

Sessie B: device security

Verslag: Erik Poll

Aanwezig:

De heer	Drs.	J.L.M. de Haas	CISSP	JCC
De heer	Dr.	J. Kerling		Lenovo International B.V.
De heer		E. Poll		Radboud Universiteit Nijmegen
De heer	Ir.	J.P. van der Burg		VZG Communications
De heer	B.Sc	J.E.F.K. van Zwietering		VZG Communications
De heer	Dr.	M.D. Oostdijk		Radboud Universiteit
De heer	Drs.	H. Braams		VASCO Data Systems B.V.
De heer	Dr.	B. Crispo		Vrije Universiteit Amsterdam
De heer		K.H.W. Pasman		TNO Defensie en Veiligheid
De heer		R. Wichers Schreur		Radboud Universiteit Nijmegen
De heer	Dr.	J.I. den Hartog		Universiteit Twente
				Ministerie van Economische Zaken
De heer	Drs.	E.R. Buddenbaum		Zaken
De heer	Dr.	W.P.G. Mooij		Irdeto Acces
De heer	Ir.	M.F. Witteman		Riscure
De heer	Dr.ir.	A.M. Bos		Chess
De heer	Dr.	S.O. Fehr		CWI
De heer		H. van Kuilenburg		Vicar Vision
				Centrum voor Wiskunde en Informatica
De heer	Dr.	D. Hofheinz		Informatica
De heer	Ir.	H.A.M. Luijff		TNO Defensie en Veiligheid
De heer	Dr. ir.	H.J. Bos		Vrije Universiteit
Mevrouw		A.K. Zych		Universiteit Twente
De heer	Prof.dr.	P.H. Hartel		Universiteit Twente
De heer	Prof.dr.	W. Jonker		Philips Research

De afbakening van het onderwerp voor deze workshop, "device security", leidde tot de nodige discussie.

Een eerste punt van discussie was over wat voor devices het zou moeten gaan, en of de discussie zich moest beperken tot bijvoorbeeld enkel smartcards en RFID tags, of een bredere klasse van devices, en zo ja hoe breed: mobiele telefoons, settop boxen, mp3-spelers, of ook PC's? Marc Witteman (Riscure) suggereerde de discussie te beperken tot devices die in enige mate tamper-resistant zijn, maar als snel kwam in de discussie naar voren dat juist software draaien op onvertrouwde hardware een uitdagend onderzoeksgebied is. Als andere reden om de workshop niet tot smartcard te beperken werd opgemerkt dat smartcards, net als cryptografie, meestal niet de zwakste schakel is in de security keten.

Een ander discussiepunt was of we ons moesten richten op onderzoeksvragen over een device in isolement, of over het device als onderdeel van een groter systeem. Ed Buddenbaum van Buitenlandse Zaken suggereerde dat onderzoeksvragen in deze workshop over device security zich primair moest richten op de security van het device zelf, zodat secure devices daarna als bouwsteen konden dienen in een groter systeem of organisatie. In reactie hierop vonden anderen juist dat er veel interessante onderzoeksvragen lagen in de rol van secure devices in groter geheel, en in methodologieën om in een gegeven context vanuit de eisen voor een systeem aks geheel te komen tot een weloverwogen keuze voor het gebruik van secure devices, en tot exacte eisen aan deze secure devices.

Marc Witteman (Riscure) had een uitgebreide inventarisatie van onderzoeksonderwerpen voorbereid, op gebied van

- Security design (Coding, Card/key/version management, requirements)
- Open issues in Hardware (Sensitivity to environmental parameters, Detection of environmental anomalies, Eavesdropping, Reduction of signal leakage)

- Open issues in Operating Systems (Fault detection, Error recovery, Leakage-free crypto, High-Order Side Channel attacks, Security of virtual machines, OS Security on non-secure hardware)
- Open issues in Applications (Vulnerabilities, Robustness, Usability vs security, Protocol weaknesses, Bad use of APIs)

Wim Mooij (Irdeto) noemde ook nog software tamper resistance als belangrijk onderzoeksgebied, en het beoordelen van de security van een computer-infrastructuur bestaande uit al dan niet tamper-resistant hardware en software. Wat betreft het laatste is vooral het gebrek aan goede metrieken voor het meten van security (meer in het bijzonder voor software tamper-resistance) een groot praktisch probleem. Dit leidde tot discussie in hoeverre het mogelijk zou zijn zulke metrieken op te stellen, en de fundamentele beperking dat metrieken alleen maar bekende security-problemen in acht kunnen nemen en nooit met nieuwe aanvallen rekening kunnen houden.

Wim Jonkers (Philips) en Bert Bos (Chess IT) noemden goedkope devices met zeer beperkte mogelijkheden als een interessante klasse van devices om onderzoek naar te doen. Meer in het bijzonder noemde van der Burg (VZG) cryptografie voor dit soort devices, met beperkte rekenkracht, als onderzoeksvraag.

Uiteindelijk werd er in kleinere groepen op specifieke vragen verder gediscussieerd, wat leidde tot drie concrete ideeën voor mogelijke onderzoeksvorstellen:

- **Veilige toepassingen op onveilige devices**
 Marc Witteman (Riscure), Martijn Oostdijk (RU), Pieter Hartel (UT), Ronny Wichers Schreur (RU)
 Centrale onderzoeksvraag hier is hoe een veilige applicatie op onveilige, niet tamper-resistant, hardware gerealiseerd kan worden. Toepassingsgebied zijn (embedded) devices waar een zekere mate van beveiliging moet worden geboden, en zoals mobiele telefoons en televisies.
- **Netwerk van goedkope sensoren met beperkte middelen**
 Bert Bos (Chess), H. Braams (VASCO Data Systems), Bruno Crispo (VU), Rieks Joosten (TNO Telecom), Melanie Rieback (VU), Anna Zyck (UT)
 Centrale onderzoeksvraag hier is hoe een (mogelijk draadloos) netwerk van simple sensoren met beperkte resources (zowel qua opslag, als rekenkracht, en mogelijk een korte levensduur) beveiligd kan worden. Concreet voorbeeld van zo'n netwerk is een systeem om bosbranden te detecteren, met sensoren met op batterijen of zonnecellen werken, wat flexibel is in deployment en hoge garantie biedt tegen valse alarms.
- **Breedband TV**
 Wim Mooij (Irdeto), Jerry den Hertog (UT), Jenno van Zwietering (VZG)
 De vraag hier was de beveiliging van de verspreiding van TV/video over breedband internet connecties naar een heterogene collectie apparaten (TVs, TV emulaties op PCs, ...) die dit afspelen. Een van de onderzoeksvragen hier is het uniek maken van de van de ontvanger, met behulp van bijvoorbeeld sleutels, of van digitale vingerafdrukken van de hardware, aan de hand van karakteristieke kenmerken van de devices.