Smartphone Security – impact op operators

Auteurs: Dr. ir. Thijs Veugen, ir. Frank Fransen, ir. Tim Hartog en ir. Frank Muller, allen bij TNO werkzaam op het gebied van information security

Oude dreigingen in een nieuw jasje

Iedereen heeft tegenwoordig wel een smartphone of een internet tablet. Het is niet alleen trendy, maar biedt ook allerlei mogelijke communicatievormen en manieren om informatie op te zoeken. Naast standaardtoepassingen als email, Facebook, Twitter en internet browsen kunnen er ook allerlei dedicated applicaties ('apps') worden gedownload die het leven een stuk eenvoudiger en leuker kunnen maken. Denk aan zakelijke toepassingen, het vertalen van teksten, financiële diensten (aandelenkoersen en banksaldo's), social communities, maar ook navigatieprogramma's en allerlei games. Diverse nieuwe business opportunities dienen zich aan. De keerzijde van de medaille is dat dergelijke toestellen een verhoogd security risico met zich meebrengen. Maatregelen tegen deze risico's richten zich vaak op de gebruiker. Hoe zit het echter met de risico's voor de operators?

Risico's voor de gebruiker

Sinds 2002 wordt, voornamelijk door leveranciers van virusscanners al gewaarschuwd voor gevaren van virussen en andere soorten kwaadwillende applicaties voor smartphones. Deze applicaties worden ook wel mobile malware, van *mal*icious soft*ware*, genoemd. Hoewel de hoeveelheid gedetecteerde mobile malware sinds 2002 telkens is toegenomen, heeft het tot nu toe nooit tot grootschalige besmetting of problemen geleid. Door de toenemende populariteit van de iPhone en Android toestellen en het succes van de virtuele markt voor applicaties (Android Market, App Store), is de verwachting echter dat deze situatie zal veranderen. De veelgebruikte webbrowser en emailclient maken het apparaat kwetsbaar. En door toename van persoonlijke en financiële data en de hoeveelheid apparaten zijn smartphones een interessanter doelwit voor cybercriminelen geworden.

Recente studies[1] naar de belangrijkste security risico's van smartphones richten zich vooral op bedrijven en consumenten. Een paar voorbeelden:

1. Als je toestel wordt gestolen, je het verliest of verkoopt, dan kan een kwaadwillende die het toestel in zijn handen krijgt eenvoudig je persoonlijke informatie achterhalen.
2. Apps hebben vaak, zonder dat de gebruiker zich daarvan bewust is, toegang tot locatie informatie, persoonlijke data op het toestel of zelfs de microfoon en camera. Dat kan een legaal onderdeel van een app zijn. Het kan echter ook gaan om illegale spyware die persoonlijke data verzamelt om er geld mee te verdienen.
3. Via internet, email, maar ook SMS, kunnen aanvallen gedaan worden die in vergelijkbare vorm al eerder in de pc-wereld zijn gebruikt, zoals phishing met fake berichten om user credentials te verzamelen. Maar ook ongewenste berichten via SMS en email (spam), en malware infectie om gevoelige financiële gegevens te achterhalen.

Er bestaan diverse maatregelen om dergelijke security risico's te reduceren die ook al worden toegepast. Een voorbeeld is het gebruik van digitale handtekeningen waarmee, doordat je zeker weet van wie de app afkomt, de integriteit ervan kan worden verbeterd. Een ander voorbeeld is de 'sandbox', waarmee er een gecontroleerde omgeving binnen het operating systeem kan worden gecreëerd waarin apps kunnen draaien. Ook capability-based security biedt de mogelijkheid tot extra controle binnen het operating systeem door toegang tot systeem bronnen te reguleren. Door af te dwingen dat apps alleen via de virtuele markt kunnen worden geïnstalleerd, krijgen Apple en Google de mogelijkheid om software van derden aan controles te onderwerpen alvorens de app kan worden aangeboden.

---

[1] Smartphones: Information security risks, opportunities and recommendations for users, ENISA, December 2010, http://www.enisa.europa.eu/act/it/oar/smartphones-information-security-risks-opportunities-and-recommendations-for-users/at_download/fullReport

De eerder genoemde risico's en maatregelen worden vaak genoemd in allerhande artikelen en zijn redelijk bekend maar richten zich vooral op de gebruiker van de smartphone. De risico's voor operators zijn echter vaak onderbelicht, en juist die vragen om andersoortige oplossingen.

Impact op operators

Een operator is gebaat bij een correcte afhandeling en betaling van mobiele telecommunicatiediensten. De twee belangrijkste dreigingen die dat in de weg staan bij gebruik van smartphones zijn dialers en Denial of Service (DoS) aanvallen op toestellen.

Dialers

Het probleem van dialers bestaat al lang in de telecommunicatiewereld. PCs hadden een inbelmodem om verbinding te maken met het internet. Zodra de gebruiker kon worden verleid om dialersoftware te installeren, vaak onder het mom van toegang tot speciale content, ontstond de mogelijkheid om de PC dure nummers te laten bellen. De aanvaller, die deze nummers beheerde, kreeg zo de mogelijkheid om illegaal geld te verdienen. Ondanks de onvoorzichtigheid van de gedupeerden, stelde de operators hen vaak deels schadeloos en kregen de operators zo een deel van de rekening gepresenteerd. De aanbieder van de dure nummers moest wel betaald worden. Dialers werden hierdoor een serieus probleem voor operators.

Door de opkomst van ADSL en kabelinternet, en daarmee het verdwijnen van inbelmodems, verdween deze dreiging naar de achtergrond. De groeiende adoptie van de smartphone, die naast een internetverbinding ook belfunctionaliteit heeft, zorgt mogelijk weer voor een opleving van de kwaadaardige dialer software. De afgelopen jaren zijn er apps voor Symbian[2] en Android[3] ontdekt die heimelijk SMS'jes sturen naar dure service nummers. Bij een recent incident[4] in China zorgde een fake anti-virus app voor malware op de smartphone, die automatisch SMS berichten met URL links ging verspreiden naar persoonlijke contacten. Meer dan een miljoen gebruikers raakten geïnfecteerd, en de kosten liepen hoog op.

---

[2] Trojan targets mobiles phones running Java applications, http://www.kaspersky.com/news?id=180984542

[3] SMS-trojan schrikt de Androidwereld op!, http://www.androidworld.nl/37236/sms-trojan-schrikt-de-android-wereld-op/

[4] Mobile Malware Targets Chinese Users, http://securitywatch.eweek.com/mobile_malware/mobile_malware_targets_chinese_users.html

Om het dialerprobleem tegen te gaan, houden operators het gebruik van klanten in de gaten. Zodra dit boven een bepaalde drempel komt is er vaak iets verdachts aan de hand. Verder kunnen de SMS berichten binnen het netwerk worden gecontroleerd op kwaadaardige content d.m.v. filtering en blacklisting.

Een alternatieve, nog niet gehanteerde methode, is het gebruik van 'whitelisting' van service requests, die een betere beheersbaarheid van de lijsten kent dan de blacklisting variant omdat de illegale services doorgaans geen lang leven beschoren zijn en dus vaak veranderd worden.

Denial of Service (DoS) aanvallen
Een tweede serieus probleem voor operators zijn de DoS aanvallen op toestellen. Malware of specifiek geconstrueerde SMS berichten kunnen toestellen dermate van slag brengen dat ze niet meer functioneren. Naast het ongemak voor de gebruiker zorgen dergelijke acties ook voor een extra belasting van de operator die wordt ingeschakeld om het probleem te verhelpen. Het kan zelfs zover gaan dat een grootschalige aanval op toestellen van een bepaalde operator wordt opgezet, om uiteindelijk de operator te kunnen afpersen om van het probleem af te komen.

Een bekend voorbeeld is de SMS-o-Death[5] van Collin Mulliner, die aantoont dat een SMS kan worden gestuurd naar diverse dedicated toestellen die daardoor crashen. De SMS-o-Death blijkt door zijn binaire formaat tevens lastig te filteren op het (home) operator netwerk. Ook via malware op het toestel kan een kwaadwillende vanaf een willekeurige plek op de wereld het toestel laten blokkeren of zelfs stuk maken. Met een beetje creativiteit kun je allerlei mogelijkheden bedenken voor zo'n aanval. Enkele voorbeelden die specifiek gericht zijn op het dwars zitten van de operator zijn: a) Het omzetten van de simlock functionaliteit naar een andere operator zodat het toestel geen verbinding kan krijgen met het eigen netwerk. b) Het blokkeren van de SIM door verkeerde PIN en PUK codes in te voeren. Naast een hoog aantal dure helpdesk-calls moet de operator dan zelfs een nieuwe SIM kaart uitgeven wat nog meer kosten met zich meebrengt.

Om te voorkomen dat de gevolgen voor de gebruiker en operator van zo'n aanval uit de hand lopen, kan als alternatief gedacht worden aan een automatische herstart en/of terugzetten naar fabrieksinstellingen van het toestel na de zoveelste verkeerde PUK code, waardoor de functionaliteit van de smartphone in ieder geval blijft behouden.

Nieuwe oplossingen
Waar de meeste artikelen over smartphone security tegenwoordig de nadruk leggen op de risico's voor de gebruiker, is de rol van de operator vaak nog onderbelicht. Bekende dreigingen in een nieuw jasje, zoals dialers en DoS, zullen voor telecom operators belangrijk worden om in de gaten te houden en nieuwe oplossingen voor te bedenken.

Er wordt wel degelijk gewerkt aan oplossingen om malware voor smartphones in internet tablets tegen te gaan. Zo zijn de Trusted Computer Group (TCG) en het Open Mobile Terminal Platform (OMTP) bezig om het platform robuuster te maken, maar dat zie je nog niet terug in de markt. Er is daarom reden om de ogen open te houden en toe te werken naar goede oplossingen, anders blijft het beperkt tot lapmiddelen en kunnen de kosten voor operators aardig uit de hand gaan lopen.

Het kan voor operators ook aanleiding zijn om zich te onderscheiden van concurrenten door extra voorzieningen op security gebied. Bekende maatregelen als backup van data, biometrie en dergelijke. zijn mogelijk, maar men moet ook blijven zoeken naar goede nieuwe maatregelen die niet uit de pc-wereld komen, en die wellicht via de virtuele markt (App Store) verkrijgbaar zijn.

[5] SMS-o-Death: from analyzing to attacking mobile phones on a large scale, http://www.mulliner.org/security/sms/feed/smsodeath_mulliner_golde_cansecwest2011.pdf