ICSI & The “Bro” Project

Vern Paxson

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

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

October 5, 2018
ICSI’s Networking & Security Group

... is not what this talk is about.

This talk is about one of our group’s numerous extensive efforts ...

... with impact – over decades – that makes it a major ICSI success story.
What the heck is “Bro”?
The Bro Network Security Monitor’s Architecture

- Taps network link passively, sends up a copy of all network traffic.
The Bro Network Security Monitor’s Architecture

- Kernel filters down high-volume stream via standard *libpcap* packet capture library.
“Event engine” decodes protocols, distills filtered stream into high-level, \textit{policy-neutral} events reflecting underlying network activity

- E.g., connection\_attempt, http\_reply, teredo\_authentication
- These span a range of semantic levels
- Currently \textasciitilde700+ different types
The Bro Network Security Monitor’s Architecture

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

… and take action:
- Record to disk - extensive logs
- Generate real-time alerts
- Execute programs as a form of response
What the heck is “Bro”? 

And why the heck is it named “Bro”?
Packet traces I’m gathering for research become of interest for operational security analysis at the Lawrence Berkeley National Laboratory (LBL).
At the time I’m an LBL staffer doing a work-study Ph.D. advised by ICSI co-founder Prof. Domenico Ferrari.
Utility of on-going/real-time monitoring at LBL leads to designing & developing Bro
Scott Shenker approaches me (and Sally Floyd) about putting together an Internet research group at ICSI.
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


First Bro semi-public release; Paper appears in USENIX Security
Our monitoring system is called Bro (an Orwellian reminder that monitoring comes hand in hand with the potential for privacy violations).
First Bro semi-public release; Paper appears in USENIX Security;  
“cat ~/.bash_history >documentation.txt”
With Scott as our fearless leader, we launch ACIRI – the *AT&T Center for Internet Research at ICSI*. ICSI becomes the home for Bro.
Interest in Bro

- LBL enables Bro to automatically block scanners
Interest in Bro

Downloads

Year

First Bro user manual sort of


Papers
Distros

Interest in Bro

Download

Year

Interest in Bro

- **Papers**
- **Distros**

**Sourcefire** founded – commercial support for Snort
Interest in Bro

Just 3 years!
Robin Sommer begins working on Bro as a student.
Robin Sommer begins working on Bro as a student; interns at ICSI
Interest in Bro

Downloads

Year


0 5000 10000 15000

Papers

Distros

Bro tutorials at CCS & Supercomputing
AT&T begins to pull out of ACIRI funding, leaving us looking for grant support.
Interest in Bro

Downloads

First Bro announcement on public mailing lists

Year
Interest in Bro

3-year grant begins for Bro work via NSF Strategic Technologies for the Internet program.
## Award Abstract #0334088

### STI: Viable Network Defense for Scientific Research Institutions

| NSF Org:          | ACI  
<table>
<thead>
<tr>
<th></th>
<th>Div Of Advanced Cyberinfrastructure</th>
</tr>
</thead>
</table>
| 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) |
**Award Abstract #0334088**

**STI: Viable Network Defense for Scientific Research Institutions**

| NSF Org:          | ACI  
<table>
<thead>
<tr>
<th></th>
<th>Div Of Advanced Cyberinfrastructure</th>
</tr>
</thead>
</table>
| 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; But does yield a steady stream of papers
Interest in Bro

- Papers
- Distros

DOE regime change cancels Bro Lite

Downloads

Year

Interest in Bro

Network traffic continues to grow relentlessly
Traffic Volume at T.U. Munich

- **Total Bytes**
- **Incoming Bytes**

TBytes / Month

- 1998
- 2000
- 2002
- 2004
- 2006

0 20 40 60 80 100 120
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 😞
Seth Hall comes on our radar – an operator who Gets It!
We pitch a large-scale continuation of the Bro project to NSF.
# CT-T: Approaches to Network Defense Proven in Open Scientific Environments

<table>
<thead>
<tr>
<th>NSF Org:</th>
<th>CNS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Division Of Computer and Network Systems</td>
</tr>
<tr>
<td>Program Manager:</td>
<td>Carl Landwehr</td>
</tr>
<tr>
<td></td>
<td>CNS Division Of Computer and Network Systems</td>
</tr>
<tr>
<td></td>
<td>CSE Direct For Computer &amp; Info Scie &amp; Enginr</td>
</tr>
<tr>
<td>Start Date:</td>
<td>October 1, 2006</td>
</tr>
<tr>
<td>End Date:</td>
<td>September 30, 2009 (Estimated)</td>
</tr>
<tr>
<td>Awarded Amount to Date:</td>
<td>$1,999,054 ?</td>
</tr>
<tr>
<td>Investigator(s):</td>
<td>Vern Paxson <a href="mailto:vern@icsi.berkeley.edu">vern@icsi.berkeley.edu</a> (Principal Investigator)</td>
</tr>
<tr>
<td></td>
<td>Mark Allman (Co-Principal Investigator)</td>
</tr>
<tr>
<td></td>
<td>Robin Sommer (Co-Principal Investigator)</td>
</tr>
</tbody>
</table>
CT-T: Approaches to Network Defense Proven in Open Scientific Environments

<table>
<thead>
<tr>
<th>NSF Org:</th>
<th>CNS Division Of Computer and Network Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Manager:</td>
<td>Carl Landwehr</td>
</tr>
<tr>
<td></td>
<td>CNS Division Of Computer and Network Systems</td>
</tr>
<tr>
<td></td>
<td>CSE Direct For Computer &amp; Info Scie &amp; Enginr</td>
</tr>
<tr>
<td>Start Date:</td>
<td>October 1, 2006</td>
</tr>
<tr>
<td>End Date:</td>
<td>September 30, 2009 (Estimated)</td>
</tr>
<tr>
<td>Awarded Amount to Date:</td>
<td>$236,066.00</td>
</tr>
<tr>
<td>Investigator(s):</td>
<td>Vern Paxson <a href="mailto:vern@icsi.berkeley.edu">vern@icsi.berkeley.edu</a> (Principal Investigator)</td>
</tr>
<tr>
<td></td>
<td>Mark Allman (Co-Principal Investigator)</td>
</tr>
<tr>
<td></td>
<td>Robin Sommer (Co-Principal Investigator)</td>
</tr>
</tbody>
</table>
Interest in Bro

Downloads

Year


0 20000 40000 60000

Checkpoint attempts to buy Sourcefire for $225M

Papers
Distros

SOURCEfire®
LBL’s Bro autoblocks more than 120,000 scanners in a single day.
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.
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) |
Award Abstract #1032889

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

| NSF Org:          | **ACI**  
<table>
<thead>
<tr>
<th></th>
<th><strong>Div Of Advanced Cyberinfrastructure</strong></th>
</tr>
</thead>
</table>
| 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)  |
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.

Investigator(s): Robin Sommer robin@icsi.berkeley.edu (Principal Investigator)
Vern Paxson (Co-Principal Investigator)
Adam Slagell (Co-Principal Investigator)
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: Cyberinfrastructure Center & Info Scie & Enginr

Start Date: 

End Date: (not specified)

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!
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! **Major Luck #2**: new collaboration *gels* highly effectively!
For long-term sustainability of the open-source project, Seth, Robin & I – with ICSI’s key support and seed investment – co-founded what becomes **Corelight**.
Interest in Bro

Cisco buys Sourcefire for $2.7B
NSF works with us to foster continuation of Bro project & community

Interest in Bro

Downloads

Year

2012 2013 2014 2015

Distros
Original Paper

NSF works with us to foster continuation of Bro project & community
**Award Abstract #1348077**

**A Bro Center of Expertise for the NSF Community**

<table>
<thead>
<tr>
<th><strong>NSF Org:</strong></th>
<th>ACI Div Of Advanced Cyberinfrastructure</th>
</tr>
</thead>
</table>
| **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) |
**Award Abstract #1348077**

**A Bro Center of Expertise for the NSF Community**

| **NSF Org:** | **ACI**  
<table>
<thead>
<tr>
<th></th>
<th><strong>Div Of Advanced Cyberinfrastructure</strong></th>
</tr>
</thead>
</table>
| **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) |
Network traffic continues to grow relentlessly.
Traffic Volume at T.U. Munich

- Total Bytes
- Incoming Bytes

49.9% / year
@Bro_IDS Twitter Followers

Year

Followers

2012 2013 2014 2015

Growth = 500+/year
@Bro_IDS Twitter Followers

Growth = 1,100+/year
Corelight, with ~6 employees, receives $9M in venture funding “A” round
Corelight, with 44 employees, receives $25M in venture funding “B” round.
Project announcement of name change … … since “bro” has become a pejorative
End of window for community to suggest new names … … several hundred are offered
New name to be announced at “BroCon”, Oct 11, 2018
<table>
<thead>
<tr>
<th>Year</th>
<th>Project Title</th>
<th>Funding Agency</th>
<th>Amount</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1996</td>
<td>Viable Network Defense for Scientific Research Institutions</td>
<td>NSF STI-034088B</td>
<td>/ $900K</td>
<td>IC1</td>
</tr>
<tr>
<td>1997</td>
<td>Detecting and Blocking Network Attacks at Ultra-High Speeds</td>
<td>DOE / $500K (IC1)</td>
<td>/ $60K</td>
<td>IC1</td>
</tr>
<tr>
<td>1998</td>
<td>Bro Lite</td>
<td></td>
<td></td>
<td>IC1</td>
</tr>
<tr>
<td>1999</td>
<td>Approaches to Network Defense Proven in Open Scientific Environments</td>
<td>NSF CNS-H073250 / $236K</td>
<td>IC1</td>
<td></td>
</tr>
<tr>
<td>2000</td>
<td>Establishing a Cross-Institutional Platform for Cooperative Security Monitoring and Forensics</td>
<td>NSF CNS-0716840 / $750K</td>
<td>IC1</td>
<td></td>
</tr>
<tr>
<td>2001</td>
<td>Exploiting Multi-Core CPUs for Parallelizing Network Intrusion Prevention</td>
<td>NSF CNS-0716830 / $500K</td>
<td>IC1</td>
<td></td>
</tr>
<tr>
<td>2002</td>
<td>Comprehensive Application Analysis and Control</td>
<td>NSF CNS-0831535 / $1.8M</td>
<td>IC1</td>
<td></td>
</tr>
<tr>
<td>2003</td>
<td>High Performance Networks - Compilation and Optimization of Protocol Analyzers</td>
<td>DOE SBIR / $750K</td>
<td>IC1</td>
<td></td>
</tr>
<tr>
<td>2004</td>
<td>Network Monitoring Infrastructure For Research in a Large-Scale Operational Environment</td>
<td>NSF CNS-0931350 / $236K</td>
<td>IC1</td>
<td></td>
</tr>
<tr>
<td>2005</td>
<td>A High-Performance Abstract Machine for Network Intrusion Detection</td>
<td>NSF CNS-0915096 / $450K</td>
<td>IC1</td>
<td></td>
</tr>
<tr>
<td>2006</td>
<td>Enhancing Bro for Operational Network Security Monitoring in Scientific Environments</td>
<td>NSF ACI-1032889 / $3M</td>
<td>IC1</td>
<td></td>
</tr>
<tr>
<td>2007</td>
<td>Cybersecurity and Networking: NIDS Front-End for Load Balancing at 100 Gigabits</td>
<td>DOE SBIR / $1M</td>
<td>IC1</td>
<td></td>
</tr>
<tr>
<td>2008</td>
<td>A Concurrency Model for Deep Stateful Network Security Monitoring</td>
<td>OSA Research / $75K</td>
<td>IC1</td>
<td></td>
</tr>
<tr>
<td>2009</td>
<td>Understanding and Exploiting Parallelism in Deep Packet Inspection on Concurrent Architectures</td>
<td>NSF CNS-1228792 / $1.5M</td>
<td>IC1</td>
<td></td>
</tr>
<tr>
<td>2010</td>
<td>Semantic Security Monitoring for Industrial Control Systems</td>
<td>NSF CNS-1314973 / $1.6M</td>
<td>IC1</td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td>A Bro Center of Expertise for the NSF Community</td>
<td>NSF ACI-1348077 / $3.8M</td>
<td>IC1</td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td>Understanding the State of TLS Using Large-scale Passive Measurements</td>
<td>NSF CNS-1528156 / $663K</td>
<td>IC1</td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td>Shared Intelligence Platform for Protecting our National Cyberinfrastructure</td>
<td>NSF CNS-1547369 / $500K</td>
<td>IC1</td>
<td></td>
</tr>
<tr>
<td>2014</td>
<td>Building the Comprehensive Bro Archive Network</td>
<td>NSF ACI-1642161 / $1.0M</td>
<td>IC1</td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td>Secure and Resilient Architecture: Effective and Economical Protection for High-Performance Research and Education Networks</td>
<td>DOE SBIR / $1.1M</td>
<td>IC1</td>
<td></td>
</tr>
<tr>
<td>2016</td>
<td>Bro at Scale: A Network Monitoring Solution for Nationally and Globally Distributed Critical Infrastructure</td>
<td>DOE SBIR / $1.1M</td>
<td>IC1</td>
<td></td>
</tr>
<tr>
<td>2017</td>
<td>Primarily Research Funding</td>
<td></td>
<td></td>
<td>IC1</td>
</tr>
<tr>
<td>2018</td>
<td>Primarily TTP Funding</td>
<td></td>
<td></td>
<td>IC1</td>
</tr>
</tbody>
</table>
Some Companies/Insts. Using Bro
Bro was one of eight 2016 highlights NSF framed for Congress.
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.

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

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

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

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

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