Onderzoeksopzet: *Ontwikkeling van een gebruiksvriendelijke threat modeling tool gebaseerd op fortunately/unfortunately methode*

Naam student(en): Mika Gielkens

Naam promotoren (en firma/onderzoeksinstelling): Prof. dr. ir. Koen Yskout (KULeuven), Dr. Eva Geurts (EDM), KULeuven/UHasselt

Afstudeerrichting: IIW Informatica

Datum: 13/10/2025

1. **SITUERING (MAX. 500 woorden)**

Cybersecurity is tegenwoordig een van de grootste uitdagingen binnen softwareontwikkeling. Met de steeds complexere software en de groeiende digitalisering, worden ook de securityrisico’s groter. Bedrijven, overheden en organisaties zijn sterk afhankelijk van digitale systemen, waardoor de impact van een security risk niet alleen economisch, maar ook maatschappelijk zeer groot kan zijn. Het vroegtijdig opsporen en beperken van mogelijke bedreigingen vormt daarom een essentieel onderdeel van het softwareontwikkelingsproces.

Een veel gebruikte aanpak om dit te doen is threat modeling: het identificeren en analyseren van potentiële bedreigingen en zwaktes in een softwaresysteem. Binnen de industrie bestaan hiervoor methodieken zoals STRIDE, CAPEC of attack trees, die ontwikkelaars ondersteunen bij het structureren van mogelijke aanvalsscenario’s. Deze methodes zijn vaak complex en vragen een zekere kennis van beveiliging, wat voor beginnende ontwikkelaars zonder sterke security achtergrond een hoge drempel kan vormen.

Om die drempel te verlagen gaat dit onderzoek te werk met een Fortunately-Unfortunately Tree, een techniek afkomstig uit het improvisatietheater. Hierbij worden mogelijke bedreigingen (“unfortunately”) en bijhorende tegenmaatregelen of positieve uitkomsten (“fortunately”) afwisselend in een boomstructuur geplaatst. Dit maakt het proces minder technisch en intuïtiever, terwijl het toch de kern van dreigingsmodellering behoudt.

De focus ligt op het ontwikkelen van een laagdrempelige, web gebaseerde tool die dit proces ondersteunt en uitbreidt met interactieve en innovatieve functies. Hierbij kan gedacht worden aan zoek- en filtermogelijkheden, visuele structuren zoals treemaps of circle plots. Het project situeert zich binnen de domeinen van secure software engineering en gebruiksvriendelijke toolontwikkeling, met een nadruk op het ondersteunen van softwareontwikkelaars zonder uitgebreide security kennis.

Zo vormt dit onderzoek een schakel tussen de academische methodes rond threat modeling en de praktische noden van ontwikkelaars. Het wil bijdragen aan de vraag naar toegankelijke en bruikbare beveiligingstools die zowel educatief (bv. bij het aanleren van security bewustzijn) als professioneel kunnen worden ingezet.

1. **PROBLEEMSTELLING / ONDERZOEKSVRAAG (MAX. 500 woorden)**

Hoewel threat modeling een essentiële techniek is om softwarebeveiliging te versterken, blijft de drempel hoog. Bestaande methoden zoals STRIDE of CAPEC vergen uitgebreide security-kennis en zijn vaak te technisch en complex voor beginners of ontwikkelaars die zich voornamelijk op functionele software richten. Hierdoor wordt threat modeling snel overgeslagen of slechts oppervlakkig uitgevoerd, met verhoogde veiligheidsrisico’s als gevolg [1].

De Fortunately-Unfortunately Tree-techniek biedt een alternatieve, laagdrempelige manier om risico’s en tegenmaatregelen in kaart te brengen. Deze methode is intuïtiever en minder technisch, maar er bestaat momenteel nog geen volwaardige digitale tool die dit proces optimaal ondersteunt. Een bestaande mindmapping- of diagramsoftware kan wel gebruikt worden, maar sluit onvoldoende aan bij de specifieke noden van threat modeling.

Daarnaast is er weinig onderzoek gedaan naar welke functies en visualisaties het meest bijdragen aan gebruiksvriendelijkheid en effectiviteit binnen dit specifieke kader. Het is dus onduidelijk welke extra features (zoals zoekfuncties, kleurcodering, ranking of een interactieve boomstructuren) effectief helpen om ontwikkelaars zonder uitgebreide security-achtergrond te ondersteunen.

De centrale onderzoeksvraag luidt daarom:

Welke functies en visualisaties maken de Fortunately-Unfortunately Tree het meest gebruiksvriendelijk en nuttig voor threat modeling in softwarebeveiliging?

Deze hoofdvraag kan opgesplitst worden in deelvragen:

1. Welke basisfunctionaliteit is minimaal noodzakelijk om threat modeling met Fortunately-Unfortunately trees te ondersteunen?
2. Welke extra functies (bv. filters, zoekfuncties, statusiconen, visuele structuren) worden door gebruikers als het meest nuttig ervaren?
3. In welke mate verhoogt de toevoeging van educatieve ondersteuning (bv. hints) de bruikbaarheid van de tool?
4. Hoe verhoudt de voorgestelde tool zich qua gebruiksvriendelijkheid en effectiviteit ten opzichte van bestaande generieke mindmap- of diagramsoftware?

Dit probleem vormt de kern van het onderzoeksproject en motiveert de ontwikkeling én evaluatie van een web gebaseerde, intuïtieve tool die threat modeling toegankelijker maakt voor een breed scala aan ontwikkelaars.

1. **DOELSTELLINGEN (MAX. 500 woorden)**

De hoofddoelstelling van dit onderzoeksproject is het ontwerpen, implementeren en evalueren van een webgebaseerde tool die de Fortunately-Unfortunately Tree-techniek ondersteunt, met als doel threat modeling in softwarebeveiliging toegankelijker, gebruiksvriendelijker en effectiever te maken voor ontwikkelaars zonder uitgebreide security achtergrond. Het project wordt als geslaagd beschouwd wanneer de tool zowel intuïtief bevonden wordt als voldoende functionaliteit biedt om realistische scenario’s te modelleren.

Om deze hoofddoelstelling concreet te maken, worden de volgende deeldoelstellingen vooropgesteld:

1. Gebruiksvriendelijkheid

* De tool moet intuïtief bedienbaar zijn, ook door ontwikkelaars zonder voorafgaande ervaring met threat modeling.
* Boomstructuren moeten helder en overzichtelijk weergegeven worden, ook bij grotere of complexere scenario’s.
* De interface moet voldoen aan basisprincipes van human-computer interaction en getest worden op bruikbaarheid.
* De tool moet een feature bieden die helpt bij het eerste gebruik van de tool.

2. Ondersteuning van threat modeling

* De tool moet het mogelijk maken om bedreigingen (“unfortunately”) en tegenmaatregelen (“fortunately”) systematisch in een boomstructuur vast te leggen.
* De tool moet features bieden die helpen bij het beantwoorden van vragen die tijdens threat modeling aan bod kunnen komen.
  + Denk aan:
    - Waar is er nog een groot risico in onze case?
    - Welke beslissing zijn nog niet geïmplementeerd?
    - Hoeveel grote risico’s zijn nog aanwezig?
    - …
* De tool moet uitbreidbaar zijn met educatieve en ondersteunende functies, zoals hints of waarschuwingen.

3. Educatieve en innovatieve functies

* AI-ondersteuning kan onderzocht en geïntegreerd worden om suggesties te geven op basis van bestaande raamwerken, controleren van dubbele fortunates/unfortunates, of om subtrees samen te vatten.

Beperkingen:

* De scope van de tool richt zich primair op gebruiksvriendelijkheid en ondersteuning van het threat modeling-proces, niet op het garanderen van volledige technische beveiliging.
* De implementatie is proof-of-concept: de nadruk ligt op bruikbaarheid en evaluatie, niet op productieklare software.
* Externe factoren zoals integratie met bedrijfsomgevingen of volgen van specifieke regelgeving vallen buiten de scope.

Het probleem wordt dus als opgelost beschouwd wanneer er een werkend prototype van de tool beschikbaar is dat ontworpen is met het doel de bruikbaarheid en toegankelijkheid van threat modeling te verhogen, en waarvan in een gebruikersevaluatie onderzocht wordt of het daadwerkelijk een meerwaarde biedt.

1. **(MATERIAAL EN) METHODE (MAX. 500 woorden)**

Om structuur aan het project te geven bestaat het project uit een aantal werkpakketten (WP’s) om de doelstellingen te behalen, deze geven elke een duidelijke omschrijving van een fase.

**WP1: Literatuurstudie en contextanalyse**

Doel: Een grondige analyse maken van bestaande methodes voor threat modeling en tools die dit ondersteunen.

Activiteiten:

* Bestuderen van security-raamwerken zoals STRIDE, attack trees, ...
* Analyse van bestaande mindmap- en diagramsoftware en hun standaarden en beperkingen voor threat modeling.
* Onderzoek naar visuele representatietechnieken (bv. tree maps, icicle plots, hyperbolic trees) en hun geschiktheid voor boomstructuren.

Materiaal/middelen: Wetenschappelijke artikels, handleidingen, bestaande tools (bv. MindMeister, Kialo, Microsoft Threat Modeling Tool).

Bijdrage: Dit werkpakket zorgt voor een theoretische basis en helpt bij het opstellen van het eisenpakket.

**WP2: Functionele en niet-functionele vereisten opstellen**

Doel: Het opstellen van een gestructureerd eisenpakket voor de te ontwikkelen tool.

Activiteiten:

* Vastleggen van minimumvereisten (bv. toevoegen, bewerken en structureren van nodes).
* Bepalen van gewenste extra functies (filters, zoekfuncties, kleurcodering, statusiconen, AI-ondersteuning).
* Definiëren van bruikbaarheidseisen (responsiviteit, overzichtelijkheid, gebruiksgemak).

Materiaal/middelen: Resultaten uit WP1, overleg met begeleiders en experts.

Bijdrage: Legt de basis voor de ontwikkeling en geeft duidelijke criteria voor evaluatie.

**WP3: Ontwerp en implementatie van de tool**

Doel: Een proof-of-concept webapplicatie ontwikkelen die de Fortunately-Unfortunately Tree ondersteunt.

Activiteiten:

* Ontwerpen van de gebruikersinterface.
* Implementeren van boomstructuren met verschillende visualisatieopties (klassiek, circular tree map).
* Toevoegen van basisfunctionaliteiten zoals toevoegfunctie, editfunctie, mogelijk tot verplaatsen van nodes
* Toevoegen van de gebruiksvriendelijkheid features
* Eventuele uitbreiding met AI-componenten voor suggesties of uitleg.
* Bij voldoende tijd kan een tussentijds gebruikersonderzoek worden ingezet om de ontwerp- en implementatiefase iteratief te herhalen en de implementatie te verbeteren.

Technologieën:

* Het framework React met Next.js.
* Visualisatiebibliotheken zoals D3.js of vis.js voor interactieve boomstructuren.

Bijdrage: Levert een prototype op dat kan worden getest in de gebruikersstudie.

**WP4: Validatie en gebruikersonderzoek**

Doel: Evalueren in welke mate de ontwikkelde tool voldoet aan de vooropgestelde doelstellingen.

Activiteiten:

* Opzetten van een user studie.
* Toewijzen van taken (bv. modelleren van een scenario) en meten van tijd, fouten, en gebruiksgemak.
* Afname van vragenlijsten (bv. SUS-score) en interviews om kwalitatieve feedback te verzamelen.
* Vergelijkende evaluatie met een bestaande mindmaptool.

Materiaal/middelen: De ontwikkelde tool, testscenario’s, enquêtes, interview.

Bijdrage: Geeft empirisch bewijs voor de meerwaarde van de ontwikkelde tool en detecteert verbeterpunten.

**WP5: Analyse en rapportering**

Doel: De resultaten structureren, analyseren en vertalen naar conclusies en aanbevelingen.

Activiteiten:

* Analyseren van kwantitatieve data (tijd, fouten, scores) en kwalitatieve feedback.
* Beantwoorden van de hoofd- en deelonderzoeksvragen.
* Formuleren van aanbevelingen voor verdere ontwikkeling of toepassing.
* Maken van abstract
* Maken van poster
* Opstellen van thesis
* Opmaken van PowerPoint

Materiaal/middelen: analysetools (bv. Python).

Bijdrage: Zorgt voor een onderbouwde eindconclusie en vormt de basis voor de masterproef.

**WP6: Masterthesis**

Doel: Opstellen van alle benodigde documentatie voor de masterproef

Activiteiten:

* Maken van abstract
* Maken van poster
* Opstellen van thesis
* Opmaken van PowerPoint

Materiaal/middelen: Word, PowerPoint

Bijdrage: Beschrijven van het verloop en de resultaten van de masterproef.

1. Afbeelding met tekst, schermopname, nummer, lijn

   Door AI gegenereerde inhoud is mogelijk onjuist.**GANTT-TABEL**

***BRONNENLIJST***

|  |  |
| --- | --- |
| [1] | S. Verreydt, „cybersercurity bites,” 3 Oktober 2024. [Online]. Available: https://cybersecurity-bites.be/cybersecuritybydesign/threat-modeling-in-nederlandse-organisaties/. [Geopend 13 Oktober 2025]. |