From the Reviews*

—-

What follows is a lightly edited selection of interesting, supportive, and contrary tidbits from the program committees reviews of the papers selected for HotNets V. The first, italicized paragraph summarizes the paper. The editing has conflated comments made by different program committee members, so I may refer to a melded PC hive mind rather than an individual. Of course, reviews reference the *submitted* versions of the accepted papers. The authors have addressed some, but not all, of our comments in their final copies; its interesting to see which comments led to revisions. We hope you enjoy this look behind the curtain.

FIGHTING COORDINATED ATTACKERS WITH CROSS-ORGANIZATIONAL INFORMATION SHARING

Outlines the design of a system to allow a small number of sophisticated network monitors ("detectives") to make use of observations made by large numbers of other machines ("witnesses"). The network monitors use the observations of witness machines to aid the discovery of bad actors in the network (e.g., a bot net). The query mechanism ensures that private information isn't revealed to witnesses, and that witness replies are believable, via a combination of hashing and encryption.

This paper is well written and describes an interesting vision. The high-level concept sounds great: it's an excellent idea to draw on observations from multiple places taken with "simple and generic traffic monitoring devices", and the scheme for sharing information seems very cunning.

The architecture of the described system is clear, but its potential benefits are only alluded to. Testing the ability of witnesses to aid the detection of bots via control traffic would be a great addition.

Another deterrent for the detectives who would consider "fishing" for private data at the witnesses is post facto auditing. If the logs at the witness show that a detective was engaging in impermissible fishing, that detective might be excluded from the system. As it is probably hard to get in, this would be a serious disincentive. Relying more on this disincentive could allow more query flexibility.

This is nice work that will most certainly move forward the efforts to put together a network-wide defense against many classes of computer hijacking techniques. The biggest problem I have with this paper is that the entire solution was pretty predictable, and the problem statement itself had nothing surprising either.

The paper leaves a lot of questions unanswered. Witnesses "log the facts", but what does this actually entail? How long are records kept for? And with how much detail? If a single witness can reveal "a wealth" of information about which hosts have downloaded the code, then witnesses are expected to be in the network, i.e., routers. If witnesses might be highly resource-constrained then it's even more important to think about the storage and processing costs of being part of this architecture. How do detectives locate witnesses? Does a witness somehow advertise itself? Since witnesses must run the software to answer queries from detectives, there's an upfront commitment to participating, so presumably this information could be stored centrally. Does every detective need to know about every witness? How much coverage of the Internet by witnesses would be required for the system to be effective? Are there timeliness constraints on queries (surely there need to be)? Also are witnesses aware of the identity of detectives? Is the encryption of returned tuples primarily intended to hide the extra records produced by collisions from the detective? or to hide the information from third-party observers? or to verify the witness's statement (in which case a cryptographic MAC could have been used instead of Kerberos-style abuse of encryption)? Maybe it's all

*This public review appeared in the HotNets V proceedings.

three? More explicit mechanisms would help disambiguate this question (e.g. using MAC and encryption would make it clear that both privacy and verification were desired).

So full of holes it will probably generate plenty of discussion.