

VA Software Assurance Secure Coding Tip

Microsoft Threat Modeling Tool Now In TRM

This week's Secure Coding Tip is to share with the VA software development community the new entry in the One-VA Technical Reference Model (TRM) for the Microsoft Threat Modeling Tool. It has been assessed and published in version 16.11 of the TRM, making it now possible to install on VA machines. Its entry in the TRM can be found [here](#).

The Microsoft Threat Modeling Tool supports the "Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege" (STRIDE) methodology. STRIDE is an iterative process where an application's design is systematically decomposed and analyzed. It can be followed to identify potential security flaws introduced early during development.

The VA Software Assurance Program Office will be publishing Standard Operating Procedures (SOP) for using the Microsoft Threat Modeling Tool at the VA during development soon. The VA Software Assurance Program Office will also be providing support for using the software, as well as assistance developing initial application threat models and validation of model diagrams.

Resources

- [VA Software Assurance Support Site](#)
- [Request VA-licensed code review tools, validations, and support](#)
- [Latest VA Software Assurance Program Office announcements](#)
- [Check if your application has been registered \(internal link\)](#)

Reminders

- [The next working group meeting is on 12/6](#)

You have received this message because you are subscribed to VA Software Assurance Secure Coding Tips. To unsubscribe to these announcements or to subscribe, email: OISSwASupportGroup@va.gov

VA



**U.S. Department
of Veterans Affairs**

**Office of Information
and Technology**

*Software Assurance
Program Office*