

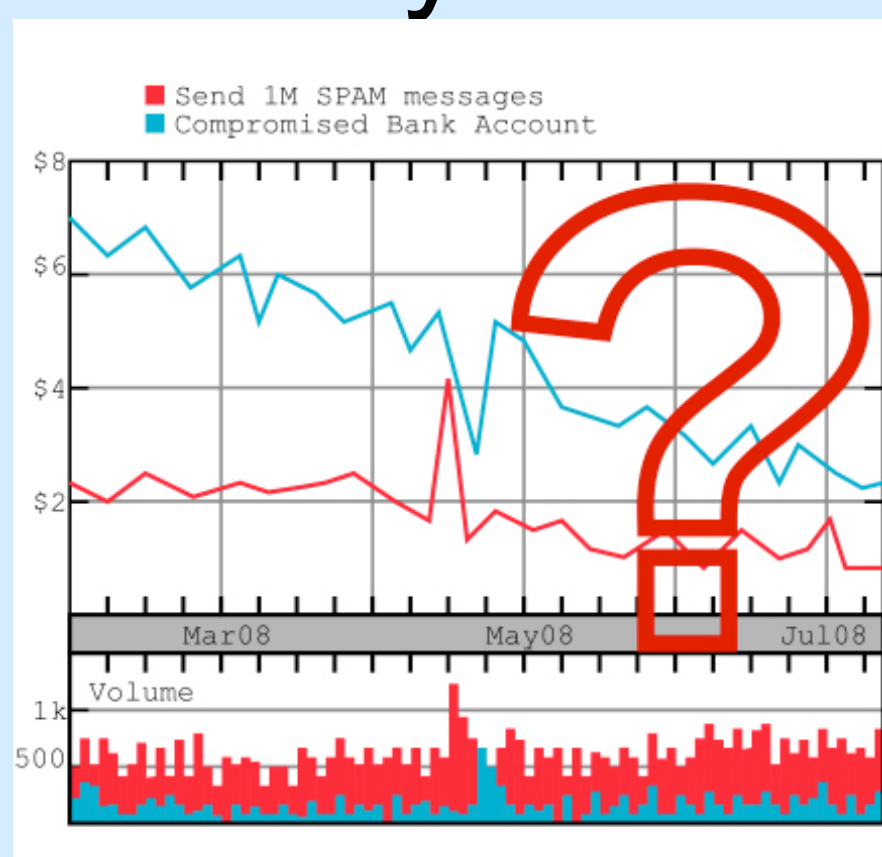
# CyberTrust Research at ICSI

Vern Paxson, Mark Allman, Christian Kreibich, Robin Sommer, and Nicholas Weaver

The International Computer Science Institute, a UC Berkeley affiliated Research Lab, maintains a focus area on network security as part of the ICSI Center for Internet Research ([www.icir.org](http://www.icir.org)).

## Understanding The Underground Economy

Computer crime is now an economic enterprise. When economies reach a certain size, markets form to efficiently exchange goods and services. In association with UC San Diego, we are developing tools to actively monitor these markets.

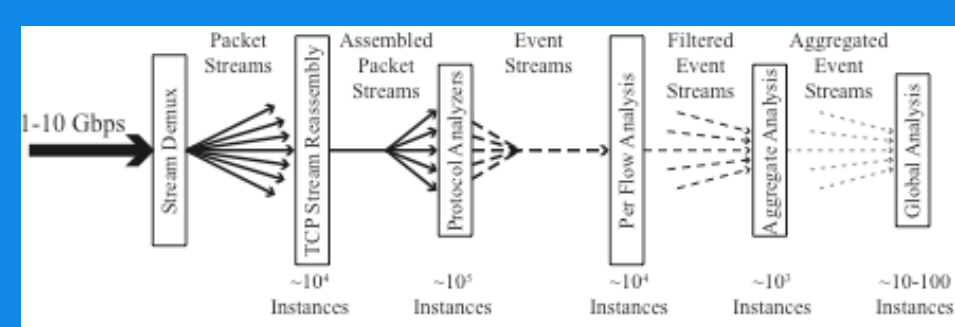


In one initial effort, we have analyzed communications in the **ccpower** IRC channel to develop a model of interrelationships, pricing, and availability in a cybercriminal marketplace. This provides a first step towards estimating the scope and scale of the market and identifying participants and relationships, including the trend towards specialization as some participants sell components for others to use.

In another effort, we are tracking a live spam operation from an inside perspective gained by *botnet infiltration*. From this vantage point we can directly observe the spamming process as orchestrated by the spammer, including developing estimates of list size, delivery efficacy, and spam campaign objectives.

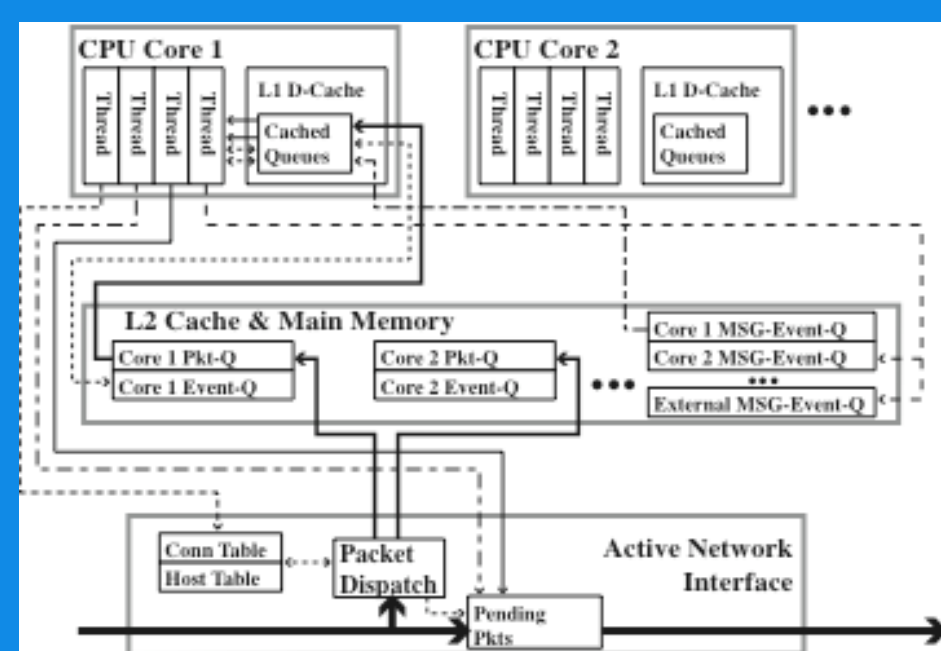
## Parallelizing Network Intrusion Detection

Moore's law has failed. In the past, Network Intrusion Detection systems could rely on processor improvements to keep up with the ever-increasing volume of traffic and complexity of analysis. Now, if we want to continue to improve our performance, we must target multicore processors, for which realizing performance gains requires parallelizing execution.



Much network analysis is amenable to parallelization since many work elements consists of "per flow" analysis.

Drawing upon the parallelism we previously developed for our scalable Bro cluster implementation, we are now pursuing a model for fine-grained operation on multicore systems, validating this approach using program traces. Unlike cluster operation, multicore execution holds promise for much deeper scalability for global analysis and reporting, with significantly lower communication overhead.



## Situational Awareness Across Time and Space

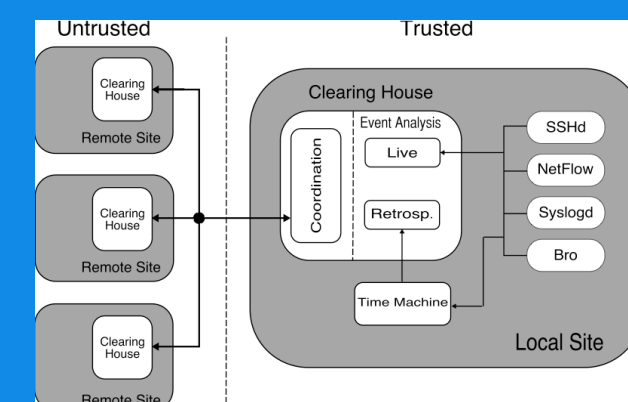
When a significant compromise occurs, questions arise: How was my network compromised?

What were the attacker's goals?

Has this happened before?

Will this happen again?

Who else was affected?



Our work in Internet Situational Awareness attempts to address the final three questions by developing a unified framework, **VAST (Visibility Across Space and Time)**, to extend the notions of policy and programmability present in the **Bro IDS** across time and multiple institutions. Like our previous **Network Time Machine**, **VAST** seeks to record traffic en masse. But instead of recording low-level packets, **Vast** records policy-neutral *activity events*.

After an incident, an analyst can construct a **Bro** program to both look for similar behavior in the past and to install a trigger to automatically watch for such behavior in the future. In the longer term, we envision tying together VAST systems at different sites to allow others to determine if they faced similar attacks, and to provide a viable means for cross-site security analysis.

## Web Tripwires

In an unfortunate trend, ISPs have begun using Layer-7 analysis to profile users and then to inject advertisements into Web pages without the consent of either the client or the server.

Malcode and attackers have also used this technique to compromise hosts by injecting exploits into a victim's Web surfing, while users may modify pages (such as stripping ads) in ways that subvert a content provider's economic interests.

With colleagues at the University of Washington, we have developed and tested **Web Tripwires**. These small JavaScript programs assess whether a Web page was modified.

We conducted a user survey of over 50,000 IP addresses by deploying a tripwire setup publicized by slashdot, digg, and other sites. 657 IP addresses exhibited some change. Most were client programs designed to reformat pages and remove advertisements (some with exploits discovered by this research), but we also detected advertisement injectors, malcode, and ISP-deployed cache rewriting that attempted to reduce traffic by recoding Web pages.

