پروژه باریم

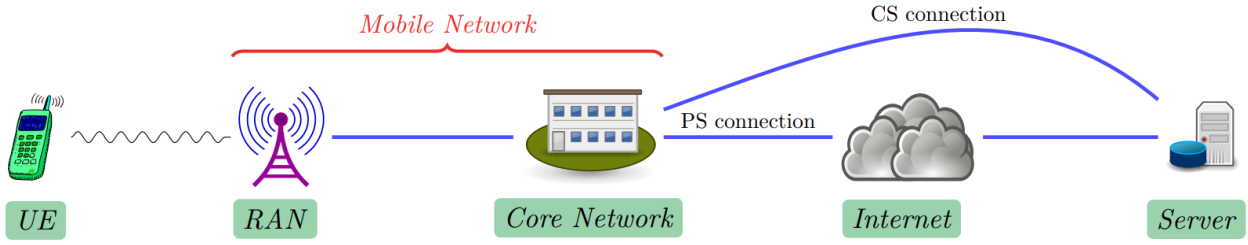
درس آشنایی با شبکه های تلفن همراه

غزل عربعلی - ۹۷۵۲۱۳۹۶، بهاره کاوسی نژاد - ۹۹۴۳۱۲۱۷

آخرین ویرایش: ۱۳ تیر ۱۴۰۳ در ساعت ۱۱ و ۴۳ دقیقه

۱ شرح پروژه

گسترش روزافزون شبکه های تلفن همراه به ویژه شبکه های نسل چهار و پنج، موجب شده است که این شبکه ها به عنوان بزرگترین شبکه دسترسی [۱] ، برای دستیابی به خدمات اینترنت بشمار آید. پرواضح است که در این بین، مساله امنیت [۲] برنامه های کاربردی [۳] و ساخت یک برنامه کاربردی با یک ارتباط امن، یکی از مهم ترین مسایل این حوزه خواهد بود. گرچه باید به این نکته توجه داشت که امنیت در یک ارتباط از طریق شبکه های تلفن همراه را، نباید تنها به مساله امنیت در دو سوی مشتری [۴] و خدمت گزار [۵] تقلیل داد؛ بلکه در جای جای این ارتباط، ما می توانیم با حملات متعددی مواجه شویم، که می تواند محرمانگی [۶] ، یکپارچگی [۷] و حریم خصوصی [۸] ما را هدف قرار دهد. شکل ۱.۱ نمایی از ارتباط یک مشتری با خدمت گزار را در بستر های مختلف از طریق شبکه های تلفن همراه به زیبایی نشان می دهد.



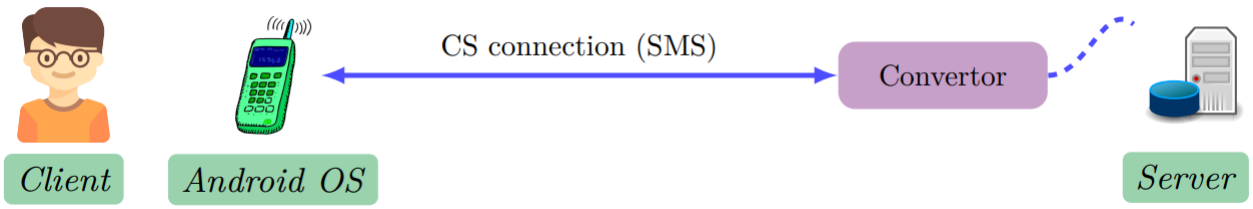
شکل ۱.۱: ارتباط بین مشتری با خدمت گزار از طریق شبکه های تلفن همراه بر روی بسترهای مختلف

در مساله پیش رو، فرض می کنیم که یک برنامه کاربردی داریم، که توسط برنامه UE می شود. UE از دیدگاه ما هر ابزاری است که توسط آن بتوان به شبکه های تلفن همراه متصل شد. UE می تواند گوشی تلفن همراه، تبلت و یا حتی هر شی در IoT [۹] باشد. گرچه در این پروژه، ما تنها بر روی گوشی های تلفن همراه و تبلت ها تمرکز خواهیم کرد.

برنامه کاربردی UE قرار است تا از طریق بسترهای موجود در شبکه های تلفن همراه به یک خدمت گزار مشخص متصل شوند و با آن تبادل اطلاعات داشته باشند. در این جا ما دو راه کار برای اتصال به خدمت گزار داریم. در راه کار نخست و بدیهی ترین شیوه، ما از طریق بستر اینترنت با خدمت گزار به تبادل داده مبادرت می ورزیم. ما اصطلاحا به این شیوه اتصال از طریق PS [۱۰] می گوییم.

[۱] Access Network
[۲] Security
[۳] Application
[۴] Client
[۵] Server
[۶] Confidentiality
[۷] Integrity
[۸] Privacy
[۹] Internet of Things
[۱۰] Packet-switched

بالاخره باید پذیرفت که دنیای اینترنت، مخاطرات پیدا و پنهان فراوانی دارد. اتصال از طریق خدمات CS [11] [12] نظیر تماس [13] و SMS [14] ، می تواند راه فراری از مخاطرات دنیای اینترنت باشد. در این پروژه، ما فرض می کنیم که اتصال مشتری به خدمت گزار را از طریق SMS ، برقرار خواهد شد.



شکل ۲.۱: معماری سطح بالای سامانه

در این جا برای سادگی فرض کنید که دو گوشی داریم. گوشی سمت مشتری و گوشی که ما به عنوان خدمت گزار از آن استفاده می کنیم. در سمت خدمت گزار (که در حقیقت یک گوشی معمولی است)، یک برنامه Android ای با کارکرد Backend نصب می شود. مشتری از طریق SMS فرمان ها را به سمت مقابل (خدمت گزار) ارسال می کند. مشتری می بایست به صورت مداوم اطلاعات مربوط به توان دریافتی و تکنولوژی سلول خدمتگزار [15] و مکان دریافت این اطلاعات را در صورتی که توان از یک سطح آستانه معین پایین بیاید در قالب یک پیام برای خدمت گزار ارسال کند. در این سامانه می بایست به نکات زیر دقت کنید:

- برنامه سمت خدمت گزار می بایست به صورت یک سرویس در Android باشد، البته برای مدیریت و پیکربندی آن می توان یک برنامه UI دار نیز داشته باشیم.
- فرض کنید که همگان پروتکل ارتباطی شما را که مبتنی بر SMS است می دانند. اگر اجازه دهیم SMS از هر شماره ای به سمت خدمت گزار ارسال شود، رویه ای در نظر بگیرید که جلوی دسترسی های غیرمجاز را بگیرد. شاید یک رویه ساده، ارسال یک رمز عبور [16] در ابتدای SMS است. تلاش کنید تا رویه های بهتری برای حل این چالش در نظر بگیرید.
- در هنگامی که مشتری درخواست خود را برای خدمت گزار ارسال می کند، خدمت گزار درخواست را می بایست اجرا کند و پاسخ را در یک SMS جداگانه برای مشتری ارسال کند. دقت کنید اگر بتوانید باید تشخیص بدهید که Delivery بر می گردد یا خیر. اگر برنگشت باید پیام را دوباره ارسال کنیم.
- در پیام ارسالی از سوی مشتری، می بایست مکان اندازه گیری، مقداری اندازه گیری و اطلاعات سلولی که به آن متصل است را ارسال کند.
- پروتکل ارتباطی را باید به صورت کامل مستند بکنید، و باید مبتنی بر پروتکل SMPP [17] باشد.

[11] Service
[12] Circuit-switched
[13] Call
[14] Short Message Service
[15] Serving Cell
[16] Password
[17] Short Message Peer-to-Peer

۲ مراجع

۱ •