怎样用好 AVISPA 工具

徐梦茗①，李　斌①，肖　聪②
（①现代通信国家重点实验室，四川 成都 610041；②总参谋部通信部驻成都地区军代室，四川 成都 610041）

【摘　要】AVISPA 安全协议分析工具是一套完整、标准的形式化自动分析工具；结合 XEmacs 模式能够设置更加直观而简便的操作和编译环境，对安全协议进行分析并得出结论。

【关键词】安全协议；AVISPA；XEmacs
【中图分类号】TP393.08　　【文献标识码】A　　【文章编号】1009-8054(2009)08-0154-02

Implementation of AVISPA Tool

XU Meng-ming①，　LI Bin①，　XIAO Cong②
（①State Key Laboratory for Modern Communications, Chengdu Sichuan 610041, China;
②Military Representative Office of Chengdu Area the Headquarter of the General Staff, Chengdu Sichuan 610041, China）

【Abstract】AVISPA is a set of complete, standard formalized automatic analysis tool. By combined with XEmacs mode, AVISPA could set up standardization more intuitive, simple and convenient environment for operation and compilation, analyzes the security protocol and acquires the conclusion method.

【Key words】security protocol; AVISPA; XEmacs

0 引言

安全协议是指使用密码技术或提供安全服务的协议，可以实现认证和密钥交换等安全目的[1]。而 AVISPA 分析工具的主要目的是将成熟的、倾向性不同的分析工具移植到标准的载体上面，使其整合成一套比较完整的、标准的自动分析工具，使协议设计者能够准确、方便的使用 AVISPA 分析工具对协议进行分析并得出结论。

1 AVISPA 分析工具

AVISPA 分析工具的结构图[2]如下页图 1 所示。HLPSL 是一种丰富的、模块化的、基于角色的形式语言，提供了一套包括控制流模式、数据结构、可选择入侵者模式、复杂的安全目标以及不同的密码初始值和代数性质的说明[3]。这些特性能够使 HLPSL 很好的描述现代的、工业化规模的协议。而且，HLPSL 不仅支持基于时间片段的逻辑行为的公开语义，还支持基于重写的中间形式化语言 IF。

HLPSL2IF 自动将 HLPSL 语言翻译成 IF 语言，并将它们依次反馈给测试后端。AVISPA 使用了 4 种后端分析工具来解决安全协议的确认问题[4]：

（1）OFMC(On-the-fly Model-Checker)：基于 IF 语言需求驱使的描述，通过探测系统的变迁，OFMC 能够完成协议的篡改和有限制的确认。OFMC 支持密码操作的代数性质的规范，以及各种协议模型。

（2）CL-AtSe（Constraint-Logic-based Attack Searcher）：CL-AtSe 通过强大的简化探测法和冗余排除技术来执行协议。它建立在模型化的方式上，并且是对密码操作的代数性质的延伸。CL-AtSe 支持输入缺陷探测和处理消息串联。

（3）SATMC（SAT-based Model-Checker）：SATMC 建立在通过 IF 语言描述的，有限域上变迁关系的编码的公式，初始状态和状态集合的说明代表了整个协议的安全特性。此公式将反馈给 SAT 状态推导机，并且建立的任何一个模型都将转化为一个攻击事件。

（4）TA4SP(Tree Automata based on Automatic Approximations for the Analysis of Security Protocols)：TA4SP 通过树形语言和重写机制估计入侵者的知识。根据不同的保密特性，TA4SP 能够判断一个协议是否有缺陷，或者是几个会合的对话后是否安全。

收稿日期：2009-04-20。
基金项目：现代通信国家重点实验室基金资助项目（编号：9140C1104090704）。
作者简介：徐梦茗（1979-），女，工程师，主要从事保密通信和网络安全方向的研究工作；李　斌（1977-），男，工程师，主要从事保密通信和网络安全方向的研究工作；肖　聪（1979-），男，技术上尉，主要从事保密通信方面的军品监制和监督工作。

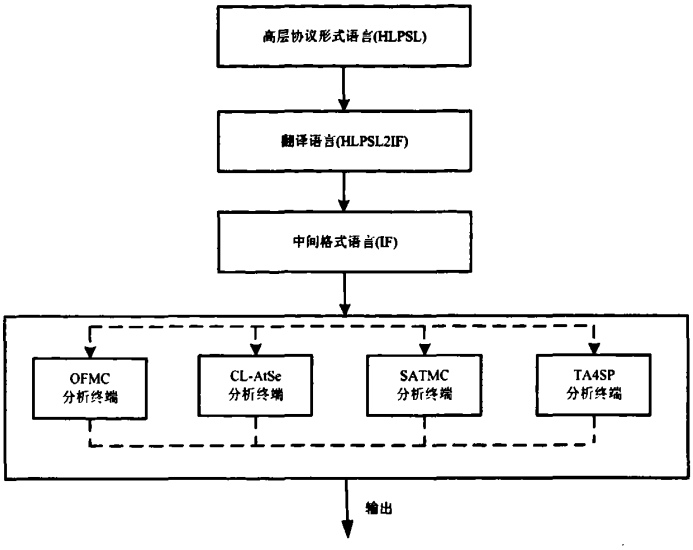

图 1 AVISPA 工具结构

2 AVISPA 工具的安装

AVISPA 工具在 AVISPA 官方网站上可以下载，运行在 Linux 操作系统环境下。首先，下载并安装 AVISPA vX.Y 版本（本文使用 AVISPA1.0 版本为例），解压安装包到对应目录；其次，需要设置工具集的环境变量，将 AVISPA_PACKAGE 关联到安装包的绝对路径；最后将 avispa 脚本语言设置在命令行解释器的执行目录中。例如：用户想安装 AVISPA 工具集在/opt 路径下，命令如下[5]：

```
cd /opt
tar -xzf /home/xyz/avispa-package-X.Y_Linux-i686.tgz
export AVISPA_PACKAGE=/opt/avispa-X.Y
export PATH=$PATH:$AVISPA_PACKAGE
```

3 XEmacs 模式的使用

（1）XEmacs 工具的安装。

AVISPA 提供和 XEmacs 工具的用户友好接口（XEmacs 工具是 Linux 操作系统下的一种编辑器），它们之间支持用户和 AVISPA 工具集之间的简单交互。首先，Linux 操作系统需要安装 XEmacs 编辑器；其次，需要对 AVISPA 进行设置，使其支持 XEmacs 模式，命令如下：

```
cd  /opt/others
tar -xzvf avispa-mode.tgz
cd temporary-avispa
make install
```

（2）XEmacs 工具按钮。

AVISPA XEmacs 模式提供了一套完整而直观的编译环境对安全协议进行说明和分析。最常用的分析出发点是通过 hlpsl 文件开始。在 AVISPA 模式下，当 XEmacs 工具自动侦测出后缀名为“.hlpsl”的文件时，会在 XEmacs 工具栏上出现对应的 AVISPA 按钮。

AVISPA 按钮的大致功能如下：

AVISPA：提供选项、模式的定制和改变后端分析工具等功能；

<<和>>：提供在同一个协议不同的分析文件（例如“.if”，“.atk”等）之间进行导航；

Process file：导入编译器对中间文件进行编译和分析，得出结论；

Update：当一个工具被 XEmacs 异步导入时，一旦此工具被中断，此按钮将刷新当前的缓存区。

4 安全协议的分析

使用 AVISPA 协议分析工具对安全协议进行分析的一般性过程如下：首先，将安全协议编码为某种形式化描述语言；然后，根据协议目标和安全属性，给出不同的消息成分的类型；最后，根据分析工作的结果判断协议是否安全，是否达到了预期目标。

（1）分析安全协议，并根据 HLPSL 语法，将协议进行建模，编辑成后缀名为“.hlpsl”的文件，具体语法见《安全协议形式化分析的研究和实现》[6]；

（下转第 158 页）

Di, Ta, Td> ，式中 *Rpt* 是推荐者信誉值，*Di* 是 *rater* 对推荐者直接交互经验值，*Ta* 是推荐者与 ratee 的交易次数，*Td* 为交易日期。R2BTM 采用的这 4 个指标已完全覆盖与交易有关的所有特征，区别于 FuzzyTrust[7]所使用的 3 个指标，FuzzyTrust 方案在决定推荐权重的时候没有考虑与推荐者直接交互的经验，是不完备的，而且直接交互的经验有时候起着至关重要的作用，不应该被忽视。

2 结语

P2P 系统中，确保节点的可信度和真实性是至关重要的。P2P 系统中的信誉度估计将会变得越来越重要。提供一种可以避免不可靠，感染和丑化节点的信誉机制，在 P2P 系统中将变的越来重要。P2P 系统的现有的信任模型主要是基于信誉机制的。限于篇幅，不能细致描述每种信任模型，只是给出了一个概括性的介绍。文中主要介绍了几种比较典型的，处于研究热点的信任模型。

Bayesian 网络信任模型的不足体现在以下三个方面：

（1）该信任机制在设计时，没有将恶意节点考虑进去，由此缺少相应的惩罚机制；

（2）该机制设计的环境过于理想化，不适用于大规模的 P2P 环境；

（3）该机制在实现大规模交易的情况时，系统开销绝大部分用于计算节点的信任度。

分布式 trust 模型的不足是：不同信任关系矩阵 *R* 的选取会使得计算某节点信任度最终结果有所不同，甚至背离其真实值；全局信任度的迭代计算开销在实际系统工作时也不容忽视。所有以上这些模型都没有考虑节点参与系统行为的单位时间交易频度给信任度带来的变化。

R2BTM 模型较目前已有的一些方案在某些指标上有明显的改善，在大规模的开放网络环境中具有很好的效果。

参考文献

[1] 廖小成，龙昭华，杨令. 基于 P2P 重叠网的 VoIP 系统实现[J]. 通信技术，2007,41(11)：208-210.

[2] 康芳，王道彬，钟朗. P2P 技术在网络电视中的应用研究[J]. 通信技术，2007,40(07)：11-12.

[3] Damiani E, D C di Vimercati, Paraboschi S, et al. Reputation-based approach for choosing reliable resources in peer-to-peer networks[C]. USA:ACM, 2002:207-216.

[4] 赵贵昉，李真，张学杰. P2P 网络资源共享中基于信誉的访问控制[J]. 云南大学学报：自然科学版，2007，29(S2)：238-240.

[5] Sepandar Kavmar, Mario Schlosser, Hector Garcia-Molina. The Eigen Trust Algorithm for Reputation Management in P2P Networks[C]. USA:ACM, 2003:640-651.

[6] 林作铨，牟克典，韩庆. 基于未知扰动的冲突证据合成方法. 软件学报，2004，15(08)：1150-1156.

[7] Song S S, Hwang K, Zhou R F. Trusted P2P transactions with fuzzy reputation aggregation[J]. IEEE Internet Computing Magazine, 2005, 9(06): 24-34.

（上接第 155 页）

（2）利用 XEmacs 将 HLPSL 文件导入，利用 HLPSL 编辑器将 HLPSL 文件转换为后缀名为“.if”的中间文件；

（3）XEmacs 将 IF 文件导入，利用选定的后端分析工具将 IF 文件分析得到后缀名“.atk”的结果文件，通过结果文件可以分析得出该协议的安全性、目标、攻击轨迹等各种细节。

5 结语

用户在 AVISPA 工具 XEmacs 模式环境下，能够直观和简便的根据形式化语言对安全协议进行建模，并快速而准确的推导出分析结果、给出分析轨迹。

AVISPA 安全协议分析工具集开发了这种丰富的形式化说明语言，能够为协议流程、安全目标和攻击轨迹建立起工业级复杂度的形式化模型；利用 XEmacs 模式、整合 4 种后端分析工具对安全协议进行全方位的自动推导和分析，并可根据分析结果设计出相应的解决方案。

AVISPA 致力于发展大规模网络安全协议和应用的工业化技术。其技术可以加速下一代网络协议的发展，提高安全性，增加公众对于基于安全协议的分布式信息技术的接 受度。

参考文献

[1] 卿斯汉. 安全协议[M]. 北京：清华大学出版社，2005：121-152.

[2] AVISPA Team. HLPSL Tutorial. European Community under the Information Society Technologies Program[EB/OL]. (2005-10-1). http://www.avispa-project.org.

[3] 卿斯汉. 安全协议 20 年研究进展[J]. 软件学报，2003,14（10）：34-37.

[4] AVISPA Team. AVISPA V1.0 User Manual. European Community under the Information Society Technologies Program[EB/OL]. (2005-10-1). http://www.avispa-project.org.

[5] 徐梦茗，肖聪，李斌，等. 安全协议形式化分析的研究和实现[J]. 信息安全与通信保密，2008(08)：76-78.

[6] 徐梦茗，肖聪，唐六华，等. 安全协议和网络攻击分析[J]. 信息安全与通信保密，2007(02)：16-18.

怎样用好AVISPA工具

作者： 徐梦茗， 李斌， 肖聪， XU Meng-ming， LI Bin， XIAO Cong
作者单位： 徐梦茗,李斌,XU Meng-ming,LI Bin(现代通信国家重点实验室,四川,成都,610041)， 肖聪,XIAO Cong(总参谋部通信部驻成都地区军代室,四川,成都,610041)
刊名： 信息安全与通信保密
英文刊名： CHINA INFORMATION SECURITY
年，卷(期)： 2009(8)

参考文献(6条)

1. 卿斯汉 安全协议 2005

2. 徐梦茗;肖聪;唐六华 安全协议和网络攻击分析[期刊论文]-信息安全与通信保密 2007(02)

3. 徐梦茗;肖聪;李斌 安全协议形式化分析的研究和实现[期刊论文]-信息安全与通信保密 2008(08)

4. AVISPA Team AVISPA V1.0 User Manual.European Community under the Information Society Technologies Program 2005

5. 卿斯汉 安全协议20年研究进展[期刊论文]-软件学报 2003(10)

6. AVISPA Team HLPSL Tutorial European Community under the Information Society Technologies Program 2005

本文读者也读过(5条)