**Security analysis of Linux package manager**

There are some very popular package managers for Linux systems (i.e. apt, apt-rpm, yum etc.) to install any software those package managers needs super user access. Once we give super-user access we lose control over what exactly they are doing while installing any new package. For attackers this opens up many new possible attack scenario. This presents a new security risk.
There could be some malicious packages which are installed with some trusted packages as an 'add-on' and that may deny updates for important packages, or may even result in host crush.
Some basic, already implemented solutions includes – marking trusted/untrusted repository, more information from the signing party of particular package, and preventing installation of untrusted packages.
Existing design of package managers do not define the way to provide security. This results in 3 design principles for building secure package manager: a. selective trust delegation, b. customized repository views, c. explicitly treating repository as untrusted.

*Roadmap:* In our project we will analyze the package managers and determine the level of security they provide. We will compare the current level of security and we can also suggest some possible improvement steps.

*Reference:*

1. Package Management Security - Justin Cappos, Justin Samuel, Scott Baker, John H. Hartman
2. Efficient Upgrading in a Purely Functional Component Deployment Model - Eelco Dolstra
3. A Look In the Mirror: Attacks on Package Managers - Justin Cappos Justin Samuel Scott Baker John H. Hartman
4. Toward a distributed package management system - Fabien Dagnat, Gwendal Simon, Xu Zhang
5. Package managers still vulnerable: how to protect your systems - Justin Samuel and Justin Cappos