Mobility en informatie beveiliging

Dennis Reumer – 9 Oktober 2013
@reumerd – dennis.reumer@arche-it.com

Dennis Reumer

CEO/Eigenaar Arché IT bv

>10 jaar ervaring met mobiele technologie en oplossingen voor smart-phone en tablets

>25 jaar ervaring met software ontwikkeling, waarvan 7 jaar mobiele applicatie ontwikkeling

Zowel een IT als Software Architect

Help en adviseert Bedrijven en outsourcing partijen op het gebied van Mobiele strategie, de implementatie van mobiele oplossingen en keuzes ten aanzien van ontwikkel strategieën voor mobiele applicaties.

Introductie

Doel van de Presentatie

* Het beveiligingsvraagstuk van Mobility duidelijk maken
* Diverse invalshoeken van Mobility en informatie beveiliging op mobiele platformen aangeven.
* Handvaten geven om de intrinsieke veiligheid van een mobiele oplossing in de vorm van een applicatie te kunnen beoordelen
* Componenten die voor een veilige applicatie benodigd zijn aangeven en toelichten.

Overzicht

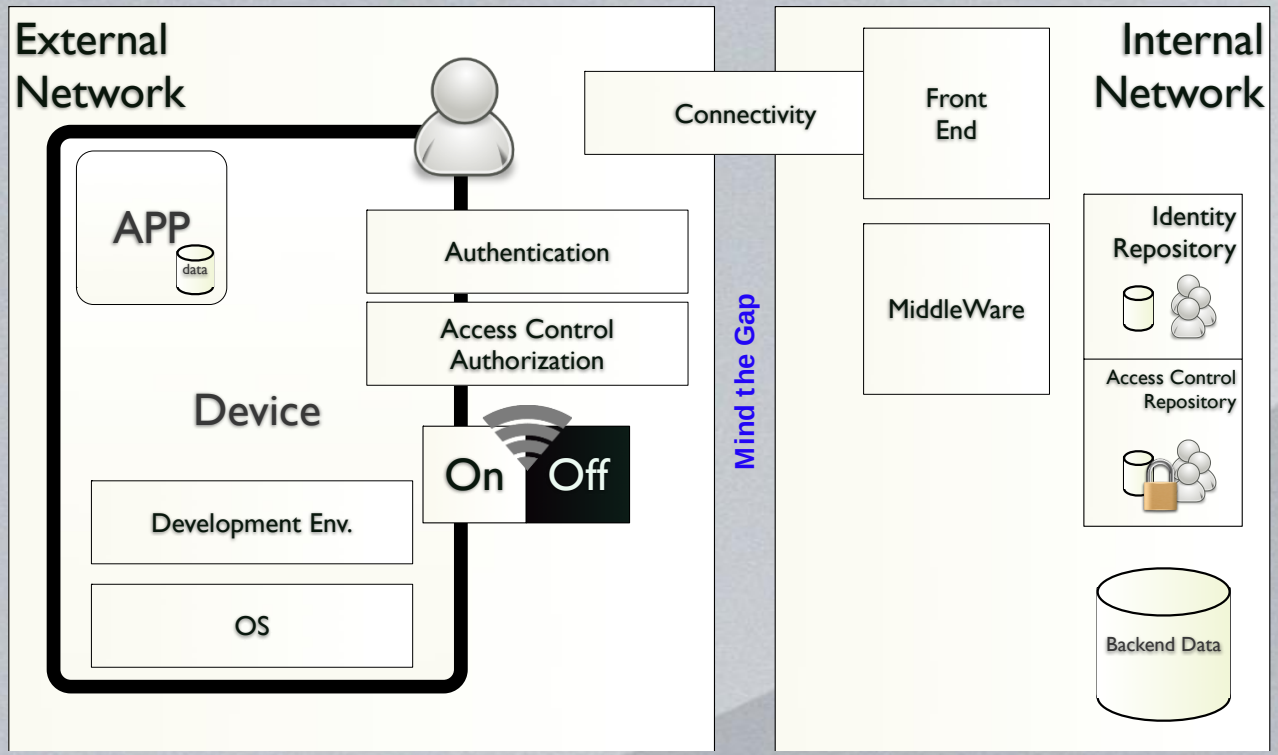
* Wat zijn Apps ?
* Alles is kapot!
* Volg de gegevens
* Aandachtsgebieden
* Invulling van beveiliging

Wat zijn Apps ?

* Icoon op een mobiele telefoon
* Een programma met native/hybride/html5 code, een User Interface, lokale data cache en een backend in the ‘cloud’
* Een Web Applicatie in een browser
* Een (Windows) applicatie via een remote desktop (vdi)
* Afgebakende functionaliteit in een specifieke context

* Buiten het bedrijfsnetwerk (IPv4)
* Geen ondersteuning voor veel gebruikte protocollen.
* Op een vreemd OS (geen windows/linux/unix, etc.)
* Geen integratie met bestaande oplossingen wat betreft Indentiteit, Authenticatie en Authorisatie (Windows AD bvb, Kerberos).
* Niet altijd aangesloten/connected. (mobility mythe)

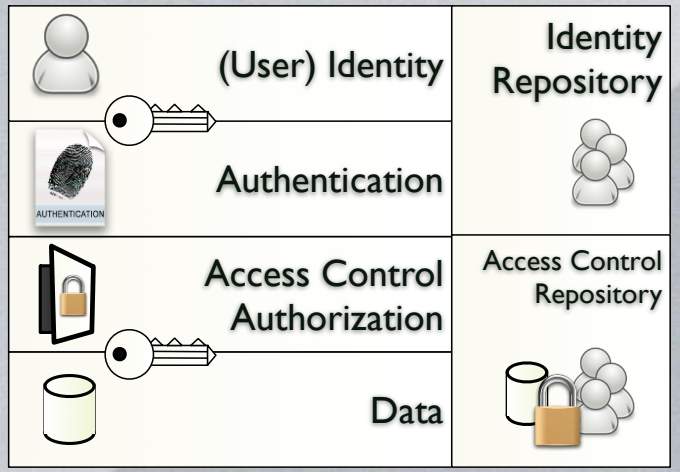
Alles is kapot!



Volg de gegevens

Aandachtsgebieden

* Data op het device
* Data transport
* Connectiviteit
* Identiteit
* Authenticatie
* Autorisatie
* Type Data



Invulling van Beveiliging

VOORKOMEN

* Encrypt Data at rest
* Gebruik encryptie voor Data transport
* Zorg ervoor dat Identiteit, Authenticatie en Autorisatie met overeenkomen met de interne mechanismen.
* Bedenk voor je gegevens deelt met andere applicaties (agenda, mail, contacten)
* Bescherm je voordeur. (Akamai)

GENEZEN

* Blokeer Dienst

* Zorg voor heldere communicatie naar eindgebruikers via de App (Dienst niet beschikbaar) ander communicatie kanaal als normaal voor de App.

* Tijdbom op informatie op device

* Plaats gepatchte dienst online, informeer eindgebruikers via de App.

Invulling van Beveiliging 2

Verantwoordelijkheden

App aanvragers:

* Privacy / Regulering rond data (wordt steeds meer)

* Opstellen, valideren van beveiligingsmaatregels en hun implementatie, inclusief procesbewaking.

App implementeerders

* Technische bekwaamheid en bekendheid met beveiligingstechnieken (encryptie, certificaat-pinning, opslag wachtwoorden en sleutels)

* Inzicht geven in de implementatie van de veiligheidsmateregels.

Informatie bronnen

OWASP Mobile:

https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_Ten_Mobile_Risks

Verantwoordelijkheden

Q&A

Q&A

Woord van Dank