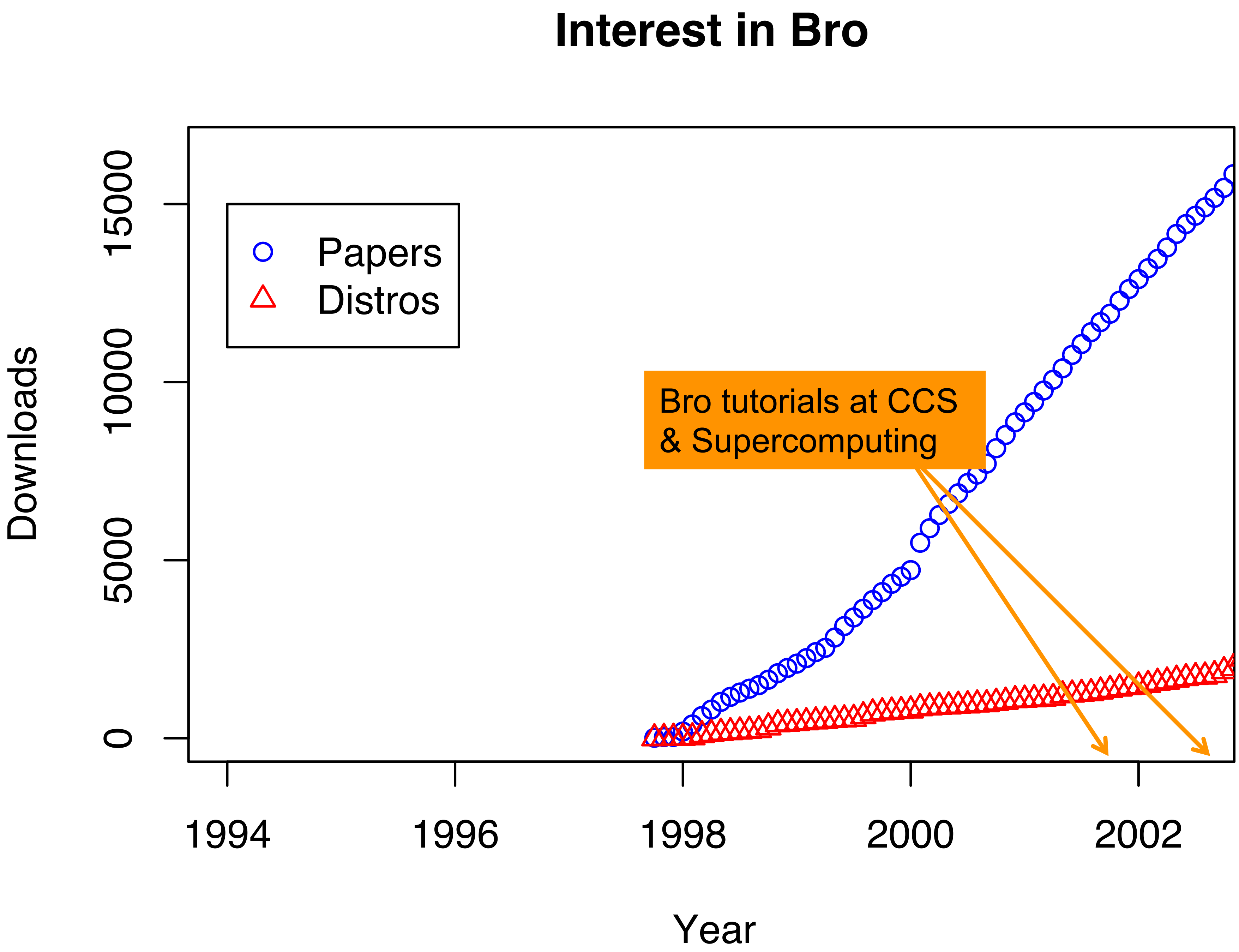
Robin Sommer begins working on Bro as a student

Interest in Bro





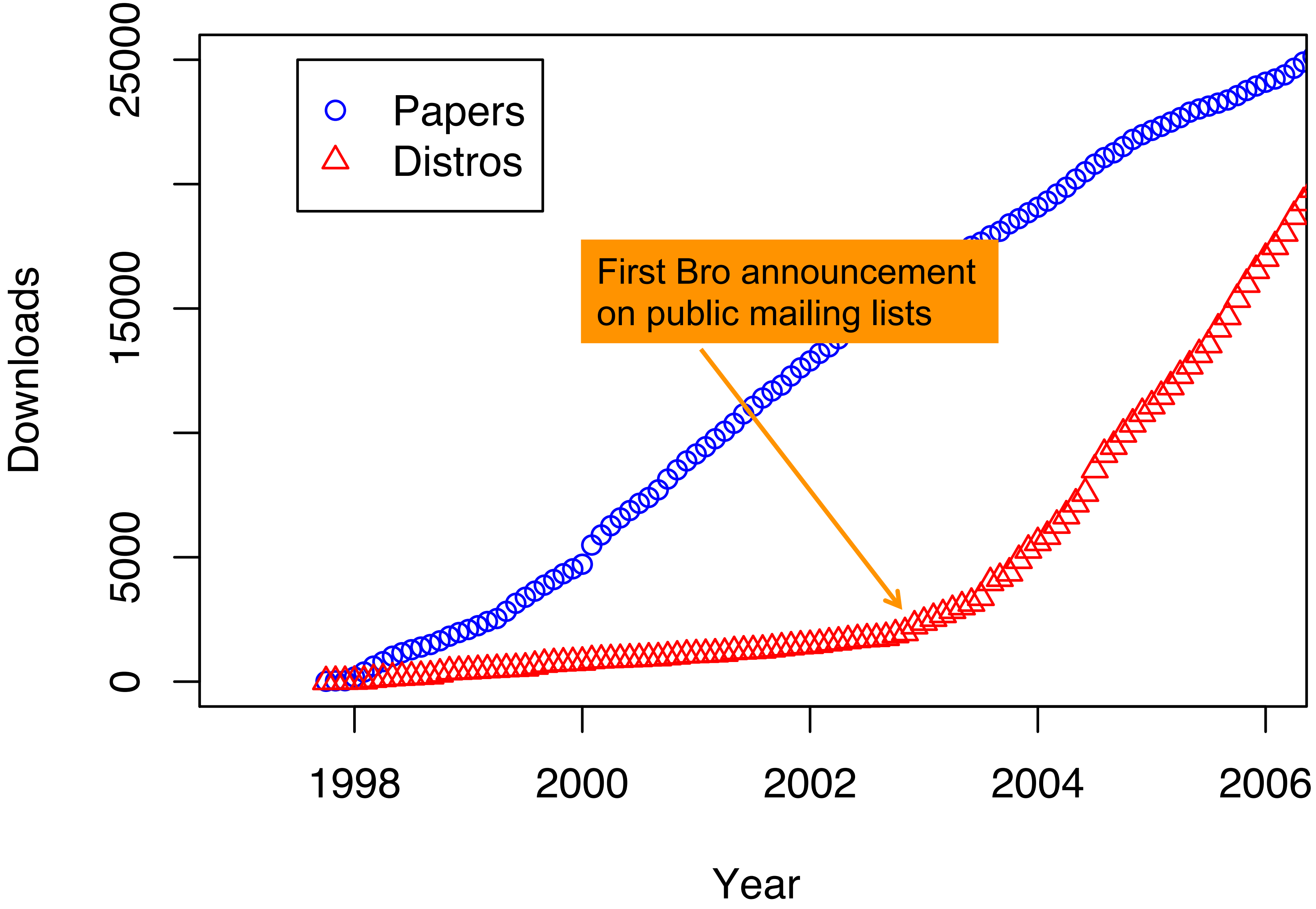
Robin Sommer begins working on Bro as a student; interns at ICSI



Interest in Bro

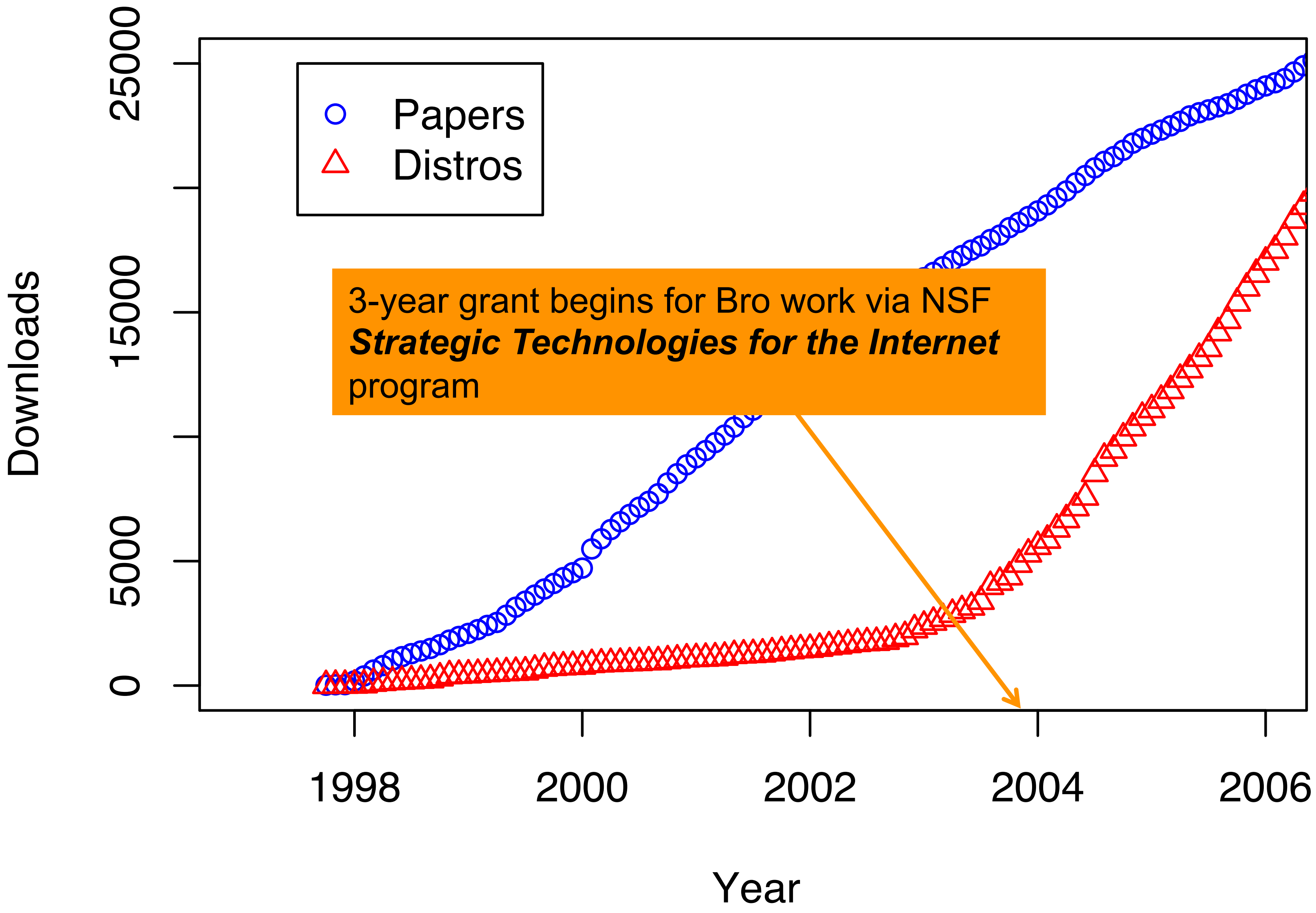
Bro tutorials at CCS & Supercomputing

Interest in Bro

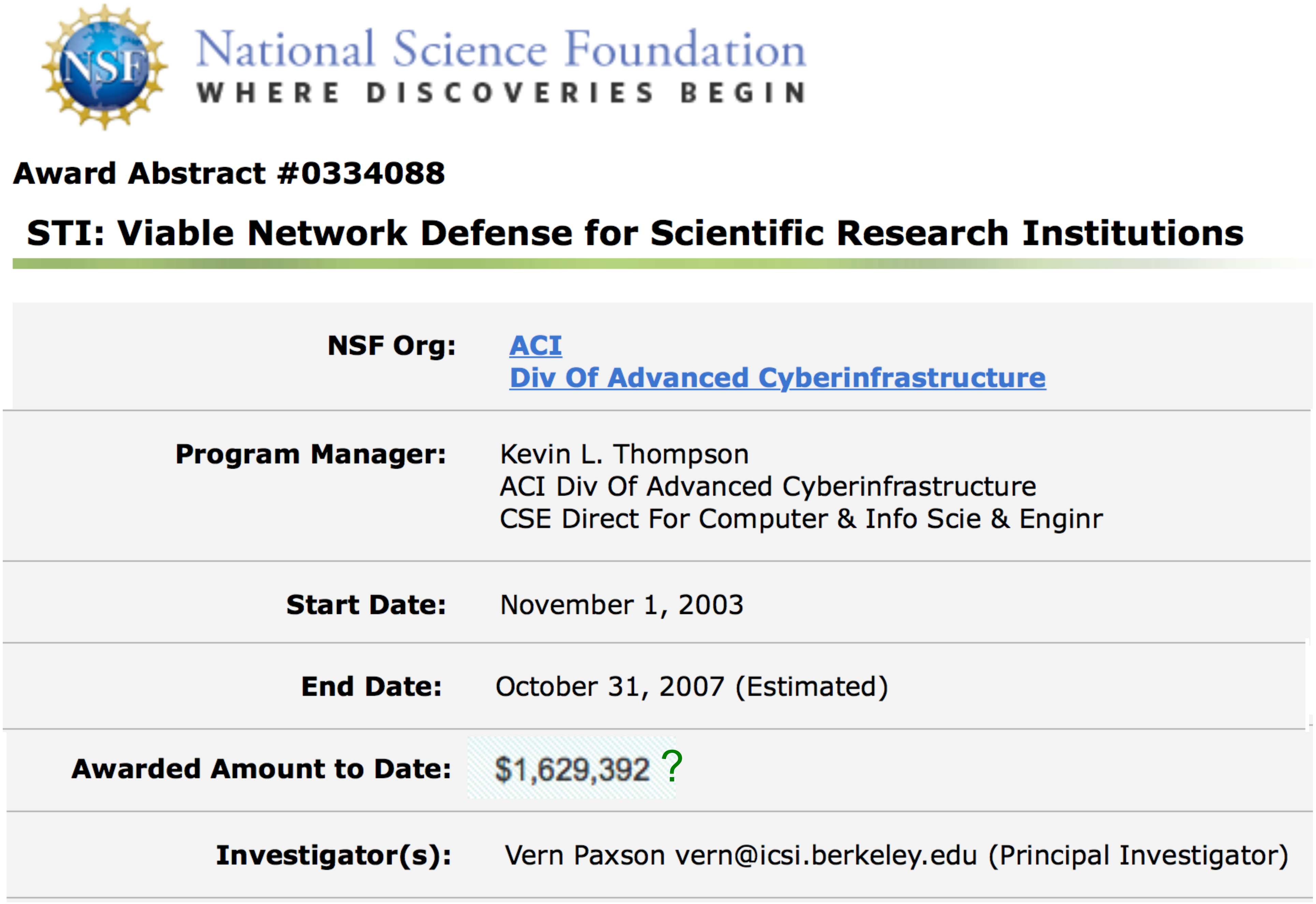


First Bro announcement on public mailing lists

Interest in Bro



3-year grant begins for Bro work via NSF ***Strategic Technologies for the Internet*** program

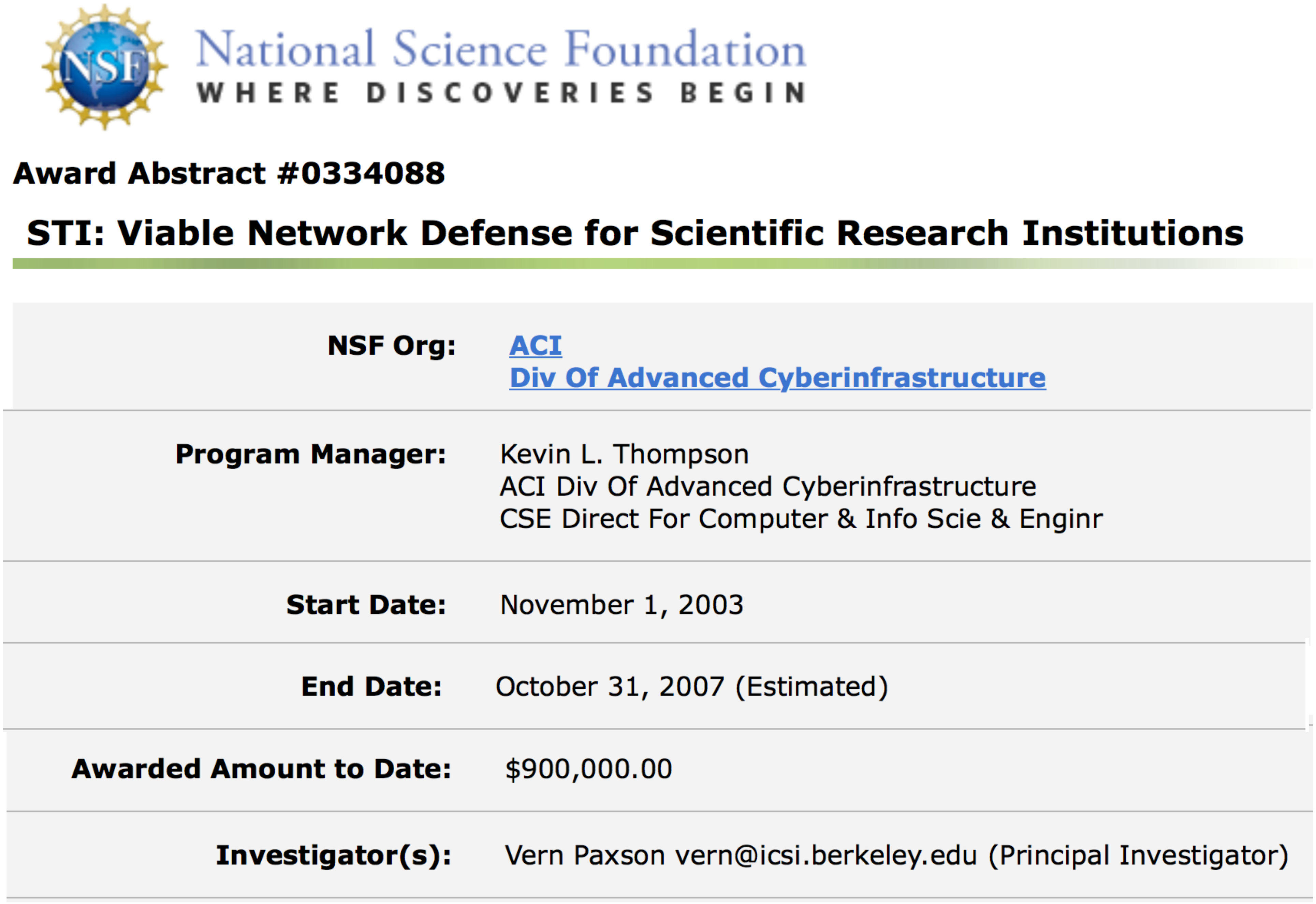


National Science Foundation
WHERE DISCOVERIES BEGIN

Award Abstract #0334088

STI: Viable Network Defense for Scientific Research Institutions

NSF Org:	ACI Div Of Advanced Cyberinfrastructure
Program Manager:	Kevin L. Thompson ACI Div Of Advanced Cyberinfrastructure CSE Direct For Computer & Info Scie & Enginr
Start Date:	November 1, 2003
End Date:	October 31, 2007 (Estimated)
Awarded Amount to Date:	$1,629,392 ?
Investigator(s):	Vern Paxson vern@icsi.berkeley.edu (Principal Investigator)

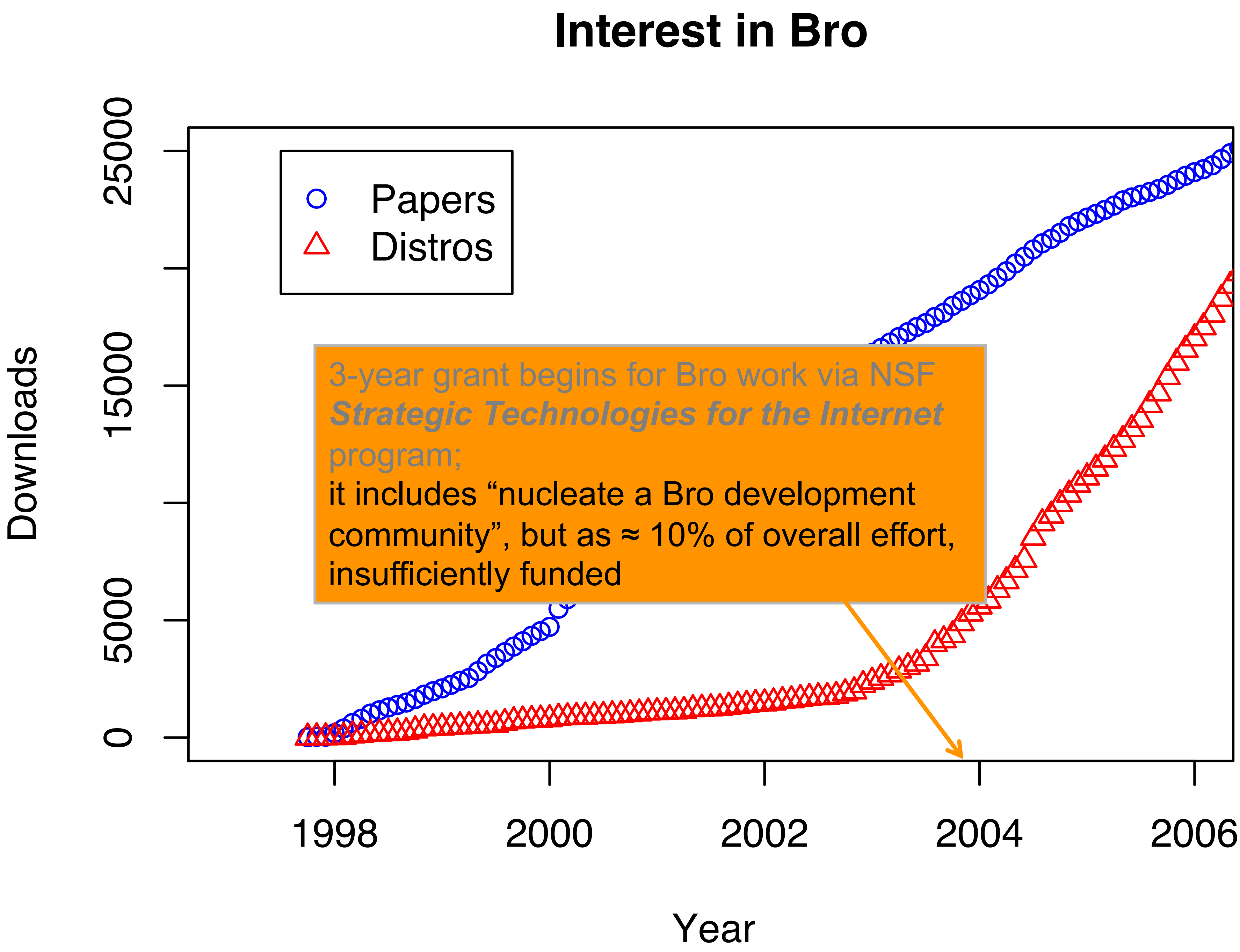


National Science Foundation
WHERE DISCOVERIES BEGIN

Award Abstract #0334088

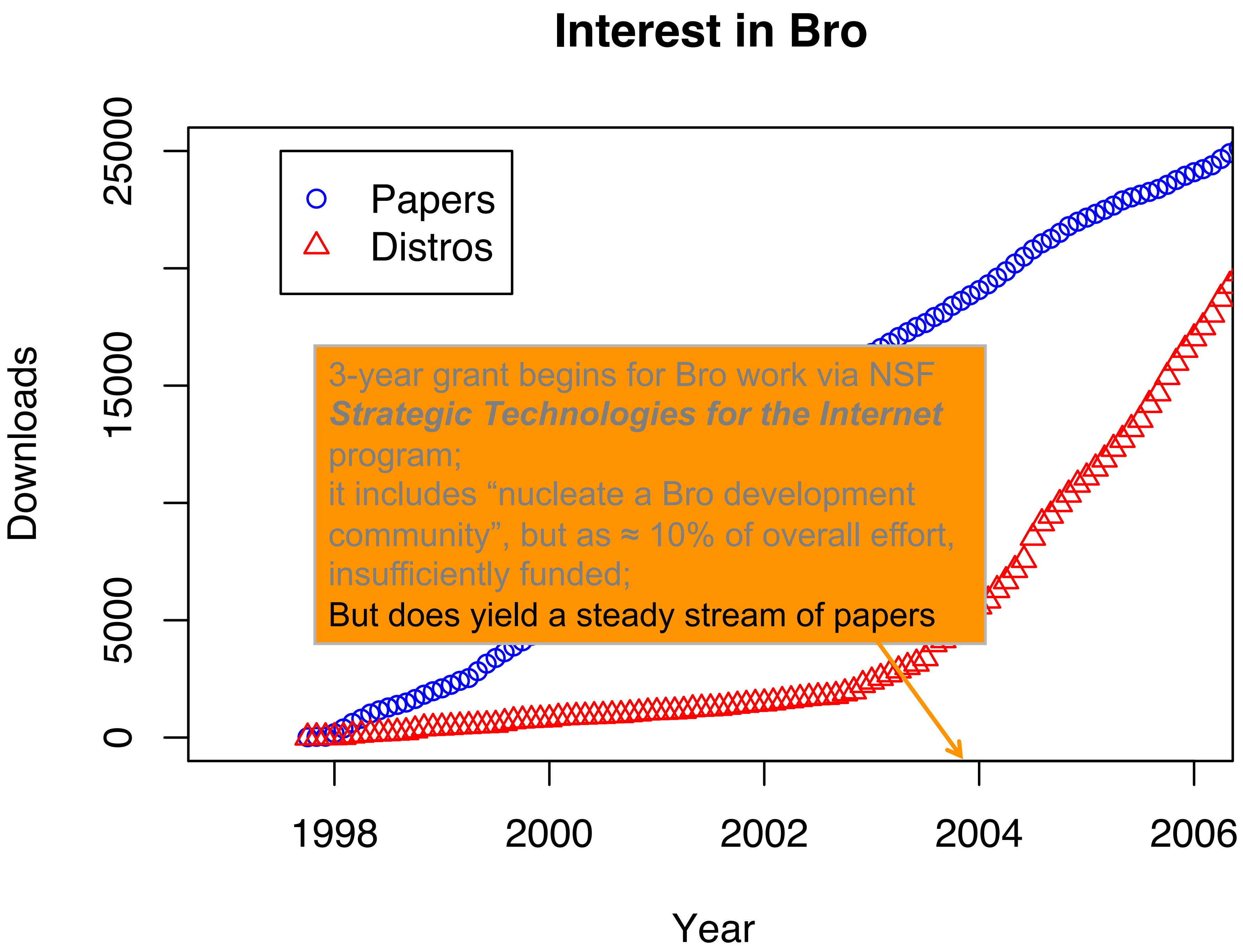
STI: Viable Network Defense for Scientific Research Institutions

NSF Org:	ACI Div Of Advanced Cyberinfrastructure
Program Manager:	Kevin L. Thompson ACI Div Of Advanced Cyberinfrastructure CSE Direct For Computer & Info Scie & Enginr
Start Date:	November 1, 2003
End Date:	October 31, 2007 (Estimated)
Awarded Amount to Date:	$900,000.00
Investigator(s):	Vern Paxson vern@icsi.berkeley.edu (Principal Investigator)



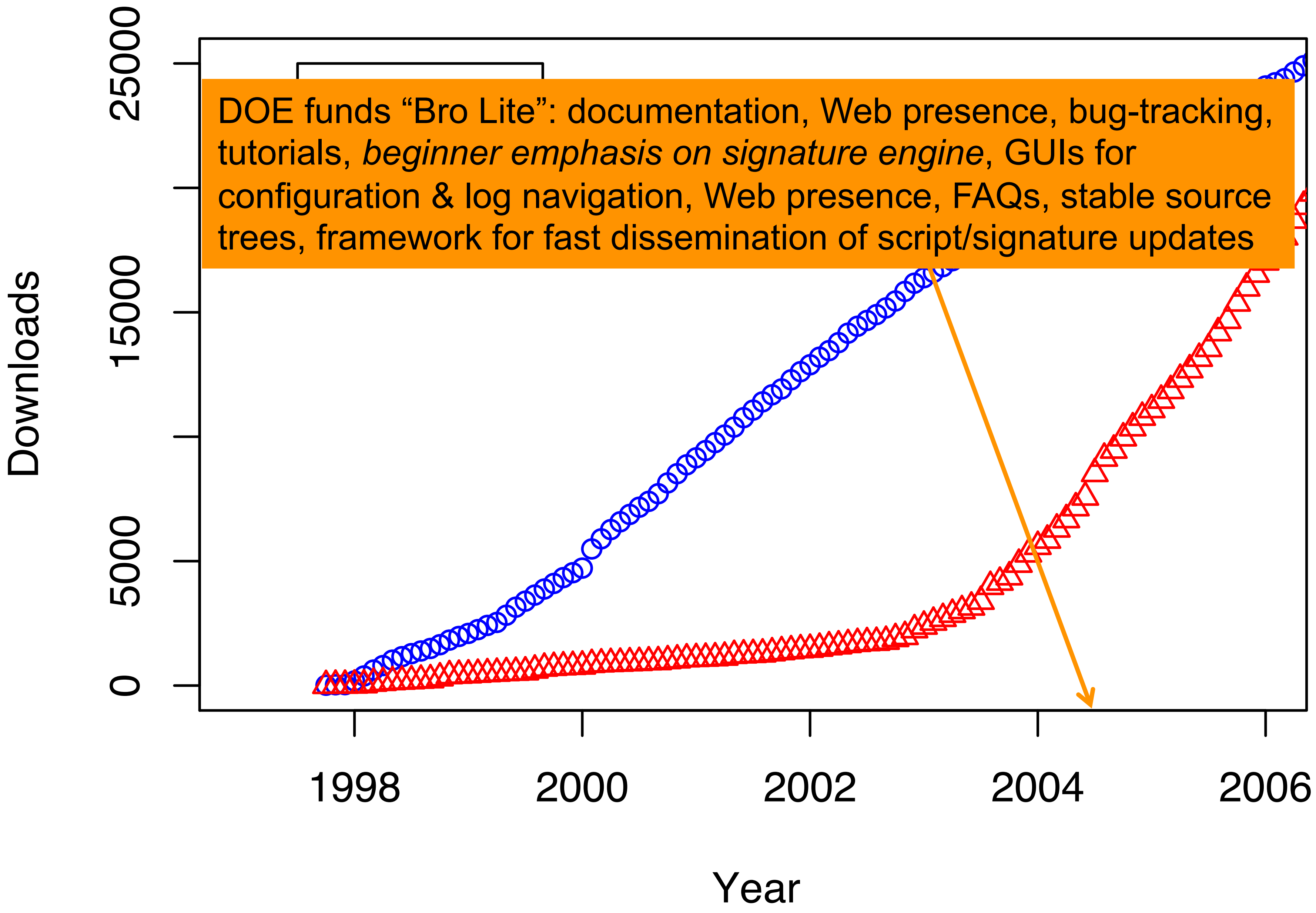
3-year grant begins for Bro work via NSF ***Strategic Technologies for the Internet*** program;

it includes “nucleate a Bro development community”, but as ≈ 10% of overall effort, insufficiently funded

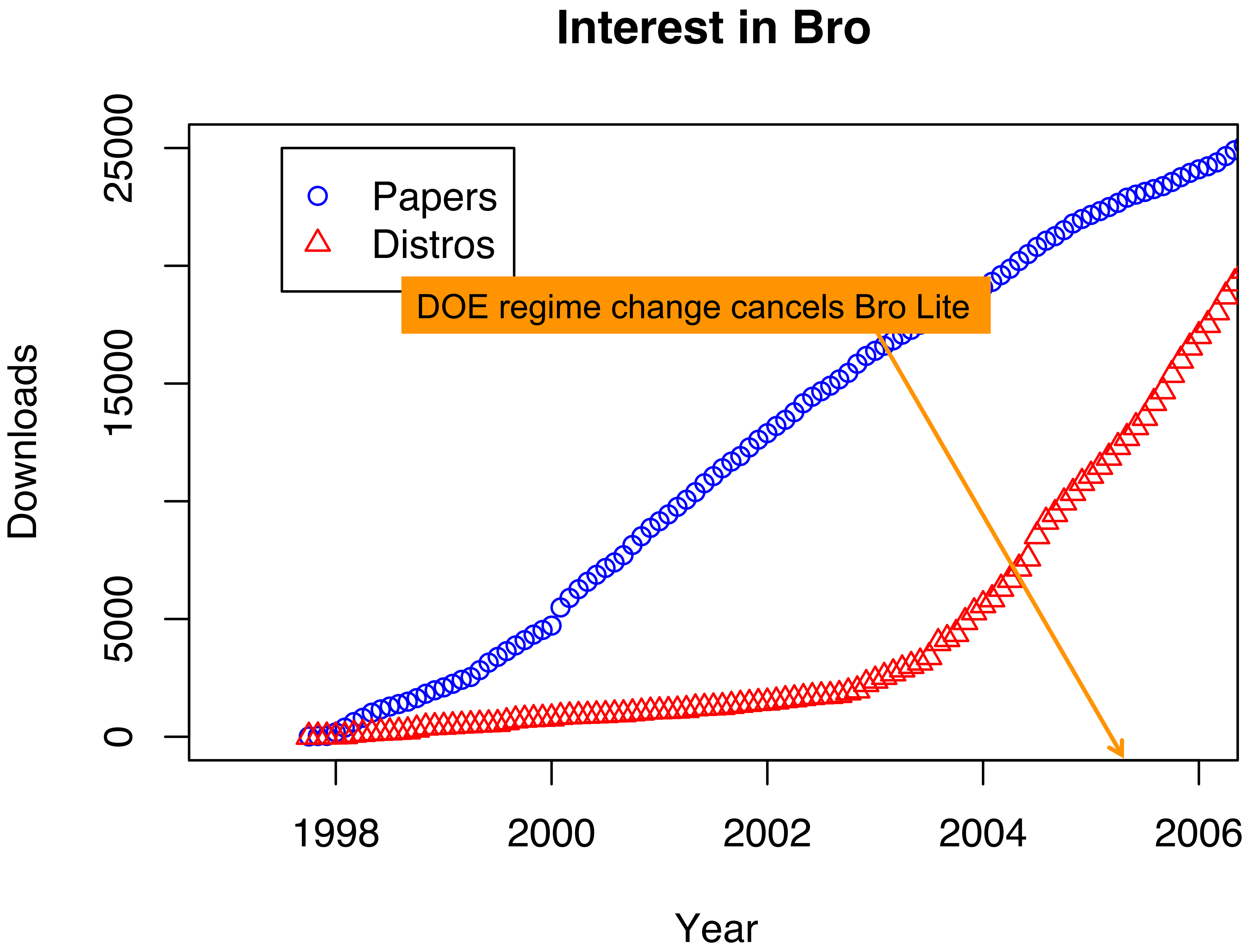


3-year grant begins for Bro work via NSF ***Strategic Technologies for the Internet*** program;
it includes "nucleate a Bro development community", but as ≈ 10% of overall effort, insufficiently funded;
But does yield a steady stream of papers

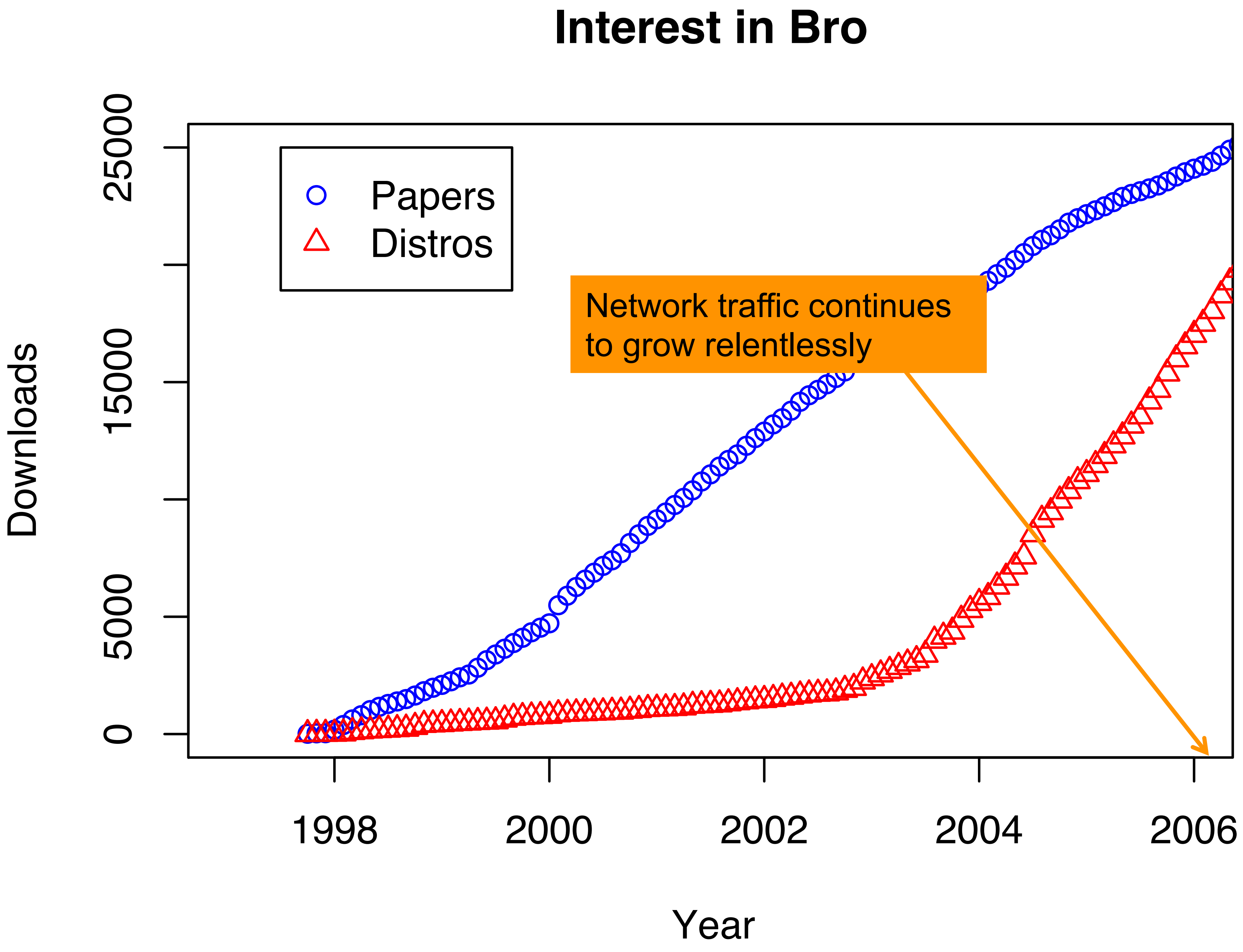
Interest in Bro



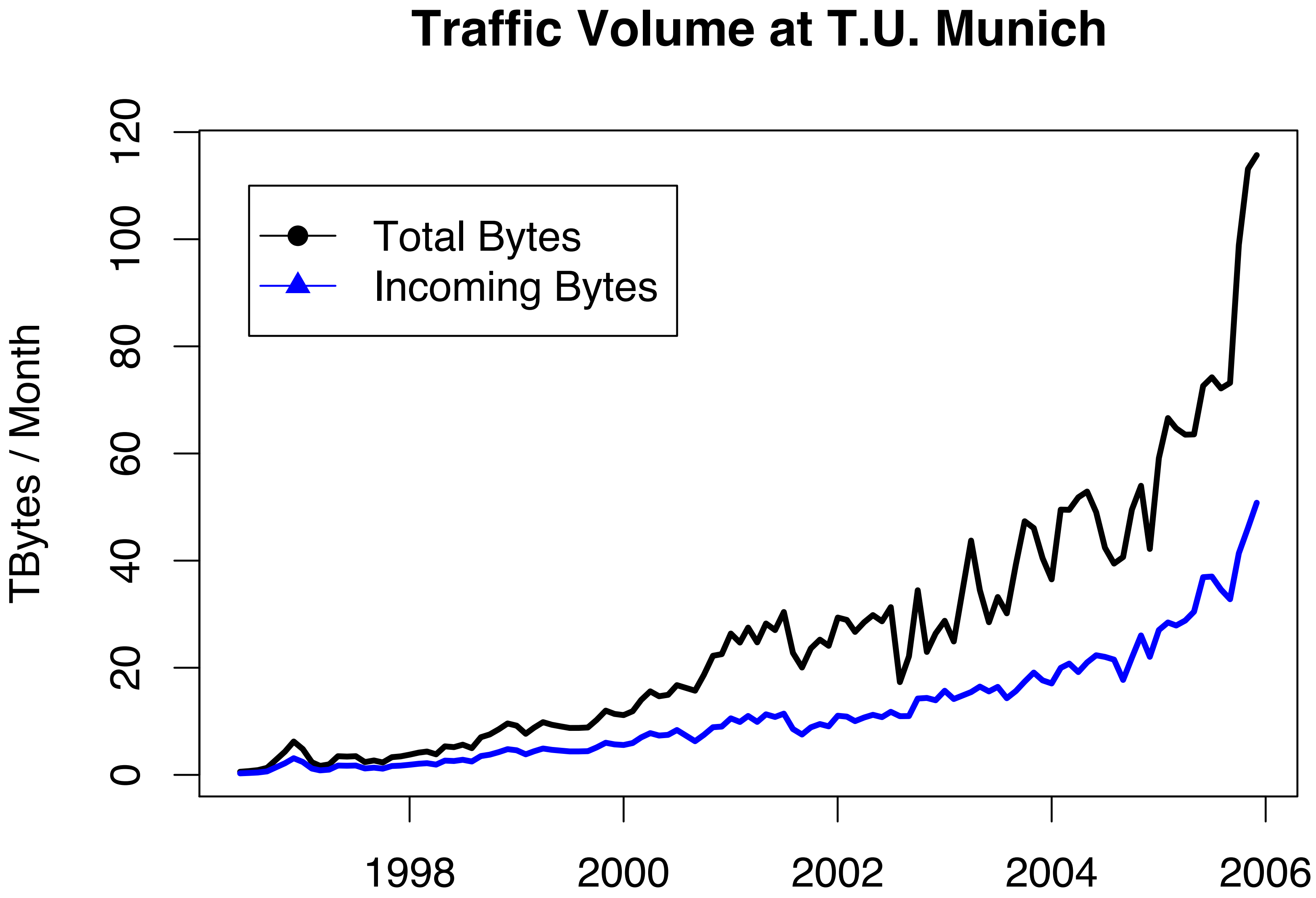
DOE funds “Bro Lite”: documentation, Web presence, bug-tracking, tutorials, *beginner emphasis on signature engine*, GUIs for configuration & log navigation, Web presence, FAQs, stable source trees, framework for fast dissemination of script/signature updates



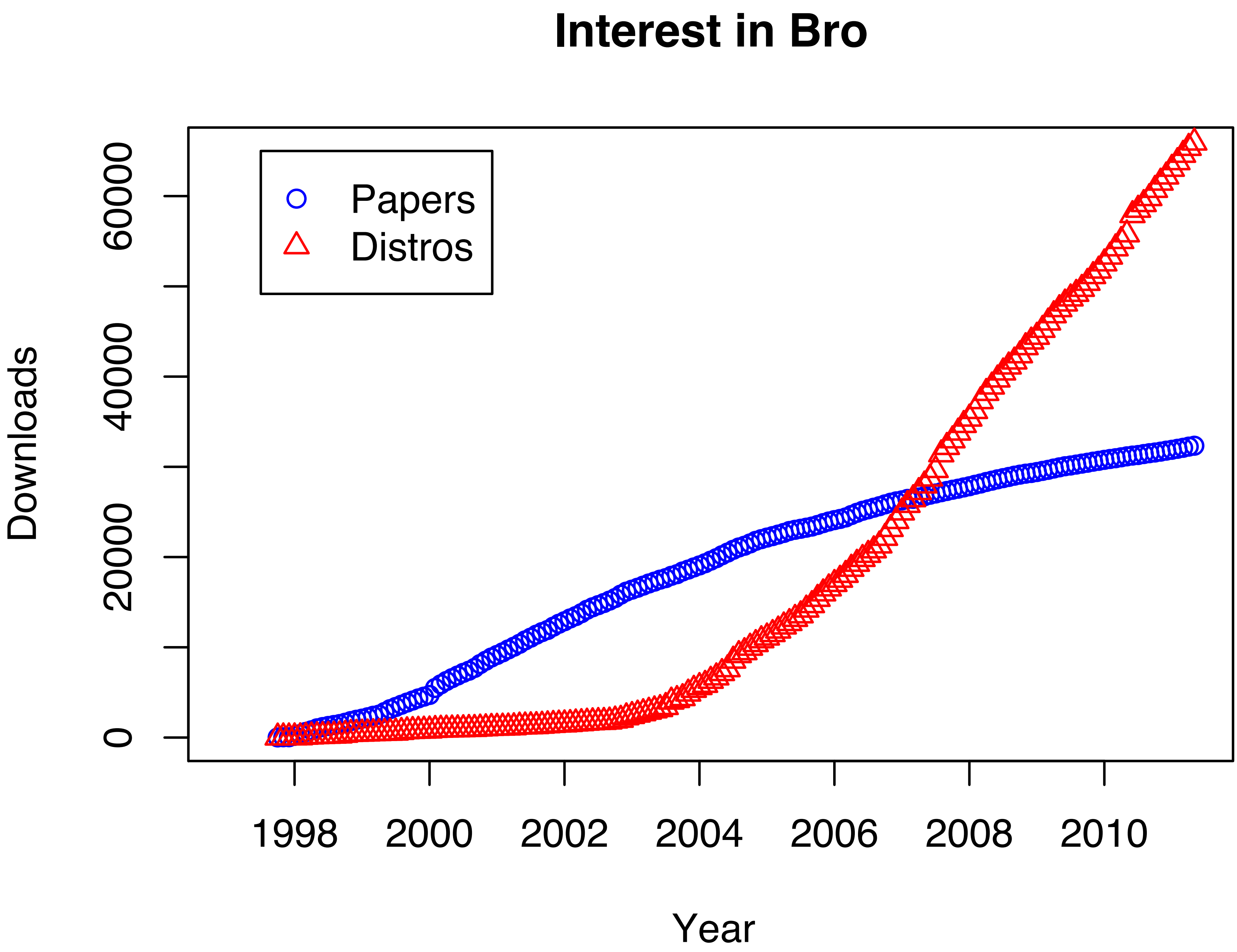
DOE regime change cancels Bro Lite

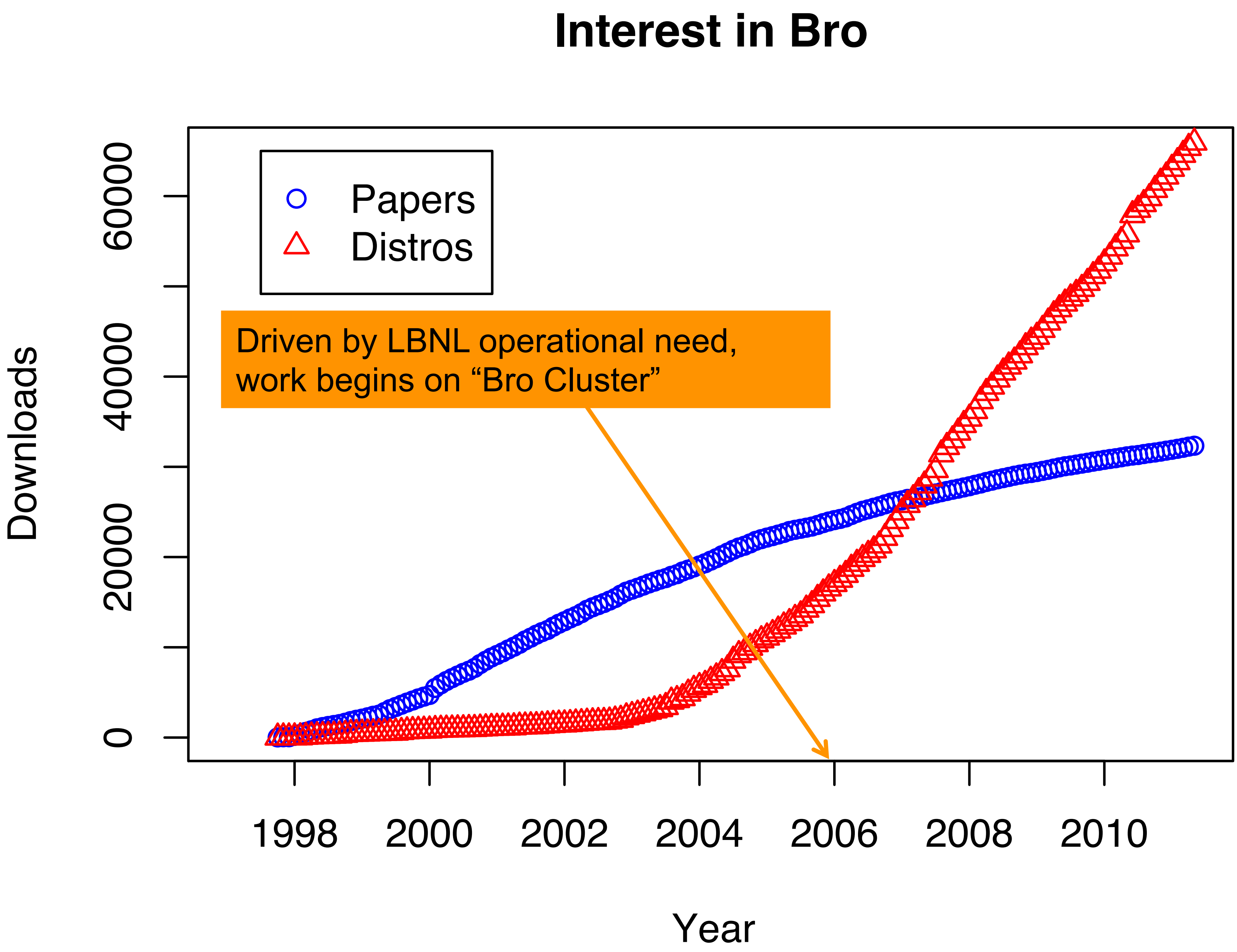


Network traffic continues
to grow relentlessly

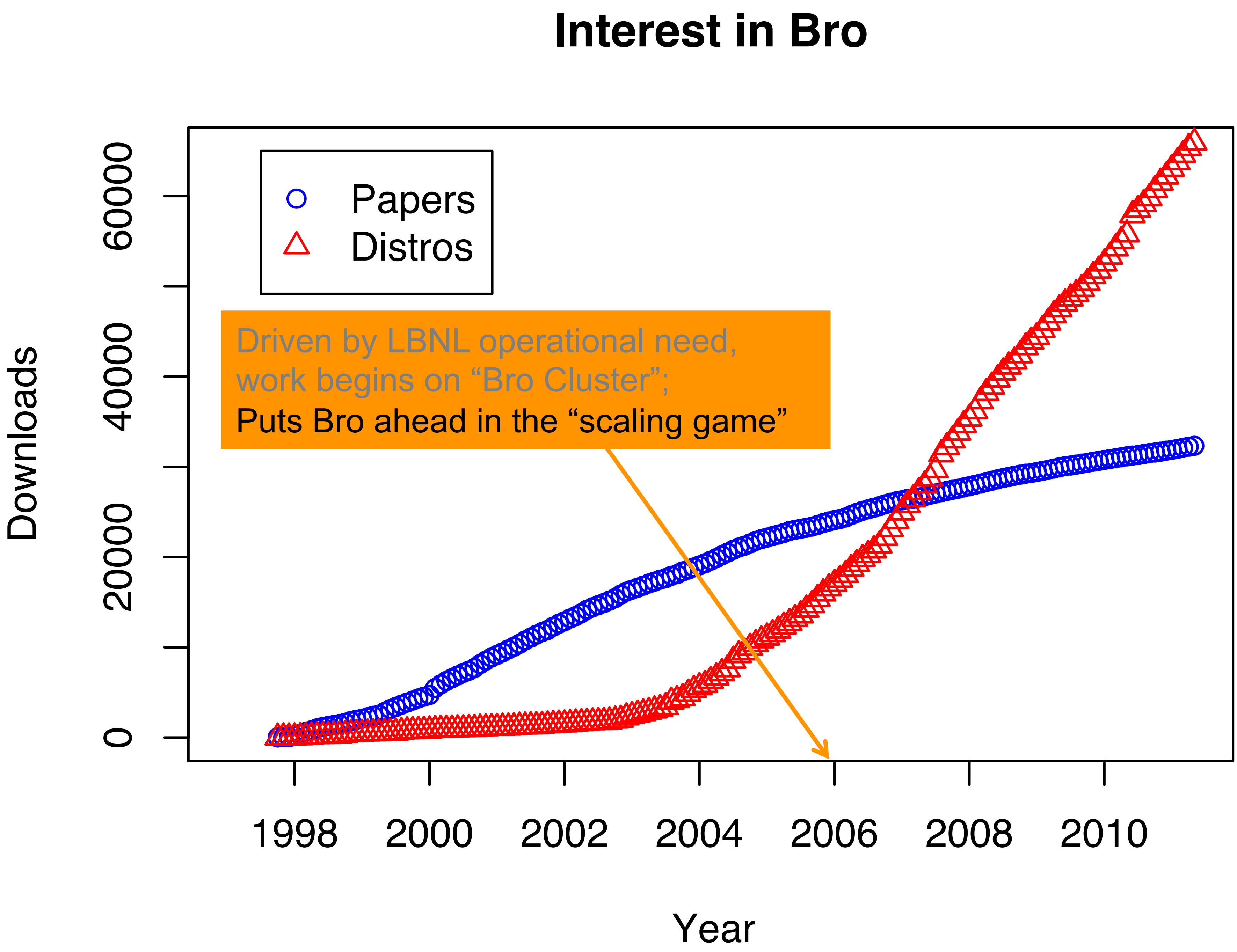


Traffic Volume at T.U. Munich

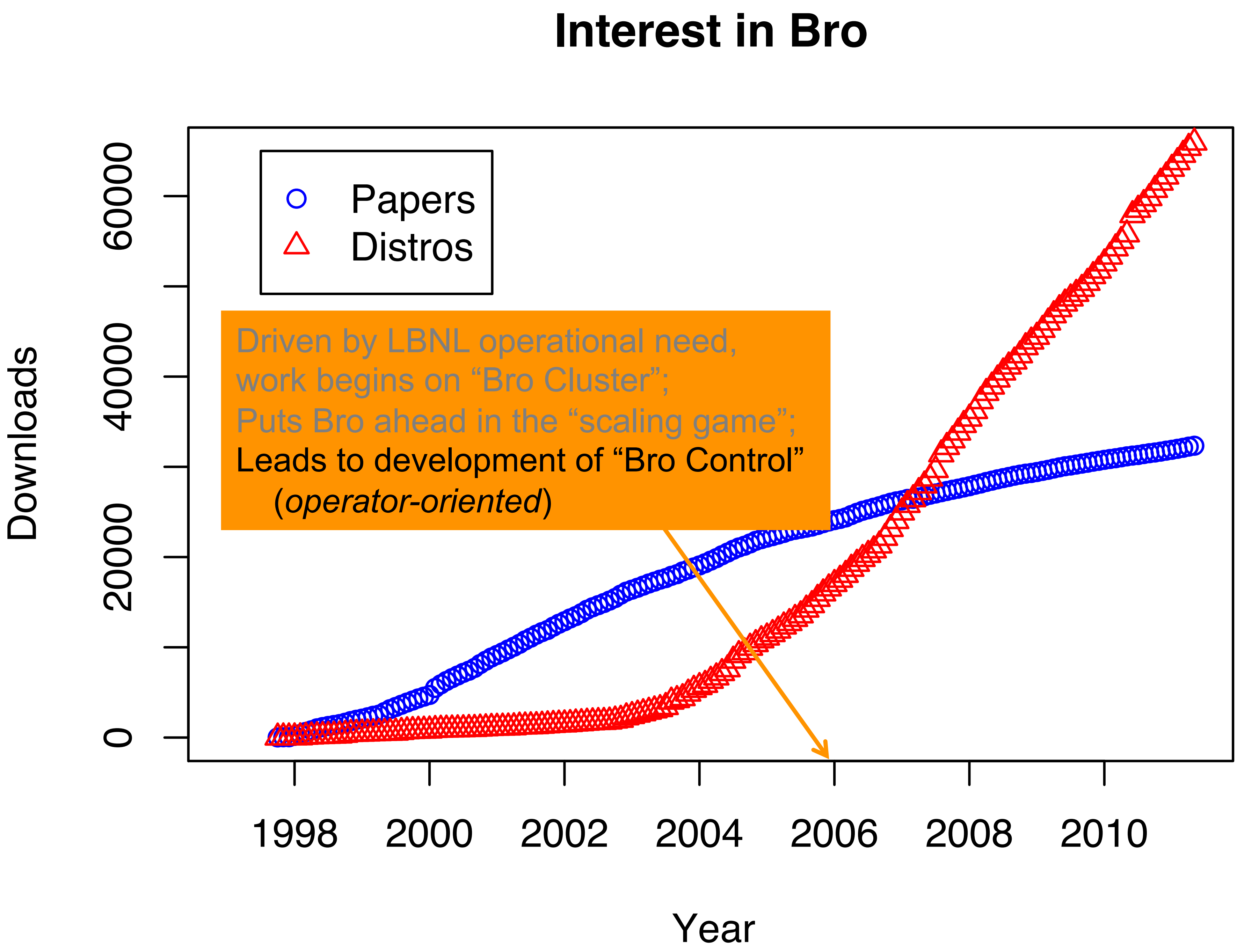

Interest in Bro
○ Papers
△ Distros
Downloads
0
20000
40000
60000
1998
2000
2002
2004
2006
2008
2010
Year



Driven by LBNL operational need, work begins on “Bro Cluster”

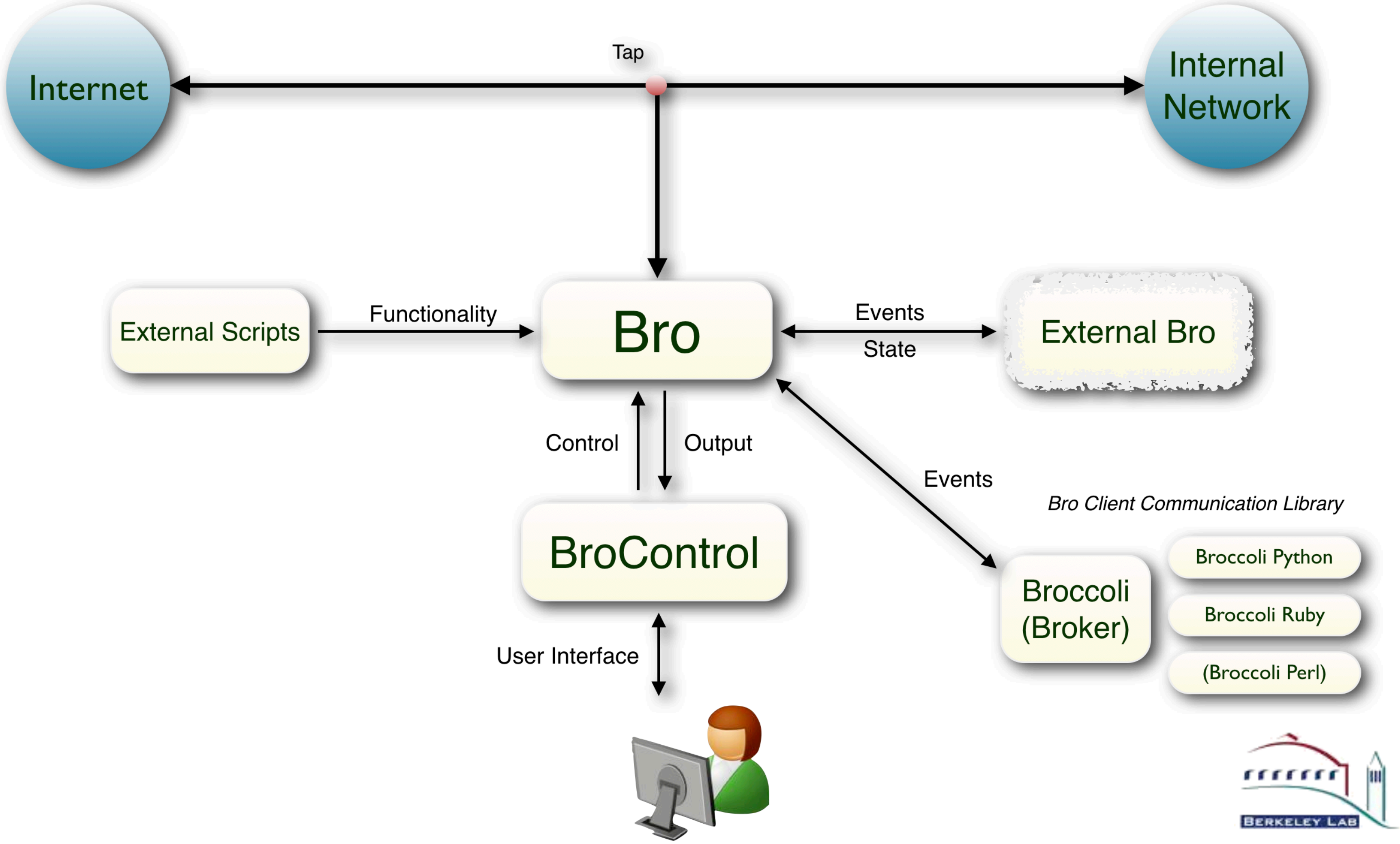


Driven by LBNL operational need,
work begins on “Bro Cluster”;
Puts Bro ahead in the “scaling game”



Driven by LBNL operational need,
work begins on “Bro Cluster”;
Puts Bro ahead in the “scaling game”;
Leads to development of “Bro Control”
(*operator-oriented*)

Bro *Cluster* Ecosystem



Internet

Tap

Internal Network

External Scripts

Functionality

Bro

Events

State

External Bro

Control

Output

Events

Bro Client Communication Library

BroControl

Broccoli (Broker)

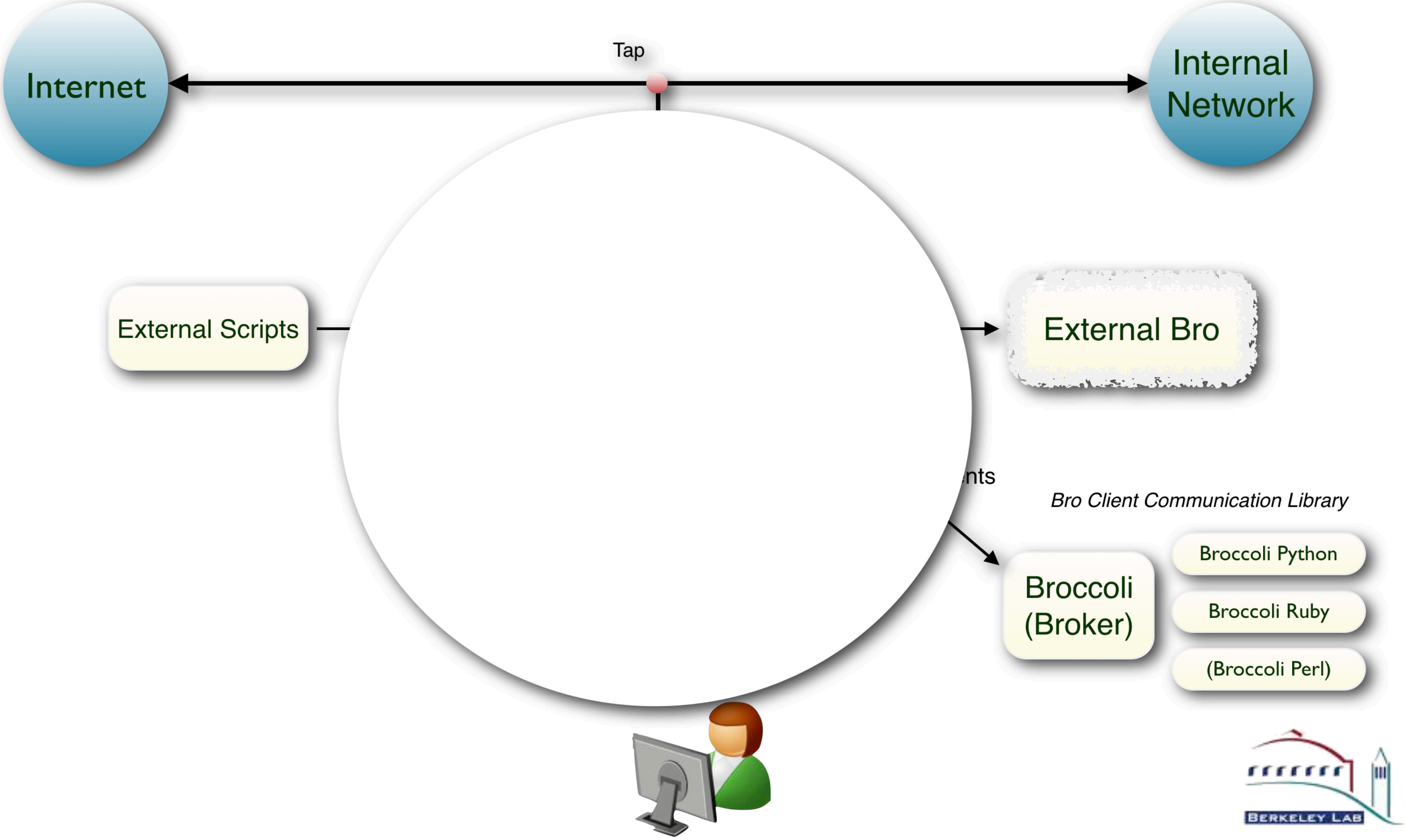
Broccoli Python

Broccoli Ruby

(Broccoli Perl)

User Interface

Bro *Cluster* Ecosystem



Internet

Tap

Internal Network

External Scripts

External Bro

nts

Bro Client Communication Library

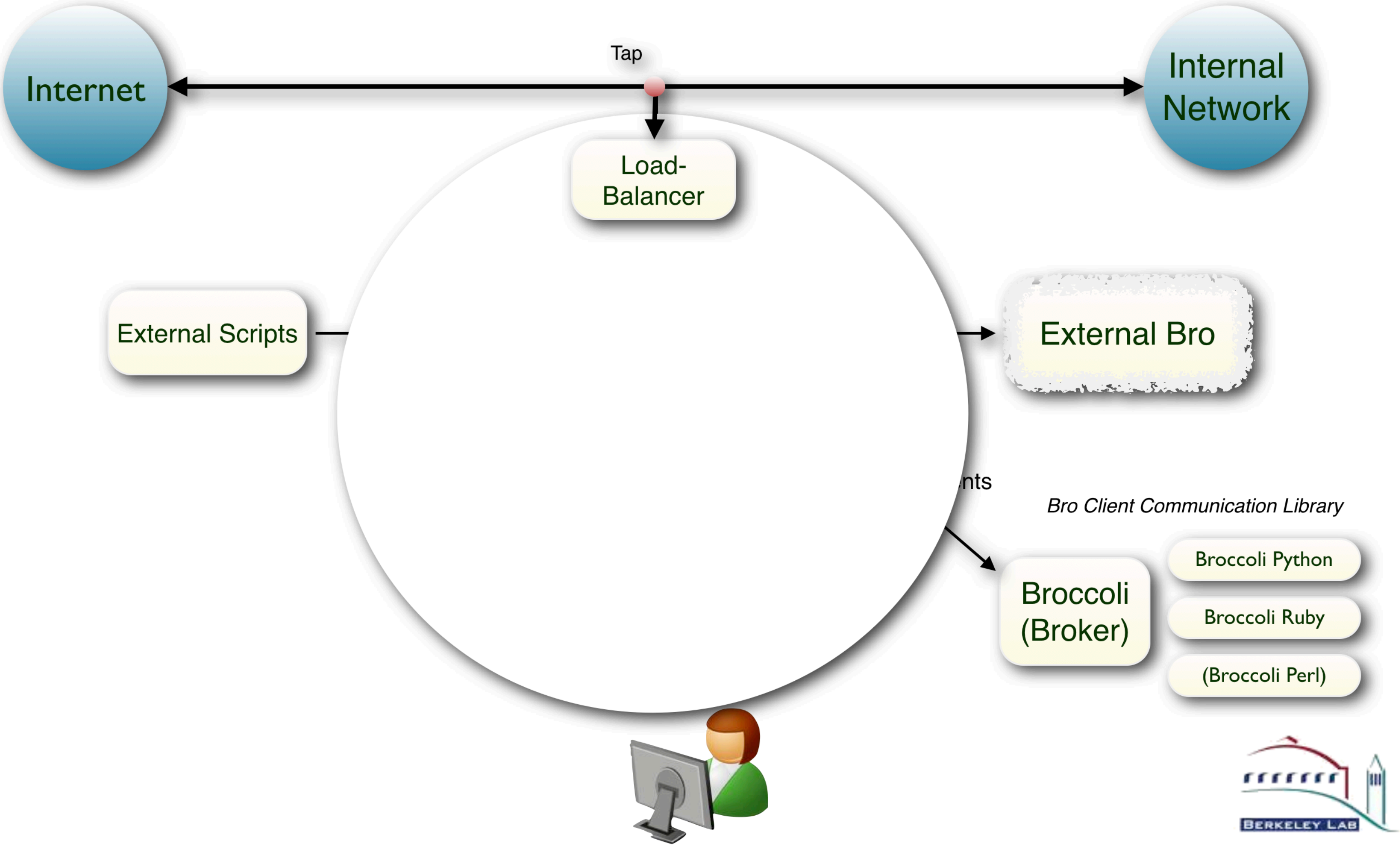
Broccoli (Broker)

Broccoli Python

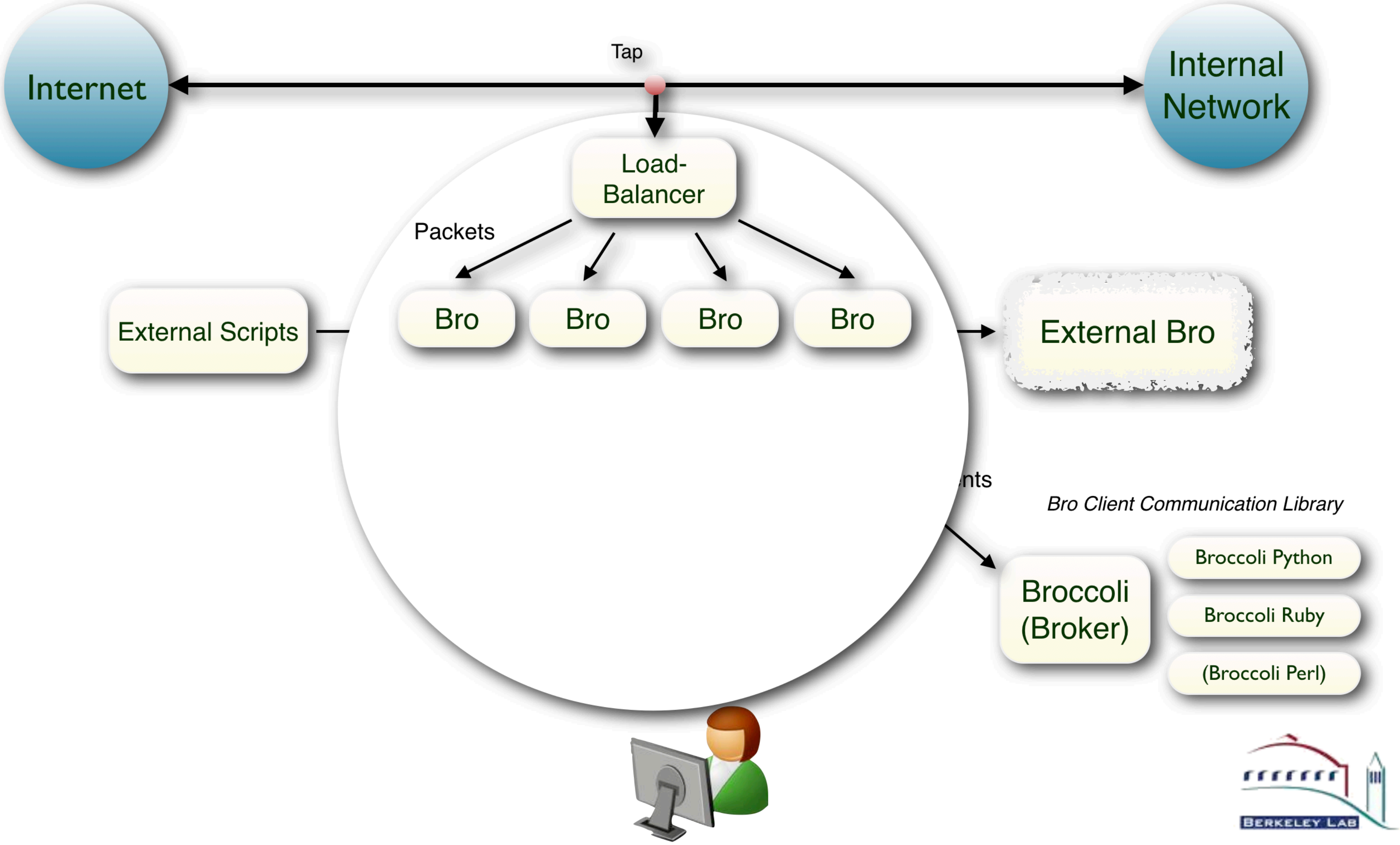
Broccoli Ruby

(Broccoli Perl)

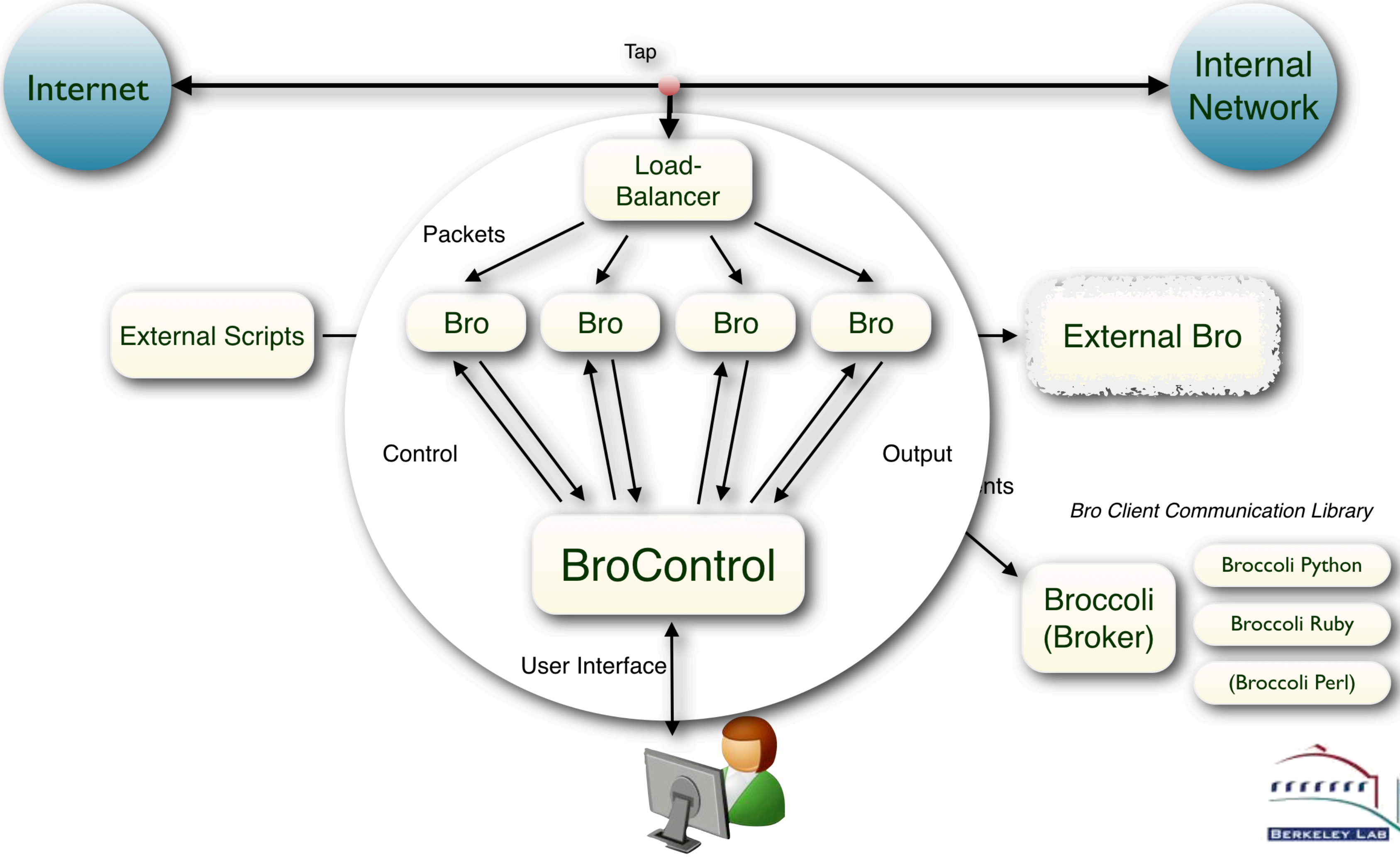
Bro *Cluster* Ecosystem



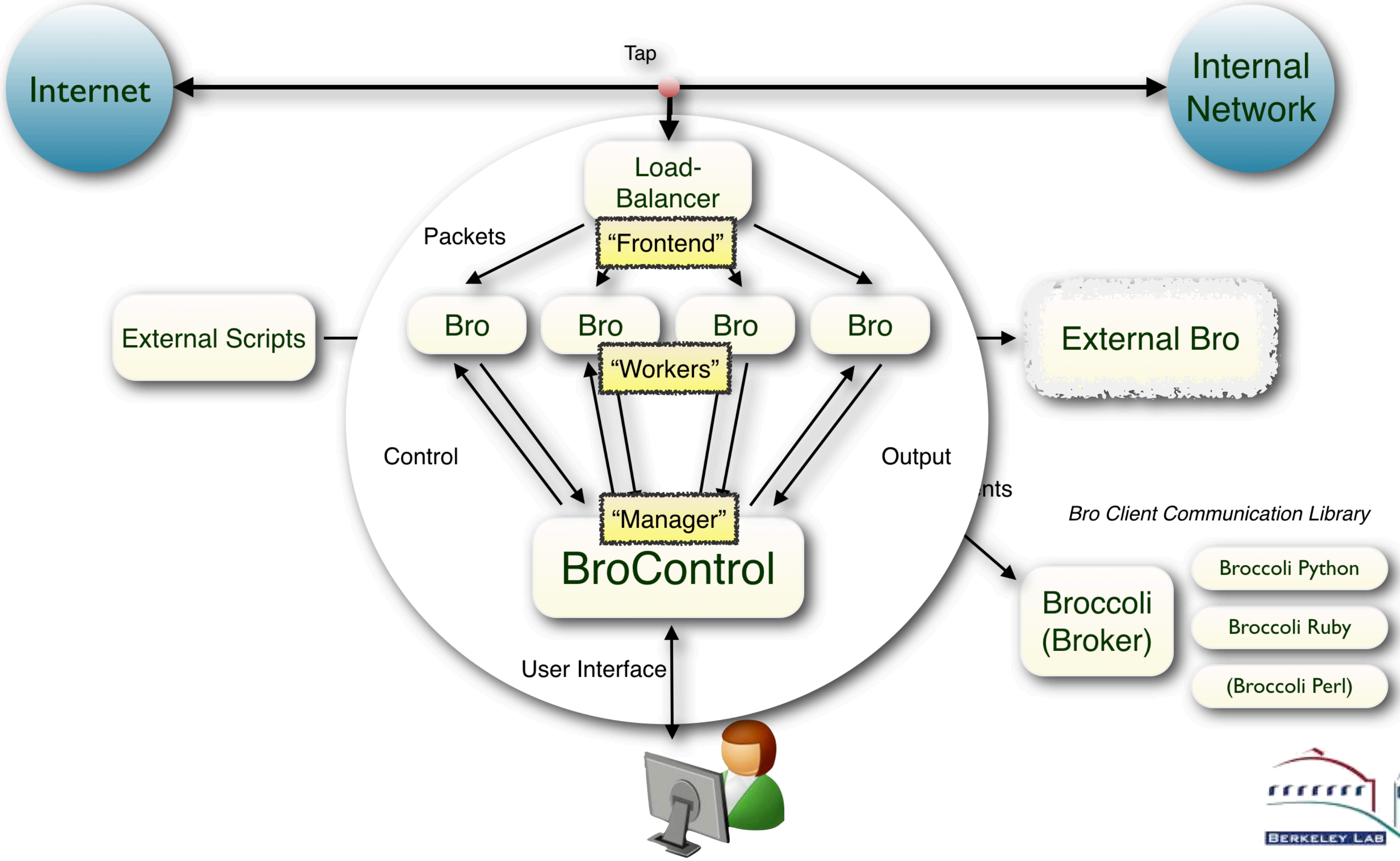
Bro *Cluster* Ecosystem



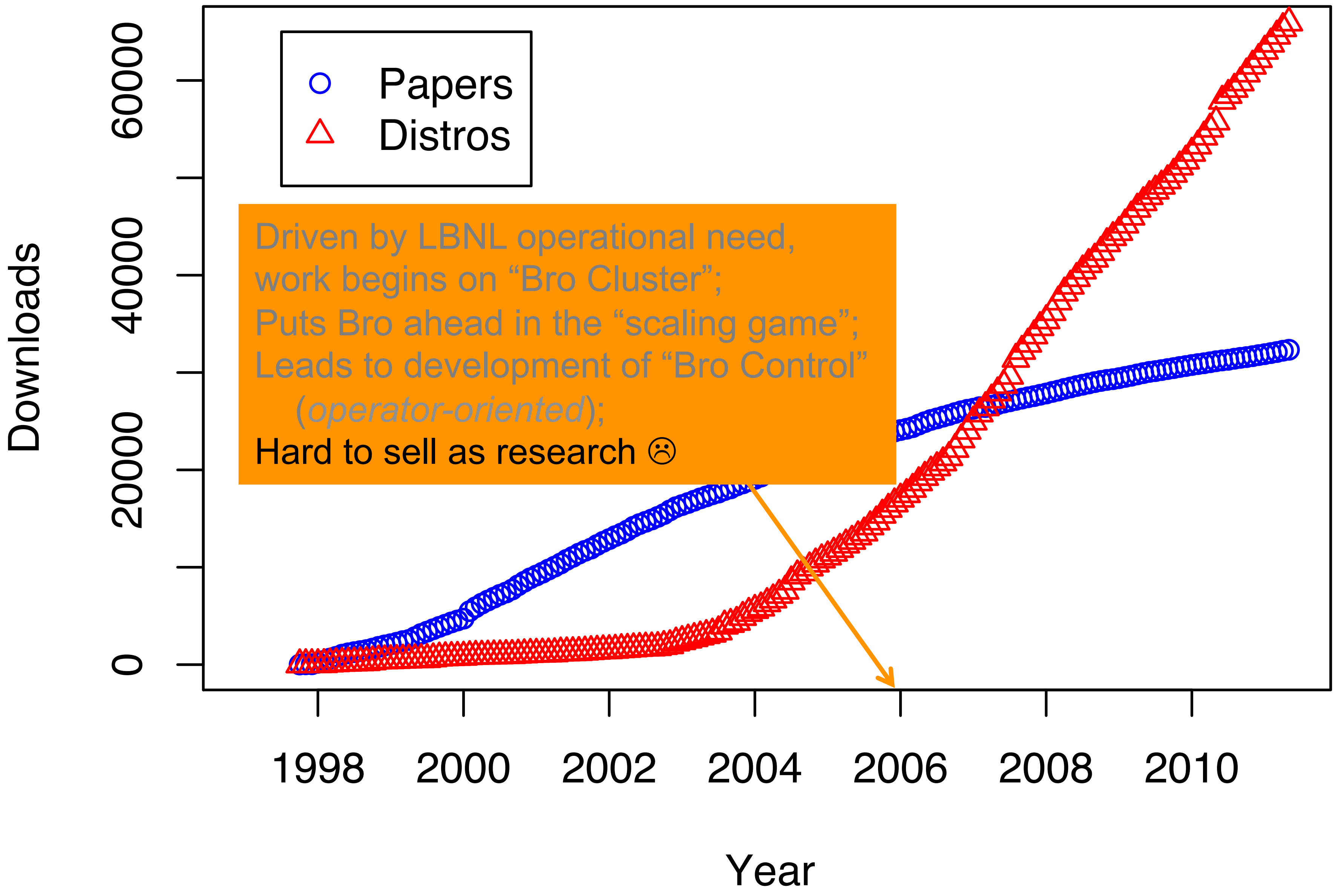
Bro *Cluster* Ecosystem



Bro *Cluster* Ecosystem

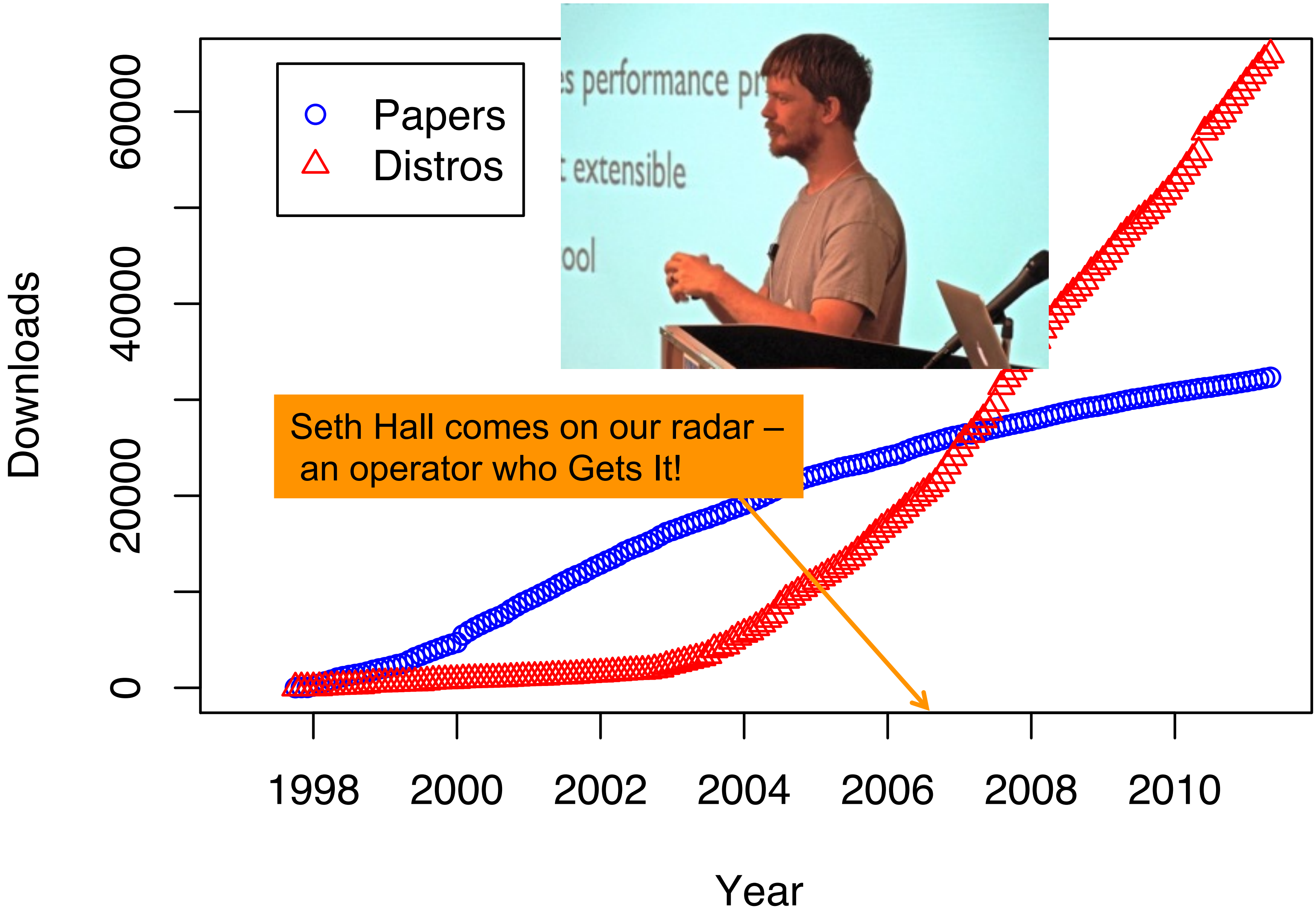


Interest in Bro

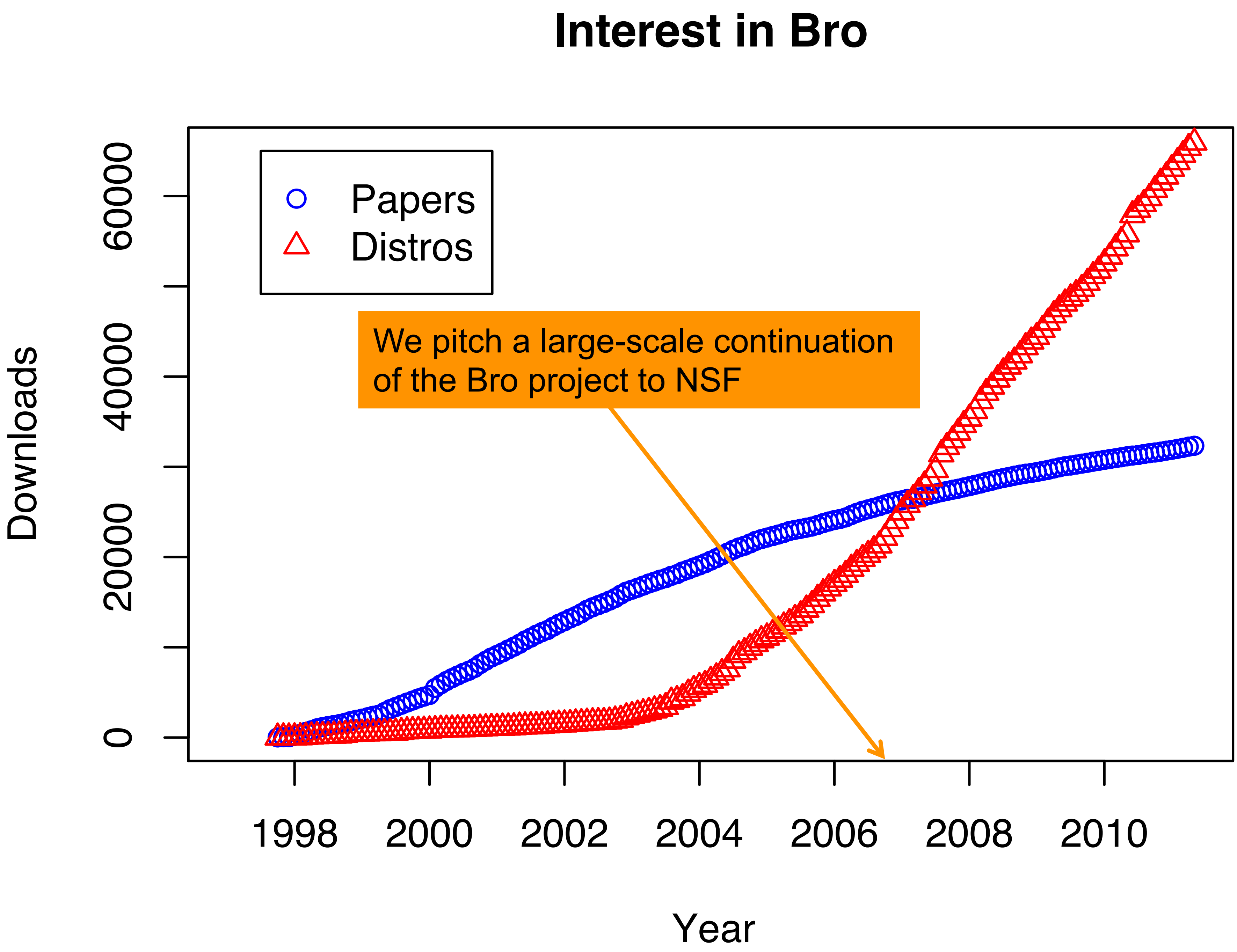


Driven by LBNL operational need, work begins on “Bro Cluster”;
Puts Bro ahead in the “scaling game”;
Leads to development of “Bro Control” (*operator-oriented*);
Hard to sell as research ☹

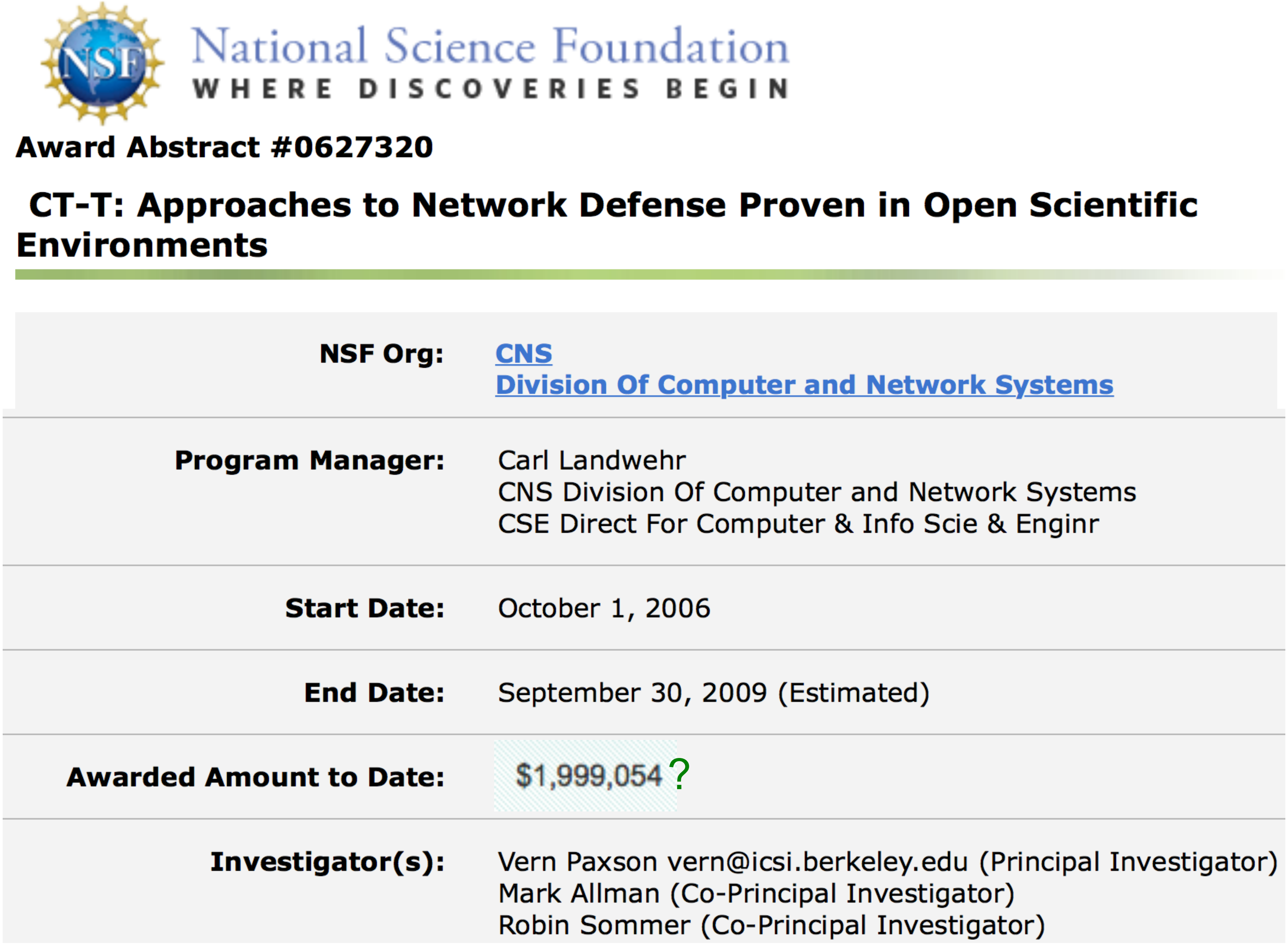
Interest in Bro



Seth Hall comes on our radar – an operator who Gets It!



We pitch a large-scale continuation of the Bro project to NSF

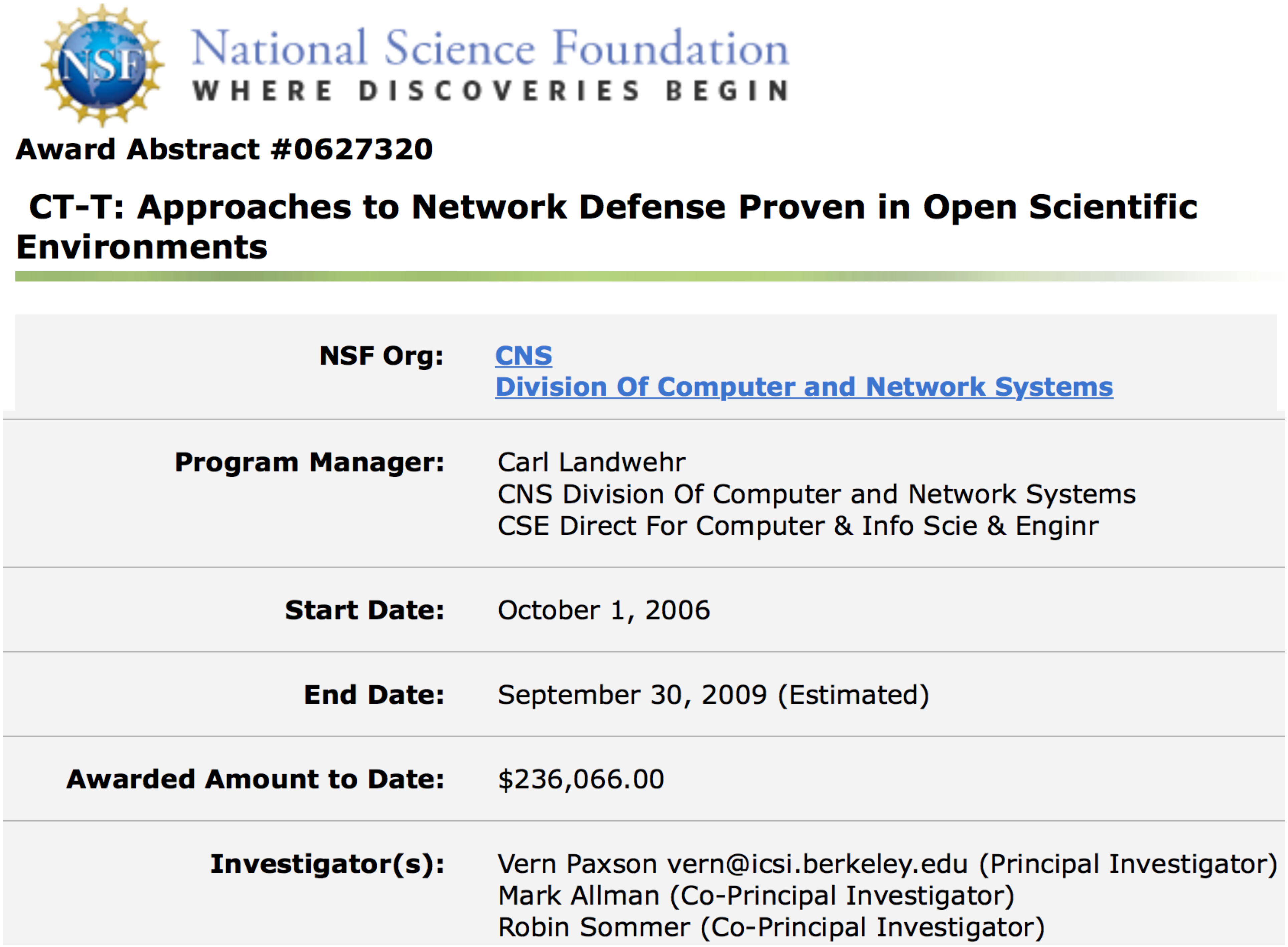


National Science Foundation
WHERE DISCOVERIES BEGIN

Award Abstract #0627320

CT-T: Approaches to Network Defense Proven in Open Scientific Environments

NSF Org:	CNS Division Of Computer and Network Systems
Program Manager:	Carl Landwehr CNS Division Of Computer and Network Systems CSE Direct For Computer & Info Scie & Enginr
Start Date:	October 1, 2006
End Date:	September 30, 2009 (Estimated)
Awarded Amount to Date:	$1,999,054 ?
Investigator(s):	Vern Paxson vern@icsi.berkeley.edu (Principal Investigator) Mark Allman (Co-Principal Investigator) Robin Sommer (Co-Principal Investigator)



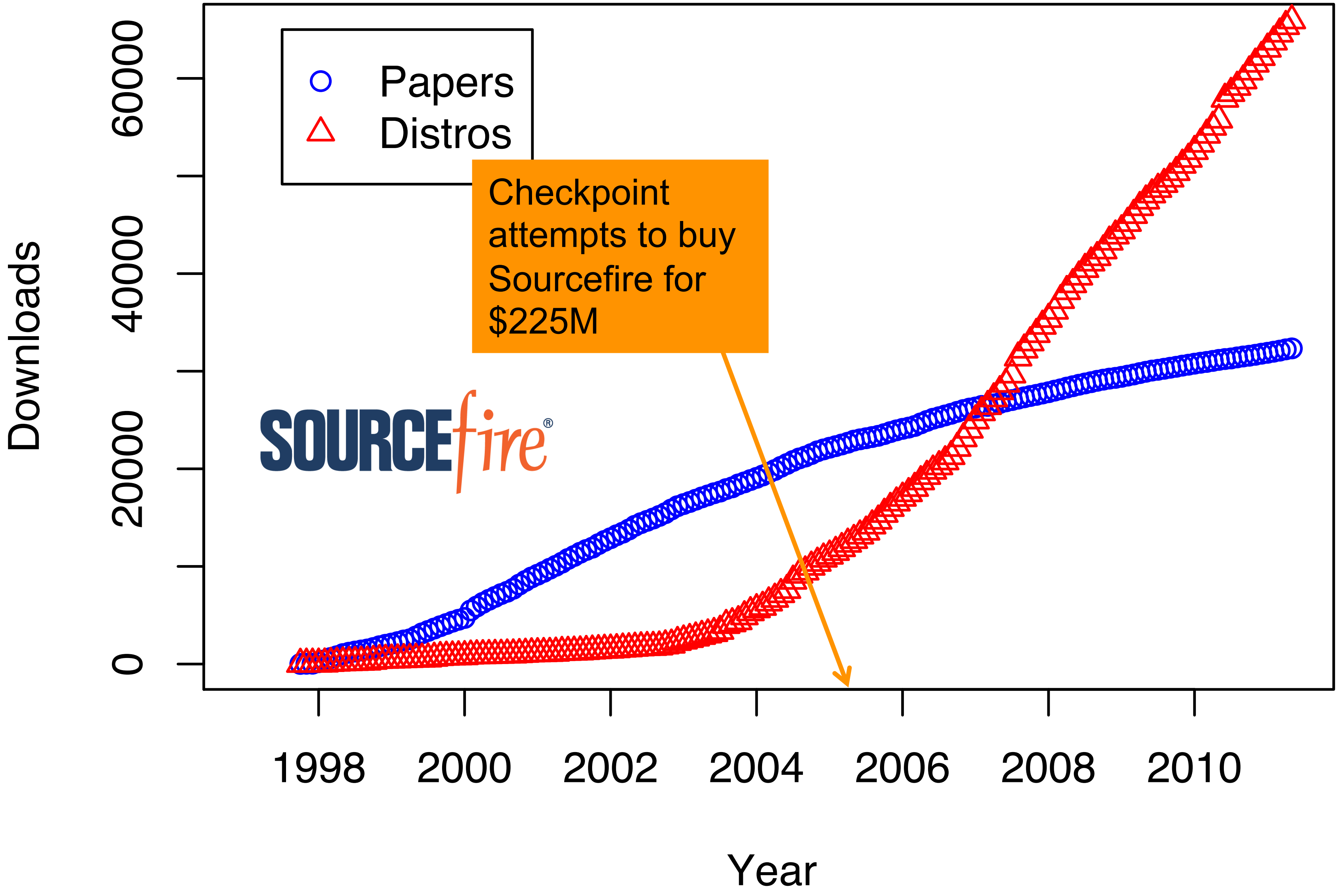
National Science Foundation
WHERE DISCOVERIES BEGIN

Award Abstract #0627320

CT-T: Approaches to Network Defense Proven in Open Scientific Environments

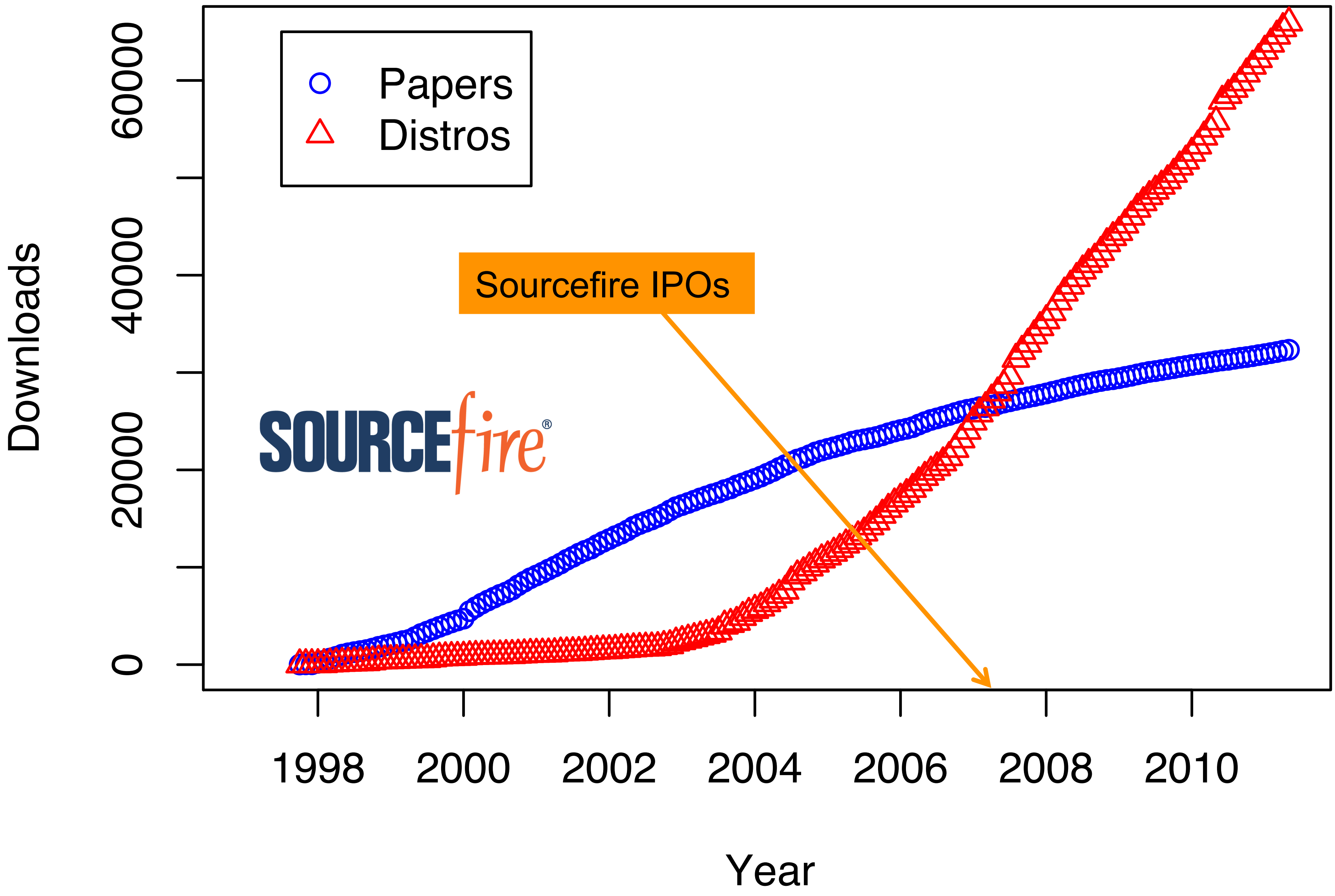
NSF Org:	CNS Division Of Computer and Network Systems
Program Manager:	Carl Landwehr CNS Division Of Computer and Network Systems CSE Direct For Computer & Info Scie & Enginr
Start Date:	October 1, 2006
End Date:	September 30, 2009 (Estimated)
Awarded Amount to Date:	$236,066.00
Investigator(s):	Vern Paxson vern@icsi.berkeley.edu (Principal Investigator) Mark Allman (Co-Principal Investigator) Robin Sommer (Co-Principal Investigator)

Interest in Bro



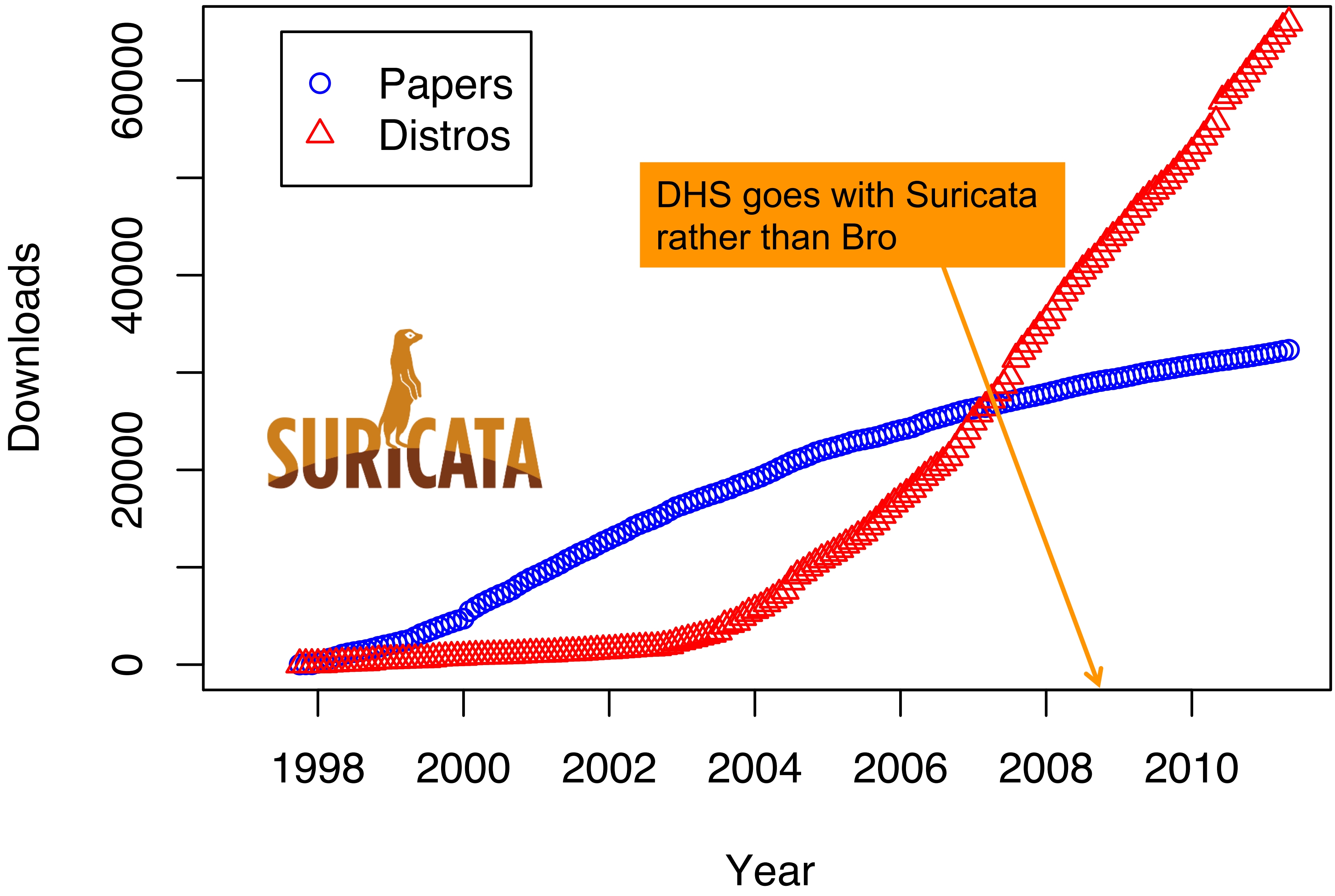
Checkpoint attempts to buy Sourcefire for $225M

Interest in Bro



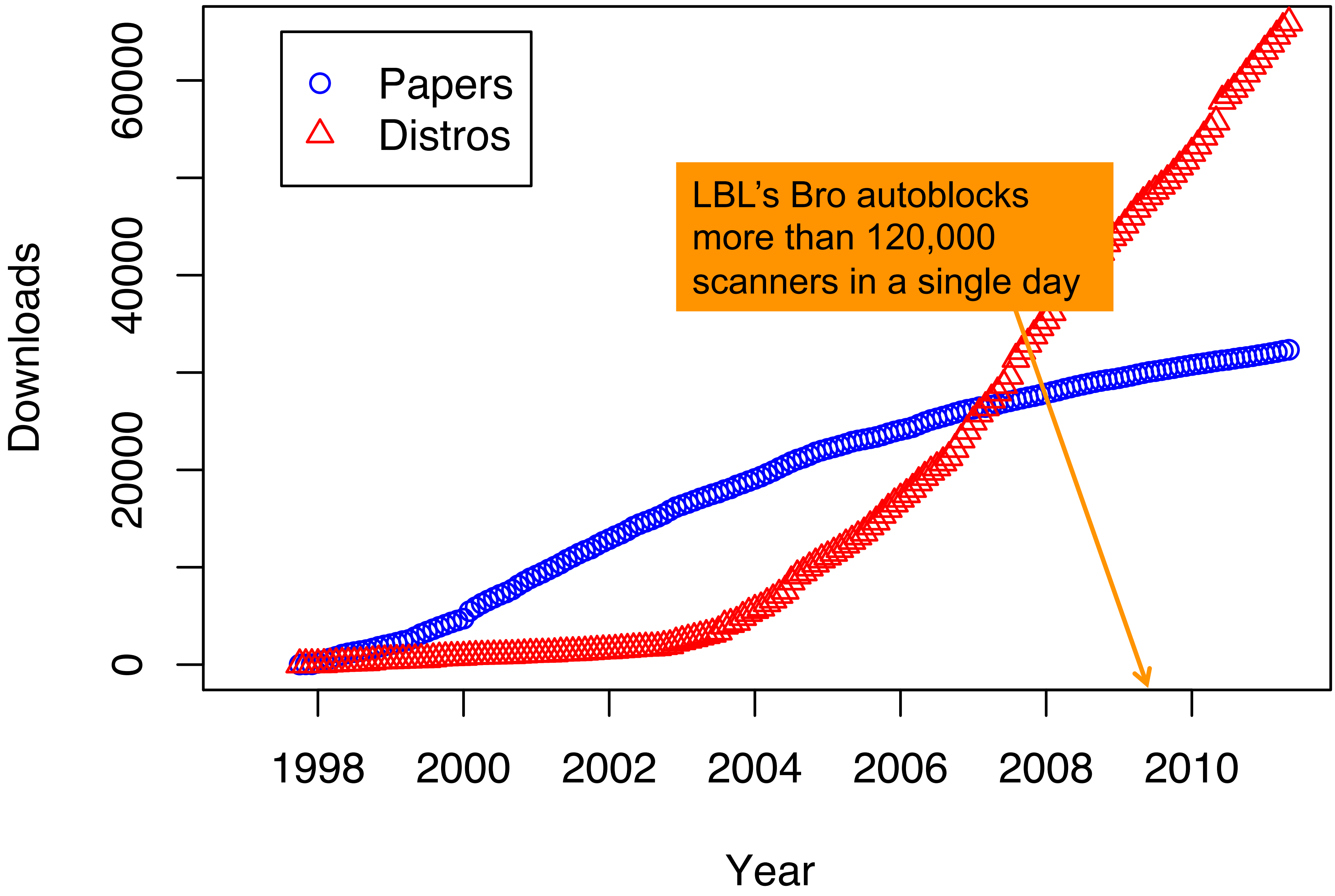
Sourcefire IPOs

Interest in Bro



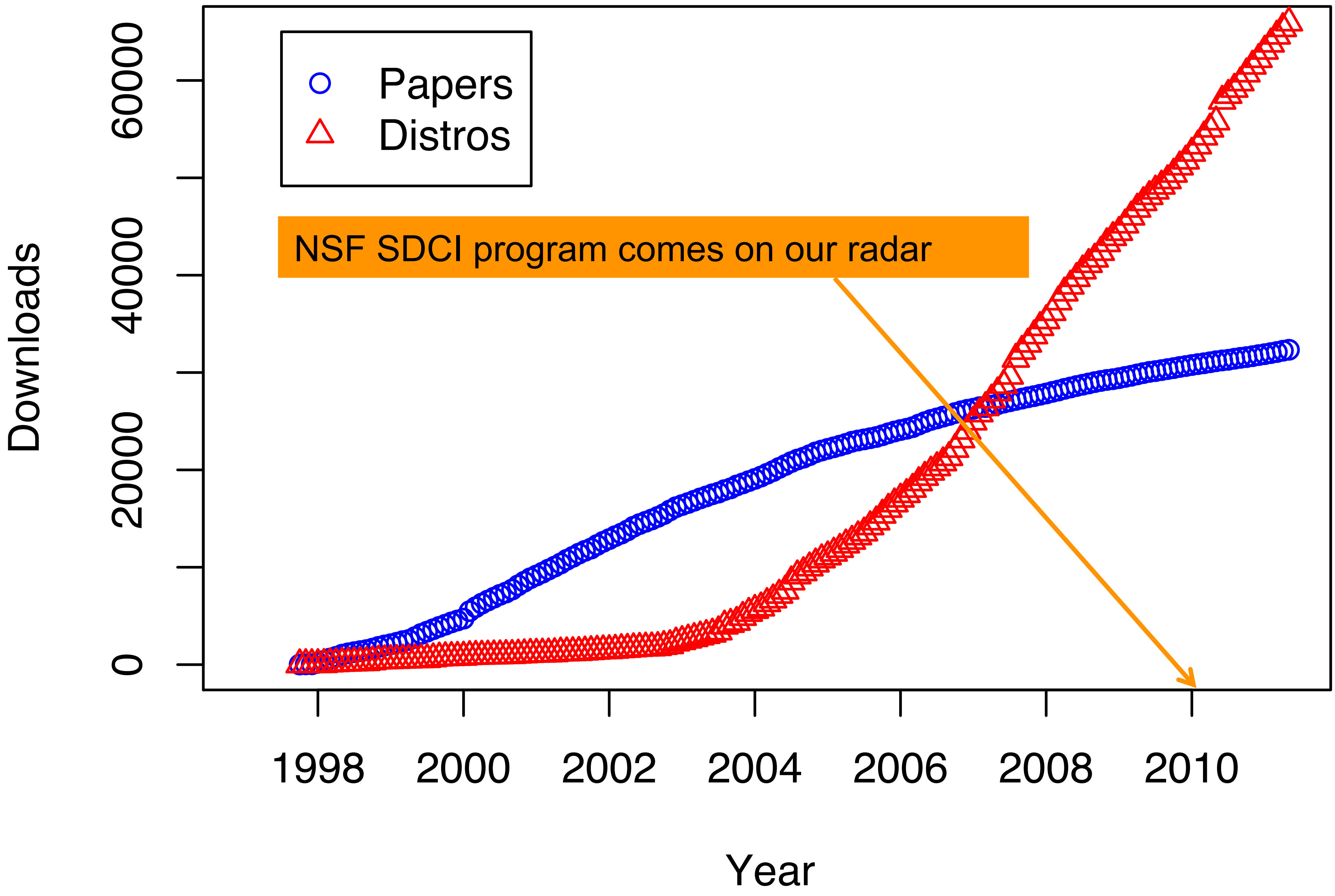
DHS goes with Suricata rather than Bro

Interest in Bro

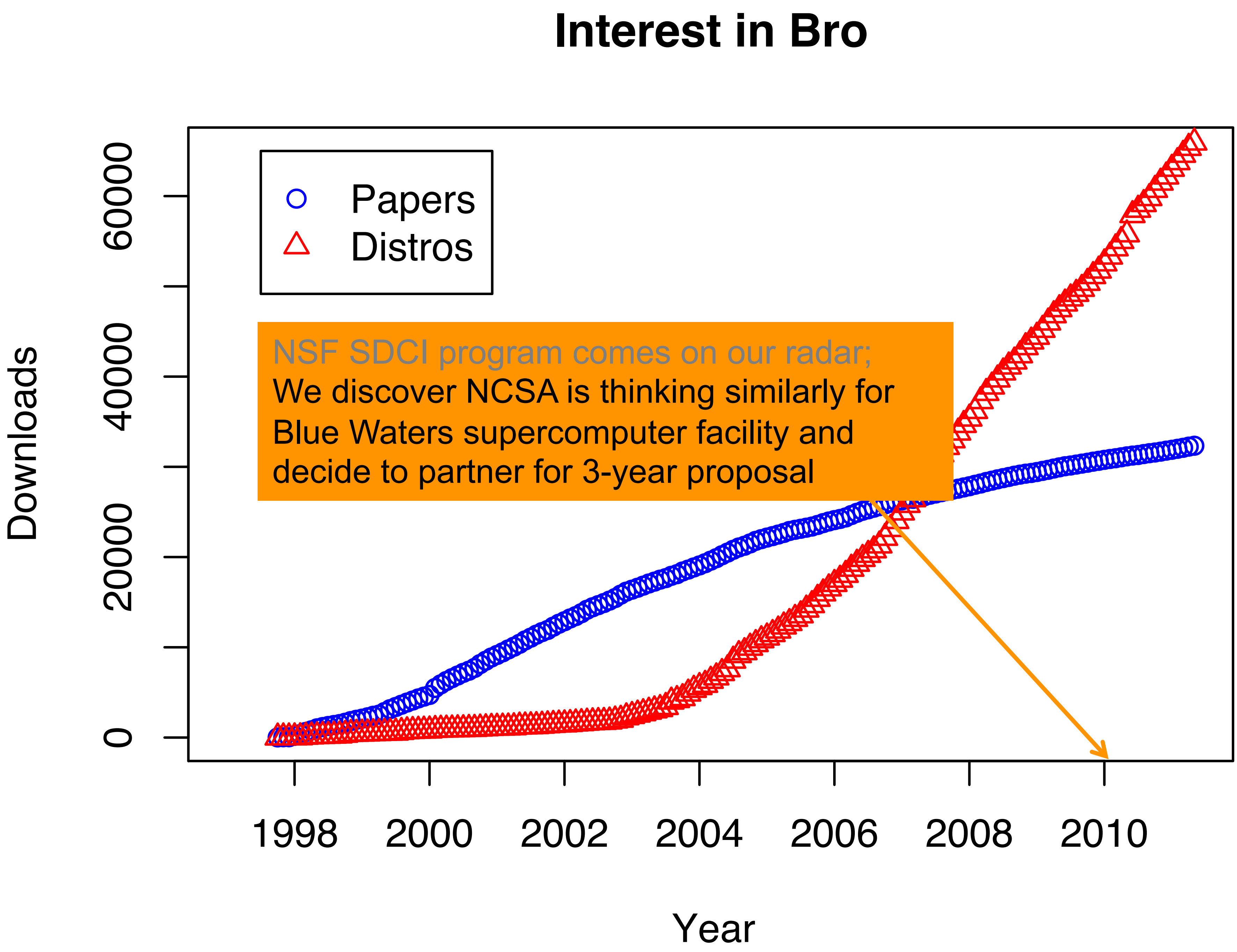


LBL's Bro autoblocks more than 120,000 scanners in a single day

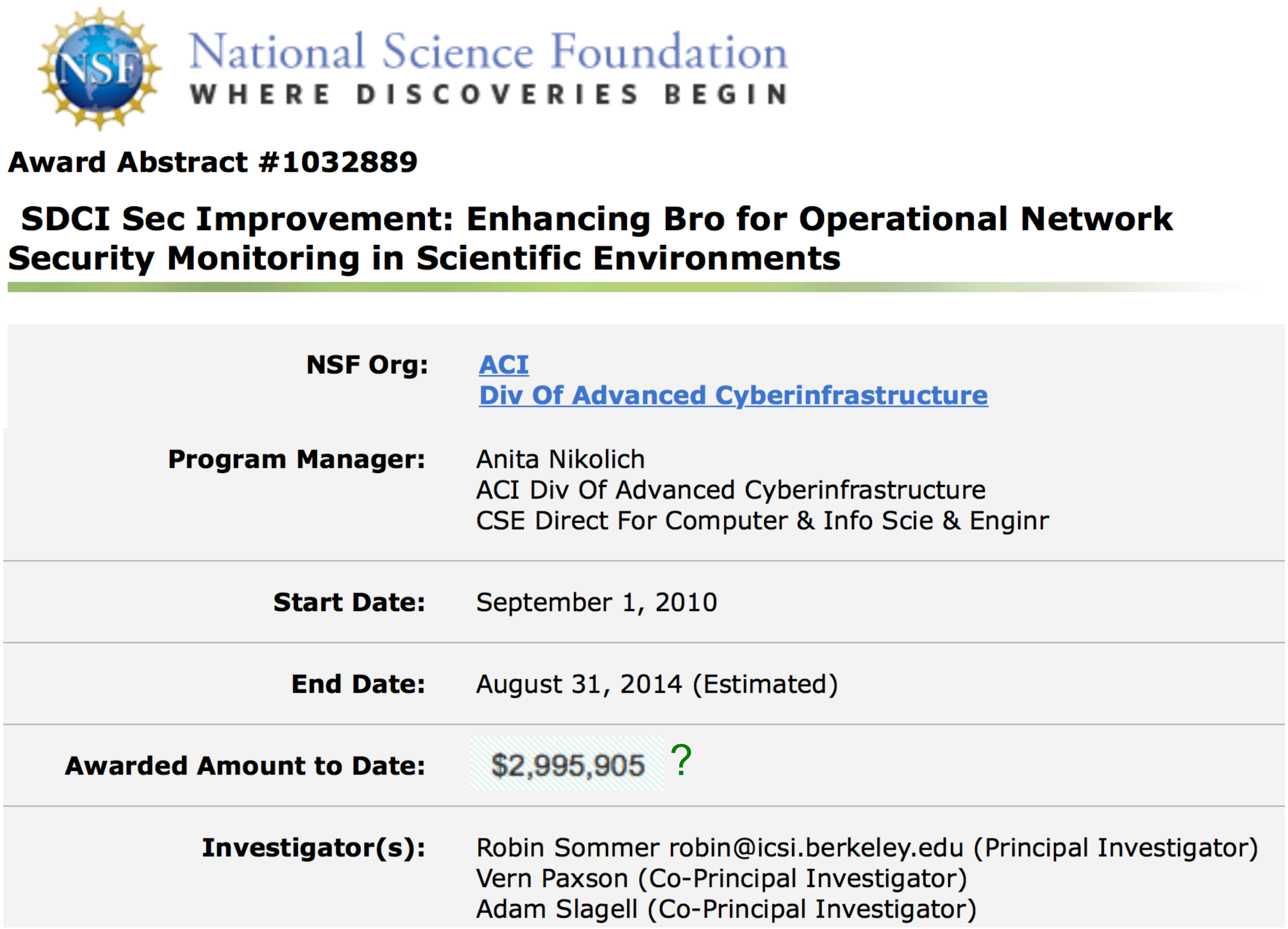
Interest in Bro



NSF SDCI program comes on our radar



NSF SDCI program comes on our radar;
We discover NCSA is thinking similarly for
Blue Waters supercomputer facility and
decide to partner for 3-year proposal

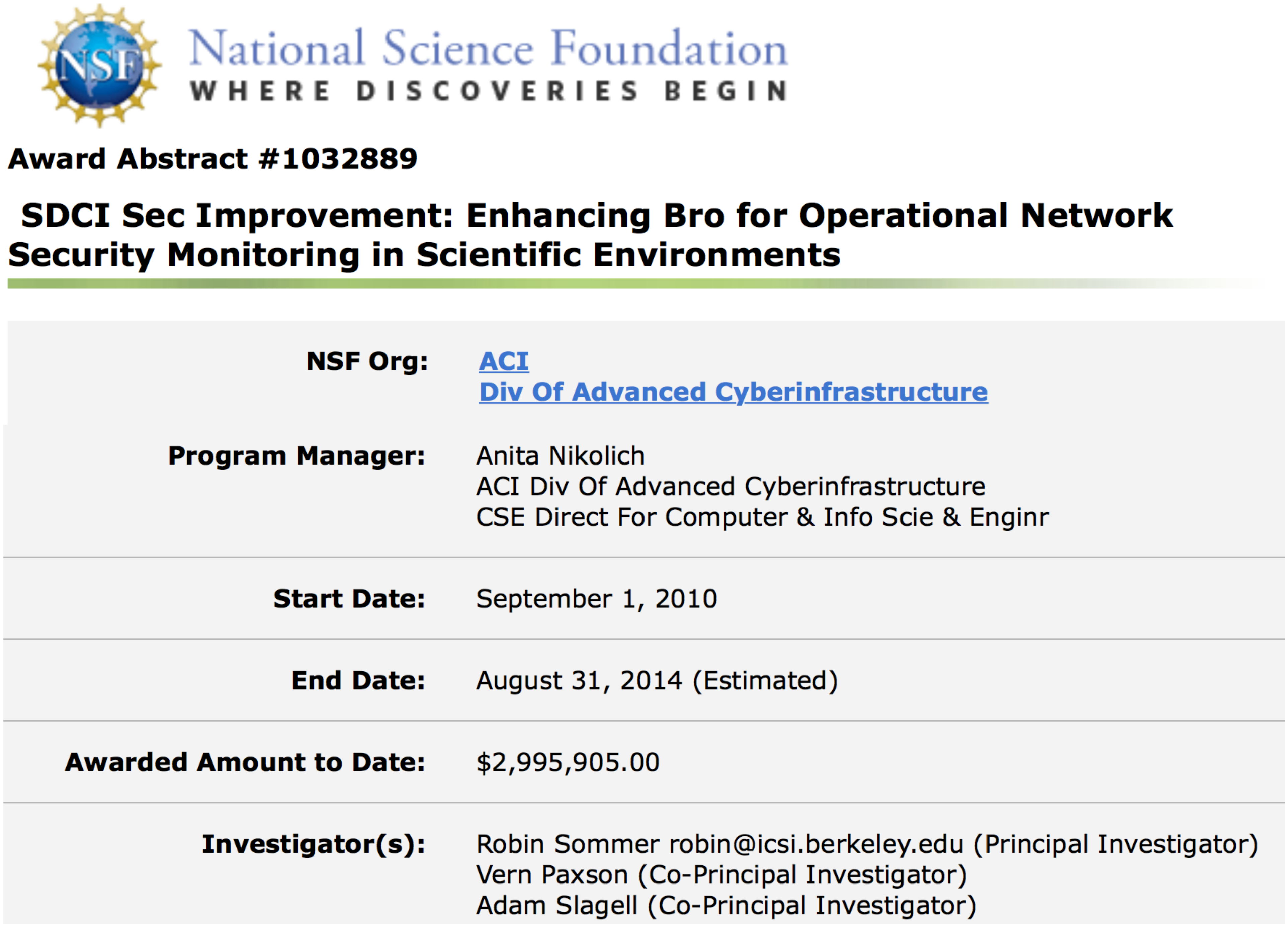


National Science Foundation
WHERE DISCOVERIES BEGIN

Award Abstract #1032889

SDCI Sec Improvement: Enhancing Bro for Operational Network Security Monitoring in Scientific Environments

NSF Org:	ACI Div Of Advanced Cyberinfrastructure
Program Manager:	Anita Nikolich ACI Div Of Advanced Cyberinfrastructure CSE Direct For Computer & Info Scie & Enginr
Start Date:	September 1, 2010
End Date:	August 31, 2014 (Estimated)
Awarded Amount to Date:	$2,995,905 ?
Investigator(s):	Robin Sommer robin@icsi.berkeley.edu (Principal Investigator) Vern Paxson (Co-Principal Investigator) Adam Slagell (Co-Principal Investigator)

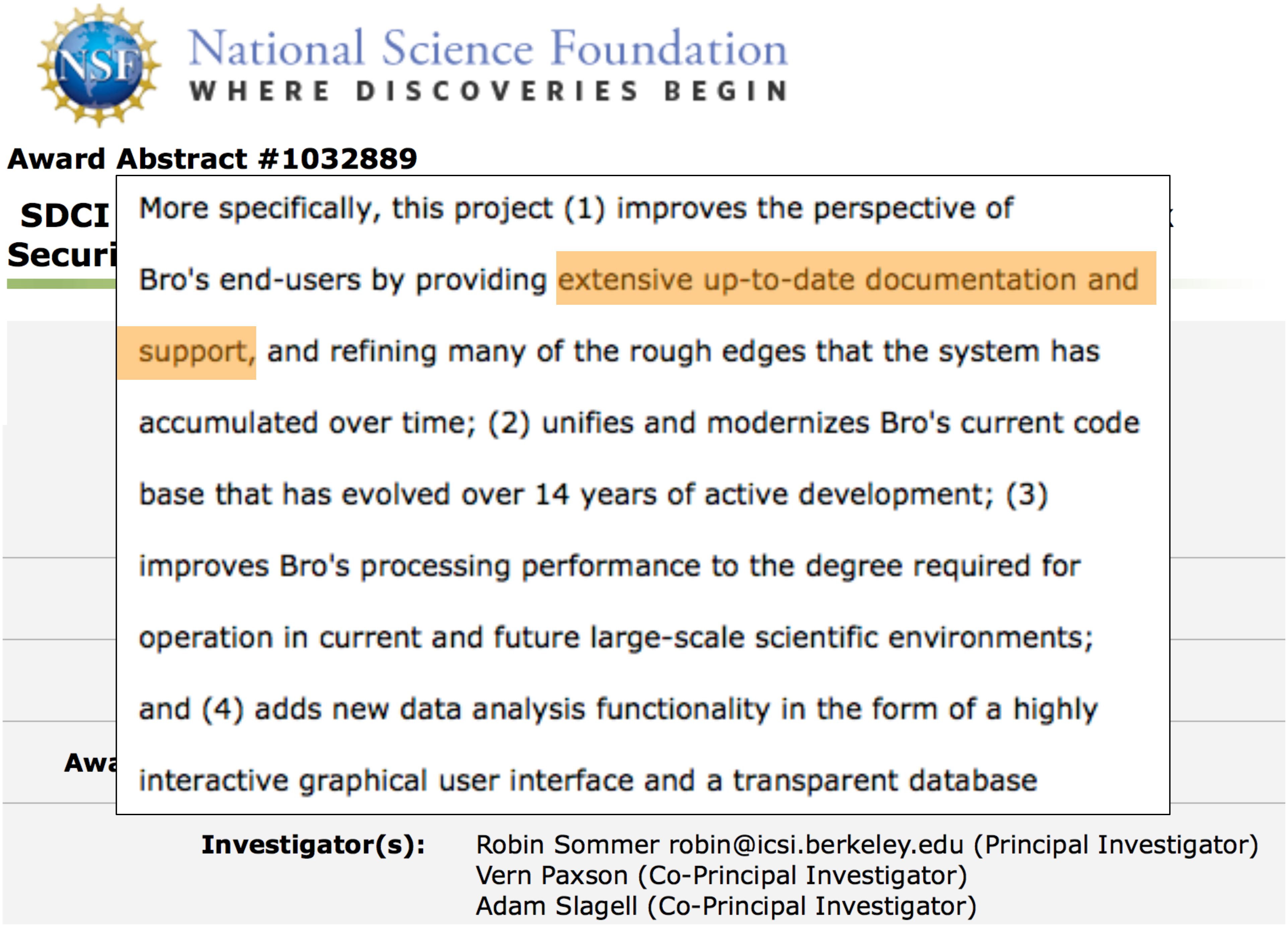


National Science Foundation
WHERE DISCOVERIES BEGIN

Award Abstract #1032889

SDCI Sec Improvement: Enhancing Bro for Operational Network Security Monitoring in Scientific Environments

NSF Org:	ACI Div Of Advanced Cyberinfrastructure
Program Manager:	Anita Nikolich ACI Div Of Advanced Cyberinfrastructure CSE Direct For Computer & Info Scie & Enginr
Start Date:	September 1, 2010
End Date:	August 31, 2014 (Estimated)
Awarded Amount to Date:	$2,995,905.00
Investigator(s):	Robin Sommer robin@icsi.berkeley.edu (Principal Investigator) Vern Paxson (Co-Principal Investigator) Adam Slagell (Co-Principal Investigator)



National Science Foundation
WHERE DISCOVERIES BEGIN

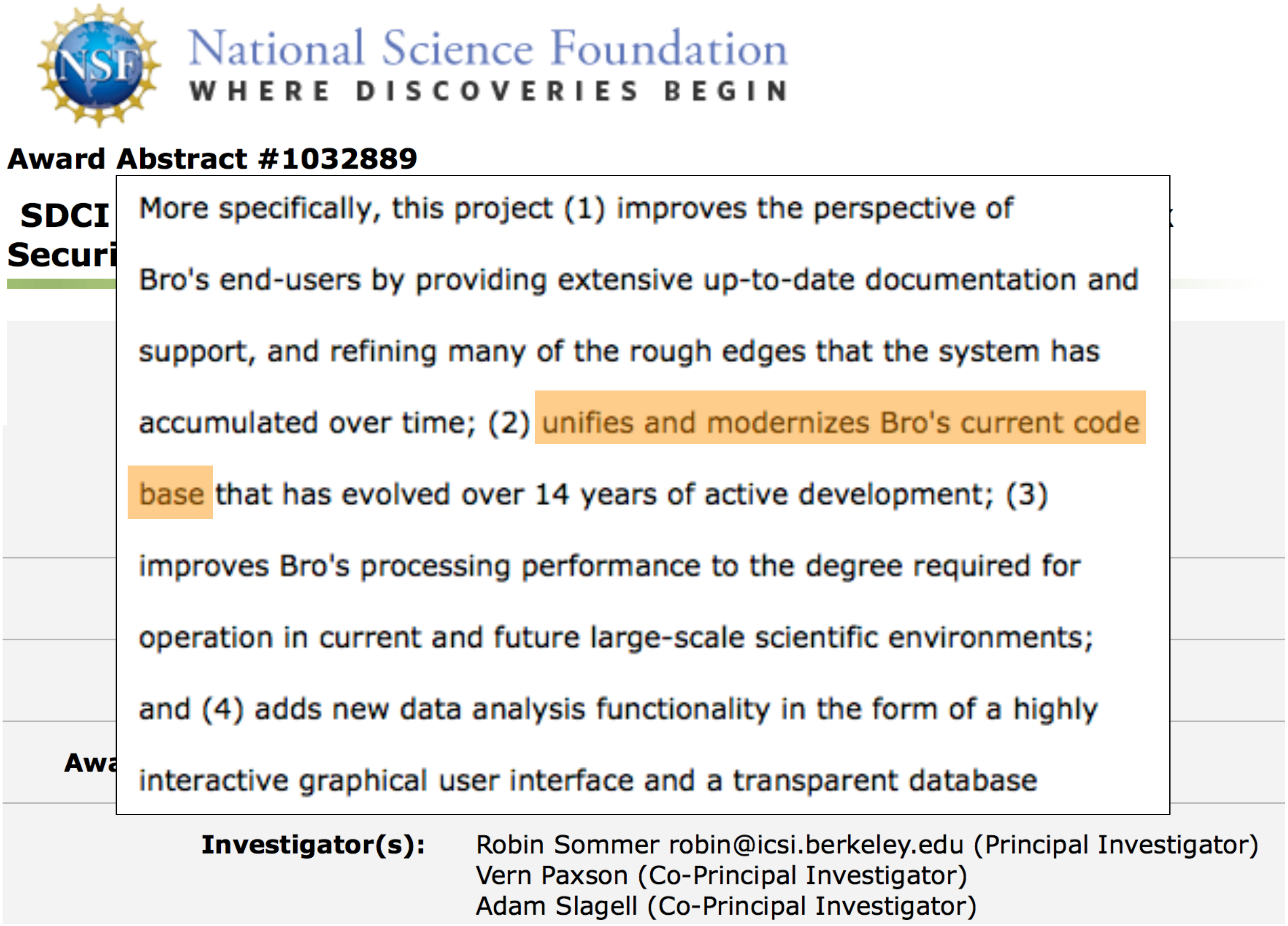
Award Abstract #1032889

SDCI
Securi

More specifically, this project (1) improves the perspective of Bro's end-users by providing extensive up-to-date documentation and support, and refining many of the rough edges that the system has accumulated over time; (2) unifies and modernizes Bro's current code base that has evolved over 14 years of active development; (3) improves Bro's processing performance to the degree required for operation in current and future large-scale scientific environments; and (4) adds new data analysis functionality in the form of a highly interactive graphical user interface and a transparent database

Awa

Investigator(s):	Robin Sommer robin@icsi.berkeley.edu (Principal Investigator) Vern Paxson (Co-Principal Investigator) Adam Slagell (Co-Principal Investigator)



National Science Foundation
WHERE DISCOVERIES BEGIN

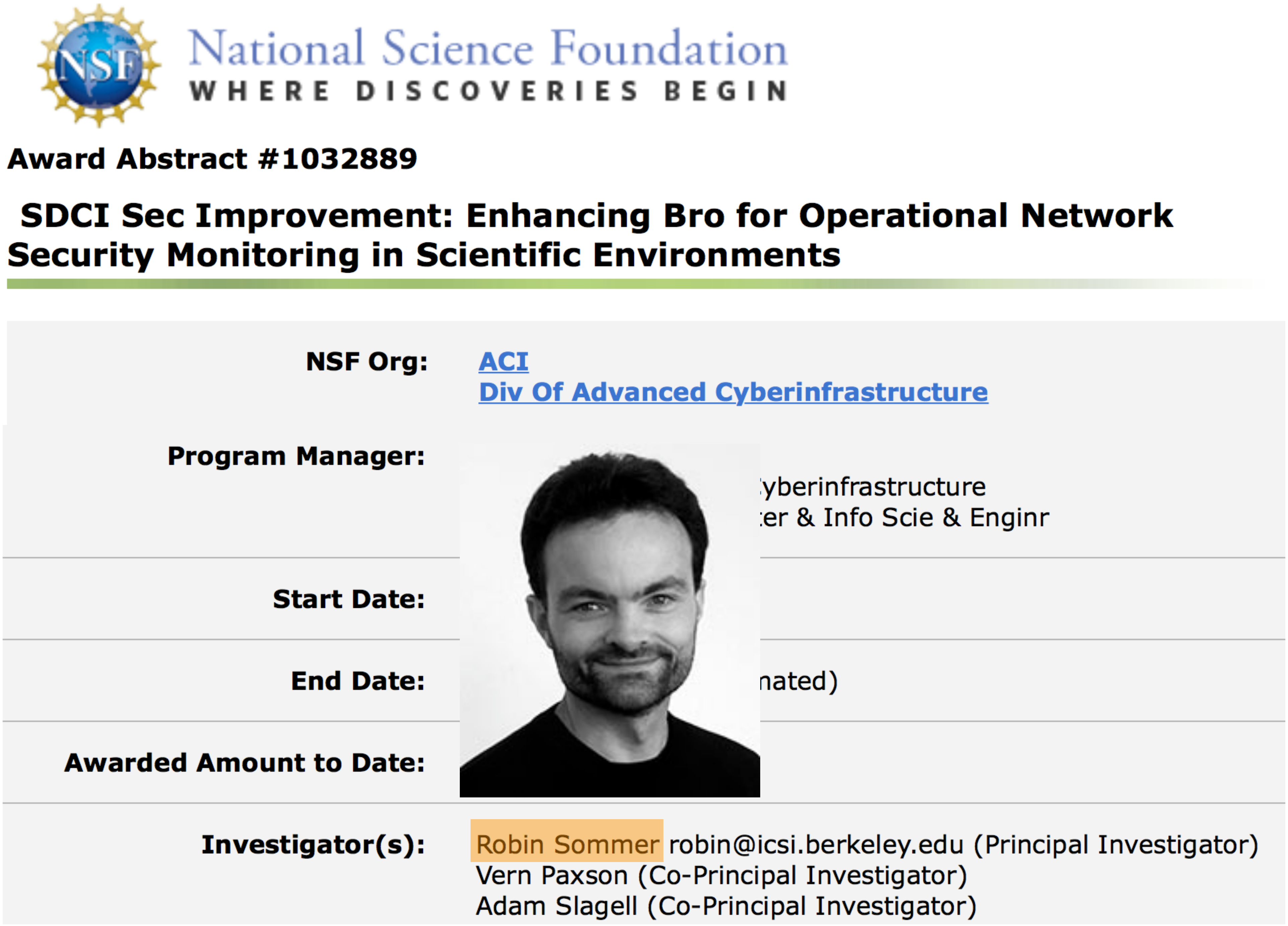
Award Abstract #1032889

SDCI
Securi

More specifically, this project (1) improves the perspective of Bro's end-users by providing extensive up-to-date documentation and support, and refining many of the rough edges that the system has accumulated over time; (2) unifies and modernizes Bro's current code base that has evolved over 14 years of active development; (3) improves Bro's processing performance to the degree required for operation in current and future large-scale scientific environments; and (4) adds new data analysis functionality in the form of a highly interactive graphical user interface and a transparent database

Awa

Investigator(s):	Robin Sommer robin@icsi.berkeley.edu (Principal Investigator) Vern Paxson (Co-Principal Investigator) Adam Slagell (Co-Principal Investigator)

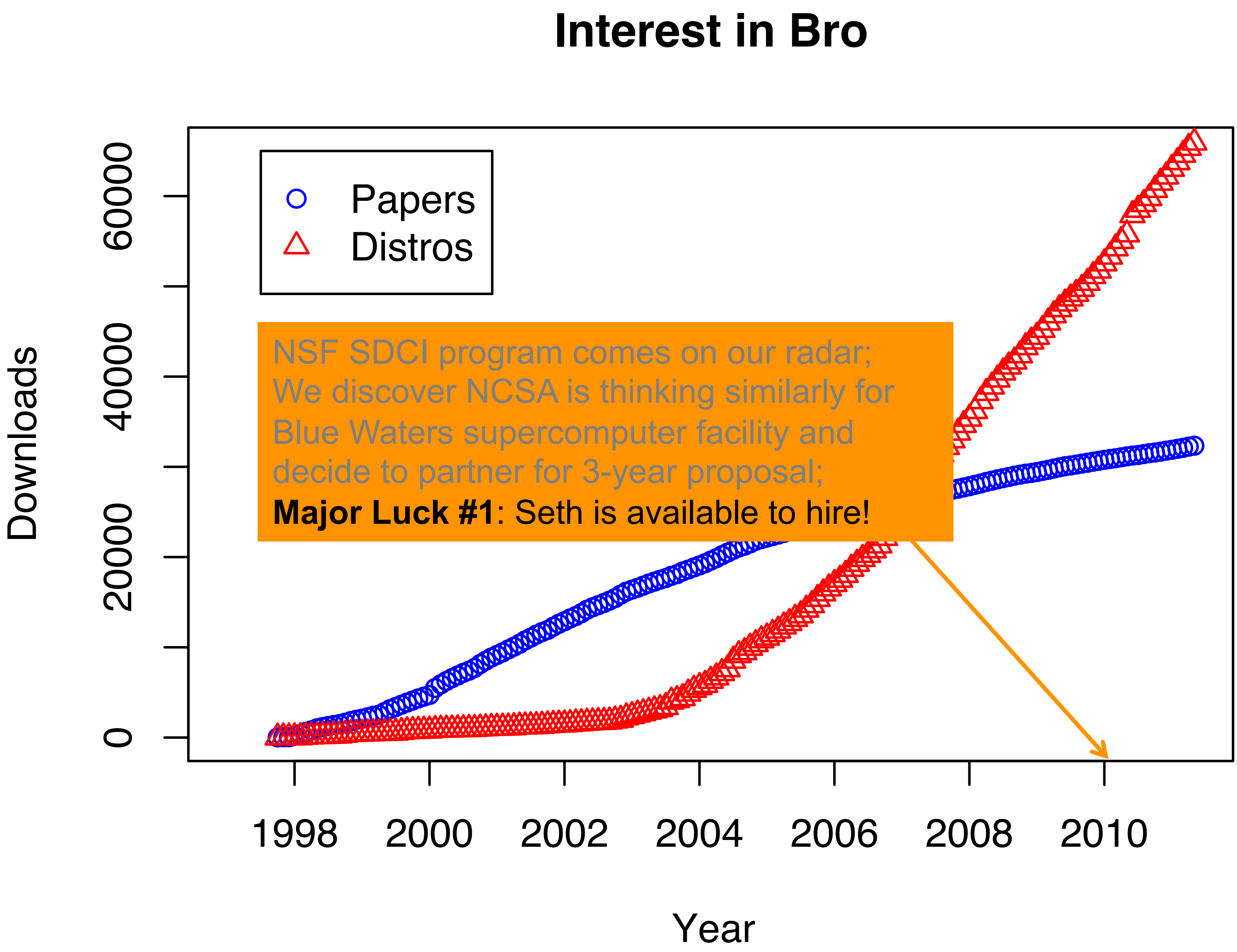


National Science Foundation
WHERE DISCOVERIES BEGIN

Award Abstract #1032889

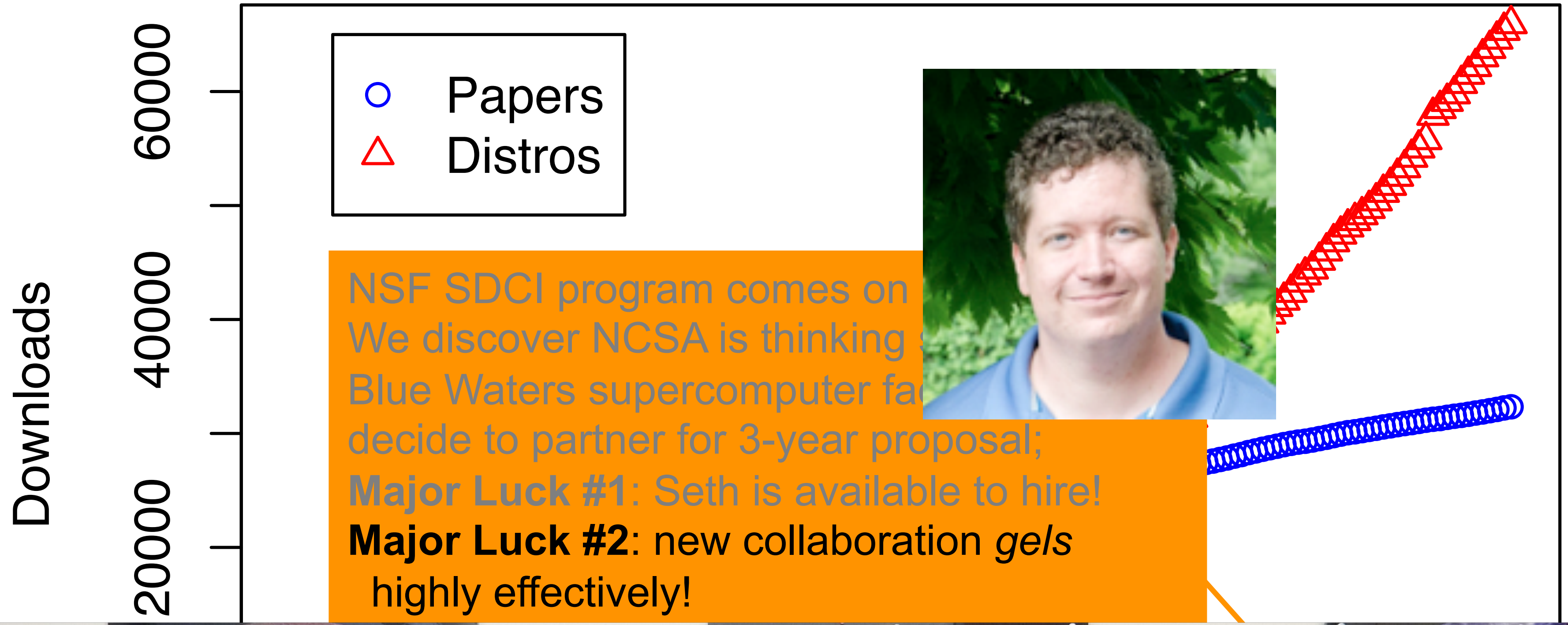
SDCI Sec Improvement: Enhancing Bro for Operational Network Security Monitoring in Scientific Environments

NSF Org:	ACI Div Of Advanced Cyberinfrastructure
Program Manager:	yberinfrastructure er & Info Scie & Enginr
Start Date:	
End Date:	nated)
Awarded Amount to Date:	
Investigator(s):	Robin Sommer robin@icsi.berkeley.edu (Principal Investigator) Vern Paxson (Co-Principal Investigator) Adam Slagell (Co-Principal Investigator)



NSF SDCI program comes on our radar;
We discover NCSA is thinking similarly for
Blue Waters supercomputer facility and
decide to partner for 3-year proposal;
Major Luck #1: Seth is available to hire!

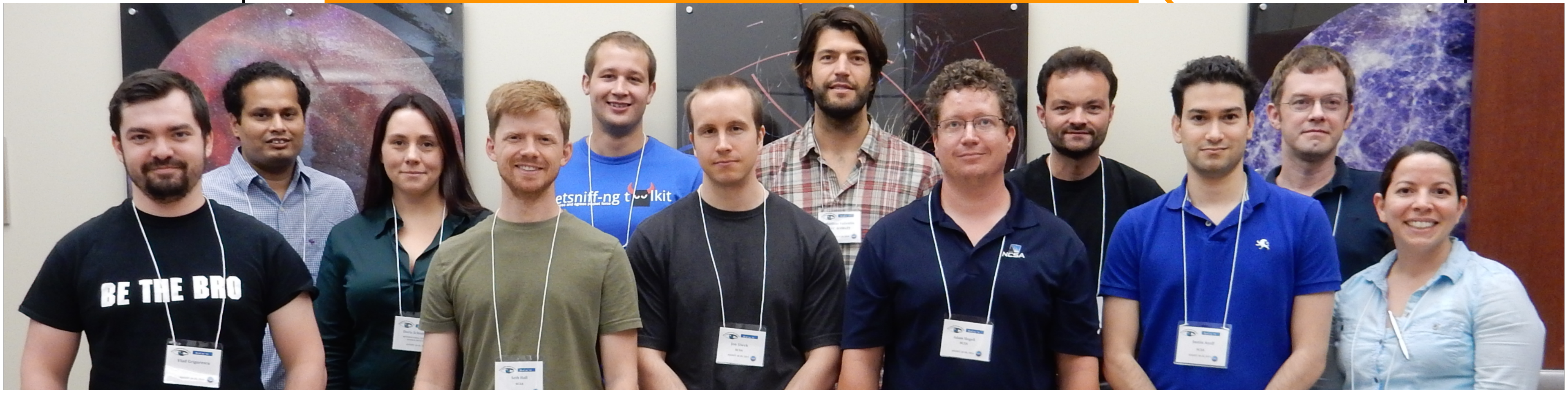
Interest in Bro

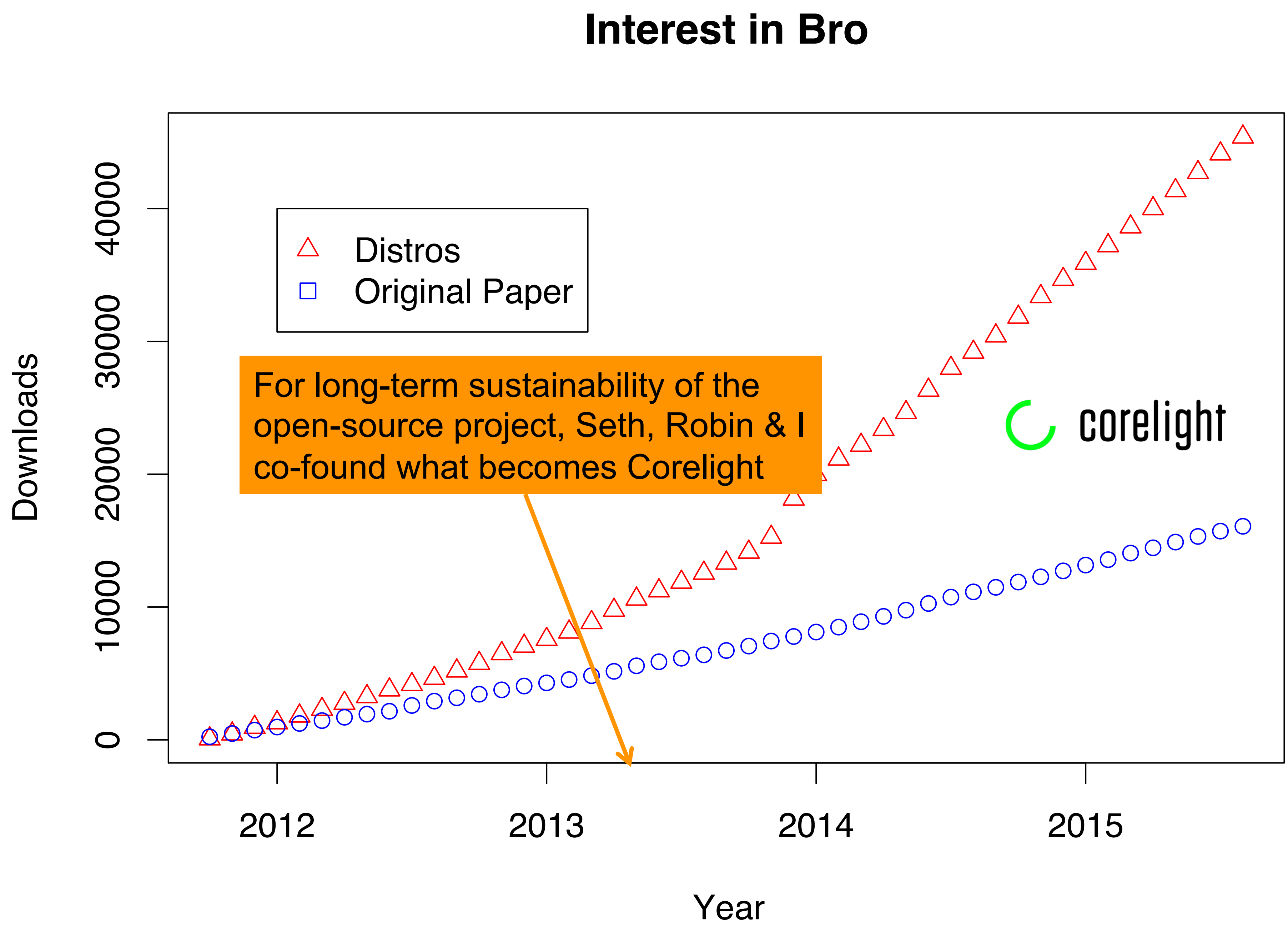


NSF SDCI program comes on
We discover NCSA is thinking
Blue Waters supercomputer fa
decide to partner for 3-year proposal;

Major Luck #1: Seth is available to hire!

Major Luck #2: new collaboration *gels* highly effectively!

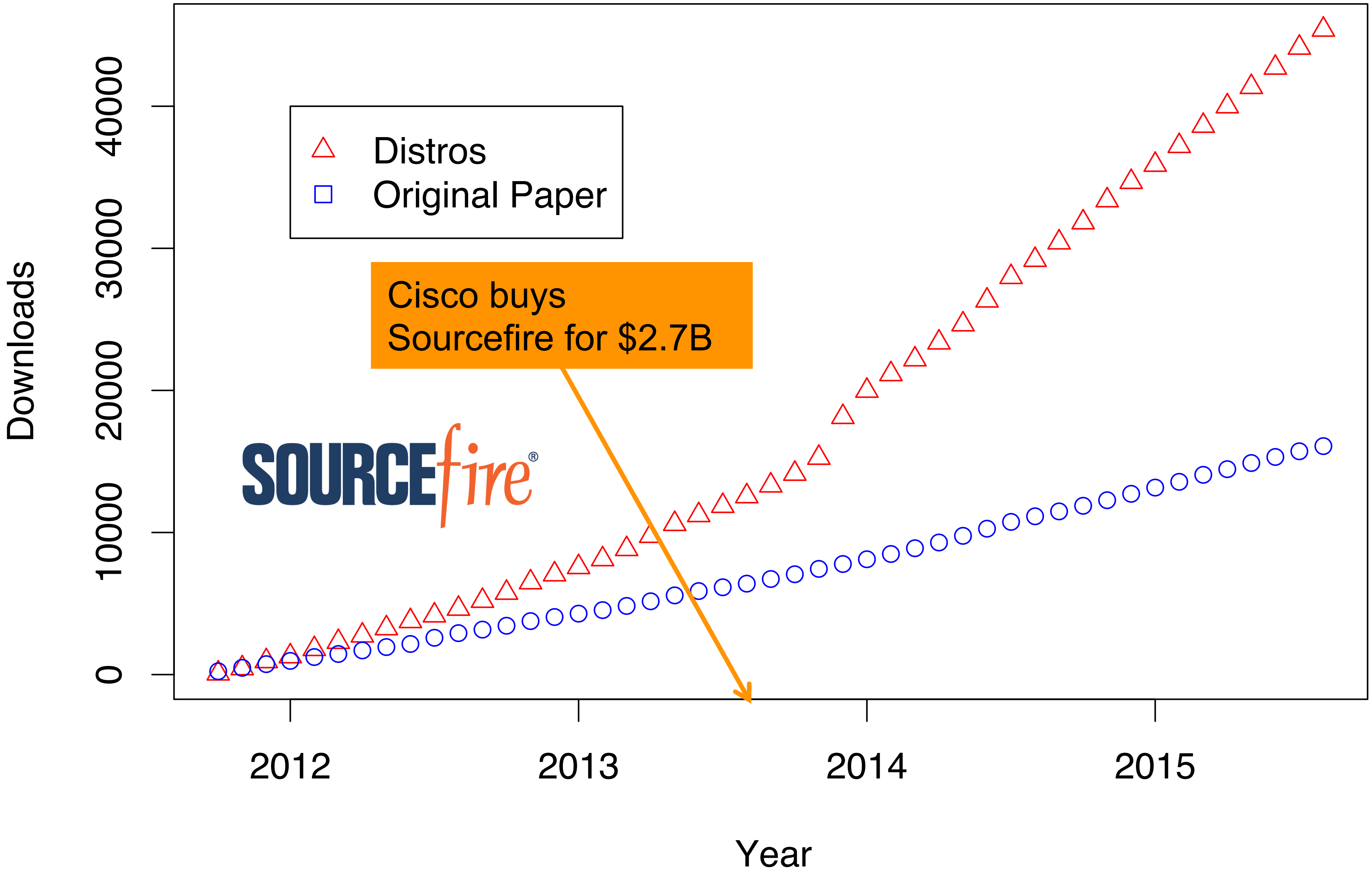




Interest in Bro

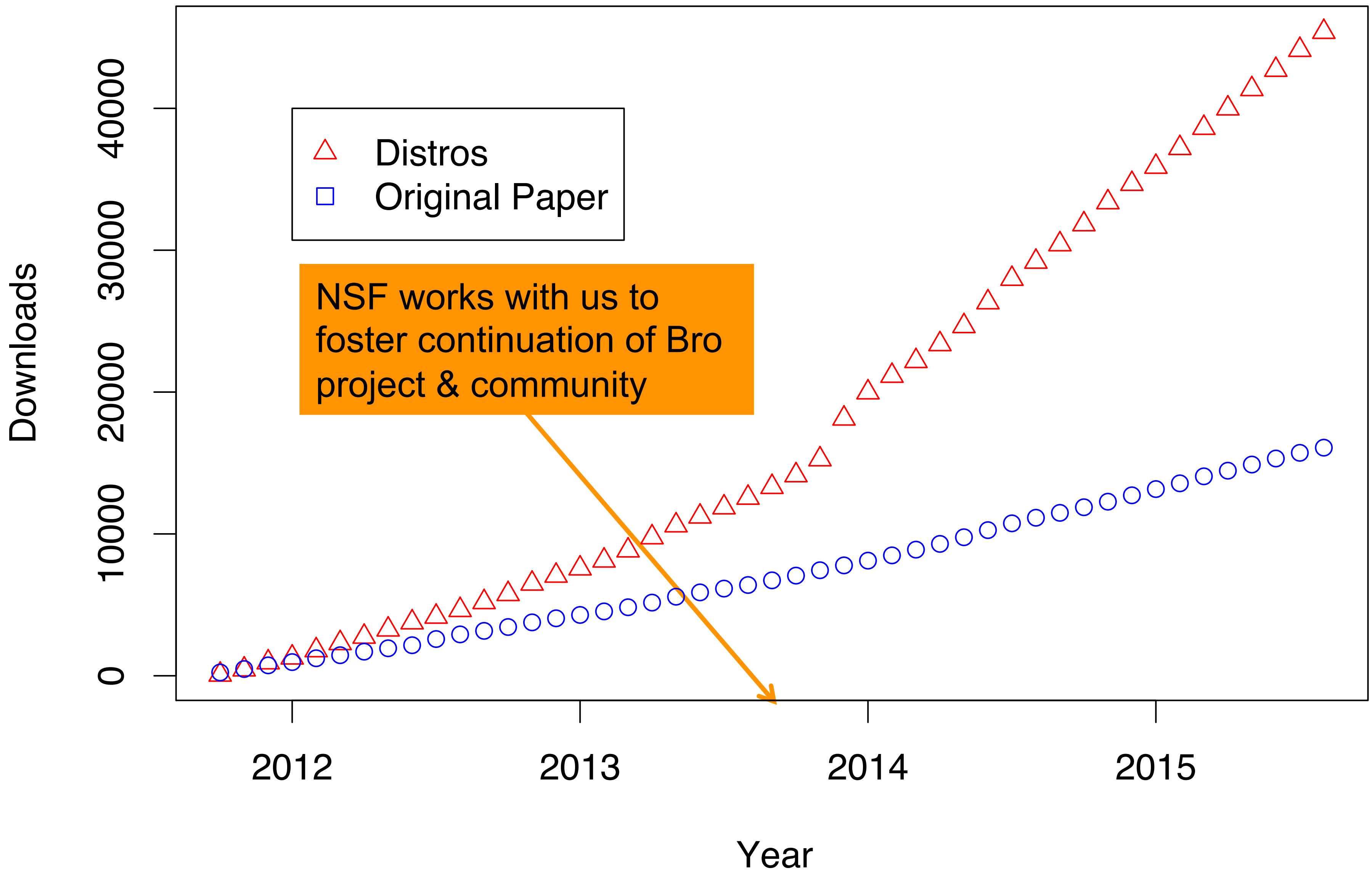
For long-term sustainability of the open-source project, Seth, Robin & I co-found what becomes Corelight

Interest in Bro

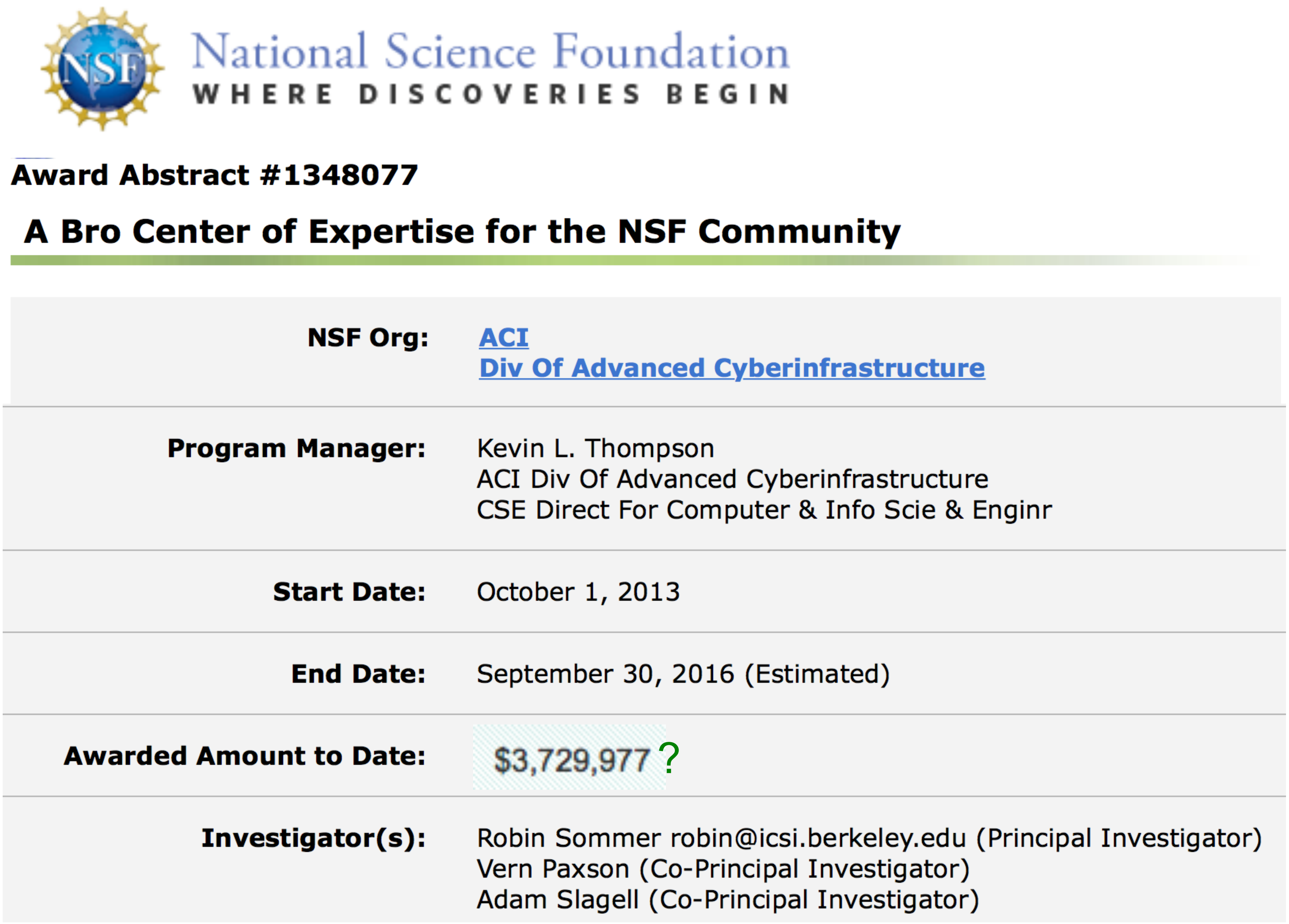


Cisco buys
Sourcefire for $2.7B

Interest in Bro



NSF works with us to foster continuation of Bro project & community

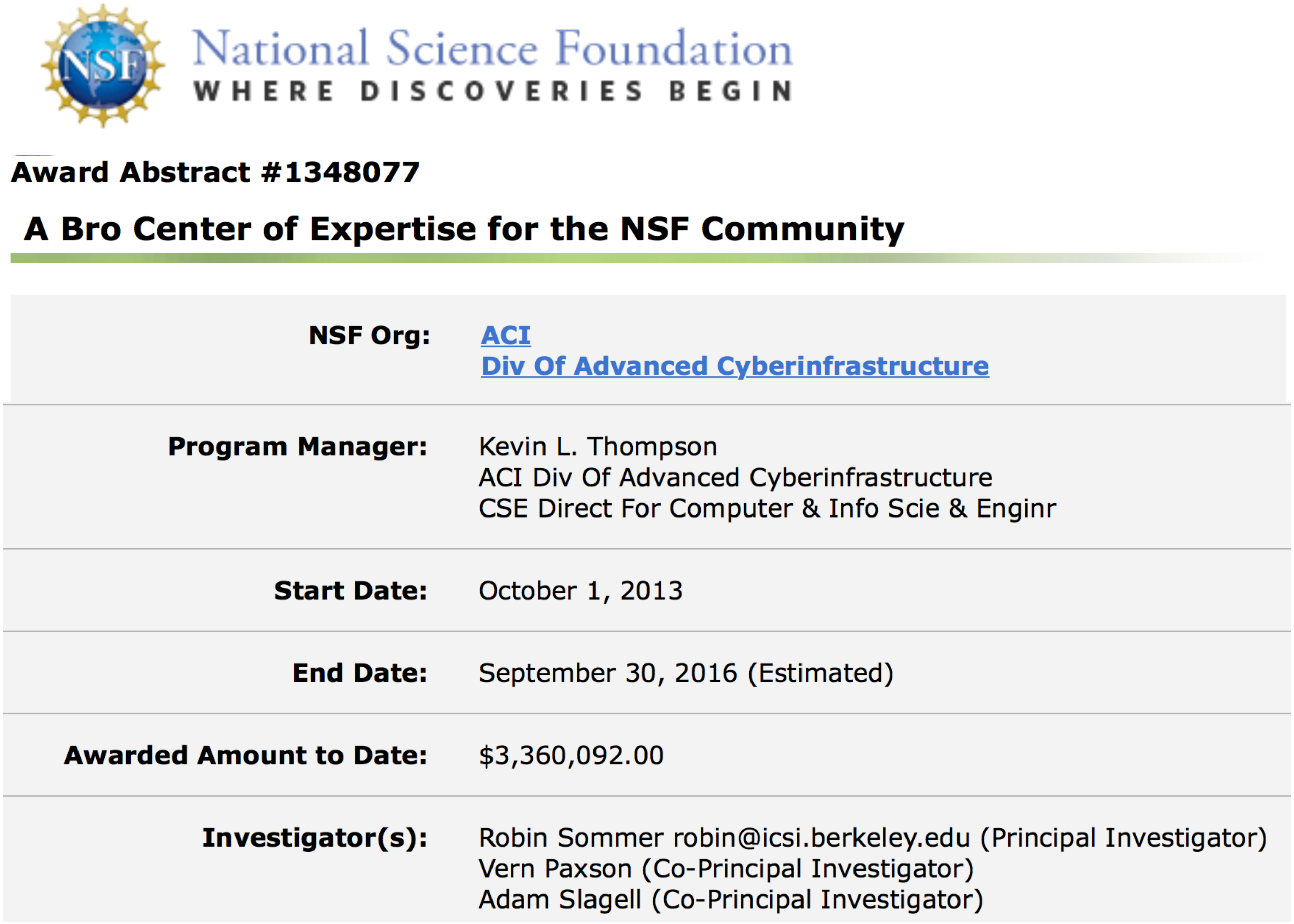


National Science Foundation
WHERE DISCOVERIES BEGIN

Award Abstract #1348077

A Bro Center of Expertise for the NSF Community

NSF Org:	ACI Div Of Advanced Cyberinfrastructure
Program Manager:	Kevin L. Thompson ACI Div Of Advanced Cyberinfrastructure CSE Direct For Computer & Info Scie & Enginr
Start Date:	October 1, 2013
End Date:	September 30, 2016 (Estimated)
Awarded Amount to Date:	$3,729,977 ?
Investigator(s):	Robin Sommer robin@icsi.berkeley.edu (Principal Investigator) Vern Paxson (Co-Principal Investigator) Adam Slagell (Co-Principal Investigator)



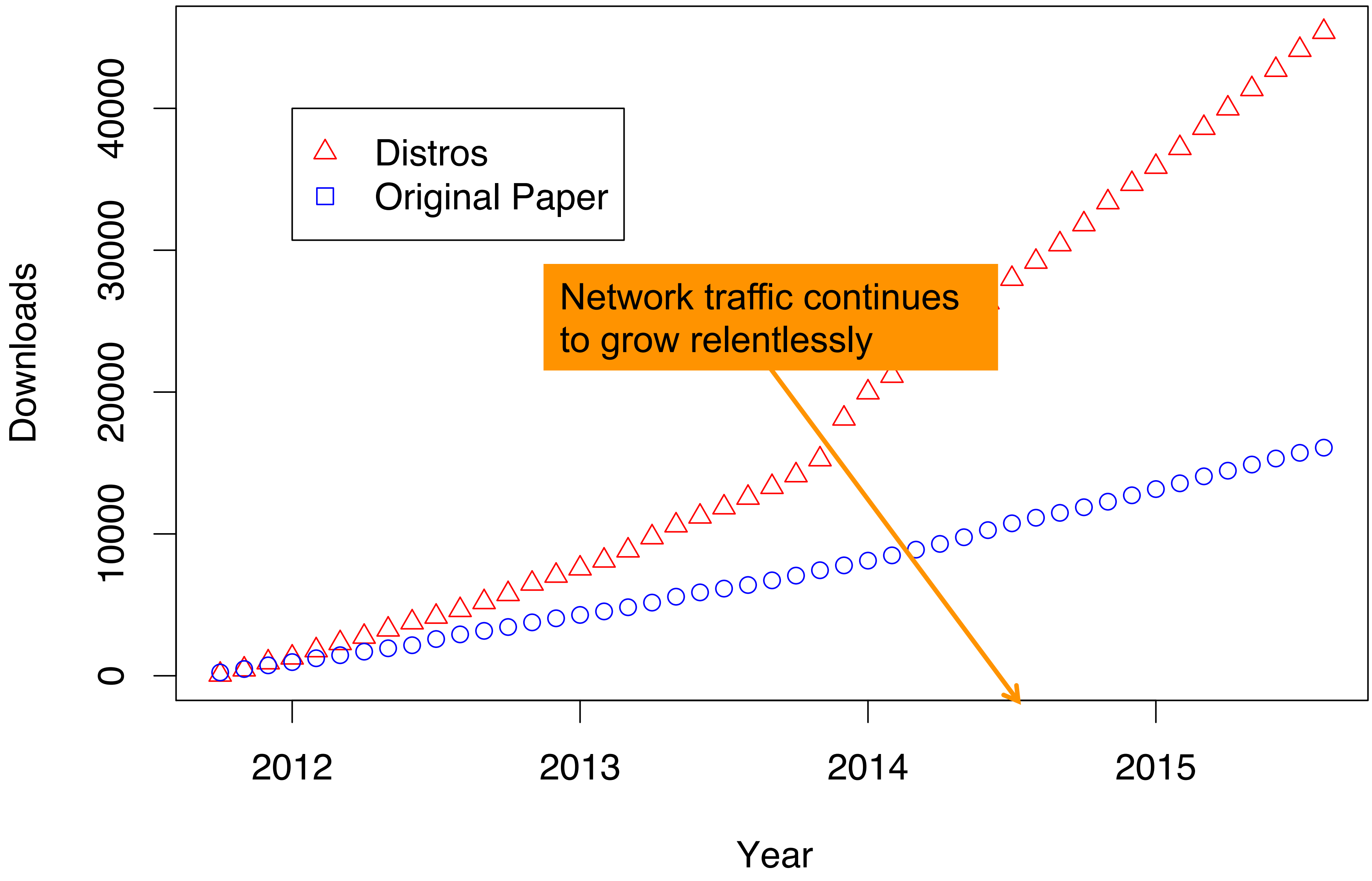
National Science Foundation
WHERE DISCOVERIES BEGIN

Award Abstract #1348077

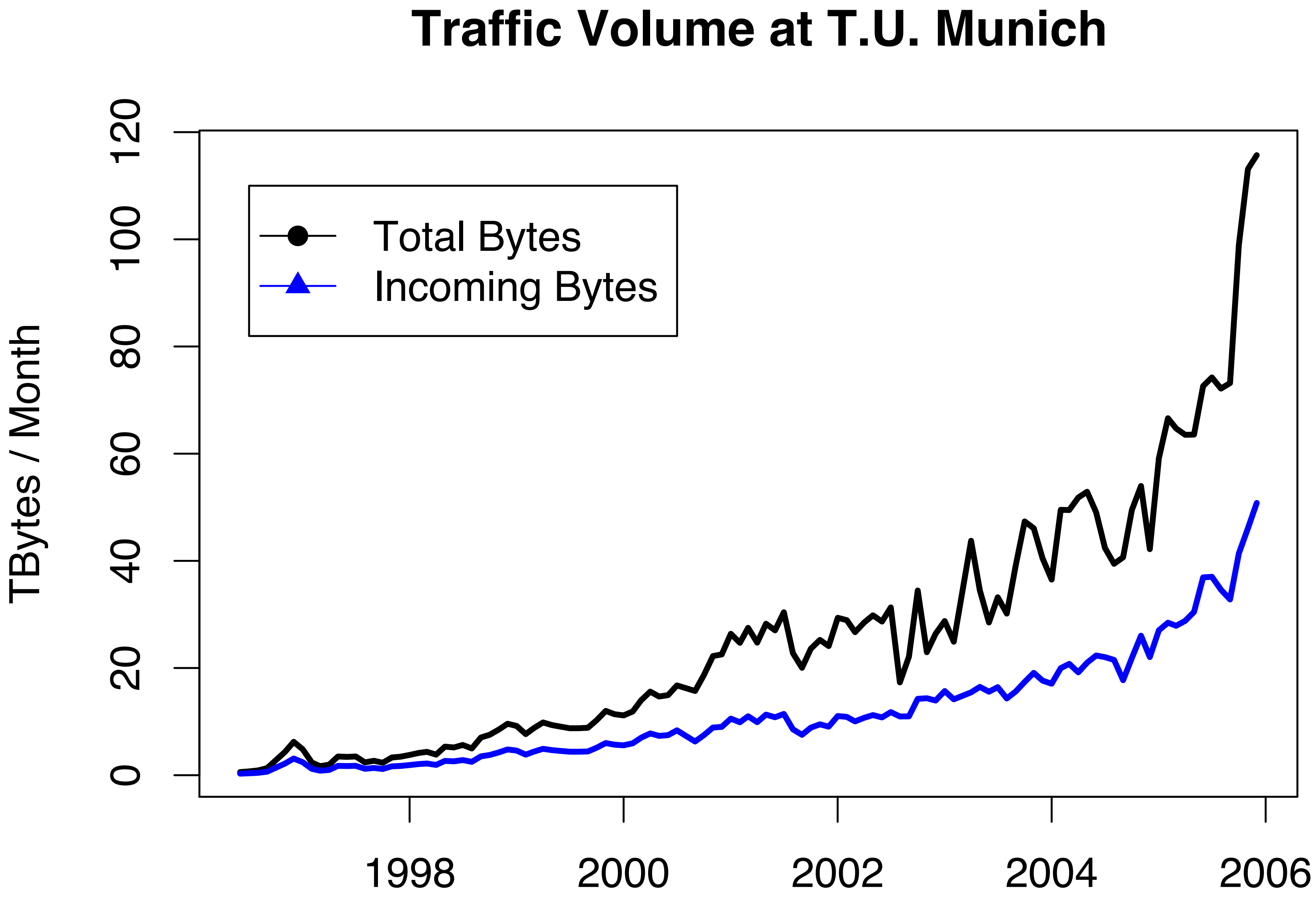
A Bro Center of Expertise for the NSF Community

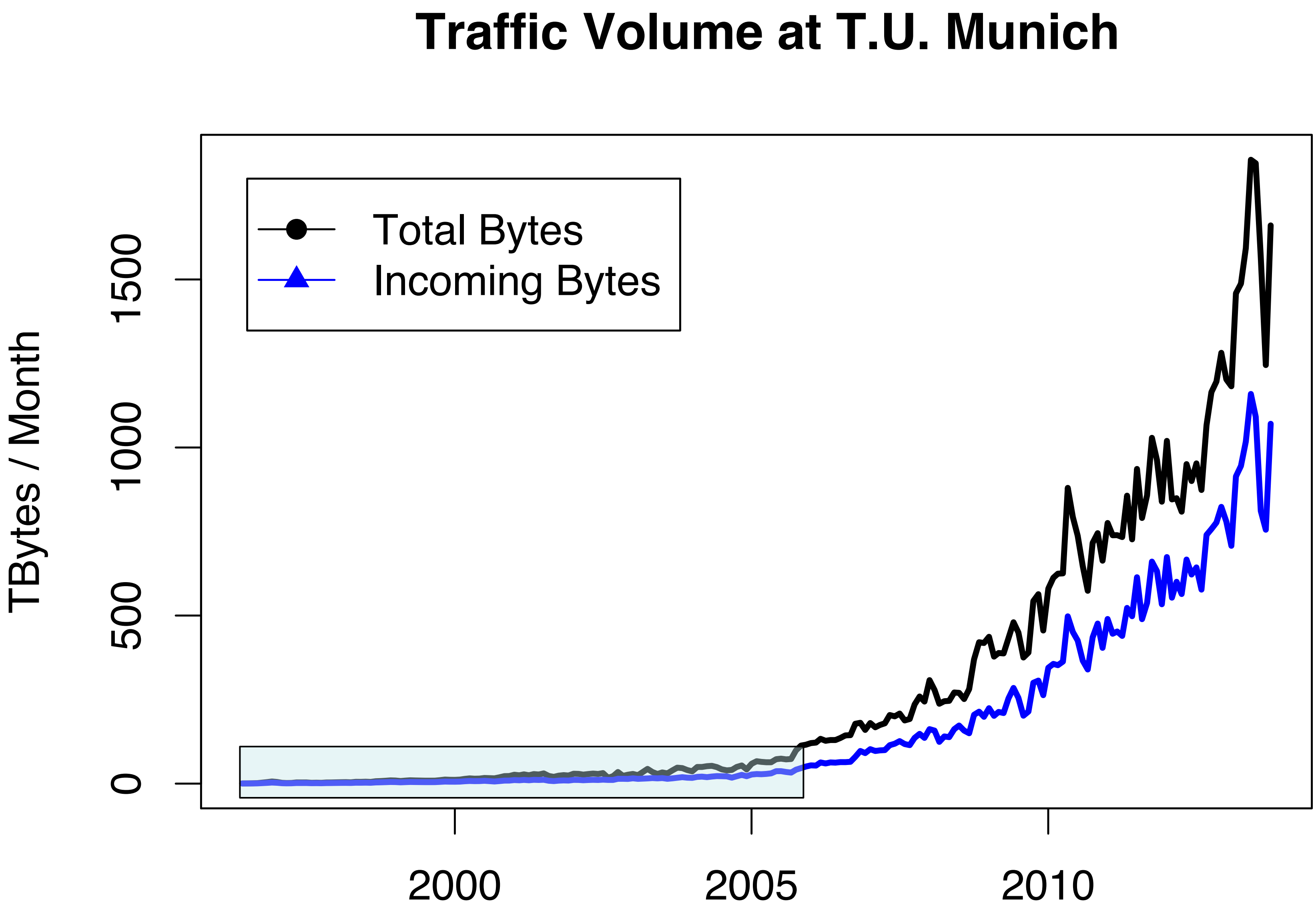
NSF Org:	ACI Div Of Advanced Cyberinfrastructure
Program Manager:	Kevin L. Thompson ACI Div Of Advanced Cyberinfrastructure CSE Direct For Computer & Info Scie & Enginr
Start Date:	October 1, 2013
End Date:	September 30, 2016 (Estimated)
Awarded Amount to Date:	$3,360,092.00
Investigator(s):	Robin Sommer robin@icsi.berkeley.edu (Principal Investigator) Vern Paxson (Co-Principal Investigator) Adam Slagell (Co-Principal Investigator)

Interest in Bro

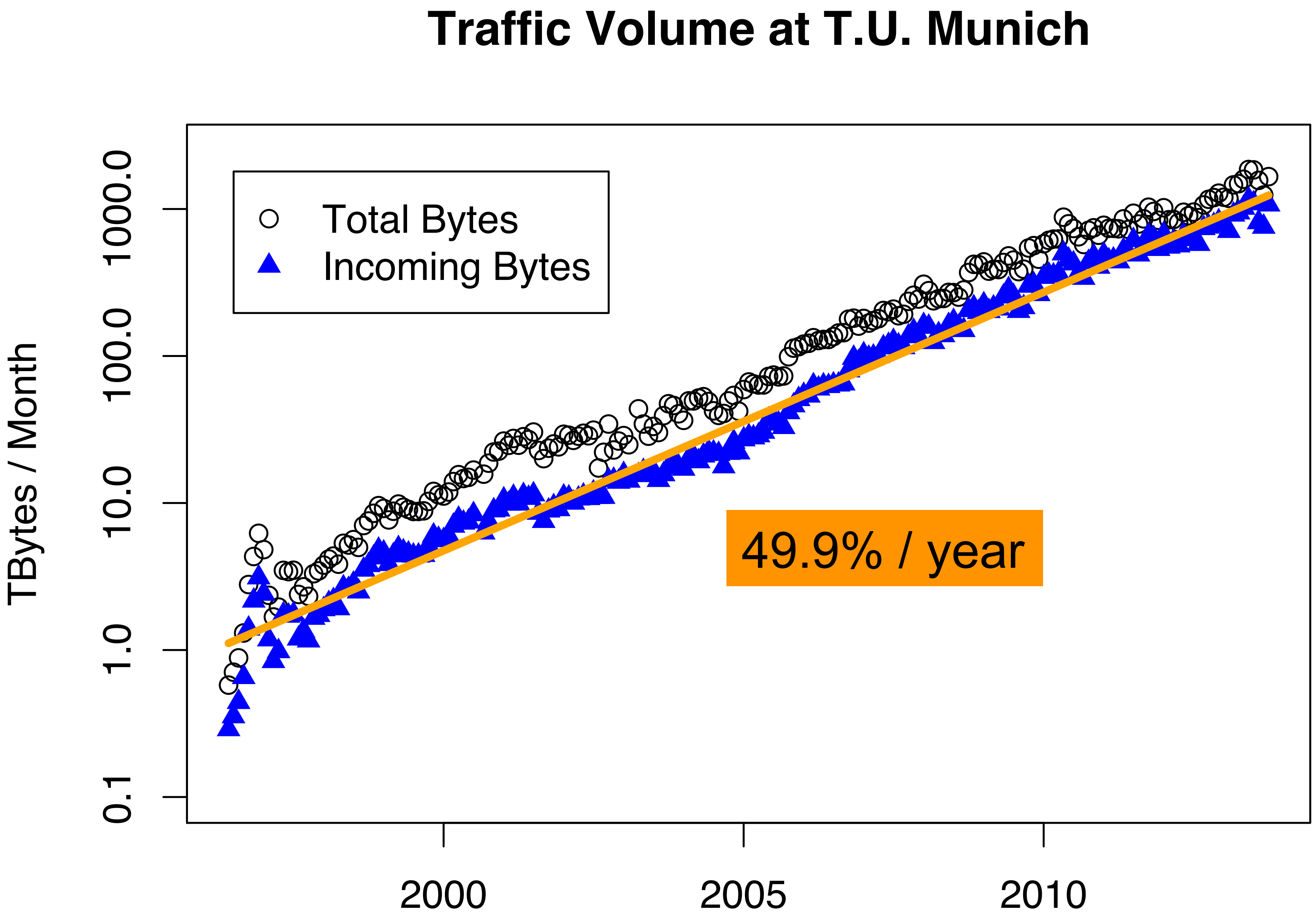


Network traffic continues to grow relentlessly

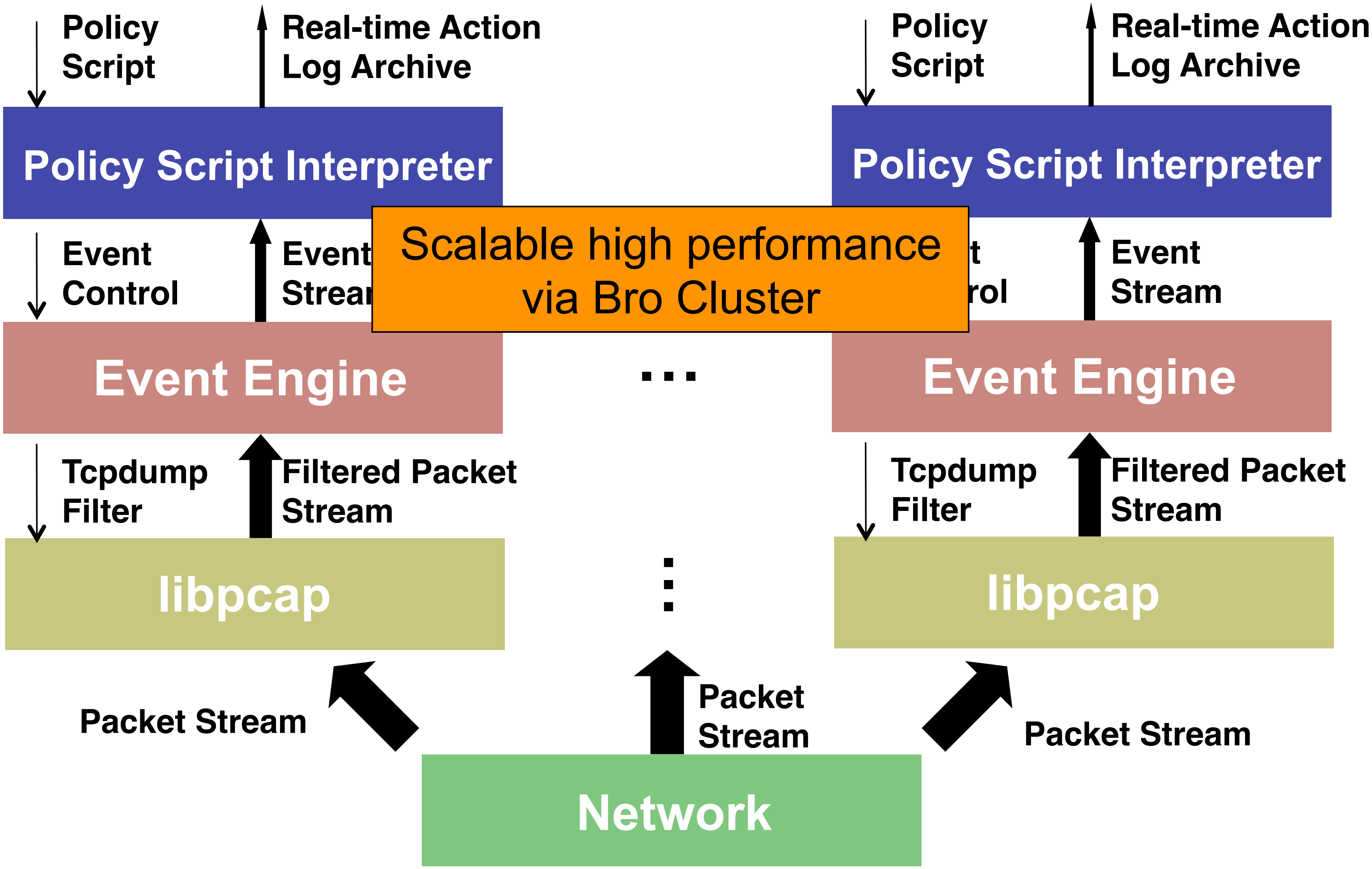

Traffic Volume at T.U. Munich
TBytes / Month
0
20
40
60
80
100
120
1998
2000
2002
2004
2006
● Total Bytes
▲ Incoming Bytes



Traffic Volume at T.U. Munich
● Total Bytes
▲ Incoming Bytes
TBytes / Month
0
500
1000
1500
2000
2005
2010

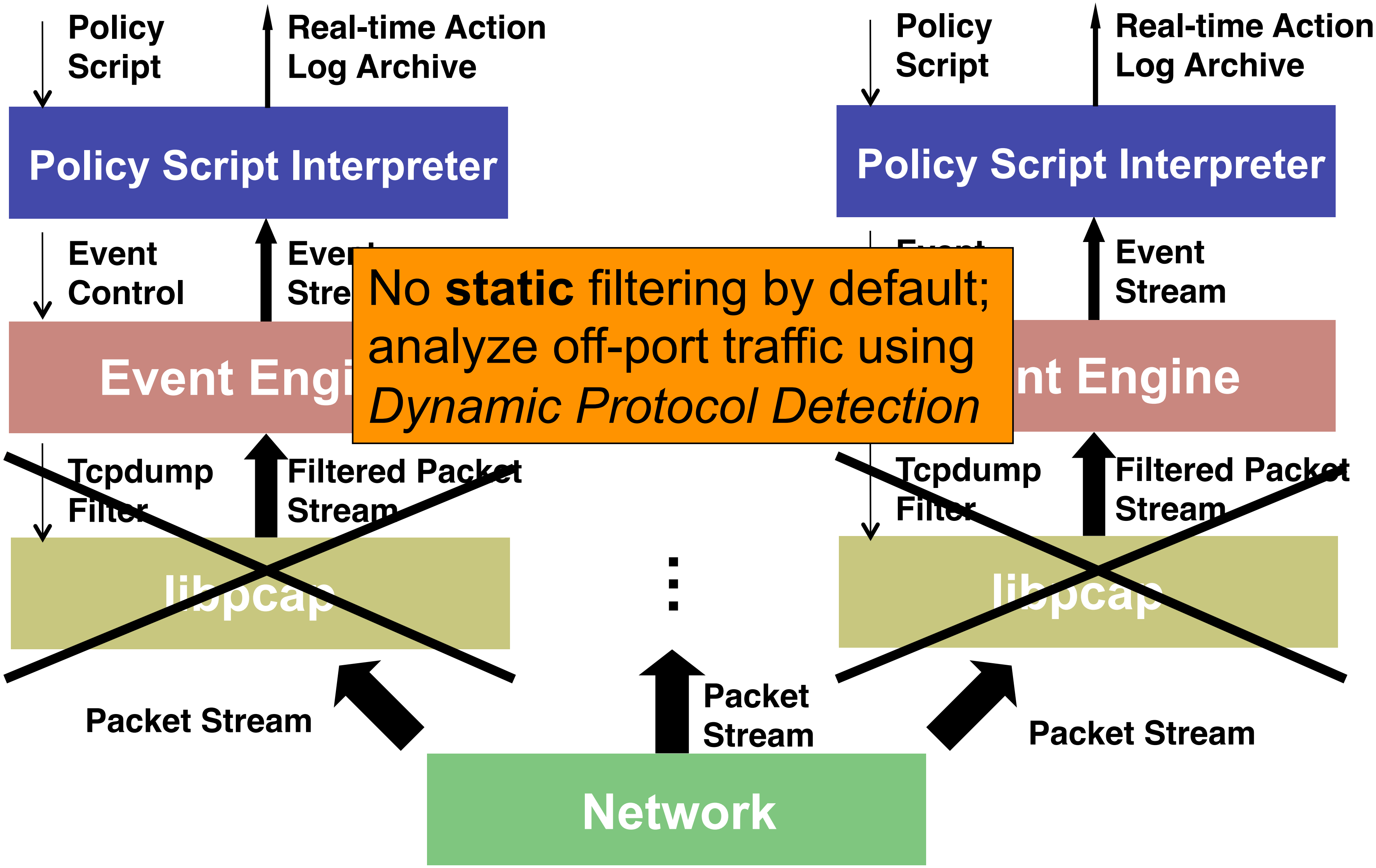

Traffic Volume at T.U. Munich
Total Bytes
Incoming Bytes
49.9% / year
TBytes / Month
0.1
1.0
10.0
100.0
1000.0
2000
2005
2010

Architecture As It Has Evolved



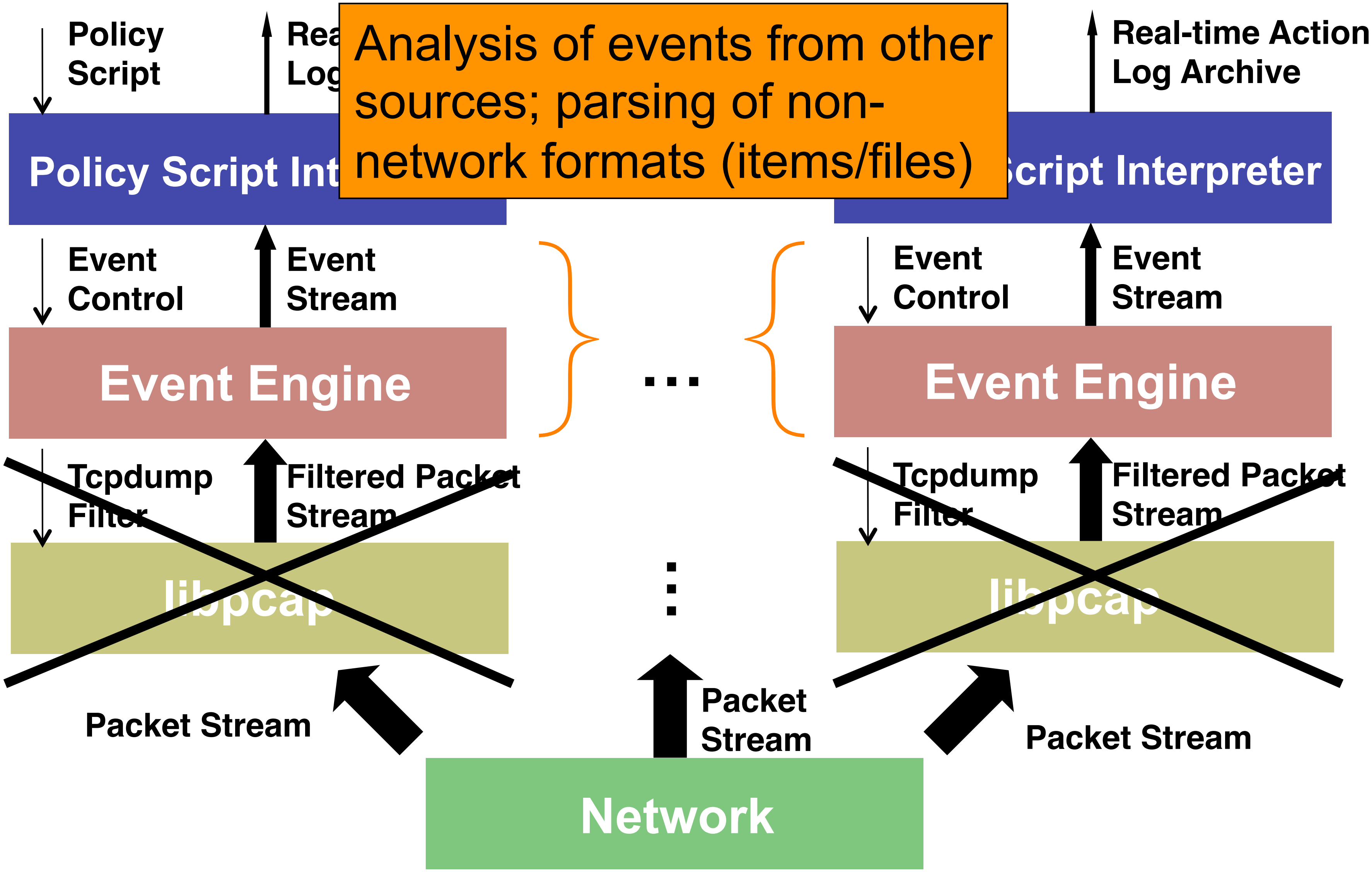
Scalable high performance via Bro Cluster

Architecture As It Has Evolved

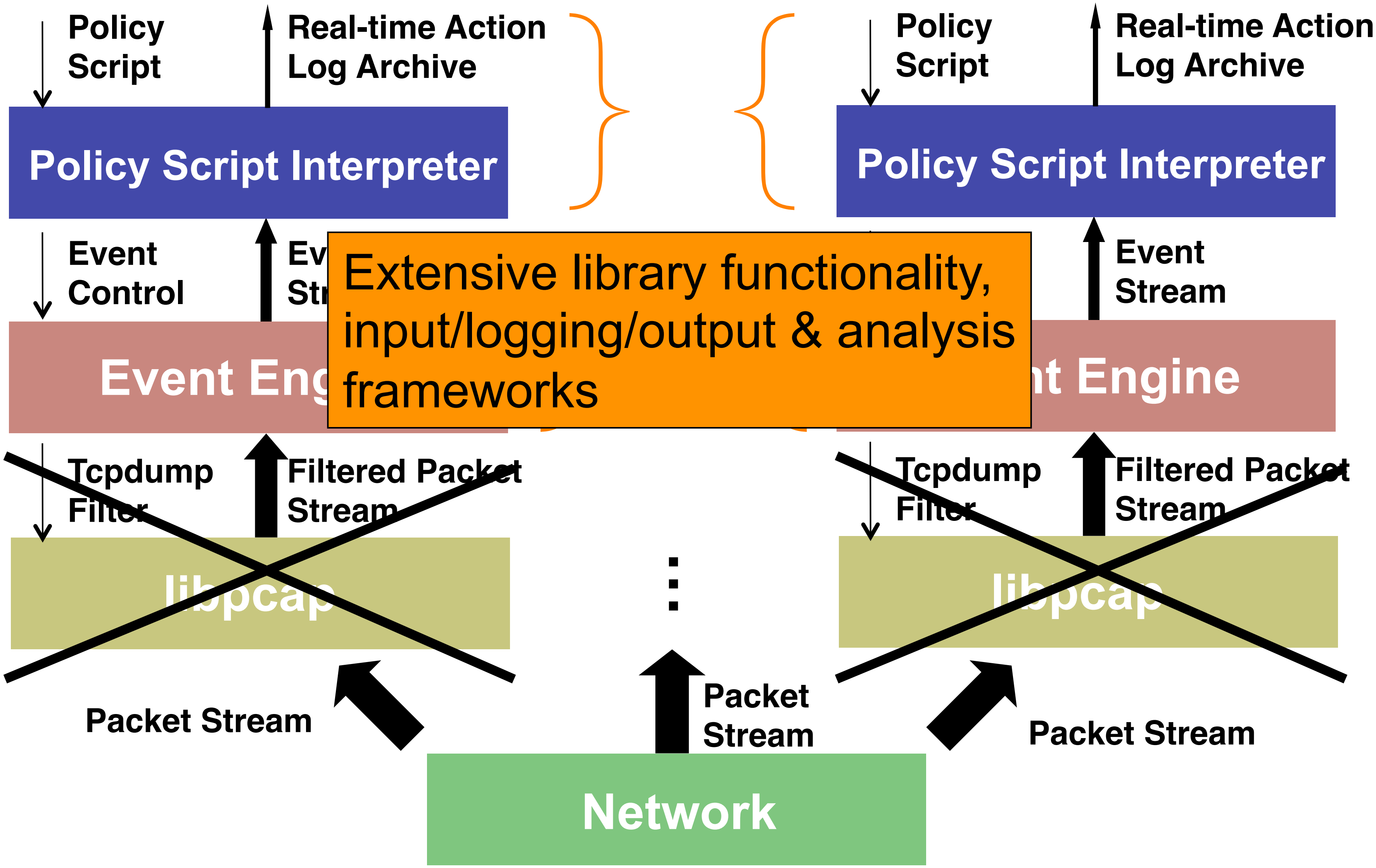


No **static** filtering by default; analyze off-port traffic using *Dynamic Protocol Detection*

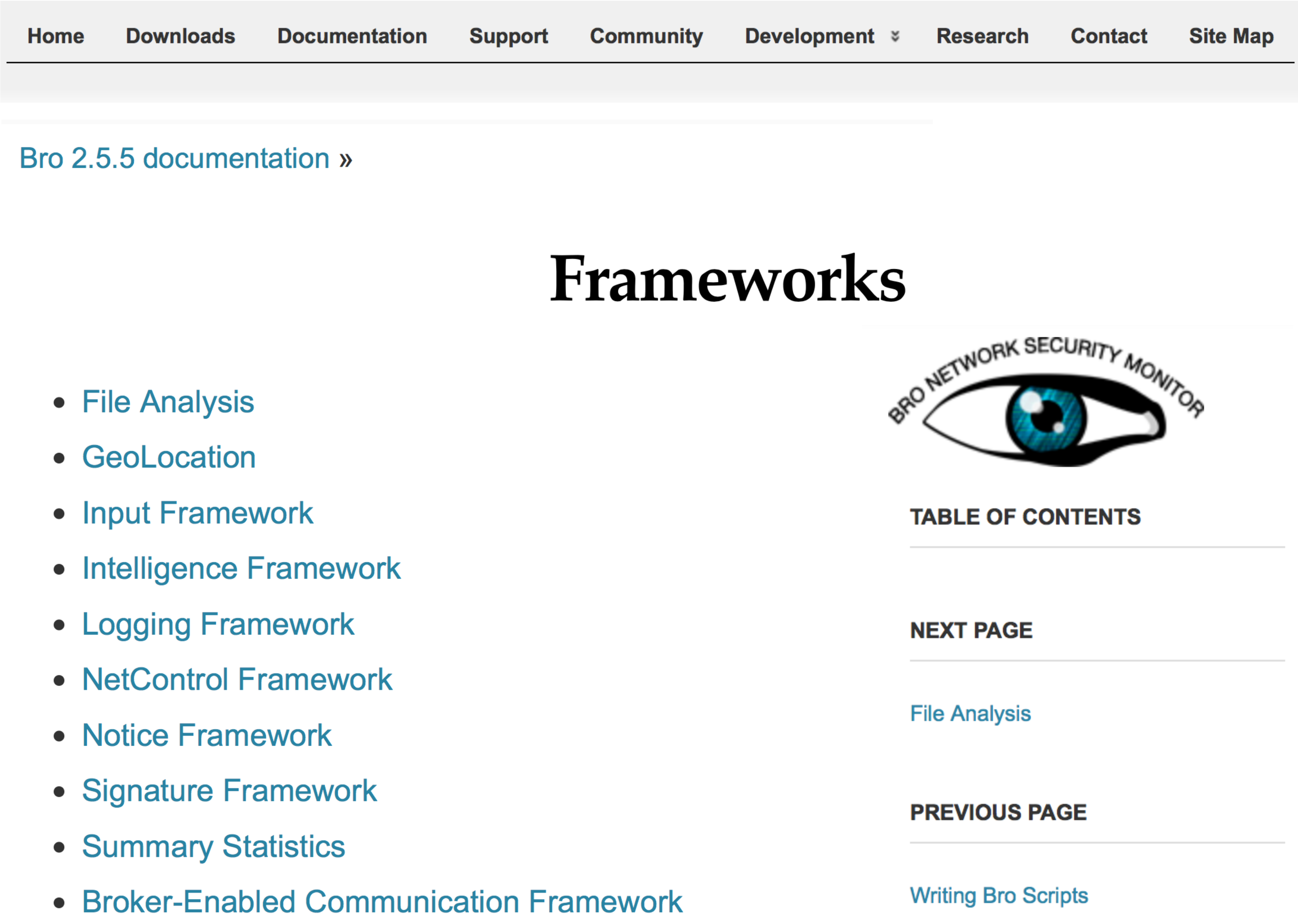
Architecture As It Has Evolved



Architecture As It Has Evolved



Extensive library functionality, input/logging/output & analysis frameworks



Home Downloads Documentation Support Community Development Research Contact Site Map

Bro 2.5.5 documentation »

Frameworks

TABLE OF CONTENTS

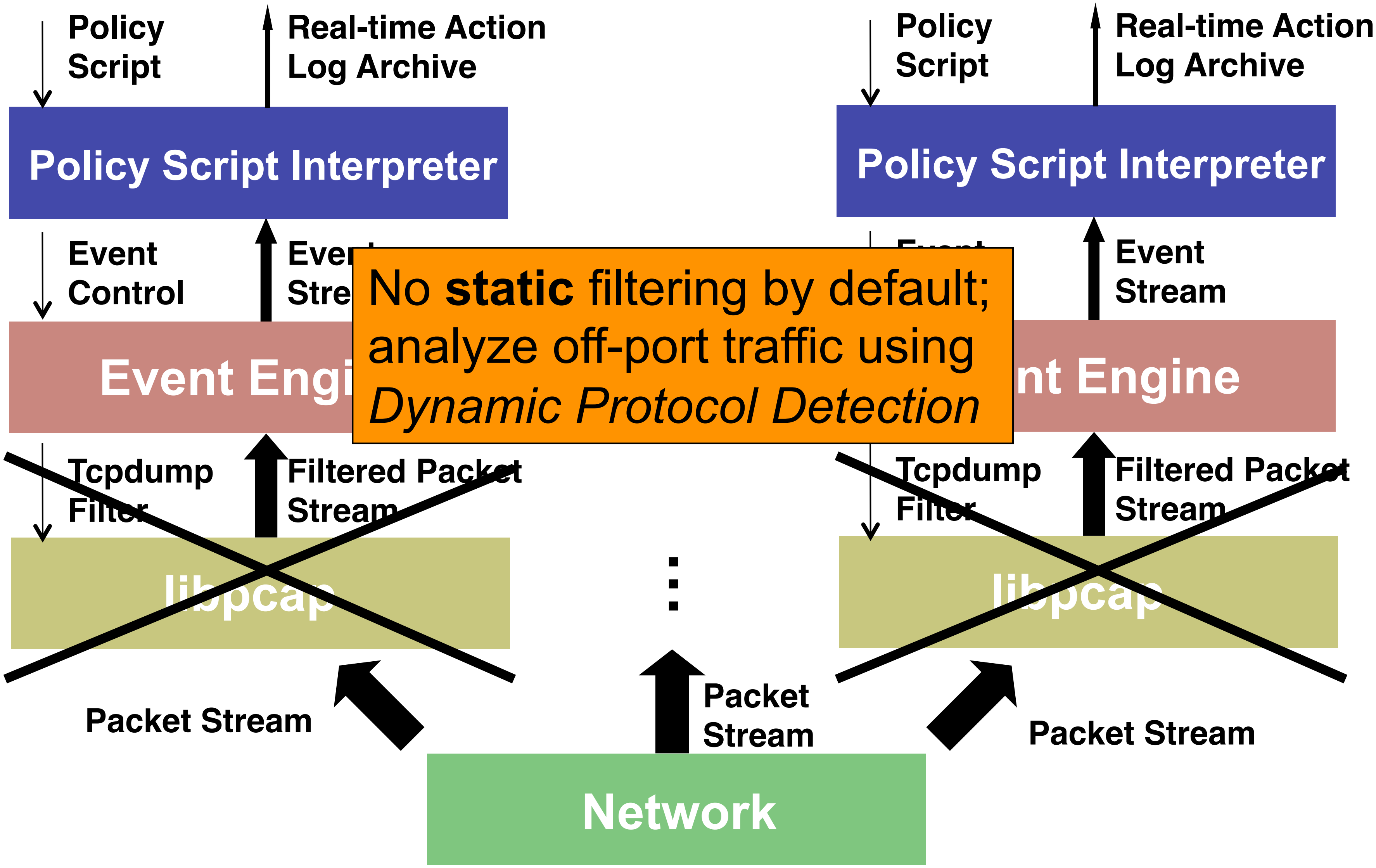
NEXT PAGE

File Analysis

PREVIOUS PAGE

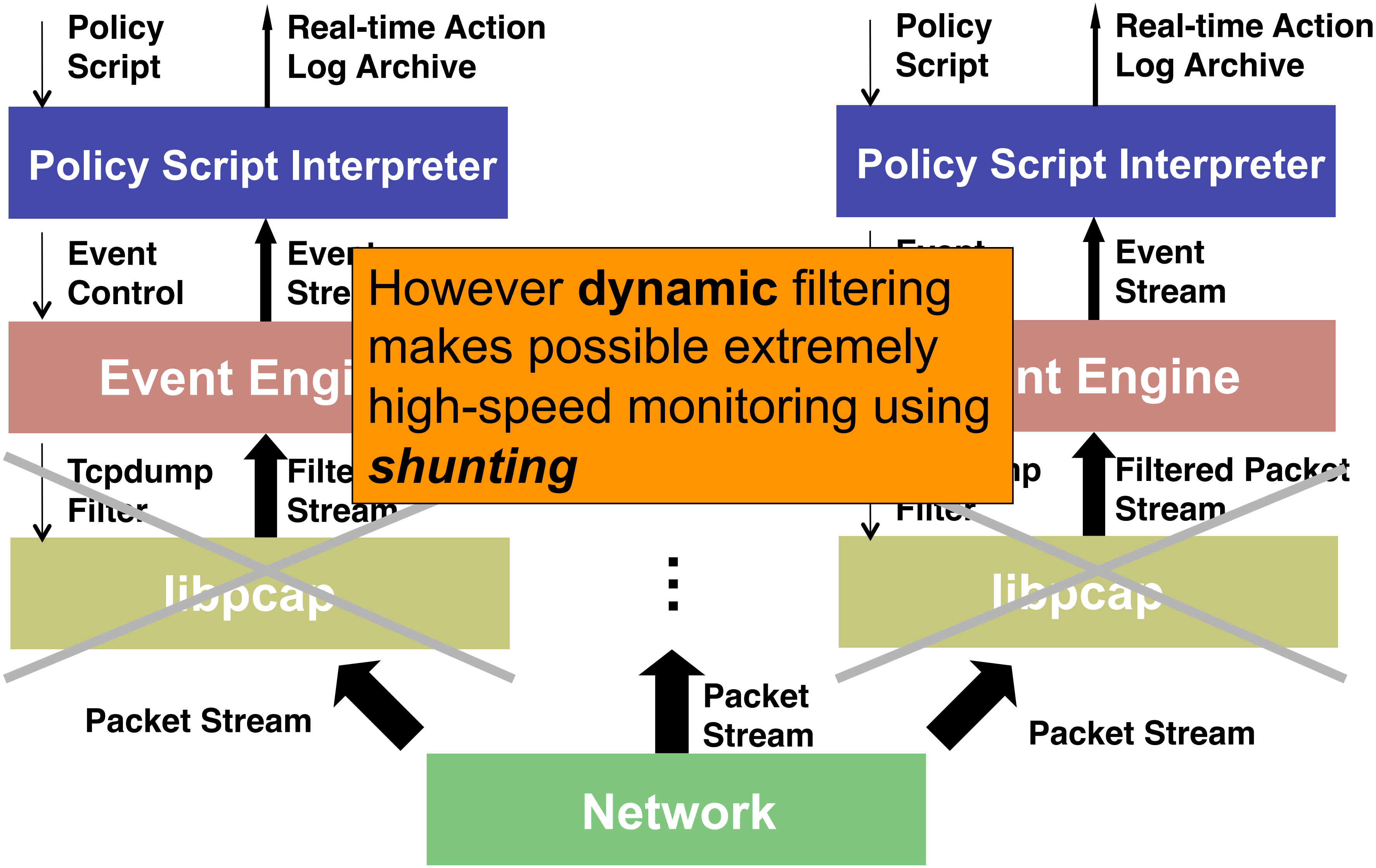
Writing Bro Scripts

Architecture As It Has Evolved



No **static** filtering by default; analyze off-port traffic using *Dynamic Protocol Detection*

Architecture As It Has Evolved



However **dynamic** filtering makes possible extremely high-speed monitoring using ***shunting***

U.S. DEPARTMENT OF ENERGY

UNIVERSITY OF CALIFORNIA

100G Monitoring

"You get to drink from the firehose!"

Aashish Sharma
Vincent Stoffer

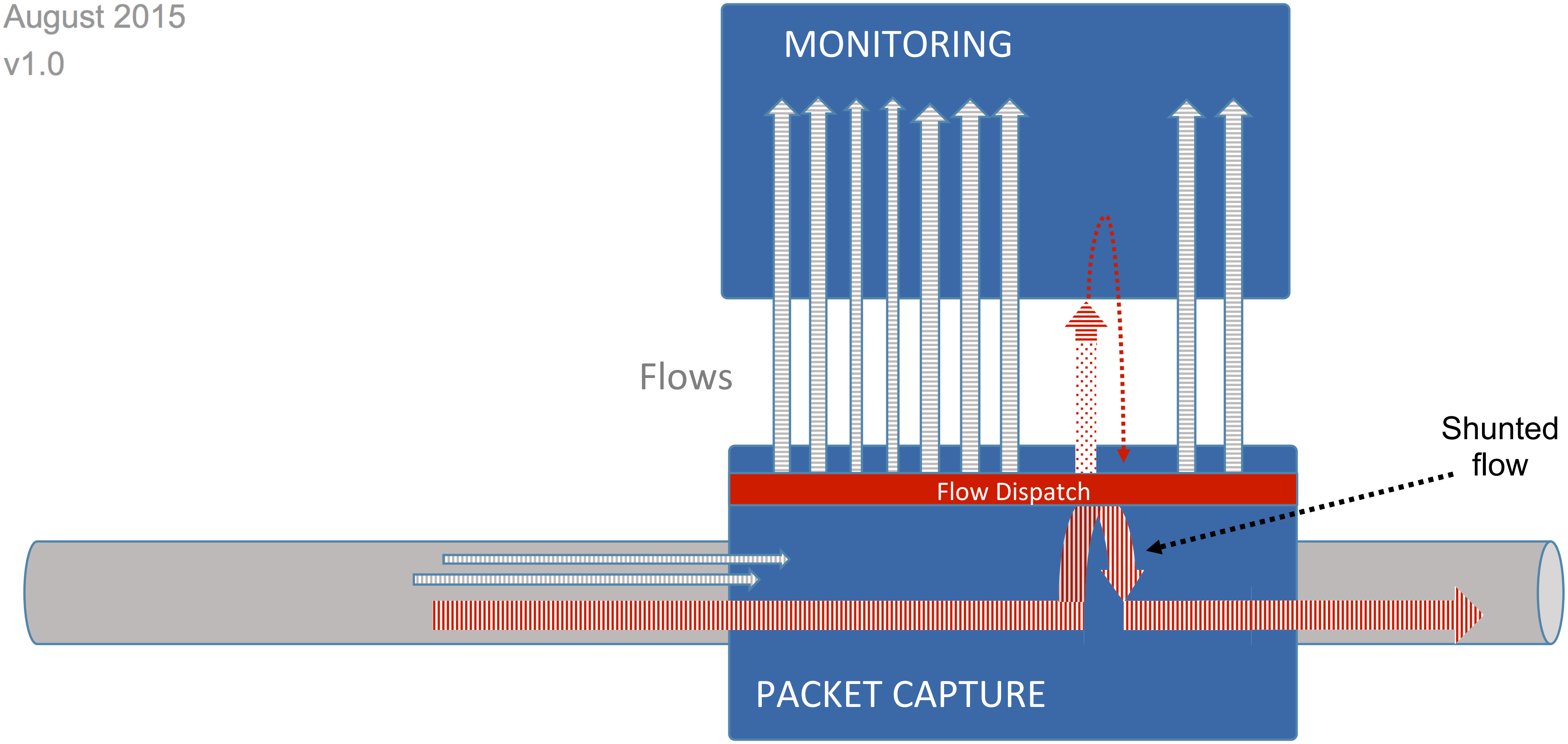
Bro4Pros
February 19th, 2015
OpenDNS, SF

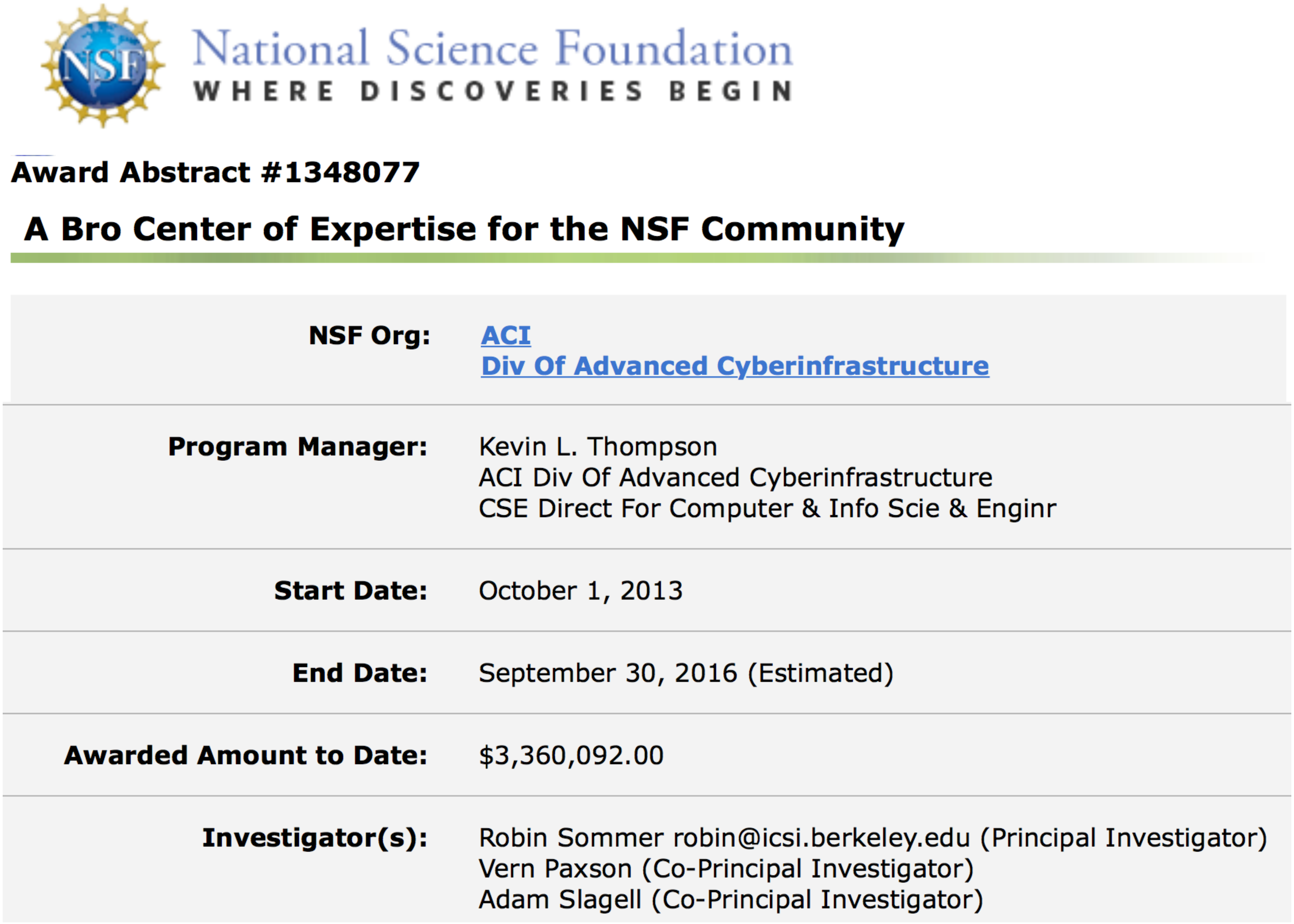
BERKELEY LAB

100G Intrusion Detection

August 2015

v1.0



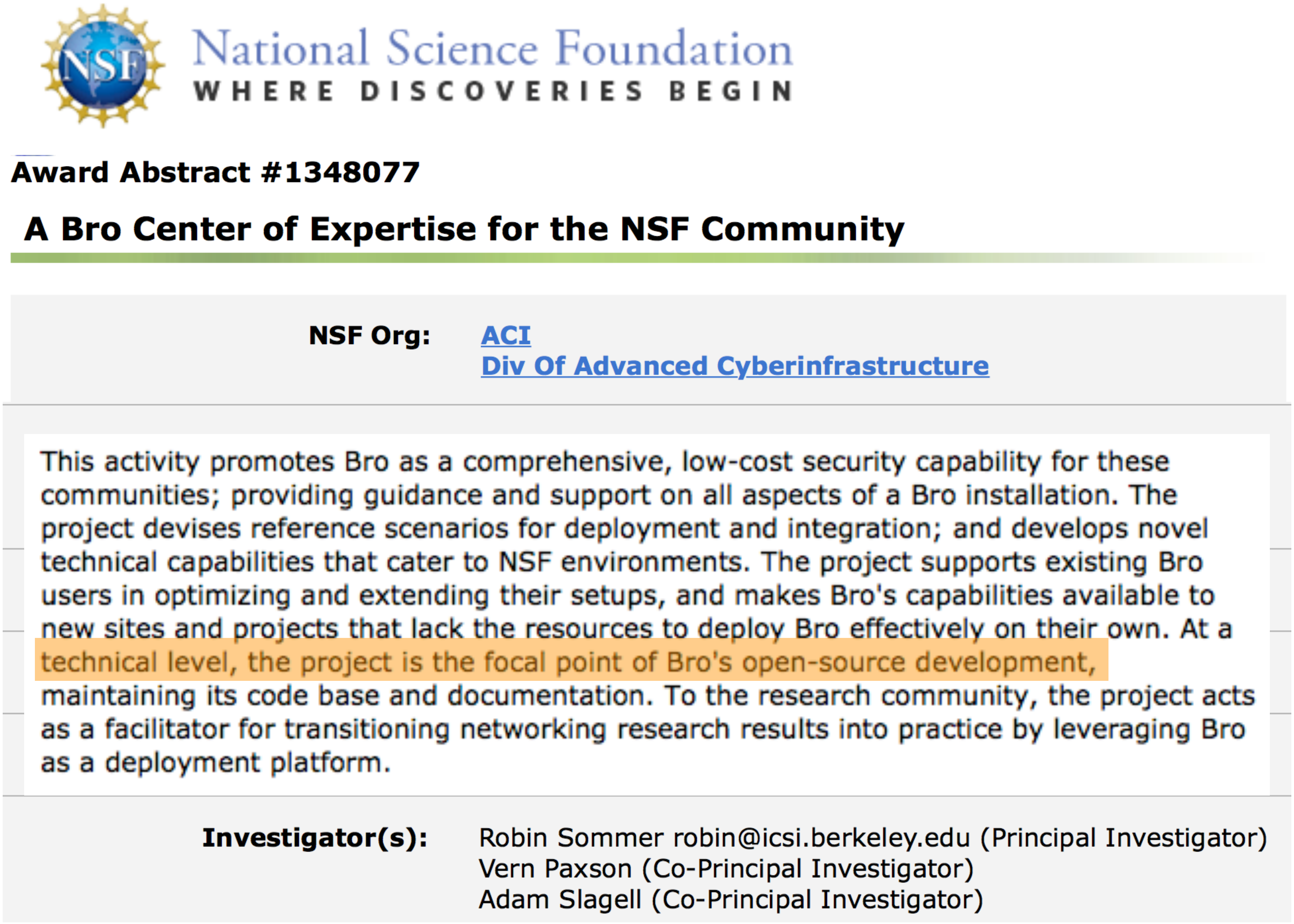


National Science Foundation
WHERE DISCOVERIES BEGIN

Award Abstract #1348077

A Bro Center of Expertise for the NSF Community

NSF Org:	ACI Div Of Advanced Cyberinfrastructure
Program Manager:	Kevin L. Thompson ACI Div Of Advanced Cyberinfrastructure CSE Direct For Computer & Info Scie & Enginr
Start Date:	October 1, 2013
End Date:	September 30, 2016 (Estimated)
Awarded Amount to Date:	$3,360,092.00
Investigator(s):	Robin Sommer robin@icsi.berkeley.edu (Principal Investigator) Vern Paxson (Co-Principal Investigator) Adam Slagell (Co-Principal Investigator)



National Science Foundation
WHERE DISCOVERIES BEGIN

Award Abstract #1348077

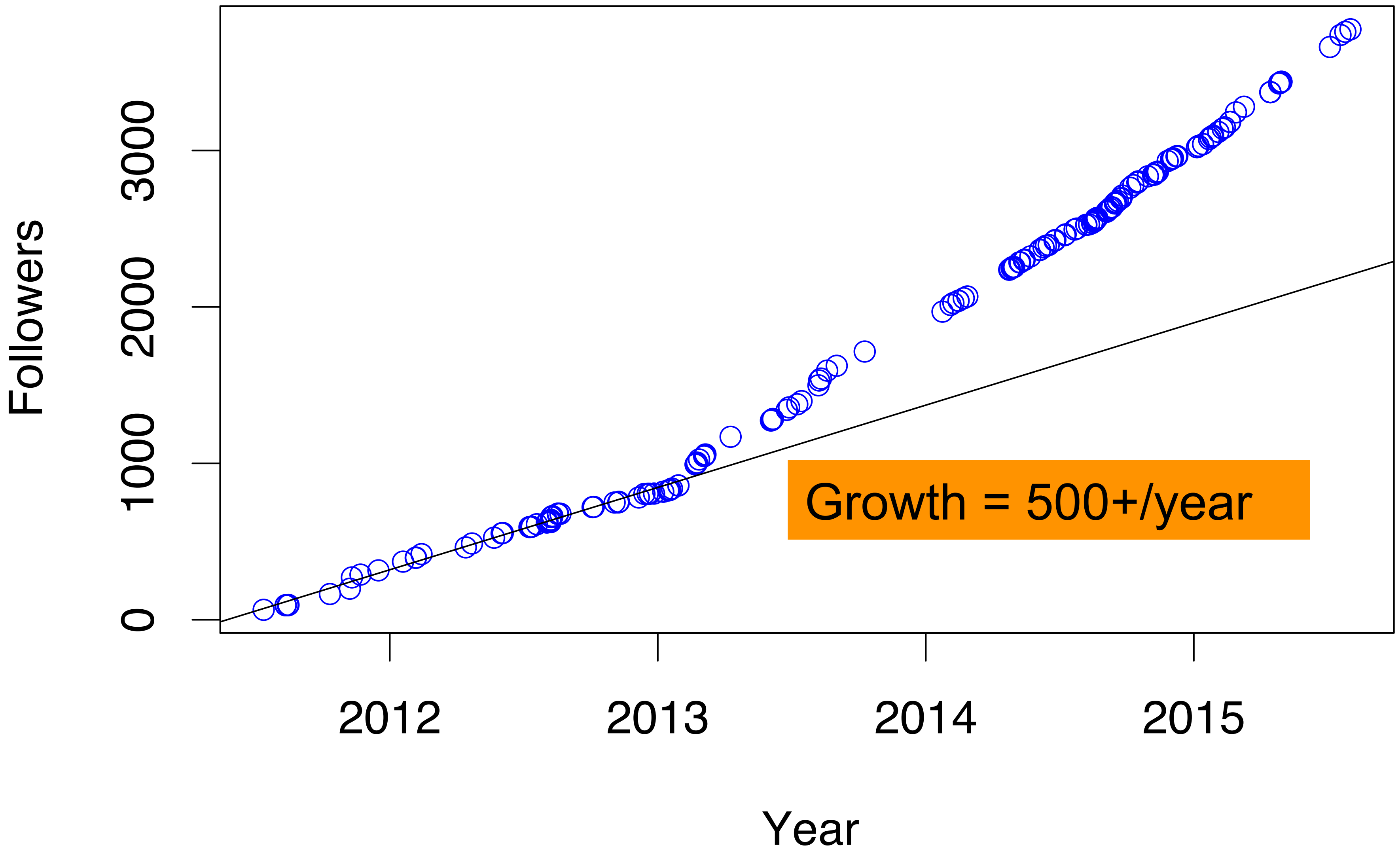
A Bro Center of Expertise for the NSF Community

NSF Org: ACI
Div Of Advanced Cyberinfrastructure

This activity promotes Bro as a comprehensive, low-cost security capability for these communities; providing guidance and support on all aspects of a Bro installation. The project devises reference scenarios for deployment and integration; and develops novel technical capabilities that cater to NSF environments. The project supports existing Bro users in optimizing and extending their setups, and makes Bro's capabilities available to new sites and projects that lack the resources to deploy Bro effectively on their own. At a technical level, the project is the focal point of Bro's open-source development, maintaining its code base and documentation. To the research community, the project acts as a facilitator for transitioning networking research results into practice by leveraging Bro as a deployment platform.

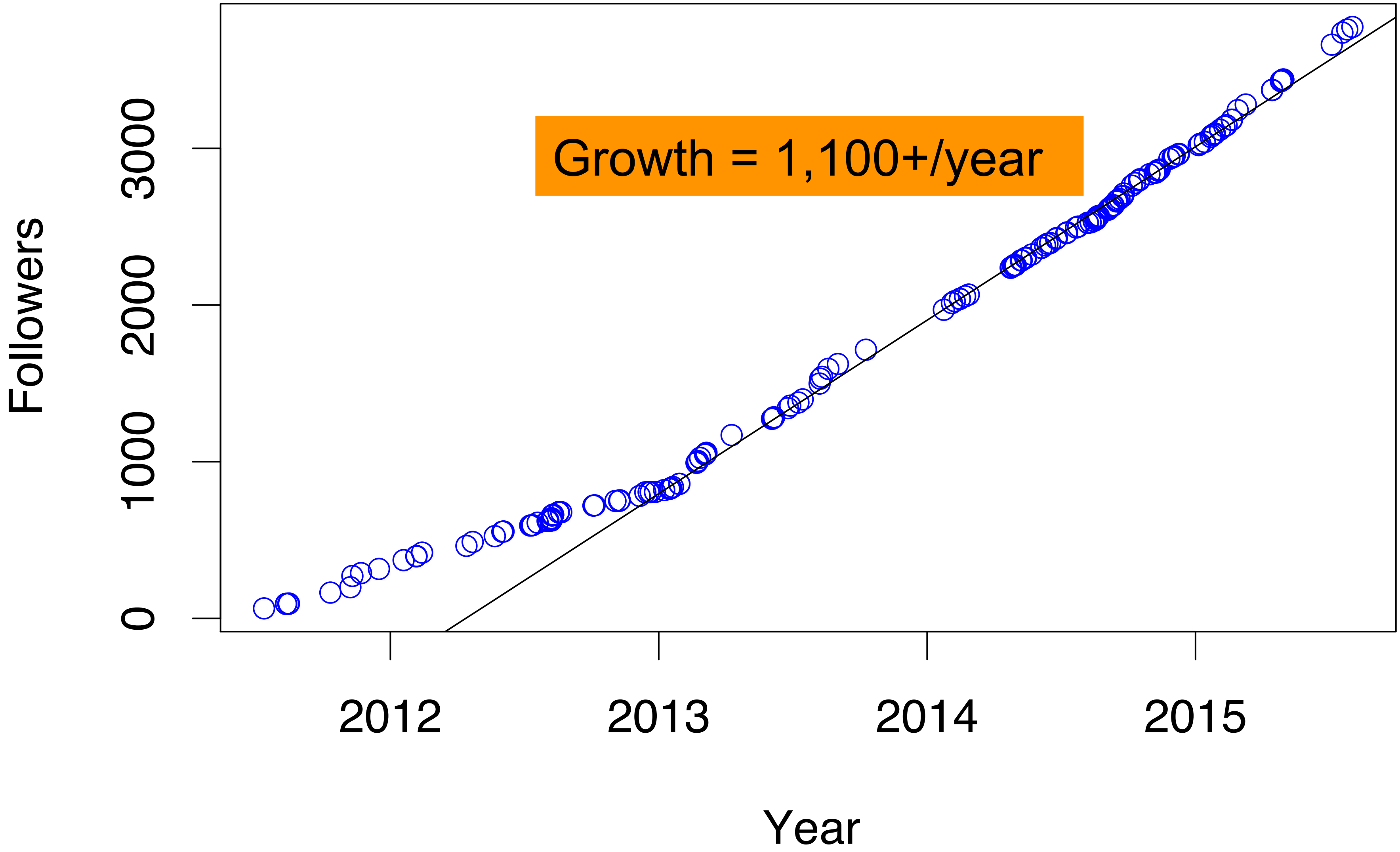
Investigator(s): Robin Sommer robin@icsi.berkeley.edu (Principal Investigator)
Vern Paxson (Co-Principal Investigator)
Adam Slagell (Co-Principal Investigator)

@Bro_IDS Twitter Followers

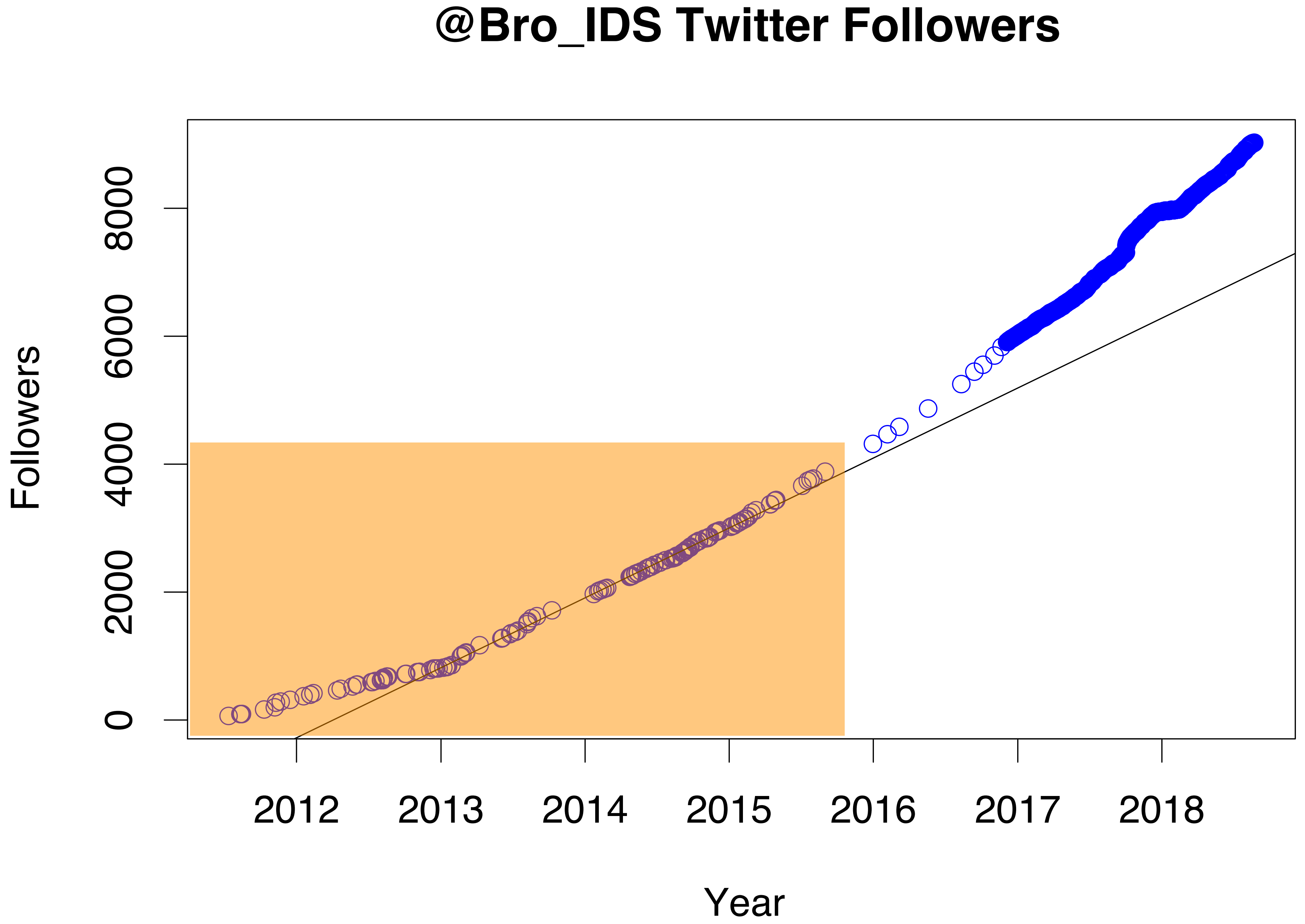


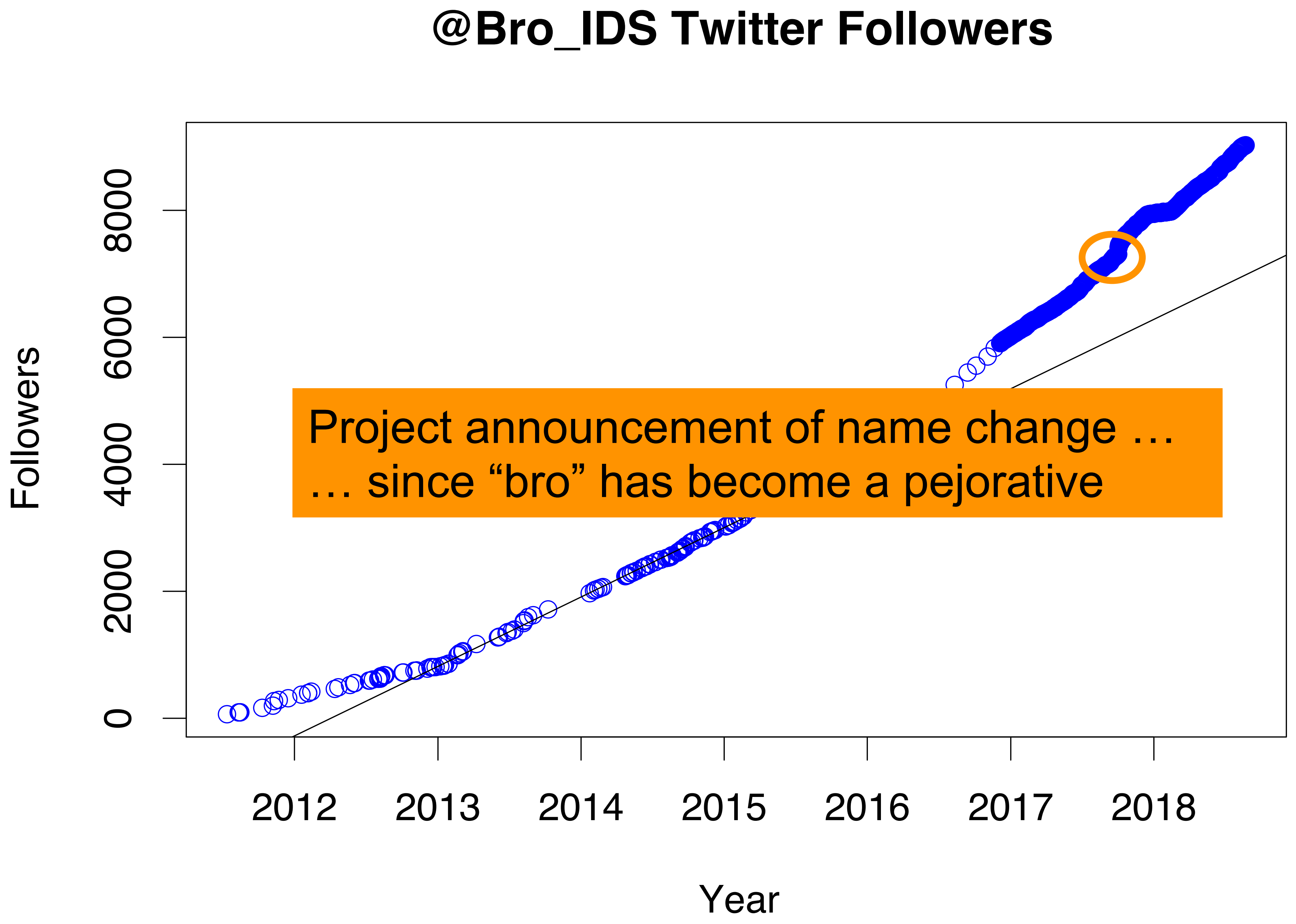
Growth = 500+/year

@Bro_IDS Twitter Followers



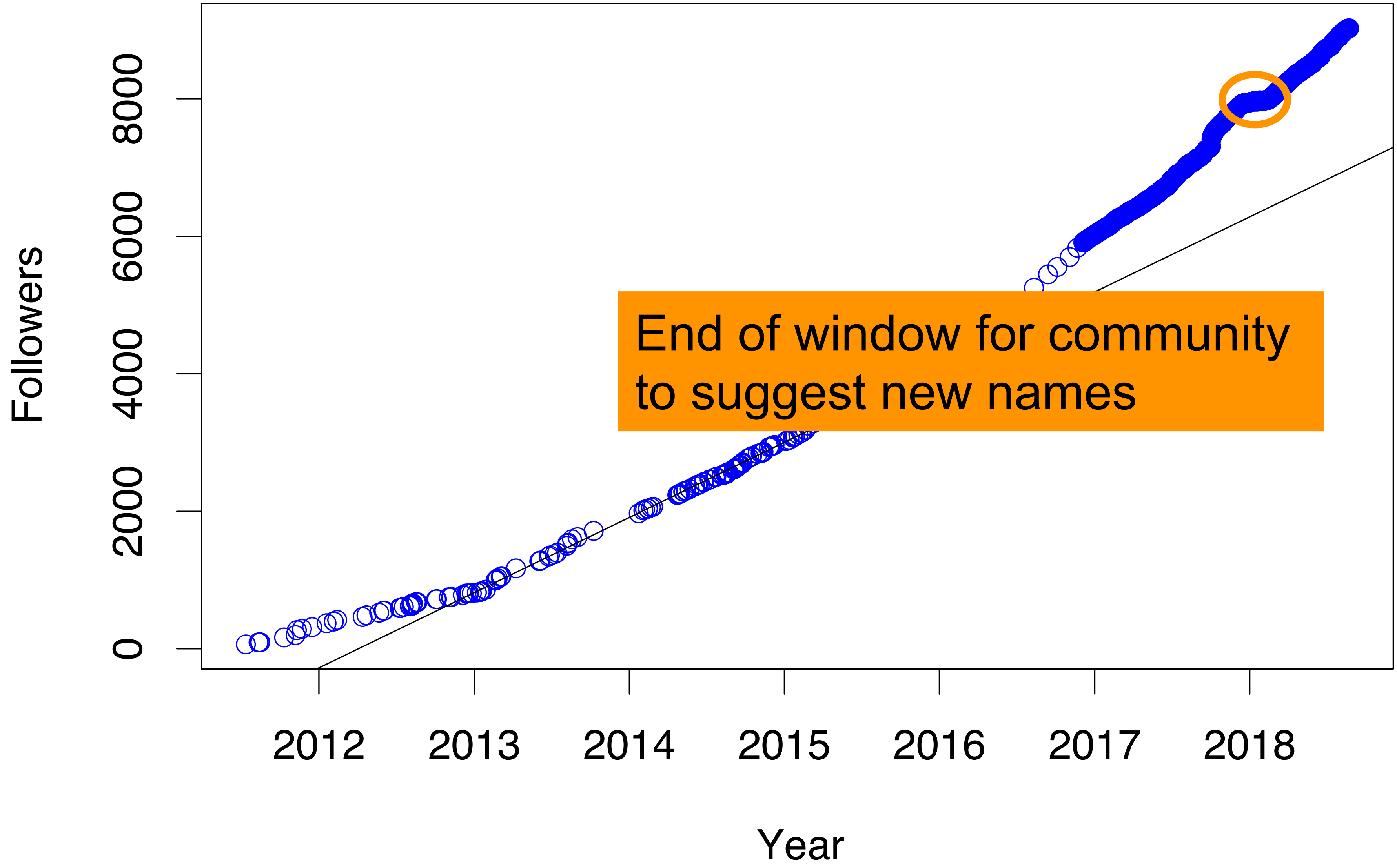
Growth = 1,100+/year


@Bro_IDS Twitter Followers
Followers
0
2000
4000
6000
8000
2012
2013
2014
2015
2016
2017
2018
Year



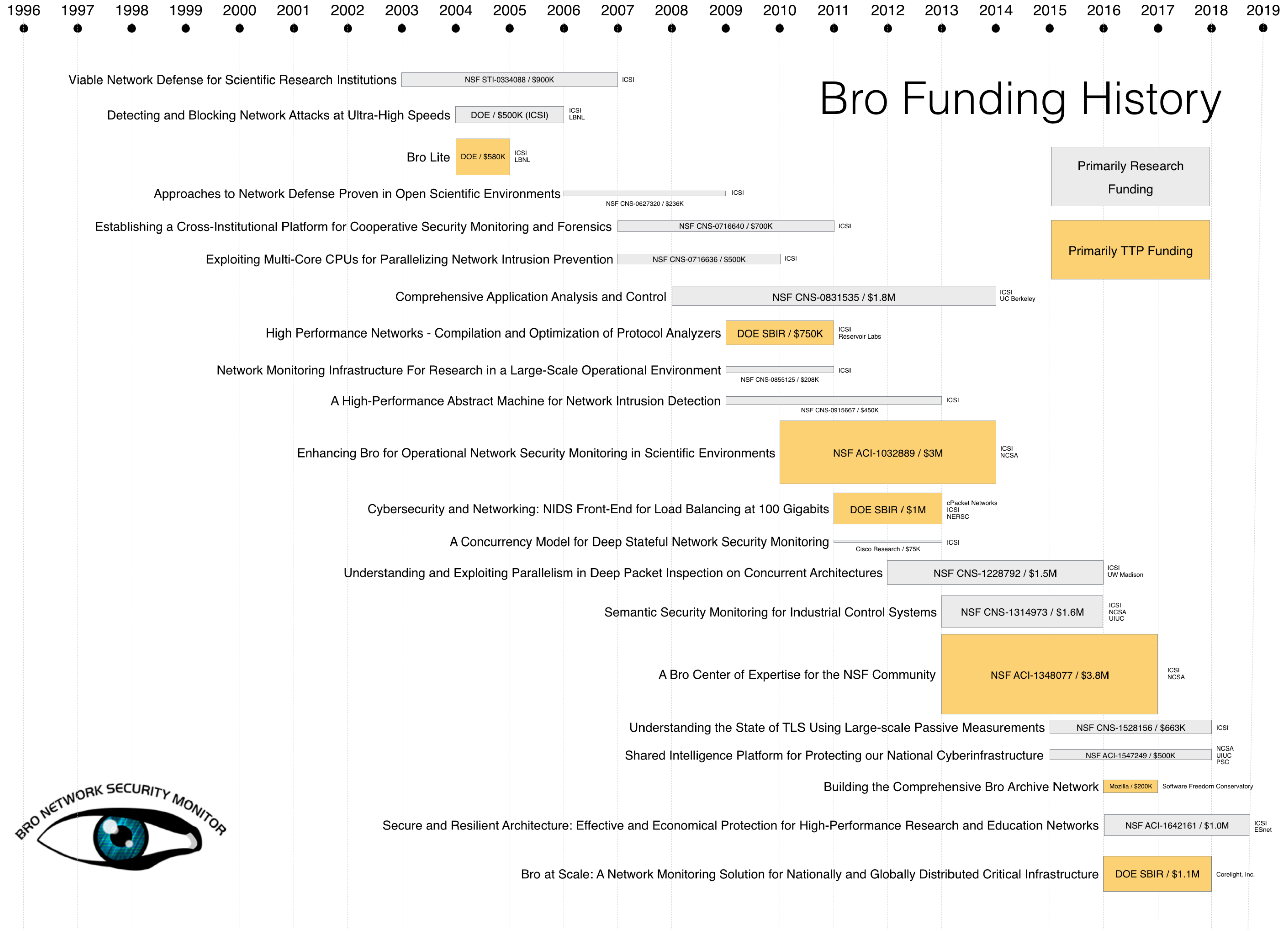
Project announcement of name change …
… since “bro” has become a pejorative

@Bro_IDS Twitter Followers



End of window for community to suggest new names

Bro Funding History

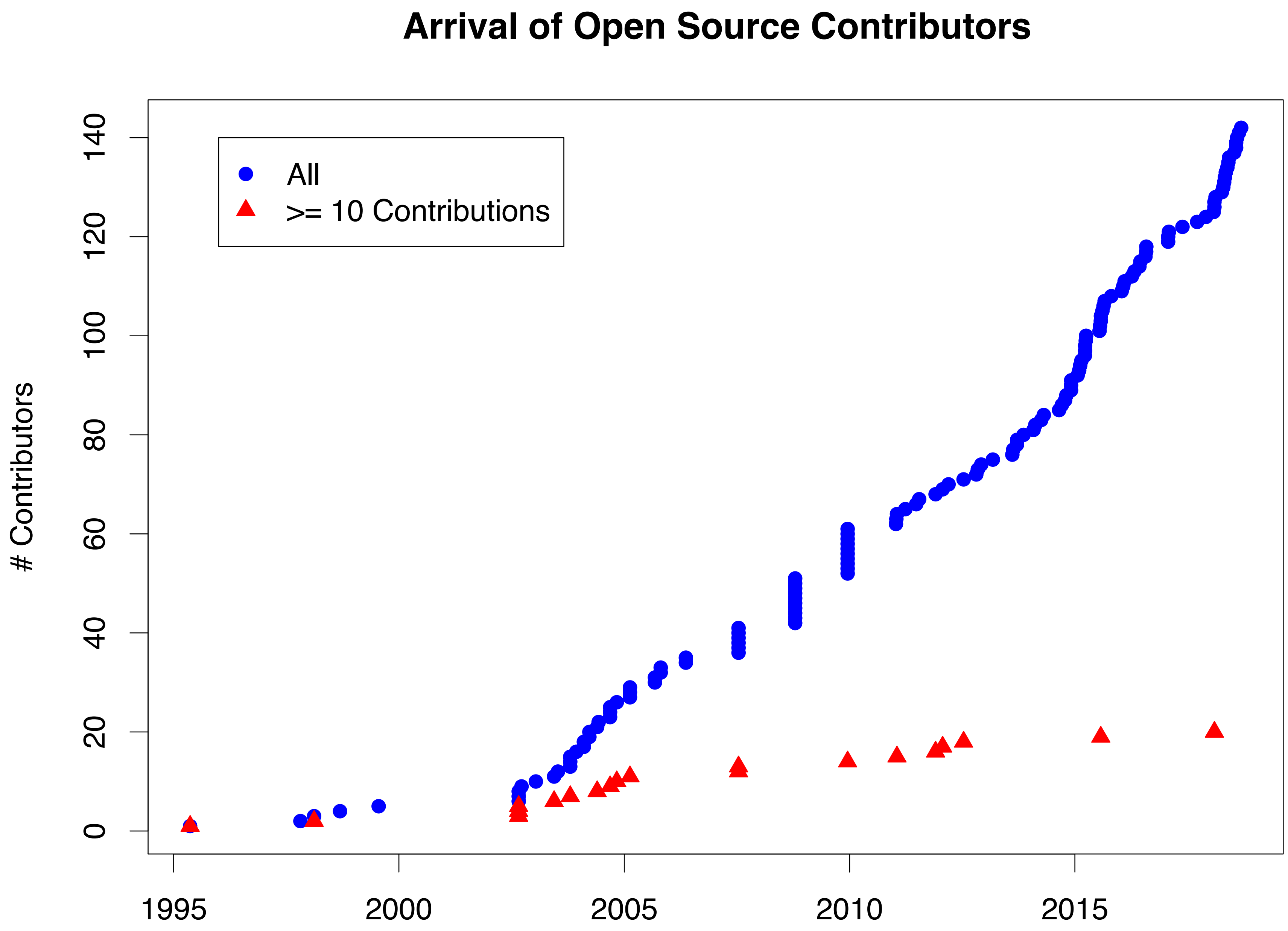


Viable Network Defense for Scientific Research Institutions	NSF STI-0334088 / $900K	ICSI
Detecting and Blocking Network Attacks at Ultra-High Speeds	DOE / $500K (ICSI)	ICSI LBNL
Bro Lite	DOE / $580K	ICSI LBNL
Approaches to Network Defense Proven in Open Scientific Environments	NSF CNS-0627320 / $236K	ICSI
Establishing a Cross-Institutional Platform for Cooperative Security Monitoring and Forensics	NSF CNS-0716640 / $700K	ICSI
Exploiting Multi-Core CPUs for Parallelizing Network Intrusion Prevention	NSF CNS-0716636 / $500K	ICSI
Comprehensive Application Analysis and Control	NSF CNS-0831535 / $1.8M	ICSI UC Berkeley
High Performance Networks - Compilation and Optimization of Protocol Analyzers	DOE SBIR / $750K	ICSI Reservoir Labs
Network Monitoring Infrastructure For Research in a Large-Scale Operational Environment	NSF CNS-0855125 / $208K	ICSI
A High-Performance Abstract Machine for Network Intrusion Detection	NSF CNS-0915667 / $450K	ICSI
Enhancing Bro for Operational Network Security Monitoring in Scientific Environments	NSF ACI-1032889 / $3M	ICSI NCSA
Cybersecurity and Networking: NIDS Front-End for Load Balancing at 100 Gigabits	DOE SBIR / $1M	cPacket Networks ICSI NERSC
A Concurrency Model for Deep Stateful Network Security Monitoring	Cisco Research / $75K	ICSI
Understanding and Exploiting Parallelism in Deep Packet Inspection on Concurrent Architectures	NSF CNS-1228792 / $1.5M	ICSI UW Madison
Semantic Security Monitoring for Industrial Control Systems	NSF CNS-1314973 / $1.6M	ICSI NCSA UIUC
A Bro Center of Expertise for the NSF Community	NSF ACI-1348077 / $3.8M	ICSI NCSA
Understanding the State of TLS Using Large-scale Passive Measurements	NSF CNS-1528156 / $663K	ICSI
Shared Intelligence Platform for Protecting our National Cyberinfrastructure	NSF ACI-1547249 / $500K	NCSA UIUC PSC
Building the Comprehensive Bro Archive Network	Mozilla / $200K	Software Freedom Conservatory
Secure and Resilient Architecture: Effective and Economical Protection for High-Performance Research and Education Networks	NSF ACI-1642161 / $1.0M	ICSI ESnet
Bro at Scale: A Network Monitoring Solution for Nationally and Globally Distributed Critical Infrastructure	DOE SBIR / $1.1M	Corelight, Inc.

Primarily Research Funding

Primarily TTP Funding

BRO NETWORK SECURITY MONITOR


Arrival of Open Source Contributors
# Contributors
0
20
40
60
80
100
120
140
● All
▲ >= 10 Contributions
1995
2000
2005
2010
2015