

УНИВЕРЗИТЕТ У НОВОМ САДУ
ФАКУЛТЕТА ТЕХНИЧКИХ НАУКА

ОБРАЗАЦ 6.

ИЗВЕШТАЈ О ОЦЕНИ ДОКТОРСКЕ ДИСЕРТАЦИЈЕ

-обавезна садржина- свака рубрика мора бити попуњена

(сви подаци уписују се у одговарајућу рубрику, а назив и место рубрике не могу се мењати или изоставити)

I	ПОДАЦИ О КОМИСИЈИ
I	DATA ABOUT THE JURY
1.	Датум и орган који је именовео комисију The date and the council that has nominated the jury 1.9.2016, Декан Факултета на основу одлуке Наставно-научног већа Факултета техничких наука
2.	Састав комисије са знаком имена и презимена сваког члана, звања, назива уже научне области за коју је изабран у звање, датума избора у звање и назив факултета, установе у којој је члан комисије запослен: Members of the jury: * др Силвиа Гилезан, ред. проф., ФТН, Нови Сад * др Луца Радовани, ванр. проф., Универзитет у Торину * др Мирослав Поповић, ред. проф, ФТН, Нови Сад * др Јелена Иветић, доцент, ФТН, нови Сад * др Mariangiola Dezani, ред. проф, Универзитет у Торину * др Јованка Пантовић, ред. проф, ФТН, Нови Сад
II	ПОДАЦИ О КАНДИДАТУ
II	DATA ABOUT THE CANDIDATE
1.	Име, име једног родитеља, презиме: Name, parent name, surname: Светлана, Светко, Јакшић
2.	Датум рођења, општина, држава: Birth date, place and country: 7.6.1981, Нови Сад, Србија
3.	Назив факултета, назив студијског програма дипломских академских студија – мастер и стечени стручни назив: Master studies: Факултет техничких наука, Математика у техници, дипломирани инжењер примењене математике-мастер
4.	Година уписа на докторске студије и назив студијског програма докторских студија: Doctoral studies, year of enrollment and study programme: 2008, Математика у техници
5.	Назив факултета, назив магистарске тезе, научна област и датум одбране: -----
6.	Научна област из које је стечено академско звање магистра наука: -
III	НАСЛОВ ДОКТОРСКЕ ДИСЕРТАЦИЈЕ:
	Типски системи за контролу меморије и приступа подацима

III PhD THESIS TITLE:

Types for Access and Memory Control

IV ПРЕГЛЕД ДОКТОРСКЕ ДИСЕРТАЦИЈЕ:

Навести кратак садржај са назнаком броја страна, поглавља, слика, шема, графикона и сл.

Докторска дисертација је написана на енглеском језику, на 186 страна. Дисертација је структурирана у 6 поглавља, на следећи начин:

1. Увод
 - 1.1. Публикације и структура тезе
2. Теоријска позадина
 - 2.1. Процесни рачуни
 - 2.1.1. Пи рачун
 - 2.2. Типски системи
3. Типови за безбедан приступ ресурсима
 - 3.1. Динамични подаци на web-у и безбедан приступ
 - 3.1.1. Примери и мотивација
 - 3.2. Формални језик
 - 3.2.1. Синтакса
 - 3.2.2. Приступ подацима и идентификација
 - 3.2.3. Семантике
 - 3.2.4. Мреже са добрим понашањем
 - 3.3. Типски систем
 - 3.3.1. Типови
 - 3.3.2. Типови локација, скриптованих процеса, показивача и стабала података
 - 3.3.3. Типови процеса и мрежа
 - 3.4. Принцип очувања типа
 - 3.5. Закључак и релевантна литература
4. Типови за приватан приступ ресурсима
 - 4.1. Отворени повезани подаци и приватни приступ
 - 4.1.1. Примери и мотивација
 - 4.2. Формални језик
 - 4.2.1. Синтакса
 - 4.2.2. ASK
 - 4.2.3. Операционе семантике
 - 4.2.4. Мреже са добрим понашањем
 - 4.3. Типски систем
 - 1.1.1. Поређење политика
 - 1.1.2. Типови
 - 1.1.3. Типови имена, података и патерна
 - 1.1.4. Типови процеса и локација
 - 4.4. Принцип очувања типа
 - 4.5. Закључак и релевантна литература
5. Типови за контролу меморије
 - 5.1. Комуникација порука без копирања и изузеци
 - 5.1.1. Мотивациони пример
 - 5.2. Формални језик
 - 5.2.1. Синтакса
 - 5.2.2. Операционе семантике
 - 5.2.3. Процеси са добрим понашањем
 - 5.3. Типски систем
 - 5.3.1. Синтакса
 - 5.3.2. Тежина типова
 - 5.3.3. Подтипови
 - 5.3.4. Типови процеса
 - 5.3.5. Типови heap-ова

- 5.3.6. Типови конфигурација
- 5.4. Принцип очувања типа
- 5.5. Закључак и релевантна литература
- 6. Закључак

Одељак Литература и извори података чине 153 референце домаће и стране литературе и материјала преузетих са Интернета. Кључна документација дата на почетку тезе садржи изводе и основне податке о докторској дисертацији на српском и енглеском језику.

PhD THESIS OVERVIEW:

The doctoral dissertation is written in English, on 186 pages. The dissertation is structured into 6 chapters, as follows:

1. Introduction
 - 1.1. Publications and structure of the thesis
2. Background
 - 2.1. Process calculi
 - 2.1.1. Pi-calculus
 - 2.2. Type systems
3. Types for secure access
 - 3.1. Dynamic web data and secure access
 - 3.1.1. Examples and motivation
 - 3.2. Language
 - 3.2.1. Syntax
 - 3.2.2. Data accessibility and identification
 - 3.2.3. Semantics
 - 3.2.4. Well-behaved networks
 - 3.3. Type system
 - 3.3.1. Types
 - 3.3.2. Typing locations, scripts, paths, pointers and data trees
 - 3.3.3. Typing processes and networks
 - 3.4. Type soundness
 - 3.5. Conclusions and related work
4. Types for private access
 - 4.1. Linked data and private access
 - 4.1.1. Examples and motivation
 - 4.2. Language
 - 4.2.1. Syntax
 - 4.2.2. Satisfaction of ask query
 - 4.2.3. Operational semantics
 - 4.2.4. Well-behaved networks
 - 4.3. Type system
 - 4.3.1. Policy comparison
 - 4.3.2. Types
 - 4.3.3. Typing names, data and patterns
 - 4.3.4. Typing processes and networks
 - 4.4. Type soundness
 - 4.5. Conclusions and related work
5. Types for memory control
 - 5.1. Copyless messaging and exceptions
 - 5.1.1. Motivating example
 - 5.2. Language
 - 5.2.1. Syntax
 - 5.2.2. Operational semantics
 - 5.2.3. Well-behaved processes
 - 5.3. Type system
 - 5.3.1. Syntax of types
 - 5.3.2. Type weight

- 5.3.3. Subtyping
- 5.3.4. Typing processes
- 5.3.5. Typing the heap
- 5.3.6. Typing configurations
- 5.4. Type soundness
- 5.5. Conclusion and related work

6. Conclusion

Bibliography consists of 153 reference. Key documentation given at the beginning of the thesis contains copies of the basic data on doctoral dissertation in Serbian and English language.

VI ВРЕДНОВАЊЕ ПОЈЕДИНИХ ДЕЛОВА ДОКТОРСКЕ ДИСЕРТАЦИЈЕ:

НАСЛОВ: Наслов докторске дисертације прецизно одражава предмет спроведених истраживања.

УВОД:

У уводу рада, кандидаткиња даје приказ значаја и актуелности спроведених истраживања. Јасно је дефинисан предмет и циљеви истраживања, у чијем контексту је дат кратак преглед добијених резултата и структуре дисертације.

ТЕОРИЈСКА ОСНОВА:

У овом поглављу, кандидаткиња даје више детаља о формализмима који су коришћени у дисертацији. Наиме, ово поглавље садржи основне појмове процесних рачуна и типских системе, преглед актуелног стања у области, као и синтаксу и семантику Пи-рачуна.

ТИПОВИ ЗА БЕЗБЕДАН ПРИСТУП РЕСУРСИМА:

У овом поглављу, кандидаткиња уводи формални модел за динамичке веб податке, са контролом приступа заснованом на улогама, као и одговарајући типски систем. У уведеном моделу, мрежа је паралелна композиција локација, где свака локација садржи процесе са улогама и стабло података чије гране су означене скуповима улога. Процеси могу да комуницирају, мигрирају са локације на другу локацију, користе податке, а такође и мењају податке или улоге у оквиру локалног стабла. На овај начин, добија се модел који контролише приступ процеса подацима. Предложени типски систем обезбеђује да се постављена политика мреже поштује током израчунавања. Ово поглавље садржи дефиницију особина које прецизније дефинишу безбедност у мрежама са добрим понашањем, типски систем који индукује претходно дефинисане особине и доказ његове коректности.

ТИПОВИ ЗА ПРИВАТАН ПРИСТУП РЕСУРСИМА:

У овом поглављу уведен је формални рачун и типски систем за моделирање приватности података у RDF формату. Уведени рачун представља модел за процесе који остварују интеракцију са подацима у RDF формату. Овакви процеси, заједно са подацима, садржани су у локацијама којима су придружена корисничка имена. Локације са подацима и процесима се компонују паралелно, градећи на тај начин мрежу корисника који међусобно могу да комуницирају. Погодна својства приватности су дефинисана увођењем појма доброг понашања мреже. Типски систем обезбеђује гаранцију приватности података у мрежи, што је последица доказа да се добро типизирана мрежа увек добро понаша.

ТИПОВИ ЗА КОНТРОЛУ МЕМОРИЈЕ:

У овом поглављу уведен је формални рачун и типски систем за моделирање комуникације порука без копирања, који обезбеђује гаранцију одсуства грешака у комуникацији, грешака меморије и цурења меморије у присуству изузетака. То је формализовано формалним рачуном чији терми су процеси који комуницирају и међусобно се усклађују кроз поруке без копирања при комуникацији, са могућношћу активирања изузетака. У том контексту, у којем размена података и експлицитна алокација меморије захтевају контролу политике власништва, посебна пажња се мора посветити активирању изузетака како би се предупредиле грешке у комуникацији (које произилазе из неусаглашених понашања на крајевима канала) и цурења меморије (услед порука заборављених у редовима који одговарају крајевима канала).

ЗАКЉУЧАК:

Ово поглавље укључује закључну дискусију о приказаним резултатима и детаље о актуелним и могућим даљим правцима истраживања.

V EVALUATION OF PARTS OF PhD THESIS:

TITLE: Title of the doctoral dissertation precisely reflects the subject of the conducted research.

INTRODUCTION:

In the introductory part, the candidate gives an overview of the originality and significance of the conducted

research. The subject and objectives are clearly defined, and its importance described in context of the. A brief overview of the structure of the doctoral dissertation is presented in the end of the Introduction.

BACKGROUND:

In this chapter the candidate gives more details on the formalisms used in the thesis. In particular, this chapter contains basic notions of process calculi and type systems, state-of-the-art in the field and the syntax and semantics of the Pi-calculus.

TYPES FOR SECURE ACCESS:

This chapter introduces a calculus for modelling dynamic web data with role-based access control and a corresponding type system. In the presented model, a network is a parallel composition of locations, where each location contains processes with roles and a data tree whose edges are associated with roles. Processes can communicate, migrate from a location to another, use the data, change the data and the roles in the local tree. In this way, a model that controls access of processes to data is obtained. Proposed type system ensures that a specified network policy is respected during computation. The chapter contains definition of desired security properties of well-behaved networks, a type system which enforces these properties and prove of its soundness.

TYPES FOR PRIVATE ACCESS:

This chapter introduces a calculus and a type system for modelling privacy (access control) of RDF data. The introduced calculus presents a core language of processes that interact with data in RDF format. These processes, together with data, are enclosed with user names which are put in parallel, representing a network of users interacting with each other. Desired privacy properties of the network are defined by introduction of a notion of the well-behaved network. Introduced type system guarantees privacy properties by proving that well-typed network is well behaved.

TYPES FOR MEMORY CONTROL:

This chapter introduces a calculus and a type system for copyless messaging that is able to guarantee the absence of communication errors, memory faults, and memory leaks in the presence of exceptions. It formalizes a core language of processes that communicate and synchronize through the copyless message passing paradigm and can throw exceptions. In this context, where the sharing of data and explicit memory allocation require controlled policies on the ownership of heap-allocated objects, special care must be taken when exceptions are thrown to prevent communication errors (arising from misaligned states of channel end-points) and memory leaks (resulting from messages forgotten in end-point queues). Introduced type system guarantees some safety properties, in particular that well-typed processes are free from communication errors and do not leak memory even in presence of (caught) exceptions.

CONCLUSION

This chapter concludes the thesis with the discussion of presented results and some details on the current and further directions of research.

VI СПИСАК НАУЧНИХ И СТРУЧНИХ РАДОВА КОЈИ СУ ОБЈАВЉЕНИ ИЛИ ПРИХВАЋЕНИ ЗА ОБЈАВЉИВАЊЕ НА ОСНОВУ РЕЗУЛТАТА ИСТРАЖИВАЊА У ОКВИРУ РАДА НА ДОКТОРСКОЈ ДИСЕРТАЦИЈИ

VI LIST OF PUBLICATIONS THAT ARE RESULTS OF THE PHD THESIS

Таксативно навести називе радова, где и када су објављени. Прво навести најмање један рад објављен или прихваћен за објављивање у часопису са ISI листе односно са листе министарства надлежног за науку када су у питању друштвено-хуманистичке науке или радове који могу заменити овај услов до 01. јануара 2012. године. У случају радова прихваћених за објављивање, таксативно навести називе радова, где и када ће бити објављени и приложити потврду о томе.

1. Svetlana Jakšić, Luca Padovani: Exception handling for copyless messaging, *Science of Computer Programming* 84: 22-51, 2014. (M23)
2. Svetlana Jakšić, [Luca Padovani](#): Exception handling for copyless messaging, [PPDP 2012](#), 151-162, 2012. (M33)
3. [Mariangiola Dezani-Ciancaglini](#), [Silvia Ghilezan](#), Svetlana Jakšić, [Jovanka Pantović](#): Types for Role-Based Access Control of Dynamic Web Data. *WFLP 2010*: 1-29. (M31)
4. Svetlana Jakšić, Jovanka Pantović, Silvia Ghilezan: Privacy for Linked Data, *Mathematical Structures in Computer Science*, 21 pages. DOI:<http://dx.doi.org/10.1017/S096012951500002X> (M23)

VII ЗАКЉУЧЦИ ОДНОСНО РЕЗУЛТАТИ ИСТРАЖИВАЊА

Дисертација садржи резултате истраживања које можемо сврстати у три уже области истраживања: Формални модели и методе за управљање подацима у XML формату и контролу приступа у дистрибуираним мрежама које конзумирају такве податке, са нагласком на питања безбедности података.

Формални модели и методе за управљање подацима у RDF формату и контролу приступа у дистрибуираним мрежама са таквим подацима, са нагласком на питања приватности.

Формални модели и методе за превенцију меморијских грешака и цурења меморије, као и комуникационих грешака приликом комуникације порука без копирања.

Циљеви тезе су да формализује претходно наведене проблеме, уз коришћење типских система за верификацију одређених особина. Процесни рачуни се базирају на комуникацији, интеракцији и синхронизацији, и као такви представљају одговарајуће формалне моделе за проблеме који се разматрају у овом раду. Употреба типских система је познати статички метод за верификацију разних релевантних особина.

VII CONCLUSIONS AND RESULTS OF THE RESEARCH

The present dissertation considers the following three research problems:

- Formal models and methods for data management and access control in a distributed network with data in XML format, with emphasis put on security issues.
- Formal models and methods for data management and access control in a distributed network with data in RDF format, with emphasis put on privacy issues.
- Formal models and methods for prevention of memory errors and leaks, as well as communication errors in copyless messaging communication paradigm.

The objectives of the thesis were to formalize these problems and use type systems to verify certain properties. Process calculi focus on communication, interaction and synchronization, and as such are appropriate formal models for the problems considered in this thesis. The use of type systems is a prominent static method for verification and enforcement of variety of properties

VIII ОЦЕНА НАЧИНА ПРИКАЗА И ТУМАЧЕЊА РЕЗУЛТАТА ИСТРАЖИВАЊА

Експлицитно навести позитивну или негативну оцену начина приказа и тумачења резултата истраживања.

Комисија оцењује начин приказа и тумачења резултата позитивно. Дисертација је написана прегледно и систематично. Оригинални резултати су јасно и прецизно формулисани, особине су детаљно доказане и дате су одговарајуће илустрације на примерима из примене у рачунарству.

VIII EVALUATION OF THE PRESENTATION AND INTERPRETATION OF THE RESEARCH RESULTS

The dissertation is well organized and clearly written. Original results are clearly and precisely formulated, all the properties are proved in detail, and adequate illustrations from applications in software practices are presented.

IX КОНАЧНА ОЦЕНА ДОКТОРСКЕ ДИСЕРТАЦИЈЕ:

FINAL EVALUATION OF THE DOCTORAL DISSERTATION:

Експлицитно навести да ли дисертација јесте или није написана у складу са наведеним образложењем, као и да ли она садржи или не садржи све битне елементе. Дати јасне, прецизне и концизне одговоре на 3. и 4. питање:

1. Да ли је дисертација написана у складу са образложењем наведеним у пријави теме?

Да, комисија сматра да је дисертација написана у складу са образложењем у пријави теме.

Is the dissertation written entirely in accordance with the reasoning given in the application?

Yes, the dissertation is written in accordance with the reasoning that was set up in the application of the research proposal.

2. Да ли дисертација садржи све битне елементе?

Да, дисертација садржи све битне елементе: прецизно су дефинисани предмет, циљеви и задаци истраживања, детаљно је анализирано стање у области и релевантни резултати, након чега су детаљно описани добијени резултати истраживања, дискусија и закључна разматрања. Списак коришћене литературе указује на темељно проучавање и познавање области истраживања.

Does the dissertation contain all the relevant elements?

Yes, the dissertation contains all the relevant elements: precisely defined subject, objectives and tasks of the research, state-of-the-art, followed by a detailed description of the research results, discussion and concluding remarks. A list of references indicates a fundamental knowledge of the field of research.

3. По чему је дисертација оригиналан допринос науци?

Кандидаткиња поставља и анализира оригиналне моделе, који претходно нису разматрани у научној литератури.

In what way the dissertation provides original scientific contribution?

The candidate sets up and analyzes original models, which have not been previously discussed in the scientific literature.

4. Недостаци дисертације и њихов утицај на резултат истраживања

На основу претходно изнетих мишљења, комисија констатује да докторска дисертација нема недостатака.

The dissertation shortcomings and their impact on research results

Based on the above judgments, the Commission concludes that the doctoral dissertation has no shortcomings.

X ПРЕДЛОГ:

На основу укупне оцене дисертације, комисија предлаже да се докторска дисертација кандидаткиње **Светлане Јакшић** прихвати, а кандидаткињи одобри одбрана.

X EVALUATION RECOMMENDATION:

Based on the overall evaluation of the dissertation, the Commission recommends to accept the doctoral dissertation of the candidate Svetlana Jakšić and to approve its defense.

Нови Сад, 2.9.2016

КОМИСИЈА

др Силвиа Гилезан, редовни професор
Факултет техничких наука, Нови Сад

др Luca Padovani, ванредни професор
Универзитет у Торину, Торино

др Мирослав Поповић, редовни професор
Факултет техничких наука, Нови Сад

др Јелена Иветић, доцент
Факултет техничких наука, Нови Сад

др Mariangiola Dezani, редовни професор
Универзитет у Торину, Торино

др Јованка Пантовић, редовни професор
Факултет техничких наука, Нови Сад