

TECHNICAL REPORT

Report No. UI-SE-MDSERG-2022-10

Date: November 10, 2022

VAnDroid3 Tool User Manual

Atefeh Nirumand
Bahman Zamani
Behrouz Tork Ladani
Jacques Klein
Tegawendé F. Bissyandé



Department of Software Engineering
University of Isfahan
Hezar-Jerib Ave.
Isfahan

Tel: +98-31-37934537
Fax: +98-31-36699529 , +98-31-37932670
zamani@eng.ui.ac.ir
<http://mdse.ui.ac.ir/TR>

VAnDroid3 Tool User Manual

Atefeh Nirumand, Bahman Zamani, Behrouz Tork Ladani,
Jacques Klein, and Tegawendé F. Bissyandé

Department of Software Engineering

University of Isfahan

Isfahan, Iran.

`{atefehnirumand, zamani, ladani}@eng.ui.ac.ir`

`{jacques.klein, tegawende.bissyande}@uni.lu`

Abstract: *VAnDroid3 is an Eclipse-based tool for security analysis of Android inter-application vulnerabilities. This tool is developed by Nirumand et al. The approach taken by VAnDroid3 has three main phases. At Model Discovery, by providing a comprehensive Intermediate Representation (IR) of each app, initial models are created without losing information. Then, at Transformation and Integration, by collecting security information in the form of domain-specific model from each app, the comprehension of the Android system is facilitated and all potential intent-based communication are extracted from a bundle of Android apps. Finally, at Analysis, intra- and inter-app security analyses are performed and the results are displayed to the user in the form of XMI models. This report provides a user manual for the VAnDroid3 tool.*

VAnDroid3 Tool User Manual

Atefeh Nirumand, Bahman Zamani, Behrouz Tork Ladani,
Jacques Klein, and Tegawendé F. Bissyandé
Department of Software Engineering
University of Isfahan
Isfahan, Iran.

{atefehnirumand, zamani, ladani}@eng.ui.ac.ir
{jacques.klein, tegawende.bissyande}@uni.lu

Abstract: *VAnDroid3 is an Eclipse-based tool for security analysis of Android inter-application vulnerabilities. This tool is developed by Nirumand et al. The approach taken by VAnDroid3 has three main phases. At Model Discovery, by providing a comprehensive Intermediate Representation (IR) of each app, initial models are created without losing information. Then, at Transformation and Integration, by collecting security information in the form of domain-specific model from each app, the comprehension of the Android system is facilitated and all potential intent-based communication are extracted from a bundle of Android apps. Finally, at Analysis, intra- and inter-app security analyses are performed and the results are displayed to the user in the form of XMI models. This report provides a user manual for the VAnDroid3 tool.*

Contents

1	Introduction	3
2	Prerequisites	3
3	VAnDroid3 Setup Guide	4

List of Figures

1	Launch the Eclipse Workspace.	4
2	Import the android.security.reports Project Into the Eclipse Workspace.	5

3	Import the android.security.reports Project Into the Eclipse Workspace (Cont.).	5
4	Configuration a New Eclipse Workspace.	6
5	Configuration a New Eclipse Workspace (Cont.).	7
6	Configuration a New Eclipse Workspace (Cont.).	7
7	Import the Android Projects Into New Workspace.	8
8	Run the VAnDroid3 Tool.	9
9	Run the VAnDroid3 Tool (Cont.).	9
10	The Android Security Application Aspects Model of UnprotectedBroadcastRecv-PrivEscalation-Benign.	10
11	The Inter-Component Communication (ICC) Model.	10
12	The Privilege Escalation Model for Explicit Communications Domain.	11
13	The Intent Spoofing Model for Implicit Communications Domain.	11
14	Register an Ecore File (i.e., ASAMM.ecore) in the Workspace.	12

1 Introduction

VAnDroid3 is developed as an open-source tool for Eclipse IDE platform. It relies on two following technologies from Model Driven Engineering (MDE) ecosystem.

1) MoDisco [1] is used to extract the comprehensive specification from each app in the form of initial models. The XML model is obtained by the XML Discoverer of MoDisco. The Java model is also extracted from the Java code of the app using the Java Discoverer of MoDisco.

2) ATL [2] is used to extract the security information contained in the initial models (i.e., the XML model and the Java model) to a homogeneous representation (i.e., the Android Application Security Aspects model). This transformation language is also used to extract all potential intent-based communications and URI-based communications at intra- and inter-app levels from a set of Android Application Security Aspects models. Then, by gathering all potential communications between apps in a single model, at the Model (Re)Generation phase, a set of model-to-model (M2M) transformations are performed to identify inter-app vulnerabilities. In these transformations, ATL and OCL rules have been used.

2 Prerequisites

1) Eclipse

Download and install Eclipse Modeling Tools from <https://www.eclipse.org/downloads/packages/release/mars/2>.

1) ATL

Check the ATL installation details from https://wiki.eclipse.org/ATL/User_Guide_-_Installation and install the ATL Transformation Language SDK in your Eclipse.

1) MoDisco

Check the MoDisco installation details from <https://wiki.eclipse.org/MoDisco/Installation> and install the MoDisco SDK in your Eclipse.

3 VAnDroid3 Setup Guide

An example of running VAnDroid3 is described in the following.

A) Launch VAnDroid3

1. Download the required resources from https://mdse.ui.ac.ir/Tools/VAnDroid3_Tool.
2. Unzip the archive file.
3. Create a new Eclipse workspace (e.g., the VAnDroid3 workspace).
4. Copy the **android.security.reports** project into the created workspace folder (i.e., the VAnDroid3 folder).
5. Open the installed Eclipse folder and run the eclipse.exe.
6. Select the created workspace from the Browse button of the Workspace Launcher window.
7. Import the **android.security.reports** project into your Eclipse workspace (see Figures. 1 , 2, and 3).

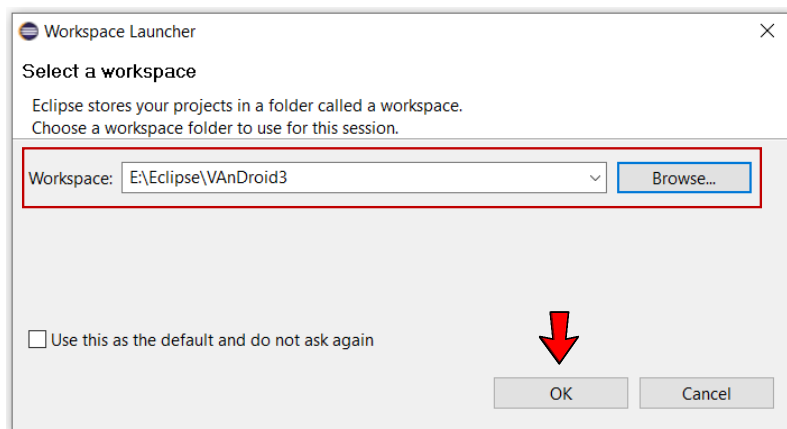


Figure 1: Launch the Eclipse Workspace.

B) Running VAnDroid3 on an example

1. Right-click on the **android.security.reports** project in the Project Explorer view and select **Run As> Run Configurations** from the pop-up menu. Select the **Eclipse Application** category on the list of the left and click on the New launch Configuration (see Figure. 4).

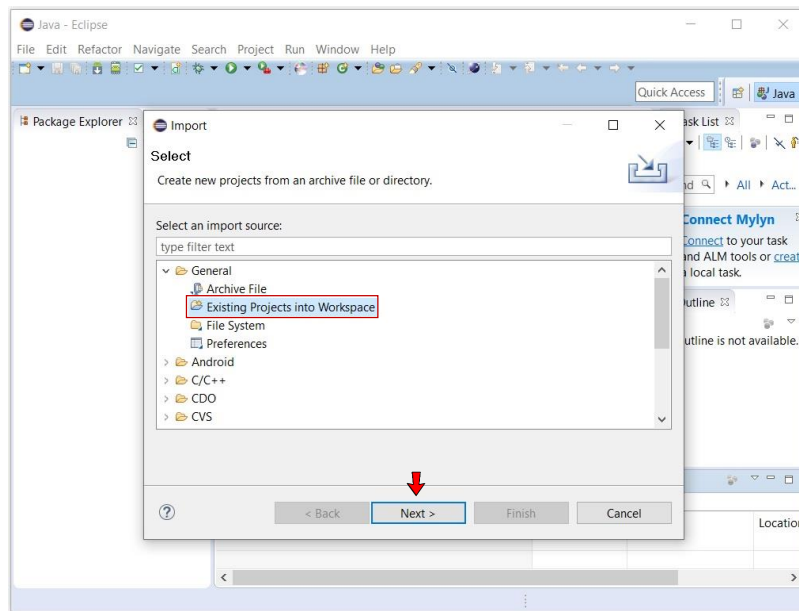


Figure 2: Import the android.security.reports Project Into the Eclipse Workspace.

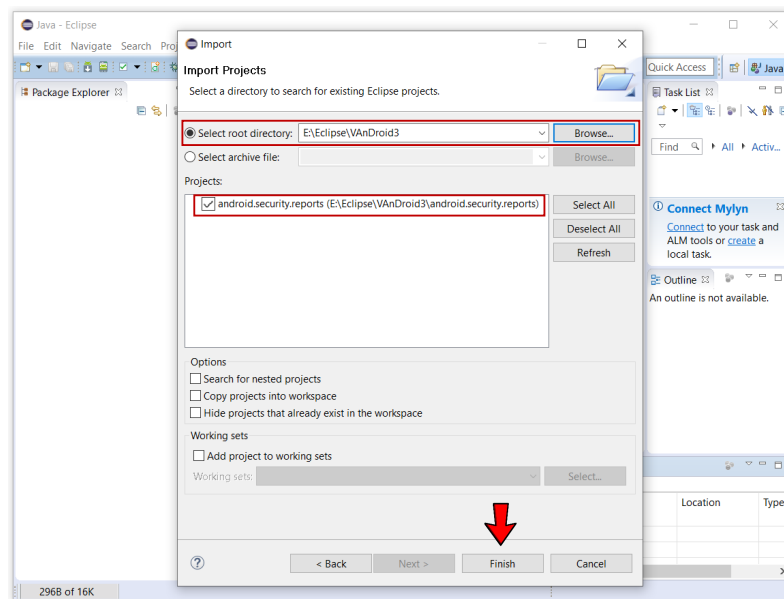


Figure 3: Import the android.security.reports Project Into the Eclipse Workspace (Cont.).

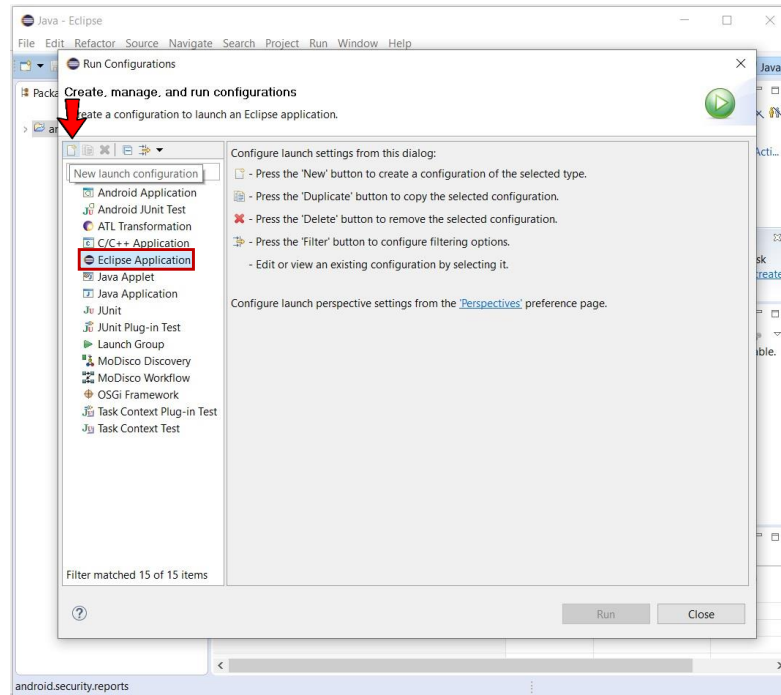


Figure 4: Configuration a New Eclipse Workspace.

2. Named the Configuration, here we named it **RunVAnDroid3** (see Figure. 5). Make sure the **android.security.reports** project is selected in the Plug-ins section (see Figure. 6)
3. Click on the Apply button and then Run button (see Figure. 6).
4. Copy the Android projects (i.e., **UnprotectedBroadcastRecv-PrivEscalation-Benign** and **UnprotectedBroadcastRecv-PrivEscalation-Malicious**) and the **RequiredMetaModel** file into the new Eclipse workspace folder (i.e., the **RunVAnDroid3** folder).
5. Import the Android projects (i.e., **UnprotectedBroadcastRecv-PrivEscalation-Benign** and **UnprotectedBroadcastRecv-PrivEscalation-Malicious**) and the **RequiredMetaModel** file into the new workspace from the **RunVAnDroid3** folder (see Figure. 7).
6. Click on **VAnDroid3** from the menu bar and then click on the **Extract** option which displays the wizard page of VAnDroid3 (see Figures. 8 and 9).
7. Click on one of the Android projects on the wizard page and then click on the Finish button (see Figure. 9).
8. After running the VAnDroid3 tool, the result models are generated,

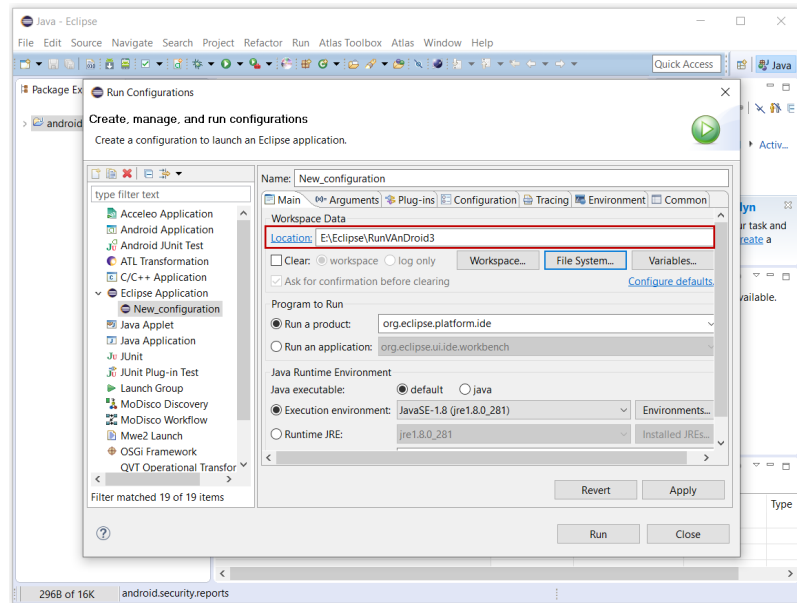


Figure 5: Configuration a New Eclipse Workspace (Cont.).

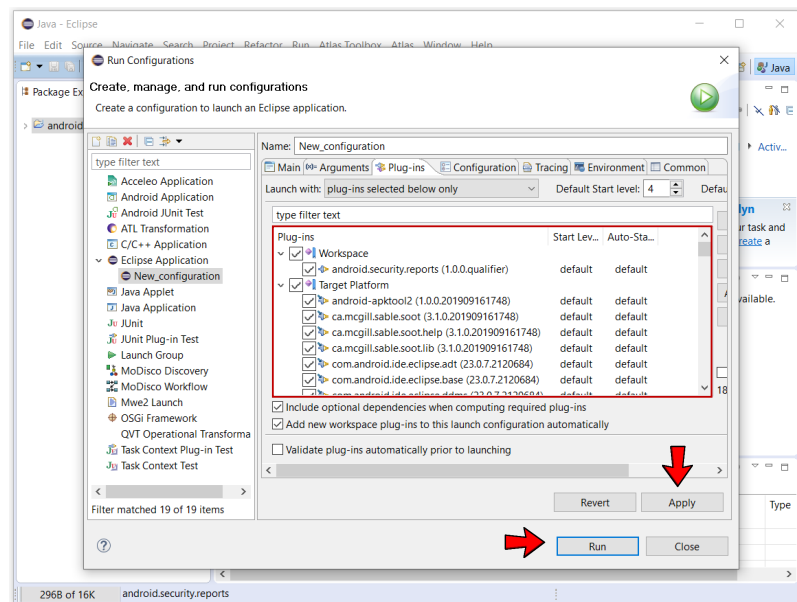


Figure 6: Configuration a New Eclipse Workspace (Cont.).

including the Android Application Security Aspects model for each app (see Figure. 10), the Inter-Component Communication (ICC) model (see

Figure. 11), the models related to the privilege escalation (see Figure. 12), and the Intent Spoofing (see Figure. 13) vulnerabilities. Before opening the XMI models, register Ecore files from the **RequiredMetaModel** project in the workspace (see Figure. 14).

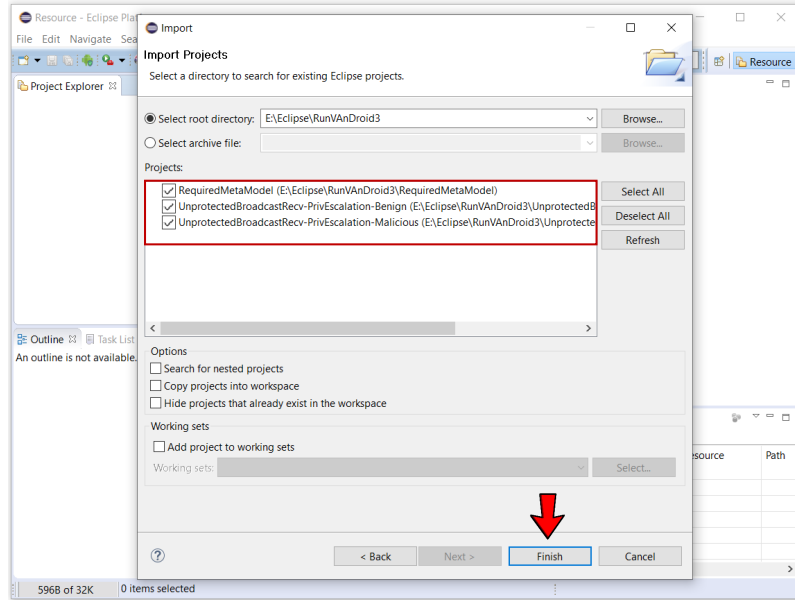


Figure 7: Import the Android Projects Into New Workspace.

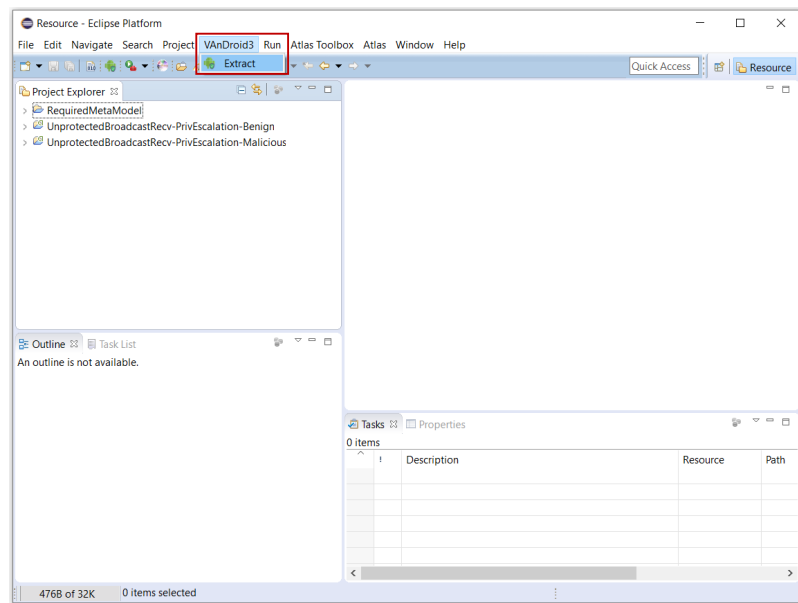


Figure 8: Run the VAnDroid3 Tool.

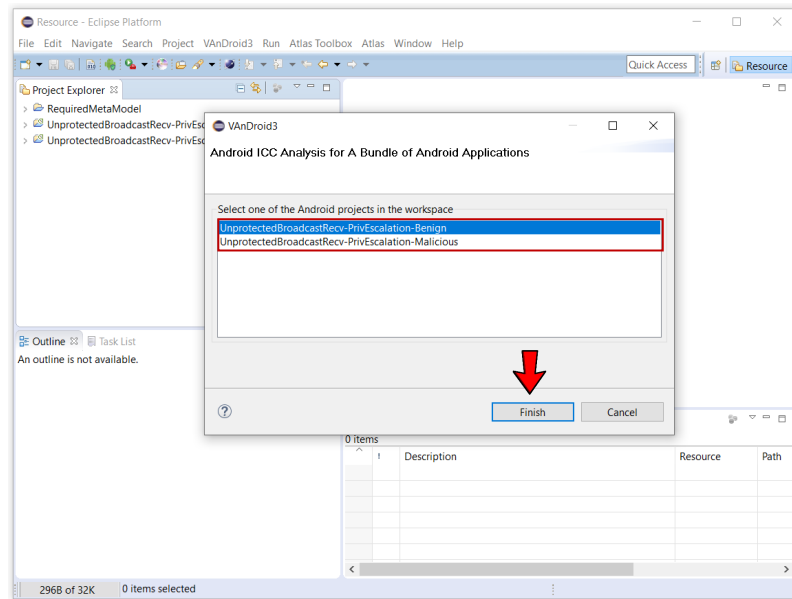


Figure 9: Run the VAnDroid3 Tool (Cont.).

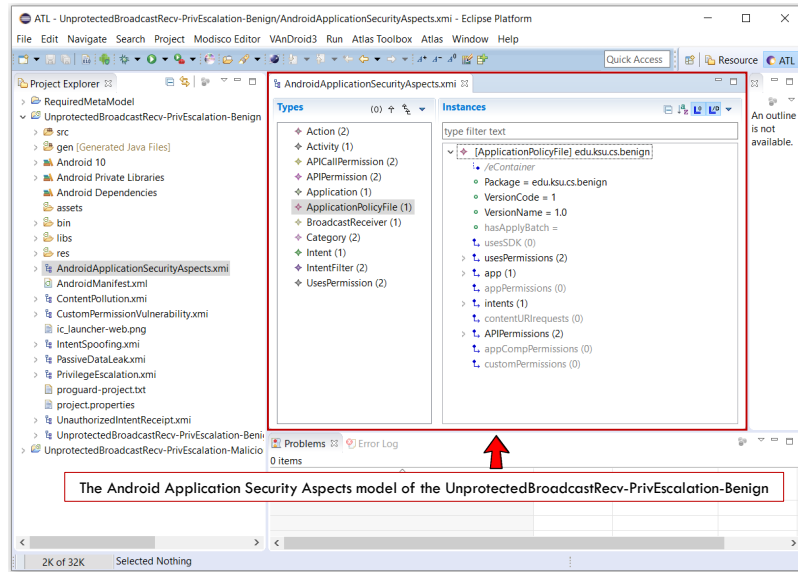


Figure 10: The Android Security Application Aspects Model of UnprotectedBroadcastRecv-PrivEscalation-Benign.

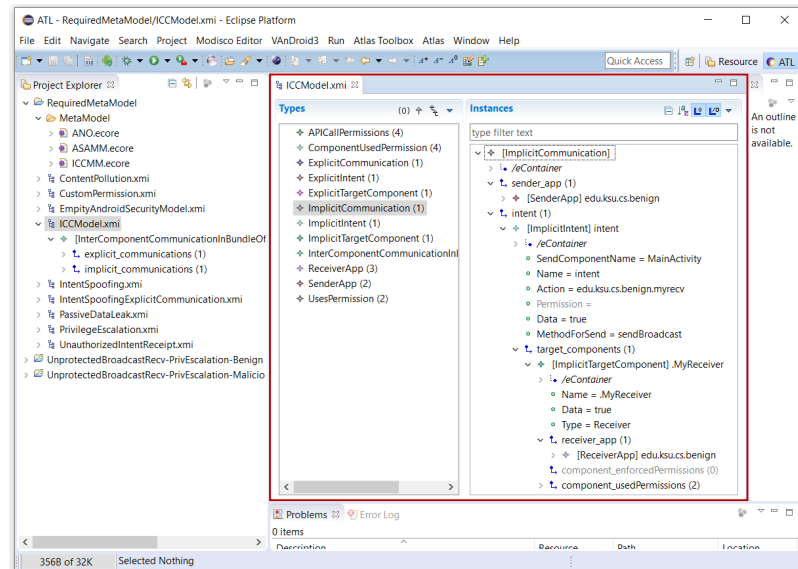


Figure 11: The Inter-Component Communication (ICC) Model.

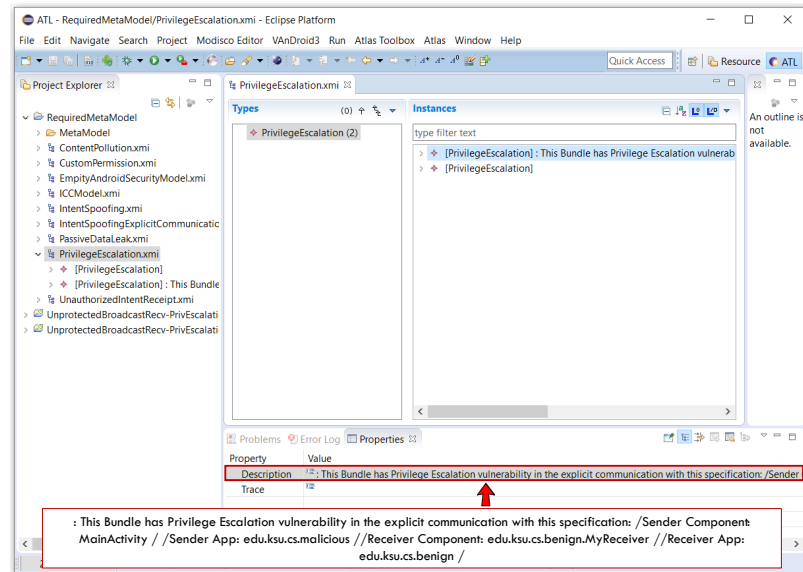


Figure 12: The Privilege Escalation Model for Explicit Communications Domain.

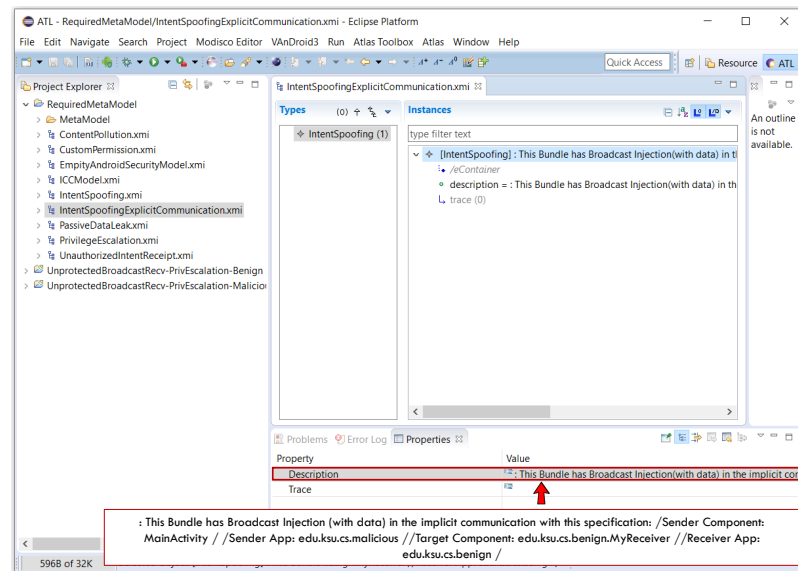


Figure 13: The Intent Spoofing Model for Implicit Communications Domain.

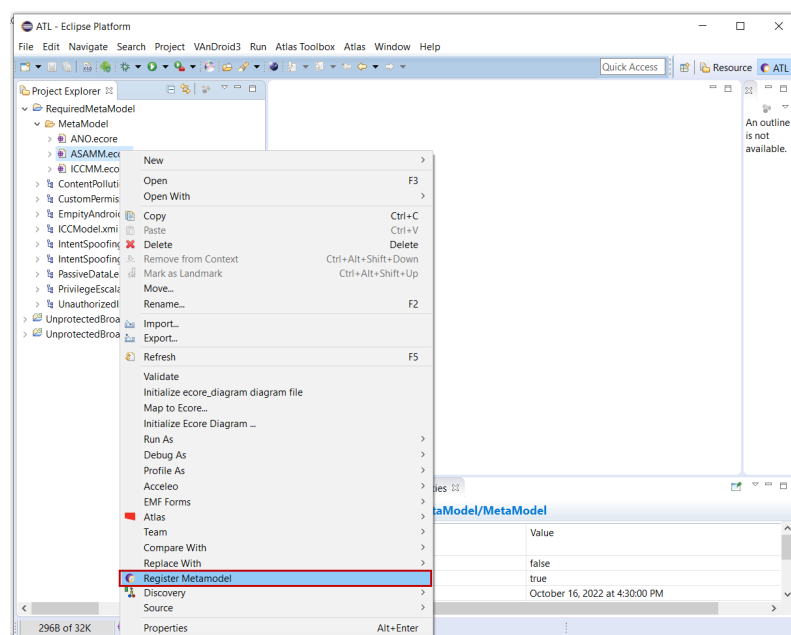


Figure 14: Register an Ecore File (i.e., ASAMM.ecore) in the Workspace.

References

- [1] The Eclipse Foundation, “Eclipse MoDisco,” <https://github.com/fgwei/ICC-Bench>, Date Accessed: Nov. 10, 2022. [3](#)
- [2] The Eclipse Foundation, “ATL,” <http://www.eclipse.org/atl/>, Date Accessed: Nov. 10, 2022. [3](#)