

AUTOMOTIVE THREAT MODELLING

UTILISING THE STRIDE MODEL

Dr. Nicolas Kylilis



CARMEL PROJECT EU NO. 833611 | H2020CARMEL.EU





SUMMARY

This report elaborates on a practical, step by step approach on modelling, analysing and providing mitigations with the use of Automotive Threat Modelling tools based on the STRIDE Model.

REQUIREMENTS

Listed below are the preconditions for the process of Automotive Threat Modeling.

MICROSOFT THREAT MODELING TOOL


Threat Modelling Tool update release 7.3.00714.2 - 07/14/2020

- Microsoft Windows 10 Anniversary Update or later
- .NET Version Required
- .NET 4.7.1 or later
- Additional Requirements
- An Internet connection

<https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling>

Threat Modeling

Threat modeling is a core element of the [Microsoft Security Development Lifecycle \(SDL\)](#). It's an engineering technique you can use to help you identify threats, attacks, vulnerabilities, and countermeasures that could affect your application. You can use threat modeling to shape your application's design, meet your company's security objectives, and reduce risk.



There are five major threat modeling steps:

- Defining security requirements.
- Creating an application diagram.
- Identifying threats.
- Mitigating threats.
- Validating that threats have been mitigated.

Threat modeling should be part of your routine development lifecycle, enabling you to progressively refine your threat model and further reduce risk.

Microsoft Threat Modeling Tool


The Microsoft Threat Modeling Tool makes threat modeling easier for all developers through a standard notation for visualizing system components, data flows, and security boundaries. It also helps threat modelers identify classes of threats they should consider based on the structure of their software design. We designed the tool with non-security experts in mind, making threat modeling easier for all developers by providing clear guidance on creating and analyzing threat models.


The Threat Modeling Tool enables any developer or software architect to:


- Communicate about the security design of their systems.
- Analyze those designs for potential security issues using a proven methodology.
- Suggest and manage mitigations for security issues.


The SDL Threat Modeling Tool plugs into any issue-tracking system, making the threat modeling process a part of the standard development process.

The following important links will get you started with the Threat Modeling Tool:


Download the Threat Modeling Tool


Read Our getting started guide


Get familiar with the features


Learn about generated threat categories



Find mitigations to generated threats

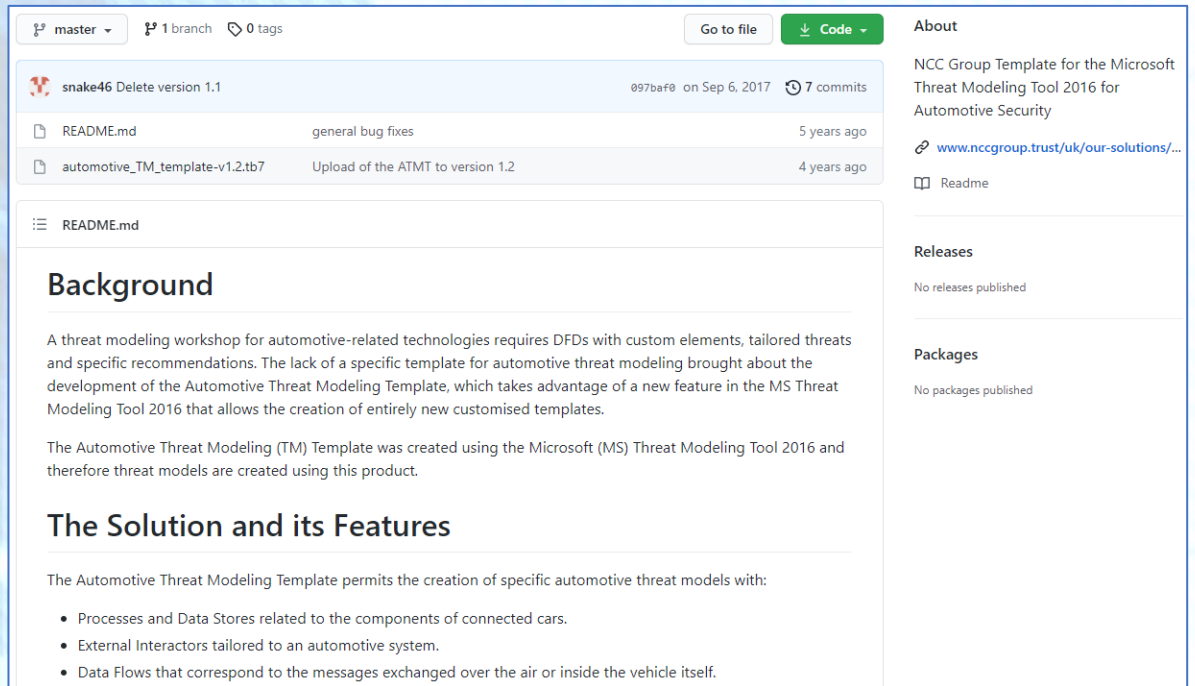
Figure 1: Microsoft Threat Modeling Tool Website

NCC GROUP TEMPLATE

NCC Group Template from github

- automotive_TM_template-v1.2.tb7

[https://github.com/nccgroup/The Automotive Threat Modeling Template](https://github.com/nccgroup/The_Automotive_Threat_Modeling_Template)



The screenshot shows the GitHub repository page for 'The Automotive Threat Modeling Template' by nccgroup. The repository is on the 'master' branch with 1 branch and 0 tags. It has 7 commits. The commit history shows a recent commit 'Delete version 1.1' and an older commit 'Upload of the ATMT to version 1.2'. The README file is selected, showing the 'Background' section which describes the template's purpose and the 'The Solution and its Features' section which lists the components of connected cars, external interactors, and data flows. The right sidebar contains 'About', 'Releases', and 'Packages' sections.

master 1 branch 0 tags Go to file Code

snake46 Delete version 1.1 097baf0 on Sep 6, 2017 7 commits

File	Commit Message	Time
README.md	general bug fixes	5 years ago
automotive_TM_template-v1.2.tb7	Upload of the ATMT to version 1.2	4 years ago

README.md

Background

A threat modeling workshop for automotive-related technologies requires DFDs with custom elements, tailored threats and specific recommendations. The lack of a specific template for automotive threat modeling brought about the development of the Automotive Threat Modeling Template, which takes advantage of a new feature in the MS Threat Modeling Tool 2016 that allows the creation of entirely new customised templates.

The Automotive Threat Modeling (TM) Template was created using the Microsoft (MS) Threat Modeling Tool 2016 and therefore threat models are created using this product.

The Solution and its Features

The Automotive Threat Modeling Template permits the creation of specific automotive threat models with:

- Processes and Data Stores related to the components of connected cars.
- External Interactors tailored to an automotive system.
- Data Flows that correspond to the messages exchanged over the air or inside the vehicle itself.

About
NCC Group Template for the Microsoft Threat Modeling Tool 2016 for Automotive Security
[www.nccgroup.trust/uk/our-solutions/...](http://www.nccgroup.trust/uk/our-solutions/)
Readme

Releases
No releases published

Packages
No packages published

Figure 2: NCC Group Template Github Website

SETUP

This section describes the process of setting up the necessary tools and creating the appropriate environment for the modelling and analysis process.

INSTALL THREAT MODELLING TOOL

Download, Install and Run Microsoft Threat Modelling Tool

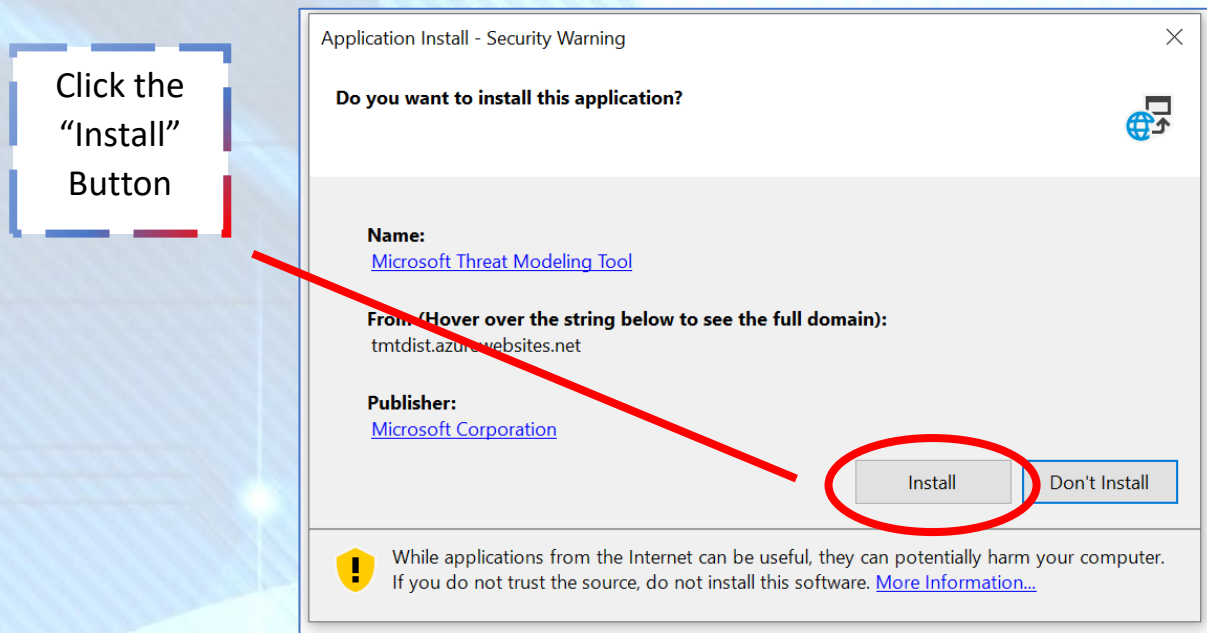


Figure 3: Install Permission Prompt

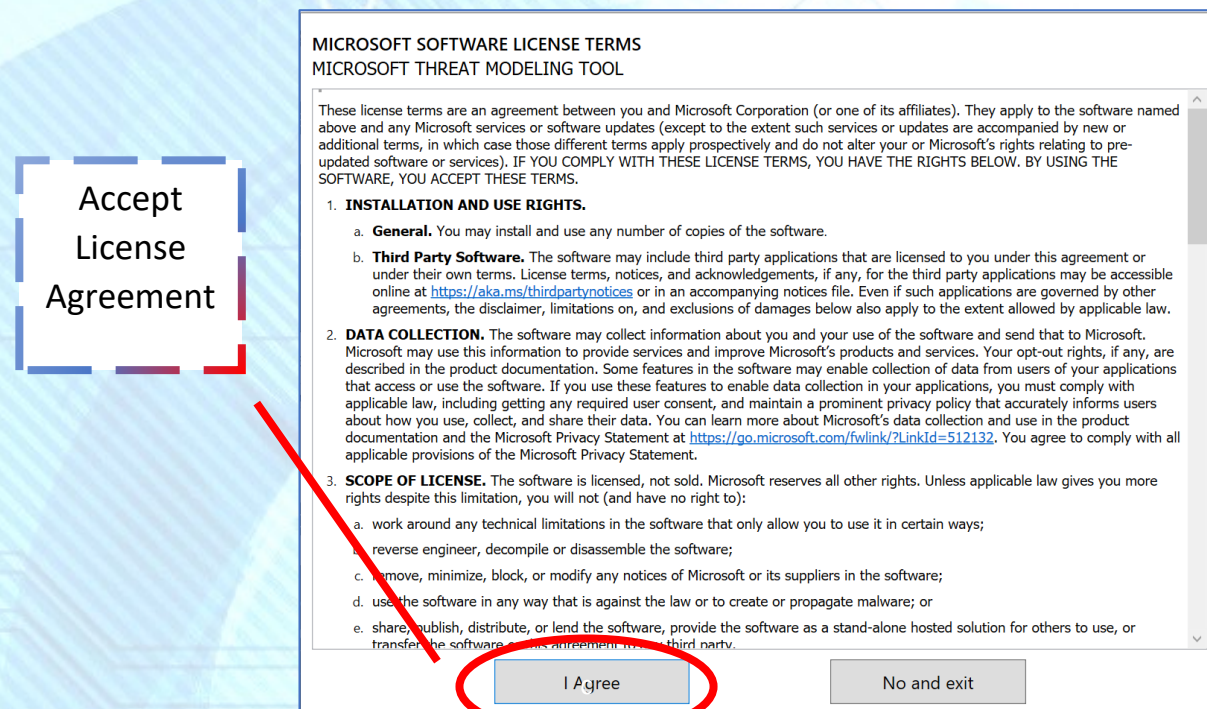


Figure 4: Software License Terms

LOAD NCC GROUP TEMPLATE

Load the NCC Group Template by selecting the downloaded template using the “Template for New Models”.

Select
Template
for New
Models

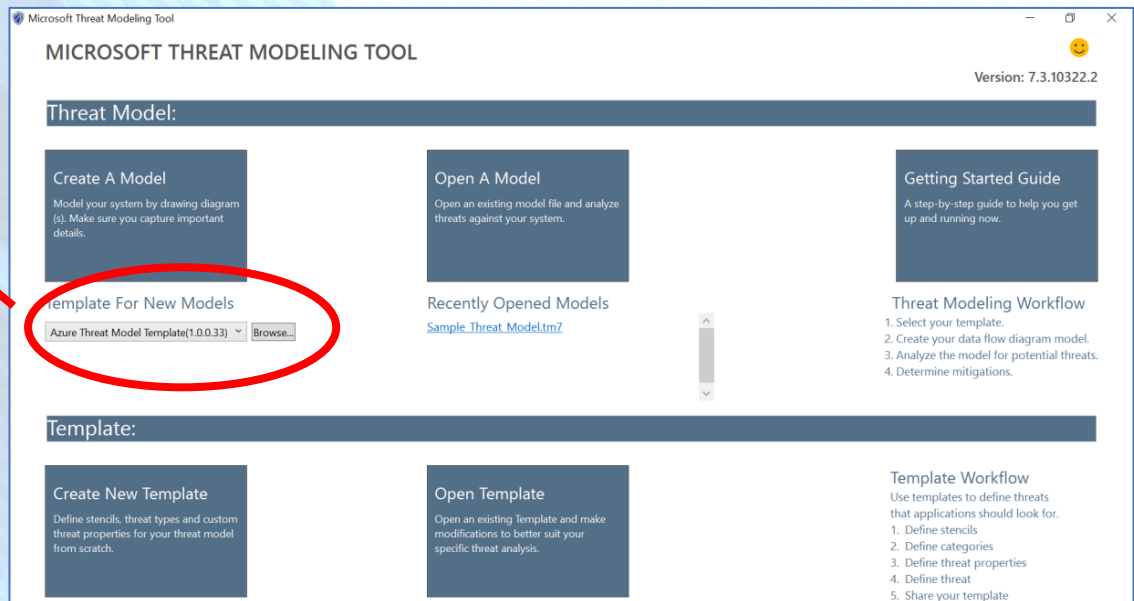
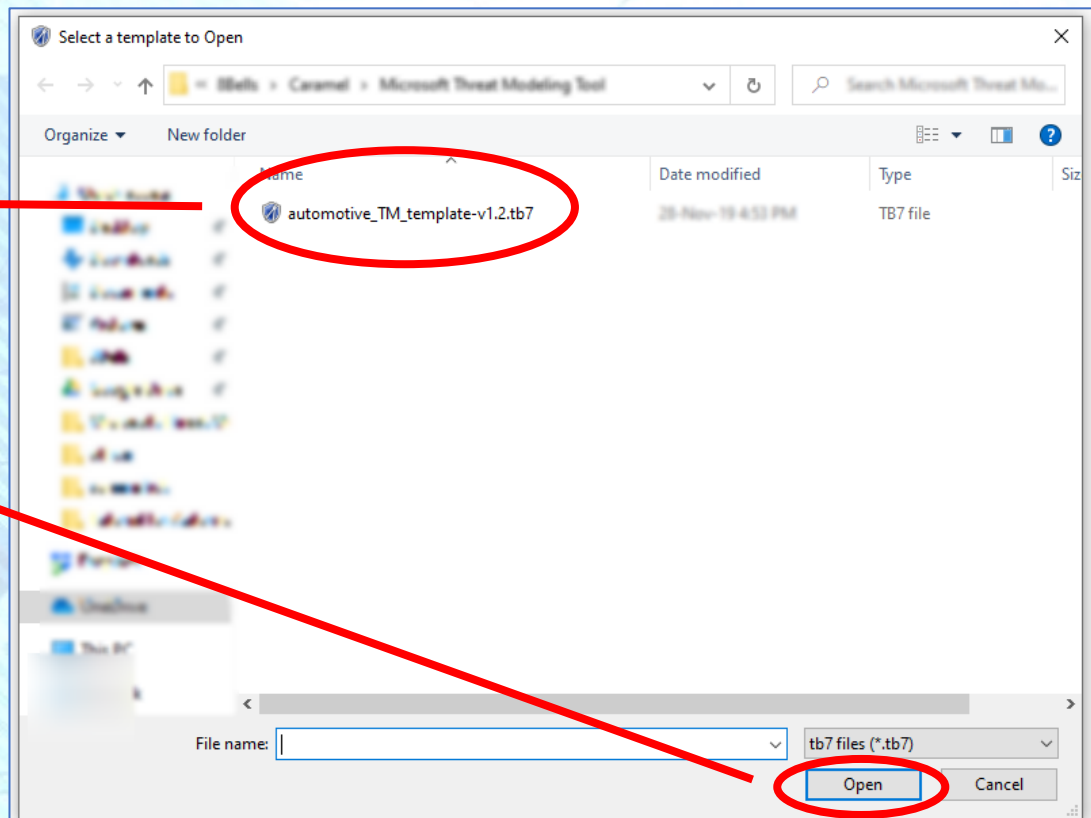


Figure 5: OPTION FOR Template for New Models

Select the
NCC Group
Template



Click the
“Open”
Button

Figure 6: Popup Dialog to Select NCC Group Template File.

Click to
Create a
Model

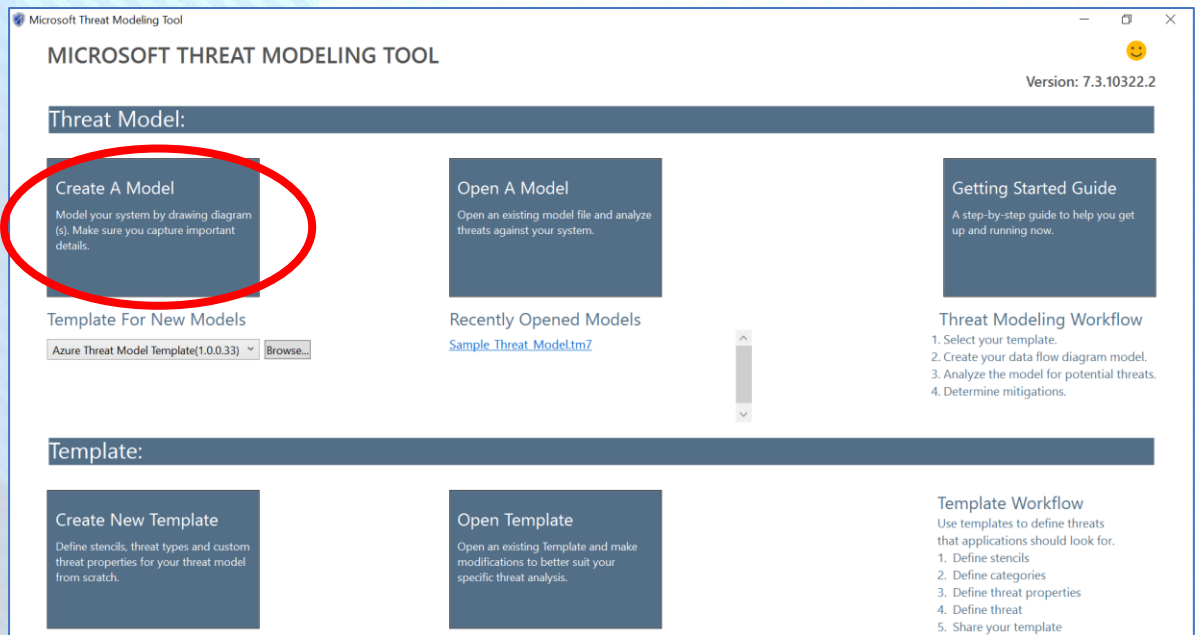


Figure 7: Option for creating a model

DATA FLOW DIAGRAM DESIGN

This step describes the process of building a model by adhering to the guidelines of a Data Flow Diagram by adding system details to the elements in the DFD. The aim is to represent a system or use case that is to be analysed, in DFD format. There are five types of elements in a DFD diagram: process, data store, data flow, external interactor, and trust boundary [1].

DATA FLOW DIAGRAM

A data-flow diagram is a way of representing a flow of data through a process or a system. The DFD also provides information about the outputs and inputs of each entity and the process itself. A data-flow diagram has no control flow, there are no decision rules and no loops. For each data flow, at least one of the endpoints, source or destination, must exist in a process. The refined representation of a process can be done in another data-flow diagram, which subdivides this process into sub-processes [1], [2].

AUTOMOTIVE STENCILS SELECTION

From the available list of stencils, select the appropriate automotive components such as Gateway or Electronic Control Unit (ECU) in order to design the current system or use case.

From the “Stencils” section, select the appropriate components.

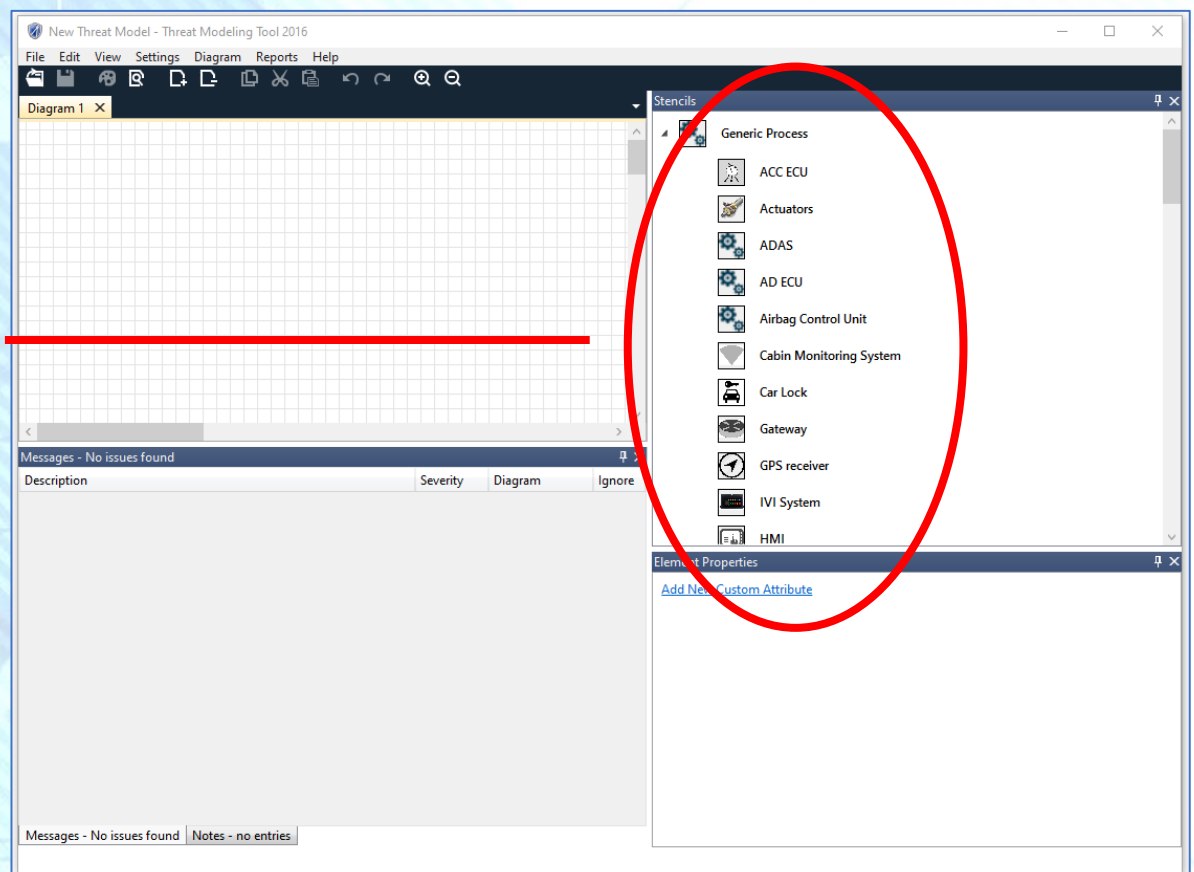


Figure 8: Canvas for Designing an Automotive Data Flow Diagram

COMPONENTS OF DATA FLOW DIAGRAM

DFD consists of processes, flows, warehouses, and terminators. There are several ways to view these DFD components.

Process

The process (function, transformation) is part of a system that transforms inputs to outputs. The symbol of a process is a circle, an oval, a rectangle or a rectangle with rounded corners (according to the type of notation). The process is named in one word, a short sentence, or a phrase that is clearly to express its essence [2], [3].

Data flow

Data flow (flow, dataflow) shows the transfer of information (sometimes also material) from one part of the system to another. The symbol of the flow is the arrow. The flow should have a name that determines what information (or what material) is being moved. Exceptions are flows where it is clear what information is transferred through the entities that are linked to these flows. Material shifts are modeled in systems that are not merely informative. Flow should only transmit one type of information (material). The arrow shows the flow direction (it can also be bi-directional if the information to/from the entity is logically dependent - e.g. question and answer). Flows link processes, warehouses and terminators [2], [3].

Warehouse

The warehouse (datastore, data store, file, database) is used to store data for later use. The symbol of the store is two horizontal lines, the other way of view is shown in the DFD Notation. The name of the warehouse is a plural noun (e.g. orders) - it derives from the input and output streams of the warehouse. The warehouse does not have to be just a data file, for example, a folder with documents, a filing cabinet, and optical discs. Therefore, viewing the warehouse in DFD is independent of implementation. The flow from the warehouse usually represents the reading of the data stored in the warehouse, and the flow to the warehouse usually expresses data entry or updating (sometimes also deleting data). Warehouse is represented by two parallel lines between which the memory name is located (it can be modeled as a UML buffer node) [2], [3].

Terminator

The Terminator is an external entity that communicates with the system and stands outside of the system. It can be, for example, various organizations (eg a bank), groups of people (e.g. customers), authorities (e.g. a tax office) or a department (e.g. a human-resources department) of the same organization, which does not belong to the model system. The terminator may be another system with which the modeled system communicates [2], [3].

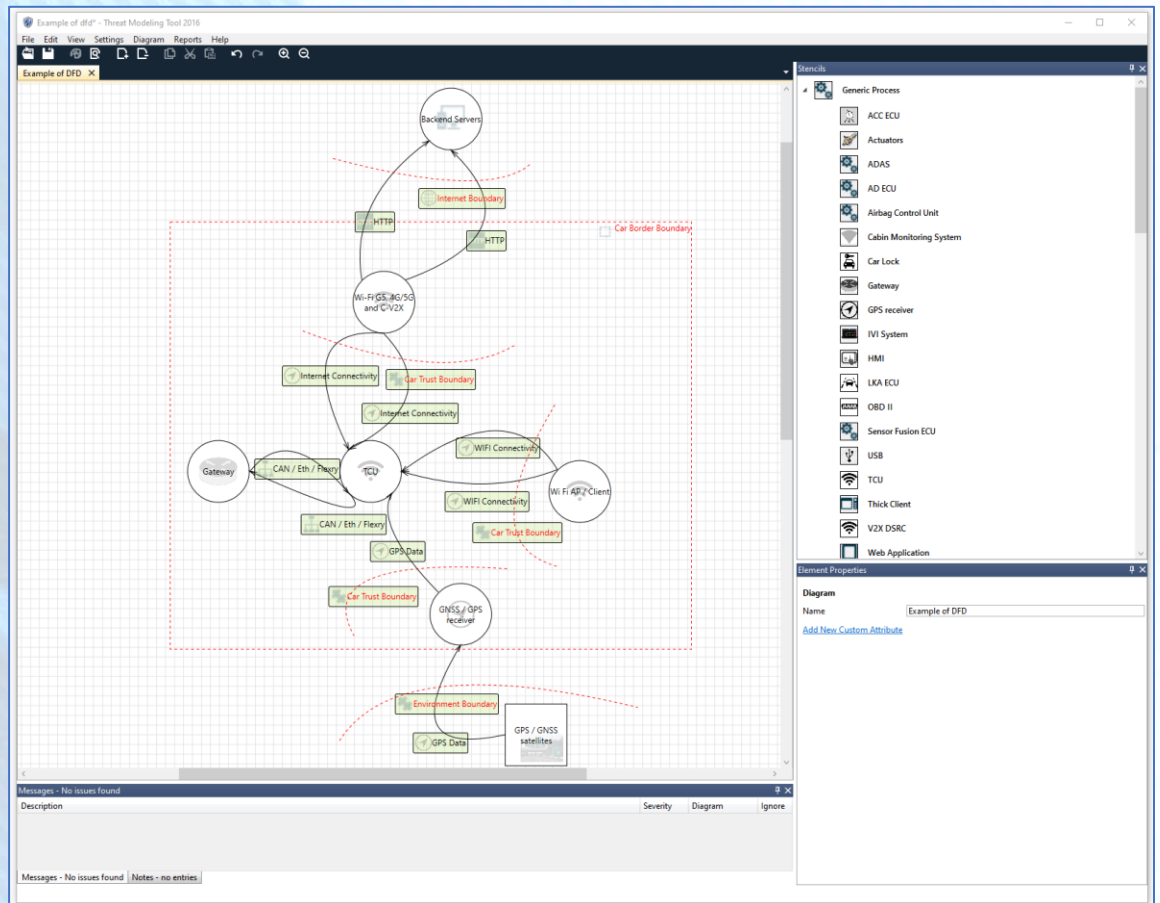


Figure 8: Example of a Data Flow Diagram designed using the Automotive Stencils

IDENTIFICATION OF THREATS USING THE STRIDE MODEL

Identify threats stemmed from data flows by using STRIDE threat identification and classification.

STRIDE THREAT MODELING

STRIDE is an acronym for six threat categories: Spoofing identity, Tampering with data, Repudiation threats, Information disclosure, Denial of service and Elevation of privileges. Two Microsoft engineers, Loren Kohnfelder and Praerit Garg, developed STRIDE in the late 1990s.

Teams can use the STRIDE threat model to spot threats during the design phase of an app or system. The first step helps find potential threats using a proactive process. The design of the system forms the basis for spotting threats. The next steps include finding the risks inherent in the way the system has been implemented, and then taking actions to close gaps.

Specifically, STRIDE aims to ensure an app or system fulfills the CIA triad (confidentiality, integrity and availability). Its designers created it to ensure that Windows software developers considered threats during the design phase. You should use STRIDE along with a model of the target system. Construct this model in parallel, including a breakdown of processes, data stores, data flows and trust boundaries. Using STRIDE, develop defenses for each threat. For example, imagine you find that an admin database is exposed to tampering with data, information disclosure and denial-of-service threats. In that case, you can implement access control logs, secure socket layer/transport layer security or IPSec authentication to counter those threats. [4]

GENERATE THREATS REPORT

The Threat Modelling Tool provides a generated report that lists several identified Threats by following the steps below.

Click the
Icon to
Switch to
Analysis

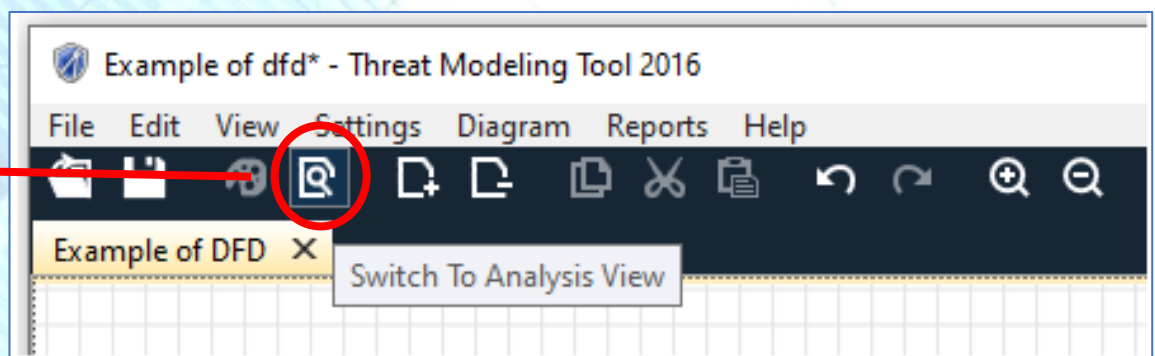


Figure 9: Switch to Analysis View

ID	Diagram	Last Modified	State	Title	Category	Description	Interaction	Risk	Attack methc	Recommendi
1	Example of DFD	Generated	Not Started	Modify Data B...	Tampering	Tamper with d...	GPS Data	High	MITM on the T...	Disable 2G co...
2	Example of DFD	Generated	Not Started	Car Could be T...	Information Di...	Information di...	GPS Data	Medium	Downgrade or...	Encrypt comm...
3	Example of DFD	Generated	Not Started	Data Flow Sniff...	Information Di...	Data flowing a...	GPS Data	Medium	Man-in-the-m...	Consider encry...
4	Example of DFD	Generated	Not Started	Updates Could...	Information Di...	Information di...	GPS Data	Medium	Reverse engine...	Ensure that co...
6	Example of DFD	Generated	Not Started	Cause the TCU...	Denial of Service	DoS on TCU th...	GPS Data	High	Flooding TCU...	Implement dat...
7	Example of DFD	Generated	Not Started	Flood TCU Wit...	Denial of Service	DoS on TCU by...	GPS Data	Medium	Either physicall...	Rely on additio...
8	Example of DFD	Generated	Not Started	Jam GPS Signal	Denial of Service	DoS on the GP...	GPS Data	Low	Use a GPS jam...	Have system u...
9	Example of DFD	Generated	Not Started	Take the TCU O...	Denial of Service	DoS on TCU.	GPS Data	Medium	Perform an net...	Have a numbe...
10	Example of DFD	Generated	Not Started	Compromise t...	Elevation of Pri...	Elevation of pri...	GPS Data	High	Network based...	Ensure that the...
11	Example of DFD	Generated	Not Started	Reflash the TC...	Elevation of Pri...	Elevation of pri...	GPS Data	High	Physically con...	All firmware sh...
34	Example of DFD	Generated	Not Started	Spoof GPS Sig...	Spoofing	Spoofing the...	WIFI Connecti...	Medium	By using a soft...	Combine GPS...
35	Example of DFD	Generated	Not Started	Modify Data B...	Tampering	Tamper with d...	WIFI Connecti...	High	MITM on the T...	Disable 2G co...
36	Example of DFD	Generated	Not Started	Car Could be T...	Information Di...	Information di...	WIFI Connecti...	Medium	Downgrade or...	Encrypt comm...
37	Example of DFD	Generated	Not Started	Data Flow Sniff...	Information Di...	Data flowing a...	WIFI Connecti...	Medium	Man-in-the-m...	Consider encry...
38	Example of DFD	Generated	Not Started	Updates Could...	Information Di...	Information di...	WIFI Connecti...	Medium	Reverse engine...	Ensure that co...
40	Example of DFD	Generated	Not Started	Cause the TCU...	Denial of Service	DoS on TCU th...	WIFI Connecti...	High	Flooding TCU...	Implement dat...
41	Example of DFD	Generated	Not Started	Flood TCU Wit...	Denial of Service	DoS on TCU by...	WIFI Connecti...	Medium	Either physicall...	Rely on additio...
42	Example of DFD	Generated	Not Started	Jam GPS Signal	Denial of Service	DoS on the GP...	WIFI Connecti...	Low	Use a GPS jam...	Have system u...
43	Example of DFD	Generated	Not Started	Take the TCU O...	Denial of Service	DoS on TCU.	WIFI Connecti...	Medium	Perform an net...	Have a numbe...

98 Threats Displayed, 98 Total

Figure 10: List of Identified Threats

Title	Category
Modify Data Being Sent to the TCU While in Transit	Tampering
Car Could be Tracked	Information Disclosure
Data Flow Sniffing	Information Disclosure
Updates Could Be Downloaded From a Web Server...	Information Disclosure
Cause the TCU to Crash or Stop Remotely	Denial of Service
Flood TCU With Invalid Data	Denial of Service
Jam GPS Signal	Denial of Service
Take the TCU Offline	Denial of Service
Compromise the TCU in Order to Deliver Malicious...	Elevation of Privilege
Reflash the TCU Firmware in Order to Send Arbitrar...	Elevation of Privilege
Spoof GPS Signals and Deliver Malicious GPS Data i...	Spoofing
Modify Data Being Sent to the TCU While in Transit	Tampering
Car Could be Tracked	Information Disclosure
Data Flow Sniffing	Information Disclosure
Updates Could Be Downloaded From a Web Server...	Information Disclosure
Cause the TCU to Crash or Stop Remotely	Denial of Service
Flood TCU With Invalid Data	Denial of Service

Figure 11: Identified Threats are Categorized using the STRIDE Model

ANALYSIS AND MITIGATION ACTIONS

A key process in Threat Modelling is the Qualitative Evaluation of the results and as a result this stage requires cybersecurity expertise and people with an in-depth understanding of the analysed system or use case. Using the information gathered so far it is possible to start analysing the threats and the potential threat-sources of the system from a qualitative perspective. A threat-source is defined as any circumstance or event with the potential to cause harm to a system. Therefore, the following steps are to be followed to evaluate and adjust the list of identified threats [5], [6].

QUALITATIVE EVALUATION OF THE AUTOMATICALLY GENERATED IDENTIFIED THREATS

At the previous stage, a list of identified threats including their impact, attack method, recommendations, etc was generated as a result of the threat analysis based on the Threat Modelling tool utilising the STRIDE model.

Description ▼	Interaction ▼	Risk ▼	Attack method ▼	Recommendation ▼
Tamper with data in transit sent to th...	GPS Data	High	MITM on the TCU for example a...	Disable 2G communications, only...
Information disclosure by performin...	GPS Data	Medium	Downgrade or false base statio...	Encrypt communications so that...
Data flowing across [Generic Data Fl...	GPS Data	Medium	Man-in-the-middle using attac...	Consider encrypting the data flow...
Information disclosure by download...	GPS Data	Medium	Reverse engineer the head unit...	Ensure that connections to the de...
DoS on TCU that crashes, halts, stop...	GPS Data	High	Flooding TCU with invalid mess...	Implement data validation and sh...
DoS on TCU by flooding with invalid...	GPS Data	Medium	Either physically by clipping on...	Rely on additional sensors in the e...
DoS on the GPS antenna by jammin...	GPS Data	Low	Use a GPS jammer/send high p...	Have system use other sources of...
DoS on TCU.	GPS Data	Medium	Perform an network attack and...	Have a number of TCU delivery se...
Elevation of privileges in order to ex...	GPS Data	High	Network based vulnerabilities, t...	Ensure that the server is kept up t...
Elevation of privileges in order to ref...	GPS Data	High	Physically connect to the target...	All firmware should be encrypted...
Spoofing the Wi Fi AP / Client in ord...	WIFI Connecti...	Medium	By using a software defined rad...	Combine GPS with other sources...
Tamper with data in transit sent to th...	WIFI Connecti...	High	MITM on the TCU for example a...	Disable 2G communications, only...
Information disclosure by performin...	WIFI Connecti...	Medium	Downgrade or false base statio...	Encrypt communications so that...
Data flowing across [Generic Data Fl...	WIFI Connecti...	Medium	Man-in-the-middle using attac...	Consider encrypting the data flow...
Information disclosure by download...	WIFI Connecti...	Medium	Reverse engineer the head unit...	Ensure that connections to the de...
DoS on TCU that crashes, halts, stop...	WIFI Connecti...	High	Flooding TCU with invalid mess...	Implement data validation and sh...

Figure 12: Auto-Generated Information related to the Identified Threats

QUALITATIVE ANALYSIS OF IDENTIFIED THREATS

The final result is adjusted to reflect both, the threat analytical power of a software tool and the qualitative perspective of human expertise in the field. The Auto-Generated List of Identified Threats (see Figure 10 and Figure 12) is the evaluated, qualitatively by employing the essential cybersecurity expertise and people with an in-depth understanding of the analyzed system or use case. This step, of analyzing the identified threats, has a degree of dependence on analyst/expert quality [7], [8]. The table below depicts an example of a custom table that was a result of the Qualitative Evaluation making the necessary adjustments to the Description, Method and Impact.

Threat ID	Title	Description	Method	STRIDE	IMPACT
ID1	Modify GPS data being sent to the vehicle	Tamper with GPS data in transit being received by the vehicle	MITM on the TCU for example a 3g to 2g downgrade attack, or false base station attack.	Tampering	High
ID35	Modify data being sent to the vehicle through wireless	Tamper with data being received by the vehicle in transit through wireless communication.	MITM on the TCU for example a 3g to 2g downgrade attack, or false base station attack.	Tampering	High
ID46	Spoof GPS signals and deliver malicious GPS data in order to cause drift off course.	Spoofing of GPS data in order to deliver malicious GPS data to vehicle to cause drift off course.	By using a software defined radio to send custom and GPS data.	Spoofing	Medium

Figure 13: STRIDE Threat Classification

QUALITATIVE ANALYSIS OF MITIGATIONS

Similar to the process of the analysis of the identified threats, a qualitative analysis of mitigations must be performed. Therefore, a list of Mitigations is produced that is the result of qualitative evaluation from the perspective of essential cybersecurity expertise and people with an in-depth understanding of the analyzed system or use case [7], [8]. The table below depicts an example of Mitigations suggested in the form of a custom table that was the result of Qualitative Evaluation, making the necessary adjustments to the recommendations for each threat.

Threat ID	Title	Description	Mitigation	STRIDE
ID1	Modify data being GPS data being sent to the vehicle	Tamper with GPS data in transit being received by the vehicle	Use a secure communication channel between the vehicle and GPS Satellite. Use commercial solutions or features like OS NMA (Open Service Navigation Message Authentication) and CAS (Commercial Authentication Service) from Galileo could be useful.	Tampering
ID35	Modify data being sent to the vehicle through wireless	Tamper with data being received by the vehicle in transit through wireless communication.	Wireless communication should be properly secured with basic configurations like hidden SSID, password protection (WPA 2 - WIFI protected access), communication encryption, etc.	Tampering
ID46	Spoof GPS signals and deliver malicious GPS data in order to cause drift off course	Spoofing of GPS data in order to deliver malicious GPS data to vehicle to cause drift off course.	Combine GPS with other sources of data to provide additional validation. Use a secure communication channel between the vehicle and GPS Satellite. Use commercial solutions or features like OS NMA (Open Service Navigation Message Authentication) and CAS (Commercial Authentication Service) from Galileo could be useful.	Spoofing

Figure 14: Mitigations for Identified Threats



REFERENCES

- [1] Z Ma and C Schmittner (2016) Advanced Science and Technology Letters. Vol.139 (SecTech 2016). Available online: https://www.researchgate.net/profile/Christoph-Schmittner/publication/312189316_Threat_Modeling_for_Automotive_Security_Analysis/links/58dbb49f92851c611d024a66/Threat-Modeling-for-Automotive-Security-Analysis.pdf
- [2] Data-flow diagram. 2021. In Wikipedia. Available online: https://en.wikipedia.org/wiki/Data-flow_diagram
- [3] Scheer, A. W. (2000). ARIS business process modeling. Springer Science & Business Media.
- [4] <https://securityintelligence.com/articles/what-is-stride-threat-modeling-anticipate-cyberattacks/>
- [5] Shostack, A. (2008). Experiences Threat Modeling at Microsoft. MODSEC@ MoDELS.
- [6] A. Stango, N. R. Prasad and D. M. Kyriazanos (2009). A Threat Analysis Methodology for Security Evaluation and Enhancement Planning. 2009 Third International Conference on Emerging Security Information, Systems and Technologies, 2009. Available online: <https://ieeexplore.ieee.org/abstract/document/5210987>
- [7] Bodeau, D. J., McCollum, C. D., & Fox, D. B. (2018). Cyber threat modeling: Survey, assessment, and representative framework. MITRE CORP MCLEAN VA MCLEAN. Available online: <https://apps.dtic.mil/sti/citations/AD1108051>
- [8] Selin, J. (2019). Evaluation of threat modeling methodologies.