



# Conclusion & Outlook

**Robin Sommer**

*Lawrence Berkeley National Laboratory &  
International Computer Science Institute*

`robin@icir.org`

`http://www.icir.org`

**Bro Workshop 2007**



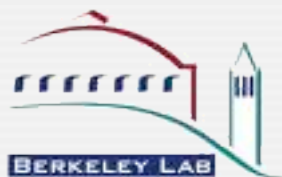
# How to get more information ...

- **Largest problem: Documentation is lacking ...**
  - Especially for new features ...
- **Still, there is quite a bit of information available:**
  - The Bro Wiki contains more current information and is our main documentation platform now. Let us know if you want to contribute.
  - Much of the new functionality is introduced in papers.  
.See [www.bro-ids.org](http://www.bro-ids.org) for a list.
  - The most up-to-date documentation is still the CHANGES file ...
  - The mailing list is open for all kinds of questions, from beginner to expert.  
We try hard to answer all questions even if it sometimes takes a bit.



# Extending Bro

- Many areas for extending Bro:
  - **New policy scripts.**  
Browse through the existing scripts to get a feel how to do analysis in Bro.
  - **New built-in functions** for functionality better implemented in the core.  
Refer to `src/bro.bif` to see how built-ins are implemented.
  - **New protocol analyzers.**  
New analyzers should be written in BinPac (“A yacc for protocol parsers”).  
See the Wiki for more information and look at `src/*.pac` for examples.
  - **New documentation.**  
Whenever you find something out, write it down. We will provide you with Wiki accounts so that all Bro users can benefit.
- All contributions are appreciated.
  - We suggest to coordinate with us for larger projects to avoid duplicating work.



# Real Soon Now ...

- **The Bro Cluster**

- A set of PCs running Bro jointly analyze large network streams
- A central manager system provides a transparent interface
- Prototypes up and running; polishing the user interface now

- **New functionality**

- Time Machine interface  
See <http://www.net.t-labs.tu-berlin.de/research/tm>
- BitTorrent analyzer
- SIP analyzer
- SSL analyzer rewritten in BinPac
- XML analyzer with XQuery support
- NetFlow analyzer



# The Future ...

- **Multi-core Support**

- Going to turn Bro into a multi-threaded application
- Will fully exploit the multi-core potential of modern CPUs
- Involves a comprehensive performance analysis of the core

- **Distributed Data Sharing**

- Extending Bro with functionality required for inter-site cooperation.
- Building a more powerful communication platform
- Providing hooks to tightly control which data is exchanged



# Thanks for your attention.

**Robin Sommer**

*Lawrence Berkeley National Laboratory &  
International Computer Science Institute*

`robin@icir.org`

`http://www.icir.org`

This work is supported by the Office of Science and Technology at the Department of Homeland Security. Points of view in this document are those of the author(s) and do not necessarily represent the official position of the U.S. Department of Homeland Security or the Office of Science and Technology.

