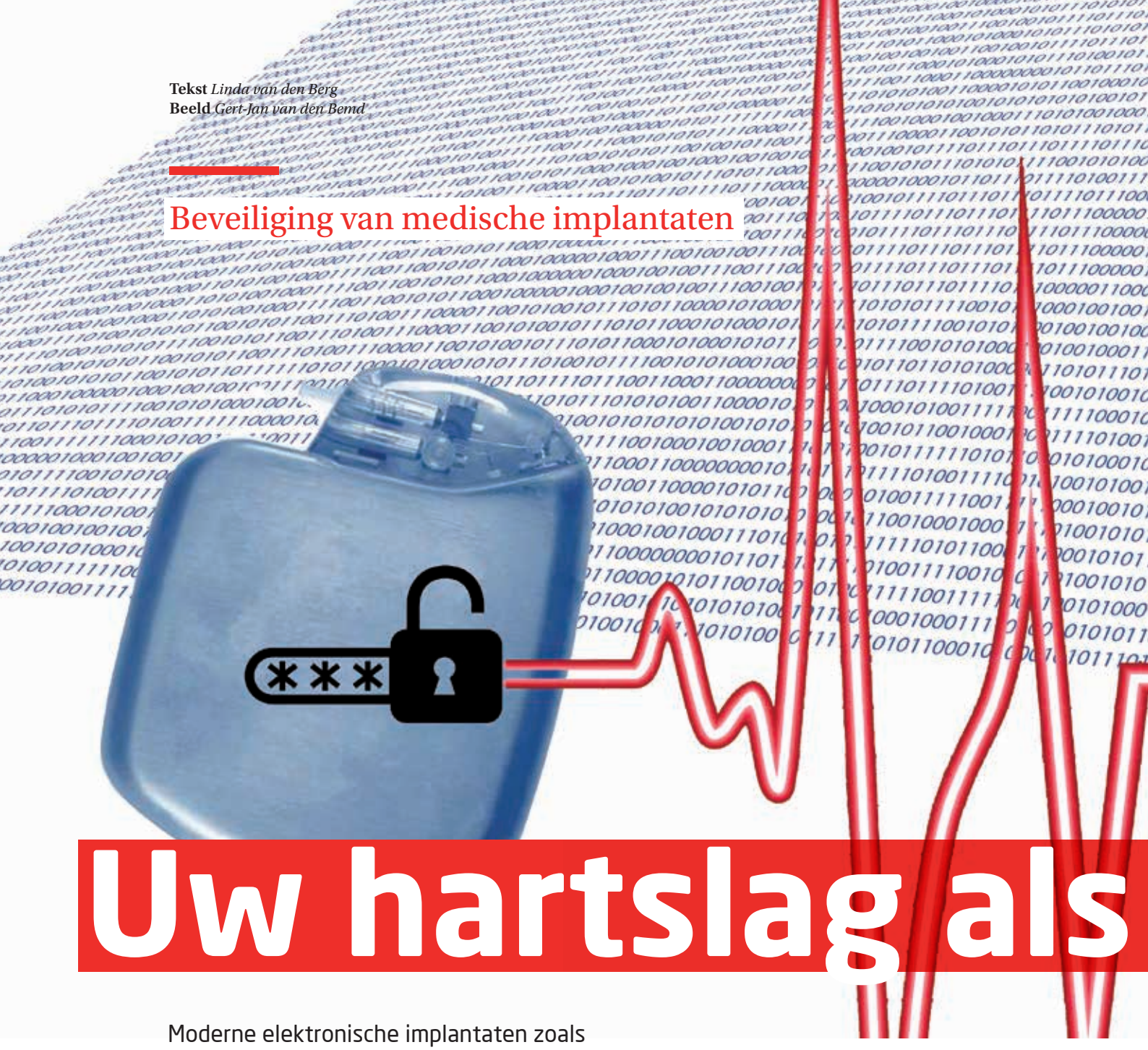
Tekst *Linda van den Berg*
Beeld *Gert-Jan van den Bemd*

Beveiliging van medische implantaten



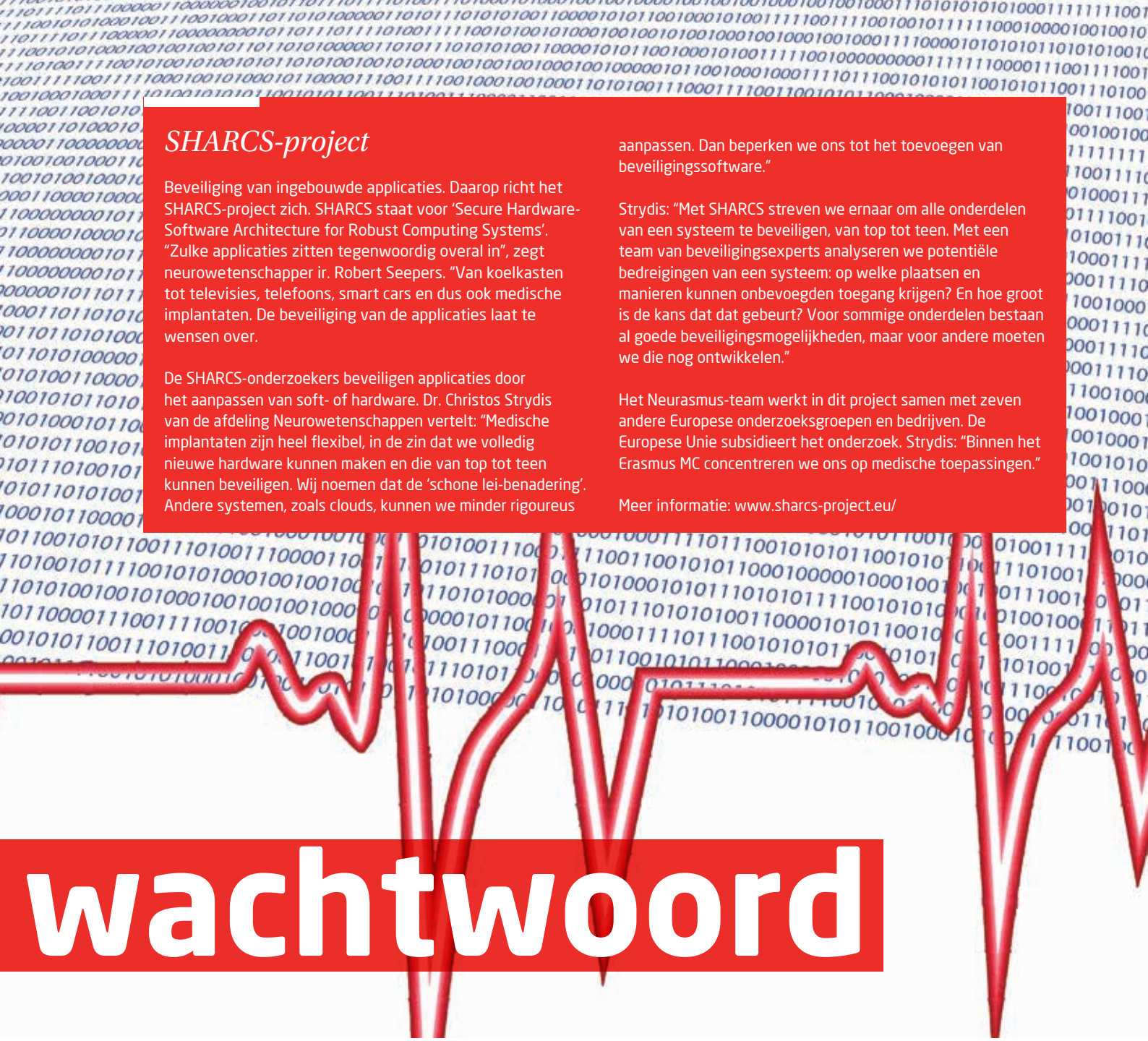
Uw hartslag als

Moderne elektronische implantaten zoals pacemakers kunnen draadloos communiceren. De apparaten zijn echter niet sterk beveiligd tegen onrechtmatige toegang. Onderzoekers van de afdeling Neurowetenschappen willen implantaten beveiligen tegen hackers met de hartslag van de patiënt als wachtwoord.

Steeds meer patiënten krijgen een elektronisch implantaat, bijvoorbeeld om het hart te ondersteunen (pacemaker). In Nederland worden jaarlijks meer dan 12.000 pacemakers ingebracht. Tegenwoordig kunnen deze apparaten ook gegevens verzamelen en opslaan, bijvoorbeeld over het hartritme. Bovendien zijn ze in staat draadloos te communiceren met andere elektronische apparatuur, zoals smartphones en computers. De patiënt kan hierdoor zijn eigen gezondheid bewaken. In het geval van een pacemaker kan hij bijvoorbeeld zien of het hartritme normaal is. Daarnaast creëert de draadloze toegankelijkheid van implantaten de mogelijkheid voor zorg op afstand. De cardioloog kan bijvoorbeeld op afstand zien of een therapie aanslaat. En bij een afwijkend hartritme kan er snel ingegrepen worden. Bovendien kunnen technische controles op afstand uitgevoerd worden, bijvoorbeeld of de batterij nog vol genoeg is en of de draden goed functioneren.

Onveilig

De draadloze toegankelijkheid van implantaten geeft patiënten en artsen dus inzicht in het ziekteproces. En het zorgt voor gebruiksgemak want de patiënt hoeft minder vaak naar het ziekenhuis. Maar er is een keerzijde. Neurowetenschapper dr. Christos Strydis: “Medische implantaten zijn momenteel niet sterk beveiligd tegen onrechtmatige toegang. In theorie kunnen hackers de patiëntgegevens dus ook uitlezen. Of ze kunnen de instellingen aanpassen (bijvoorbeeld van de maximale hartslag, *red.*), met mogelijk levensbedreigende gevolgen. De kans dat dat gebeurt is heel klein. Een hacker moet namelijk specialistische kennis hebben om in te kunnen breken. Niettemin moet er een betere beveiliging komen voor



wachtwoord

SHARCS-project

Beveiliging van ingebouwde applicaties. Daarop richt het SHARCS-project zich. SHARCS staat voor 'Secure Hardware-Software Architecture for Robust Computing Systems'. "Zulke applicaties zitten tegenwoordig overal in", zegt neurowetenschapper ir. Robert Seepers. "Van koelkasten tot televisies, telefoons, smart cars en dus ook medische implantaten. De beveiliging van de applicaties laat te wensen over.

De SHARCS-onderzoekers beveiligen applicaties door het aanpassen van soft- of hardware. Dr. Christos Strydis van de afdeling Neurowetenschappen vertelt: "Medische implantaten zijn heel flexibel, in de zin dat we volledig nieuwe hardware kunnen maken en die van top tot teen kunnen beveiligen. Wij noemen dat de 'schone lei-benadering'. Andere systemen, zoals clouds, kunnen we minder rigoureus aanpassen. Dan beperken we ons tot het toevoegen van beveiligingssoftware."

Strydis: "Met SHARCS streven we ernaar om alle onderdelen van een systeem te beveiligen, van top tot teen. Met een team van beveiligingsexperts analyseren we potentiële bedreigingen van een systeem: op welke plaatsen en manieren kunnen onbevoegden toegang krijgen? En hoe groot is de kans dat dat gebeurt? Voor sommige onderdelen bestaan al goede beveiligingsmogelijkheden, maar voor andere moeten we die nog ontwikkelen."

Het Neurasmus-team werkt in dit project samen met zeven andere Europese onderzoeksgroepen en bedrijven. De Europese Unie subsidieert het onderzoek. Strydis: "Binnen het Erasmus MC concentreren we ons op medische toepassingen."

Meer informatie: www.sharcs-project.eu/

medische implantaten." Strydis ontwikkelt samen met zijn promovendus ir. Robert Seepers een sterkere beveiliging, gebaseerd op de hartslag van de patiënt. De onderzoekers werken bij Neurasmus, een spin-off bedrijf van de afdeling Neurowetenschappen van het Erasmus MC.

Wachtwoord

Seepers legt uit hoe hun methode werkt: "Het implantaat kan de hartslag van de patiënt meten. Ieders hartslag is uniek. Het tijdsinterval tussen opeenvolgende hartslagen varieert een beetje. Wij benutten dat om wachtwoorden te maken. Er bestaan ook smartphone apps die de hartslag kunnen meten met de camera van de smartphone. Je houdt dan je wijsvinger op de camera en de flitslamp schijnt op je vinger. Dat onthult kleurverschillen die samenhangen met de doorbloeding van de vinger. De app bepaalt dan de hartslag op basis van die kleurverschillen. Wij maken hardware en software die de twee hartslagpatronen met elkaar vergelijken. De smartphone krijgt uitsluitend toegang tot implantaatgegevens als de hartslagmetingen corresponderen."

Uitdagingen

Maar de twee patronen zijn nooit exact hetzelfde. De metingen van twee verschillende apparaten zijn namelijk nooit identiek. Seepers: "Onze methode moet het implantaat goed beveiligen, maar tegelijk een klein verschil tussen de twee wachtwoorden toestaan." Een tweede uitdaging is de beperkte variatie van het hartslaginterval. Seepers legt uit: "Vergelijk het maar met een wachtwoord dat je verzint voor internetbankieren of voor je e-mailbox. Een wachtwoord met een combinatie van letters, cijfers en leestekens is veel sterker dan een wachtwoord met alleen letters. Dus hoe meer variatie, hoe sterker het wachtwoord. Wij gebruiken een wiskundige methode om de variatie in het hartslaginterval uit te vergroten. Daardoor creëren we sterkere wachtwoorden." Dit project is onderdeel van een Europees project, SHARCS (zie kader). Het doel van SHARCS is het ontwikkelen van een complete beveiliging voor ICT-systemen: van medische implantaten tot smart cars en cloud-opslagsystemen.

Toekomstperspectief

Gezondheidsapps zijn populair. Volgens The New York Times stonden er in maart 2015 meer dan 100.000 gezondheidsapps in de iTunes en Google Play stores. "Ik verwacht dat veel gezondheidsapps in de toekomst implantaten uit kunnen lezen. Wij hopen dat onze methode allerlei implantaten kan beveiligen, van pacemakers tot implantaten voor Parkinson-patiënten, maar bijvoorbeeld ook gehoorapparaten", concludeert Strydis.