Logging failed authorization attempts and an install request form using the sudo plugin API

(title pending)

Tim Ransom

I. Abstract

One of the most useful and commonly installed applications on Unix based systems is the utility `sudo`. This application is critical for live maintenance and highly configurable to fit the requirements of any system. In particular `sudo` has implemented a plugin system allows administrators to add their own functionality. We use this API to log the failed attempts of users and produce metrics for administrator review.

II. Background & Motivation

System administration often involves data collection that is transparent to the system users. The amount of resources used in the execution of their applications, the times and locations where resources are most accessed, and additional privileges requested for the execution are examples of potentially useful data points. There is a common access point for escalated privileges, namely the `sudo` application.

Unix users often absent-mindedly invoke `sudo` when on a command prompt attempting to install software, access files, or use additional resources (eg run a webserver). Many system administrators have enabled an automated email to be sent on a failed attempt but simply ignore the message. The amount of information in each message is too low and difficult to contextualize to warrant the attention of the busy and wonderful systems staff. This motivates an application to aggregate and present this information rather than inundate email with every data point.

Some users who are aware that emails are sent on failed attempts will intentionally spam attempts in order to gain the attention of the systems staff. These users are likely to forgo this practice when the time penalty for it is raised. The `sudo` plugin API allows a 'conversation' with the user when a failed login attempt requesting a package install has been parsed. Asking if the user wants to fill out a form can make the user feel more heard in their request and save unneeded emails.

III. System Description

A. Failed attempt logging

The `sudo` plugin API (introduced in version 1.8) is accessed through either a compiled dynamic shared object or through statically compiling the policy into the `sudo` binary itself. Testing and deployment of this logging and install form policy will be handled through the shared object route for ease of deployment.

The logging of failed attempts is fairly simple; when the policy is activated a message is logged and then gathered nightly to be processed. The logging has two possibilities - either in a local, encrypted, temporary file which would be simple to implement or through a dbus access to journald which would be more efficient.

Gathering of logs will be handled by a single node and happen while resource requirements are low in order to not bother the users. Frequent gatherings would help prevent data loss and processing of logs is not needed on every gathering.

Processing of gathered logs attempts to answer some obvious questions. Which commands are most commonly executed with `sudo`? Are some packages requested on certain hardware stacks more than others (ie are GPU related packages being asked for)? Simple questions can be answered with a generated text document, which is packaged in an email and sent to the system administration staff.

B. Package install request form

The conversation policy is much simpler to describe. When a failed attempt to use `sudo` to install a package with `apt` or equivalent tool is detected, the conversation is triggered. An example session is shown below, newlines have been added for clarity. The response will be packaged in an email and sent to the systems staff for consideration.

```
$ sudo apt install some-cool-package
[sudo] password for tsranso:
Sorry, try again.
[sudo] password for tsranso:
Sorry, incorrect password. Would you
like to submit a request to SoCIT to
install this package? (y/N) y

Before we begin, have you considered
installing this package local to
your home directory? (y/N) y

Succinctly, why should this package
be installed?
(Hitting enter sends the email)

This package is super cool and makes
 everything better.

Thank you, the email has been sent.
$
```