DeepSec 1.0:
DEciding Equivalence Properties in SECurity protocols
User manual

Vincent Cheval[1], Steve Kremer[1], and Itsaka Rakotonirina[1]

[2]Inria Nancy, LORIA, Université de Lorraine, France

May 15, 2018

Contents

1 Introduction

Test for citations (Cheval, Kremer, and Rakotonirina 2018).

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nullam a dui volutpat, placerat ante eu, tempor purus. Cras tempor id turpis quis mollis. Integer a orci fermentum, tempor mauris porta, pharetra risus. Nullam eu blandit justo, non dapibus purus. Praesent in magna non sem semper vestibulum. Ut semper bibendum sem varius eleifend. Morbi feugiat malesuada sapien eu facilisis. Vivamus mattis enim ac suscipit commodo. Vivamus ac purus venenatis, viverra purus non, eleifend mauris. Fusce laoreet nisi sed nunc blandit vulputate ut ut velit. Etiam ac orci eget elit posuere viverra sit amet eu justo.

Nunc mi tortor, euismod sit amet purus sit amet, ultrices viverra lorem. Mauris ornare augue dignissim velit auctor, non suscipit mi ullamcorper. Etiam a odio vitae odio rutrum euismod at ut magna. Nunc finibus non massa eu vulputate. Ut convallis mattis elit quis venenatis. Cras molestie at sapien in posuere. Nam hendrerit odio nec massa pellentesque, vel gravida est viverra.

Interdum et malesuada fames ac ante ipsum primis in faucibus. Aenean euismod in ante at consectetur. Quisque consectetur congue purus, in hendrerit magna egestas eget. Morbi vehicula ultricies nisi sit amet rutrum. Etiam at dolor turpis. Duis interdum nulla eget rhoncus aliquet. Phasellus enim arcu, aliquet vel arcu vel, semper ullamcorper erat. Vestibulum elementum arcu dolor, non tristique metus ullamcorper ac. Sed varius tellus at egestas ornare. In felis metus, euismod at magna eget, maximus eleifend justo. Cras id interdum nulla. Nulla et finibus urna. Nam ut accumsan arcu.

Suspendisse blandit congue ultricies. Nullam magna eros, tristique sit amet tincidunt nec, rutrum id lorem. Curabitur sodales, magna ac vulputate blandit, nulla dui pharetra odio, imperdiet pretium odio arcu sit amet dui. Nam placerat neque neque, ut vehicula libero luctus ac. Sed urna leo, maximus ac lacus id, hendrerit vulputate nunc. Suspendisse vitae laoreet nunc, eget porttitor tortor. Pellentesque nisi ante, volutpat eu bibendum vitae, porttitor id dui. Fusce id tellus laoreet, placerat felis non, convallis tortor. Suspendisse lectus nunc, ultricies id egestas eu, mattis eu est.

Suspendisse ultrices tortor vel gravida ultricies. Proin malesuada erat nec eleifend viverra. Vivamus porta sodales porta. Nulla vitae aliquet mi. Duis facilisis placerat commodo. Nulla facilisi. Donec vestibulum euismod varius. Integer sit amet commodo risus, eget interdum tortor. Duis aliquam non turpis ut blandit. Aliquam cursus blandit nibh, vitae consequat est pretium at. Nulla eu dapibus mi. Nulla quis tortor eget lorem sollicitudin laoreet vitae sed nunc. Praesent hendrerit efficitur fermentum. Nunc porttitor ultricies diam nec lacinia. Phasellus condimentum fermentum dignissim.

Etiam ac tincidunt quam, at convallis nibh. Curabitur accumsan purus in sapien mollis, eu iaculis est rhoncus. Morbi vehicula neque at dapibus volutpat. Cras eleifend mauris nisi, id cursus metus bibendum at. Praesent fringilla, leo in cursus feugiat, mauris lorem congue elit, eu sodales nisl tellus et odio. Proin orci nunc, feugiat ac aliquet quis, porttitor id metus. Nullam mattis sem ut neque laoreet hendrerit. Aenean faucibus blandit tortor quis cursus. Suspendisse ut ullamcorper massa, sed tempor turpis. Nulla blandit posuere aliquam. Pellentesque tempor orci hendrerit, finibus lorem bibendum, lobortis justo. Aliquam et elit ornare, euismod turpis sed, efficitur massa. Pellentesque vitae suscipit ante.

Praesent tristique bibendum purus non suscipit. Cras nisi dolor, venenatis in nisi et, lobortis lacinia elit. Proin maximus quis nibh nec elementum. Nunc et felis id metus consectetur porttitor sed in quam. Interdum et malesuada fames ac ante ipsum primis in faucibus. Proin

lacinia nibh nec sem viverra, in accumsan ante rutrum. Donec nec turpis in mauris interdum finibus. Nulla consectetur eros a dolor convallis pulvinar. In nec nunc ut tortor rutrum maximus in non magna. Vivamus commodo elit sed gravida suscipit. Vivamus semper nulla ac mattis feugiat.

Nulla auctor at neque vitae suscipit. In nec sem in quam tincidunt suscipit. Nulla eget mauris iaculis, congue lacus ac, tempor lectus. Curabitur lobortis id neque a bibendum. Nullam luctus dapibus pharetra. Aenean in ex vestibulum, pulvinar velit eget, congue massa. Donec interdum nulla quam, ultricies blandit nunc condimentum a. In ultrices volutpat orci id imperdiet. Donec eu tellus id felis sodales dictum. Maecenas posuere scelerisque turpis eu dictum. Vestibulum gravida mollis quam in hendrerit.

Etiam elementum enim dignissim lacus maximus posuere. Donec laoreet consectetur ipsum, sed euismod eros volutpat id. Nulla sollicitudin sit amet neque sed vestibulum. Phasellus posuere, arcu id pellentesque finibus, metus nulla consectetur nisl, sit amet mollis urna arcu vitae risus. In hac habitasse platea dictumst. Donec vel diam mi. Duis erat turpis, imperdiet ut faucibus dictum, sodales quis lectus. Mauris id turpis vitae urna vulputate sodales.

Curabitur faucibus interdum mauris eget vehicula. Nullam lobortis euismod condimentum. Suspendisse placerat ante sed placerat blandit. Proin at tincidunt tortor. Praesent metus mauris, facilisis non sapien in, ultricies laoreet est. Fusce egestas vulputate orci vitae posuere. Nulla vel velit et ligula vulputate iaculis sed nec risus. Donec ac orci sed nisi aliquam aliquet non non ligula. Praesent id ex sit amet massa pretium euismod. Phasellus malesuada varius augue sit amet consectetur.

2 Installation

Installation of `DeepSec`

3 Tutorial

Tutorial of `DeepSec`

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nullam a dui volutpat, placerat ante eu, tempor purus. Cras tempor id turpis quis mollis. Integer a orci fermentum, tempor mauris porta, pharetra risus. Nullam eu blandit justo, non dapibus purus. Praesent in magna non sem semper vestibulum. Ut semper bibendum sem varius eleifend. Morbi feugiat malesuada sapien eu facilisis. Vivamus mattis enim ac suscipit commodo. Vivamus ac purus venenatis, viverra purus non, eleifend mauris. Fusce laoreet nisi sed nunc blandit vulputate ut ut velit. Etiam ac orci eget elit posuere viverra sit amet eu justo.

Nunc mi tortor, euismod sit amet purus sit amet, ultrices viverra lorem. Mauris ornare augue dignissim velit auctor, non suscipit mi ullamcorper. Etiam a odio vitae odio rutrum euismod at ut magna. Nunc finibus non massa eu vulputate. Ut convallis mattis elit quis venenatis. Cras molestie at sapien in posuere. Nam hendrerit odio nec massa pellentesque, vel gravida est viverra.

Interdum et malesuada fames ac ante ipsum primis in faucibus. Aenean euismod in ante at consectetur. Quisque consectetur congue purus, in hendrerit magna egestas eget. Morbi vehicula ultricies nisi sit amet rutrum. Etiam at dolor turpis. Duis interdum nulla eget rhoncus aliquet. Phasellus enim arcu, aliquet vel arcu vel, semper ullamcorper erat. Vestibulum elementum arcu dolor, non tristique metus ullamcorper ac. Sed varius tellus at egestas ornare.

In felis metus, euismod at magna eget, maximus eleifend justo. Cras id interdum nulla. Nulla et finibus urna. Nam ut accumsan arcu.

Suspendisse blandit congue ultricies. Nullam magna eros, tristique sit amet tincidunt nec, rutrum id lorem. Curabitur sodales, magna ac vulputate blandit, nulla dui pharetra odio, imperdiet pretium odio arcu sit amet dui. Nam placerat neque neque, ut vehicula libero luctus ac. Sed urna leo, maximus ac lacus id, hendrerit vulputate nunc. Suspendisse vitae laoreet nunc, eget porttitor tortor. Pellentesque nisi ante, volutpat eu bibendum vitae, porttitor id dui. Fusce id tellus laoreet, placerat felis non, convallis tortor. Suspendisse lectus nunc, ultricies id egestas eu, mattis eu est.

Suspendisse ultrices tortor vel gravida ultricies. Proin malesuada erat nec eleifend viverra. Vivamus porta sodales porta. Nulla vitae aliquet mi. Duis facilisis placerat commodo. Nulla facilisi. Donec vestibulum euismod varius. Integer sit amet commodo risus, eget interdum tortor. Duis aliquam non turpis ut blandit. Aliquam cursus blandit nibh, vitae consequat est pretium at. Nulla eu dapibus mi. Nulla quis tortor eget lorem sollicitudin laoreet vitae sed nunc. Praesent hendrerit efficitur fermentum. Nunc porttitor ultricies diam nec lacinia. Phasellus condimentum fermentum dignissim.

Etiam ac tincidunt quam, at convallis nibh. Curabitur accumsan purus in sapien mollis, eu iaculis est rhoncus. Morbi vehicula neque at dapibus volutpat. Cras eleifend mauris nisi, id cursus metus bibendum at. Praesent fringilla, leo in cursus feugiat, mauris lorem congue elit, eu sodales nisl tellus et odio. Proin orci nunc, feugiat ac aliquet quis, porttitor id metus. Nullam mattis sem ut neque laoreet hendrerit. Aenean faucibus blandit tortor quis cursus. Suspendisse ut ullamcorper massa, sed tempor turpis. Nulla blandit posuere aliquam. Pellentesque tempor orci hendrerit, finibus lorem bibendum, lobortis justo. Aliquam et elit ornare, euismod turpis sed, efficitur massa. Pellentesque vitae suscipit ante.

Praesent tristique bibendum purus non suscipit. Cras nisi dolor, venenatis in nisi et, lobortis lacinia elit. Proin maximus quis nibh nec elementum. Nunc et felis id metus consectetur porttitor sed in quam. Interdum et malesuada fames ac ante ipsum primis in faucibus. Proin lacinia nibh nec sem viverra, in accumsan ante rutrum. Donec nec turpis in mauris interdum finibus. Nulla consectetur eros a dolor convallis pulvinar. In nec nunc ut tortor rutrum maximus in non magna. Vivamus commodo elit sed gravida suscipit. Vivamus semper nulla ac mattis feugiat.

Nulla auctor at neque vitae suscipit. In nec sem in quam tincidunt suscipit. Nulla eget mauris iaculis, congue lacus ac, tempor lectus. Curabitur lobortis id neque a bibendum. Nullam luctus dapibus pharetra. Aenean in ex vestibulum, pulvinar velit eget, congue massa. Donec interdum nulla quam, ultricies blandit nunc condimentum a. In ultrices volutpat orci id imperdiet. Donec eu tellus id felis sodales dictum. Maecenas posuere scelerisque turpis eu dictum. Vestibulum gravida mollis quam in hendrerit.

Etiam elementum enim dignissim lacus maximus posuere. Donec laoreet consectetur ipsum, sed euismod eros volutpat id. Nulla sollicitudin sit amet neque sed vestibulum. Phasellus posuere, arcu id pellentesque finibus, metus nulla consectetur nisl, sit amet mollis urna arcu vitae risus. In hac habitasse platea dictumst. Donec vel diam mi. Duis erat turpis, imperdiet ut faucibus dictum, sodales quis lectus. Mauris id turpis vitae urna vulputate sodales.

Curabitur faucibus interdum mauris eget vehicula. Nullam lobortis euismod condimentum. Suspendisse placerat ante sed placerat blandit. Proin at tincidunt tortor. Praesent metus mauris, facilisis non sapien in, ultricies laoreet est. Fusce egestas vulputate orci vitae posuere. Nulla vel velit et ligula vulputate iaculis sed nec risus. Donec ac orci sed nisi aliquam aliquet non non ligula. Praesent id ex sit amet massa pretium euismod. Phasellus malesuada varius

augue sit amet consectetur.

4 Input grammar

We describe in details the input grammar of **DeepSec**.

4.1 Type system

4.2 Function symbols

4.3 Processes

4.3.1 Precedences

4.4 Queries

5 Command-line options

Command-line options of DeepSec.

References

[CKR18] Vincent Cheval, Steve Kremer, and Itsaka Rakotonirina. "DEEPSEC: Deciding Equivalence Properties in Security Protocols - Theory and Practice". In: *Proceedings of the 39th IEEE Symposium on Security and Privacy (S&P'18)*. Accepted for publication. San Francisco, CA, USA: IEEE Computer Society Press, May 2018.