**Threat Modelling Overview**

Hi. In this video, we'll be introducing the concept of threat modelling. In particular, what it is, why it can be useful, and the general purpose of threat modelling. Let's start with the definition. It can be considered a systematic and structured way of determining the threat landscape for a particular context. The context could be, for example, an application a software development team is creating or, indeed, a part or whole of a system.

It's important to note that it must be systematic. That is, it's clearly defined and has repeatable steps. The threat landscape can be thought of as the range of attacks which are present within the current landscape. In this digital age, more and more, systems and information is accessible through networks such as the internet.

Thus, when looking at the security of any system, we need to consider the whole range of possible attacks. Threat actors, that is, those individuals with malicious intent to compromise the security of a system, have an easier job than those trying to defend the system. Threat actors need only find one way into a system, whereas defenders need to try and patch up all possible vulnerabilities. When looking at the security of the system, we need to consider possible threats, the potential impact if those attacks were realised, and we need to look at the kind of mitigation techniques we might employ. Threat modelling provides a structured approach for considering the possible threats against a given context. This gives us a much more structured way for achieving this, rather than an ad hoc approach which may be more inclined to miss particular elements.

Knowing this, let's move on to the general approach for such a process. Threat modelling can generally be thought of as a process for answering four questions. First of all, what are we building? Then, what can go wrong? Moving on to what we're going to do about it and then always including some form of reflection to revisit, see how we performed, and revise any mechanisms, policies, or procedures, as appropriate. Looking at each of these in a little bit more detail, what are we building activities might include things like explaining and exploring a system.

The output could be diagrams, such as components of the software, class diagrams, or data

flow diagrams, and so forth. Moving on to what can go wrong, this can generally be thought of as brainstorming potential threats and attacks such as denial of service. At this stage, it can be helpful to have a framework to structure any discussions around.

There are a range of options available, such as STRIDE, cyber kill chains, and attack trees, to name but a few. The next step is what will we do about it. This involves considering the mitigation techniques which could be employed, prioritising them, and then obviously going on and actually implementing them.

And, at the end, reflecting and revising any of these procedures or mitigation techniques, as appropriate. We've now covered a general overview of what threat modelling is and how it can be used. There are a variety of different techniques. And, clearly, as you develop your experience, you'll become better at achieving those.

However, I'd like to leave you with one thought, and it's a quote from Bruce Schneier, and that is that, "Security is a process, not a product." Threat modelling is a process which helps us consider the security of a system in a more structured fashion, and we'll see different techniques of achieving this in other videos.

I hope you've enjoyed this video, and I'll see you next time.

REF UK TOP 20 RESEARCH-INTENSIVE UNIVERSITY
THE UK UNIVERSITY OF THE YEAR WINNER
THE UK ENTREPRENEURIAL UNIVERSITY OF THE YEAR WINNER

The place of useful learning

The University of Strathclyde is a charitable body, registered in Scotland, number SC015263