NLUUG Najaarsconferentie

"Security"

http://www.nluug.nl

NLUUG Najaarsconferentie 2010
11 november 2010
'ReeHorst', Bennekomseweg 24, Ede (Gld)

Tijdschema

	Studio 3		
09:00-09:00u	Opening		
09:30-10:30u	De sociale geschiedenis van de telefoon **Karin Spaink**		
	Bach 1+2	**Studio 3**	**Bach 3+4**
10:35-11:20u	Waarom het makkelijk doen als het moeilijk kan? Sudo en RBAC **Jan Sepp**	Security awareness **Hans van de Looy**	Cloud services under your control **Frank Karlitschek**
11:20-11:50u	**Koffie**		
11:50-12:35u	Hoe samenleven met SELinux? **Toshaan Bharvani**	Informatiebeveiliging en ICT-Architectuur, een 'match made in heaven'. **Willem Kossen**	Hardened Linux AT Keyboard Driver **Yuri Schaeffer**
12:35-13:55u	**Lunch**		
13:10-13:55u	**ALV**		
13:55-14:40u	DNSSEC als toegeleverde dienst **Rick van Rein**	Devops; "What's Missing" **John M Willis**	Security through the use of digital certificates and Cacert **Pieter van Emmerik**
14:45-15:30u	Het hoe en waarom van geheugendumps **Ruud van Baar**	Current state of Rainbowtable **Sebastian Graf (Naxxatoe)**	SSL is in de praktijk schijnveiligheid? **Teus Hagen**
15:30-16:00u	**Koffie**		
16:00-16:45u	GSM security: feit en fictie **Fabian van den Broek**	VPN technieken en gebruik **Mendel Mobach**	De beveiliging van Blackboard **Jobert Abma**
16:50-17:35u	Applet-based e-Ticketing **Pim Vullers**	The road to hell is paved with best practices **Frank Breedijk**	SWAN: de Secure Wireless Access Node **Rick Woelders**
17:35-18:00u	**Borrel** **De borrel is mede mogelijk gemaakt door Snow**		

Inhoudsopgave

Tijdschema			1
Inleiding			5
Keynote			
	K1	Karin Spaink De sociale geschiedenis van de telefoon	9
Lezingen			
	L1	Jobert Abma en Michiel Prins De beveiliging van Blackboard	12
	L2	Ruud Van Baar Het hoe en waarom van geheugendumps	13
	L3	Toshaan Bharvani Hoe samenleven met SELinux?	14
	L4	Frank Breedijk The road to hell is paved with best practices...	15
	L5	Fabian Van den Broek GSM security: feit en fictie	17
	L6	Rick van Rein DNSSEC als toegeleverde dienst	19
	L7	Pieter Van Emmerik Security through the use of digital certificates and CAcert	20
	L8	Naxxatoe (Sebastian Graf) Current state of Rainbowtable	21
	L9	Teus Hagen SSL is in de praktijk schijnveiligheid?	22

L10	Frank Karlitschek Cloud services under your control	24
L11	Willem Kossen Informatiebeveiliging en ICT-architectuur, een 'match made in heaven'	25
L12	Hans Van de Looy Security awareness	27
L13	Mendel Mobach VPN technieken en gebruik	28
L14	Yuri Schaeffer Hardened Linux AT Keyboard Driver	30
L15	Jan Sepp Waarom het makkelijk doen als het moeilijk kan? Sudo en RBAC	31
L16	Pim Vullers Applet-based e-Ticketing	33
L17	John Willis Devops " What's missing"	34
L18	Rick Woelders SWAN: de Secure Wireless Access Node	35
Personalia		37
Organisatie en locatie		38
Aanmelding en registratie		39
Plattegrond treinstation Ede-Wageningen		41
Plattegrond locatie		42
Expositie en sponsoring		44
Information for our foreign guests		45

Inleiding

In de laatste decenia worden steeds meer gegevens toevertrouwd aan IT systemen. In het begin waren deze slechts beperkt gekoppeld en ontsloten. En iedereen die toegang had kende elkaar en kon elkaar vertrouwen. Naarmate het gebruik van IT groeide werd deze vorm van informatie beveiliging echter steeds minder houdbaar. Niet alleen worden de informatie systemen steeds meer ontsloten; wij vertrouwen er ook steeds meer gegevens aan toe. En veel van deze gegevens zijn privacy gevoelig. De gegevens komen de laatste jaren ook steeds meer te liggen op systemen waarop de eigenaar van de gegevens geen directe invloed meer heeft (Cloud computing). Systemen worden ook steeds meer gekoppeld, waardoor er nog meer (privacy gevoelige) informatie uit te destileren valt. Helaas is niet iedereen te vertrouwen en is een goed beveiligings beleid dus noodzakelijk. De kunst is de balans te vinden tussen het ontsluiten van gegevens, en het waarborgen van de beveiliging en privacy. En dit probleem speelt niet alleen tussen organisatie en klant, maar ook binnen de organisatie.

Ter beveiliging van de gegevens zijn in de loop daar jaren vele technieken ontwikkeld. Maar met het simpelweg toepassen van de beschikbare technieken ben je er niet. IT beveiliging moet een intergraal onderdeel zijn van de IT architectuur in al zijn facetten, met een goede balans tussen beveiliging, bruikbaarheid en beheersbaarheid. IT beveiliging is ook continu in ontwikkeling. Oude technieken raken achterhaald, en er komen nieuwe technieken en producten bij. En ook de 'bad guys' zitten niet stil. Dat een goede IT beveiliging nog niet zo makkelijk is blijkt ook wel uit de vele boeken, discussies en conferenties over dit ontwerp. En deze najaarsconferentie is er een van.

We hebben geprobeerd met de lezingen zoveel mogelijk facetten van de IT beveiliging te belichten en hopen we u hierdoor weer een stap verder te helpen door nieuwe inzichten en constructieve discussies met vakgenoten. Namens de hele programmacommissie wens ik u een prettige en leerzame dag toe.

Jeroen de Meijer, Programmacommissie Najaar 2010

Keynote

De sociale geschiedenis van de telefoon

Karin Spaink

Het huis uit
De sociale geschiedenis van de telefoon – die vreemd genoeg niet eerder is beschreven – laat zien hoe de nieuwe manieren van communiceren die we uitvinden, ook onszelf en onze relaties verandert.

In een halve eeuw is de telefoon flink van vorm veranderd. Van zwaar bakelieten wandtoestel via modern huiskamersierraad werd hij een flitsend gadget dat we overal bij ons hebben: zelfs op de wc. Hij verhuisde met elke gedaanteverwisseling: van een koude gang trok hij op naar de woon- en slaapkamer. Met elke nieuwe kamer die hij in huis veroverde, werden de gesprekken die we ermee voerden persoonlijker.

Tegenwoordig nemen we via de telefoon onze privésfeer overal mee de buitenwereld in: onze leefwereld past in onze handpalm, in onze broekzak. Wat doen die draagbare, ons overal vergezellende relaties met ons gevoel voor privacy, met onze netwerken, met de publieke en politieke ruimte? En hoeveel mensen hebben door dat de telefoon langzaam ook onderdeel wordt van een nieuw maatschappelijk middenveld?

Biografie

Karin Spaink (1957) is columnist voor onder meer *Het Parool*, *Medisch Contact* en *de Praktijk*. Ze schreef inmiddels tien boeken, waaronder *Het strafbare lichaam*, *Vallende vrouw* en *Medische geheimen*. Ze is hoofdredacteur van *The Next Ten Years*, een serie van zes boeken over technologie en maatschappij. Ze was jarenlang voorzitter van Bits of Freedom, was bestuurslid van Spamvrij.nl, en is juryvoorzitter van de Big Brother Awards. Voor haar onderzoek naar de veiligheid van elektronische patiëntendossiers kreeg ze in 2006 de ISOC Award. Momenteel werkt ze aan een boek over *Hack-Tic*, XS4all en het ontstaan van het publieke internet in Nederland.

Lezingen

De beveiliging van Blackboard

Jobert Abma en Michiel Prins

Online 24

Begin dit jaar heeft Online 24 een grootschalig onderzoek uitgevoerd naar de beveiliging van Blackboard Academic Suite en Blackboard Learn. Uit het onderzoek is gebleken dat veel hogescholen en universiteiten grote beveiligingsrisico's lopen. In eerste instantie zijn de resultaten van het onderzoek als vertrouwelijk beschouwd, maar zijn vanwege nationaal belang openbaar gemaakt.

Tijdens de presentatie zal de privacy van gebruikers en integriteit van informatie worden besproken. Daarnaast zal er aan de hand van een Proof of Concept gedemonstreerd worden hoe een student in vijf minuten de rol van een docent aan kan nemen en zich hiermee toegang kan verschaffen tot meerdere systemen.

Biografie

Michiel Prins en Jobert Abma zijn ethical hackers bij Online 24. In het dagelijks leven doen ze onderzoek naar de beveiliging van applicaties, infrastructuren en organisaties. Beide hebben een grote rol gespeeld in het beveiligingsonderzoek van Blackboard Academic Suite en Blackboard Learn.

Het hoe en waarom van geheugendumps

Ruud Van Baar

Nederlands Forensisch Instituut

Het maken van geheugendumps wordt binnen de forensische wereld steeds meer onderdeel van de zogenaamde best practices. In het geheugen van een computer kunnen zich sporen bevinden die zich niet op de harde schijf bevinden en het uitzetten van een mogelijk gecompromitteerd systeem kan er toe leiden dat deze sporen verloren gaan.

Aan de hand van de Honeynet-challenge en andere voorbeelden wordt gekeken wat geheugendumps kunnen toevoegen aan een onderzoek. Hoe kan informatie worden geanalyseerd in geheugendumps, hoe extraheren we de malware en welke tools en technieken zijn beschikbaar? Naast de publiekelijk beschikbare tools zal een bibliotheek ontwikkeld door het NFI worden getoond.

Biografie

Ruud van Baar is sinds september 2007 werkzaam bij het Nederlands Forensisch Instituut als digitaal onderzoeker. In 2008 is zijn onderzoek naar bestanden in geheugendumps gepubliceerd onder de titel "Forensic memory analysis: Files mapped in memory" in de speciale uitgave van Digital Investigation behorende bij de DFRWS conferentie (www.dfrws.org).

Hoe samenleven met SELinux?

Toshaan Bharvani

VanTosh

Security Enchanced Linux, wordt normaal afgezet, omdat mensen in de meeste gevallen niet de tijd wensen te nemen om te leren hoe men met SELinux dient te werken. SELinux verdeelt applicaties in containers en zondert elke container tot een bepaalde groep van porten, files en daemons. Deze verdeling laat toe dat indien er toch iemand op het systeem zou binnen hacken er nog een abstractieniveau is waar men eerst door dient te komen. Ook door het beperken van deze daemons tot hun container en deze containers beter te beveiligen kan met voor de hand liggende "fouten" voorkomen en zo de beveiliging van het systeem verhogen. Ondertussen zijn er reeds veel tools die het gebruik van SELinux vergemakkelijken in RHEL / CentOS / Fedora. Er zal uitgelegd worden hoe om te gaan met de predefined policies en hoe men gemakkelijk nieuwe custom policies kan definiëren.

Biografie

Toshaan is reeds enige tijd bezig in IT. Hij is als IT consultant bezig met het implementeren en het promoten van Linux naar zakelijke klanten met als onderwijs een Master in Handelsingenieur in de beleidsinformatica - Informatietechnologie en een technische achtergrond door werkervaring en extracurriculaire activiteiten.

Momenteel is hij bezig met collaboratie systemen, virtualizatie, ERP/CRM met algemene system administratie. Als bijkomende interesse en hobby houd hij security altijd in het achterhoofd, niet enkel op IT niveau, maar ook op een breder niveau.

The road to hell is paved with best practices…

Frank Breedijk

Schuberg Philis

This light talk will try to address the "unaskable" question "will best practices make use more secure?" in a light and entertaining manner. Will a strong password policy result in stronger passwords? When are there too many admins on the system? In good cop/bad cop style Frank Breedijk and Ian Southam will address this topic from the firm believe that IT Security should actually make IT more secure.
As obvious as that statement seems, security measures often do not achieve this goal but sometimes hurt it. E.g. enforcing "very strong" password policies will often result in people not being able to remember their passwords and writing them down, or reverting to passwords like Password01, Password02, etc. In the process the hope to plant the seed for some of the serious self reflection that is required from the IT Security industry.

What will the audience gain:
Besides the fact that I plan to give an entertaining presentation, we also hope to trigger some self reflection in the IT security community. We hope to help break the inertia of certain log lived best practices that, e.g. force us to change our password every month because it takes two months to crack such a password with a PDP-11.

Biografie

Frank Breedijk (@Seccubus) is employed as a Security Engineer at Schuberg Philis since 2006. He is responsible for the technical information security of Schuberg Philis Mission Critical outsourcing services. This including, Security Awareness, Vulnerability management, Internal security consultancy and technical audits and Seccubus Development Frank Breedijk has been active in IT Security for over 10 years. Before joining Schuberg Philis he worked as a Security Consultant for INS/BT and Security Officer for Interxion. He managed the European Security Operations Center (SOC) for Unisys' managed security services. During this period Gartner labeled Unisys leader in the magic quadrant for Managed Security Services in Europe.
He is also the author of the open source security tool Seccubus and blogs for cupfighter.net

GSM security: feit en fictie

Fabian Van den Broek

Radboud universiteit Nijmegen

Wereldwijd maken ongeveer 4.1 miljard mensen gebruik van GSM. Het is inmiddels meer dan 20 jaar geleden sinds GSM werd ontworpen en sindsdien zijn er verschillende security problemen gevonden, zowel in de protocollen als in de, oorspronkelijk geheime, cryptografie. Het praktisch uitbuiten van deze zwaktes is echter ingewikkeld, met name door alle signaalbewerking die daarbij komt kijken.

Vrij recent zijn SDRs (Software Defined Radios) op komen zetten. In een SDR wordt een deel van een radio systeem, dat traditioneel in hardware wordt geproduceerd, geimplementeerd in software, wat leidt tot relatief goedkope en flexibele radio ontvangers. Een goed voorbeeld hiervan is de veelgebruikte combinatie van de USRP (Universal Software Radio Peripheral) met GNU Radio.

Hierdoor is er de laatste tijd veel meer praktisch onderzoek gedaan naar GSM veiligheid door verschillende groepjes hackers, voorlopig culminerend in de rainbow-table aanval op de GSM encryptie gepresenteerd door Karsten Nohl eind december 2009 in Berlijn. Deze laatste aanval heeft, met name in de on-line media, geleid tot vrij wilde claims over het kunnen afluisteren van GSM gesprekken. Toch loopt zo'n aanval op dit moment nog tegen grote praktische problemen aan. Wat overigens niet wil zeggen dat GSM daarmee op dit moment veilig is.

Hoewel UMTS, de opvolger van GSM, al enige tijd succesvol wordt gebruikt zijn we voorlopig nog niet van GSM af. Met de veiligheid van GSM zijn enorme belangen gemoeid. Mijn presentatie zal ingaan op de huidige stand van zaken van de veiligheid van GSM. Ik zal enkele recent gepresenteerde aanvallen en hun (on)haalbaarheid bespreken, maar ook ingaan op andere open-source initiatieven, zoals een open-source zendmastimplementatie.

Biografie

Fabian Van den Broek heeft recent zijn Masteropleiding informatica afgerond met de scriptie:"Catching and Understanding GSM-Signals"
Sinds April is hij werkzaam als junior onderzoeker voor de digital security groep aan de Radboud universiteit Nijmegen. Daar doet hij onderzoek naar de veiligheid van draadloze communicatie technieken als GSM, GPRS en UMTS.

DNSSEC als toegeleverde dienst

Rick van Rein

OpenFortress Digital signatures

Lange tijd is DNS een doorn in het oog geweest van elk project dat netwerkveiligheid probeerde te verwezenlijken. Maar na lang talmen is het eindelijk zo ver: DNSSEC is uitgerold in de root, en zit nu in de fase waarin top-level domeinen ze implementeren. Ook SIDN zal DNSSEC nog voor deze NLUUG-conferentie hebben gerealiseerd voor onze eigen .NL zone.
Het met DNSSEC ondertekenen van een bescheiden domein is doenlijk, maar wanneer het 24x7 actieve domeinen betreft wordt het moeilijker.
Echt ingewikkeld wordt het wanneer DNSSEC moet worden ingericht als toegeleverde dienst, bijvoorbeeld bij een ISP. Toch moeten we die kant op, want de complexiteit van DNSSEC maakt het aantrekkelijk om het uit te besteden. Er is dus mogelijk commerciele meerwaarde te halen, wat de introductie zal helpen versnellen. Gelukkig is het daarbij niet nodig dat elke ISP zelf het wiel moet uitvinden.
SURFnet is de ISP voor Nederlandse universiteiten en hogescholen, en zij heeft een voortrekkersrol op dit gebied op zich genomen. Doel was om DNSSEC met een simpel vinkje in een web-interface te kunnen inschakelen. Via een zorgvuldig uitgeknobbelde architectuur van high-availability signers en hardware security modules is dit tot een robuuste dienst ontwikkeld, die dankzij het openbare karakter van SURFnet door anderen als voorbeeld kan worden gebruikt. In deze lezing leggen we uit hoe we de opzet bij SURFnet hebben ontworpen, welke software daarvoor is gebruikt (en welke niet) en welke lessen we bij de ontwikkeling hebben geleerd.
We gaan tenslotte op een aantal punten van technische (en wellicht
commerciele) meerwaarde in, want het zou van gebrek aan fantasie getuigen om DNSSEC alleen te beschouwen als bescherming tegen cache poisoning. Aan de vertrouwenspaden die DNSSEC uitstippelt kan een scala aan zekerheden worden onttrokken voor alledaagse protocollen als TLS, PGP en SSH.

Biografie

Deze voordracht wordt gepresenteerd door Rick van Rein van OpenFortress Digital signatures. Het besproken werk is uitgevoerd voor SURFnet's Roland van Rijswijk, die tevens tweede auteur is van deze voordracht.

Security through the use of digital certificates and CAcert

Pieter Van Emmerik

Thales Netherlands

Secure your email, website or software using (free) digital certificates (issued by CAcert). Digital certificates can be used to secure your email or website and can be used to sign software. Security issues that can be addressed are Identification (who am I talking to), Integrity (is the information changed during transport), and Confidentiality (no listening in on the conversation). Digital certificates can also be used for authentication for example for log-in to a website. CAcert is a community based Certificate Authority providing free certificates just for this purpose and aims to educate people in the use of digital certificates to improve the security on the internet. In this talk I will give a basic introduction on Digital Certificates and show a number of examples of how we are using certificates within the CAcert community. Then I will explain about the CAcert community and association and give some information on how CAcert ensures the trust for the certificates by using a web of trust by assurers and how we make the rules to make all this possible. Last but not least some information on the status of the distribution (or the lack thereof) of the CAcert root certificates in mainstream browsers and distributions.

Biografie

Born on 1958 in Bendigo - Australia, but grew up in the Netherlands. Studied Mechanical Engineering at Twente University from 1977. Graduated 1986 with a Master of Science degree in engineering (the old Dutch Ir title). From 1986 to 1994 I worked on developing Computer Aided Design and Computer Aided Manufacturing systems for Signaal, a Dutch Defense Contractor. After that I have worked for a Project company creating technical automation solutions among which systems to monitor and secure the perimeter of sites owned by the Dutch Gasuni. In 1998 I started working for a Thales Netherlands to manage the Configuration Management and Product Data Management applications they use, including the security around them. CAcert assurer since 2008 and CAcert association member since 2009.

Current state of Rainbowtable

Naxxatoe (Sebastian Graf)

NNC

A talk on secuity from my point of view, bundled with usability.
A talk on whats currently going on in the rainbowtable field

Biografie

Naxxatoe is a IT Security Researcher / Analyst currently resident in Austria. His Technical Skill and Abilities as well as his knowledge about IT Security lead him to travel the world and give bleeding edge talks at various IT Sec Conferences and work as a Consultant for various Global Companies. Combining the best from both the Ethical Hacking and the Dark Arts, he is able to provide good and balanced Advice on Potential Threats / Attacks and Counter measures.

SSL is in de praktijk schijnveiligheid?

Teus Hagen

Een overzicht en commentaar zal gegevens worden van de checks, alsmede een overzicht van de feedback op de waarschuwing als de beveiliging van de SSL service beneden niveau was.

De meeste sites maken gebruik van Apache als web service hosting. In de prersentatie worden tips gegeven om de configuratie van ssl_mod van Apache te verbeteren en een web applicatie firewall in te richten.

Veel guru' s uit de NLUUG gelederen zijn security adviseurs. Dit wil niet zeggen dat zij verantwoordelijk gesteld kunnen worden voor de soms slechte configuraties van web hosts.
Zij zijn echter wel afhankelijk van hun broodheren tav waarschuwingen over de slechte status en zij zijn daardoor mogelijk terughoudend met dergelijke SSL-test bevindingen.

Privacy kan zo simpel gewaarborgd worden in internetland. Dat was en is de theorie. Deze praktijkcheck toont helaas wat anders, vooral tav bescherming van de privacy bij de lokale overheid. Banken hebben hun standaard beveiligingsregels en de overheidsinstellingen hebben...? Wat zou CBP doen of kunnen doen? Hoe verbeteren we het certificaat gebruik. Wanneer is DNSsec volledig ingevoerd (Nld: juli 2010?)?

Biografie

Teus Hagen denkt nog steeds dat hij de eerste was met UNIX en internationale netwerking in Europa. Hij initieerde "Open Source" gebaseerde organisaties zoals NLUUG, European Unix User Group, European Unix netwerk EUnet en nam later het voortouw in vele besturen zoals bijv. NLnet (eerste Nederlandse Internet Provider), Internet Software Consortium (bind/dhcp), NLnet als grote netwerk technologie sponsor, en publieke X509 certificaat autoriteit CAcert. Hij initieerde de eerste Open Source software distributies. De vrije beschikking van software en services is de rode draad van zijn werk.
Vanwege zijn leeftijd heeft hij zich teruggetrokken uit alle functies.
Zijn interesse gaat uit naar Open Source netwerk technologie en alles wat erbij komt kijken om het veilig te houden en vrij voor iedereen beschikbaar te krijgen en te behouden.
Zijn dochter vertelt haar vrienden dat Teus een computer nerd is, die maar niets begrijpt van haar MS software probleem.

Cloud services under your control

Frank Karlitschek

KDE

One of the biggest trends of the last years were the move from classic desktop applications to cloud based services. People can easily share documents, access them from all devices and don´t have to care about backup. The problem is that the users has to give up control over the data to benefit from the advantages of cloud computing. This is of course a problem for the free software community and everybody who cares about privacy.

The idea of ownCloud is to enable the user to access all the data from all devices, allow to share stuff with others and have automatic versioning and backup of files. All this is possible without uploading your data to an untrusted service or server.

ownCloud.org was first announced during the Camp KDE keynote in January 2010 in San Diego. The current version 1.0 is already popular among developers and users.

This talk will present the ideas behind the ownCloud project, the current state and a vision for the future

Biografie

Frank Karlitschek was born 1973 and lives in Stuttgart, Germany. He is a KDE contributor since 2001. Frank worked in the artist team, coorganized the first Akademy conference and is the maintainer of KDE-Look.org, KDE-Apps.org and the openDesktop.org network. He invented the Social Desktop idea and founded the ownCloud project. He is current Vice President and member of the board of directors of the KDE e.V.

Informatiebeveiliging en ICT-architectuur, een 'match made in heaven'

Willem Kossen

M&I Partners BV

In deze lezing leg ik informatiebeveiliging en ICT architectuur tegen elkaar aan. De overeenkomsten zijn gelijk duidelijk. Waar architectuur samenhang zoekt tussen verschillende onderwerpen en belangen binnen en tussen organisaties, focust informatiebeveiliging meer op de in het speelveld. Architectuur en informatiebeveiliging kunnen niet zonder elkaar. Architectuur zonder security is onzin, maar andersom eveneens. Dan blijft informatiebeveiliging beperkt tot het ad-hoc bedenken van maatregelen op risico's wat kan leiden tot technocratisme. Daar wordt een organisatie meestal niet beter van.

De vraag die ik zal proberen te beantwoorden is hoe je informatiebeveiliging kunt toepassen op een manier dat de gebruiker en/of klant het best is geholpen, en het minst wordt gehinderd, zodat bedrijfsdoelen (inclusief veranderingen) worden gehaald en de risico's worden beheerst. De kern van de zaak is de samenhang die juist door architectuurdenken wordt ondersteund. Maar dat gaat niet zomaar vanzelf. Net als bij veiligheid speelt ook bij architectuur bewustzijn een grote rol. in plat engels: Architectural awareness as a precursor for security-awareness.

In de lezing zal ik de begrippen definieren en vooral ingaan op de relaties tussen

- trends en ontwikkelingen, standaarden, bestpractices,
- organisatiedoelen, strategie en visie
- functionele en operationele requirements
- risico's en andere beperkingen (bijvoorbeeld financieel)
- ontwikkeling, realisatie.

De verbinding daartussen is architectuur, en security is een van de views die we daarop kunnen toepassen. Door op deze integrale manier naar veiligheid te kijken verbeteren we de besluitvorming, vermijden we risico's, voorkomen we tunnelvisie en profiteert iedereen zo goed mogelijk van de mogelijkheden van de informatievoorzieningen van de organisatie(s). Oh, en dat het mensenwerk blijft spreekt voor zich…

Biografie

Willem Kossen is een ICT-adviseur en –architect met meer dan 13 jaar ervaring binnen een groot aantal branches. Enkele van zijn specialiteiten zijn interoperabiliteit en integratie, informatiebeveiliging, ICT-architectuur, Open source en standaarden,en Business en ICT alignment. Dagelijks is Willem bezig met creativiteit te zoeken naar innovatieve, maar ook pragmatische oplossingen voor ICT gerelateerde vraagstukken. Willem is naast techneut ook een verbinder, spreker en netwerker.

Willem is getrouwd, vader van 2 kinderen, speelt in de vrije tijd in een Bluesband.

Security Awareness

Hans Van de Looy

Madison Gurkha

Tijdens deze security conferentie zal ik geen presentatie verzorgen over een diepgaand technisch onderwerp. Dit keer wil ik aandacht vragen voor een moeilijk, ondergewaardeerd maar uiterst belangrijk onderwerp genaamd beveiligingsbewustzijn. Hopelijk draagt de inhoud bij tot een meer evenwichtige invulling van informatiebeveiliging en nodigt deze uit tot discussie.

Biografie

Hans (J.C.G) Van de Looy is een van de oprichters van Madison Gurkha. Hij helpt organisaties bij het opzetten en up-to-date houden, maar vooral bij het testen, van hun beveiliging. Hij is een bekende spreker op (internationale) conferenties, gastdocent op universiteiten en hogescholen en publiceert regelmatig in vakbladen over beveiliging en het doorbreken daarvan. Zijn interesse omvat, maar is zeker niet gelimiteerd tot, beveiliging in de meest brede zin van het woord (inclusief tijdverdrijf zoals `Lockpicking'), fotografie, lezen en muziek. Hans kan middels e-mail worden bereikt via hans@madison-gurkha.com.

VPN technieken en gebruik

Mendel Mobach

Systemhouse Mobach BV

Virtual Private Networks zijn een erg leuke manier om zeker te zijn dat er enige vorm van security en wat meer privacy is. Het is ook een zinvolle manier om zeker Network Address Translation uit het buideltje met netwerk benodigdheden te halen. Ook levert het kans op meer controle over clients, verplichte encryptie, authenticatie en soms zelfs authorizatie.

Daarnaast is het een groot gevaar als je het op de verkeerde manier doet; meerdere klanten met elkaar verbinden, een rechte lijn dwars door de firewall heen met virussen/wormen geinficteerde machines en natuurlijk routing attacks.

Deze lezing focust op 2 verschillende aspecten: Als eerste de gebruikte technieken binnen het grote scala aan VPN software, de gevolgen van de gekozen technieken, de (in)compatabiliteit in de wereld, en veiligheids risico's bij het gebruik van VPN's en de kans op succesvol client policies forceren, de voor- en nadelen van split tunneling en natuurlijk de verschillen tussen IPSEC en SSL vpn implementaties.

Ten tweede gaat het over het beheer en administratie; zeker weten welke client wie is en zeker weten dat deze ook nog toegang mag hebben. Er zijn verschillende mogelijkheden zoals username/password, token generatoren, X509 certificaten, RSA keys, gedeelde geheime sleutels en combinaties hiervan. Dit alles hangt natuurlijk af van de gebruikte software, en welke functies standaard worden meegeleverd met operating systemen, welke clients beschikbaar zijn, en dit alles wordt langzaam steeds meer ingewikkeld door nieuwe technieken zoals operatingsystem op mobile devices, IPv6 en natuurlijk clients achter IPv4 NAT.

En natuurlijk worden ook de coorporate VPN netwerken zoals aangeboden door ISP's om verschillende kantoren met elkaar te verbinden niet vergeten.

Biografie

Mendel Mobach is a fulltime geek for Systemhouse Mobach BV. and involved in a couple community projects like NLLGG, CCC events, HAR2009, CACert server administration and a lot more. He is active opensource user, contributer, hacker and has a serious interest for security systems not only limited to computers and networks.

Hardened Linux AT Keyboard Driver

Yuri Schaeffer

NLnet Labs

This paper is the result of a practical assignment for the course Intrusion Detection Systems at the System and Network Engineering program. Hardware keystroke loggers are said to be undetectable by other means than physical inspection. This research will prove this assumption false by patching the current Linux keyboard driver to be able to detect such malicious devices. This talk will give an overview about the hardware and software involved with AT keyboards on x86 compatible architectures. To see how and why detection could be made to work. Finally two implemented features will be introduced and explained. One feature that is able to detect a key stroke logger and an other feature that tries to render the data useless for an attacker by polluting its log file with random data.

Biografie

Yuri Schaeffer was born in 1983 and lives in Haarlem, The Netherlands.

After a Computer Science study his affinity with open source led him to System and Network Engineering master at the University of Amsterdam.

As of 2009, with the latter in a finishing state, 90 percent of his time is spend for the NLnet Labs foundation as a software developer.

Waarom het makkelijk doen als het moeilijk kan? Sudo en RBAC

Jan Sepp

S2eP2

Ik kom in mijn beroepspraktijk drie misvattingen tegen:

- Waarom zou je RBAC (Role-Based Access Control) gebruiken als je precies hetzelfde kunt bereiken met sudo?
- RBAC is ongelofelijk ingewikkeld
- RBAC is alleen geïmplementeerd in Solaris

Ik zet RBAC af tegen sudo, om te starten bij wat de toehoorders wèl weten. De conclusie is dat je sòms het ene tool moet gebruiken, soms het andere.

- Wat is het probleem?
    - Root mag te veel, gebruikers mogen te weinig
    - identificatie, authenticatie, authorisatie, audit
    - least privilege als een van de oplossingen
    - multi-layer security
    - "one protocol to bind them all". Oftewel: platform onafhankelijkheid
- afkomst sudo
- afkomst RBAC (DOD, NIST, ANSI/INCITS 359-2004)
- werking sudo
- werking RBAC: privilege, (profile) role, user. "Roles" en "rules".
- voordelen sudo
- voordelen RBAC
- RBAC in de echte wereld: implementaties
- uitbreidingen op RBAC: attributen, process privileges
- conclusies:
    - wanneer moet je moeilijk doen, wanneer kun je het makkelijk houden?
    - RBAC is ingewikkeld, want de use cases zijn ingewikkeld. Maar ongelofelijk ingewikkeld, nou nee.

Biografie

Jan Sepp (1953) is ZZP-er, Unix consultant en docent. In 1977 kwam hij bij toeval met Unix in aanraking en sindsdien heeft hij er zijn brood mee verdiend. Hij is meegegroeid met Unix: van de mini-computers naar de workstations; van de workstations naar het datacenter. Vanaf 1994 werkt hij ook met Linux – eerst om te kijken wat het was, en al snel voor productie. “Linux is voor mij gewoon een Unix dialect.”

Applet-based e-Ticketing

Pim Vullers

Radboud Universiteit Nijmegen

De huidige OV-chipkaart is niet veel meer dan een geheugenchip met een vastgestelde data-layout. Moderne smart cards bevatten een micro-processor en hebben daardoor, naast geheugen, ook rekenkracht. Met zo'n nieuwe kaart is het mogelijk een slimmere OV-chipkaart te ontwikkelen. De beveiliging kan verbeterd worden door gebruik te maken van standaard authenticatie protocollen en versleutelingsmechanismen. Daarnaast is het ook mogelijk om de privacy te verbeteren door nieuwe technieken in te zetten. Zo kan er bijvoorbeeld gekozen worden voor attribuut-gebaseerde authenticatie in plaats van identiteit-gebaseerd. Zo verteld de kaart bijvoorbeeld enkel dat je een NS jaar-abonnement hebt, maar niet je identiteit. Hierdoor wordt traceren en profileren onmogelijk gemaakt. Tijdens deze lezing zal ik een overzicht geven van de mogelijkheden voor een slimmere, veiligere en privacy-vriendelijkere OV-chipkaart en de resultaten die we al bereikt hebben op weg naar zo'n kaart.

Biografie

Pim Vullers is een Digital Security promovendus aan de Radboud Universiteit Nijmegen waar hij onderzoek doet naar "Applet-based e-Ticketing". Zijn belangstelling voor computerbeveiliging ontstond aan het eind van zijn Bachelor Technische Informatica aan de Technische Universiteit Eindhoven. De Computer Security Master track van het Kerckhoffs Instituut, een samenwerking tussen de Universiteit Twente, de Technische Universiteit Eindhoven en de Radboud Universiteit Nijmegen, was dan ook een logische keuze. Na zijn afstudeerproject aan de Universiteit van Luxemburg leidde zijn interesse voor het doen van onderzoek tot de beslissing om verder te gaan als promovendus.

Devops “What’s Missing?”

John Willis

Opscode

The Devops movement is gaining tremendous adoption. This presentation will cover some of the important themes of this movement and try to address some of the important areas that aren't being discussed. The session will start with an overview what “Devops” people are talking about CAMS (Culture, Automation, Measurement, and Sharing). Then we will dive into the missing voices (Network and Security). The presenter will gather a perspective from some of the leading “new” infrastructure experts on “NET/SEC” and provide a summary review of “Devops What's Missing”.

Biografie

John Willis has worked in the IT management industry for 30 years. He started as a tape operator on an IBM mainframe while working for his high school computer club, and began his professional career at Exxon as an IT infrastructure analyst. He is the founder of four successful startups over the past 20 years and is currently the VP of Services at Opscode . Willis is known internationally for his IT Management and Cloud blog. He also has two podcast series on clouds called 'Cloud Cafe' and 'Cloud Droplets'. Willis is also the co-host of Redmonk's 'IT Management Guys' podcast series.

SWAN: de Secure Wireless Access Node

Rick Woelders

Hogeschool Leiden

Om roaming en gastgebruik van een (draadloos) netwerk en bijbehorende infrastructuur mogelijk te maken is mede door SurfNet voor de onderwijsdoelgroep een authenticatie systeem ontwikkeld. Eduroam maakt het mogelijk om met credentials van het ene instituut het wireless netwerk en internet connectivity te gebruiken van een ander deelnemend instituut. Om deze dienst te gebruiken buiten de instituten is het wenselijk om niet afhankelijk te zijn van eigen verbindingen en bijvoorbeeld een open publieke infrastructuur te gebruiken. De SWAN node, ontwikkeld in een project bij Hogeschool Leiden kan de Eduroam dienst veilig over een publieke infrastructuur distribueren. In Leiden is gekozen om Wireless Leiden hier voor (in de prototype fase) te gebruiken. Deze lezing zal de technische architectuur, omgeving en opbouw van het SWAN concept behandelen, met nadruk op het end-to-end security aspect. Security is een van de top design criteria binnen het SWAN concept.

Biografie

Rick Woelders studeert Informatica aan de Hogeschool Leiden. Hij is betrokken bij PHP softwareprojecten en de ontwikkeling van embedded Unix systemen.

Algemene informatie

Personalia

De NLUUG verenigt (professionele) gebruikers van Open Systemen en Open Standaarden in Nederland; een gemeenschap van systeembeheerders, programmeurs en netwerk-specialisten. Het doel van de NLUUG is de verbreding van de toepassing en kennis over "Open" en UNIX/Linux.

De NLUUG programmacommissie bestaat uit:

Jos Jansen	jos@snow.nl
Walter Belgers	walter@nluug.nl
Kris Buytaert	Kris.Buytaert@inuits.be
Jeroen de Meijer	jdemeijer@competa.com
Marcel Nijenhof	marceln@pion.xs4all.nl
E-mail:	pc-nj2010@nluug.nl

Het bestuur van de NLUUG bestaat uit:

Voorzitter:	Luc Nieland *(Solstice)*
Secretaris:	Mark Overmeer *(MARKOV Solutions)*
Penningmeester:	Klaas van Gend *(MontaVista)*
Leden:	Adriaan de Groot *(KDE)*
	Jos Jansen *(Snow)*
	Rudi van Drunen *(Competa IT)*
	Patrick Reijnen (*Capgemini)*
E-mail:	bestuur@nluug.nl
Congresorganisatie:	Organisatie- en Congresbureau Interactie
	http://www.interactie.org
	info@interactie.org

Organisatie en locatie

U bent als deelnemer aan de NLUUG Voorjaarssconferentie vanaf 8:30 uur welkom voor de inschrijving, koffie en thee. De lezingen zijn gepland van 9:15 uur tot ongeveer 17:35 uur. Het gedetailleerde programma vindt u in het tijdschema.

Bij aankomst ontvangt u een badge en informatiemap.

Op de bijeenkomst zullen tevens een aantal uitgevers aanwezig zijn.

Locatie

Hotel en Congrescentrum ReeHorst
Bennekomseweg 24
6717 LM Ede (Gld)
The Netherlands
Telefoonnummer: 0318 – 750300
http://www.reehorst.nl

Congrescentrum 'ReeHorst' ligt op loopafstand (circa 10 minuten) van het NS-station Ede-Wageningen, aan de Bennekomseweg 24. Indien u met eigen vervoer komt staat in Ede 'ReeHorst' duidelijk aangegeven op ANWB-borden. Er is voldoende parkeergelegenheid bij het congrescentrum (EUR 3,50 per dag).

Aanmelding en registratie

U kunt zich elektronisch aanmelden voor de bijeenkomst via de NLUUG website: http://www.nluug.nl/events/nj10

Uw aanmelding voor deze Najaarsconferentie is definitief wanneer voor 4 november 2010:

1. uw aanmeldingsformulier is ontvangen; en
2. het deelnamegeld is bijgeschreven op de NLUUG-rekening

Onderstaand treft u een overzicht aan van de deelnamekosten:

	Incl. 19% BTW	Excl. BTW
NLUUG-leden (of zusterorg.)	€ 135,00	€ 113,45
Niet-leden	€ 290,00	€ 243,70
Studenleden	Gratis toegang	€ Niet van toepassing
Studenten	€ 26,00	€ Niet van toepassing

Studenten dienen hun collegekaart of bewijs van inschrijving op de dag van de conferentie bij de registratiebalie te tonen.

Studenten die een NLUUG studentenlidmaatschap hebben kunnen *gratis* aan deze conferentie deelnemen. U dient zich echter wel vooraf in te schrijven, zodat er een badge voor u kan worden klaargelegd.

Nadat u zich heeft ingeschreven ontvangt u een bevestiging en een factuur. Het inschrijfgeld dient uiterlijk **4 november 2010** bijgeschreven te zijn op de NLUUG ING-rekening (23.53.318), onder vermelding van het factuurnummer en uw naam. U bent dan pas definitief ingeschreven. Op 11 november 2010 zal uw badge bij de inschrijfbalie voor u klaarliggen. Let wel: als u binnen zeven werkdagen na inschrijving nog geen bevestiging van ons heeft ontvangen verzoeken wij u vriendelijk om contact met ons op te nemen om een correcte inschrijving te garanderen.

De eerste 75 betaalde registraties ontvangen bij inschrijving een kleine attentie, ook wel bekend als de "**Early Bird"**.

Indien het bedrag niet op 4 november 2010 is bijgeschreven dient u op 11 november 2010 contant aan de registratiebalie te betalen. Houdt u dan rekening met mogelijke wachtrijen.

Betaling aan de registratiebalie kan via:

1. PIN betaling (bank- of giropas)
2. Contant
3. Incassomachtiging

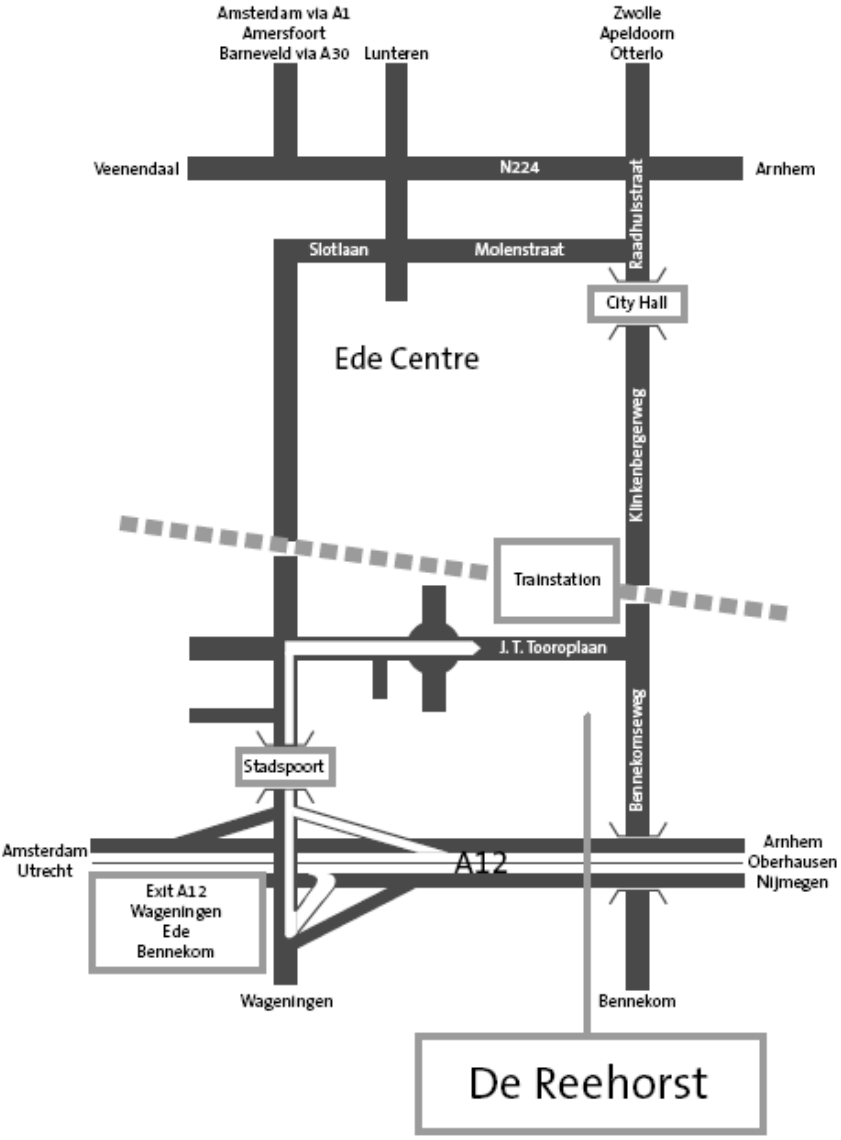
Wanneer na de conferentie blijkt dat uw betaling alsnog via de ING is ontvangen, wordt dit bedrag per omgaande teruggestort.

Betaling met creditcard is helaas niet mogelijk.

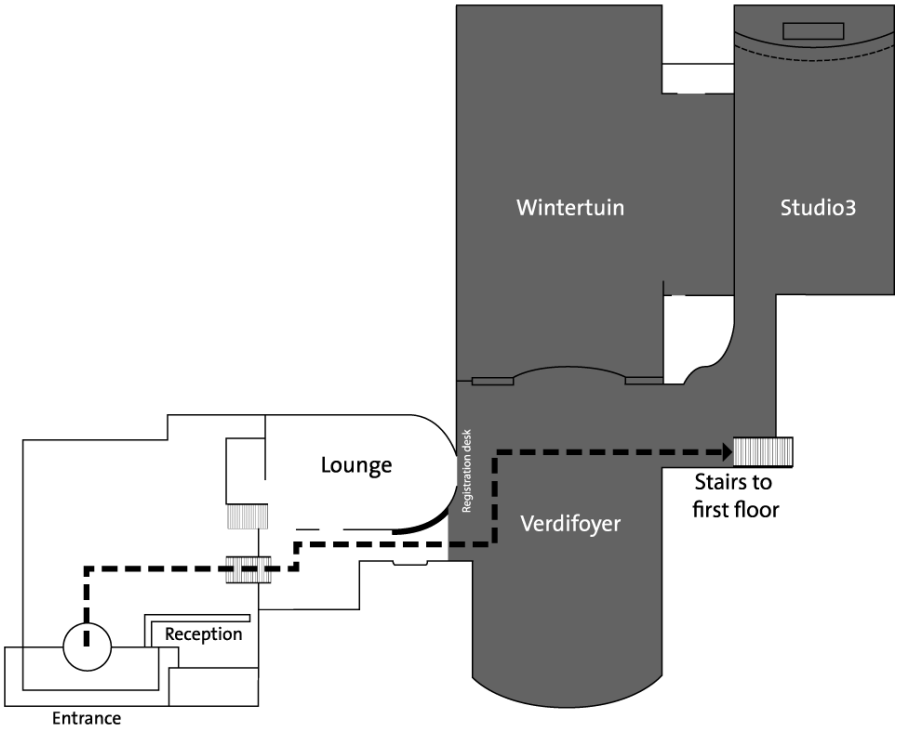
Annulering

Bij annulering tot 10 werkdagen voor het NLUUG Najaarsconferentie op 11 november 2010 wordt een annuleringsvergoeding van € 35,00 berekend. Na deze termijn zijn de totale inschrijfkosten verschuldigd. Alleen schriftelijke annuleringen worden geaccepteerd. Wanneer u verhinderd bent is het ook mogelijk iemand anders in uw plaats aan deze conferentie te laten deelnemen.

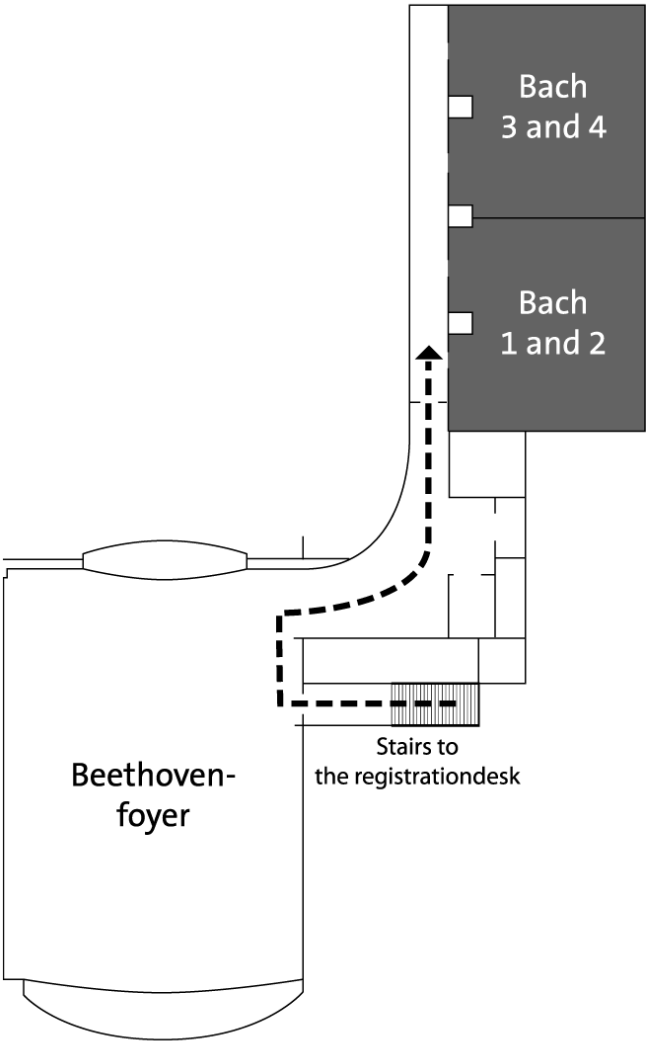
Plattegrond treinstation



Plattegrond locatie



Plattegrond locatie



Expositie en sponsoring

Ook tijdens deze NLUUG-conferentie staat er weer ruim 300 vierkante meter expositieruimte ter beschikking voor geïnteresseerden. Deze expositie staat tevens in het teken van het conferentiethema: Security & Privacy.

Tevens zijn er diverse andere mogelijkheden tot sponsoring.

Voor meer informatie over deelname aan de expositie en/of andere mogelijkheden tot sponsoring kunt u contact opnemen met ons organisatiebureau:

Organisatie- en Congresbureau Interactie
Horapark 9
6717 LZ Ede
T: 0318-693501
F: 0318-693365
E: info@interactie.org

Information for our foreign guests

The NLUUG is the association of (professional) Open Source and Open Standards users in the Netherlands. Since the late seventies, the NLUUG has brought together the community of systems administrators, programmers, researchers and IP network professionals. The primary goal of the NLUUG is to extend the application of, and knowledge about, open systems and UNIX.

The NLUUG conferences are held at:

Hotel en Congrescentrum ReeHorst
Bennekomseweg 24
6717 LM Ede (Gld)
The Netherlands
Phone: +31 (0)318 750 300
http://www.reehorst.nl

ReeHorst is conveniently located at walking distance (about 10 minutes) from train station Ede-Wageningen.

Arriving from Amsterdam Schiphol Airport
If you arrive at Amsterdam Schiphol Airport, do not take a taxi to the hotel, this will cost you approximately 200 euros! Instead, buy a train ticket to "Ede-Wageningen", the cost for a single fare is € 13.50 in second class or € 23.00 in first class. From Amsterdam Schiphol Airport, take the train to "Treinstation Nijmegen" from platform 3 and you can go directly to "Ede-Wageningen". When you take the train to "Treinstation Utrecht" from platform 1-2 get off at "Utrecht Centraal Station" and from there take the train to "Ede-Wageningen". When you arrive at Ede-Wageningen, follow the sign to the Reehorst.

Arriving from Rotterdam Airport
If you arrive at Rotterdam Airport, take the bus to Rotterdam Centraal Station (every 10 minutes), take the train to Utrecht Centraal Station and change to catch the train heading in the direction of "Ede-Wageningen". The cost for a single fare is € 14.70 in second class or € 25.00 in first class.

ICE high speed train
If you arrive with the ICE high speed train from Germany, change at Arnhem station to catch the train heading in the direction of "Ede-Wageningen". More information on the Dutch railway system is available on their website: http://www.ns.nl/en

Registration
Please register in advance. This is the only way we can guarantee there will be a badge and a conference folder for you and enough food and drinks.

Registration for the conference will be open at the Reehorst on Thursday November 11, registration opens at 8:30. During registration, you will receive your badge, a conference bag with the schedule, the proceedings and some goodies.

NLUUG
Members of the NLUUG or sister associations (incl. GUUG, UKUUG and USENIX) pay € 135.00 for the day. Student members of the NLUUG pay € 26.00 per day. Non NLUUG-members pay € 290.00. It is usually cheaper to register as an NLUUG member first.

See the NLUUG website at http://www.nluug.nl for more information about how to become a member of NLUUG and other benefits for NLUUG members. All registrations through the NLUUG website will have access to the NLUUG sessions on November 11, 2010.

All participants have to pay the VAT, including all employees of European companies. Your accounting department will know how to get the VAT refunded. Students will have to prove their status by bringing a valid student ID card and showing it at the registration desk.

Payment
In the Netherlands, it is very customary to wire money in advance or use debit cards to pay at the conference. We do also accept cash payments at the registration desk.

Your registration is only considered complete if:
1. We have confirmed your registration by e-mail and
2. We received your payment before November 4, 2010

Advance payments can be wired to ING account 2353318 for "NLUUG". Please indicate the invoice number from your confirmation.

For non-Dutch attendees:
IBAN: NL77 ING 0002 3533 18
BIC/SWIFT: INGBNL2A

If you have not received any confirmation within 7 days of your registration, please contact the NLUUG office:
buro@nluug.nl
phone: +31 (0)318 694416

If your payment has not been made before November 4, 2010, you will have to pay at the registration desk. You can use PIN (Maestro) or pay cash.

The first 75 (paid) NLUUG registrations will also receive a free Early Bird gift.

Cancellation policy
Cancellations must be submitted in writing to Interactie bv before October 28, 2010. A € 35,- administration fee will be charged. No cancellation requests will be accepted after October 28, 2010.