به نام خدا

سوالات طراحی شده مبحث امنیت NFC(Near Field Communication)

درس امنیت شبکه دکتر فانیان

سید شایان هاشمی – 9518504

1. انواع حالت های کاری NFC را نام برده و توضیح دهید؟

حالت Active: این حالت تراشه انرژی مورد نیاز خود را از یک منبع مخصوص برای خود تامین می‌کند.

حالت Passive: در این حالت انرژی مورد نیاز تراشه از میدان مغناطیسی که توسط یک مدار دیگر ایجاد شده تامین می‌شود.

حالت Card Simulation: در این حالت که مخصوص برخی از تراشه های Active است، تراشه مانند یک تراشه Passive عمل می‌کند در حالی که خود یک منبع تغذیه مستقل دارد.

2. نحوه کار پروتکل Android Beam را توضیح دهید؟
این پروتکل حالت NFC دستگاه ارسال کننده را به Card Simulation و دریافت کننده را به Active تغییر می‌دهد، سپس با قرار گرفتن فرستنده در میدان دریافت مغناطیسی دریافت کننده در طریق پروتکل NFC برروی یک بستر ارسال(عموما Wi-Fi Direct و Bluetooth Low Energy) و یک کلید توافق می‌کنند. سپس ارسال کننده در بستر مورد نظر به دریافت کننده متصل شده و فایل یا اطلاعات مورد نظر خود را ارسال می‌کند.
3. چرا در پروتکل های انتقال فایل از NFC برای بستر اصلی ارتباط استفاده نمی‌کنند؟
بستر NFC بستری کندی برای انتقال فایل های بزرگ است و به محض خارج شدن یکی از طرف‌های ارتباط از میدان، ارتباط قطع شده.

4. درباره Contactless Token ها توضیح دهید.

این Application یکی از کاربردهای رایج NFC است. در این کاربرد یکی از طرفین حامل یک token یا یک یا چند پارامتری است که بتوان token را به کمک آنها به دست آورد. این به این معناست که پردازنده ای در بخش token وجود ندارد و صرفا عملیات خواندن و نوشتن از آن انجام می‌شود. (منظور از نبودن پردازنده، پردازنده هایی که قابلیت برنامه ریزی شدن توسط کاربر را داشته باشند است)

5. درباره Ticketing / Micro Payment توضیح دهید.

این Application یکی از کاربردی های NFC است که در سال های اخیر بسیار مورد استفاده قرار گرفته است. تفاوت عمده این کاربرد با Contactless Token در پردازنده قابل برنامه ریزی شدن توسط کاربر در بخش token است. این پردازنده هیچ پارامتری را به صورت مستقیم در اختیار سمت Active ارتباط قرار نمی‌دهد و فقط با استفاده از پارامتر های ذخیره شده و دریافتی از سمت Active نتیجه هایی را تولید می‌کند.

6. با فرض داشتن 2 دستگاه Active که یکی از آنها قابلیت Card Simulation را دارد، یک پروتکل طراحی کنید که بتوان پرداخت را از طریق NFC و به صورت امن و بدون ارسال مستقیم کلید انجام دهد.

در این پروتکل که الهام گرفته از Google Wallet است، از بستر PKI استفاده می‌کند و پرداخت کننده قبلا کلید عمومی خود را در یک مخزن کلید (مثلا مخزن Google Wallet) قرار داده است و همچنین کلید عمومی مخزن نیز در برنامه وجود دارد. هر دستگاه POS دارای یک کلید خصوصی است که کلید عمومی متناظر آن توسط مخزن امضا شده. در ابتدا دستگاه POS یک صورت حساب تولید شده را امضا کرده و همراه با کلید عمومی امضا شده برای پرداخت کننده می‌فرستند، پرداخت کننده پس از بررسی صحت کلید عمومی، امضای صورت حساب را بررسی کرده و در صورت درست بودن آن را به کاربر نمایش می‌دهد. پس تایید صورت حساب توسط کاربر صورت حساب را با کلید خصوصی خود امضا کرده و مجددا برای دستگاه POS می-فرستد. بعد از دریافت امضا توسط دستگاه POS این دستگاه اقدام به ارسال اطلاعات به مخزن و خواهان بررسی امضا می‌شود. در صورت درست بودن مخزن پول را به حساب دستگاه انتقال می‌دهد.

7. چرا در NFC حمله ی Man in The Middle وجود ندارد؟

در حمله Man in The Middle نیاز است که یک جزء ما بین ارتباط دو جزء دیگر قرار گرفته و مانع از ارتباط مستقیم بین آن دو شده. این عملیات در NFC امکان پذیر نیست. حتی اگر با

استفاده از قوی‌ترین آنتن ها امکان شنود برقرار شود. امکان تغییر یا اختلال وجود ندارد چرا که با ارسال به یک جزء به جزء دیگر نیز همزمان ارسال می‌شود و A با مشاهده داده های ارسالی غلط توسط خود، عملیات را متوقف می‌کند.

8. روش مقابله با حمله Data Corruption را توسط تراشه های NFC را توضیح دهید.

تراشه های NFC قابلیت خواندن در عین نوشتن را دارند. این امکان را می‌توان برای بررسی حمله Data Corruption استفاده کرد. در این حمله که حمله کننده اقدام به ارسال پارازیت بر روی ارتباط دو طرف می‌کند، کافیست ارسال کننده در حال ارسال به داده های خود گوش دهد و از صحت آنها مطلع گردد و در صورت نیاز عملیات ارسال را مجددا انجام دهد.

9. یک پروتکل Key Exchange برای توافق برای روی یک کلید به صورت امن در بستر NFC ارائه دهید.

دو طرف اقدام به تولید عدد تصادفی می‌کنند. سپس شروع به ارسال اعداد کرده و در عین حال به میدان ایجاد شده گوش می دهند. در این صورت برای تراشه چهار حالت مختلف رخ می-دهد. 1) خود 0 باشد میدان نیز 0 باشد. 2) خود 0 باشد میدان 1 باشد 3) خود 1 باشد میدان 0 باشد 4) خود 1 باشد میدان نیز 1 باشد. هر دو تراشه بعد از ارسال اعدادی که حاصل از حالت 1 و 4 بوده را دور میریزند و دیگر اعداد را نگه می‌دارند. این کلید مشترک بین هر دو خواهد بود.

10. با فرض این که baud rate در پاسخ سوال قبل برابر با 106k باشد. زمان متوسط مورد نیاز برای رسیدن به یک کلید 128 bit مشترک را محاسبه کنید.

احتمال نگه داشتن کلید $\frac{2}{4} = \frac{1}{2}$ است. پس برای ارسال 128 بیت کلید معتبر حدود 256 بیت بایستی ارسال شود. و با توجه به نرخ 106k زمان ارسال برابر با 2.4ms خواهد بود.

$$\left(\frac{1}{106000}\right) \times 256 = 0.002415$$