



The NSF Bro Center of Expertise

Robin Sommer

International Computer Science Institute, &
Lawrence Berkeley National Laboratory

`robin@icsi.berkeley.edu`
`http://www.icir.org/robin`



The Bro Network Monitor

Open Source
BSD License

Analyses

Intrusion
Detection

Vulnerabilit.
Mgmt

File Analysis

Traffic
Measure-
ment

Traffic
Control

Compliance
Monitoring

Platform

Programming Language

Standard Library

Packet Processing

Tap

Network





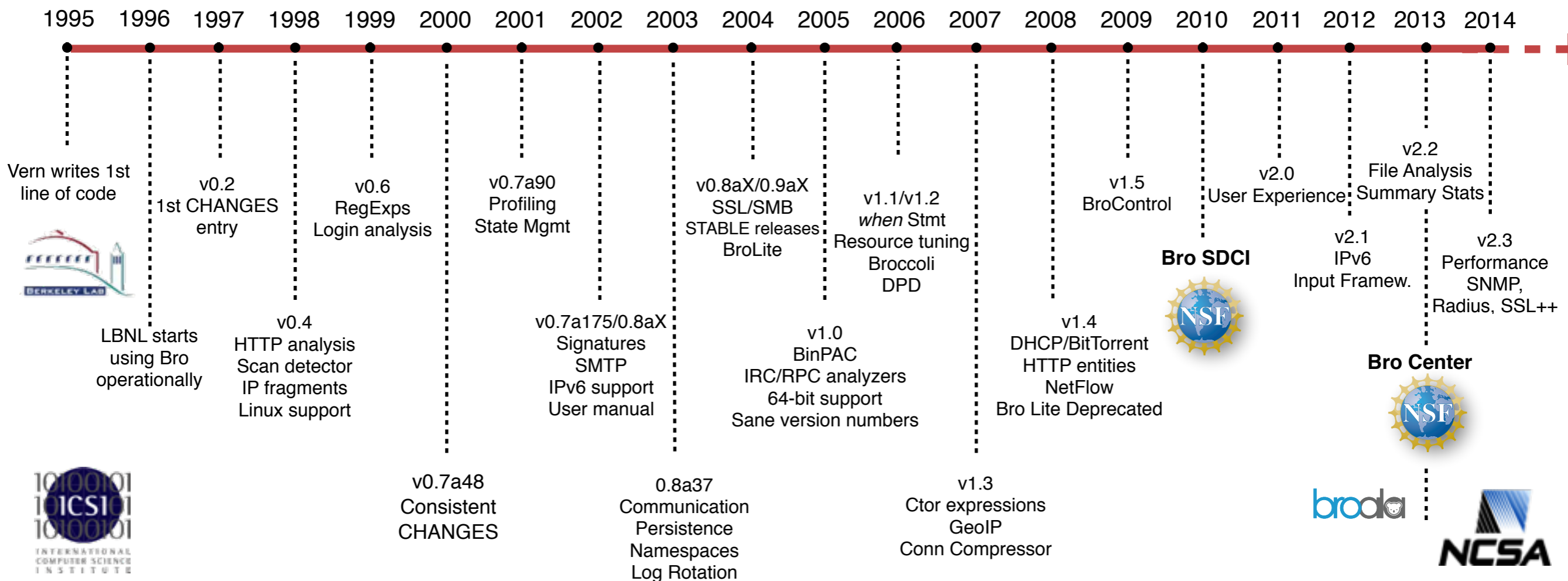
Bro History

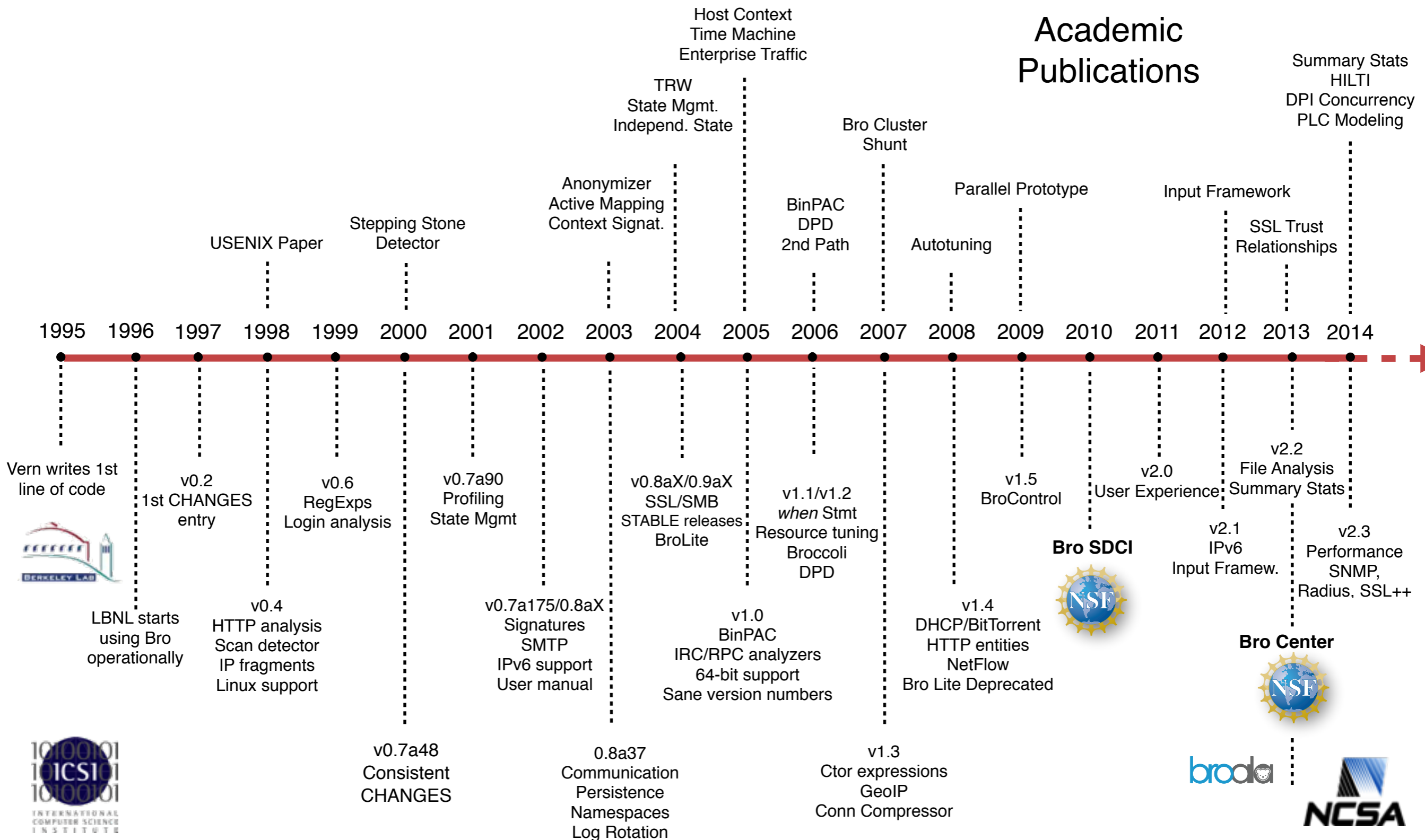


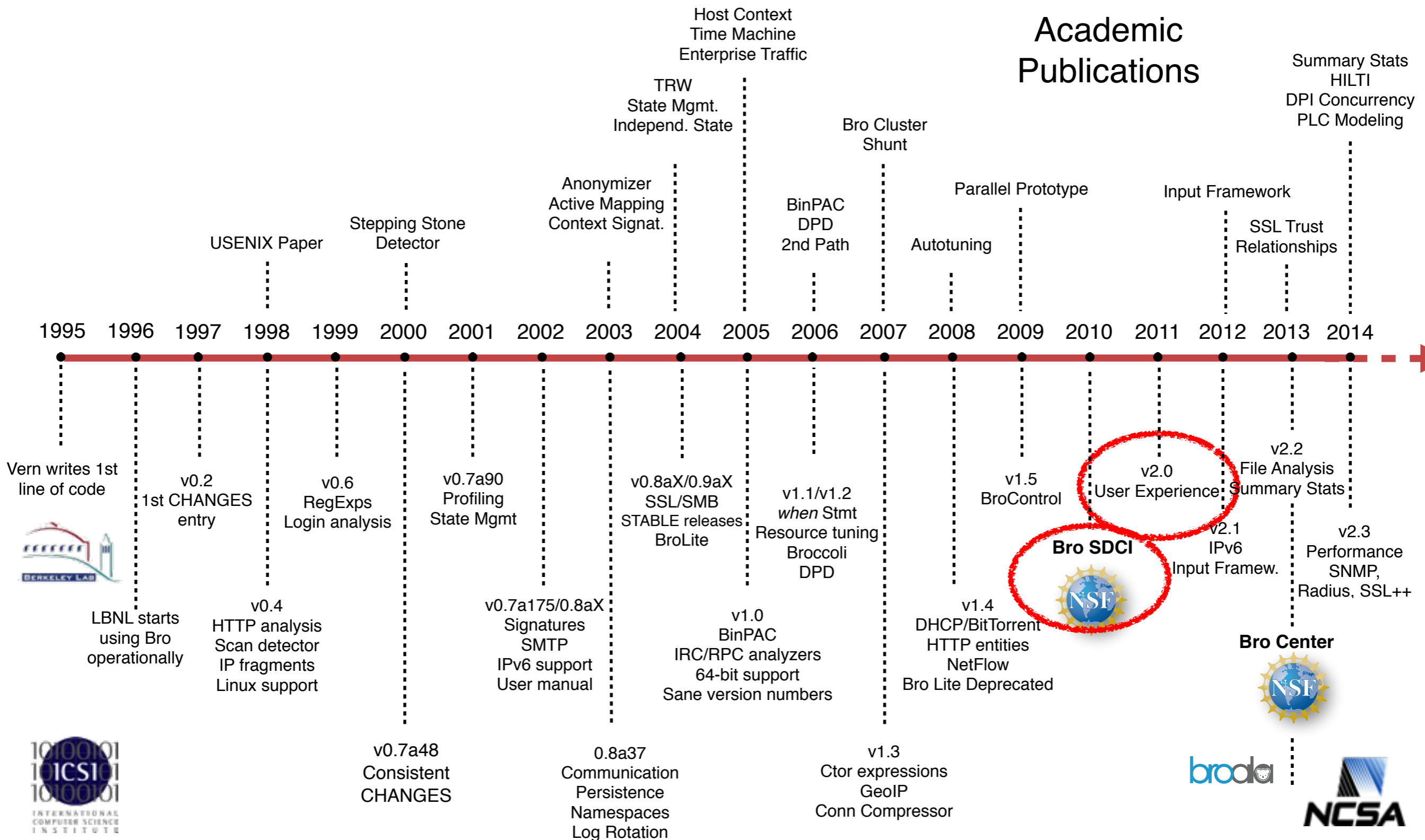
1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014

Vern writes 1st
line of code









Deployments

Installations across the US

Universities
Research Labs
Supercomputer Centers
Government Organizations
Fortune 50 Enterprises

Examples

Lawrence Berkeley National Lab
National Center for Supercomputing Applications
Indiana University
Carnegie Mellon
National Center for Atmospheric Research
... and many more sites I can't talk about.

Fully integrated into Security Onion

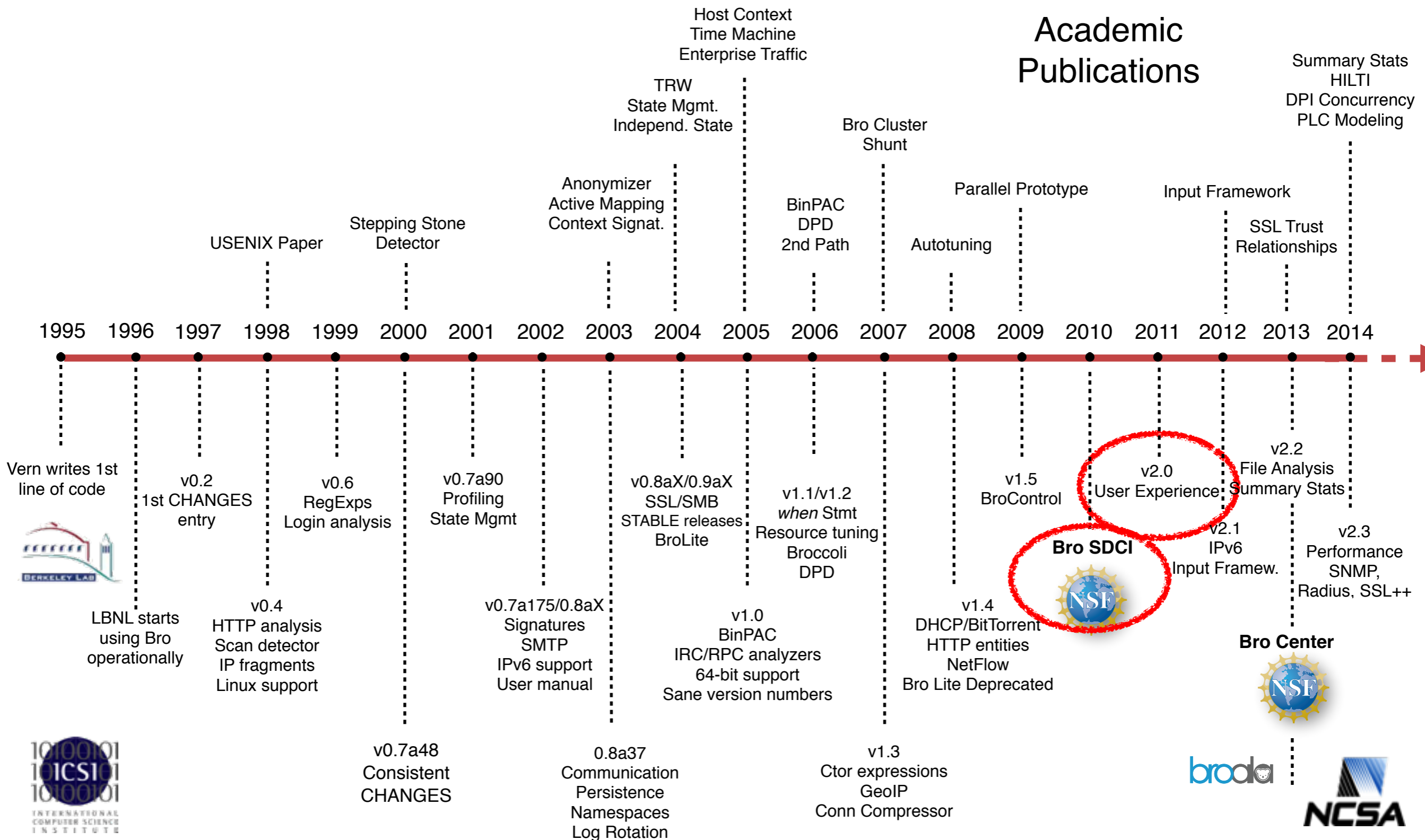
Popular security-oriented Linux distribution

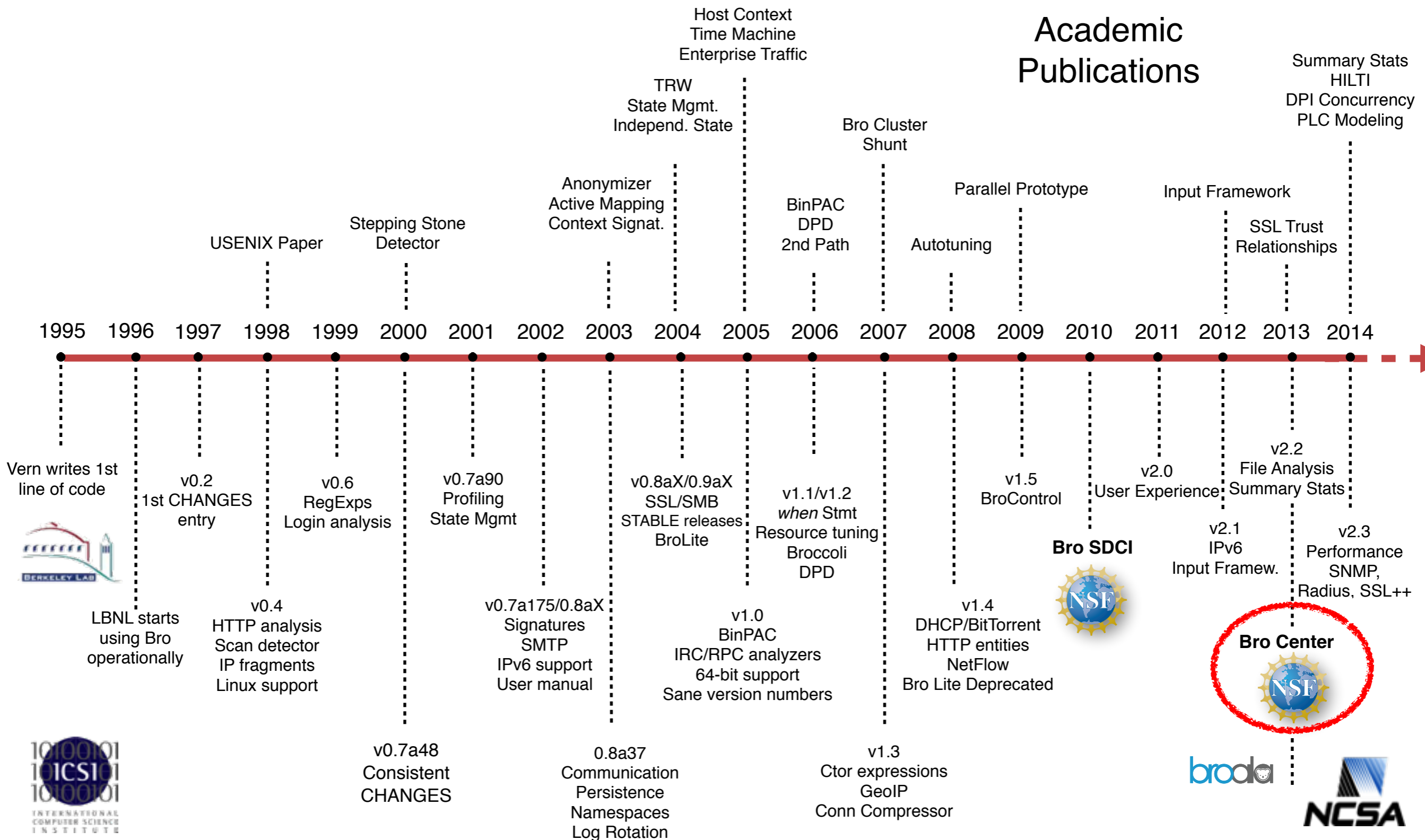


Community

50/90/150 attendees at BroCon '12/'13/'14
60 organizations at BroCon '14
2,500 Twitter followers
800 mailing list subscribers
70 users average on IRC channel
10,000 downloads / version
from 150 countries
> 30,000 Onion downloads ('12)







The NSF Bro Center of Expertise

Promote Bro as a comprehensive, low-cost security capability for the NSF community.

<http://nsf.bro.org>

<mailto:nsf@bro.org>



The NSF Bro Center of Expertise

Promote Bro as a comprehensive, low-cost security capability for the NSF community.



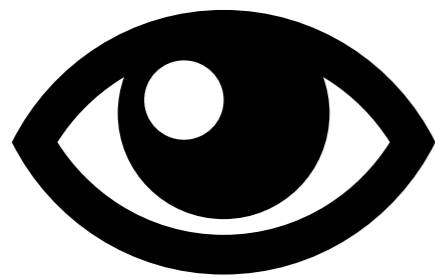
<http://nsf.bro.org>

<mailto:nsf@bro.org>



The NSF Bro Center of Expertise

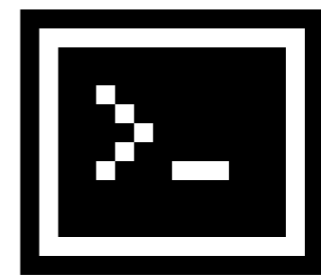
Promote Bro as a comprehensive, low-cost security capability for the NSF community.



Individual
Advice



Training Material,
Guidelines,
Best Practices



Development,
Maintenance

<http://nsf.bro.org>

<mailto:nsf@bro.org>



Center Team



Located at *International Computer Science Institute*, Berkeley, CA; and the *National Center for Supercomputing Applications*, Urbana-Champaign, IL.



Events

BroCon 2014.

2.5 days, 150 attendees, 4 corporate sponsors.
Presentations, training, demos.

Bro Workshops.

NSF Cybersecurity Summits '13 & '14.
DOE NSM Meeting, June '14.

In Planing.

Advanced Workshop at ICSI.
BroCon '15 (East coast, tentatively).
Co-organize BoFs/demos at Internet2 & Supercomputing.



Current Engagements & Collaborations

Individual Advice.


Universities, NSF MREFs, K-12 schools.

Collaborations.

CTSC	Outreach & training, security reviews.
ESnet	SDN, Science DMZ security.
RIT	Teaching Community.


Teaching Bro - Material

Video Tutorials




The More You Bro: Basics of BroControl
1 month ago · 499 views
This video is a summary of BroControl's most common and useful commands. Full command reference documentation can be found here:...

The Basics of BroControl **4:12**



The More You Bro: Setting up a Bro Cluster
2 months ago · 341 views
This video reviews some basic instructions for installing Bro as a cluster configuration. Find more documentation here: <http://bro.org/sphinx-git/configuration/index.html>...

Setting up a Bro Cluster **5:54**



The More You Bro: Log Mining Efficiency
3 months ago · 445 views
This video goes into more detail about log mining, this time focusing on efficiency. You can find the cf tool we used in the video here:...

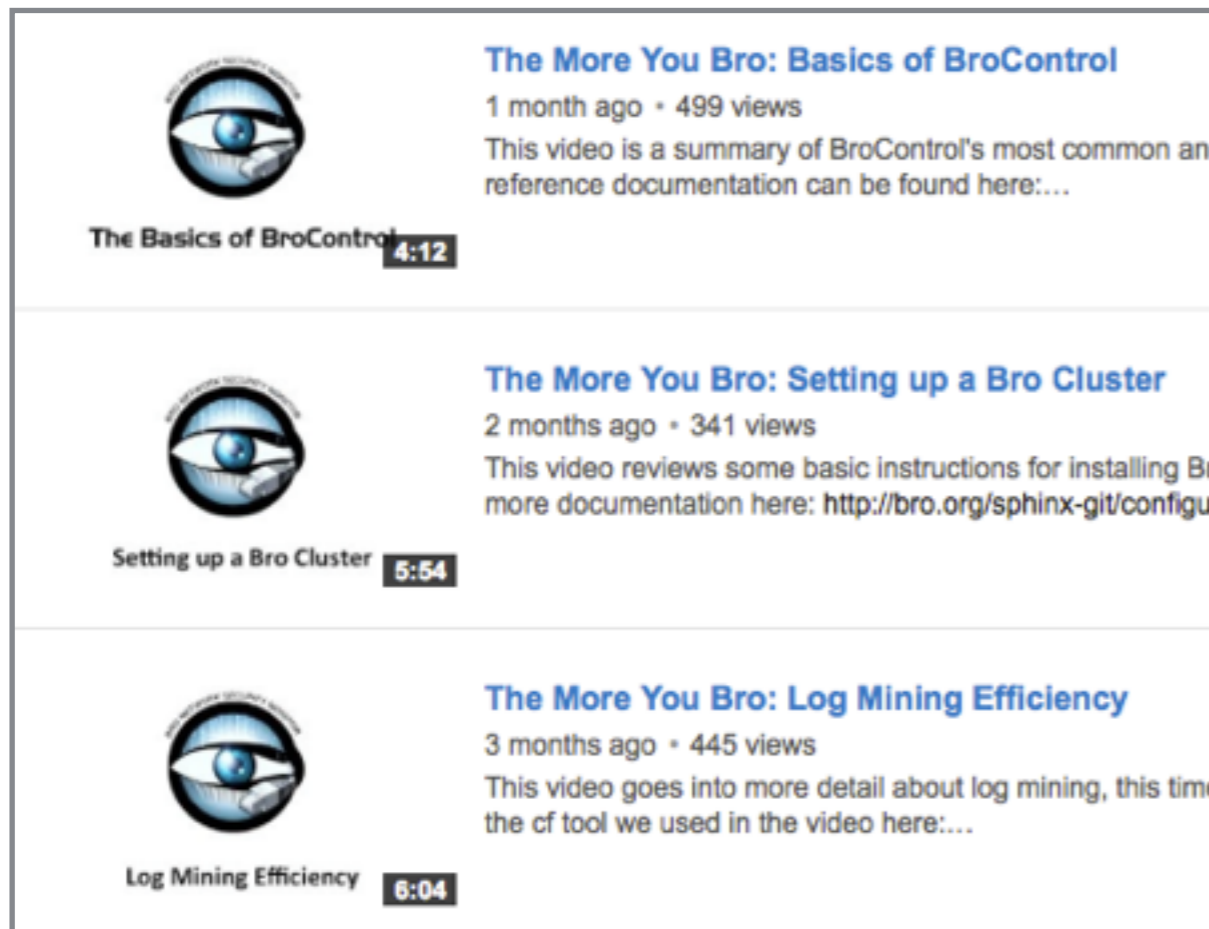
Log Mining Efficiency **6:04**

<http://www.youtube.com/user/BroPlatform>

Teaching Bro - Material

Video Tutorials

Exercises



The image shows three YouTube video thumbnails. Each thumbnail features the Bro logo (an eye) on the left and text on the right. The first thumbnail is titled 'The More You Bro: Basics of BroControl', posted 1 month ago with 499 views, and has a duration of 4:12. The second is 'The More You Bro: Setting up a Bro Cluster', posted 2 months ago with 341 views, and has a duration of 5:54. The third is 'The More You Bro: Log Mining Efficiency', posted 3 months ago with 445 views, and has a duration of 6:04.

The Basics of BroControl 4:12

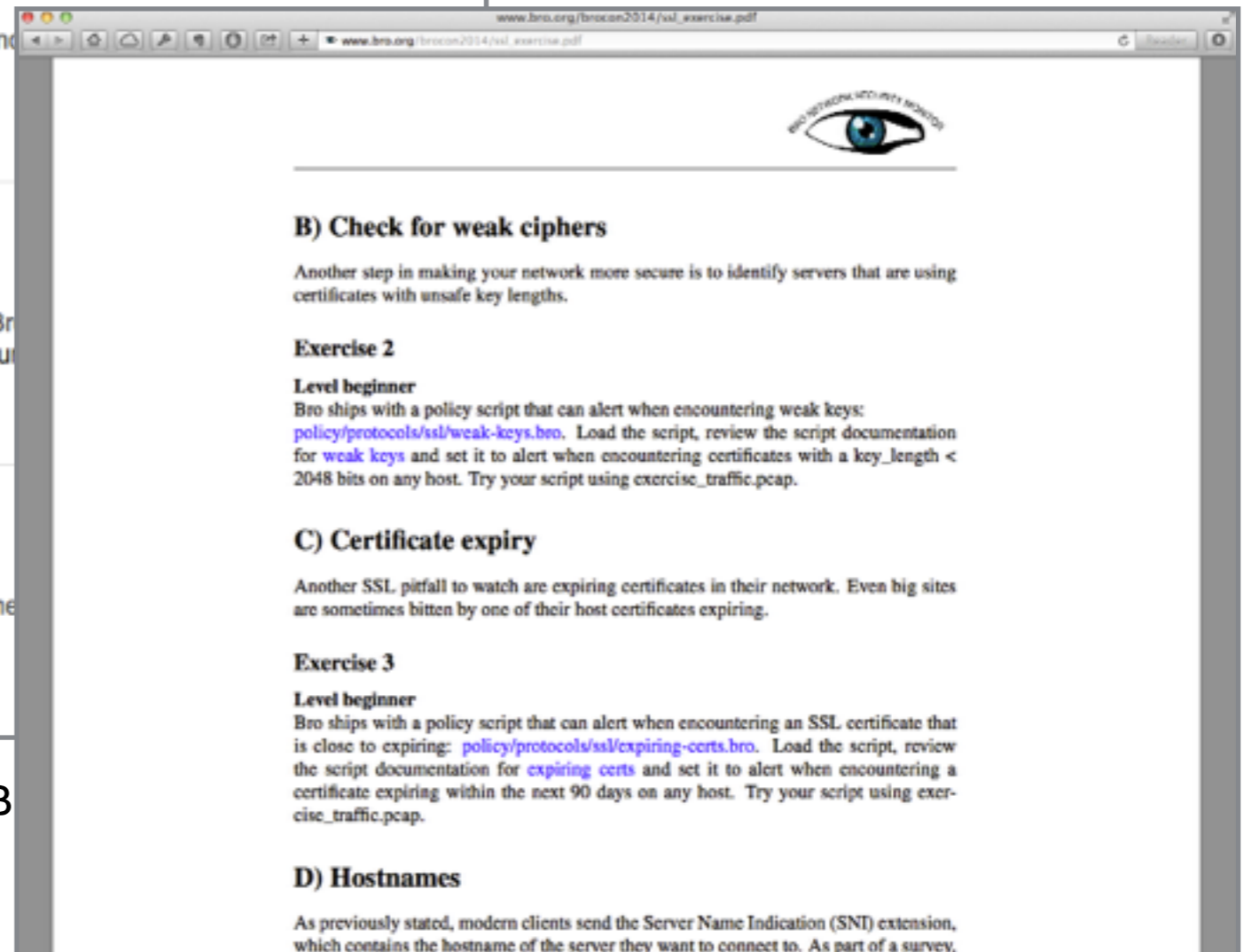
The More You Bro: Basics of BroControl
1 month ago · 499 views
This video is a summary of BroControl's most common and reference documentation can be found here:...

Setting up a Bro Cluster 5:54

The More You Bro: Setting up a Bro Cluster
2 months ago · 341 views
This video reviews some basic instructions for installing Bro more documentation here: <http://bro.org/sphinx-git/configur>

Log Mining Efficiency 6:04

The More You Bro: Log Mining Efficiency
3 months ago · 445 views
This video goes into more detail about log mining, this time the cf tool we used in the video here:...



The image is a screenshot of a PDF document titled 'ssl_exercise.pdf' from the website www.bro.org. The document contains several sections related to SSL exercises. The first section is 'B) Check for weak ciphers', which discusses identifying servers using unsafe key lengths and includes 'Exercise 2' (Level beginner) with instructions on using a policy script to alert on weak keys. The second section is 'C) Certificate expiry', which discusses expiring certificates and includes 'Exercise 3' (Level beginner) with instructions on using a policy script to alert on certificates expiring within 90 days. The third section is 'D) Hostnames', which discusses the Server Name Indication (SNI) extension.

B) Check for weak ciphers

Another step in making your network more secure is to identify servers that are using certificates with unsafe key lengths.

Exercise 2

Level beginner
Bro ships with a policy script that can alert when encountering weak keys: [policy/protocols/ssl/weak-keys.bro](#). Load the script, review the script documentation for [weak keys](#) and set it to alert when encountering certificates with a `key_length < 2048` bits on any host. Try your script using `exercise_traffic.pcap`.

C) Certificate expiry

Another SSL pitfall to watch are expiring certificates in their network. Even big sites are sometimes bitten by one of their host certificates expiring.

Exercise 3

Level beginner
Bro ships with a policy script that can alert when encountering an SSL certificate that is close to expiring: [policy/protocols/ssl/expiring-certs.bro](#). Load the script, review the script documentation for [expiring certs](#) and set it to alert when encountering a certificate expiring within the next 90 days on any host. Try your script using `exercise_traffic.pcap`.

D) Hostnames

As previously stated, modern clients send the Server Name Indication (SNI) extension, which contains the hostname of the server they want to connect to. As part of a survey,

<http://www.youtube.com/user/B>

Teaching Bro - Infrastructure

`live.bro.org`

SSH into a virtual Bro environment.

Teaching Bro - Infrastructure

live.bro.org

SSH into a virtual Bro environment.

```
demo@bro: ~ (ssh)
Welcome to Bro Live!
=====
      -----
      /         \
      (  (0)  )
      \         /
      <====// /
      -----

A place to try out Bro.

Are you a new or existing user? [new/existing]: new

A temporary account will be created so that you can resume your session. Account is valid for the
length of the event.

Choose a username [a-zA-Z0-9]: happyuser
Your username is happyuser
Choose a password:
Verify your password:
Your account will expire on Mon 25 Aug 2014 07:33:09 PM UTC

Enjoy yourself!
Training materials are located in /exercises.
e.g. $ bro -r /exercises/beginner/http.pcap

demo@bro:~$
```



Teaching Bro - Infrastructure

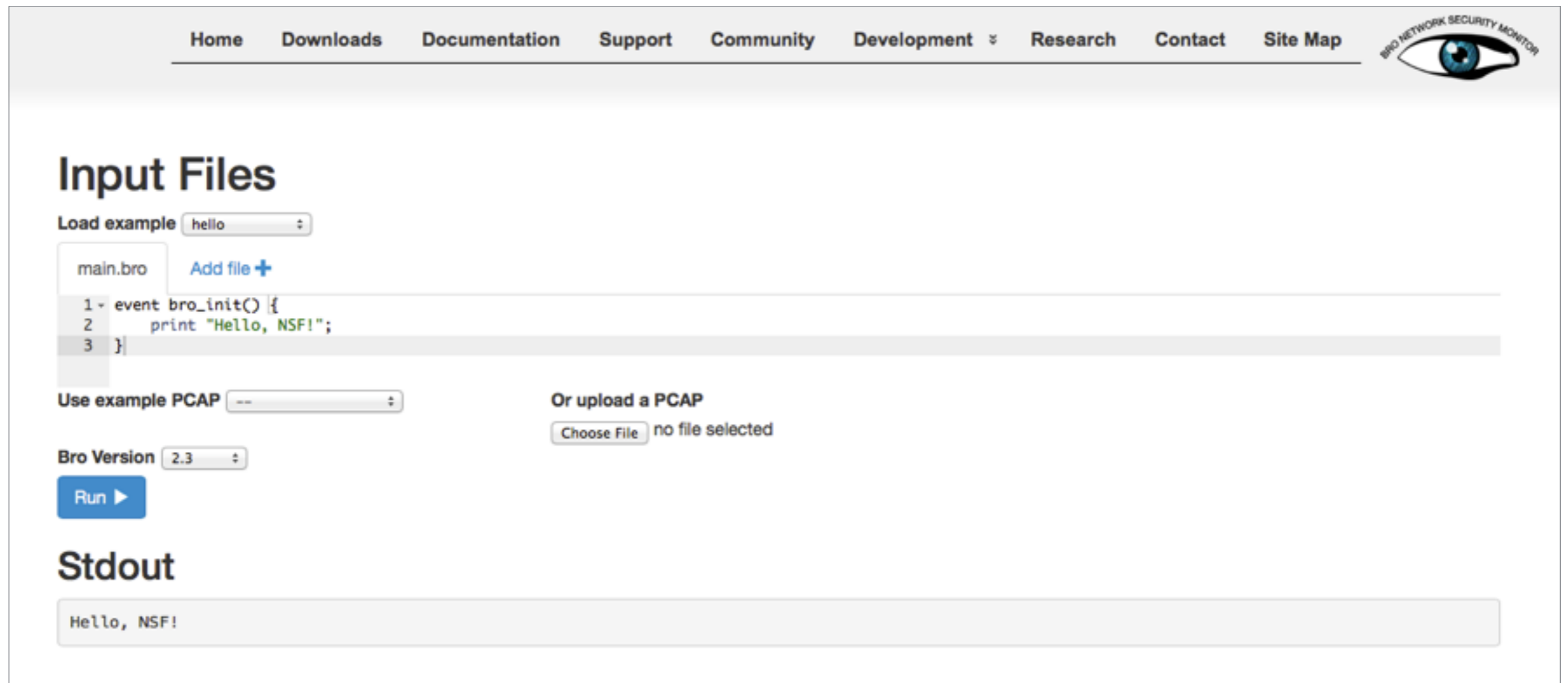
`try.bro.org`

A web-based Bro sandbox.

Teaching Bro - Infrastructure

try.bro.org

A web-based Bro sandbox.



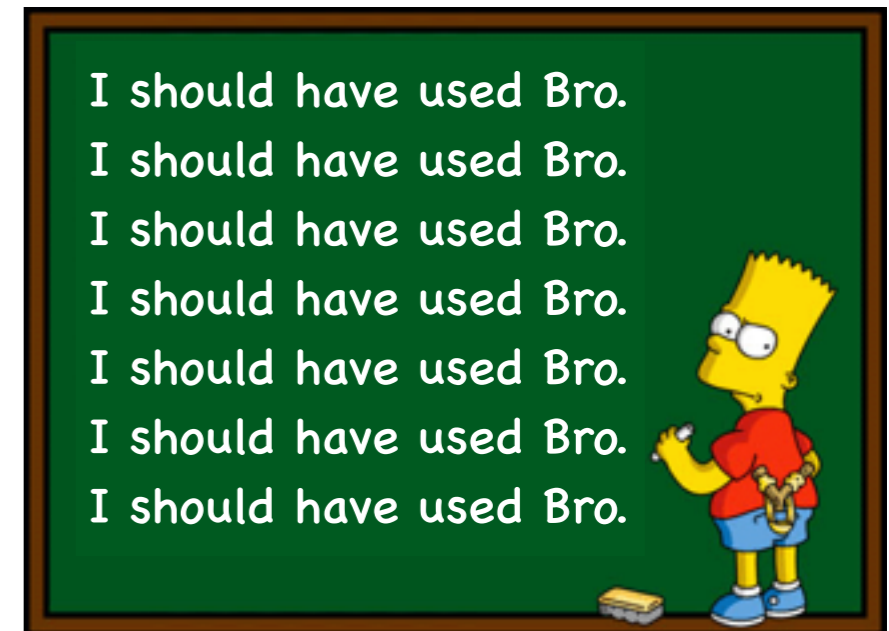
The screenshot displays the try.bro.org web interface. At the top, there is a navigation menu with links for Home, Downloads, Documentation, Support, Community, Development, Research, Contact, and Site Map. A logo for 'BRO NETWORK SECURITY MONITOR' featuring an eye icon is positioned in the top right corner. The main content area is titled 'Input Files' and includes a 'Load example' dropdown menu set to 'hello'. Below this, a code editor shows a Bro script named 'main.bro' with the following content:

```
1 event bro_init() {  
2     print "Hello, NSF!";  
3 }
```

There is an 'Add file +' button next to the code editor. Below the code editor, there is a 'Use example PCAP' dropdown menu and a section for uploading a PCAP file with a 'Choose File' button and the text 'no file selected'. The 'Bro Version' is set to '2.3'. A blue 'Run' button with a play icon is located below the code editor. The 'Stdout' section at the bottom shows the output of the script: 'Hello, NSF!'.

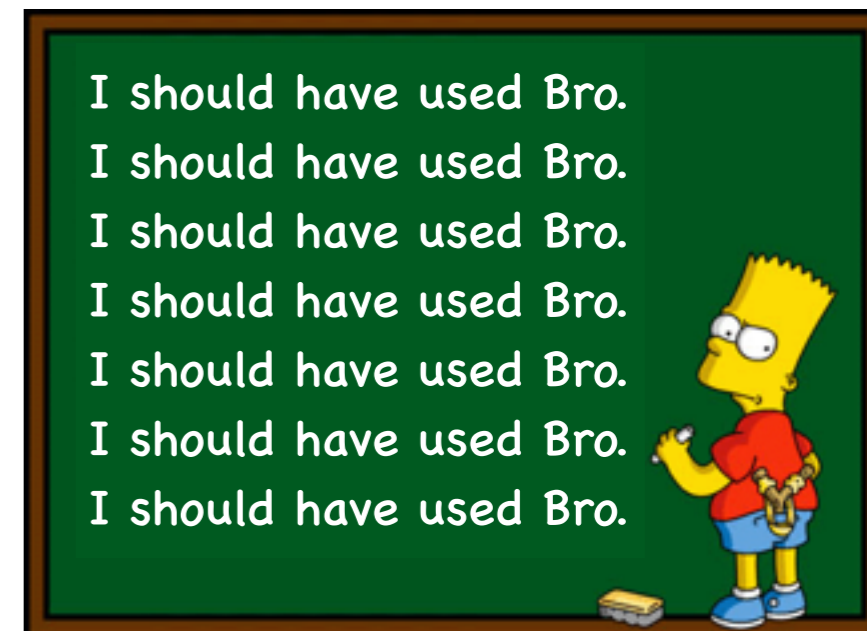
The Bro Teaching Community

People are learning Bro—and they are using Bro to learn.



The Bro Teaching Community

People are learning Bro—and they are using Bro to learn.



Kick-start community of educators teaching (with) Bro.

Exchange experiences, methods, & material.

We provide logistics and technical advice.

Weekly calls, mailing list, repository with seed material, access to team

Our initial solicitation met broad interest.

Universities & colleges, corporate IT, government organizations.

The Center is promoting Bro as a comprehensive, low-cost security capability for the NSF community.

The Bro Project

www.bro.org
info@bro.org

Bro Center of Expertise

nsf.bro.org
nsf@bro.org

Twitter

@Bro_IDS

Facebook

TheBroPlatform

The Center is promoting Bro as a comprehensive, low-cost security capability for the NSF community.

The Bro Project

www.bro.org
info@bro.org

Bro Center of Expertise

nsf.bro.org
nsf@bro.org

Twitter

@Bro_IDS

Facebook

TheBroPlatform

