A Perspective on

Transitioning Research to an Open Source Product

Vern Paxson

EECS Department, University of California
International Computer Science Institute
Lawrence Berkeley National Laboratory
Berkeley, California USA
vern@cs.berkeley.edu

November 28, 2012

Context

- Bro: real-time network monitoring/analysis
  - Grew out of coupling research analyzing tcpdump data w/ operational needs
  - Open source culture (e.g., tcpdump)
  - 130K+ LOC

- Sustained in early years by security operations funding
- Ties with operation = Research Gold
  - Access to data & problems *at scale*

Detecting Stepping Stones

Yin Zhang and Vern Paxson*

Operational Experiences with High-Volume Network Intrusion Detection

Holger Dreger
TU München
Germany
dreger@in.tum.de

Anja Feldmann
TU München
Germany
anja@in.tum.de

Vern Paxson
ICSI / LBNL
Berkeley, CA, USA
vern@icir.org

Robin Sommer
TU München
Germany
sommer@in.tum.de

Synergies & Anti-Synergies

- Building up open-source community can lead to research opportunities:

Enhancing Byte-Level Network Intrusion Detection Signatures with Context

Robin Sommer
TU München
Germany
sommer@in.tum.de

Vern Paxson
International Computer Science Institute and
Lawrence Berkeley National Laboratory
Berkeley, CA, USA
vern@icir.org

- … but focus on practical issues can also go under-appreciated:

Exploiting Independent State For Network Intrusion Detection

Robin Sommer
TU München
sommer@in.tum.de

Vern Paxson
ICSI/LBNL
vern@icir.org

A Delicate Balance

- Need to craft research proposals so that some engineering/development is in scope
  - Tricky in terms of personnel: grad students?
  - Documentation is especially hard (also: training)
  - NSF *Transition Plans* highly helpful here!
    - As is Broader Impact if the story is solid
- NSF Strategic Technologies for the Internet (past) and Software Development for Cyberinfrastructure (present) programs *invaluable*

The Bro Network Security Monitor

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.

Forensics
Bro comprehensively logs what it sees and provides a

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.

Open Source
Bro comes with a BSD license, allowing for free use with

EVENTS

No events scheduled currently.

See past events.

BLOG

Using the ICSI Certificate Notary
11/02/2012

Bro 2.1 Release
08/29/2012

Bro 2.1 Public Beta
08/01/2012

Bro Exchange 2012 Registration Form Posted
06/21/2012

Bro Exchange 2012: Dates finalized
06/11/2012

TWITTER @BRO_IDS