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.

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.
Packet traces I’m gathering for research become of interest for operational security analysis.
Utility of on-going/real-time monitoring at LBL leads to designing & developing **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:
TCPDUMP(1)

NAME
tcpdump - dump traffic on a network

SYNOPSIS
tcpdump [ -AbDefhgiJKLmNopqRstuUvxX ] [ -B buffer_size ] [ -c count ]
          [ -C file_size ] [ -G rotate_seconds ] [ -F file ]
          [ -i interface ] [ -i t stamp_type ] [ -k (metadata arg) ]

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

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

Downloads

<table>
<thead>
<tr>
<th>Year</th>
<th>Papers</th>
<th>Distros</th>
</tr>
</thead>
<tbody>
<tr>
<td>1994</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1996</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1998</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2002</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

First Bro user manual sort of
LBL enables Bro to automatically block scanners
Interest in Bro

First release of Snort


Year

0  5000  10000  15000

Downloads

Papers
Distros
Interest in Bro

![Graph showing the interest in Bro from 1994 to 2002 with the number of downloads and papers over time.]

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

- **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

Downloads

Year


0 5000 10000 15000

Sourcfire
directed –
commercial support for Snort

Sources

Papers

Distros
Interest in Bro

Year

Downloads

0


Papers

Distros

Just 3 years!
Interest in Bro

- Downloads over time from 1994 to 2002
- Blue circles represent Papers, red triangles represent Distros
- LBL Bro's auto-blocking of scanners breaks due to Code Red worm

Year:
- 1994
- 1996
- 1998
- 2000
- 2002

Downloads:
- 0
- 5000
- 10000
- 15000
Interest in Bro

Robin Sommer begins working on Bro as a student
Robin Sommer begins working on Bro as a student; interns at ICSI.
First Bro announcement on public mailing lists
3-year grant begins for Bro work via NSF Strategic Technologies for the Internet program.
**STI: Viable Network Defense for Scientific Research Institutions**

<table>
<thead>
<tr>
<th>NSF Org:</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:   | 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) |
**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

Interest in Bro

Downloads

Year

DOE regime change cancels Bro Lite


0 5000 10000 15000 20000 25000

Papers
Distros
Network traffic continues to grow relentlessly
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 -> Load-Balancer

Internal Network

External Scripts

External Bro

Broccoli (Broker)

Broccoli Python
Broccoli Ruby
(Broccoli Perl)

Bro Client Communication Library
Bro Cluster Ecosystem

Internet -> Tap -> BroControl

Packets

BroBalancer

Bro -> BroControl

Control

Bro -> BroControl

Output

Bro -> BroControl

External Scripts

BroControl -> User Interface

Bro (Broker)

Bro Client Communication Library

Broccoli Python

Broccoli Ruby

(Broccoli Perl)

Internal Network
Bro *Cluster* Ecosystem

- **Internet**
- **Internal Network**
- **Load-Balancer**
  - "Frontend"
- **Bro**
- **Bro**
- **Bro**
- **Bro**
- **External Bro**
- **External Scripts**
- **BroControl**
  - "Workers"
  - "Manager"
  - Control
  - Output
- **User Interface**
- **Broccoli**
  - (Broker)
  - Python
  - Ruby
  - (Perl)
- **Bro Client Communication Library**

Diagram showing the interactions and components of the Bro Cluster Ecosystem.
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**

| **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) |
## 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>
</table>
| **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

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

Checkpoint attempts to buy Sourcefire for $225M

Download count over years:
- **1998**
- **2000**
- **2002**
- **2004**
- **2006**
- **2008**
- **2010**

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

<table>
<thead>
<tr>
<th>NSF Org</th>
<th>ACI Div Of Advanced Cyberinfrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Manager</td>
<td>Anita Nikolich</td>
</tr>
<tr>
<td></td>
<td>ACI Div Of Advanced Cyberinfrastructure</td>
</tr>
<tr>
<td></td>
<td>CSE Direct For Computer &amp; Info Scie &amp; Enginr</td>
</tr>
<tr>
<td>Start Date</td>
<td>September 1, 2010</td>
</tr>
<tr>
<td>End Date</td>
<td>August 31, 2014 (Estimated)</td>
</tr>
<tr>
<td>Awarded Amount to Date</td>
<td>$2,995,905</td>
</tr>
<tr>
<td>Investigator(s)</td>
<td>Robin Sommer <a href="mailto:robin@icsi.berkeley.edu">robin@icsi.berkeley.edu</a> (Principal Investigator) Vern Paxson (Co-Principal Investigator) Adam Slagell (Co-Principal Investigator)</td>
</tr>
</tbody>
</table>
Award Abstract #1032889

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

<table>
<thead>
<tr>
<th>NSF Org:</th>
<th>ACI Div Of Advanced Cyberinfrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Manager:</td>
<td>Anita Nikolich</td>
</tr>
<tr>
<td></td>
<td>ACI Div Of Advanced Cyberinfrastructure</td>
</tr>
<tr>
<td></td>
<td>CSE Direct For Computer &amp; Info Scie &amp; Enginr</td>
</tr>
<tr>
<td>Start Date:</td>
<td>September 1, 2010</td>
</tr>
<tr>
<td>End Date:</td>
<td>August 31, 2014 (Estimated)</td>
</tr>
<tr>
<td>Awarded Amount to Date:</td>
<td>$2,995,905.00</td>
</tr>
<tr>
<td>Investigator(s):</td>
<td>Robin Sommer <a href="mailto:robin@icsi.berkeley.edu">robin@icsi.berkeley.edu</a> (Principal Investigator)</td>
</tr>
<tr>
<td></td>
<td>Vern Paxson (Co-Principal Investigator)</td>
</tr>
<tr>
<td></td>
<td>Adam Slagell (Co-Principal Investigator)</td>
</tr>
</tbody>
</table>
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)
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)
**SDCI Sec Improvement: Enhancing Bro for Operational Network Security Monitoring in Scientific Environments**

<table>
<thead>
<tr>
<th>NSF Org:</th>
<th>ACI Div Of Advanced Cyberinfrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Manager:</td>
<td>[Image] Cyberinfrastructure Center &amp; Info Scie &amp; Engnr</td>
</tr>
<tr>
<td>Start Date:</td>
<td>[Image]</td>
</tr>
<tr>
<td>End Date:</td>
<td>[Image] (Estimated)</td>
</tr>
<tr>
<td>Awarded Amount to Date:</td>
<td></td>
</tr>
<tr>
<td>Investigator(s):</td>
<td>Robin Sommer <a href="mailto:robin@icsi.berkeley.edu">robin@icsi.berkeley.edu</a> (Principal Investigator) Vern Paxson (Co-Principal Investigator) Adam Slagell (Co-Principal Investigator)</td>
</tr>
</tbody>
</table>
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 co-founded what becomes Corelight.
Cisco buys Sourcefire for $2.7B
NSF works with us to foster continuation of Bro project & community
### A Bro Center of Expertise for the NSF Community

<table>
<thead>
<tr>
<th>NSF Org:</th>
<th>ACI Div Of Advanced Cyberinfrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Manager:</td>
<td>Kevin L. Thompson</td>
</tr>
<tr>
<td></td>
<td>ACI Div Of Advanced Cyberinfrastructure</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, 2013</td>
</tr>
<tr>
<td>End Date:</td>
<td>September 30, 2016 (Estimated)</td>
</tr>
<tr>
<td>Awarded Amount to Date:</td>
<td>$3,729,977 ?</td>
</tr>
<tr>
<td>Investigator(s):</td>
<td>Robin Sommer <a href="mailto:robin@icsi.berkeley.edu">robin@icsi.berkeley.edu</a> (Principal Investigator)</td>
</tr>
<tr>
<td></td>
<td>Vern Paxson (Co-Principal Investigator)</td>
</tr>
<tr>
<td></td>
<td>Adam Slagell (Co-Principal Investigator)</td>
</tr>
</tbody>
</table>
**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>
<tbody>
<tr>
<td><strong>Program Manager:</strong></td>
<td>Kevin L. Thompson</td>
</tr>
<tr>
<td></td>
<td>ACI Div Of Advanced Cyberinfrastructure</td>
</tr>
<tr>
<td></td>
<td>CSE Direct For Computer &amp; Info Scie &amp; Enginr</td>
</tr>
<tr>
<td><strong>Start Date:</strong></td>
<td>October 1, 2013</td>
</tr>
<tr>
<td><strong>End Date:</strong></td>
<td>September 30, 2016 (Estimated)</td>
</tr>
<tr>
<td><strong>Awarded Amount to Date:</strong></td>
<td>$3,360,092.00</td>
</tr>
<tr>
<td><strong>Investigator(s):</strong></td>
<td>Robin Sommer <a href="mailto:robin@icsi.berkeley.edu">robin@icsi.berkeley.edu</a> (Principal Investigator)</td>
</tr>
<tr>
<td></td>
<td>Vern Paxson (Co-Principal Investigator)</td>
</tr>
<tr>
<td></td>
<td>Adam Slagell (Co-Principal Investigator)</td>
</tr>
</tbody>
</table>
Network traffic continues to grow relentlessly.
Traffic Volume at T.U. Munich

TBytes / Month

- Total Bytes
- Incoming Bytes

Traffic Volume at T.U. Munich

- Total Bytes
- Incoming Bytes

49.9% / year
Architecture As It Has Evolved

Packet Stream

libpcap

Event Engine

Policy Script Interpreter

Real-time Action Log Archive

Event Control

Tcpdump Filter

Filtered Packet Stream

Packet Stream

Network

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

Analysis of events from other sources; parsing of non-network formats (items/files)
Architecture As It Has Evolved

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

- File Analysis
- GeoLocation
- Input Framework
- Intelligence Framework
- Logging Framework
- NetControl Framework
- Notice Framework
- Signature Framework
- Summary Statistics
- Broker-Enabled Communication Framework
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.
100G Monitoring

Aashish Sharma
Vincent Stoffer

Bro4Pros
February 19th, 2015
OpenDNS, SF
100G Intrusion Detection

August 2015

v1.0
**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) |
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
Project announcement of name change …
… since “bro” has become a pejorative
@Bro_IDS Twitter Followers

End of window for community to suggest new names
Arrival of Open Source Contributors

- All
- >= 10 Contributions