

ITS Emergency Response Protocol for Removing Networked Devices* From the Cal Poly Network

Overview

The cost and risk to the campus from a potentially compromised system must be weighed against the potential impact of an individual user or service being temporarily disconnected from the network.

The large number of infected devices has overwhelmed the limited number of human resources available to identify and repair them. Invoking the emergency protocol will enable technical support staff to identify and repair the backlog of vulnerable machines without adding to the problem. ITS is currently surveying campus technical staff to assess the cost to mitigate this current crisis.

An operating system that has not been properly patched can be readily detected and exploited by a virus or worm, and used to launch a network attack. Leaving a vulnerable system on the network for even a short period of time can put the University at high risk of infecting other computers, which adds to the human cost of identification and repair.

Given the current situation, ITS has determined that the cost and risks to the University are significant enough to warrant temporarily invoking this emergency protocol.

We recognize that this new protocol may result in false positives: systems displaying the symptoms of infection (but not actually infected) may be disconnected as well. However, this can only be determined by checking the suspect system after the fact.

When invoked, the following message will be posted on the website linking to the emergency protocol:

“Due to the severity and extent of campus systems infected by or suspected of being infected by recent worms and/or viruses, Information Technology Services has temporarily invoked an emergency protocol for removing devices from the campus network. This protocol will remain in effect until the number of potentially infected devices (currently estimated to be XX) is substantially reduced.”

Other Actions

The California State University (CSU) Network Operations Center recommends blocking traffic at the firewall on several network ports to mitigate the recent worms. Cal Poly has chosen to block activity on the most problematic ports to minimize the impact on users.

As of 10/14/03, approximately 60 campus systems have pinholes in the firewall at the vulnerable ports. ITS is currently assessing how much these systems have used these pinholes since the firewall was implemented.

We will be providing that information to the appropriate LAN Coordinator and asking them to reaffirm the academic, research or campus requirement for maintaining these pinholes for the systems in their college or department.

If the department confirms that it is no longer necessary to use a pinhole, ITS Network Administration will close it.

If the department validates that continued use is necessary, the department will be required to apply and maintain current virus protection and operating system security patches or risk being disconnected if a problem occurs or the protocol is invoked.

If departments are not responsive and problem systems are not corrected, the issue will be escalated by ITS to the appropriate campus administrator for action.

Once the current crisis has abated, the emergency protocol will be discontinued and ITS will revert to its standard protocol for disconnecting systems from the network, which is posted on the web at <http://security.calpoly.edu/policies/index.html>.

ITS will continue to investigate long-term strategies and solutions for preventing and mitigating vulnerabilities on a campus level.

IACC Recommendations

IACC recently reviewed and endorsed the emergency protocol and other proactive steps to mitigate such risks. In addition, they recommended finding secure and expedient methods for identifying vulnerabilities and disseminating information and patches to the campus individuals responsible for ensuring that systems are secured and remedial steps are taken, e.g., a secure website that is password protected. Finally, they requested a checklist or other tool for verifying that systems are clean. They suggested that these be referenced in the protocol.

ITS Emergency Response Protocol for Removing Networked Devices* From the Cal Poly Network

Purpose

The procedures below outline steps taken when removing a device from the Cal Poly network during a major outbreak (e.g., virus or worm-related infections) or emergency situation that may put the campus community and the University at high risk. This risk includes exponential growth in the number of affected systems due to one potentially infected system remaining connected to the network, liability for damage to systems on and off-campus, loss in employee productivity, and substantial investment in human and other resources required to identify and repair each affected system. The intent of this protocol is to reduce such risks by preventing a potentially infected system from accessing the network until it is determined to be harmless. We have experienced incidents that can proliferate at such rapid rates that we must at times act on both clear evidence and symptoms pending full diagnosis to isolate and interdict and protect broad impact on our operational capability.

Background

This protocol is consistent with the "Information Technology Resources Responsible Use Policy" (RUP) and "Procedures for Removal of Networked Devices From the Cal Poly Network" as posted on <http://security.calpoly.edu/policies/index.html>.

Under Policy Application, Item #3, the RUP states:

"The University reserves the right to limit access to its resources when policies or laws are violated and to use appropriate means to safeguard its resources, preserve network/system integrity, and ensure continued service delivery at all times. This includes monitoring routing information of communications across its network services and transaction records residing on University resources, scanning systems attached to the Cal Poly network for security problems, disconnecting systems that have become a security hazard, and restricting the material transported across the network or posted on University systems."

The procedure specifies:

In instances where the Cal Poly network is being placed at high risk by the offending network device or a serious security threat exists (e.g., denial of service attacks), ITS will remove the offending device from network connectivity before alerting the responsible party (advisor, owner, LAN coordinator, etc.) of the removal. The notification will take place as soon as possible before, during, or after the removal.

This protocol is consistent with and complies with the current campus and California State University (CSU) network, responsible and acceptable use and security policies, and reflects best practices as recommended by the CSU, national information technology security organizations, and other institutions of higher education.

ITS Emergency Response Protocol for Removing Networked Devices* from the Cal Poly Network:

- 1) If the Office of the CIO (OCIO) in Information Technology Services (ITS) determines, based on complaints, security alerts, network/system logs and/or other reliable evidence, that an emergency situation/outbreak exists, the OCIO may invoke this emergency protocol. The primary point of contact for authorizing use of this emergency protocol is the VP/CIO and/or the Policy Assurance Officer.
- 2) The OCIO will notify appropriate campus technical support staff and the Campus Information Security Officer that the protocol is being invoked and why. They will then actively seek and report status on actions and progress towards assessing and controlling the incident(s) and threat(s) as well as restoring full functioning and protection of our campus resources and network assess.
- 3) Using standard network diagnostic tools or information provided by the OCIO or other internal sources, ITS Network Administration will identify potentially infected systems by IP and hardware address and block access at the campus network.
- 4) ITS Network Administration will update an Excel spreadsheet with the following information for each IP address:
 - a) Hardware address
 - b) VLAN
 - c) Router
 - d) Identifiable Owner and Contact Information
 - e) Date Blocked
- 5) ITS Network Administration will attempt to notify the listed owner of the device by phone within 2-4 hours of access being blocked. The campus directory listing will be used. This may be an individual user, LAN Coordinator, or department office. Voice mail will be left if the individual does not answer the phone. A written notice may also be posted at the individual's office. Email may be used to notify the system owner if the affected system is not the owner's individual workstation. Notification will specify which computer has been blocked and why and ask the system owner to contact the ITS Service Desk (805-756-7000) for more information.
- 6) ITS Network Administration will create a Remedy ticket for each identifiable system.
 - a) All Remedy cases will be initiated with the system owner/user as the requester.

- b) Network Administration will update the Remedy ticket work log with time spent creating the ticket (3 minutes) and notifying the user (45-60 minutes depending on whether the individual was reached).
 - c) Network Administration will reassign the Remedy ticket to the appropriate college/departmental technical support group or ITS Specialized Support Services for remediation and updating.
 - d) Network Administration will create a group Remedy ticket for all unknown users or DHCP addresses that have been blocked and update the ticket with the boilerplate time spent per address.
 - e) Network Administration will notify the LAN Coordinator based on the subnet for DHCP and, if they acknowledge the use of the DHCP, reassign the Remedy ticket to the LAN Coordinator for remediation and updating.
- 7) ITS Specialized Support Services will work with users and LAN Coordinators to diagnose and repair individual systems as needed. This includes running diagnostic tests, applying current operating system patches and updates, installing and updating Cal Poly's anti-virus software and definitions, and finally verifying that the system is free of any viruses and worms.
- 8) The responsible technical support group will update the Remedy ticket work log with information about the type of infection, steps taken to correct it, verification that it was successful and a request to reinstate network access. Those without Remedy access will provide the same information to ITS Specialized Support Services or ITS Network Administration so they can update the Remedy ticket accordingly.
- 9) ITS Network Administration will unblock the hardware address within two hours of initial notification by ITS Specialized Support Services or the responsible LAN Coordinator that the affected system no longer represents a risk to the campus.
- 10) ITS Network Administration will update the network database and DNS, if applicable; update the Excel spreadsheet with date and time; provide the updated spreadsheet to the following ITS offices: OCIO, Service Desk, Specialized Support Services, and Central Systems Administration; and resolve the individual Remedy ticket or remove the IP address from an existing group Remedy ticket. Boilerplate time for releasing, documenting and closing the case is 20 minutes.
- 11) A weekly progress report will be provided to the OCIO to determine if escalation or intervention is required in specific areas or to discontinue the emergency protocol. The OCIO will update the Campus Information Security Officer regarding status.

Contact Information

Information Technology Services, Office of the CIO
Policy and Program Assurance
Mary Shaffer, mshaffer@calpoly.edu
Office: (805) 756-5538
FAX: (805) 756-2000

- A networked device includes but is not limited to the following types of equipment assigned to individuals, departments, clubs, auxiliary organizations or individuals from off-campus utilizing university network resources: personal computers, laptops, workstations, wireless devices (e.g. PDAs, laptops, handheld phones, base stations or pods), networked printers/copiers, servers, switches, routers, firewalls, network security devices, network appliances or any device that is network-capable and connected to university network resources.