Contribution ID: **89** Type: **Presentation**

# Spam Analysis-Confronting Security Threats and Trends in today's world

*Tuesday, 13 May 2008 15:30 (40 minutes)*

Today's spam and its effect on lab security:

The increasing maliciousness of hackers coupled with the cleverness of spammers to bypass spam filters and penetrate our networks with viruses and malware is a problem demanding acute attention. Recent incidents of virus and malware attacks have been severe enough for some DOE facilities to have lost domain controllers and data and been forced to shut down operations for several days.

Five perspectives solution:

The problem must be addressed from five main categories: increased knowledge of how virus and hacking infiltration occurs, awareness of current spam trends being used, information on available email defense systems, implementation of these systems and finally, a methodology of joint effort and outstanding communication between key teams.

A multi-tiered approach:

The overall approach is to utilize spam analysis and virus detection software on several layers of protection.

Effectiveness:

The keys to effective protection are proper configuration and a methodology which outlines fast team interaction. For example: teams create custom policies and monitor mailboxes created to work in conjunction with those policies.

Conclusion:

Current use of email as a means for sophisticated phishing and virus attacks directed at national lab security is a modern threat and a reality. A multi tiered approach is a key prevention factor.

**Primary author:** CANTRELL, Leslie (Sandia National Laboratories)

**Presenter:** CANTRELL, Leslie (Sandia National Laboratories)

**Session Classification:** Tuesday Breakout 1