

Radionica posvećena temama iz oblasti sigurnosti

Datum održavanja	22. februar 2011. god.
Mesto održavanja	Beograd U zgradi u dvorištu Elektrotehničkog fakulteta, Bulevar Kralja Aleksandra 73 Vidi mapu

Cilj održavanja radionice

Radionica/seminar/workshop se organizuje u okviru aktivnosti na GEANT3 projektu, grupa GN3/NA3/T4 „Campus Best Practice”. Aktivnosti se sprovode u četiri pilot zemlje: Norveška, Finska, Republika Češka i Srbija, a vezane su za iskustva stečene u šest oblasti. Oblasti su: fizička infrastruktura, *campus networking* (uključuje IPv6), *wireless*, komunikacije u realnom vremenu (uključuje VoIP, video), nadgledanje mreže i sigurnost. Sve zemlje nisu istakle interes za svaku oblast. Srbija je aktivna u tri oblasti: fizička infrastruktura, nadgledanje mreže i sigurnost.

Namera o okupljanju grupe za sigurnost u akademskoj mreži Srbije objavljena je krajem 2009. godine. Cilj formiranja grupe je da kroz razmenu mišljenja, iskustava i upoznavanje rešenja koje institucije primenjuje, doprinese boljem razumevanju pitanja bezbednosti i pomogne institucijama da podignu efikasnost i kvalitet zaštite u svojim lokalnim mrežama. Članovi grupe (još mogu postati oni koji žele da) učestvuju u izradi AMRES BP (Best Practice Document) dokumenata i definisanju preporuka za primenu lokalnim mrežama članica AMRES-a.

Do sada su izrađena dva BD dokumenta. Prvi dokument sadrži preporuke o filtriranju paketa u okviru AMRES-a. Drugi dokument promoviše usvajanje digitalnih sertifikata u institucijama članicama AMRES-a za uspostavljanje sigurnih kanala komunikacije ka svojim serverima. BP dokumenti su objavljeni na [stranici https://www.bpd.amres.ac.rs](https://www.bpd.amres.ac.rs).

Radionica pruža priliku administratorima ne samo da upoznaju sadržaj BP dokumenata, već i da iznesu mišljenja o ponuđenim predlozima, nedostacima sa kojima se susreću u svakodnevnoj implementaciji i time doprinesu poboljšanju postojećih prakse.

Sledeći zadatak ovog okupljanja je uvid u stanje i rešenja koje se koriste u institucijama članicama u suočavanju sa drugim sigurnosnim izazovima (zaštita od spam-a, logovanje pristupa mreži i sl.), a vezano za ideje o uvođenju novih servisa u AMRES-u. Nadamo se da će tokom diskusije biti definisane potencijalne teme narednih BP dokumenata.

Namera je i da se o prvi put u AMRESu govori i o prednostima (i pozitivnom uticaju na sigurnost) uspostavljanja i održavanja baza sa podacima o krajnjim korisnicima i njihovim privilegijama u unifikovanom elektronskom formatu, te povezivanju ovih baza u jedinstvenu infrastrukturu za autentifikaciju i autorizaciju. Upoznaćemo se i sa iskustvom GRNET-a u uspostavljanju takve

infrastrukture u akademskoj mreži Grčke, sa primerima korišćenja same infrastrukture.

Radionica je namenjena administratorima, koji učestvuju u razvoju i/ili svakodnevno obavljaju poslove održavanja lokalnih računarskih mreža i servisa u institucijama članicama AMRESa.

Informacije o registraciji učesnika

[Lista učesnika](#)

Ako želite prisustvovati ovom događaju, molimo da se [registrujete](#).

Prijave se primaju zaključno sa 17.2.2011.

Broj mesta je ograničen veličinom prostora u kome se događaj organizuje.

Program

Apstrakte prezentacija takođe možete pogledati. Nalaze se ispod dnevnog reda.

Utorak, 22 Februar 2011

Sesija	Naslov prezentacije	Predavač	Trajanje prezentacije
S1	09:00 - 10:30		
S1.1	Otvaranje i dobrodošlica: Uvod u dan posvećen sigurnosti	Mara Bukvič, Dušan Pajin	10 min
S1.2	AMRES CSIRT - Statistika u 2010. godini	Dušan Pajin	20 min
S1.3	Pregled bezbednosnih dokumenata i sadržaja dostupnih na NA3/T4 i AMRES wiki-ju	Mara Bukvič	15 min
S1.4	AMRES Pravilnik o filtriranju saobraćaja	Mara Bukvič	30 min
S1.5	Diskusija o predlozima	Svi učesnici	15 min
Pauza za kafu			
S2	11:00 - 13:00		
S2.1	BPD: Filtriranje saobraćaja u krajnjim institucijama	Bojan Jakovljevič	60 min
S2.2	Bezbednosni problemi u AMRES institucijama (zaštita od spam-a, firewall, proxy, logovanje informacija i sl.) Diskusija i razmena iskustava: 1) Saša Milašinović: Propisi za korišćenje ICT sistema na Učiteljskom fakultetu u Beogradu 2) Saša Babić: Bezbednosna politika na Farmaceutskom fakultetu Definisanje tema za buduće BPD-ove	vodi Dušan Pajin	60 min
Ručak			

S3	14:00 - 15:30		
S3.1	Jedinstveni digitalni identitet korisnika – kada, zašto, kako ?	Marina Vermezovi?	35 min
S3.2	Iskustvo GRNET-a: rešenje i primene *)	Faidon Liambotis	45 min
S3.3	Pitanja i odgovori	Svi učesnici	10 min
Pauza za kafu			
S4	16:00 - 17:00		
S4.1	BDP: Upotrebom digitalnih sertifikata do sigurnog pristupa servisima (1. deo)	Milica Kovini?	20 min
S4.2	BPD: Izdavanje i korišćenje TCS serverskih sertifikata u AMRES-u - praktični primeri (2. deo)	Milica Kovini?	30 min
S4.3	Pitanja i odgovori vezani za preuzimanje i upotrebu serverskih TCS sertifikata	Milica Kovini?	10 min

*) Predavanje će biti održano na engleskom jeziku

Abstrakti prezentacija

S1.2 AMRES CSIRT - Statistika u 2010. godini

Informacija o uspostavljanju CSIRT-a u AMRES-u. Služajevi rešavani u 2010. godini - karakteristični primeri.

S1.3 Pregled bezbednosnih dokumenata i sadržaja dostupnih na NA3/T4 i AMRES wikiju

Sem grupe za sigurnost u AMRES-u, slične grupe u drugim zemljama su radile na BP dokumentima iz oblasti sigurnosti. Obuhvaćen je širok spektar tema, od predloga pravilnika („*Information security policy*”), do preporuka za zaštitu konkretnih servisa (*wireless*).

Prezentacija je koncipirana tako da pruži potpunu informacije o bezbednosnim dokumentima, nameni, formi i mestu na kome se nalaze, kako onim dokumentima koji su završeni i dostupni, tako i o dokumentima koja su još u izradi i drugim materijalima koji su dostupna na zaštićenim stranicama AMRES *wiki* -ija.

S1.4 AMRES Pravilnik o filtriranju saobraćaja

Filtriranje saobraćaja u AMRES-u se obavlja po pravilima utvrđenim kodeksom ustanovljenom u ranijim razvojnim fazama AMRES-a. Uočljiv je problem nedostataka Pravilnika o filtriranju saobraćaja, a ispoljio se i prilikom izrade BP dokumeta sa preporukama o filtriranju saobraćaja za krajnje institucije.

Paralelno sa izradom BD dokumenta o filtriranju saobraćaja za krajnje institucije, AMRES servisni centari su diskutovali o postojećim i drugim mogućim rešenjima, te pitanjima koja se moraju urediti Pravilnikom o filtriranju saobraćaja u AMRESu. To su sledeća pitanja. Pre svega, pitanje filtriranje saobraćaja - kako AMRES nije komercijalni provajder, propusni opseg kojim AMRES raspolaže nije neograničen. Svi sadržaji u akademskoj mreži nisu od podjednake važnosti. Postoji saobraćaj i sadržaji koji su potpuno nepoželjni u AMRESu, o čemu korisnici moraju biti permanentno obaveštavani i upozoravani. Ograničavanje nepoželjnog saobraćaja je obaveza administratora u svim institucijama članicama AMRESa, a ne samo u servisnim centrima AMRES-a. Zatim, pitanje filtriranje sadržaja - za nepoželjan i nedopustiv saobraćaj i sadržaj. Sledeće je pitanje upotreba proxy-a i usvajanje rešenja za evidenciju saobraćaja i logovanje, što je zakonska obaveza internet provajdera. I na kraju, pitanje sankcionisanja nedopustivog ponašanja.

AMRES servisni centri su se inicijalno saglasili oko predloga koji su formulisani u radnoj verziji dokumenta „Pravilnik o filtriranju saobraćaja u AMRESu”. Biće predstavljeni aktuelni predlozi i ostavljena mogućnost da se diskutuje o njima.

S2.1 BPD: Filtriranje saobraćaja u krajnjim institucijama (1. deo)

Filtriranje saobraćaja je jedna od bazičnih i neobilaznih tema u oblasti sigurnosti mrežne infrastrukture i servisa.

U prvoj prezentaciji, biće predstavljeni TCP/IP i OSI slojevi na kojima se može vršiti filtriranje saobraćaja, biće predstavljene osnovne preporuke za filtriranje saobraćaja i predstavljene osnovne tehnologije koje se mogu primeniti (filtriranje paketa, firewall uređaji, proxy serveri itd.). Takođe, biće predstavljene i tehnologije koje se mogu kombinovati sa tehnologijama filtriranja (NAT, VPN, IDP sistemi).

S2.2 BPD - Filtriranje saobraćaja u krajnjim institucijama (2. deo)

Druga prezentacija se odnosi na proces definisanja i implementaciju pravila o filtriranju saobraćaja. U okviru ove prezentacije biće razmatrana pitanja izbora strategije filtriranja, mehanizama definisanja i implementacije pravila, a zatim će biti predstavljeni i najčešće korišćeni servisi i protokoli u kampus mrežama. Na kraju prezentacij biće dat primer konfiguracije liste pristupa za Cisco L3 uređaje.

S2.3 Bezbednosni problemi u AMRES institucijama

Sesija će se baviti glavnim bezbednosnim problemima u AMRES institucijama. Konkretno teme kojima ćemo se baviti biće rezultat upitnika na temu bezbednosti koji će popuniti mrežni administratori AMRES institucija. Sesija će biti interaktivna i administratori mogu da uzmu učešće u sesiji i predstave neka bezbednosna rešenja i procedure u njihovim mrežama. Takođe, biće

pretstavljani teorijski koncepti skeniranja ranjivosti i iskustva iz RCUB-a, kao i novi VPN servis u AMRES-u koji je trenutno u pilot fazi.

Upitnik se nalazi na [sledećem linku](#). Biće aktivan do 16. februara.

Nadamo se da će tokom diskusije biti definisane potencijalne teme za buduća BP dokumenata.

S3.1 Jedinstveni digitalni identitet korisnika - kada, zašto, kako ?

Kako bi se prilikom pristupa mrežnim ili web resursima izvršila provera identiteta korisnika (autentifikacija) i odredila prava i privilegije korisnika (autorizacija) neophodno je da korisnik poseduje digitalni identitet. Digitalni identitet predstavlja skup podataka o korisniku kao što su: korisničko ime, lozinka, podaci koji opisuju prava i privilegije korisnika, kontakt podaci itd.

Sistem u kome svaki resurs ponaosob održava bazu digitalnih identiteta korisnika je neskalabilan i neprimenljiv jer bi korisnici morali da za svaki resurs otvaraju i pamt poseban nalog, a administratori resursa bi morali da rade dodatni posao otvaranja i održavanja naloga. Umesto toga, rešenje je da korisnik poseduje jedinstven digitalni identitet koji se čuva na jednom mestu - u bazi digitalnih identiteta matične institucije korisnika. Tada korisnik upotrebljava isti digitalni identitet za pristup lokalnim resursima institucije, a otvara se i mogućnost (ako se ostvari inter-institucionalna autentifikacija i autorizacija) da može da pristupi i resursima drugih institucija. Jedan od primera servisa, sada već svetskih razmera, koji se nudi i korisnicima van matične institucije jeste eduroam. Infrastruktura za Autentifikaciju i Autorizaciju - AAI omogućava inter-institucionalnu autentifikaciju i autorizaciju, u kojoj se korisnik autentifikuje na svojoj matičnoj instituciji, a pristupa resursima drugih institucija. Institucije koje svojim korisnicima obezbeđuju digitalni identitet nazivaju se davaoci identiteta (Identity Provider - IdP), a institucije koje nude resurse su davaoci resursa (Resource Provider - RP). Kao što je već pomenuto, osnovni gradivni element AAI jeste jedinstveni digitalni identitet korisnika koji se nalazi u bazi davaoca identiteta, tj. matične institucije.

Neki od preduslova za implementaciju AAI rešenja jeste jedinstveno razumevanje i tumačenje podataka o korisnicima, kao i garancija (od strane davaloca identiteta) da su podaci o korisnicima koji održavaju tačni (Identity Management - IdM). Na prezentaciji će biti objašnjen koncept AAI, biće dat uvod u korisničke direktorijume kao i neke od preporuka za procedure održavanja identiteta korisnika - IdM. Takođe će biti predstavljena rsEdu šema koja detaljno opisuje atribute o korisnicima koje bi svaka institucija koja će učestvovati u AMRES AAI trebalo da održava, a što je neophodan preduslov za interoperabilnost pri inter-institucionalnoj autentifikaciji i autorizaciji.

S3.2 Iskustvo GRNET-a: rešenje i primene

“Greek Research and Technology Network: Authentication & Authorization Infrastructure”

The presentation will focus on GRNET's Authentication & Authorization Infrastructure. It will

describe the motivation behind its development, the history of it, the design choices that were taken along the way and the current status and penetration of it. Among other things, the services that GRNET currently provides and is planning to provide, as well as the ways they can find to collaborate between our respective communities, will be summarized.

S4.1 BPD: Sigurna komunikacija - osnovi kriptografije i PKI (1. deo)

Prvi deo prezentacije objašnjava osnovne komponente neophodne da bi se ostvarila bezbedna komunikacija preko javne računarske mreže kao što je Internet. Dat je pregled kriptografskih protokola i tehnika. Objašnjen je koncept infrastrukture javnih ključeva (PKI - Public Key Infrastructure) i potreba za njenom implementacijom. Pregled potreba za sertifikatima u AMRESu. Postoje različite načini i procedure pribavljanja (tj. realizacije PKI infrastrukture) sertifikata u AMRES.

S4.2 BPD: Izdavanje i korišćenje TCS serverskih sertifikata u AMRES-u - praktični primeri (2. deo)

Drugi deo prezentacije objašnjava šta je TCS servis (TERENA Certificate SERVICE), prednosti koje on pruža, kao i njegova realizacija u okviru AMRESa. Objašnjene su vrste digitalnih sertifikata koji mogu da se dobiju preko TCS servisa, kako institucija može da postane korisnik i koji su sve koraci potrebni za registraciju i dobijanje TCS digitalnog sertifikata. Dalje, data su odgovori na probleme sa kojima se korisnici najčešće sreću pri samom procesu dobijanja sertifikata, kao i pri kasnijoj instalaciji istog.

From:

<http://www.bpd.amres.ac.rs/> - AMRES wiki

Permanent link:

http://www.bpd.amres.ac.rs/doku.php?id=amres_cbp_wiki:ws_security_feb_2011

Last update: 2011/09/01 23:49