Ref. : trustgraph1.tex
Version Code : 20140520a

Creating dependency graphs with LaTeX

S. Parthasarathy
drpartha@gmail.com

Abstract

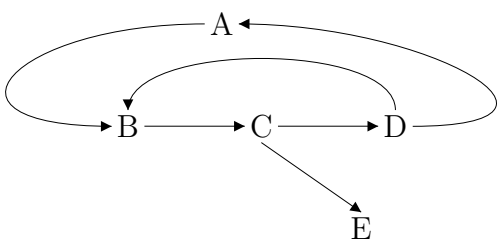
We model the GPG web of trust graphically in LaTeX using the `tree-dvips` package [2].

1 GPG Web of Trust

GPG [1] offers a mechanism for implementing asymmetric-key cryptography. An actor A uses the public key of actor B if A trusts B. B may use the public keys of C D and E because B trusts C D and E. C D and E may trust any of the other actors, creating a "web of trust".

It is often convenient to view the trust relationships between different actors, as a directed graph (called as a graph of trust). The nodes/vertices of the graph of trust are the respective actors. We draw a directed edge (denoted by an arrow) from A to B if A trusts B. The graph of trust is similar to dependency graphs used in many contexts.

Consider the following simple graph of trust :



From a graphical model of the GPG web of trust, we can infer that :

- Trust is not a symmetric relation. A may trust B, but B is not obliged to trust A
- Trust is not a transitive relation. A may trust B, and B may trust C. It is not necessary that A will trust C.

The set of actors which are represented by a graph of trust may be called a community. We can use the graph of trust, to derive various operational properties of the community which the graph models. For instance, from the graph of trust shown above, we may infer the following :

- B is trusted by both A and D. Both A and D can send encrypted messages to B.
- E does not trust anybody. E cannot send any encrypted message to anyone of the other 4 actors.

2 Concluding Remarks

This is a LaTeX document, created under Linux, using Kile. You can get the LaTeX source of this document from drpartha@gmail.com. Please mention the Reference Code, and Version code, given at the top of this document. Please follow the "basic rules of decency" explained in [4]

If you found this article useful, please send a note to `drpartha@gmail.com` As always, suggestions and constructive comments are always welcome.

This document is released under a Creative Commons By Attribution - Non Commercial - ShareAlike 3.0 Unported License. See[3]

The author's GPG public key is available at :
http://algolog.tripod.com/publikey.htm.
The key ID is ::
F1D99755 (Date 2010-09-24).
The key fingerprint is ::
A9E7 287C A58A 2FF0 15D0 952A E0E9 DD26 F1D9 9755.

References

[1] GNU, The GNU Privacy Guard, `https://www.gnupg.org/`

[2] Emma Pease, Tree macros, texdoc.net/texmf-dist/doc/latex/tree-dvips/tree-manual.pdf,

[3] Creative Commons By Attribution - NonCommercial - ShareAlike 3.0 Unported License. http://$creativecommons.org/licenses/by-nc-sa/3.0/deed.en_US$

[4] S. Parthasarathy, The enquiry counter phenomenon. http://drpartha.wordpress.com/2012/04/12/16-2012-the-enquiry-counter-phenomenon/