Oznaka poročila: ARRS-RPROJ-ZP-2014/11

ZAKLJUČNO POROČILO RAZISKOVALNEGA PROJEKTA

A. PODATKI O RAZISKOVALNEM PROJEKTU

1.Osnovni podatki o raziskovalnem projektu

Šifra projekta	J2-3635
Naslov projekta	Pristopi za zagotovitev varnosti in zaupanja v novi generaciji P2P omrežij
Vodja projekta	1339 Borka Džonova Jerman B.
Tip projekta	J Temeljni projekt
Obseg raziskovalnih ur	8430
Cenovni razred	B
Trajanje projekta	05.2010 - 04.2013
Nosilna raziskovalna organizacija	106 Institut "Jožef Stefan"
Raziskovalne organizacije - soizvajalke	
Raziskovalno področje po šifrantu ARRS	2 TEHNIKA 2.08 Telekomunikacije
Družbeno-ekonomski cilj	13.02 Tehnološke vede - RiR financiran iz drugih virov (ne iz SUF)
Raziskovalno področje po šifrantu FOS	2 Tehniške in tehnološke vede 2.11 Druge tehniške in tehnološke vede

B. REZULTATI IN DOSEŽKI RAZISKOVALNEGA PROJEKTA

2.Povzetek raziskovalnega projekta[1]

SLO

Nove generacije omrežij vsak-z-vsakim (P2P, Peer-to-Peer) zagotavljajo nižjo ceno platform z napredno interaktivno prednostjo v telekomunikacijskih omrežjih pri posredovanju multimedijskih vsebin. Cilji predlaganega projekta J2-3635 so bili usmerjeni v načrtovanje varnosti in razvoj novih varnostnih rešitev za prihajajoče generacije omrežij P2P.

V projektu je raziskovalna skupina raziskala in razvila različne varnostne storitve in mehanizme, namenjene izboljšavi varnosti v internetnih omrežjih P2P. Poudarek je bil na problemu nadzora dostopa do vsebin v omrežju, vzpostavitvi zaupanja za varno vključevanje

uporabnikov v omrežje in natančnejši določitvi osnovnih varnostnih konceptov bodočega interneta, kot je na primer varnost v odvisnosti od okolja uporabe in na to vezanih storitev.

Med pomembnejšimi rezultati projekta navajamo protokol zaprtega roja (Enhanced Closed Swarm protocol, ECS), ki v omrežjih P2P zagotovi porazdeljen nadzor dostopa do vsebin. Protokol zapolnjuje dolgoletno vrzel v tehnologijah P2P in ponuja rešitev za eno od najbolj občutljivih zahtev glede varnosti v omrežnih sistemov, ki delujejo na tehnologiji P2P. Protokol poveča tudi učinkovitost pri posredovanju multimedijskih vsebin uporabniku, zlasti video podatkov.

Rezultati raziskav, ki izboljšajo zaupanje uporabnikov na podlagi utrjevanja ugleda posameznih ponudnikov vsebin na internetu, so zajeti v dopolnjeni taksonomiji sistemov za upravljanje zaupanja uporabnikov ter rešitvi za njihovo načrtovanje. Učinkovitejši sistemi, ki na podlagi izkušenj in zbranih podatkov samodejno gradijo zaupanje, so izjemno pomembni pri uporabi protokolov P2P in izbiri zaupanja vrednih deležnikov za dostavo vsebin. Poleg tega je bil definiran nov formalni model varnostnega konteksta za bolj fleksibilno delovanje varnostnih rešitev. Model upošteva socialne elemente v internetnih omrežjih in sistemih ter omogoča bistveno poenostavljeno izdelavo varnostne politike konkretnega sistema in njeno implementacijo v kompleksnih okoljih sodobnih telekomunikacijskih omrežij.

Razvite varnostne rešitve so bile evalvirane v eksperimentalnem laboratoriju, vzpostavljenem v sodelovanju z RTV Slovenija, in v okolju svetovnega testnega omrežja PlanetLab.

Rezultati projekta so bili objavljeni v štirih izvirnih znanstvenih člankih s faktorjem vpliva ter predstavljeni na osmih mednarodnih znanstvenih konferencah. Za eno od objav smo prejeli nagrado za najboljši referat na konferenci SecureWare 2011. Razviti protokol ECS je bil predlagan internetni standardizacijski organizaciji Internet Engineering Task Force (IETF) kot standard internetnega pretočnega protokola v okviru tehnologij P2P (Peer to Peer Streaming Protocol, PPSP). Izsledki raziskav so že vključeni v pedagoški proces na Mednarodni podiplomski šoli Jožefa Stefana. V povezavi s projektom sta bili do sedaj dokončani eno magistrsko in eno diplomsko delo, v prvi polovici leta 2014 pa bosta potekala zagovora dveh doktorskih disertacij z rezultati projekta.

ANG

The new generation of PeerToPeer (P2P) protocols and the aligned system solutions provide low cost content distribution platforms and advanced interactive features. The main project 's objective was to develop solutions that would improve the security in the new generation P2P networks and guarantee respective user trust to the P2P based systems. In that context the research carried out provided for the design and implementation of various security services and mechanisms for the desired security features provision. One of those features developed in the project was the solution for content access control in P2P networks, then the next one was aimed towards ensuring trust between the peers in P2P networks. At last the precise definition of the basic security concepts, such as security context acting in different networking environments was defined as a framework for security features provision.

Among the project results is certainly important the Enhanced Closed Swarm protocol (ECS) which enables flexible and distributed access control provision for the peer entities in P2P networks. The protocol fills a decade old gap in the P2P content delivery technologies and provides solution to one of the most exposed professional content providers requirements, i.e. protection of the P2P content delivery from unauthorized usage. The protocol also enables automatic creation of a hierarchical structure of a live streaming swarm for provision of more efficient multimedia content distribution to the users.

Trust and reputation management was studied in the context of the research for acceptable and efficient but not user biased reputation systems. In that context new elements were added to the taxonomy of trust in the online environment and the framework for designing not biased human-centric trust systems was developed. Another result in this area was the conceptual model of a security context that takes into account social elements within the Internet networks and systems and provides a basic framework for specification and implementation of security policies in complex Internet service and network environments.

The developed security solutions were evaluated, assessed and tested in the world known experimental PlanetLab network and in the Living Lab testing laboratory created in cooperation with RTV Slovenia.

The project results have been published in four publications with impact factor and were presented at eight international scientific conferences. On the scientific conference SecureWare 2011 the paper presenting the results of the project was awarded a best paper award. The developed protocol has been submitted to the IETF Peer to Peer Streaming Protocol Working Group (PPSP) for standardization. The results of the project are now part of the study programme at Jozef Stefan International Postgraduate School. One M.Sc. and one diploma theses on the topic of the project were defended for graduation and two Ph.D. theses are ready for defence in first half of 2014.

3.Poročilo o realizaciji predloženega programa dela na raziskovalnem projektu[2]

Aktivnosti v projektu so bile razdeljene v štiri sklope: zahteve uporabnika (DS1), aplikacijske rešitve (DS2), mrežne rešitve (DS3) in evalvacija (DS4). Prvi sklop je zajel uporabniške zahteve in okrepil uporabniško usmerjeni pogled na sistem. V sklopu DS2 so bila obravnavana varnostna vprašanja aplikacije in skladnosti s priporočili standardizacijskih organizacij (IETF), na primer vprašanja glede nadzora dostopa do vsebin v omrežju, ki deluje na podlagi protokola P2P. V tretjem delovnem sklopu so bili obravnavani širši omrežni vidiki, povezani z upravljanjem zaupanja in sistemov ugleda v on-line digitalnem okolju, zadnji pa je bil namenjen razvoju evalvacijskega okolja in oceni doseženih rezultatov.

DS1 - Uporabnik
Uporabnik v novi generaciji omrežij P2P je lahko končni uporabnik, ponudnik vsebine, ponudnik razpršenega oddajanja, oglaševalec, ponudnik omrežnih storitev, razvijalec ali ponudnik razširitev omrežnih vozlišč. Vsaka vrsta uporabnikov ima svoj pogled na sistem in njegovo varnost ter določena pričakovanja glede lastne varnosti, ki jih zagotavljajo varnostne storitve sistema.

Uporabniške zahteve glede zasebnosti in varnosti so bile obravnavane v luči tehnologij in struktur omrežij ter sistemov bodočega interneta, da bi bile prilagojene okolju prihodnje uporabe. Izpostavljeni so bili predvsem nadzor dostopa do posredovalnih kanalov vsebin ter možne težave pri zagotavljanju zanesljivosti prenosa linearnega video signala. Pozornost pri tem je bila namenjena predvsem vidikom v zvezi s poslovno uporabo in ponudniki vsebin. Njihove zahteve glede varnosti pri posredovanju (plačljivih) vsebin so bile natančno preučene, ti rezultati pa pozneje uporabljeni v sklopu DS2 kot izhodišče pri razvoju rešitev.

Ostale zahteve uporabnikov (na primer TV hiš, ki posredujejo vsebine po P2P omrežju) in lastnosti sistemov v povezavi z zagotavljanjem mehanizmov zaupanja in ugleda, ki pomembno vplivajo na zanesljivost delovanja sistema ter izboljšajo uporabnikove izkušnje pri njegovi uporabi, so bile posebej obdelane. Pristopi pri specifikaciji varnostnega konteksta in njegovi obravnavi v kontekstno odvisnih varnostnih sistemih so bili raziskani zaradi kompleksnosti zagotavljanja varnostnih storitev v različnih okoljih sodobnih e-storitev. Na podlagi ugotovljenih pomanjkljivosti je bil izdelan nov model za načrtovanje varnostnih storitev ob upoštevanju uporabnikovega varnostnega konteksta. Model omogoča bistveno poenostavitev priprave, uporabe in izvedbe varnostnih politik v kompleksnih okoljih, kot so na primer nove generacije omrežij P2P.

Rezultati sklopa so bili objavljeni v znanstveni reviji s faktorjem vpliva po SCI in na treh konferencah:
- JOVANOVIKJ, Vladimir, GABRIJELČIČ, Dušan, KLOBUČAR, Tomaž. A Conceptual Model of Security Context. International journal of information security, Springer, ISSN 1615-5262 (v tisku), 2014, 11 strani. [COBISS.SI-ID 27547431]
- AŽDERSKA, Tanja, GABRIJELČIČ, Dušan, JERMAN-BLAŽIČ, Borka. Providing trust and reputation in P2P network. V: ERK 2010, Portorož, Slovenija, str. 139-142. [COBISS.SI-ID 23959079]
- JOVANOVIKJ, Vladimir, GABRIJELČIČ, Dušan, KLOBUČAR, Tomaž. Context modelling in context-aware security systems. V: ERK 2011, Portorož, Slovenija, str. 51-54. [COBISS.SI-ID 25071143]
- JOVANOVIKJ, Vladimir, GABRIJELČIČ, Dušan, KLOBUČAR, Tomaž. Security issues of the future Internet with focus on access control in the content delivery platforms. V: ERK 2010, Portorož, Slovenija, str. 151-154. [COBISS.SI-ID 23959335]

DS2 - Aplikacija
Drugi sklop je pokrival varnostne aspekte, specifične za storitve in aplikacije. Aplikacije so v središču pozornosti arhitektur P2P, saj tečejo na vseh vozliščih omrežja P2P in hkrati igrajo

vlogo odjemalca in strežnika iz klasičnih internetnih omrežij. Glavni poudarek raziskav je bil na nadzoru dostopa do vsebin v omrežju P2P. Glede na preučene zahteve uporabnikov je bil izdelan in implementiran izpopolnjen mehanizem nadzora dostopa, ki s pomočjo prožnih politik nadzora dostopa omogoča vrsto novih aplikacij varnostnega mehanizma. Razviti protokol je bil poimenovan izboljšan protokol zaprtega roja (Enhanced Closed Swarm protocol, ECS). Tekom projekta je bilo osnovni različici protokola dodano več razširitev: (1) poenostavitev overjene vzpostavitve povezave med dvema soležnikoma, (2) določeni so bili natančni parametri ter način kodiranja, s čimer je bila zagotovljena skladnost z nepovezavnimi protokoli iz skladovnice TCP/IP, kot je protokol UDP, (3) razširjene so bile varnostne storitve zaščite komunikacije, primerljive z uveljavljenima protokoloma SSL in DTLS, (4) natančneje so bili definirani kriptografski parameteri protokola in prilagojeni smernicam varnostnih organizacij za naslednje desetletje, ter (5) mehanizmi in elementi vzpostavitve varnega oz. zaprtega roja, kot je certifikat zaprtega roja.

Pri nadzoru dostopa je bila omogočena uporaba kontekstualnih podatkov kot so čas, lokacija, poraba virov, zaupanje v soležnika itd. S tem je bila ponudniku storitev omogočena izvedba vrste aplikacij uporabe vsebine, ki prej v sistemih, zasnovanih na omrežjih protokola P2P, niso bile mogoče. Hkrati je bil protokol zaprtih rojev izboljšan z dodatno zaščito pred napadi s prestrezanjem. Stranski produkt tega načrta in izvedbe je bila zagotovljena možnost avtomatske vzpostavitve hierarhičnega drevesa soležnikov pri posredovanju pretočnega video toka podatkov, kar omogoča učinkovitejše posredovanje pretočnih vsebin uporabniku.

Opravljeno delo je vodilo v pripravo osnutka standarda IETF za standardizacijo v delovni skupini "Peer to Peer Streaming Protocol" (PPSP). Predlog standarda zapolnjuje dolgoletno vrzel glede informacijske varnosti v tehnologijah P2P in tako izpolnjuje eno izmed najbolj občutljivih zahtev sistemov P2P s strani ponudnikov vsebin. Predlog opisuje potrebne varnostne mehanizme za varno deljenje vsebin in mehanizme za upravljanje zaupanja v roju. Mehanizmi omogočajo zaščito komunikacijskih kanalov med soležniki, overjanje soležnikov in nadzor dostopa do vsebin. Pri pripravi osnutka je projektna skupina določila tudi, kako protokol ECS skladno deluje z jedrnim protokolom "Peer-to-Peer Streaming Peer Protocol" (PPSPP). Protokol PPSPP je protokol nove generacije tehnologij P2P, zasnovan tako, da deluje tudi prek nepovezavnega protokola, kot je UDP. Podpira vse predvidene primere uporabe, od pretočnega videa, videa na zahtevo do deljenja datotek. Predlagani osnutek protokola ECS je minimalno prepleten s tem protokolom in prav tako podpira vse predvidene primere uporabe. V osnovi protokol ECS združuje storitve overjanja, celovitosti podatkov, zaupnosti ter nadzora dostopa in tako razširja in poenostavlja obstoječe rešitve, kot je npr. IETF Datagram TLS (DTLS).

Rezultati sklopa so bili objavljeni na treh mednarodnih konferencah in kot predlog internetnega standarda:

- JOVANOVIKJ, Vladimir, GABRIJELČIČ, Dušan, KLOBUČAR, Tomaž. Access control in BitTorrent P2P networks using the enhanced closed swarms protocol. V: Netware 2011, Nice - Saint Laurent du Var, Francija, str. 97-102. [COBISS.SI-ID 24977959]
- JOVANOVIKJ, Vladimir, GABRIJELČIČ, Dušan, KLOBUČAR, Tomaž. Access control in BitTottent P2P networks using the enhanced closed swarms protocol. V: Zbornik prispevkov 3. študentske konference MPŠ Ljubljana, Slovenija, 2011, str. 68-73. [COBISS.SI-ID 24778023]
- BORCH, Njaal, MITCHELL, Keith, GABRIJELČIČ, Dušan. Access control to Bit Torrent swarms using closed swarms. V: AVSTP2P '10: proceedings of the 2010 ACM Workshop on Advanced Video Streaming Techniques for Peer-to-Peer Networks and Social Networking, co-located with ACM Multimedia 2010, Firence Italija, str. 25-30. [COBISS.SI-ID 24358695]
- GABRIJELČIČ, Dušan. Enhanced Closed Swarm protocol, http://tools.ietf.org/html/draft-ppsp-gabrijelcic-ecs-01.

DS3 - Omrežje

Tretji delovni sklop je obravnaval varnostne probleme v omrežju, usmerjen pa je bil predvsem v uporabo zaupanja in ugleda pri zagotavljanju varnostnih storitev. Skupina je glede na zahteve, zbrane v prvem delovnem sklopu, najprej kritično ovrednotila vrsto sistemov za upravljanje zaupanja in ugleda. S pomočjo sistematičnega pristopa in splošne teorije sistemov je opozorila na vrsto pomanjkljivosti v obstoječih sistemih in predlagala možne izboljšave. Na podlagi sistemske teorije so bile določene sistemske lastnosti zaupanja in predlagan nov okvir za načrtovanje sistemov za upravljanje zaupanja. Opredeljene so bile sistemske lastnosti, ki so v obstoječih raziskavah manjkale, ter predlagana vključitev novih dejavnikov, ki so potrebni pri načrtovanju sistemov zaupanja. Štirje ključni dejavniki so bili posebej obdelani, ker je opravljena študija pokazala, da njihovo upoštevanje pri načrtovanju sistemov zaupanja vodi k skladnosti teh sistemov s temeljnimi principi splošnih sistemov, ki jih določa sistemska teorija. Verodostojnost predlagane nove taksonomije sistemov zaupanja in ugleda je bila preverjena s

pomočjo sistemov BarterCast in Yahoo!Answers.

Dodatno so bili obravnavani matematični modeli sistemov upravljanja in zaupanja. V sklopu teh aktivnosti je bil pripravljen simulator upravljanja zaupanja in ugleda in povezan z obstoječim simulatorjem omrežij BitTorrent.

Rezultati sklopa so objavljeni kot izvirna znanstvena članka v reviji s faktorjem vpliva po SCI (kategorija A2) in Springer Lecture Notes (kategorije A4) ter v zbornikih dveh mednarodnih konferenc:

- AŽDERSKA, Tanja, JERMAN-BLAŽIČ, Borka. A holistic approach for designing human-centric trust systems. Systemic practice and action research, ISSN 1573-9295, 2013, vol. 26, no. 5, str. 417-450. [COBISS.SI-ID 21257190]
- AŽDERSKA, Tanja, JERMAN-BLAŽIČ, Borka. A novel systemic taxonomy of trust in the online environment. Lect. notes comput. sci., 2011, vol. 6994, str. 122-133. [COBISS.SI-ID 25130535]
- AŽDERSKA, Tanja, JERMAN-BLAŽIČ, Borka. Developing trust and reputation taxonomy for a dynamic network environment. V: ICONS 2012, Saint Gilles, Reunion Island, str. 109-114. [COBISS.SI-ID 25708583]
- AŽDERSKA, Tanja, JERMAN-BLAŽIČ, Borka. Online trust and reputation: towards socially aware taxonomy of trust. V: 1st UNITE doctoral symposium (ISSN 2247-6040), Bukarešta, 2011, str. 79-85. [COBISS.SI-ID 25399079]

DS4 - Evalvacija
Razvite rešitve so bile preverjene v živem eksperimentalnem laboratoriju, ki smo ga vzpostavili v sodelovanju z RTV Slovenija, in v okolju svetovnega testnega eksperimentalnega omrežja PlanetLab. Pripravljena je bila izvedba platforme P2P za posredovanje vsebine na podlagi izvorne kode projekta P2PNext iz 7. OP EU in razširjena in posodobljena z izvedbo narejenega protokola ECS. Izvedba je bila implementirana v jeziku Python in z uporabo paketa M2Crypto/OpenSSL. Izdelana so bila tudi orodja, ki omogočajo upravljanje poizkusov v eksperimentalnem okolju, merilni mehanizmi in orodja za zbiranje merilnih rezultatov ter njihovo nadaljnjo obdelavo. S tako pripravljeno platformo je bilo opravljenih več preizkusov na rojih do 400 uporabnikov. Pri pripravi metrik delovanja celotne platforme so bili eksperimenti usmerjeni predvsem na tiste, ki omogočajo zaznati spremembe med delovanjem nespremenjene ter varne platforme, kot so indeks povezanosti, čas predpomnenja, zakasnitve signala in indeks deljenja. Rezultati preizkusov so pokazali minimalen časovni vpliv varnostnih mehanizmov na učinkovito delovanje platforme. Za posamezne nabore določenih kriptografskih parametrov v delovnem sklopu DS2 so bili ocenjeni tudi dejanski stroški uporabe varnostnih mehanizmov pri končnem uporabniku in predvidena poraba virov za pametne mobilne naprave.

Razvite tehnologije projekta so bile uporabljene v živo pri prenosu zelo odmevnega dogodka Noč raziskovalcev, ki je bil septembra 2011 organiziran v okviru projekta INSARTY iz 7. OP EU.

4. Ocena stopnje realizacije programa dela na raziskovalnem projektu in zastavljenih raziskovalnih ciljev[3]

Delo v projektu je potekalo v skladu z načrtom dela. Skupina je potrdila znanstveno hipotezo, da je mogoče izboljšati varnost in zanesljivost novih generacij sistemov za posredovanje vsebin na podlagi tehnologij P2P brez zviševanja cene in zmanjševanja učinkovitosti pri končnih uporabnikih. Na podlagi zajema zahtev v okviru delovnega sklopa DS1-Uporabnik so bile v okviru delovnega sklopa DS3-Omrežje predlagane in razvite izboljšave sistema za upravljanje z zaupanjem in ugledom sistemov v omrežju. Na podlagi zahtev DS1 so bili v sklopu DS2-Aplikacija razviti in implementirani mehanizmi, protokoli in vmesniki za varen dostop in posredovanje vsebin v omrežjih P2P. Zahteve sklopa DS1, ki se nanašajo na prilagajanje sistema glede na kontekst uporabnika in njegovo uporabo, so bile obravnavane v sklopih DS1 in DS3. V DS3 je bila v obravnavo konteksta vključena raziskava glede zaupanja in ugleda on-line sistemov, v sklopu DS1 pa so bile podrobno obravnavane varnostne značilnosti konteksta, njegov odnos z drugimi deli sistema ter njegovo uporabo za zagotavljanje varnosti. Delovni sklop DS4–Evalvacija je omogočil raznovrstno evalvacijo več vidikov opravljenih raziskav in implementacij ter objavo rezultatov projekta: z drugimi udeleženci v okviru živega eksperimentalnega laboratorija, v okolju mednarodnega testnega omrežja Planetlab in v lokalnem laboratorijskem okolju. Znanstvena hipoteza projekta je bila potrjena skozi objave v štirih izvirnih znanstvenih člankih s faktorjem vpliva po SCI in na osmih mednarodnih znanstvenih konferencah ter s predlogom tehničnega standarda v IETF.

5.Utemeljitev morebitnih sprememb programa raziskovalnega projekta oziroma sprememb, povečanja ali zmanjšanja sestave projektne skupine[4]

Pri izvedbi projekta ni bilo odstopanj oziroma sprememb glede na zastavljeni program.

6.Najpomembnejši znanstveni rezultati projektne skupine[5]

	Znanstveni dosežek			
1.	COBISS ID		21257190	Vir: COBISS.SI
	Naslov	*SLO*	Holistični pristop k načrtovanju sistemov za upravljanje zaupanja	
		ANG	A holistic approach for designing human-centric trust systems	
	Opis	*SLO*	P2P sistemi oz. omrežja se zelo pogosto uporabljajo pri izmenjavi vsebin v virtualnem svetu. Pri zagotavljanju zaupanja v te sisteme se pričakuje, da so varni in vredni zaupanja, tako kot to velja v tradicionalnem okolju. Vse pogostejši pojavi kriminalnih dejanj na internetu zahtevajo celovitejšo obravnavo varnosti omrežja in sistemov zaupanja. V opravljeni raziskavi so bile določene in obdelane sistemske lastnosti, ki so bile v obstoječi literaturi izpuščene, ter predlagana njihova vključitev v načrtovanje sistemov za upravljanje zaupanja. Nadalje so bili določeni štirje ključni dejavniki pri izgradnji sistema za zaupanje in ugleda. Z raziskavo na podatkih iz omrežja je bilo dokazano. da njihovo upoštevanje pri razvoju teh sistemov vodi k skladnosti s teorijo sistemov.	
		ANG	Online trust systems aim to translate the role that trust has in the traditional world onto the virtual platforms based on the use of network infrastructure built with the modern P2P networks. Establishing the interdependence between these systems and the human factor is essential for reducing the inherent complexity of the open platforms, and for improving the user experience and system performance. They enable building trust and solid on-line reputation systems. This work determines the systemic features of trust and introduces a novel framework of design properties based on the principles of General Systems Theory. The systemic properties that were neglected in the current technical solutions were further studied, enriched with social and human factors into the design guidelines of the on-line trust and reputation systems.	
	Objavljeno v		Kluwer; Systemic practice and action research; 2013; Vol. 26, no. 5; str. 417-450; Impact Factor: 0.559;Srednja vrednost revije / Medium Category Impact Factor: 1.581; Avtorji / Authors: Ažderska Tanja, Jerman-Blažič Borka	
	Tipologija		1.01 Izvirni znanstveni članek	
2.	COBISS ID		26036007	Vir: COBISS.SI
	Naslov	*SLO*	Celostno obravnavanje zaupanja kot lastnosti internetnih sistemov in storitev	
		ANG	Trust as an organismic trait of Internet systems	
	Opis	*SLO*	Vzorci obnašanja, kot rezultat vzajemnega delovanja entitet na internetu, na katerem potekajo poslovni procesi v tki. internetno povezanih oziroma sodelujočih podjetjih, so lahko precej bolj zapleteni kot obnašanje ene same posamične entitete. Iz preprostih pravil zaupanja se pojavljajo novi, bolj zapleteni vzorci, ki včasih delujejo v obratni smeri (tki. »biased systems«). Obravnava teh, zapletenejših vzorcev v sistemih zaupanja v literaturi ni dovolj obdelana. Razlog za to je obravnava sistemov zaupanja na mehanistični način, kot vsota posameznih delov, pri čemer se zanemarja	

			medsebojni vpliv posameznih komponent. V objavljenem prispevku je sistem zaupanja obravnavan kot organizem oziroma celota. Izpostavljena je vloga različnosti, zapletenosti ter odgovornosti ponudnika internetne storitve in obravnavana z vidika uporabnika storitve.	
		ANG	The behaviour patterns resulting from the interactions of many trusting entities in ecommerce systems may be much more complex than the performance of each of the individuals separately; thus, simple rules of trusting behaviour give rise to complex, emergent patterns. A major reason these emergent properties were neither successfully captured nor adequately treated by the current formal models is the global trend of addressing issues related to technical systems in a mechanistic manner considering the system simply as a sum of its components and neglecting the interactions between those components. The work published introduces the concept of an organismic property of human centric ecommerce systems and reveals new areas of applicability of trust as an organismic system trait. The goal of the research presented, is twofold: providing a novel view of treating trust related issues in ecommerce systems, and pointing to the missteps that can be brought by a systemic ignorance of the organismic nature of online trust systems.	
	Objavljeno v		Springer; Multidisciplinary research and practice for informations systems; Lecture notes in computer science; 2012; Vol. 7465; str. 161-175; Avtorji / Authors: Ažderska Tanja, Jerman-Blažič Borka	
	Tipologija		1.01 Izvirni znanstveni članek	
3.	COBISS ID		25130535	Vir: COBISS.SI
	Naslov	*SLO*	Nova taksonomija sistemov za upravljanje zaupanja v internetu	
		ANG	A novel systemic taxonomy of trust in the online environment	
	Opis	*SLO*	V članku je predstavljena nova izboljšana taksonomija sistemov za upravljanje zaupanja v internetu. Razviti in predstavljeni večdimenzionalni okvir omogoča ocenjevanje in primerjavo obstoječih sistemov, iskanje njihovih pomanjkljivosti in lažje načrtovanje novih, boljših in celovitejših sistemov zaupanja. Predstavljeni novi okvir je zasnovan na podlagi principov sistemske teorije. Okvir identificira ključne komponente sistema za upravljanje zaupanja ter odnose med njimi. Pri pripravi je bila upoštevana dinamičnost sistemov zaupanja, časovna komponenta, odvisnost od okolja in usmerjenost v sodelovanje med entitetami. Predstavljeni okvir je bil preverjen na konkretnem primeru mehanizma BarterCast, in sicer na njegovi izvedbi v odjemalcu BitTorrent, znanem pod imenom Tribler. Članek je bil najprej predstavljen kot vabljeno predavanje na konferenci ServiceWave 2011.	
		ANG	Trust and reputation comprise a wide research area in social sciences, but these are also pillars of many social phenomena that shape the Internet socio-economic scene especially in the user oriented services where users are looking for trustable recommendations and opinions. The blossoming of virtual communities, especially when social networks are considered, largely changed the way trust is on-line formed and propagated. The few existing taxonomies provide only initial insights into the ways trust-benefits can be felt; they are neither complete nor elaborated in a systemic manner to provide a proper framework guided by real system-principles. In this paper, we propose a multidimensional framework for guiding the design-process, and assessing the completeness and consistency of reputation systems. The framework developed in the presented study is based on System theory principles; it identifies reputation system components, and more importantly, defines their interrelations. It considers the interaction-centric, dynamic and environment dependent trust-establishment and detects five major factors that guide reputation mechanisms design. The presented framework was applied to BarterCast reputation mechanism	

			deployed in the BitTorrent protocol based client known as Tribler. The published paper based on this study was first presented as an invited paper on the ServiceWave conference in 2011.
	Objavljeno v		Springer; Towards a service-based internet; Lecture notes in computer science; 2011; Vol. 6994; str. 122-133; Avtorji / Authors: Ažderska Tanja, Jerman-Blažič Borka
	Tipologija		1.01 Izvirni znanstveni članek
4.	COBISS ID		27547431 Vir: COBISS.SI
	Naslov	*SLO*	Konceptualni model varnostnega konteksta
		ANG	A conceptual model of security context
	Opis	*SLO*	Kontekstno odvisni sistemi so obetaven pristop k reševanju vrste varnostnih izzivov v modernih internetnih omrežjih in sistemih. Vendar je načrtovanje rešitev v tovrstnih sistemih še vedno zelo zahtevno. Eden izmed pomembnejših razlogov za tako stanje je nedoločenost, kateri del konteksta in kako je dejansko pomemben z varnostnega vidika. V okviru projekta so bili analiziran številni raznorodni primeri uporabe konteksta, od socialno komunikacijskih do primerov posredovanja vsebin. Analiza tako širokega nabora primerov uporabe je omogočila določitev konceptualnega modela varnostnega konteksta, ki bo zagotavljal varnostne rešitve glede na vrsto okolja, v katerem poteka storitev ali deluje sistem v omrežju. Model določi ozek nabor pomembnih konceptov varnostnega kontesta in njihove odnose. Študije so pokazale, da je opredeljeni okvir primeren za vnaprejšno obravnavo ciljnih primerov uporabe z varnostnega stališča ter da zadostuje potrebam, ki so jih izpostavili do sedaj obravnavani pristopi kontekstno odvisne varnosti. Model, ki ga je razvila skupina, omogoča določitev varnostnega konteksta in enostavnejše upravljanje in udejanjenje od konteksta odvisnih varnostnih politik. Predstavljeno delo predstavlja osnovo za varno, kontekstno odvisno posredovanje vsebine v modernih omrežnih sistemih vsak z vsakim.
		ANG	Context-aware security is a promising approach for overcoming many of the security problems in modern Internet networks and systems. Engineering context-aware security solutions for these challenges is difficult, since there is no precise understanding of the notion of context relevant for security. On the other hand such solutions are intended to be used in a number of different situations or use case. Through an analysis of diverse use cases ranging from social group based to content distribution oriented we have defined a conceptual model of security context. The model identifies the important concepts that constitute security context and the relations that exist between them. We show that our model is suitable for analysing target situations in advance from security perspective, as well as for representing the security context that state-of-the-art approaches take into consideration. Our model promises to facilitate the specification of security context and the management of context-aware security policies. The model paves the path for secure context-aware content distribution and consumption as perceived by the project.
	Objavljeno v		Springer; International journal of information security; 2014; 11 str.; Impact Factor: 0.480;Srednja vrednost revije / Medium Category Impact Factor: 1.252; WoS: ET, EW, EX; Avtorji / Authors: Jovanovikj Vladimir, Gabrijelčič Dušan, Klobučar Tomaž
	Tipologija		1.01 Izvirni znanstveni članek
5.	COBISS ID		24977959 Vir: COBISS.SI
	Naslov	*SLO*	Nadzor dostopa v omrežjih P2P na podlagi protokola BitTorrent
		ANG	Access control in BitTorrent P2P networks uisng the enhanced closed swarms protocol

	Opis	*SLO*	V objavi iz leta 2011 je predstavljena izboljšava varnostnega mehanizma za nadzor dostopa Closed Swarm v omrežjih P2P na podlagi internetnega protokola BitTorrent. Izboljšava omogoča večjo fleksibilnost nadzora dostopa ter specifikacijo in izvedbo podrobnejših varnostnih politik.
		ANG	The future content delivery platforms are predicted to be efficient, user-centric, low-cost and participatory systems, with social and collaborative connotation. The peer-to-peer (P2P) architectures, especially ones based on BitTorrent protocol, give a solid basis for provision of such future systems. However, current BitTorrent P2P networks lack flexible access control mechanisms. In the paper enhancements regarding the efficiency of the existing access control mechanism for BitTorrent systems – the Closed Swarms protocol are presented, providing additional flexibility in access control mechanism, enabling fine grained security policies specification and enforcement. The enhancements fulfil a number of content providers' requirements and promise efficient, flexible and secure content delivery in the future content delivery scenarios based on the P2P based protocols.
	Objavljeno v		IARIA; Netware 2011; 2011; Str. 97-102; Avtorji / Authors: Jovanovikj Vladimir, Gabrijelčič Dušan, Klobučar Tomaž
	Tipologija		1.08 Objavljeni znanstveni prispevek na konferenci

7.Najpomembnejši družbeno-ekonomski rezultati projektne skupine[6]

	Družbeno-ekonomski dosežek			
1.	COBISS ID		2701076	Vir: vpis v poročilo
	Naslov	*SLO*	Uredništvo mednarodnih znanstvenih revij	
		ANG	Editorship of international scientific journals	
	Opis	*SLO*	• International journal on advances in internet technology. 2008- • Information systems frontiers. 2013-. [Online ed.]. Nizozemska: Kluwer Online • TheScientificWorldjournal. 2012-. Boynton Beach (FL): Scientific World	
		ANG	• International journal on advances in internet technology. 2008- • Information systems frontiers. 2013-. [Online ed.]. Netherlands: Kluwer Online • TheScientificWorldjournal. 2012-. Boynton Beach (FL): Scientific World	
	Šifra		C.04 Uredništvo mednarodne revije	
	Objavljeno v		Information systems frontiers. Jerman Blažič, Borka (član uredniškega odbora 2013). [Online ed.]. Nizozemska: Kluwer Online, 1999. ISSN 13873326	
	Tipologija		4.00 Sekundarno avtorstvo	
2.	COBISS ID			Vir: vpis v poročilo
	Naslov	*SLO*	Pridobitev novih mednarodnih raziskovalnih projektov	
		ANG	Obtaining new international research projects	
	Opis	*SLO*	Rezultati projekta so pripomogli k pridobitvi novih EU projektov na področju informacijske varnosti. Člani projektne skupine so bili na razpisih 7. OP EU (varnost), CIP (konkurenčnost in inovacije) in ISEC (računalniška kriminaliteta) uspešni s petimi predlogi, od katerih je bil eden (COURAGE) najboljše ocenjen izmed več kot 100 predlogov na razpisu 7. OP EU. Seznam pridobljenih projektov je: • ReDIRNET, 7. OP EU • COURAGE, 7. OP EU • D-FET, ISEC, DG-HOME • STORK 2.0 (CIP)	

			• E-SENS (CIP)
		ANG	Project results helped us to obtain new EU projects in the area of information security. Members of the project team were successful in calls in the EU FP7 (security), CIP (competitiveness and innovation) and ISEC (cybercrime) with five project proposals, one of them (COURAGE) being top-ranked among more than 100 proposals. These are: • ReDIRNET, FP7 SECURITY CALL • COURAGE, FP7. SECURITY CALL • D-FET, ISEC, DG-HOME • STORK 2.0 (CIP) • E-SENS (CIP)
	Šifra		D.01 Vodenje/koordiniranje (mednarodnih in domačih) projektov
	Objavljeno v		Dokumentacija in spletne strani projektov.
	Tipologija		2.14 Projektna dokumentacija (idejni projekt, izvedbeni projekt)
3.	COBISS ID		24977959 Vir: COBISS.SI
	Naslov	*SLO*	Nagrada za najboljši članek na medarodni znanstveni konferenci
		ANG	Best papers award at an international scientific conference
	Opis	*SLO*	Članek, v katerem smo predlagali izboljšavo protokola Closed Swarms za nadzor dostopa v omrežjih P2P, je prejel nagrado za najboljši članek na konferenci SecureWare 2011.
		ANG	The paper on the enhancement of the Closed Swarms protocol that enables access control in P2P networks received the best papers award at the SecureWare 2011 conference.
	Šifra		E.02 Mednarodne nagrade
	Objavljeno v		IARIA; Netware 2011; 2011; Str. 97-102; Avtorji / Authors: Jovanovikj Vladimir, Gabrijelčič Dušan, Klobučar Tomaž
	Tipologija		1.08 Objavljeni znanstveni prispevek na konferenci
4.	COBISS ID		Vir: vpis v poročilo
	Naslov	*SLO*	Razvoj in standardizacija protokola za porazdeljen nadzor dostopa do virov sistema
		ANG	Development and standardization of a protocol for distributed access control
	Opis	*SLO*	V okviru razvojnega projekta je bil razvit prožen in porazdeljen protokol za nadzor dostopa do virov sistema za posredovanje vsebin na podlagi tehnologij vsak z vsakim (peer-to-peer, P2P) in posledično do samih vsebin. Protokol, ki se imenuje Enhanced Closed Swarm (ECS) protocol, je v procesu standardizacije v okviru Internet Engineering Task Force (IETF) v delovni skupini P2P (Peer to Peer Streaming Protocol, PPSP). Predlog standarda zapolnjuje dolgoletno vrzel glede informacijske varnosti v tehnologijah P2P in tako izpolnjuje eno izmed najbolj občutljivih zahtev sistemov P2P s strani ponudnikov vsebin. Predlog opisuje potrebne varnostne mehanizme za varno deljenje vsebin in mehanizme za upravljanje zaupanja v roju. Mehanizmi omogočajo zaščito komunikacijskih kanalov med soležniki, overjanje soležnikov in nadzor dostopa do vsebin. Predlog standarda opiše tudi zahteve in izvedbo združljivosti z jedrnim protokolom delovne skupine PPSP, PeertoPeer Streaming Peer Protocol (PPSPP). Predlog standarda izpolnjuje del varnostnih zahtev delovne skupine PPSP in je pomemben korak k širši uveljaviti predlaganih protokolov skupine predvsem pri komercialnih ponudnikih vsebin. Hkrati predlagani protokol izboljša varnost in zasebnost deljenja vsebin tudi za končne uporabnike.
			In the project a protocol named Enhanced Closed Swam protocol was

		ANG	designed and developed. The protocol provides flexible and distributed access control mechanisms for peer-to-peer systems and protects the content provisioning system resources from unauthorized usage. The protocol has been submitted to the Internet Engineering Task Force (IETF) WG on Peer to Peer Streaming (PPSP). The WG has published the document in the WG charter as draft standard. The submitted document answers most of the PPSP charter security requirements and fills a decade old gap in the P2P content delivery technologies. Besides, as the requirement to protect the P2P content delivery from unauthorized usage was one of the most exposed professional content providers requirement the submitted document answers to the set requirements. The draft describes how to implement the access control security mechanisms like users authentication, distributed access control policies, data origin authentication, integrity and confidentiality services, prevention of security threats like replay attacks, and mechanisms for swarm trust management. The protocol specifies also how to be used with the core Peer to Peer Streaming Peer Protocol (PPSPP).
	Šifra		F.31 Razvoj standardov
	Objavljeno v		http://tools.ietf.org/html/draft-ppsp-gabrijelcic-ecs-01
	Tipologija		3.25 Druga izvedena dela

8.Drugi pomembni rezultati projetne skupine[7]

Članstvo v ICT Standardisation Board of EU, programskem odboru 7. OP EU za področje varnosti, odboru ekspertov nagrade World Summit Award for Information Society of United Nations, v svetovalnem odboru za Varne družbe Obzorja 2020, Svetu za elektronske komunikacije Republike Slovenije ter v svetovalnem odboru za IKT EU programa COST.

Izsledki raziskav so že bili vključeni v pedagoški proces na Mednarodni podiplomski šoli Jožefa Stefana. V povezavi s projektom sta bili do sedaj dokončani eno magistrsko in eno diplomsko delo, v prvi polovici leta 2014 pa pričakujemo še zagovora dveh doktorskih disertacij.

9.Pomen raziskovalnih rezultatov projektne skupine[8]

9.1.Pomen za razvoj znanosti[9]

SLO

Varnost in zasebnost sta ključni zahtevi sodobnih informacijskih in komunikacijskih sistemov, tudi nove generacije omrežij P2P. Zagotavljanje varnosti in zasebnosti je v takšnih omrežjih še težje zaradi porazdeljene in decentralizirane narave sistemov.

Glavni cilj pričujočega projekta je bil zagotoviti varnostne storitve in rešitve za naslednjo generacijo omrežij P2P. Projekt je zapolnil več vrzeli na tem znanstvenem področju in prispeval k večji varnosti v takšnih omrežjih. Razviti izboljšani protokol zaprtega roja (Enhanced Closed Swarm Protocol) podaja rešitev za enega najpomembnejših problemov komercialnih ponudnikov vsebine, to je, kako zaščititi vsebino v omrežjih P2P pred nepooblaščeno uporabo. Razširitve protokola dajejo dodatno prožnost mehanizmom za nadzor dostopa in omogočajo specifikacijo in udejanjenje finejših varnostnih politik. Z njimi lahko zagotovimo učinkovito in prilagodljivo razdeljevanje vsebine v raznovrstnih primerih uporabe v omrežju, ki deluje z internetnim protokolom P2P.

Nadalje smo določili sistemske lastnosti zaupanja in pripravili nov okvir za načrtovanje sistemov za upravljanje zaupanja. Prvi smo uporabili osnovne znanstvene principe družbenih ved in splošne teorije sistemov za gradnjo in evalvacijo v uporabnika usmerjenih tehničnih rešitev. Razviti večdimenzionalni okvir bodo lahko raziskovalci in razvijalci uporabili kot orodje pri načrtovanju sistemov za upravljanje zaupanja in ugleda ter pri preverjanju popolnosti in

konsistentnosti razvitih sistemov zaupanja in ugleda v omrežju.

Nov konceptualni model varnostnega konteksta določa za varnost pomembne elemente konteksta na različnih ravneh abstrakcije. Model je uporaben za številne oblike družabnih internetnih sistemov, ne le za omrežja P2P. Natančno in obširno opiše varnostni kontekst in omogoča pripravo varnostnih politik in kontekstno odvisnih varnostnih sistemov, s pomočjo katerih lahko prilagajamo varnostne storitve in mehanizme spremembam konteksta. Pričakujemo, da bo predlagana rešitev olajšala specifikacijo, upravljanje in ponovno uporabo varnostnih politik za najrazličnejše vrste družabnih internetnih sistemov.

ANG

Security and privacy are crucial elements of modern information and communication systems, such as new generations of P2P networks and the new e-services being developed under the EU Directive for e-services recently adopted by EU Parliament. Security and privacy provisioning is much harder in complex networks due to distributed and decentralized nature of the network systems.

The project's primary objective was security services and solutions provisioning in new generation P2P networks. The project has filled several scientific gaps in this area and improved security provision in the networks. The developed Enhanced Closed Swarm Protocol (ECS) answered to one of the most important professional content providers' requirements, i.e. how to protect the P2P content delivery from unauthorized usage. The protocol enhancements provide additional flexibility in the access control mechanism, enabling fine grained security policies specification and enforcement. Moreover, they enable efficient and flexible content delivery in various scenarios.

In the area of trust and reputation management, the systemic features of on-line trust were determined and a framework of design properties based on the principles of general systems theory was introduced. This work represents the first attempt of fundamental social science principles from general systems theory to be applied on pure technical on-line solutions. The created multidimensional framework is intended to guide the researchers and developers in the design-process of on-line trust and reputations systems, and to help them assessing their completeness and consistency.

On the other hand, the novel conceptual model of security context defines higher level security context abstractions that are meaningful for security relevant decisions in diverse use cases of many internet social network based systems, not just in P2P networks. The model clarifies and complements the notion of security context and enables specification of security policies that will guide security relevant system adaptation upon context changes. The developed approach will facilitate specification, management and reuse of security policies for various types of internet networks and systems.

9.2. Pomen za razvoj Slovenije[10]

SLO

Internet vsebin in znanja je eden od glavnih smernic razvoja bodočega interneta. Pričakuje se, da se količina digitalnih vsebin v bližnji prihodnosti ne bo povečala zgolj v številkah, ampak tudi po velikosti, predvsem zaradi povečanja resolucije, enostavnosti ustvarjanja ter prirejanja in rasti števila uporabnikov in naprav, ki služijo njihovim potrebam. Naslednja generacija omrežij P2P obljublja, da bo postala najpomembnejša tehnologija za posredovanje digitalnih vsebin. Tako proste kot komercialne vsebine bodo dostopne prek tega okolja, ki temelji tudi na uporabnikovih osebnih podatkih za podporo osebno prilagojenim storitvam. Zato je zagotovitev varnosti in zasebnosti izjemnega pomena.

Rezultati projekta povečujejo raven varnosti infrastrukture za posredovanje vsebin, ki temelji na naslednji generaciji omrežij, zasnovanih na protokolih P2P. Od rezultatov imajo lahko koristi različni slovenski akterji v vrednostni verigi medijske distribucije:
• Lastniki in ponudniki vsebin lahko razširijo svoje trge in imajo več dobička.
• Za ponudnike linearnih televizijskih vsebin lahko varno omrežje P2P predstavlja še eno možnost za distribucijo lastnih programov in vsebin.

• Ponudniki omrežja lahko zmanjšajo celotno obremenitev v omrežju.
• Strokovnjaki za varnost in razvijalci sistemov bodo imeli koristi od razvitih posplošenih mehanizmov za zagotavljanje zaupanja in ugleda in ostalih varnostnih mehanizmov.
• Končni uporabniki lahko varneje sodelujejo pri izmenjavi vsebin.

Rezultati projekta so bili vpeljani tudi v slovenski visokošolski prostor skozi programe podiplomskega in dodiplomskega izobraževanja na Mednarodni podiplomski šoli Jožefa Stefana, kjer poučujejo člani projektne skupine. V okviru projekta so bile opravljene raziskave za dve doktorski disertaciji, katerih zagovor pričakujemo v prvi polovici leta 2014, in zaključeni magistrsko in diplomsko nalogo. Rezultati so pripomogli k uspešnejšemu nastopu članov projektne skupine na razpisih EU na področju informacijske varnosti, s čimer Slovenija še naprej ohranja stik z evropskimi in svetovnimi varnostnimi raziskavami, ki so ključne za delovanje informacijske družbe.

Ne nazadnje je treba omeniti še pred kratkim objavljeno strategijo EU v okviru Evropske digitalne agende, kjer je platforma NIS (Network and Information Security) v direktivi o omrežni in storitveni varnosti definirana kot najbolj pomembno področje razvoja enotnega digitalnega trga v EU v naslednjih štirih letih.

ANG

Internet of content and knowledge is one of the main vectors of growth of the Future Internet. It is expected that digital content will not only increase in number in the near future, but also in size, due to increases in resolution, the ease of creation and manipulation, and growth of the number of users and devices supporting the users' needs. Next generation P2P networks hold the promise to become the most important digital content distribution technology. Both free and commercial content will be delivered via this environment that will also be based on users' personal data in order to support personalized services. This is why security and privacy are so important in those networks.

The project results increase security level of a content distribution infrastructure based on the next generation of P2P networks. Various actors of the media distribution value chain in Slovenia can benefit from them:
• Content owners and providers can enlarge their markets and can make more profits.
• For broadcasters, a secure P2P network can represent yet another outlet for distributing their programmes and contents.
• Network providers can benefit as the overall network load is reduced.
• Security experts and system developers will benefit from the developed generalized trust and reputation mechanisms and other security mechanisms.
• End users will more securely participate in the content distribution.

The project results have been introduced into Slovenian Higher Education system through undergraduate and graduate programmes of the Jozef Stefan International Postgraduate School where members of the project team are teaching. So far, research activities for two doctoral theses, which will be defended in the first half of 2014, one M.Sc. thesis and one diploma thesis have been conducted. The results have also contributed to more successful participation of the project team members at the EU calls in the field of information security. Newly obtained research projects will ensure that Slovenia stays in touch with the latest European security research activities, which are crucial for the Information society.

It should be mentioned here the recent Directive on Network and Information Security (NIS) adopted by the EU Parliament that focuses on the NIS platform as the basic strategy for the next four years of development of the single digital market in EU.

10. Samo za aplikativne projekte in podoktorske projekte iz gospodarstva!
Označite, katerega od navedenih ciljev ste si zastavili pri projektu, katere konkretne rezultate ste dosegli in v kakšni meri so doseženi rezultati uporabljeni

Cilj		
F.01	**Pridobitev novih praktičnih znanj, informacij in veščin**	
	Zastavljen cilj	◯ DA ◯ NE

	Rezultat	
	Uporaba rezultatov	
F.02	**Pridobitev novih znanstvenih spoznanj**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	
F.03	**Večja usposobljenost raziskovalno-razvojnega osebja**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	
F.04	**Dvig tehnološke ravni**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	
F.05	**Sposobnost za začetek novega tehnološkega razvoja**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	
F.06	**Razvoj novega izdelka**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	
F.07	**Izboljšanje obstoječega izdelka**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	
F.08	**Razvoj in izdelava prototipa**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	
F.09	**Razvoj novega tehnološkega procesa oz. tehnologije**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	
F.10	**Izboljšanje obstoječega tehnološkega procesa oz. tehnologije**	

	Zastavljen cilj	◯ DA ◯ NE
	Rezultat	
	Uporaba rezultatov	
F.11	**Razvoj nove storitve**	
	Zastavljen cilj	◯ DA ◯ NE
	Rezultat	
	Uporaba rezultatov	
F.12	**Izboljšanje obstoječe storitve**	
	Zastavljen cilj	◯ DA ◯ NE
	Rezultat	
	Uporaba rezultatov	
F.13	**Razvoj novih proizvodnih metod in instrumentov oz. proizvodnih procesov**	
	Zastavljen cilj	◯ DA ◯ NE
	Rezultat	
	Uporaba rezultatov	
F.14	**Izboljšanje obstoječih proizvodnih metod in instrumentov oz. proizvodnih procesov**	
	Zastavljen cilj	◯ DA ◯ NE
	Rezultat	
	Uporaba rezultatov	
F.15	**Razvoj novega informacijskega sistema/podatkovnih baz**	
	Zastavljen cilj	◯ DA ◯ NE
	Rezultat	
	Uporaba rezultatov	
F.16	**Izboljšanje obstoječega informacijskega sistema/podatkovnih baz**	
	Zastavljen cilj	◯ DA ◯ NE
	Rezultat	
	Uporaba rezultatov	
F.17	**Prenos obstoječih tehnologij, znanj, metod in postopkov v prakso**	
	Zastavljen cilj	◯ DA ◯ NE
	Rezultat	
	Uporaba rezultatov	
F.18	**Posredovanje novih znanj neposrednim uporabnikom (seminarji, forumi, konference)**	
	Zastavljen cilj	◯ DA ◯ NE
	Rezultat	

	Uporaba rezultatov	
F.19	**Znanje, ki vodi k ustanovitvi novega podjetja ("spin off")**	
	Zastavljen cilj	◯ DA ◯ NE
	Rezultat	
	Uporaba rezultatov	
F.20	**Ustanovitev novega podjetja ("spin off")**	
	Zastavljen cilj	◯ DA ◯ NE
	Rezultat	
	Uporaba rezultatov	
F.21	**Razvoj novih zdravstvenih/diagnostičnih metod/postopkov**	
	Zastavljen cilj	◯ DA ◯ NE
	Rezultat	
	Uporaba rezultatov	
F.22	**Izboljšanje obstoječih zdravstvenih/diagnostičnih metod/postopkov**	
	Zastavljen cilj	◯ DA ◯ NE
	Rezultat	
	Uporaba rezultatov	
F.23	**Razvoj novih sistemskih, normativnih, programskih in metodoloških rešitev**	
	Zastavljen cilj	◯ DA ◯ NE
	Rezultat	
	Uporaba rezultatov	
F.24	**Izboljšanje obstoječih sistemskih, normativnih, programskih in metodoloških rešitev**	
	Zastavljen cilj	◯ DA ◯ NE
	Rezultat	
	Uporaba rezultatov	
F.25	**Razvoj novih organizacijskih in upravljavskih rešitev**	
	Zastavljen cilj	◯ DA ◯ NE
	Rezultat	
	Uporaba rezultatov	
F.26	**Izboljšanje obstoječih organizacijskih in upravljavskih rešitev**	
	Zastavljen cilj	◯ DA ◯ NE
	Rezultat	
	Uporaba rezultatov	
F.27	**Prispevek k ohranjanju/varovanje naravne in kulturne dediščine**	
	Zastavljen cilj	◯ DA ◯ NE

	Rezultat	
	Uporaba rezultatov	
F.28	**Priprava/organizacija razstave**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	
F.29	**Prispevek k razvoju nacionalne kulturne identitete**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	
F.30	**Strokovna ocena stanja**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	
F.31	**Razvoj standardov**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	
F.32	**Mednarodni patent**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	
F.33	**Patent v Sloveniji**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	
F.34	**Svetovalna dejavnost**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	
F.35	**Drugo**	
	Zastavljen cilj	DA NE
	Rezultat	
	Uporaba rezultatov	

Komentar

11. Samo za aplikativne projekte in podoktorske projekte iz gospodarstva!
Označite potencialne vplive oziroma učinke vaših rezultatov na navedena področja

	Vpliv	Ni vpliva	Majhen vpliv	Srednji vpliv	Velik vpliv	
G.01	**Razvoj visokošolskega izobraževanja**					
G.01.01.	Razvoj dodiplomskega izobraževanja	○	○	○	○	
G.01.02.	Razvoj podiplomskega izobraževanja	○	○	○	○	
G.01.03.	Drugo:	○	○	○	○	
G.02	**Gospodarski razvoj**					
G.02.01	Razširitev ponudbe novih izdelkov/storitev na trgu	○	○	○	○	
G.02.02.	Širitev obstoječih trgov	○	○	○	○	
G.02.03.	Znižanje stroškov proizvodnje	○	○	○	○	
G.02.04.	Zmanjšanje porabe materialov in energije	○	○	○	○	
G.02.05.	Razširitev področja dejavnosti	○	○	○	○	
G.02.06.	Večja konkurenčna sposobnost	○	○	○	○	
G.02.07.	Večji delež izvoza	○	○	○	○	
G.02.08.	Povečanje dobička	○	○	○	○	
G.02.09.	Nova delovna mesta	○	○	○	○	
G.02.10.	Dvig izobrazbene strukture zaposlenih	○	○	○	○	
G.02.11.	Nov investicijski zagon	○	○	○	○	
G.02.12.	Drugo:	○	○	○	○	
G.03	**Tehnološki razvoj**					
G.03.01.	Tehnološka razširitev/posodobitev dejavnosti	○	○	○	○	
G.03.02.	Tehnološko prestrukturiranje dejavnosti	○	○	○	○	
G.03.03.	Uvajanje novih tehnologij	○	○	○	○	
G.03.04.	Drugo:	○	○	○	○	
G.04	**Družbeni razvoj**					
G.04.01	Dvig kvalitete življenja	○	○	○	○	
G.04.02.	Izboljšanje vodenja in upravljanja	○	○	○	○	
G.04.03.	Izboljšanje delovanja administracije in javne uprave	○	○	○	○	
G.04.04.	Razvoj socialnih dejavnosti	○	○	○	○	
G.04.05.	Razvoj civilne družbe	○	○	○	○	
G.04.06.	Drugo:	○	○	○	○	
G.05.	**Ohranjanje in razvoj nacionalne naravne in kulturne dediščine in**	○	○	○	○	

	identitete					
G.06.	**Varovanje okolja in trajnostni razvoj**	○	○	○	○	
G.07	**Razvoj družbene infrastrukture**					
G.07.01.	Informacijsko-komunikacijska infrastruktura	○	○	○	○	
G.07.02.	Prometna infrastruktura	○	○	○	○	
G.07.03.	Energetska infrastruktura	○	○	○	○	
G.07.04.	Drugo:	○	○	○	○	
G.08.	**Varovanje zdravja in razvoj zdravstvenega varstva**	○	○	○	○	
G.09.	**Drugo:**	○	○	○	○	

Komentar

12.Pomen raziskovanja za sofinancerje[11]

	Sofinancer			
1.	Naziv			
	Naslov			
	Vrednost sofinanciranja za celotno obdobje trajanja projekta je znašala:			EUR
	Odstotek od utemeljenih stroškov projekta:			%
	Najpomembnejši rezultati raziskovanja za sofinancerja			Šifra
		1.		
		2.		
		3.		
		4.		
		5.		
	Komentar			
	Ocena			

13.Izjemni dosežek v letu 2013[12]

13.1. Izjemni znanstveni dosežek

Kontekstno odvisni sistemi so obetaven pristop k reševanju vrste varnostnih izzivov v modernih internetnih omrežjih in sistemih. Eden od pomembnejših razlogov za zahtevnost načrtovanja rešitev v tovrstnih sistemih je nedoločenost, kateri del konteksta in kako je dejansko pomemben z varnostnega vidika. V okviru projekta smo analizirali vrsto raznorodnih primerov uporabe konteksta, od socialno komunikacijskih do posredovanja vsebin. Analiza širokega nabora primerov nam je omogočila določiti konceptualni model varnostnega konteksta. Pokazali smo, da je model primeren za obravnavo ciljnih primerov uporabe z varnostnega stališča ter da zadosti potrebam, ki so jih izpostavili do sedaj obravnavani pristopi kontekstno odvisne varnosti. Model omogoča določitev varnostnega konteksta in enostavnejše upravljanje in udejanjenje od konteksta odvisnih varnostnih politik. Predstavljeno delo predstavlja osnovo za varno, kontekstno odvisno posredovanje vsebine v modernih sistemih “vsak z vsakim”.

13.2. Izjemni družbeno-ekonomski dosežek

C. IZJAVE

Podpisani izjavljam/o, da:

- so vsi podatki, ki jih navajamo v poročilu, resnični in točni
- se strinjamo z obdelavo podatkov v skladu z zakonodajo o varstvu osebnih podatkov za potrebe ocenjevanja ter obdelavo teh podatkov za evidence ARRS
- so vsi podatki v obrazcu v elektronski obliki identični podatkom v obrazcu v pisni obliki
- so z vsebino zaključnega poročila seznanjeni in se strinjajo vsi soizvajalci projekta

Podpisi:

zastopnik oz. pooblaščena oseba raziskovalne organizacije:	in	*vodja raziskovalnega projekta:*
Institut "Jožef Stefan"		Borka Džonova Jerman B.

ŽIG

Kraj in datum: Ljubljana 14.4.2014

Oznaka prijave: ARRS-RPROJ-ZP-2014/11

---

[1] Napišite povzetek raziskovalnega projekta (največ 3.000 znakov v slovenskem in angleškem jeziku) Nazaj

[2] Napišite kratko vsebinsko poročilo, kjer boste predstavili raziskovalno hipotezo in opis raziskovanja. Navedite ključne ugotovitve, znanstvena spoznanja, rezultate in učinke raziskovalnega projekta in njihovo uporabo ter sodelovanje s tujimi partnerji. Največ 12.000 znakov vključno s presledki (približno dve strani, velikost pisave 11). Nazaj

[3] Realizacija raziskovalne hipoteze. Največ 3.000 znakov vključno s presledki (približno pol strani, velikost pisave 11) Nazaj

[4] V primeru bistvenih odstopanj in sprememb od predvidenega programa raziskovalnega projekta, kot je bil zapisan v predlogu raziskovalnega projekta oziroma v primeru sprememb, povečanja ali zmanjšanja sestave projektne skupine v zadnjem letu izvajanja projekta, napišite obrazložitev. V primeru, da sprememb ni bilo, to navedite. Največ 6.000 znakov vključno s presledki (približno ena stran, velikost pisave 11). Nazaj

[5] Navedite znanstvene dosežke, ki so nastali v okviru tega projekta. Raziskovalni dosežek iz obdobja izvajanja projekta (do oddaje zaključnega poročila) vpišete tako, da izpolnite COBISS kodo dosežka – sistem nato sam izpolni naslov objave, naziv, IF in srednjo vrednost revije, naziv FOS področja ter podatek, ali je dosežek uvrščen v A'' ali A'. Nazaj

[6] Navedite družbeno-ekonomske dosežke, ki so nastali v okviru tega projekta. Družbeno-ekonomski rezultat iz obdobja izvajanja projekta (do oddaje zaključnega poročila) vpišete tako, da izpolnite COBISS kodo dosežka – sistem nato sam izpolni naslov objave, naziv, IF in srednjo vrednost revije, naziv FOS področja ter podatek, ali je dosežek uvrščen v A'' ali A'.

Družbeno-ekonomski dosežek je po svoji strukturi drugačen kot znanstveni dosežek. Povzetek znanstvenega dosežka je praviloma povzetek bibliografske enote (članka, knjige), v kateri je dosežek objavljen.

Povzetek družbeno-ekonomskega dosežka praviloma ni povzetek bibliografske enote, ki ta dosežek dokumentira, ker je dosežek sklop več rezultatov raziskovanja, ki je lahko dokumentiran v različnih bibliografskih enotah. COBISS ID zato ni enoznačen, izjemoma pa ga lahko tudi ni (npr. prehod mlajših sodelavcev v gospodarstvo na pomembnih raziskovalnih nalogah, ali ustanovitev podjetja kot rezultat projekta … - v obeh primerih ni COBISS ID). Nazaj

[7] Navedite rezultate raziskovalnega projekta iz obdobja izvajanja projekta (do oddaje zaključnega poročila) v primeru, da katerega od rezultatov ni mogoče navesti v točkah 6 in 7 (npr. ni voden v sistemu COBISS). Največ 2.000 znakov, vključno s presledki. Nazaj

[8] Pomen raziskovalnih rezultatov za razvoj znanosti in za razvoj Slovenije bo objavljen na spletni strani:

http://sicris.izum.si/ za posamezen projekt, ki je predmet poročanja Nazaj

[9] Največ 4.000 znakov, vključno s presledki Nazaj

[10] Največ 4.000 znakov, vključno s presledki Nazaj

[11] Rubrike izpolnite / prepišite skladno z obrazcem "izjava sofinancerja" http://www.arrs.gov.si/sl/progproj/rproj/gradivo/, ki ga mora izpolniti sofinancer. Podpisan obrazec "Izjava sofinancerja" pridobi in hrani nosilna raziskovalna organizacija – izvajalka projekta. Nazaj

[12] Navedite en izjemni znanstveni dosežek in/ali en izjemni družbeno-ekonomski dosežek raziskovalnega projekta v letu 2013 (največ 1000 znakov, vključno s presledki). Za dosežek pripravite diapozitiv, ki vsebuje sliko ali drugo slikovno gradivo v zvezi z izjemnim dosežkom (velikost pisave najmanj 16, približno pol strani) in opis izjemnega dosežka (velikost pisave 12, približno pol strani). Diapozitiv/-a priložite kot priponko/-i k temu poročilu. Vzorec diapozitiva je objavljen na spletni strani ARRS http://www.arrs.gov.si/sl/gradivo/, predstavitve dosežkov za pretekla leta pa so objavljena na spletni strani http://www.arrs.gov.si/sl/analize/dosez/. Nazaj

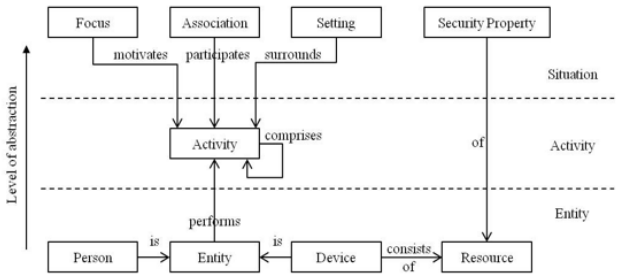
Obrazec: ARRS-RPROJ-ZP/2014 v1.03
5F-20-98-7C-4A-B6-3A-AC-8B-D0-6F-64-3B-F3-0A-DD-80-F4-D0-4D

Priloga 1

VEDA: TEHNIKA
Področje: 2.08 Telekomunikacije

Znanstveni dosežek: Konceptualni model varnostnega konteksta

Vir: JOVANOVIKJ, Vladimir, GABRIJELČIČ, Dušan, KLOBUČAR, Tomaž. A Conceptual Model of Security Context. International journal of information security, Springer, ISSN 1615-5262 (v tisku) 11 strani. [COBISS.SI-ID 27547431]



Konceptualni model varnostnega konteksta

Ref.	Name	Context										Adaptable Behaviour
		Entity			Activity		Social			Property		
		Person	Device	Resource	Simple	Complex	Focus	Assoc	Setting	SP	OP	
[16]	Env. roles	✓	✓	✓	✓							AC
[3]	Cerberus	✓	✓		✓	✓				✓		A, AC
[34]	Shrink-wrap. sec.			✓	✓					✓		AC
[59]	Proteus	✓		✓	✓	✓						AC
[27]	Mob. Soc. ecosys.	✓		✓	✓			✓				AC
[46]	Progressive auth.	✓	✓	✓	✓					✓	✓	A
[22]	Smart Space Arc.	✓	✓	✓	✓		✓	✓	✓	✓		Sev.Serv.
[54]	Serenity	✓	✓	✓	✓	✓				✓		Sev.Serv.
[36]	Adapt. PKI			✓	✓					✓		SC
[6]	CASec for NGN	✓	✓	✓	✓							SC
[48]	Adapt. protocols		✓	✓	✓					✓	✓	SC
[37]	CA-RBAC		✓	✓	✓			✓				AC
[4]	ConUCON	✓	✓	✓	✓							AC
[56]	Daidalos	✓	✓		✓	✓		✓				IM
[24]	Persist	✓	✓		✓	✓		✓		✓		IM
[2]	CRAAC		✓	✓	✓							AC
[17]	OrBAC	✓	✓	✓	✓	✓	✓					AC
[25]	Auth. Confidence	✓			✓					✓		A
[31]	CS Adapt. Auth.		✓	✓	✓					✓		A
[51]	Auto. Sec. FW	✓	✓	✓	✓	✓				✓	✓	A, AC, SC
[41]	CoDiS	✓	✓	✓	✓							Sev.Serv.
[23]	Data UCON	✓		✓	✓	✓						AC
[62]	RelBAC	✓	✓	✓	✓				✓			AC
[49]	Chameleon	✓	✓	✓	✓					✓		AC

Varnostni kontekst v kontekstno odvisnih sistemih

Kontekstno odvisni sistemi so obetaven pristop k reševanju vrste varnostnih izzivov v modernih internetnih omrežjih in sistemih. Vendar je načrtovanje rešitev v tovrstnih sistemih še vedno zelo zahtevno. Eden od pomembnejših razlogov za tako stanje je nedoločenost, kateri del konteksta in kako je dejansko pomemben z varnostnega vidika. V okviru projekta smo analizirali vrsto raznorodnih primerov uporabe, od socialno komunikacijskih do primerov posredovanja vsebin. Analiza tako širokega nabora primerov uporabe nam je omogočila določiti konceptualni model varnostnega konteksta, prikazanega na sliki levo. Model določi ozek nabor pomembnih konceptov varnostnega konteksta in njihove relacije. V delu smo pokazali, da je model primeren za obravnavo ciljnih primerov uporabe s stališča varnosti ter da zadosti potrebam, ki so jih izpostavili do sedaj obravnavani pristopi kontekstno odvisne varnosti, prikazani na sliki desno. Naš model tako omogoča določitev varnostnega konteksta in od konteksta odvisnih varnostnih politik. Delo predstavlja podlago za varno, kontekstno odvisno posredovanje vsebine v modernih sistemih vsak z vsakim.