

# elektro DATA

3

Jaargang 23  
maart 2004

## Inhoud

X

nieuwe  
producten

Sense  
of Contact  
march 23  
www.fhi.nl/senseofcontact

**NATIONAL  
INSTRUMENTS™**  
zie pagina 3

**ADVIES**  
MACHINEBOUW & ELEKTROTECHNIEK  
zie pagina 36



Vakblad over industriële elektronica en  
industriële automatisering voor Nederland en België



*Chip voorkomt diefstal van identiteit*

## Hardwarebeveiliging tegen virussen

Alarmerende berichten over nieuwe computervirussen zijn de laatste tijd aan de orde van de dag. Kennelijk schept een aantal al dan niet begaafde programmeurs er genoeg in om anderen het leven zuur te maken. Gelukkig zijn er dan ook weer technische 'ghostbusters' die de plagen effectief bestrijden.

Halfgeleiderfabrikant Atmel introduceert een hardwareoplossing voor het virusleed.

Nu het Internet zo ongeveer gemeengoed is geworden, valt ook een enorme toename te constateren van de zogenoemde Internetcriminaliteit. Die manifesteert zich bijvoorbeeld in de vorm van hacking of van worms, waarbij informatie wordt gestolen van het slachtoffer. Worms zoeken naar gaten in de beveiliging van netwerken of servers en dringen vervolgens via die gaten binnen, om dan het netwerk plat te leggen of te verstoren. Hackers maken gebruik van het feit dat in veel computers, PDA's en mobiele telefoons geen beschermende

maatregelen zijn genomen. Bij virussen en spam neemt het slachtoffer zelfs ongewild actief deel aan de criminaliteit. Trojans en virussen verspreiden zich via de e-mail en doen dan hun vernietigende werk in de geadresseerde computers. Het virus Blaster infecteerde binnen een week 500 000 computers en richtte daarbij een schade aan van naar schatting een miljard euro. En het virus MyDoom bleek zich sneller te verspreiden dan al zijn voorgangers: een op de

*Vervolg op pagina 7*

[www.engineersonline.nl](http://www.engineersonline.nl)

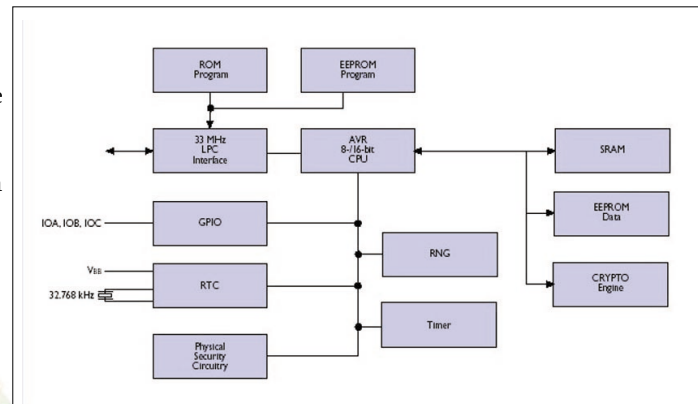
twalf PC's raakte ermee besmet. Een andere vorm van computercriminaliteit is die waarbij het slachtoffer wordt overgehaald om vertrouwelijke informatie – bijvoorbeeld zijn creditcardnummer – af te geven. Gewoonlijk wordt de internetcriminaliteit bestreden met antivirus-software en beveiligingssoftware. Jammer genoeg is het antivirus-wapen meestal pas beschikbaar nadat het virus zijn eerste schadelijke werk al heeft verricht en beveiligingssoftware betekent soms niet meer dan een extra uitdaging voor de kwaadwillende.

### Trusted Computing Group

Om te komen tot een effectieve bestrijding van de computercriminaliteit hebben de ICT-bedrijven Intel, Microsoft, AMD, IBM

daarvoor toestemming geeft. Geen enkel ander systeem kan doen alsof het de computer van deze eigenaar is. Verder geeft de TPM - alleen voor de eigenaar - de mogelijkheid om hem aan- of uit te schakelen, om het gebruikerswachtwoord te veranderen en om bepaalde opties te wijzigen.

Atmel stelt dat met de onlangs door deze firma geïntroduceerde TPM-chips 'identiteitsdiefstal' kan worden voorkomen. Volgens Atmel draait het bij virussen, wor-

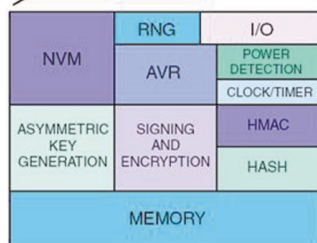


Blokschema van het IC.

## Hier nog een streamer? Hier nog een streamer? Hier nog een streamer?

en Hewlett Packard samen de Trusted Computing Group opgericht. Doelstelling van deze TCG is het creëren van open industriestandaarden voor hardware en software voor het ontwikkelen van betrouwbare computerplatforms. De groep heeft daarvoor specificaties en standaarden opgesteld, de jongste versie daarvan is de TCG1.2. Hierin worden onder meer TPM's (Trusted Platform Modules) gespecificeerd – System On Chip oplossingen voor de beveiliging van computers en netwerken. Deze TPM's verrichten in de computer diverse taken. Zo genereren zij paren sleutelcodes met behulp van een random getalengenerator. Deze sleutels worden in de TPM opgeslagen, die ze gebruikt om een signatuur te geven aan berichten en voor de decryptie van data. Verder houdt de TPM exact in de gaten wat er gebeurt als de computer wordt opgestart. De gebruiker kan later ook terug kijken om te zien wat er precies is gebeurd. De TPM identificeert de computer, maar alleen als de eigenaar van de computer

Indeling van de TPM-chip.



men en andere internetcriminaliteit altijd om 'identiteit'. Kan de identiteit van degene die data verzendt op betrouwbare manier worden vastgesteld? Kan de gebruiker, of het besturingssysteem, vaststellen dat een programma veilig kan worden gedraaid, alvorens dat ook daadwerkelijk gebeurt? Bij toepassing van TPM-chips is het antwoord op beide vragen een volmondig ja, want zij kunnen de authenticiteit en integriteit van programma's en machines verifiëren. Er zijn maar twee manieren om de chip voor de gek te houden: het kopiëren van de inhoud van de TPM of de chip verwijderen en plaatsen in een andere computer. In beide gevallen zal de TPM het systeem echter uitschakelen.

### Geen kans

Het concept van het bewaken van de identiteit kan worden uitgebreid tot de BIOS, het besturingssysteem en de catalogus van geregistreerde programma's. De catalogus wordt beschermd door het TPM-IC. Wormen en virussen zijn computerprogramma's. En als de BIOS en het OS uitsluitend de uitvoering van veilig geregistreerde programma's toelaten, hebben die wormen en virussen dus geen kans. Ook spam kan worden uitgebannen met behulp van het TPM-IC: het IC kan ervoor zorgen dat alleen e-mail wordt geaccep-


teerd van geauthenticeerde bronnen, met identificatie van de hardware waarop deze e-mail is gegenereerd. Als creditcardorganisaties en hun klanten de TPM-chip in hun systeem opnemen kunnen dieven hun slag niet meer slaan.

De Atmel-chip, de AT97SC3202, is een complete turnkey-oplossing, die volledig voldoet aan de TCG1.2 en bevat een low-power RISC-processor, een 500 ms, 2048-bit RSA cryptoversneller, een random getalengenerator, veilige EEPROM-opslag voor twintig sleutelcodes, SRAM, een timer, een real-time klok, een LPC-interface naar Intel-processoren, een tweedraads seriële interface voor embedded toepassingen en een preventieschakeling die de chip uitschakelt als iemand de inhoud ervan probeert te lezen. Andere beveiligingen van de chip zelf omvatten onder meer metalen afschermingslagen boven de actieve elektronica, versleutelde interne bussen en bescherming tegen 'aanvallen' via de timing of de voedingsspanning. De TPM's hebben unieke, niet-toegankelijke identificatiecodes, die worden gebruikt om de origine te markeren van data die vanaf het systeem worden verzonden. Bij de Atmel-chips horen drivers voor Linux, Windows 98, 2000, XP en NT4.0, en bovendien MAD- en MPD-BIOS-drivers.

De TPM is ook geschikt voor gebruik in embedded toepassingen, zoals PDA's, mobiele telefoons, kassa's en settop-boxes, bijvoorbeeld ter beveiliging van e-commerce transacties.

Henk de Vries

 [www.alcom.nl](http://www.alcom.nl)  
[info@alcom.nl](mailto:info@alcom.nl)  
(010) 288 25 00

 [www.ebv.com](http://www.ebv.com)  
[ebv.nl@ebv.com](mailto:ebv.nl@ebv.com)  
(0346) 58 30 10