

Bro Project Overview



Brian L. Tierney

Lawrence Berkeley National Laboratory

Styles of Intrusion Detection



- **Signature Detection:** look for specific, known attacks.
 - Example (from Snort):
 - content:"leb2f 5feb 4a5e 89fb 893e 89f2|"
 - msg:"EXPLOIT x86 linux samba overflow"
 - Many commercial systems (e.g.: ISS RealSecure) use signatures
- **Anomaly-detection:** attacks are peculiar.
 - Approach: build/infer a profile of “normal” use, flag deviations.
 - Very hard to make work in a open science environment
 - Too many false positives
- **Activity-based:** look for activity that deviates from site policy.
 - Examples:
 - user joe is only allowed to log in from host A.
 - Only hosts A and B are allowed to receive email
 - This is the primary approach used by Bro
 - (Bro includes a signature engine too)

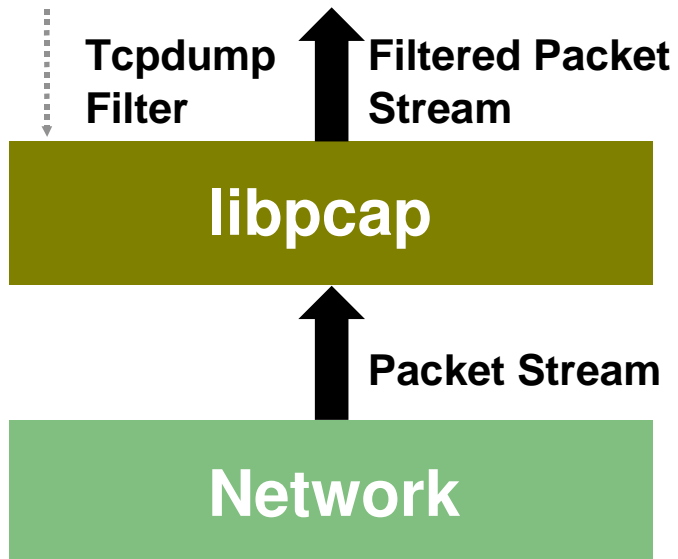
How Bro Works



Network

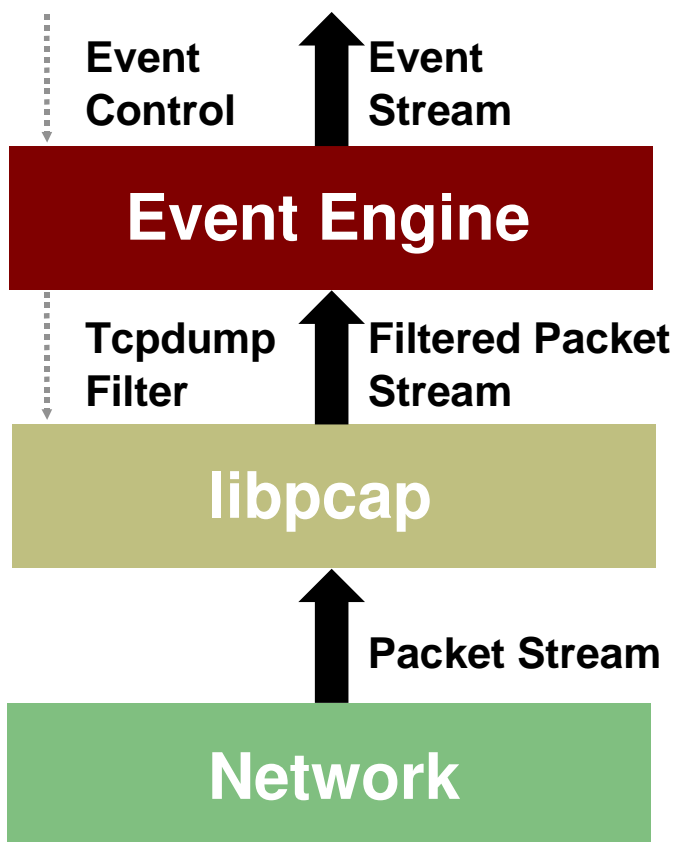
- Taps GigEther fiber link passively, sends up a copy of all network traffic.

How Bro Works



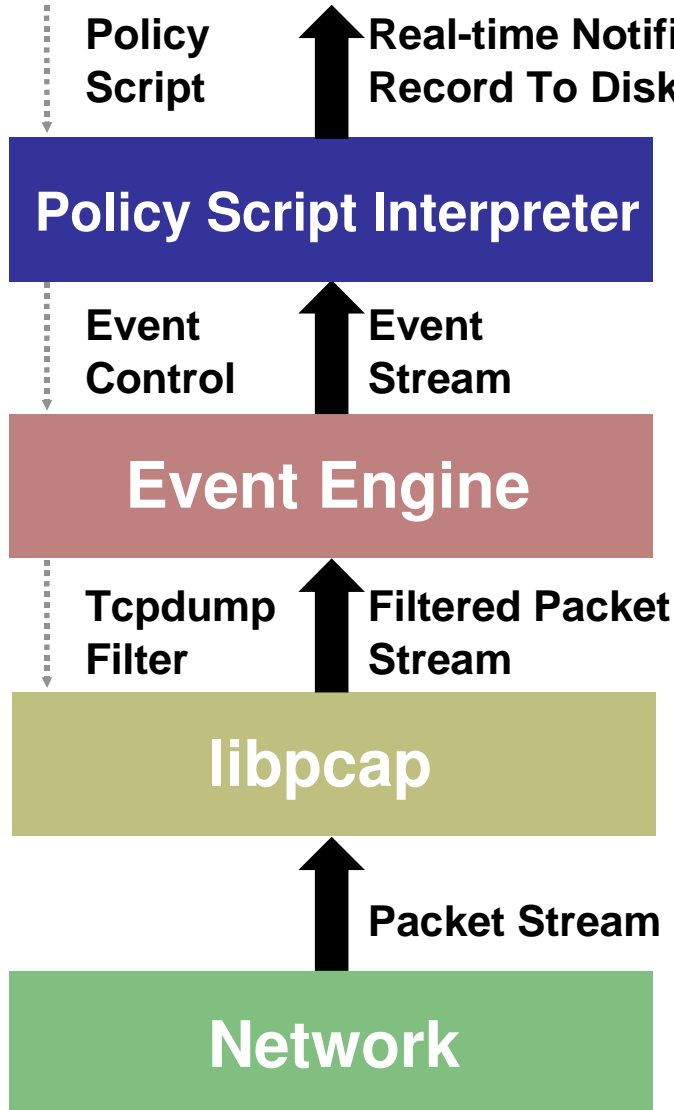
- Kernel filters down high-volume stream via standard *libpcap* packet capture library.

How Bro Works



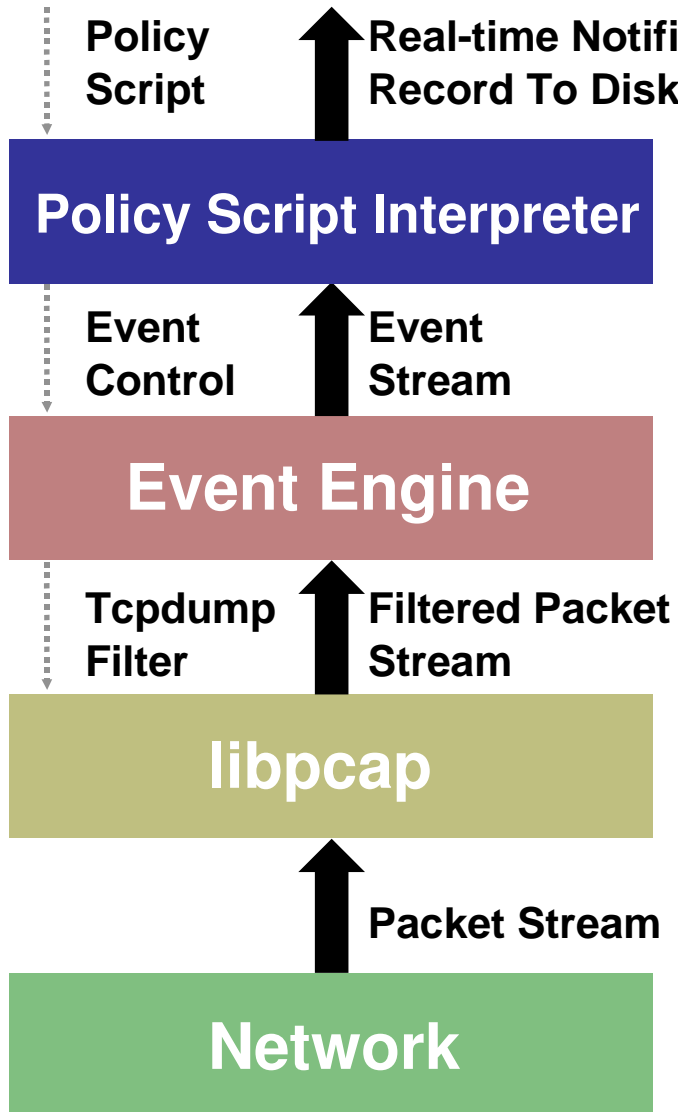
- “Event engine” distills filtered stream into high-level, *policy-neutral* events reflecting underlying network activity
 - E.g. Connection-level:
 - connection attempt
 - connection finished
 - E.g. Application-level:
 - ftp request
 - http_reply
 - E.g. Activity-level:
 - login success

How Bro Works



- “Policy script” processes event stream, incorporates:
 - Context from past events
 - Site’s particular policies

How Bro Works



- “Policy script” processes event stream, incorporates:
 - Context from past events
 - Site’s particular policies
- ... and *takes action*:
 - Records to disk
 - Generates alerts via *syslog*, paging, etc.
 - Executes programs as a form of response

Updated Bro Architecture



Domain-Specific Analysis Language

Protocol Analyzer Specs

Event Stream

Event Engine

~~Static Filtering~~

Full Packet Stream

Network

~~10x - 100x filtering reduction~~

With DPD, must analyze full stream, e.g. to detect botnets

Gbps stream passively tapped

Bro Protocol Analyzers



- Bro includes the following protocol analyzers
 - full analysis:
 - HTTP, FTP, telnet, rlogin, rsh, RPC, DCE/RPC, DNS, Windows Domain Service, SMTP, IRC, POP3, NTP, ARP, ICMP, Finger, Ident
 - partial analysis:
 - NFS, SMB, NCP, SSH, SSL, TFTP, Gnutella
 - in progress:
 - AIM, BGP, DHCP, Windows RPC, SMB, NetBIOS, NCP

Bro Releases



- At any given time, there are 2 Bro releases:
 - Stable release (currently 1.1c)
 - Development release (currently 1.2)
- These are 2 separate source trees
 - Bug fixes from *development* release are backported to the *stable* release
- We test Bro extensively before releasing a new development release, so it should be fairly solid
 - We recommend using the *stable* release if Bro is your primary IDS, and the development release otherwise
 - Please run the *development* release and help us find bugs and improve Bro
- We try to do a new development release every 6-12 months
 - This will hopefully include making the previous *development* release the new *stable* release

What is “Bro-Lite”?



- Bro-Lite was a project 2 years ago to repackage Bro to make it easy to install and configure
- ‘make install-brolite’ does the following:
 - all the needed host configuration and tuning for FreeBSD and Linux
 - Installs a default policy that should be useful for most sites
- See: <http://www.bro-ids.org/Bro-user-manual/Install.html>
- (Project is currently on hold pending continued funding)

Bro Community



- We would like to expand and better involve the Bro Community
- How you can help:
 - Ask / answer questions on the email list (bro@bro-ids.org)
 - Help us document Bro on the wiki
 - http://www.bro-ids.org/wiki/index.php/Main_Page
 - Not open to anyone to edit, but email us for a wiki account
 - Contribute Bro fixes, analyzers, and/or analysis scripts
 - when developing new analyzers, contact us first so we can coordinate
 - Contribute code to the Bro 'contrib' directory
 - Will be included in the next development release
 - Report scripts, database interfaces, etc
 - BSD-style open source preferred over GPL

Who's Who



- Vern Paxson, ICSI/LBNL : fearless leader, grand puba, etc.
- Scott Campbell, NERSC/LBNL : Scan detection, Bro Fabric, etc.
- Holger Dreger, TUM : Dynamic Protocol Detection Work, Bro autoconf
- Chris Grier, ICSI : Windows Analyzers
- Christian Kreibich, ICSI : Broccoli, Bro Packaging, sequence alignment
- Jason Lee, LBNL : Bro Packaging, Bro Cluster
- Craig Leres, LBNL : FreeBSD Guru, PC Hardware Guru, Bro Cluster
- Ruoming Pang, Princeton : BinPac, Packet Rewriting, Bro Core
- Robin Sommer, LBNL/ICSI : Bro core, Distributed analysis, etc
- Brian Tierney, LBNL : Bro Testing, outreach, etc
- Matthias Vallentin, TUM : Bro Cluster
- Nicholas Weaver, ISCI : Shunting Hardware