Creating Security Threat Models For Your Applications

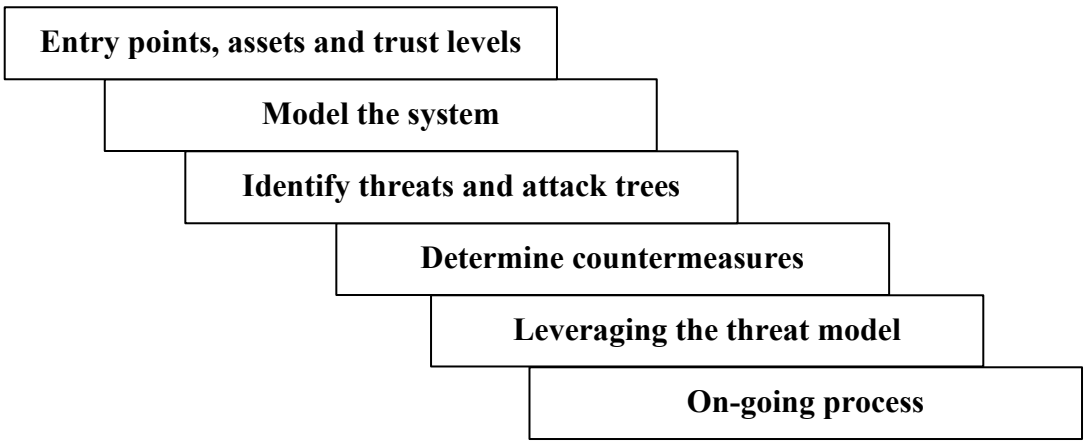
Goals of threat modelling, Steps for building a threat model, Thinking like an attacker, Vulnerabilities and countermeasures, Managing privilege, Model uses, On-going process

Overview

Of the three general forms of security - network, host and application, the last of these is the one software developers have to most concern themselves with most. Competent system administrators will be able to stop many – but not all - forms of attack at the network or host level. Threat modelling helps developers stop application attacks (e.g. a seemingly valid HTTP message may well get through outer defences and be delivered to an application – whether it is actually valid often depends on application-specific context).

This workshop lasts one or more days (depending on application size) and is facilitated by a security expert from Clipcode who helps software development teams create threat models.

Six-Stage Strategy



- **Entry points, assets and trust levels** - Developers need to think what is of value directly within or exposed via their application; how it can be accessed and what privilege is associated with groups of users.
- **Model the system** – Creating a compact model of the application with the necessary detail from a security perspective (data flow diagrams, etc.) .
- **Identify threats and attack trees** – Creating a prioritised list of how the system may be attacked (STRIDE/DREAD). Attacks often involve a series of steps, that at first may seem unconnected.
- **Determine countermeasures** – If a threat were to evolve into a real attack, what steps are needed to ensure the application is prepared to react robustly? Need to minimise vulnerabilities.
- **Leveraging the threat model** – Once the model is complete, deciding what to do with it. Showing how the software's security is demonstratively improved.
- **On-going process** – Threat models should fit in with the application development life cycle, be it agile or a more structured formal process.

Features & Benefits

Entry points, assets and Trust Levels	Understanding what is of value and how exposed it is helps in clarifying what needs to be protected.
Model the system	Understanding how and why data flows across trust boundaries, software components and network hosts is a key precursor to identifying threats.
Identity threats and attack trees	Knowing all the ways an application may be attacked is needed in order to ensure appropriate mitigation is in place.
Determine countermeasures	Countermeasures are what ensure threats do not become vulnerabilities. For each threat, having a clear action plan in place ensures improved security.
Leveraging the threat model	Fixing problems with architecture early on; basis for security-specific testing; proving the security characteristics of application to potential customers.
On-going process	As software architecture changes, so too must the threat models. Building on knowledge of initial threat models helps us investigate how more advanced attacks be countered.

Target Market

This workshop targets software engineering teams who need to ensure they are correctly designing security into their systems. Such teams need to consider the various threats that their applications face and put in place appropriate countermeasures.

Security Software Architect from Clipcode

The security software architect that Clipcode provides has excellent software design and development skills along with ample software security expertise, particularly in the area of application security.

Who Should participate from the Client

For each feature under consideration, the threat modelling team should consist of the senior developers for that feature, the software architect for the application and the developer with overall responsibility for the application's security. Depending on the attendees' level of knowledge, overview and advanced presentations on threat models can be provided as part of the workshop if desired by the client.

How to proceed

If you are concerned that security threats your applications face may become (unmitigated) vulnerabilities and would like to counter this by arranging a Threat Model Workshop on-site in your company's offices, please contact Clipcode below. We need to discuss arrangements further, agree goals for the engagement and set a tentative schedule.

CLIPCODE™ www.clipcode.net	**If your dev team is starting an important project and needs help, please contact us via email at sales@clipcode.com to discuss how we can be of assistance.**