One of our master’s degree students Roy Nielsen (You may contact him at roy.nielsen17@gmail.com.) works at Los Alamos National Lab (LANL) and desires collaboration on building out the functionality of Stonix to include the yet un-implemented rules. If that might be interesting to you, please read his description below and contact him directly.

-------------

Two security tools have recently been released to secure non-windows systems. These projects could be the basis for graduate research, projects and reports.

One project comes from the National Security Agency (NSA), called Simple Integrity Management Platform(SIMP)(NSA, 2015). An introduction to SIMP can be found on their github repository:

“SIMP is a framework that aims to provide a reasonable combination of security compliance and operational flexibility.

The ultimate goal of the project is to provide a complete management environment focused on compliance with the various profiles in the SCAP Security Guide Project and industry best practice.

Though it is fully capable out of the box, the intent of SIMP is to be molded to your target environment in such a way that deviations are easily identifiable to both Operations Teams and Security Officers.”

Another project released by the Department Of Energy's(DOE) Los Alamos National Laboratory(LANL) called the Security Tool On *nix(STONIX) also has the goal of security and flexibility. One paper gives a brief description of Stonix as the following:

“National laboratories with oversight from the National Nuclear Security Administration are required to manage their computers diligently. We follow NIST, DISA, NSA, CIS and other guidance for securing computer systems. About a decade ago, we developed tools to harden systems to an amalgamation of these security standards. Some of these included the Security Tool On Mac(STOM)(Marcus, 2008) and Security Tool on RedHat(STOR)(Kennel, 2009). Running the security tool is required for a machine to be put on the network. The Los Alamos National Laboratory(LANL) unix community wanted support for other unix related operating systems, but we did not have the manpower to accomplish this.

We are now working on a security tool we call Security Tool On *nix or STONIX(Kennel, 2014). This tool will harden unix related systems using methods similar to STOM and STOR. STONIX will cover a wide variety operating systems, such as RedHat, Ubuntu, Debian, BSD, Gentoo, Solaris, Mac OS and derivatives. As of now, developers test their own code in their own virtual machines, which leads to inconsistencies in testing process and results.”(Nielsen, 2014)
Potential graduate collaboration could include some of the following:

- Analysis of automated test suites for testing these products
  
  Tools such as Jenkins, Bamboo, Buildbot, TeamCity, TravisCI running automated tests potentially on virtual systems, for speed and consistency. Nightly build vs. trigger on check-in.

- Analysis of project tracking tools that could be used for projects like SIMP and STONIX
  
  Frameworks such as Redmine, Trac, Sourceforge and Jira. Which are more applicable to specific development styles such as agile or the old waterfall method?

- Analysis of a network, which tool would work better and why? (performance, simplicity, etc)

  Specify a network such as:

  - Education: Wireless computer lab at a community college
  - Government: Top secret network
  - Industrial: Network of 3d printers and CNC machines
  - Business: Infrastructure for a large Computer Chip Manufacturer
  - . . . and others

- Presentation of Stonix and/or SIMP at a conference.

  - Why the tool is needed
  - What the tool does
  - How mature are the products
  - Sample Application
  - A summary of any of the above projects

- Writing the results of any of the above for a scholarly journal

- A project performing one of the above topics and publishing the results

  - Simulate specific network: 3d printers – simulate with several embedded devices such as the Raspberry Pi, Banana Pi, Parallela, or other embedded devices networked together
  - Simulate specific network: using a large server and several to many virtual machines

References:
