

Cal Poly Campus Anti-Spyware Initiative – 3/14/05

IRMPPC Actionable Recommendation: Implement Spring 2005, Complete by August 2005

Cal Poly will proceed with implementation of an enterprise, integrated anti-spyware solution and strategy that includes faculty, staff and students (ASI/Foundation/State) for on and off-campus users.

The Problem

In the last year there have been significant increases in the volume and complexity of security related incidents attributable to spyware involving campus workstation, laptops and servers. These incidents have negatively impacted campus productivity and required the costly intervention of ITS staff and LAN Coordinators in the Colleges and Divisions. Increasing regulatory and audit compliance pressures are also requiring more stringent security to be implemented at the campus workstation and server level.

Similarly, the broader Cal Poly computing community continues to experience a significant increase in the number of spyware attacks that have directly impacted teaching and learning activities, have resulted in data and security breaches, and/or have generally decreased productivity.

Spyware has outpaced viruses as a primary threat to campus computing.

Solution Strategy

Cal Poly needs to adopt an integrated, campus-wide approach to anti-spyware to address these issues which should include ASI, Foundation, State and Auxiliaries. The solution would be available to faculty, staff, and students. Active involvement of ITS and LAN Coordinators is essential and a phased implementation methodology should be adopted. The following documentation should inform and guide this process:

- Cal Poly's Information Security Program
- Cal Poly's Responsible Use Policy
- CSU audit recommendations
- State and Federal legislation mandates
- Industry Best Practices

Goals

- Reduce on-campus disruptions that impact teaching and learning, the administrative processes of the university and the productivity of students, faculty and staff.
- Protect confidential information.
- Ensure campus compliance with state and federal legislation regarding the protection of sensitive personal information.

Existing Campus Products

Cal Poly currently utilizes two anti-spyware solutions – even when combined, they are inadequate in fighting off the complex attacks.

The primary anti-spyware solution is included in the Cal Poly site license for Symantec anti-virus software; test results indicate it is roughly 30% as effective as other anti-spyware tools. The secondary anti-spyware solution utilized by Cal Poly is Spybot Search and Destroy; this is a standalone freeware product and does not offer centralized management or reporting.

It is industry consensus that no single solution exists to completely protect against spyware attacks; it is also industry consensus that “doing nothing” is not an option. Cal Poly recognizes that this conundrum; the situation is no different than existing anti-virus solutions (e.g. no targeted tool will ever prevent, detect, or remove all spyware).

To fully “clean” a compromised computer, the only sure method is a complete reinstallation of the operating system, applications and data.

Cal Poly Community Requirements

As a result of on-going dialog with the LAN Coordinators, campus computing committees and ITS, the following needs for an enterprise anti-spyware solution have been identified:

- Automated updates of server and clients (manual updates by exception)
- Available to the campus community 24 X 7 X 365 (failover)

Cal Poly Campus Anti-Spyware Initiative – 3/14/05

- Available services on and off-campus (mobile users)
- Ability to designate groups at department, college or division level
- Anti-spyware screening that occurs in real-time and is seamless to the user
- Real time reporting to allow response to new attacks before reaching an epidemic level
- Reporting capabilities for trend analysis to improve protection of the campus
- Quarantine capabilities at the client level for isolation of new spyware
- Centralized client management to enable prompt updating against new threats
- Centralized administration and hardware to reduce overall cost to the campus

Service Metrics and Cost Analysis

Remedy service-request metrics that are formally submitted indicate 140 specific campus spyware attacks/incidents since September 2004. In consultation with LAN Coordinators it was determined that over 300 computers were infected during this same period. Normally, two hours per incident are required for “average” infections and ten hours for “severe” infections to remove of spyware to return the computer to service.

As a conservative campus estimate, using both LAN Coordinators and student assistants, the remediation cost for spyware is \$60,000 per year. The productivity impact to users, disruption to teaching and learning activities far exceeds this number.

Industry projections conservatively estimate that 85% of all computers have some level of existing spyware infection. It is projected that the number of spyware attacks and infections will substantially increase in the next year.

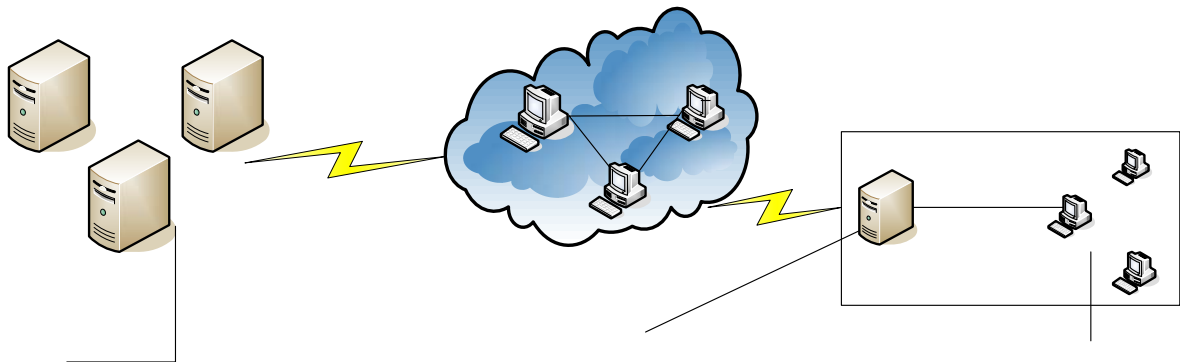
It is projected that the proposed campus enterprise anti-spyware solution will have a payback period of less than six months.

Recommendation Solution

The candidate of choice for an *enterprise* anti-spyware solution is Webroot SpySweeper. The recommendation is based upon input from LAN Coordinators over the past year to establish anti-spyware requirements; extensive research of industry simulation and testing; Cal Poly hands-on pilot testing (e.g. ITS, open access computing labs, Service Level Agreement); competitive quotes and client reference checks.

Campus Implementation and Standards

Webroot will be implemented in a phased approach, utilizing the existing and successful anti-virus infrastructure model. As a result, centralized campus standards are established with decentralized management and reporting capabilities. This model ensures the most current anti-spyware definitions are pushed to all computers, real-time and regularly scheduled scans are performed. The following high-level diagram illustrates the Cal Poly Webroot implementation model.



Timeline and Funding

Webroot will be implemented in a phased approach, beginning Spring 2005 and completed by August 2005. ITS is funded for the two-year agreement for on-campus users.