

## **The DoD DC3 2011 Digital Forensic Challenge Competition**

Dr. Tu supervised a graduate team from DSU and has earned the #1 US Graduate Team in the 2011 Department of Defense Cyber Crime Center (DC3) international competition to test skills in digital forensics science. The DC3 challenge is an online competition which requires participants to perform a series of tasks throughout the year, challenging participants to discover information deleted, encrypted, encoded or hidden by using other sophisticated mechanism in digital media. The competition consists of challenge questions with or without known solutions.

The DSU team members are awarded with a trip to the 2012 Department of Defense Cyber Crime Conference in January in Atlanta, where the team will be formally recognized and receive the awards.

The graduate students involved are Brian Edwards and Jason Nikolai. For more details, please refer to <http://dc3.mil/challenge/2011/stats/winners.php>.

### **Project: Information Security and Forensics in Distributed Business Information Systems.**

Dr. Tu supervised NSF REU undergraduate students as well as DSU graduate students engaging in the project on information security and forensics in distributed business information systems. Their work analyzes and models the potential malicious activities which exploit the vulnerabilities existed in distributed business information systems. Anomaly detection and malicious source tracking algorithms were provided to prevent and control such activities. Automatic event reconstruction mechanisms and tools are being developed to aid the quick response to security incidents. The results yield a few papers published and to be published in peer-reviewed conference and journals, and one of them has recently won the Best Paper Award in an International Conference (IASTED PDCS 2011).

The REU students involved are: Logan Smith, Eugene Butner, Mikal Ustad, and Tom Swiftbird. The graduate student I am current work with is Raj Nepali.

Paper:

- E. Butner and **M. Tu**. Forensic Readiness through augmented attack graphs. In *Proceedings of 2011 Mid West Instruction and Computing Symposium (MICS'11)*, April 2011.
- **M. Tu**, D. Xu, Z. Xia, Logan Smith. Securing epidemic based update protocol for P2P systems. In *Proceedings of IASTED PDCS 2011*. Best Paper Award, December 2011.
- **M. Tu**, D. Xu, E. Butler, and M. Ustad. Locating and identifying forensic evidence for attacks against online business information systems by using honeynet. *Journal of Digital Forensics, Security, and Law*, Elsevier. major revision, November 2011.