Radionica posve?ena temama iz oblasti sigurnosti

Datum održavanja	22. februar 2011. god.
Mesto održavanja	Beograd U zgradi u dvorištu Elektrotehni?kog 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 ?etri pilot zemlje: Norveška, Finska, Republika ?eška i Srbija, a vezane su za iskustva ste?ene u šest oblasti. Oblasti su: fizi?ka infrastruktura, *campus networking* (uklju?uje IPv6), *wireless*, komunikacije u realnom vremenu (uklju?uje VoIP, video), nadgledanje mreže i sigurnost. Sve zemlje nisu istakle interest za svaku oblast. Srbija je aktivna u tri oblasti: fizi?ka 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. ?lanovi grupe (još mogu postati oni koji žele da) u?estvuju u izdradi AMRES BP (Best Practice Document) dokumenata i definisanju preporuka za primenu lokalnim mrežama ?lanica AMRES-a.

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

Radionica pruža priliku administratorima ne samo da upoznaju sadržaj BP dokumenata, ve? i da iznesu mišljenja o ponu?enim predlozima, nedostacima sa kojima se susre?u u svakodnevnoj implementaciji i time doprinesu poboljšanju postoje?e prakse.

Slede?i zadatak ovog okupljanja je uvid u stanje i rešenja koje se koriste u institucijama ?lanicama u suo?avanju sa drugim sigurnosnim izazovima (zaštita od spam-a, logovanje pristupa mreži i sl.), a vezano za ideje o uvo?enju novih servisa u AMRES-u. Nadamo se da ?e 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. Upozna?emo se i sa iskustvom GRNET-a u uspostavljanju takve

infratrukture u akademskoj mreži Gr?ke, sa primerima korištenja same infrastrukture.

Radionica je namenjanja administratorima, koji u?estvuju u razvoju i/ili svakodnevno obavljaju poslove održavanja lokalnih ra?unarskih mreža i servisa u institucijama ?lanicama AMRESa.

Informacije o registraciji u?esnika

Lista u?esnika

Ako želite prisustvovati ovom doga?aju, molimo da se registrujete.

Prijave se primaju zaklju?no sa 17.2.2011.

Broj mesta je ograni?en veli?inom prostora u kome se doga?aj organizuje.

Program

Apstrakte prezentacija tako?e možete pogledati. Nalaze se ispod dnevnog reda.

Utorak, 22 Februar 2011

Sesija	Naslov prezentacije	Predava?	Trajanje prezentacije
S1	**09:00 - 10:30**		
S1.1	Otvaranje i dobrodošlica: Uvod u dan posve?en sigurnosti	Mara Bukvi?, 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 Bukvi?	15 min
S1.4	AMRES Pravilnik o filtriranju saobra?aja	Mara Bukvi?	30 min
S1.5	Diskusija o predlozima	Svi u?esnici	15 min
Pauza za kafu			
S2	**11:00 - 13:00**		
S2.1	BPD: Filtriranje saobra?aja u krajnjim institucijama	Bojan Jakovljevi?	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 Milašinovi?:Propisi za koriš?enje ICT sistema na U?iteljskom fakultetu u Beogradu 2)Saša Babi?:Bezbednosna politika na Farmaceutskom fakultetu Definisanje tema za budu?e BPD-ove	vodi Dušan Pajin	60 min
Ru?ak			

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 u?esnici	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 korištenje TCS serverskih sertifikata u AMRES-u - prakti?ni 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 ?e biti održano na engleskom jeziku

Abstrakti prezentacija

S1.2 AMRES CSIRT - Statistika u 2010. godini

Infomacija o uspostavljanju CSIRT-a u AMRES-u. Slu?ajevi rešavani u 2010. godini - karakteristi?ni primeri.

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

Sem grupe za sigurnost u AMRES-u, sli?ne grupe u drugim zemljama su radile na BP dokumentima iz oblasti sigurnosti. Obuhva?en je širok spektar tema, od predloga pravilnika („*Information security policy*"), do preporuka za zaštitu konkretanih 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 zašti?enim stranicama AMRES *wiki* -ija.

S1.4 AMRES Pravilnik o filtriranju saobra?aja

Filtriranje saobra?aja u AMRES-u se obavlja po pravilima utvr?enim kodeksom ustanovljenom u ranijim razvojnim fazama AMRES-a. Uo?ljiv je problem nedostataka Pravilnika o filtriranju saobra?aja, a ispoljio se i prilikom izrade BP dokumeta sa preporukama o filtriranju saobra?aja za krajnje institucije.

Paralelno sa izradom BD dokumenta o filtriranju saobra?aja za krajnje institucije, AMRES servisni centari su diskutovali o postoje?im i drugim mogu?im rešenjima, te pitanjima koja se moraju urediti Pravilnikom o filtriranju saobra?aja u AMRESu. To su slede?a pitanja. Pre svega, pitanje filtriranje saobra?aja - kako AMRES nije komercijalni provajder, propusni opseg kojim AMRES raspolaže nije neograni?en. Svi sadržaji u akademskoj mreži nisi od podjednake važnosti. Postoji saobra?aj i sadržaji koji su potpuno nepoželjni u AMRESu, o ?emu korisnici moraju biti permanentno obaveštavani i upozoravani. Ograni?avanje nepoželjnog saobra?aja je obaveza administratora u svim institucijama ?lanicama AMRESa, a ne samo u servisnim centrima AMRES-a. Zatim, pitanje filtriranje sadržaja - za nepoželjan i nedopustiv saobra?aj i sadržaj. Slede?e je pitanje upotreba proxy-a i usvajanje rešenja za evidenciju saobra?aja 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 saobra?aja u AMRESu”. Bi?e predstavljeni aktuelni predlozi i ostavljena mogu?nost da se diskutuje o njima.

S2.1 BPD: Filtriranje saobra?aja u krajnjim institucijama (1. deo)

Filtriranje saobra?aja je jedna od bazi?nih i neobilaznih tema u oblasti sigurnosti mrežne infrastrukture i servisa.

U prvoj prezentaciji, bi?e predstavljeni TCP/IP i OSI slojevi na kojima se može vršiti filtriranje saobra?aja, bi?e predstavljene osnovne preporuke za filtriranje saobra?aja i predstavljene osnovne tehnologije koje se mogu primeniti (filtriranje paketa, firewall ure?aji, proxy serveri itd.). Tako?e, bi?e predstavljene i tehnologije koje se mogu kombinovati sa tehnologijama filtriranja (NAT, VPN, IDP sistemi).

S2.2 BPD - Filtriranje saobra?aja u krajnjim institucijama (2. deo)

Druga prezentacija se odnosi na proces definisanja i implementaciju pravila o filtriranju saobra?aja. U okviru ove prezentacije bi?e razmatrana pitanja izbora strategije filtriranja, mehanizama definisanja i implementacije pravila, a zatim ?e biti predstavljeni i naj?eš?e koriš?eni servisi i protokoli u kampus mrežama. Na kraju prezentacij bi?e dat primer konfiguracije liste pristupa za Cisco L3 ure?aje.

S2.3 Bezbednosni problemi u AMRES institucijama

Sesija ce se baviti glavnim bezbednosnim problemima u AMRES insitucijama. Konkretne teme kojima ?emo se baviti bi?e rezultat upitnika na temu bezbednosti koji ?e popuniti mrežni administratori AMRES institucija. Sesija ce biti interaktivna i administratori mogu da uzmu u?eš?e u sesiji i predstave neka bezbednosna rešenja i procedure u njihovim mrežama. Tako?e, bi?e

pretstavljeni 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 slede?em linku. Bi?e aktivan do 16. februara.

Nadamo se da ?e tokom diskusije biti definisane potencijalne teme za budu?a 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: korisni?ko 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 da otvaraju i pamte 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 ?uva na jednom mestu - u bazi digitalnih identiteta mati?ne institucije korisnika. Tada korisnik upotrebljava isti digitalni identitet za pristup lokalnim resursima institucije, a otvara se i mogu?nost (ako se ostvari inter-institucionalna autentifikacija i autorizacija) da može da pristupi i resursima drugih institucija. Jedan od primera servisa, sada ve? svetskih razmera, koji se nudi i korisnicima van mati?ne institucije jeste eduroam. Infrastruktura za Autentifikaciju i Autorizaciju - AAI omogu?ava inter-institucionalnu autentifikaciju i autorizaciju, u kojoj se korisnik autentifukuje na svojoj mati?noj instituciji, a pristupa resursima drugih institucija. Institucije koje svojim korisnicima obezbe?uju digitalni identitet nazivaju se davaoci identiteta (Identity Provider - IdP), a institucije koje nude resurse su davaoci resursa (Resource Provider - RP). Kao što je ve? pomenuto, osnovni gradivni element AAI jeste jedinstveni digitalni identitet korisnika koji se nalazi u bazi davaoca identiteta, tj. mati?ne institucije.

Neki od preduslova za implementaciju AAI rešenja jeste jedinstveno razumevanje i tuma?enje podataka o korisnicima, kao i garancija (od strane davaloca identiteta) da su podaci o korisnicima koji održavaju ta?ni (Identity Management -IdM). Na prezentaciji ?e biti objašnjen koncept AAI, bi?e dat uvod u korisni?ke direktorijume kao i neke od preporuka za procedure održavanja ideniteta korisnika – IdM. Tako?e ?e biti prestavljena rsEdu šema koja detaljno opisuje atribute o korisnicima koje bi svaka institucija koja ?e u?estvovati 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 ra?unarske mreže kao što je Internet. Dat je pregled kriptografskih protokola i tehnika. Objašnjen je koncept infrastrukture javnih klju?eva (PKI – Public Key Infrastructure) i potreba za njenom implementacijom. Pregled potreba za sertifikatima u AMRESu. Postoje razli?ite na?ini i procedure pribavljanja (tj. realizacije PKI infrastrukture) sertifikata u AMRES.

S4.2 BPD: Izdavanje i korištenje TCS serverskih sertifikata u AMRES-u - prakti?ni 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 naj?eš?e sre?u pri samom procesu dobijanja sertifikata, kao i pri kasnijoj instalaciji istog.