Security engineering | Formal methods

Formal verification as a basis for secure systems

Construction companies will only start building when the architect has shown, using calculations, that their design will not collapse. Similarly, robust designs are also desired for the digital systems protecting our communications, business processes and more. Often, these systems contain cryptographic components and are notoriously hard to check by hand. (Partially) automated formal verification methods can be used to improve the resilience of the designs and implementations of these systems during early phases of development.

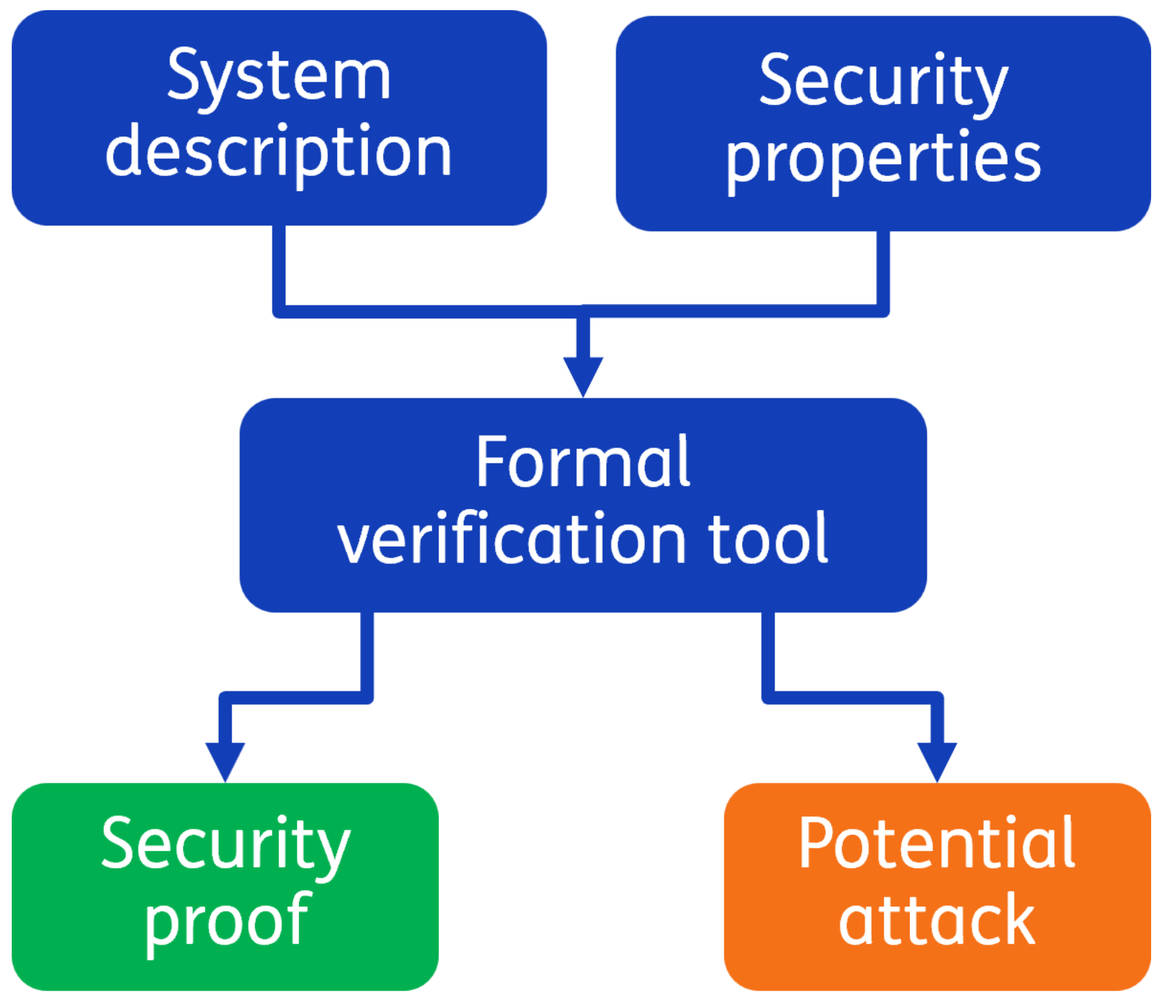
Protecting communication
Our phones communicate with our lights, our laptops with each other and our PLCs with sensors. Time has shown that even standardised cryptographic protocol implementations used in such widely deployed systems may contain critical vulnerabilities. Traditionally, their designs are checked by hand and their implementations by testing. However, even a seemingly easy protocol may be misused in unexpected ways by a clever entity. To prove that desired security properties like secrecy of messages or authentication of communication partners hold, automated formal verification tools can be used.

Secure protocol design
Using protocol verification tooling, such communication protocols along with their security properties can be modeled. These models are then used to automatically verify the properties.

For example, it can be shown that man-in-the-middle attacks are not feasible for a malicious agent with capabilities like eavesdropping the line and modifying sent messages. Alternatively, the tool may show that a property cannot be verified. In that case, an attacks scenario will be presented. This can then be used to repair the design flaw.

Verified implementations
When implementing these designs, new vulnerabilities can be introduced. To find these, implementations can be checked against a specification using another type of formal verification tools. Even leakage of information via some side-channels can be detected.

You already benefit
This kind of tooling has been used to verify widely-used protocols such as TLS 1.3, EMV and Apple iMessage. Will your systems be the next that have their security assured?



Contact

Anne Nijsten
anne.nijsten@tno.nl
+31 6 2397 6449
linkedin.com/tno

TNO innovation for life