

# APT Proposal

Title: **Automated System Intrusion Discovery (ASID)**

Supervisor: Dr. Guillermo Francia, III

Keywords: Computer Security, Windows Registry, Security Assessment, File System Check, Process Monitor, Intrusion Discovery

Objective: To develop a system tool that will automate the process of intrusion discovery.

Description: The purpose of an intrusion detection system (IDS) is to detect unauthorized access or misuse of a computer system. IDSs are to computers as burglar alarms are to homes. They raise alarms and, at times, may even take corrective actions when needed. Detection schemes generally fall into two main categories: statistical anomaly detection and pattern-matching detection. Statistical anomaly detection looks for behavior that deviates from the norm. Pattern-matching detectors look for behavior that matches a known attack scenario.

The APT requires the design of a system tool that will automate the process of intrusion discovery through pattern-matching and the implementation of the design in either the Windows or the Linux operating system. The implementation tools are primarily limited to the scripting tool available in each operating system. Students will be provided with tutorials on Windows and Linux shell scripting techniques, the Linux **Cron** facility, the Windows **Scheduled Tasks** tool, the detection of compromised systems, and the methods of attack investigation.

Timing: (25 days total)

- Attend tutorial lectures (3 days)
- Research (3 days)
- Design (3 days)
- Implementation (10 days)
- Testing (3 days)
- Report and presentation preparation (3 days)

References:

- [1] Axelsson, S. and Sands, D. Understanding Intrusion Detection Through Visualization. Springer-Verlag. 2005.
- [2] Intrusion Detection System FAQ. SANS Reading Room. Website: <http://www.sans.org/resources/idfaq>. Access date: December 07, 2006.
- [3] Gite, Vivek. "Linux Shell Scripting Tutorial v1.05r3. A Beginner's handbook." Online version. Website: <http://www.freeos.com/guides/lsst>. Access date: 12/01/06.
- [4] Windows Script Center. Website: <http://www.microsoft.com/technet/scriptcenter/default.mspcx>. Access date: 12/07/06.
- [5] Scripting with Windows Power Shell. Website: <http://www.microsoft.com/technet/scriptcenter/hubs/msh.mspcx>. Access date: 12/08/06.
- [6] Lunt, Teresa F. A survey of intrusion detection techniques. In *Computers and Security*, 12(1993), pages 405-418.
- [7] Mukherjee, B, Heberlein, T. and Levitt, K. Network Intrusion Detection, IEEE Network, May/June 1994, pages 26-41.