SECURE CAV

T — Threat Modelling

Automotive threat modelling: off-the-shelf solutions

by **James Tyrrell** · 9 July, 2020

In this article, James Tyrrell looks at the rise of ready-made tools, highlighting the growth in threat

modelling support for the automotive sector – activity that's been boosted by calls for cybersecurity management systems and upfront security design.

Shared values: libraries and templates provide opportunities for collaboration across the automotive threat modelling community. Photo credit – James Tyrrell

Threat modelling provides a structured approach to gathering vulnerability information and is an important step in delivering product security by design. Hunting down potential cyber threats ahead of major phases in product development gives designers the opportunity to consider countermeasures and incorporate them into upcoming devices.

In a previous post we gathered information on a number of tools – ranging from simple drawing and flow-charting applications through to more automated threat-generation solutions – that can help developers by highlighting possible security weaknesses in a given scenario or use case.

Many of these packages are closely associated with software development, where threat modelling has long been applied – for example, as a core element of the Microsoft Security

Development Lifecycle. But that's not to say that off-the-shelf solutions don't exist for the automotive sector.

The availability of commercial tools primed with domain-specific knowledge illustrates how threat modelling has begun to focus on the needs of Tier 1 suppliers and OEMs.

New tool on the block

Launched just a few months ago, ThreatGET – a plug-in for the Enterprise Architect platform – has been jointly developed by the Austrian Institute of Technology and Sparx Services, a maker of business modelling software. Their solution builds on the popular STRIDE framework and features a large 'knowledgebase' of more than 1400 threats, accessed via a subscription.

Looking more closely at user requirements, the developers note the significance of United Nations Economic Commission for Europe (UNECE) guidelines (link to summary slides), which discuss the adoption of a certified cybersecurity management system by manufacturers.

Such a system should be able to assess the cybersecurity of all vehicle types, identify and document potential threats, suggest countermeasures and verify solutions – areas where threat modelling solutions can make a positive impact. The UNECE guidelines also propose that processes cover all phases of a vehicle's life until scrappage.

At the same time, the automotive community is being urged to consider ISO 21434 – "Road vehicles – Cybersecurity engineering" – released this month as a draft international standard (DIS).

One of the key purposes of ISO 21434 is to define a structured process to ensure that cybersecurity is designed-in upfront. And, much like with the adoption of the UNECE proposals, ISO 21434 is likely to prompt more widespread use of threat modelling tools in the automotive sector.

Model-based security risk assessment

ThreatGET's developers aren't the only tool providers keeping a close eye on recommendations being made to vehicle manufacturers. As we've mentioned in a previous post, Itemis – the developer of Yakindu Security Analyst – has blogged on the topic of how a

model-based security risk assessment can help with the adoption of cybersecurity standards in the automotive space. Their tool considers the protection needs of assets within the vehicle ecosystem and then prompts users to focus on related threats together with the damage potential and attack effort required.

Risk calculations are then engineered through a look-up table that ties parameters together. The package also outputs a bubble chart to help users in visualising the distribution of risk for a particular security goal.

Opportunities to team up

In the introduction, we hinted at prospects for collaboration across the threat modelling community and one of the biggest opportunities is to open-source automotive threat libraries. Speaking with tool developers, all are keen to avoid users having to re-work similar threat lists.

One idea on the table is vehicleLang – a meta attack language compiled by researchers at KTH Royal Institute of Technology in Sweden, which has been made available through GitHub. The scheme provides a syntax for describing and evaluating, by applying probability functions, vehicular cybersecurity.

In its current form, vehicleLang can be paired with SecuriCAD – a threat modelling tool developed by KTH spin-off company foreseeti. Equipped with the automotive-specific data, SecuriCAD is then able to generate estimates of the time taken to compromise high-value vehicle assets.

There are other broader options too such as MITRE's STIX – a standardised structured language for cyber threat intelligence, which is designed to improve collaborative threat analysis.

James Tyrrell

James Tyrrell is a Threat Modelling Analyst at Copper Horse