Vrije Universiteit, Faculteit Exacte Wetenschappen,
Afdeling Informatica

Tentamen **Pervasive Computing**
18 december 2008 12:00–14:45

Uitwerkingen

Dit is een gesloten boek schriftelijk tentamen.
Tijdens het tentamen mogen geen schriftelijke of elektronische artikelen worden geraadpleegd.
De antwoorden kunnen in het Nederlands of Engels gegeven worden.

Minimaal 5.5 voor het huiswerk is vereist voor het deelnemen aan het tentamen.
Minimaal 5.5 voor het tentamen is vereist voor een voldoende voor het hele vak.
Er zijn 6 tentamenvragen, Q1..Q6 en de som ervan is maximum 90p.
Het tentamencijfer wordt berekend als: (Q1+Q2+…Q6+10)/100
Het eindcijfer is berekend als 0.3*huiswerk + 0.7*tentamen.
Een eindcijfer >=5.5 betekent een voldoende voor dit vak.

	Q1	**Q2**	**Q3**	**Q4**	**Q5**	**Q6**	**ΣQi**	**Maximum = (ΣQi+10)/10**
a)	**3**	**3**	**8**	**5**	**5**	**5**		
b)	**3**	**3**	**8**	**5**	**5**	**5**		
c)	**4**	**4**	**6**					
d)		**5**	**6**					
e)		**7**						
Totaal	**10**	**22**	**28**	**10**	**10**	**10**	**90**	**10**

1. Pervasive Computing Algemeen [10p]

a) Marc Weiser zegt in zijn artikel "The computer for the 21st Century": "The most profound technologies are those that disappear". Geef een voorbeeld van een dagelijkse technologie die aan dit criterium al voldoet. [3p]

b) Deze vraag gaat over de specifieke artikelen van huiswerk HW1 die jullie groep gelezen heeft. Voor een van de twee projecten beschrijf een eigenschap die volgens jullie de applicatie pervasive maakt. [3p]

c) Noem en beschrijf 4 uitdagingen (challenges) die pervasive computing met zich meebrengt. [4p]

---

a) Here diverse examples are possible: The writing technology, the glasses, electrical motors, etc. IT is good if the student also specified why is this a good example.
b) For example: in Lifetrack the music is suggested that matches your activity. Wikicity gives suggestions about what route should you follow due to traffic congestion, etc. It is important to see that students have read their articles.
c) There are more than 4 challenges: scalability, device heterogeneity, device mobility, invisibility, context-awareness, energy management, coping with uncertainty, etc. See article Saha & Muherjee . Each term should be explained.

2. Computer systemen [22p]

a) Wat beweert de wet van Moore? [3p]

b) Wat is een device driver? [3p]

c) Hoeveel adreslijnen zijn nodig voor een 1-byte brede 24 Mbyte geheugen? [4p]

d) Welke bits zijn naar de computer gestuurd als je op het toetsenbord het woord Lego toetst? (ASCII code is te vinden in de bijlage) [5p]

e) Noem de belangrijke componenten van een CPU. Laat stapwijs zien wat gebeurt in een CPU bij uitvoering

van de instructie 5 + 2. [7p]

a) Moore's law: the number of transistors that can be packed inexpensively on a chip doubles approx. every two years.
b) Device driver: small program used to communicate with peripheral devices (monitors, printers, video cards, etc)
c) 1Mbyte = 2^20 bytes. 16Mbytes =2^24 bytes. 32 Mbytes = 2^25 bytes. So we need 24 lines for 16 Mbytes and 25 lines for 32Mbytes. 24Mbytes is in between, but it requires all 25 lines – you cannot have a fraction of an address line!
d) 01001100 01000101 01000111 01001111
e) The main components of a CPU (from Morley's book p. 81) Arithmetic/Logic Unit (ALU) a floating point (FPU), Control unit. Prefetch unit. Decode Unit. Internal Cache and registers, Bus interface unit. What happens when 5+2 command is processed has to be described in 4 steps, like in the book at page 85. Or like the Intel museum tour demo used during the lecture shows.

---

3. Computernetwerken [28p]

a) Noem 2 types fout-detecterende codes die gebruikt worden bij datatransmissie in netwerken, en beschrijf kort hoe ze werken [8p]

b) Leg uit waarom fragmentatie nodig is en hoe het werkt in het IP protocol. [8p]

c) Wat is het verschil tussen transmission delay en propagation delay in een packet-switched netwerk? [6p]

d) Hoe werkt het CSMA/CD protocol? [6p]

a) Any 2 of these 3 are OK: parity bit, check sum (used by UDP and TCP) or CRC (used by Ethernet). A parity bit is the simplest error detecting code. It is a bit added by the sender to the transmitted message in order to enable a check on the correctness of the transmission. There are 2 types of parity bits: even and uneven. For even parity the added bit ensures that the sum of all 1 bits in the message is even.
For example if this string has to be sent:
01000001 (has an even nr. of 1s)
Then in case of an odd parity, the parity bit added has to be an 1, so that the total pattern has an odd nr. of 1's.

The receiver can calculate the sum of the total pattern 1's and detect a possible transmission error.
The checksum is calculated by binary adding all the transmitted words and then performing a 1's complement of the sum. It is part of the header of different network protocols.

b) Fragmentation is necessary because each network link has a MTU maximum transfer size largest possible link-level frame length that it can carry. Large IP datagrams are divided (fragmented) in shorter fragments (aprox. MTU) that travel independently. The reassembly happens at the destination. The IP header (offset, flag) is used to identify and order related fragments. Offset shows the place of the fragment in the datagram. Flag is 1 for all fragments except for the last fragment.
c) Transmission delay is the amount of time required for the router to push out a packet: it is a function of packet's length and the transmission rate of the link., but does not depend on the distance between 2 routers. The propagation delay is the time it takes a bit to propagate from one router to the next. It depends on the distance between the routers but not on the packet length or transmission rate of the link.
d) CSMA/CD is a multiple access control (MAC) protocol used by Ethernet. It means carrier sensing multiple access /collision detection. A network card (NIC) creates a frame and senses the channel. If channel is idle, it starts frame transmission. If frame can be sent without collisions, NIC is ready with the frame. If collision is detected during sending the frame, transmission is aborted and a jam signal is sent. After aborting, NIC waits a random time by entering a so-called exponential backoff. Until the channel is again idle.

---

4. Sensoren [10p]

a) Kan de topologie van een WSN spontaan veranderen? Zorg dat je jouw antwoord motiveert! [5p]

b) Noem 3 sensoren uit de Lego Mindstorms set en 2 fysiologische sensoren en leg uit wat ze precies meten. [5p]

---

a) Yes. Because sensors can go to sleep, can run out of batteries or different interference factors can disturb their functioning.
b) Here more answers are possible. Ultrasound: measures the distance to an object by sending a sound and measuring the round trip time. Microphone: measures the ambient sound level. Light sensor. Sends a light beam and measures the reflected light or measures the ambient light.
Finapress measures the oxygen level in blood, Galvanic skin response: measures the resistance between 2 point on the skin when a small electrical current is applied to the body.

5. Lokalisatie [10p]

a) Hoe werkt time-of-arrival lokalisatie techniek? Wat is haar grootste nadeel? [5p]

b) Wat is GPS? Welke lokalisatie techniek wordt gebruikt in GPS? Welke parameters krijgt een user van de GPS? [5p]

---

a) A sender station A sends a radio signal and the receiver station B measures the time until it gets this signal. The distance between A and B is then d = c * t, where c is the speed of the signal, usually speed of light in air 3x10^8m/s. The problem is that the clock used by the receiver and the clock used by the sender might not be synchronized.

b) GPS (Global Positioning System) is a constellation of 24 satellites that provide navigation data to military and civilian users all over the world. It uses time of arrival localization technique. The data a user (GPS receiver) can obtain from a GPS are 3 user coordinates (longitude, latitude, height) and the universal coordinated time (UTC).

6. Privacy en security [10p]

a) Deze vraag gaat over het HW4 artikel over MasterKey. Wat is een traditionele master key? Hoe hebben de auteurs van MasterKey approach de privacy probleem van authentication opgelost? [5p]

b)Wat is RFID malware? Noem en beschrijf 3 mogelijke vormen van RFID malware. [5p]

---

a) A traditional master key is designed to enable accessing multiple locks with a single key. A standard authentication protocol sends identification in clear text. The authors used exchanges in code words to protect privacy information. The code is secretly shared between the master key and the lock.

b) Malware is short for malicious software, whose main purpose is to break into and disrupt computer systems. By extension, *RFID malware* is malware that is transmitted and executed via an RFID tag.

An *RFID exploit* is malicious RFID tag data that "exploits" some part of the RFID system that encounters it. RFID systems are susceptable to hacker attacks, just like conventional computing systems. When an RFID reader scans a tag, it expects to get back information in a certain format. However, a malicious person can write carefully crafted data whose format and content is so unexpected that it can corrupt the RFID reader's software and potentially its database.
An *RFID worm* is an RFID-based exploit that abuses a network connection to achieve self-replication. RFID worms may propagate by exploiting online RFID services, but can also spread via RFID tags. The RFID worm code causes unsuspecting RFID servers to download and execute some file from a remote location. This file then proceeds to compromise the RFID middleware server in the same fashion as most Internet-based malware. The worm infected RFID software can then "infect" new RFID tags by overwriting their data with a copy of the RFID worm code.

An *RFID virus* is an RFID-based exploit that autonomously self-replicates its code to new RFID tags, without requiring a network connection. RFID viruses may or may not have a payload, which modifies or disrupts the workings of the back-end RFID system. Once the newly-infected RFID tags are sent on their way, they infect other RFID systems (assuming use of the same software system). These RFID systems then infect other RFID tags, which infect other RFID software systems, etc..

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

Source: www.pubblinet.com

Bijlage: ASCII code