Onderzoeksplan Informatica
Auteur: Dion Scheper, s4437578, d.scheper@student.ru.nl

Bewijs je attributen met bluetooth

0.1 Onderwerp

Bluetooth, Zero-Knowledge, Security, Android, Mobile, Authentication

0.2 Probleemstelling

In recente jaren is er veel gewerkt door de Radboud Universiteit aan het IRMA project [3]. Er zijn echter nog een aantal toepassingen waar IRMA niet aan kan beantwoorden. Het is op dit moment mogelijk om met een server die online is, en de IRMA server api implementeerd, je attributen te bewijzen. Op dit moment kan het nog niet dat je van device naar device lokaal attributen bewijst, denk hier bijvoorbeeld aan je leeftijd bij de kassa. Om dat wel te kunnen doen in de toekomst heb je een draadloze technologie nodig die op minimaal een meter afstand data kan delen. Er zijn verschillende draadloze technologien die dit zouden kunnen[18], en de technologie die het beste lijkt te passen is Bluetooth. Dit is vanwege het bereik, de energie consumptie, en het device-device connectie principe. De onderzoeksvraag luid: 'Hoe kunnen twee Android devices, via Bluetooth, IRMA attributen aan mekaar bewijzen?'. Om deze vraag te beantwoorden ga ik onderzoeken wanneer je face to face attributen uit zou willen wisselen. Daarna ga ik op zoek naar de technische eisen die er aan een Android app worden gesteld. En ten slot ga ik onderzoeken hoe IRMA dit zou moeten implementeren

0.3 Verantwoording

Burgers in de maatschappij hebben meestal geen idee wat privacy precies inhoud en waarom het is opgenomen in het verdrag van Geneve[5]. Wat een veel geluid antwoord is met betrekking tot het recht op privacy is 'maar ik, als goede burger, heb toch niks te verbergen'. Om daar een tegenantwoord tegen in te brengen kan soms best lastig zijn.

Schlingensiepen beschrijft de 'Reichstagsbrandverordnung'. Dit is een decreet dat in 1933 is ondertekend door toemalig Duits president Hindenburg onder druk van Hitler. Hij noemt in zijn biografie over Dietrich Bonhoeffer[14]

op pagina 119 dat verdrag: "the right to privacy of communication by mail or telephone no longer existed".

Het mag dan nu best goed zijn in Nederland, je wordt niet zomaar veroordeeld om je geloof of huidskleur, maar dat kan in de toekomst veranderen. Technologie veranderd ook, maar als we nu niet kiezen voor privacy by design dan hebben we misschien geen tijd meer om te veranderen wanneer het wel nodig blijkt te zijn.

Maar dat is niet het enige waar de burger emotioneel mee over te halen is. Er zijn ook statistieken en cijfers, zoals bijvoorbeeld het aantal meldingen van identiteits fraude. Zo kun je lezen in een onderzoek van PwC uit 2013 dat in de periode 2007-2010 naar schatting 5,6% van de nederlandse bevolking slachtoffer is geweest van identiteitsfraude [12]. Dit is een indicatie dat we goed na moeten denken over onze (digitale) identiteiten en hoe we daar mee om gaan.

Dit verantwoord waarom er onderzoek nodig is naar privacy vriendelijke technologieen zoals IRMA. En dit verantwoord ook waarom het belangrijk is om te onderzoeken hoe verschillende draadloze technieken dit kunnen ondersteunen om de gebruikers situaties te beantwoorden.

0.4 Theoretisch kader

IRMA is een project van de Digital Security Group Nijmegen, en het Privacy and Identity lab. IRMA staat hier voor I Reveal My Attributes. Als persoon hebben we verschillende attributen, denk bijvoorbeeld aan je geboortenaam, woonplaats, paspoort etc. Maar je kunt niet zo maar een enkel attribuut bewijzen. Bijvoorbeeld wanneer je je paspoort laat kopieren op de camping in Frankrijk hebben ze al je gegevens van je paspoort, terwijl ze maar enkele nodig hebben. Met IRMA kan je wel selectief je attributen delen, het is een open source project en het protocol staat hier beschreven[1]. Het stelt je in staat om precies die informatie prijs te geven die de ander nodig heeft.

Bluetooth is een draadloze technologie die devices in staat stelt om data te delen. Deze technologie is geimplementeerd in verschillende computers, laptops en andere communicatie apparaten. Maar daarnaast ook keyboards, audio headsets, etc.[18]. De beveiliging van de technologie, en dan met name de authenticatie procedure, is al meerdere keren onderzocht[8][17]. Omdat bluetooth een lange 'pairing' authenticatie procedure heeft, die tot wel 6 seconden in beslag kan nemen, zijn er al verschillenden die naar alternatieve methoden hebben gezocht om twee devices te pairen zoals bijvoorbeeld gesuggereerd in [16]. Hier passen ze het protocol aan zodanig dat een authenticatie poging van een aanvaller kan worden afgeslagen. Een covert channel manier, zonder pairing, om bluetooth data uit te wisselen is beschreven in [15].

Ondanks dat sommige onderzoeks niet in dezelfde tak van sport zitten is

hun werk zeer relevant. Het authenticeren van je smartphone als een soort token naar de computer toe is bijvoorbeeld onderzocht [7]. Deze techniek is ook zeer toepasbaar op de IRMA situatie, en ze maken slim gebruik van een Diffie-Hellman key exchange.

Een formele beveiligings analyse van bluetooth is onderzocht in [6]. Ze laten zien dat ook het simple pairing protocol nog niet veilig is tegen aanvallen waarbij er meerdere sessies worden geopent. Het simple pairing protocol is ook beschreven in Bluetooth® Secure Simple Pairing Using NFC[9]. Samen met [10] laten ze een specificatie zien om de initalisatie met NFC te doen om vervolgens data uit te wisselen met bluetooth.

Om toch een gebruikers bevestiging te hebben in plaats van de pin zijn er onderzoekers op zoek naar bijvoorbeeld het herkennen van geluiden o.i.d. bij bluetooth authenticatie [13]. En je hebt ook nog een andere manier van die een zero knowledge ontwerp heeft gemaakt om apparaten te laten communiceren [11].

Een open source proof of concept dat de onderzoeksvraag beantwoord geeft ruimte aan andere onderzoekers om de toepassingen van vergelijkbare technologien te onderzoeken.

0.5 Methode

Voordat het design en create process in gegaan wordt, zal er eerst een vooronderzoek plaatsvinden. Dit vooronderzoek is het vaststellen van de scenarios waarin IRMA device-device gebruikt zou kunnen worden. Dit zal de context geven aan het onderzoek, en vooral ook een manier zijn om de effectiviteit van het onderzoek te kunnen toetsen nadat de proof of concept Android app is gemaakt.

En dat is precies het volgende punt. Volgens een iteratief design and create process wordt een proof of concept Android app gemaakt. Deze zal steeds bij elke iteratie worden getoetst aan de scenarios die zijn beschreven.

Om de app te bouwen worden er meerdere bronnen gebruikt. Deze bronnen zijn de specificaties van de desbetreffende technologien:

- Bluetooth [4]
- Android [2]
- IRMA [1]

Deze specificaties vormen dus de basis van de compromisen die gemaakt zullen moeten worden. En elk compromis zal dan ook een verantwoording terugvinen in het uiteindelijke onderzoeksrapport.

0.6 Planning

Deze methode zal een aantal maanden in beslag nemen.

- Beschrijven en documenteren van use cases en scenarios (1 week)
- Iteratieve design process (8 weken).
  - Gesprek met begeleider over: scenario's, implementatie
  - Werken aan de Android app
  - Documenteren van tussentijdse compromisen en resultaten
  - Deze resultaten terug koppelen naar begeleider voor gespreksstof

Bibliografie

[1] https://credentials.github.io/protocols/irma-protocol/.

[2] https://developer.android.com.

[3] https://privacybydesign.foundation/irma/.

[4] https://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=286439.

[5] http://www.ohchr.org/en/udhr/documents/udhr_translations/eng.pdf.

[6] Richard Chang and Vitaly Shmatikov. Formal analysis of authentication in bluetooth device pairing. 2007.

[7] F. Dellutri, G. Me, and M. A. Strangio. Local authentication with bluetooth enabled mobile devices. In *Joint International Conference on Autonomic and Autonomous Systems and International Conference on Networking and Services - (icas-isns'05)*, pages 72–72, Oct 2005.

[8] C. M. Fan, S. Shieh, and B. H. Li. On the security of password-based pairing protocol in bluetooth. In *2011 13th Asia-Pacific Network Operations and Management Symposium*, pages 1–4, Sept 2011.

[9] Bluetooth Special Interest Group. Bluetooth secure simple pairing using nfc, 2014.

[10] Eddie laCosta. Automating bluetooth pairing with near-field communications (nfc), 2014.

[11] Yan Michalevsky, Suman Nath, and Jie Liu. Mashable: Mobile applications of secret handshakes over bluetooth le. In *Proceedings of the 22Nd Annual International Conference on Mobile Computing and Networking*, MobiCom '16, pages 387–400, New York, NY, USA, 2016. ACM.

[12] PwC. 2013-update onderzoek 'omvang van identiteitsfraude & maatschappelijke schade in nederland', 2013.

[13] Nitesh Saxena, Md. Borhan Uddin, and Jonathan Voris. Universal device pairing using an auxiliary device. In *Proceedings of the 4th Symposium on Usable Privacy and Security*, SOUPS '08, pages 56–67, New York, NY, USA, 2008. ACM.

[14] Ferdinand Schlingensiepen. *Dietrich Bonhoeffer 1906–1945: martyr, thinker, man of resistance*. T&T Clarke, 2010.

[15] Yakov Shafranovich. Bluetooth data exchange between android phones without pairing. *CoRR*, abs/1507.00650, 2015.

[16] P. R. Suri and S. Rani. Bluetooth security - need to increase the efficiency in pairing. In *IEEE SoutheastCon 2008*, pages 607–609, April 2008.

[17] J. Xu, T. Zhang, D. Lin, Y. Mao, X. Liu, S. Chen, S. Shao, B. Tian, and S. Yi. Pairing and authentication security technologies in low-power bluetooth. In *2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing*, pages 1081–1085, Aug 2013.

[18] Y. Zou, J. Zhu, X. Wang, and L. Hanzo. A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE*, 104(9):1727–1765, Sept 2016.