UNIVERSITEIT VAN AMSTERDAM

Faculteit der Natuurwetenschappen, Wiskunde en Informatica

Science Park 107
1098 XG Amsterdam

Eerste Kamer der Staten Generaal
Aan de leden van de Vaste Commissie voor
Volksgezondheid, Welzijn en Sport / Jeugd en Gezin (VWS/JG)
Postbus 20017
2500 EA 'S-GRAVENHAGE

Betreft: Beveiliging landelijk EPD
Bijlagen: Samenvatting, Onderzoeksartikel

Amsterdam, 18 februari 2010

Geachte Commissieleden,

Uit een onderzoek naar de beveiliging van het elektronisch patiëntendossier (EPD) komen een aantal zaken naar voren die relevant kunnen zijn voor de besluitvorming rond de kaderwet EPD. In deze brief worden de belangrijkste resultaten van dit onderzoek toegelicht.

Achtergrond

De oorsprong van het onderzoek ligt in een studentenproject[1] waarin is gekeken naar de beveiliging van het EPD op basis van de AORTA documentatie[2]. Dit project heb ik begeleid als onderzoeker op het gebied van de beveiliging van grootschalige computersystemen aan de Universiteit van Amsterdam. Naar aanleiding van dit project is een uitgebreid onderzoek gedaan naar de architectuur en de protocollen die worden gebruikt in het landelijk EPD. Hiertoe heb ik onder meer de AORTA documentatie bestudeerd en overleg gevoerd met het Nictiz om helder te krijgen hoe het EPD op detailnivo werkt.

Inleiding – het Landelijk EPD

Het EPD wordt veelal gekarakteriseerd als een decentraal systeem. Patiëntgegevens zijn opgeslagen bij de zorgaanbieders die een behandelrelatie met een patiënt hebben, en die daarmee verantwoordelijk zijn voor het bijhouden van het dossier van deze patiënt. Er is dus geen sprake van een centrale database, waarin alle gegevens van patiënten worden opgeslagen. Relevante dossierstukken, zoals professionele samenvattingen, worden aangemeld bij het centrale deel van het EPD, het Landelijk Schakelpunt (LSP), dat zorg draagt voor het koppelen en transporteren van de decentrale gegevensbestanden. Een verwijsindex bevat de verwijzingen naar aangemelde gegevens.

1 Niels Sijm, Onderzoeksrapport LSP, M.Sc scriptie, System and Network Engineering, Universiteit van Amsterdam, 2008
2 Nictiz AORTA Documentatie Release, October 2008

De verwijsindex is een van de belangrijkste componenten van het LSP, waarmee zorgverleners (of het LSP) relevante patientendossiers kunnen vinden en opvragen bij de betreffende decentrale systemen, vermits zij daartoe geautoriseerd zijn.

Het beeld van het EPD als decentraal systeem waarin alleen verwijsgegevens worden opgeslagen, doet echter geen recht aan de werkelijke situatie. Het EPD kan ten hoogste als een gedeeltelijk gedecentraliseerd systeem worden gekenschetst. Het LSP regelt (schakelt) namelijk niet alleen gegevensstromen, maar bevat ook de centrale componenten waarmee beslissingen met betrekking tot toegang tot de aangemelde patiëntgegevens worden uitgevoerd. Dit betekent dat het EPD beter gezien kan worden als een virtueel landelijk EPD waarin patiëntgegevens weliswaar decentraal worden opgeslagen, maar belangrijke beslissingen ten aanzien van de toegang tot deze gegevens centraal worden genomen; in die zin verschilt het EPD niet zo veel van een gecentraliseerd systeem.

In het LSP worden persoonsgegevens opgeslagen. De verwijsindex bevat verwijzingen waarin onder meer de BSN van patient, de categorie van de patiëntgegevens, en ook gedetailleerde gegevens van de zorgaanbieder en de beroepsbeoefenaar die de vermelding heeft opgenomen te vinden zijn[3]. Dit zijn privacygevoelige gegevens omdat hieruit onder meer kan worden afgeleid bij welke instellingen en zorgverlener(s) een patiënt precies onder behandeling is, alsmede om wat voor gegevenscategorie het gaat. Het LSP bevat verder verkeers- en loggingsgegevens, waaruit onder meer behandelrelaties kunnen worden afgeleid (zie bijlage). Verwijsindex gegevens zijn normaal gesproken beschermd door (rol-gebaseerde) toegangscontrole en zijn daarom normaliter alleen voor geautoriseerde zorgverleners toegankelijk. Loggingsgegevens zijn normaliter alleen voor beheerders en toezichthouders toegankelijk. Echter, bij een inbraak in het LSP – of bij ander misbruik van de gegevens in het LSP, zoals in deze brief beschreven –, is deze informatie kwetsbaar.

Een van de uitgangspunten van dit onderzoek is dat kwaadwillenden zich toegang zullen proberen te verschaffen tot het inwendige van het systeem, om zodoende te proberen om het systeem te gebruiken en/of patiëntgegevens te bemachtigen. Het onderzoek richt zich niet op risico's die bestaan bij een normaal gebruik van het EPD door zorgverleners. Eventuele aanvallen op de techniek van UZI-passen vallen ook buiten de reikwijdte van dit onderzoek.

Samenvatting van de resultaten

Op technisch vlak constateer ik dat ten gevolge van een aantal ontwerpbeslissingen, gedocumenteerd in de AORTA specificatie, onvoldoende beveiliging wordt geboden ten aanzien van een aantal bedreigingen. Verbeteringen zijn mogelijk, maar vereisen een aanzienlijke herziening van de EPD architectuur. In het bijzonder zijn aanpassingen noodzakelijk aan Goed Beheerde Zorg (GBZ) systemen, aan het Landelijk Schakelpunt (LSP), en aan de protocollen die voor de communicatie met het LSP worden gebruikt. Tevens is een sterk identificatie- en authenticatiemiddel gewenst ten behoeve van onder meer de toegang van patiënten tot het virtuele klantenloket.

Hieronder volgt een korte samenvatting van de belangrijkste technische problemen die ik heb geconstateerd in het huidige ontwerp. Voor de volledige analyse en referenties verwijs ik u naar de uitgebreide samenvatting in de bijlage, en het wetenschappelijke artikel die bij deze brief zijn meegestuurd.

3 Wijziging van de Wet gebruik burgerservicenummer in de zorg in verband met de elektronische informatieuitwisseling in de zorg, Tweede Kamer, vergaderjaar 2008-2009,13 466 Nr. 13, Artikel 13a lid 1.

- Het huidige EPD ontwerp ondersteunt geen 'end-to-end' authenticatie van berichten die door zorgverleners worden verstuurd. De benodigde authenticatie informatie wordt wel naar het LSP gestuurd, maar vervolgens niet doorgestuurd naar de decentrale informatiesystemen die de patiëntgegevens bevatten. Dit betekent dat deze informatiesystemen bij onvangst van een verzoek niet zelfstandig kunnen controleren of dit verzoek daadwerkelijk door een zorgverlener was verstuurd. Dit maakt het systeem erg kwetsbaar bij een succesvolle aanval op het LSP.

- Het regelen van mandateringen vindt op dit moment vrijwel geheel decentraal plaats. Er is op dit moment geen technische mogelijkheden om de geldigheid van een mandatering te controleren wanneer een verzoek van een (gemandateerde) medewerker bij het LSP binnenkomt. Een dergelijke controle kan alleen achteraf door middel van mandateringstabellen plaatsvinden. Dit is geen dekkende methode. Medewerkers (UZI) passen staan weliswaar op naam, maar zijn niet gebonden aan een bepaalde gegevenscategorie; ook kunnen medewerkers technisch –vanuit het LSP bezien– zelfstandig een behandelrelatie claimen uit naam van een zorgverlener.

  Bij een compromittering van een (deel van een) GBZ kan een aanvaller die de beschikking heeft over een (gestolen) medewerkerspas met PIN-code, eenvoudig misbruik maken van het mandateringsmechanisme om dossierstukken namens een willekeurige arts binnen hetzelfde GBZ uit het EPD op te vragen. Dit beschouw ik als een zeer ernstig probleem. Merk op dat zorgverleners altijd zélf direct, zonder mandatering, het EPD kunnen gebruiken.

- Ten behoeve van beheersfuncties, worden in het LSP toegangs- en verkeersgegevens opgeslagen. Hierin wordt bijgehouden welke patiëntgegevens door welke zorgaanbieder zijn opgevraagd[4]. Ook moet het volgens de AORTA documentatie mogelijk zijn om een situatie in het verleden te reconstrueren[5]. Verwijdering van historische gegevens lijkt daarom niet mogelijk, ook niet wanneer een patient expliciet gegevens uit de verwijsindex heeft verwijderd. Het artikel bespreekt een aantal oplossingen in relatie tot centrale opslag van (reconstructie) gegevens, waarbij valt te denken aan volledige verwijdering of patient-specifieke versleuteling van gegevens in het LSP.

- De beoogde toegang van patiënten tot het virtuele klantenloket gebaseerd op DigiD met SMS authenticatie bevat een aantal inherente zwakheden[6]. Veiliger is over te gaan tot het distribueren van een sterk authenticatiemiddel ten behoeve van patiëntidentificatie en authenticatie. Een dergelijk authenticatiemiddel kan tevens voor patient-specifieke versleuteling van (historische) gegevens worden gebruikt. Ten behoeve van het gebruik van een dergelijk authenticatiemiddel, kunnen eventueel inlogplekken worden ingericht bij de zorgverleners.

Ten slotte zien wij verbeterpunten ten aanzien van het informed consent model, in het bijzonder in het licht van de geconstateerde privacy risico's bij het gebruik van het EPD. De kaderwet voorziet in toestemming door de patient voorafgaand aan het raadplegen van gegevens in het EPD (Artikel 13f lid 3). Deze toestemming geldt echter alleen bij raadpleging, en wordt alleen decentraal vastgelegd[7]. Dit biedt weinig tot geen bescherming bij een aanval op het inwendige van het EPD.

---

4 Nictiz, Bedrijfsarchitectuur AORTA, versie 6.5.0.0, 30, November 2009, p.68, par. 9.3.

5 Nictiz, Informatiesysteemarchitectuur AORTA, versie 6.0.1.0, 16 April 2009, p.55, par. 4.9.

6 B. Jacobs, S. Nouwt, A. de Bruijn, O. Vermeulen, R. van der Knaap, C. de Bie: "Beveiligingseisen ten aanzien van identificatie en authenticatie voor toegang zorgconsument tot het Electronisch Patientendossier (EPD)", rapport in opdracht van VWS uitgevoerd door PriceWaterhouseCoopers, Universiteit Nijmegen, en Universiteit van Tilburg, December 2008. http://www.minvws.nl/kamerstukken/meva/2008/elektronisch-patientendossier.asp

7 Er kan overwogen worden om per gegegevenssoort (bijvoorbeeld voor psychische gegevens) te beslissen dat behandelrelaties *centraal* in het LSP moeten worden bevestigd door de patiënt (en dus niet alleen decentraal door de zorgverlener), vóórdat toegang wordt verleend tot een bepaald dossier. Er moet dan wel worden voorkomen dat een dergelijke bevestiging in zichzelf extra privacyconsequenties geeft.

Patiënten hebben, op een per-zorgverlener of algeheel bezwaar na, weinig concrete, wettelijk geregelde of technisch ondersteunde mogelijkheden om te voorkomen dat specifieke (gevoelige) gegevens in het EPD (LSP) worden aangemeld. Bovendien is verwijdering van gegevens uit de verwijsindex en logbestanden lastig of onmogelijk compleet uit te voeren.

Alleen het voorkomen van registratie van gegevens (in de verwijsindex) kan volledige bescherming van gegevens bieden. Een oplossing zou kunnen zijn om Artikel 13f lid 2 zo uit te breiden dat er een mogelijkheid wordt geboden -aan patiënten die er niet voor kunnen (of willen) kiezen om een volledig of per-zorgverlener bezwaar te maken- om aan te geven dat eerst toestemming moet worden gevraagd alvorens (nieuwe) gegevens in het EPD mogen worden aangemeld. Op deze manier kunnen patienten, in samenspraak met de zorgverlener, controle uitoefenen over welke informatie wel en welke informatie niet in het Landelijk EPD wordt aangemeld.

Conclusie

Er zijn reëele beveiligings- en privacyrisico's verbonden aan het huidige ontwerp van het EPD. Technische en/of organisatorische oplossingen zijn in een aantal gevallen mogelijk, maar een volledige bescherming bieden is uiterst complex en waarschijnlijk nooit volledig haalbaar.

Een onderzoek naar de (technische) mogelijkheden om de geconstateerde problemen te verbeteren op korte termijn noodzakelijk. Bijgevoegd artikel probeert hiertoe een aanzet te geven. Echter, ook mét de in het artikel voorgestelde verbeteringen bestaan er nog altijd risico's – ook al zullen deze na het invoeren van verbeteringen mogelijk minder bedreigend en minder grootschalig zijn dan op dit moment. Met name de schijnbare onmogelijkheid om tijdig en volledig informatie uit het LSP te verwijderen valt op. Een aangepast consentmodel met een versterkte rol voor de patiënt kan een oplossing bieden zodat patiënten die dat willen meer controle kunnen uitoefenen op welke informatie wel, en welke informatie niet in het EPD wordt geregistreerd.

Merk op dat het fijnmazig regelen van autorisatie door patiënten dat in de toelichting bij het wetsvoorstel genoemd wordt als een mogelijkheid om toegang tot dossierstukken te regelen en met name af te schermen, geen soelaas biedt tegen de genoemde risico's bij een inbraak op het LSP, of tegen misbruik van het mandateringsmechanisme – het autorisatieprofiel kan in deze gevallen eenvoudig worden omzeild.

UNIVERSITEIT VAN AMSTERDAM

Het vervolg

Het onderzoek is recentelijk afgerond. Op korte termijn zal het onderhavige artikel ter publicatie worden opgestuurd naar een wetenschappelijke conferentie. Het Nictiz heeft het artikel reeds gelezen en van commentaar kunnen voorzien.

Ik ben te allen tijde graag bereid tot een nadere uitleg van mijn bevindingen en aanbevelingen.

Hoogachtend,

Guido van 't Noordende

Onderzoeker security en privacy in gedistribueerde systemen
System and Network Engineering (SNE) groep
Faculteit der Natuurwetenschappen, Wiskunde en Informatica (FNWI)
Universiteit van Amsterdam
Science Park 107 1098 XG Amsterdam

Email: <verwijderd>
Telefoon: <verwijderd>

Alternatief contact:
Prof. dr. ir. Cees de Laat
hoofd SNE groep

Email: <verwijderd>
Telefoon: <verwijderd>