

Opmerking: helaas zijn sommige lange opmerkingen niet volledig overgekomen, onze excuses hiervoor.

workshop	Interesse	Prioriteit
	Cryptologisch Onderzoek en onderzoek aan Side Channel Attacks	Kansen geven aan de beste crypto-analyticus ter wereld
	De verankering van IT-security in het ondernemingsbeleid en in de enterprise architectuur van de onderneming. Er moet een einde komen aan de lappendeken van weinig coherente (deel-) oplossingen.	Security dient strategisch te worden ingestoken. Er moeten in een onderneming op concernniveau security principes worden vastgesteld die leidende zijn bij de verdere implementatie van security maatregelen. Sommige security principes staan op gespannen voe
	Het programma KWINT (kwetsbaarheid internet), een privaat-publiek samenwerkingsprogramma (EZ + ECP.NL) loopt eind van dit jaar af. Wij maken op dit moment - in opdracht van EZ - een nieuw programma voor Veilige Elektronische Communicatie (looptijd 3 jaar)	Wij lopen aan tegen diverse vraagstukken, zoals: = waaraan heeft het MKB nu behoefte als het gaat om informatiebeveiliging? = kan er een lichte variant van de BS7799 ontwikkeld worden of niet? = hoe segmenteer je MKB-ers t.b.v. een gerichte doelgroepbenad
	Identity Management Trust Mobile Security Context Aware Security	Hoe op een dynamische manier trust te creëren tussen verschillende entiteiten (users, services, sensors, etc.) - Context (location, velocity, temperature, heartbeat, behaviour)aware security
	Ik kom niet wegens meeting in het buitenland, EU project.	
	Moderator van één van de workshops	
	Secure identification technology (e.g. biometrics)	
	Video observatie via IP Netwerken ten behoeve van security en service doeleinden	storage of data
A	Bescherming Vitale Infrastructuur, informatiebeveiliging SCADA/proces control systemen	Hoog (EU is R&D netwerk op dit gebied aan het opzetten)
A	Cryptografische toepassingen in de informatiebeveiliging.	Nauwe aansluiting met het bedrijfsleven. Direct toepasbaar op bestaande of nieuwe producten en diensten.
A	Honeypots IDS Patchingsystemen Flow analyse Incident response	Flow analyse Security awarenes Patchingsystemen
A	Informatiebeveiliging	Match tussen onderzoek en toepassing verbeteren.
A	Integratie van beveiliging van IT-voorzieningen in operationele en tactische sturing van organisaties.	Integratie van beveiliging van IT-voorzieningen in operationele en tactische sturing van organisaties.
A	Juridische aspecten informatiebeveiliging	Het integreren van de juridische (en maatschappelijke) vraagstukken van ICT-security-onderzoek, direct vanaf de start van het onderzoek (en niet gaandeweg)
A	Netwerk security in het bijzonder	hoog
A	Netwerken, besturingssystemen, security, wormen	bestrijding van snelle wormen die zichzelf versturen over encrypted channels (en vooral die waarvan nog geen signalement bekend is)
A	Privacy en anonimiteit	Onderzoek naar bescherming persoonsgegevens, zowel vanuit een rechten-oogpunt (wie mag welke gegevens bekijken, veranderen, doorspelen en hoe kun je met dergelijke autorisaties omgaan) als vanuit een mogelijk-oogpunt (hoe kun je simpelweg voorkomen dat ie
A	Risk Management & Business Continuity	Praktisch toepasbaar Door industrie en eindgebruiker
A	Security protocollen Ad-hoc/mobiele/sensornetwerken Threat modeling DRM Security in bancaire omgeving	
A	Web Services security	access control Internet denial-of-service attacks
B	Architectuur van informatie beveiliging.	Geheimhouding in sensor clouds.
B	Device security	
B	mobile security	
B	Security & Tokens	
B	security, distributed systems, sensor networks, protocols, RFID	
B	smartcards (secure devices) software security	
B	strategieën in het beveiligen van informatiesystemen, methodieken om de kwaliteit van beveiligingsoplossingen te meten (metriek) en tactische uitvoeringen van test scenario's met als doel om beveiligingsoplossingen in de praktijk te kunnen beproeven (bijv	Onderzoek naar een metriek om de kwaliteit van de beveiligingsoplossingen te meten en onderzoek naar nieuwe beveiligingsmethodieken. Bijvoorbeeld het meten van de hoeveelheid Shannon-informatie in gecodeerde berichten.
B	Technische ondersteuning PC gebruik, incl security	Zeer belangrijk
B	Zelf organiserende Sensor Netwerken en de security daarvan	Hoге prioriteit
C	architectuur en mobiele beveiliging	
C	Bij de NVB in het beveiligingsoverleg worden interbancair afspraken gemaakt over standaards en minimumeisen. In dat kader ben ik ook geïnteresseerd in innovatie en wetenschappelijk onderzoek: zover dit niet concurrentievervalsend	Mogelijk is de toegevoegde waarde van IPv6 interessant. Rekenen onder crypto kan interessant zijn. Biometrie is een andere LT-trend die mogelijk interessant is.
C	Biometrie	Biometrie
C	Biometrie	Goede integratie van biometrische herkenning in beveiligingssystemen en aandacht voor "convenience" aspecten.
C	Certificering. Access management Awareness	Praktische standaardisatie Laagdrempeligheid
C	Communicatie en voorlichting over informatiebeveiliging.	Verbetering communicatie over informatiebeveiliging, een nog steeds ondergeschoven kind. Juiste en doordachte voorlichting over beveiliging maakt dat ingevoerd beleid en opgestelde maatregelen daadwerkelijk effectief zijn.
C	Cryptography, Secure Computing, Private Matching, Biometrics, Mobile Software Agents	
C	Face recognition	Belangrijk
C	Identificatie op het gebied van safety (biometrie, intelligent cameratoezicht).	Veel doorbraken komen niet van de grond omdat naast technologische belemmeringen er complexe (publiek-private) samenwerkingen vereist zijn of ondernemers het risico niet nemen (mbt financiering, regelgeving). Een integrale onderzoeks-aanpak is daarom nodig
C	IT Security bij banken.	
C	oriënterend; alg security beleid	
C	PKI, intrusion detection	hoe Nederland beveiligen tegen terroristische aanvallen via het Internet
C	Privacy van contact informatie	
C	Reflectie op security: wijsgerige, historische en sociale aspecten van computerbeveiliging. In het bijzonder authenticatie en vertrouwen. Informatica en samenleving.	Trust and security. Security and civil society

workshop	Interesse	Prioriteit
C	Secure Identification	In het kader van de huidige ontwikkelingen rondom het gebruik van digitale handtekeningen zoals in het nieuwe e - passport en Nationale identiteitskaart het doorvoeren van deze identificatie middelen in de ICT infra structuren om op deze wijze een uniform
C	Security & Privacy of Information Systems	o.a.: - Privacy-vriendelijke legitimatie i.p.v. ongebreidelde identificatie. - Simpel gebruik van makkelijk te onthouden wachtwoord (pincode), maar dan wel met goede bescherming tegen 'shoulder surfing'. - Simpel beheer voor gebruiker (en simpel gebruik)
C	Software security, identity management @ privacy security protocols, societal aspects of security.	
D	Authenticatie en autorisatie van processen, services, etc. in open netwerk systemen (bijv. in Grid omgevingen). Wellicht speelt trust een rol als niet alle principals (root) certificates kunnen overleggen bij maken van contact. Rol van mobiliteit in secu	
D	Beveiliging van wireless sensor networks.	
D	Cryptografie, m.n. Distributed Trust Management Searching in encrypted data	
D	data stream mining, fraud detection, detection of misuse of information systems, web mining	data stream mining, distributed data mining
D	De systemen worden steeds opener als het gaat om het uitwisselen van informatie. De kennis over de beveiliging is voor ons een punt van aandacht	Zal steeds belangrijker worden
D	Digital media watermarking and fingerprinting, Peer-to-Peer networks, Rights management, Secure media computing/signal processing	
D	Digital Rights Management, content protection, controlled distribution, video and audio, encryption technologies, smartcards, embedded systems, multiplatform developments (Windows, MacIntosh, Linux)	Hoe de samenwerking tussen organisaties en kleinere bedrijven te stimuleren zonder tender procedures.
D	DRM, Copyprotection, (Home) Network security, Tamper resistance	
D	IT-Governance (IT beleid) Prestaties met IT Risico's verbonden aan IT Waardering van IT	Hoe zorg ik ervoor dat mijn gegevens mijn gegevens blijven en dat ik er de vruchten van pluk? Als ik derden, opdrachtgevers, klanten, wil laten zien welke gegevens ik heb zonder deze meteen weg te geven, wat moet ik dan doen? Welke mogelijkheden heb ik mi
D	security policies kosten/baten analyse van security integratie fysieke en digitale security	kosten/baten analyse van security integratie fysieke en digitale security
D	Software	interdisciplinaire validatie van onderzoeksresultaten dmv modeleren en simulatietechnieken.
D	Trust Management, Access Control, Virtual Communities.	
D	zoeken in ge-encrypted data	
	Biometrie	
	Cryptologie	
	decentralisatie van content -interoperabiliteit -secure agent technology	sociale "awareness" -onderzoek naar social engineering -zo veel mogelijk decentraliseren -semantiek toevoegen aan content die beveiligd dient te worden, waardoor juiste techniek geselecteerd kan worden
	Decentralized Trust Management, Logic Programming	
	Distributed systems security, trusted computing, digital rights management.	
	In de olie en gasindustrie worden gebruik gemaakt van zowel de proces domein als office domein. wat van belang is dat je vanuit office domein incidenteel in de proces domein het e.e.a in de proces installatie moet kunnen wijzigen. deze handeling moet echt	het is van belang met concrete oplossingen (standaarden) te komen om fenomenen als hackers, virussen, usb, laptop hangen aan bedrijfsnetwerken dat hiervoor security spelregels voor komen.
	Interim & project management ICT	Content moet beter beschermd en beveiligd worden tegen ongeoorloofd gebruik en kopiëren
	Netwerk- en applicatiebeveiliging	
	Network Security ... Access Control	
	RFID + Security	Toegepaste beveiliging
	security analyse security protocollen	
	Security at network level and at service level, security of the traffic and applications in personal networks	user centric security
	Security en architectuur	Security en architectuur, met bijzondere aandacht voor integriteit van het ontwerp en het gebruik van organisaties, processen en systemen, zodat "bijvoorbeeld" grotere bedrijven op efficiënte wijze deugdelijke (af)rekeningen kunnen versturen.
	Security in Networking	
	Smart cards security	
	software security assessments d.b.v. broncode analyse	Naast huidige onderzoek ook aandacht voor detectie van vulnerabilities en malicious code in broncode en executables
	software/web security	
	Wireless security, security in health, security in emergency networks	Wireless security