



Industriell ekonomi och organisation

Ansökan om examensarbete på Indek

Anmälan mejlas till examensarbete@indek.kth.se

Student/studenter fyller i:

Kurskod och seminariegrupp

Kurskod: ME211X	Önskad seminariegrupp:	Kontaktad/föreslagen handledare (om du har kontaktat någon eller har förslag)
---------------------------	------------------------	---

Kurskoder:

ME210X Examensarbete inom industriell ekonomi. Betygsskala P/F.

För TINEM2-studenter och för TIEMM2-studenter som endast avser ta ut masterexamen.

ME211X Examensarbete inom industriell ekonomi. Betygsskala P/F.

För TINEM2-studenter och för TIEMM2-studenter som avser ta ut både civilingenjörsexamen och masterexamen.

ME200X Examensarbete inom industriell ekonomi. Betygsskala A-F.

TINEM2-studenter och TIEMM2-studenter antagna före H15 kan välja denna kurs som alternativ till ME210X eller ME211X (gäller både studenter som endast avser ta ut masterexamen och studenter som avser ta ut både masterexamen och civilingenjörsexamen).

ME270X Examensarbete inom innovations- och tillväxtekonomi. Betygsskala A-F. För TEINM studenter.

ME271X Examensarbete inom innovations- och tillväxtekonomi. Betygsskala P/F För TEINM studenter.

4D1005 Examensarbete inom industriell ekonomi. Betygsskala P/F.

För dig som är antagen senast 2007-06-30.

Student/Studenter och förslag på examensarbete

Personnummer: 900629-9797	Namn och e-postadress: Nick Nyman, vnyman@kth.se	Program (Master och Civ.ing): CDATE/TINEM
Personnummer:	Namn och e-postadress:	Program (Master och Civ.ing):

Preliminär titel på examensarbetet:

Implementing threat modelling processes for financial microservices

Företag (om bestämt):

Nordea Bank AB

Kontaktperson på företaget samt dennes e-postadress (om bestämt):

Hannes Salin, hannes.salin@nordea.com

Jag/vi ger KTH rätt att publicera min/vår examensarbetsrapport på KTHs webbsidor	JA/NEJ: JA
--	---------------

Ansökningsdatum: 2019-11-29	Termin: VT20	Underskrift student/studenter:
---------------------------------------	------------------------	--------------------------------

Förkunskaper och bidrag:

Min/vår kompetens inom kunskapsområdet (kurser/moment/inriktning):

Mjukvarukonstruktion, DD1392 – Understanding of development processes

Datasäkerhet, DD2395 – Introduction to compSec concepts and considerations

IT management with Enterprise Architecture I & II, EH2770, EH2771 – Familiarity with architectural modelling conventions for interfaces between systems. Industry project surrounding critical evaluation of a framework in development processes.

Project leadership, ME2015 – Familiarity with project management tools and routines

Several projects under the TINEM track focussing on frameworks or models, and their implementation in team routines. Most notably in a large industry project in the CPIM-course ME2502.

Varför valt företag är lämpligt för min/vår utbildning (t ex i förhållande till ingenjörsmässiga aspekter av din utbildning och dess teknikområde):

Nordea Bank develops a lot of software to complement their banking services, as there is high demands on banks to be easily accessible while still maintaining a high level of security. The division at Nordea I'll be writing at develops microservices with APIs for external parties to use in their projects.

På vilket sätt föreslaget examensarbetet bidrar till kunskapsutvecklingen inom huvudområde/teknikområde för din utbildning:

CompSci:

Threat modelling for software development has been around for decades, and there exists several popular frameworks for general development. I'll be focussing on microservices in the financial services industry, which is growing rapidly in demand, to identify what framework is suitable in that environment and whether there are specific needs or considerations with which a framework can be modified to better support microservices-development.

Management:

The current body of research is primarily focussed on the threat modelling tool. I'll be performing a case study evaluating a way of including threat modeling into the development processes to find out how threat modelling can support the developers rather than the other way around. This will result in a detailed implementation proposal aimed towards ensuring acceptance into established processes.

Indeks administration fyller i:***Student 1 uppfyller poängkrav för att antas till examensarbete***

Datum och underskrift behörig administrativ personal

Student 2 uppfyller poängkrav för att antas till examensarbete

Datum och underskrift behörig administrativ personal

Förslaget godkänns som examensarbete

Datum och underskrift studierektor eller examinator

Beskrivning av examensarbetet

Nedan beskrivs det du/ni i dagsläget vet om examensarbetets inriktning (max två sidor).

The thesis will focus on software threat modeling for development of microservices within the financial services sector.

The world of online banking has seen immense change over the last decade, and major financial services providers are seeing customer demands of a plethora of always-available services as well as sudden competition from smaller, more specialized and agile fintech actors. The pressure is on to keep up, and even lead development in a direction which is beneficial for both customers and providers. Enter microservices, a way for major providers to stay in the game and collaborate with other fintech actors on the market by providing APIs for them to use to connect with the services. It's paramount to any financial services that data is kept secure at all times, but with opening up API access comes a whole new collection of security aspects to consider and manage, which is why threat modeling is relevant. Threat modeling is a way to create an overview of potential threats to a system, which in turn gives the possibility to mitigate these threats and to prioritize between them.

Goal/Scope

The goal of the thesis project is to specify a threat modeling method, a framework, that a team of financial microservices developers, with no prior experience of threat modelling, will be able to integrate into their processes and apply to their product. The threat model's scope will be the API endpoints for the microservices, and will thus not be expected to include other areas of threat modeling, such as for example internal threats.

I'll be writing the thesis with supervision from Nordea Bank's financial microservices division. A successful thesis will produce a two-fold deliverable: In the first stage of the thesis project, I aim to propose a prototype threat modeling framework for use with financial microservices, consisting of both a threat modeling method and implementation processes. In the second stage of the project the proposed prototype framework will be evaluated in a case study using one or several development teams at Nordea.

Stage 1

The first stage will include a comprehensive literature study of threat modelling frameworks currently popular in software development as a whole, their strengths and weaknesses, and main areas of use. This stage will also include a mapping of development processes at the case company as a stand-in for "standard" development life-cycle processes, as well as interviews with developers of different experience levels to get a better understanding of the climate for implementing a threat modeling method at the case company.

This literature study is also likely to dip into software development processes, team management strategies, and/or implementation of other frameworks/routines in smaller teams in order to create a basis for implementation proposal.

Following this literature study, and partly parallel to it as well, I aim to develop a prototype threat modeling framework for use in financial microservices development. This will mean prioritizing the most important factors to consider for the development team in making security decisions, and choosing/modifying a framework which supports these factors. Another important aspect in the consideration of framework is of course availability and ease-of-use in the development environment to ensure user compliance and actual acceptance of the method into the already established development life-cycle. This stage will produce a routine specification which can be used by a development team to insert threat modeling routines into their development process.

Part of developing the prototype may be, depending on the chosen framework, either modifying an existing tool or developing a threat modeling tool, either fully usable or an algorithmic concept draft. There will be an interest in including certain important factors, as decided in the mapping of the case company, as parameters in the model which will allow for the tool itself being used to grade or prioritize threats.

Stage 2

Stage 2 will commence once both tool/framework and routine spec. has been produced, as this stage consists of a case study testing the prototype framework on a project at the case company.

The case study will be made on one or more development teams or 5-12 people as natural part of their development lifecycle for a chosen project. The case study will include surveys and interviews before and after implementation, and is likely to include some workshop-element on the threat modelling itself.

The case study will be evaluated partly using the developer input from surveys and interviews as well as with further parameters on efficacy to be decided through dialogue with the case company IT-security division.

Övergripande projektschema

Exjobbet löper uppskattningsvis v 4 – 22?

4 – 8 Literature study

9 – 11 Developing the framework and routine spec.

12 – 13 Collecting surveys, performing pre-interviews, preparing for case study

14 – 16 Perform case study (main part, if several stages of threat-modeling that needs more time between it may expand as needed)

17 – 19 Collecting surveys, performing post-interviews, evaluating case study

20 – 22 Preparing for final delivery, re-writes, review, analysis, and planning presentation & opposition

Assume some overlap, especially during case-study weeks when the actual time conducting case study will not be full-time, and ongoing writing throughout.