SMARTPHONE SECURITY

Drs. ing. D.H. Hut, Security specialist bij TNO en E.G. Broenink M.Sc., Security specialist bij TNO

Volgens de IDC Worldwide Quarterly Mobile Phone Tracker groeit de wereldwijde smartphonemarkt naar verwachting 49,2% in 2011. Geen wonder want deze apparaten met hun krachtige processors en snelle videochipsets worden door leveranciers in een hoog tempo geüpgraded. Gecombineerd met een multi-touch besturingssysteem en een breed palet aan telecommunicatiemogelijkheden voor zowel korte als lange afstand zijn smartphones de 'one-stop-shop' aan het worden voor al uw mobiele computing- en communicatiewensen. Zowel thuis, onderweg, als op het werk. Het enorme aanbod aan apps biedt veel flexibiliteit en keuze voor een relatief lage prijs vergeleken met de traditionele software- en games-markt. De populariteit van smartphones is dan ook terug te zien in de verkoopcijfers van een aantal grote leveranciers.

Dat toch niet alles koek en ei is, blijkt uit de vele nieuwsberichten op security georiënteerde websites en in magazines. Moet u zich als gebruiker zorgen maken over de beveiliging van uw smartphone? En dan bedoelen we dit in de brede zin. Niet alleen de informatie die u erop zet of die u ermee consumeert of produceert maar bijvoorbeeld ook de informatie die ontstaat uit de sensoren of het gebruik van bepaalde applicaties of specifieke functies.
In dit artikel wordt aan de hand van enkele voorbeelden toegelicht met welke beveiligingsproblemen gebruikers van smartphones te maken kunnen krijgen. Ook worden enkele zowel bestaande als nieuwe security-ideeën beschreven die als tegenmaatregel kunnen worden ingezet om de smartphone veiliger te maken. Daarbij moet wel worden opgemerkt dat sommige maatregelen wellicht wat te ver gaan voor de gemiddelde smartphone-gebruiker.

Achtergrond

Waar een telefoon vroeger uitgeleverd werd met een beperkt aantal simpele basisfuncties, bieden smartphones veel functionaliteit. Mede daardoor zijn ze vergelijkbaar geworden met personal computers. Beide zijn opgebouwd volgens een relatief open 'verticale stack' van hardware en software (fig. 1) en op beide platformen is veel software beschikbaar van externe partijen.

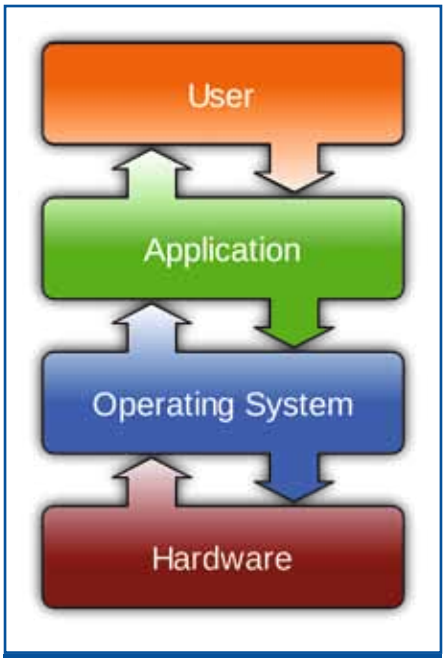

Fig. 1. Verticale stack.

Verticale stack

In elke laag van de stack kunnen, afhankelijk van het type smartphone, verschillende leveranciers actief zijn. Voor het besturingssysteem gebruiken fabrikanten soms hun eigen implementatie en soms een versie van een derde partij, eventueel aangevuld met een user-interface schil.

Vele apps

Gebruikers kunnen allerlei apps op hun smartphone installeren. Soms gaat dat via een online 'app'-winkel zoals Google's Android Market, Apple's iPhone App Store of Amazon Appstore. Soms kunnen gebruikers apps buiten zo'n winkel om installeren. De markt van apps is relatief open, in de zin dat externe partijen apps kunnen ontwikkelen en deze kunnen aanbieden in de verschillende app-winkels.

Veel data

Mede doordat smartphones zijn uitgerust met sensoren die waardevolle informatie kunnen opleveren, is de hoeveelheid gebruikersinformatie op een smartphone sterk gestegen. Ook kunnen smartphones gebruikt worden als mobiele storage devices, vergelijkbaar met bijvoorbeeld een usb-stick, voor het opslaan van foto's, filmpjes, muziek, e-mail, elektronische boeken enz.

Deze aspecten kunnen beveiligingsrisico's introduceren. De flexibiliteit rondom het kunnen installeren van apps is prettig voor de gebruiker maar schept ook verplichtingen. Een gebruiker moet aan de hand van de door een app aangevraagde permissies kunnen inschatten wat de consequenties zijn van het installeren van een app. De grote hoeveelheid gebruikersdata op de smartphone inclusief sensorinformatie zoals locatie zorgt ervoor dat een gebruiker een steeds grotere 'aanvals-

> Moet u zich zorgen maken over de beveiliging van uw smartphone?

oppervlakte' krijgt waarvan misbruik gemaakt kan worden. De verschillende aanbieders van de app-winkels ten slotte hanteren verschillende niveaus van kwaliteitscontrole waardoor kwaadaardige apps al dan niet doorgang vinden via een app-winkel naar de gebruiker.

Beveiligingsrisico's

Gebruikers van smartphones kunnen worden geconfronteerd met beveiligingsproblemen in allerlei categorieën. We schetsen kort enkele voorbeelden en verwijzen per categorie naar gevallen uit de praktijk op basis van artikelen in de media.

Toegang tot microfoon, camera of locatie

Door het ongemerkt aanzetten of op een andere manier misbruiken van de microfoon [1] of camera [2] is het mogelijk dat een aanvaller telefoongesprekken of omgevingsgeluid kan afluisteren of foto's in handen krijgt. Ook is het mogelijk dat locatiegegevens worden doorgestuurd naar derden doordat de GPS-sensor wordt uitgelezen [3].

Flexibiliteit installeren apps prettig, maar schept ook verplichtingen

Ongewenst bellen of sms'en

Een spelletje dat rondgaat voor smartphones, blijkt in werkelijkheid kwaadaardige software te zijn dat gebruikers met hoge kosten opzadelt door te bellen naar dure nummers [4].

Afluisteren inloggegevens, wachtwoorden en transactiecodes

De uit de pc-wereld bekende kwaadaardige software 'Zeus' heeft de overstap naar smartphones gemaakt en steelt toetsaanslagen en inloggegevens [5]. De malware SpyEye heeft een mobiele variant en onderschept sms'jes met tan-codes en stuurt die naar een externe server [6].

Een smartphone kan op verschillende manieren geïnfecteerd raken met kwaadaardige software. Bijvoorbeeld door het installeren van een kwaadaardige app. Soms worden bekende apps gekopieerd en opnieuw in een app store gezet maar pas nadat ze zijn voorzien van kwaadaardige functies. Soms is het openen van een link in een sms of e-mail of het surfen naar een kwaadaardige website al genoeg. Ook kan in de firmware zelf al ongewenste functionaliteit zitten [7, 8].

Voor wat betreft de security-prestaties van de verschillende mobiele platformen beschikken wij niet over onafhankelijke data om een goed vergelijk te kunnen maken. Symantec, een grote aanbieder van security software, heeft in een whitepaper [9] de verschillende sterke en zwakke punten van zowel iOS als Android vergeleken. De conclusie is dat mobiele devices productiviteit verhogen maar ook nieuwe risico's introduceren. Volgens een rapport [10] van McAfee (peildatum 2-2011), een andere grote aanbieder van security software, is kwaadaardige software voor Android OS sterk in opkomst en is Android OS nu het meest aangevallen platform. Lookout, een bedrijf dat zich richt op het leveren van smartphone security software, noemt in haar Mobile Threat Report 2011 [11] dat de hoeveelheid met 'malware' geïnfecteerde Android apps gestegen is van 80 apps in januari 2011 tot meer dan 400 apps in juni 2011.

Conclusie: mobiele devices verhogen productiviteit en introduceren nieuwe risico's

Maatregelen

Voor het preventief voorkomen of ten minste voor het kunnen detecteren van de beschreven beveiligingsproblemen is de gebruiker vooral afhankelijk van systeemupdates van de leverancier en de kwaliteitscontrole van de app winkels. Virusscanners zoals we die kennen uit de pc-wereld zijn langzaam in opkomst voor smartphones maar het is nog maar de vraag wat dit type product voor gevolgen heeft

voor de performance van de smartphone en de accuduur. Er zijn echter ook andere beveiligingsmaatregelen denkbaar die minder belastend zijn voor de smartphone zelf maar meer inspanning vereisen van de gebruiker.

Runtime permissiemodel

Sommige smartphones vragen de gebruiker tijdens de installatie van een app akkoord te gaan met bepaalde permissies die een app nodig zegt te hebben. Veel apps vragen echter teveel rechten en bovendien geven veel gebruikers gewoon toestemming voor alles wat een app vraagt. Een mogelijke verbetering zou zijn om niet bij installatie om permissies te vragen, maar een 'runtime' permissiemodel te gebruiken waarbij de gebruiker meer dynamisch kan toestaan of een app bijvoorbeeld bij de adressenlijst of bij de GPS mag komen. Bij deze oplossing bestaat wel het gevaar dat gebruikers continu om input worden gevraagd.

Lockdown

In het geval van diefstal kan het wenselijk zijn om de smartphone te kunnen locken of wissen op afstand. Er zijn apps verkrijgbaar die deze functionaliteit bieden zoals MobileIron, soms in combinatie met een website of soms met een enterprise server binnen een bedrijfsomgeving.

> Veel gebruikers geven toestemming voor alles wat een app vraagt

Custom firmware

Personal computers kunnen allerlei variaties aan besturingssystemen draaien en sommige daarvan hebben een expliciete focus op beveiliging. Ook voor Android smartphones ontstaan speciale varianten van dit besturingssysteem met specifieke security en/of privacy features die niet in de oorspronkelijke versie zitten.

Conclusie

De vele referenties over kwaadaardige software voor smartphones zijn een indicatie dat gebruikers geconfronteerd kunnen worden met beveiligingsproblemen. Het Android OS platform laat een sterke stijging zien in de hoeveelheid malware. Er worden echter ook, net als bij personal computers, beveiligingsmaatregelen ontwikkeld. Het is de vraag hoe deze markt zich gaat ontwikkelen. Volgt de smartphone-markt haar grotere broer, de personal computer-markt, in de ontwikkeling van virusscanners en firewalls of zullen andere type maatregelen tegen kwaadaardige software noodzakelijk gaan worden?

Referenties

1. New apps hijack the microphone in your cell phone to listen in on your life, 19 april 2011, http://info-wars.org/2011/04/19/new-apps-hijack-the-microphone-in-your-cell-phone-to-listen-in-on-your-life/

2. Mobile Malware Threats Grow! Now They can Steal Photos From Your Phone, August 22, 2011, http://slashnext.com/2011/08/mobile-malware-threats-grow-now-they-can-steal-photos-from-your-phone/

3. Mobile Apps Invading Your Privacy, 5 april, 2011, www.veracode.com/blog/2011/04/mobile-apps-invading-your-privacy/

4. Trojan jaagt mobiele bellers op torenhoge kosten, 9 april 2010, www.security.nl/artikel/33007/1/Trojan_jaagt_mobiele_bellers_op_torenhoge_kosten.html

5. Don't bank on your phone – it could be hacked by Zeus, 22 July 2011, www.guardian.co.uk/money/2011/jul/22/smartphones-hacked-zeus-malware

6. Android-malware steelt sms'jes van je bank, 15 september 2011, www.zdnet.be/news/131236/android-malware-steelt-sms-jes-van-je-bank/

7. Apple sued over iPhone location tracking, 25 april 2011, www.theregister.co.uk/2011/04/25/apple_sued_for_location_tracking

8. Google faces $50 million lawsuit over Android location tracking, 1 mei 2011, http://arstechnica.com/tech-policy/news/2011/04/google-faces-50-million-lawsuit-over-android-location-tracking.ars

9. The Current State of Mobile Device Security, Symantec, 28 Jun 2011, www.symantec.com/connect/blogs/new-symantec-research-current-state-mobile-device-security

10. McAfee Threats Report: Second Quarter 2011, McAfee Labs, www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2011.pdf

11. 2011 Mobile Threat Report, Lookout Mobile Security, August 2011, www.mylookout.com/mobile-threat-report

SCHRIJF U NU IN ALS VIP VAN INFORMATIEBEVEILIGING
EN UW DAG IS GEHEEL GRATIS!

8e editie

IT & Information Security

Voorkom reputatieschade

Donderdag 2 februari 2012
Congrescentrum 1931, 's-Hertogenbosch

Waarom mag u dit congres niet missen:

- 300 aanwezige vakgenoten
- Uitgebreide netwerkmogelijkheden
- Inspirerende visie verhalen en praktijkvoorbeelden
- Beursvloer met 20 aanbieders en specialisten
- Dagvoorzitter ing. John Hermans, Partner, KPMG IT Advisory

VIP Vermeld de VIP-code 8789/07 bij uw inschrijving. Alleen dan is uw dag geheel gratis met lunch en parkeerkaart. Uitsluitend eindgebruikers kunnen zich als VIP aanmelden.

security.heliview.nl