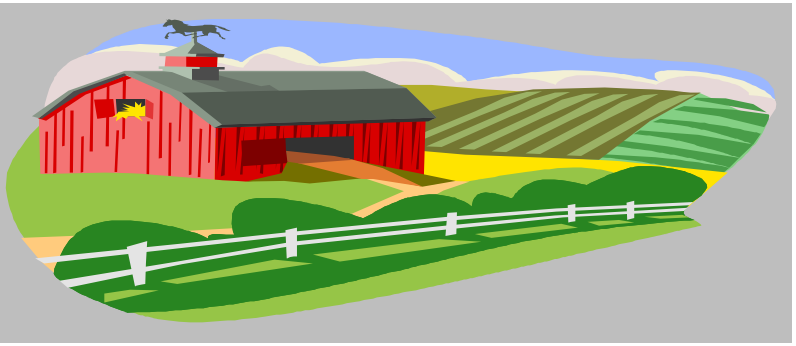
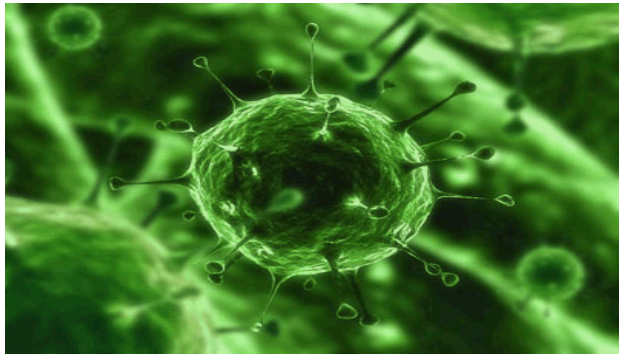
SAND2014-0832P

*Exceptional service in the national interest*

Sandia National Laboratories





# FARM

Levi Lloyd and Ken Chiang

U.S. DEPARTMENT OF ENERGY | NNSA

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

# Malware is a problem

- Exponential growth in the number of malicious files
- Limited analyst resources available
- Sensitivities around malware infections make sharing and collaboration difficult
- Researchers need access to malware and analysis results to develop tools

# FARM to the rescue

Sandia National Laboratories

- Forensic Analysis Repository for Malware
  - Scalable
  - Static and dynamic analysis
- Saves time and resources
  - Automates much of the malware analysis
  - Speeds up incident response and malware triage
  - Uncovers relationships between malware files
- Promotes information sharing
  - Users from different organizations can share malware files and analysis results
  - Hash-based reputation database
- Easy to integrate with other tools

# Ongoing Research

Sandia National Laboratories

- Clustering
- Similarity Detection
- VM introspection for dynamic analysis
- Generic Unpacking
- Mobile malware analysis