THREAT MODELING & DESIGN REVIEWS

THREAT MODELING AND DESIGN REVIEWS

Practicing 'security by design' starts with applying secure design principles. Once the design of a system has reached a sufficient level of detail, it can be extremely valuable to perform a design review and/or threat modeling exercise. Also in existing systems it can be essential to know where additional mitigation measures are necessary to lower risks to your systems and data.

Secura uses the STRIDE methodology for threat modeling and likes the simplicity yet effectiveness of raising security awareness during the process. The goal of the STRIDE methodology is to identify security threats in a stakeholder-driven workshop. Our design review approach can use common methodologies like SABSA lifecycle, however the exact approach is highly dependent on the system/network in scope.

Applications and systems are often part of a chain of information-processing systems. When securing an application, system or the complete chain, it is important to know from which perspective threats arise and how a system can be attacked. In a highly interactive session with developers, architects, business owners and other stakeholders, Secura identifies the possible threats per component system and interface. Secura will perform threat modeling according to the STRIDE model via four steps; Diagram, Identify Threats, Mitigate and Validate (see Figure 1).

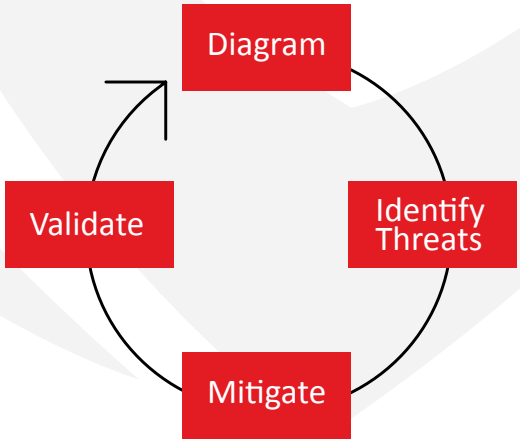

Figure 1: Four process steps in Threat Modeling [1]

The first step is a so-called Data Flow Diagram (see figure 2 for an example Data Flow Diagram). The advantage of threat modeling is that the graphical representation of the (information flows within the) applications / systems can be used to detect and prevent security errors more quickly.

[1] Source: Microsoft Technet

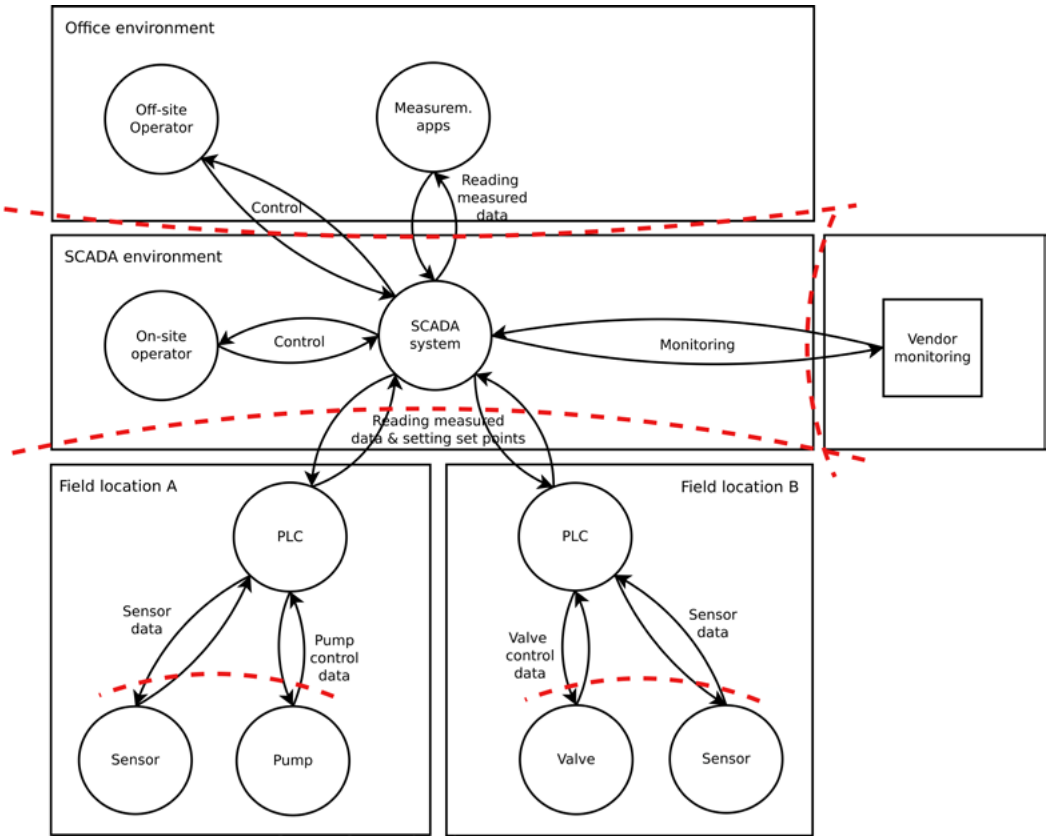

Figure 2: Example data flow diagram

In the second step, we look at every transfer between different trust levels in the chain, various data flows and interfaces. We do this by applying the principles of the STRIDE methodology to analyse for threats and weaknesses (where STRIDE stands for the first letters of the following threats):

Threat	Relevant Aspect
Spoofing	Authenticity
Tampering	Integrity
Repudiation	Non-repudiation
Information disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorisation checks

In the third step the identified threats can subsequently be used for instance to create efficient test scenarios, design adjustments or to define methods to mitigate the threats. Within the workshop we align the way forward, which provides the customer with a decision document for upper management (if not present in the workshop).

In the last step (Validate) we advise to actually test and validate whether the implemented mitigations remove the identified threats, and whether these mitigations potentially create new threats. This step takes place outside the workshop after mitigating measures have been designed and are being tested. This step can be executed by the company itself or Secura can provide support to investigate whether the threats have been correctly resolved.

ATTACK TREES

The threat modeling sessions will be held in the form of a workshop where our consultants together with your developers, designers and other stakeholders will discuss the relevant threats per data flow and per threat. This gives a complete picture of the threats and possible attack paths. Not only are our consultants trained in the STRIDE methodology, they also have plenty of experience in thinking like an attacker to identify many new attack scenarios. Depending on the situation, Secura can employ other methodologies such as attack trees and attack libraries instead of STRIDE. Methodologies such as attack trees are very well suited in situations where security depends on both physical and digital security measures, or in situations where the environment is too big to threat model properly using STRIDE. Larger environments, that consist of hundreds of components and data flows, are not very well suited to threat model using STRIDE. In situations such as these, an attack tree can provide a better-suited approach, by identifying the paths an attacker can take to reach its goal.

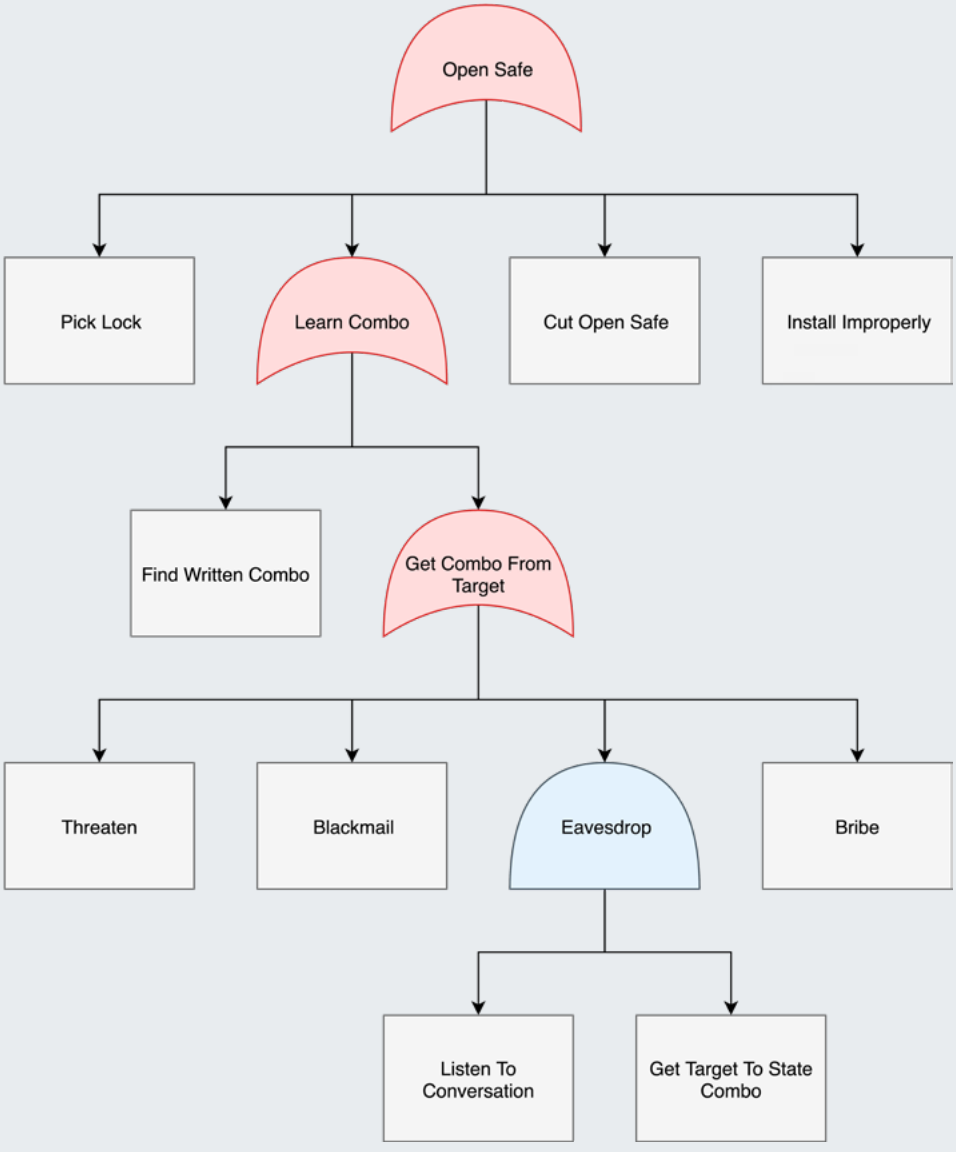

Figure 3: Example attack tree

DIFFERENCE BETWEEN DESIGN REVIEW AND THREAT MODELING

Design Review

With a design review Secura will read and review all available (relevant) design documentation and discuss this with the architect, technical owner, designers and/or developers. Finally, Secura will analyse all information and verify this against information security policies (if available) and best practices.

Benefits: with limited available time amongst staff or with many open questions within the design (early stage) this might be a better option.

Threat Modeling Session

With a threat modeling session Secura will prepare a workshop session for all relevant (internal) stakeholders and sketch the design on the spot, while identifying data streams and potential threats.

Benefits: The threat modeling workshop is great to raise security awareness and collaboration amongst stakeholders. Instead of focusing on the design, which is often incomplete and/or implemented differently in practice, the threat modeling session will take the situation in practice as the starting point to determine which threats are applicable. Next to this, it combines the knowledge and creativity of multiple people, to determine the threats applicable.

Design Reviewing and Threat Modeling are powerful methods to identify risks before abuse takes place. Therefore they are relatively cost-effective as often substantial new risks are identified prior to implementation or before risks actually become reality.

With nearly two decades of experience and a huge body of knowledge, Secura is in the fortunate position of being one of the few parties who can perform effective design review and threat modeling on virtually all types of systems, from embedded and IoT devices, to ephemeral cloud solutions that could be anywhere in the world. With our in-depth knowledge of state-of-the-art attacks and our hacker mindset the result will enable you to target the weakest spots in any system.

INTERESTED?
Would you like to learn more about our services?
Please do not hesitate to contact us.

Follow us on

Vestdijk 59
5611 CA Eindhoven
Netherlands

Karspeldreef 8
1101 CJ Amsterdam
Netherlands

T +31 (0)40 23 77 990
E info@secura.com
W www.secura.com