اولين همايش بين‌المللي
بانكداري الكترونيک و
نظام هاي پرداخت
(اول اسفند 1390 ــ برج ميلاد)

پروتكلهاي ارتباطي در پرداخت همراه و امنيت آنها

ارائه دهندگان

دكتر هادي‌شهريار شاه‌حسيني
عضو هيات علمي دانشكده مهندسي برق
دانشگاه علم و صنعت ايران

مهندس خديجه افهامي
دانشجوي دكتراي دانشكده مهندسي برق
دانشگاه علم و صنعت ايران

اولین همایش بین‌المللی بانکداری الکترونیک و نظام های پرداخت
(اول اسفند 1390 ــ برج میلاد)

پروتکلهای ارتباطی در پرداخت همراه و امنیت آنها

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

فهرست مطالب

۵ سامانه های پرداخت الکترونیکی همراه

- مقدمه و تاریخچه سامانه‌های پرداخت الکترونیکی همراه
- ویژگی ها و مزایای سرویس‌های کیف پول الکترونیکی
- بررسی اجزای و واحدهای یک سامانه پرداخت الکترونیکی همراه
- معرفی معماری‌های ارتباطی در سامانه‌های پرداخت الکترونیکی همراه
- بررسی معماری NFC مورد استفاده در سامانه‌های پرداخت الکترونیکی همراه

۶ چالش‌های امنیتی سامانه‌های پرداخت الکترونیکی همراه

- مبانی امنیت در شبکه و پروتکل‌های ارتباطی
- بررسی چالش‌های امنیتی در کیف پول الکترونیکی
- آسیب‌پذیری‌های پروتکل‌های پرداخت الکترونیکی همراه
- امنیت سامانه‌های پرداخت مبتنی بر NFC

قسمت اول: سامانه های پرداخت الکترونیکی همراه

خدمات مالی همراه

خدمات مالی همراه شامل:

پول همراه، پرداخت همراه، بانکداری همراه، انتقال پول همراه و کیف همراه

ویژگی:

۱- براساس قوانین مالی

۲- وسیله همراه

پرداخت همراه:

- یک پرداخت به صورت یک انتقال وجه برای کالاها و سرویسها می‌باشد که تلفنهای همراه درگیر راه اندازی (initiation) و تاییدیه (confirmation) می‌باشند.

- در پرداخت همراه موقعیت پرداخت کننده (payer) و زیرساختارهای پشتیبانی شده مهم نمی‌باشد.

ارائه دهنده:
دكتر شاه حسيني
مهندس افهامي

ارائه دهنده:
دکتر شاه حسيني
مهندس افهامي

خدمات مالی همراه

سفارش همراه

- استفاده از تلفن همراه برای راه اندازی سفارش بدون پرداخت.
- مثال: سفارش غذا از طریق تلفن همراه و پرداخت در تحویل

تحویل همراه

- تراکنش هنگامی که تلفن همراه برای تحویل کالاها و سرویس‌ها بدون انجام پرداخت.
- مثال: هنگامی که بلیط بر روی تلفن همراه رویت شود

احراز اصالت همراه

- استفاده از وسایل همراه برای احراز اصالت کاربر به عنوان یک قسمت از تراکنش های پرداخت یا جهت دسترسی به برخی اطلاعات یا کارکردها.
- یک کد با یک تلفن همراه فرستاده می شود که کاربر در کاربردهای برخط شناسه خود را معتبر کند.

مشخصات پرداخت همراه

یک خدمت پرداخت همراه به عنوان یک روش پرداخت در بازار پذیرفته می‌شود اگر مشخصات زیر را در بازار تامین کند:

سادگی و قابلیت استفاده

- ✓کاربرد پرداخت موبایل باید کاربر پسندانه باشد.
- ✓مشتری نیز باید قادر باشد پرداخت موبایل مطابق با نیازهای خود تغییر دهد.

عمومیت (Universality)

- ✓پرداخت خدمات باید برای انجام معاملات بین یک مشتری به یکی دیگر از مشتری (C2C)، و یا از یک کسب و کار به مشتری (B2C)و یا بین کسب و کار(B2B) بتواند استفاده شود.
- ✓محیط تحت پوشش باید شامل محیط های داخلی، منطقه ای و جهانی باشد.
- ✓پرداخت ها باید برای پرداختهای کم ارزش و ارزش بالا قابل استفاده باشد.

همکاری (Interoperability)

- ✓توسعه باید بر اساس استانداردها و فناوری های باز است.
- ✓پیاده سازی سیستم باید قادر تعامل با سیستم های دیگر قادر باشد.

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

مشخصات پرداخت همراه

یک سرویس پرداخت همراه به عنوان یک روش پرداخت در بازار پذیرفته می‌شود اگر مشخصات زیر را در بازار تامین کند (ادامه):

امنیت، حریم خصوصی و اعتماد مشتری

- ✓یک کاربر باید به فراهم کننده پرداخت همراه اعتماد کند
- ✓ عدم امکان سو استفاده (تراکنشات محرمانه باشد که عدم افشای اطلاعات کارت مشتری)
- ✓ سیستم پرداخت باید قادر باشد دربرابر حمله نفوذگران مصنون بماند.

هزینه

- ✓سامانه های پرداخت همراه نباید نسبت به سامانه های پرداخت موجود پر هزینه تر باشند.

سرعت

- ✓ سرعت سامانه های پرداخت همراه باید برای مشتریان و بازرگانان قابل قبول باشد.

اتصال به سایر سامانه های پرداخت

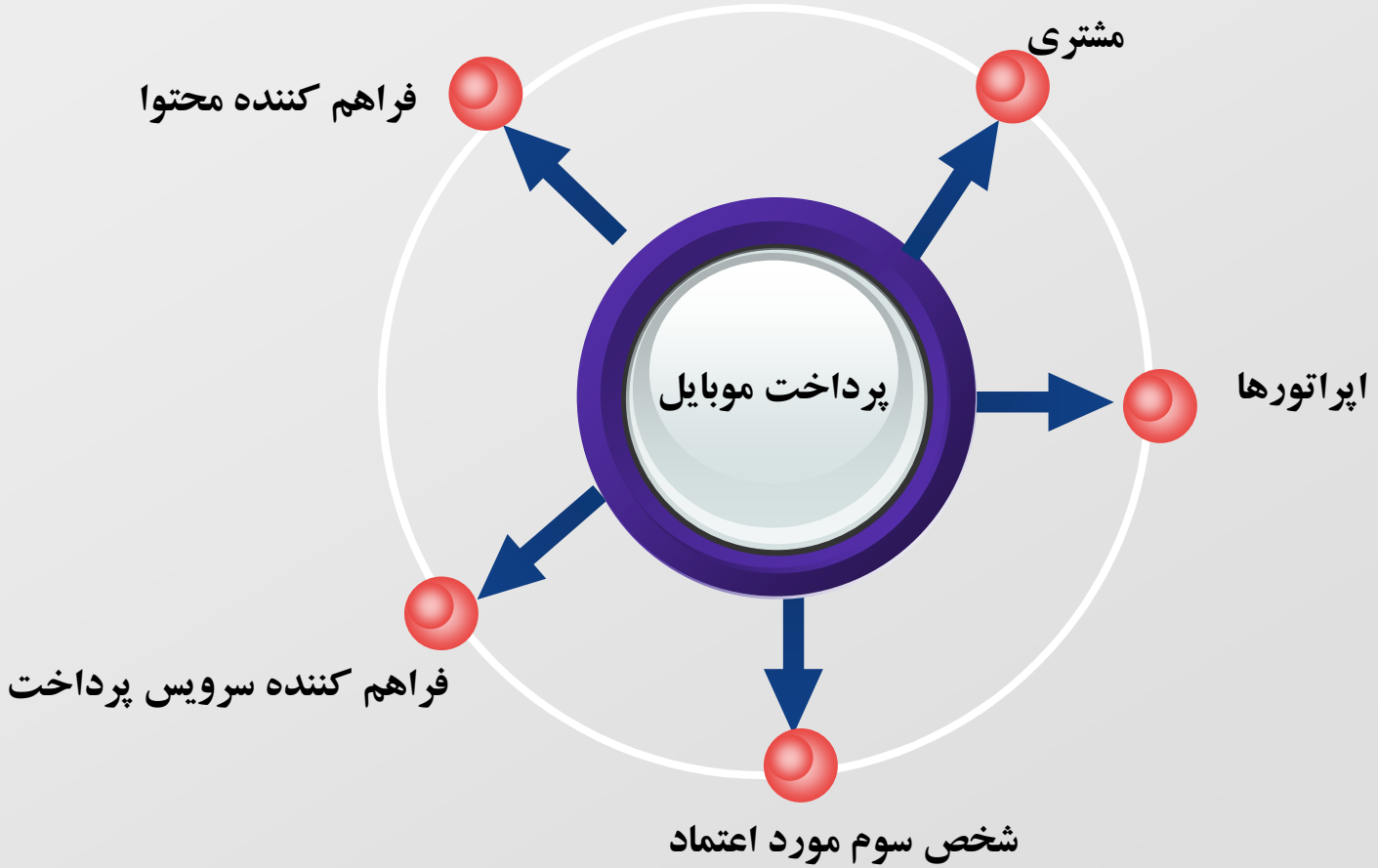
- ✓ برای پذیرفتن کاربردهای پرداخت همراه، سامانه پرداخت همراه باید در سراسر جهان باید قابل استفاده باشد

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

پروتکلهاي
ارتباطي در
پرداخت همراه و
امنيت آنها

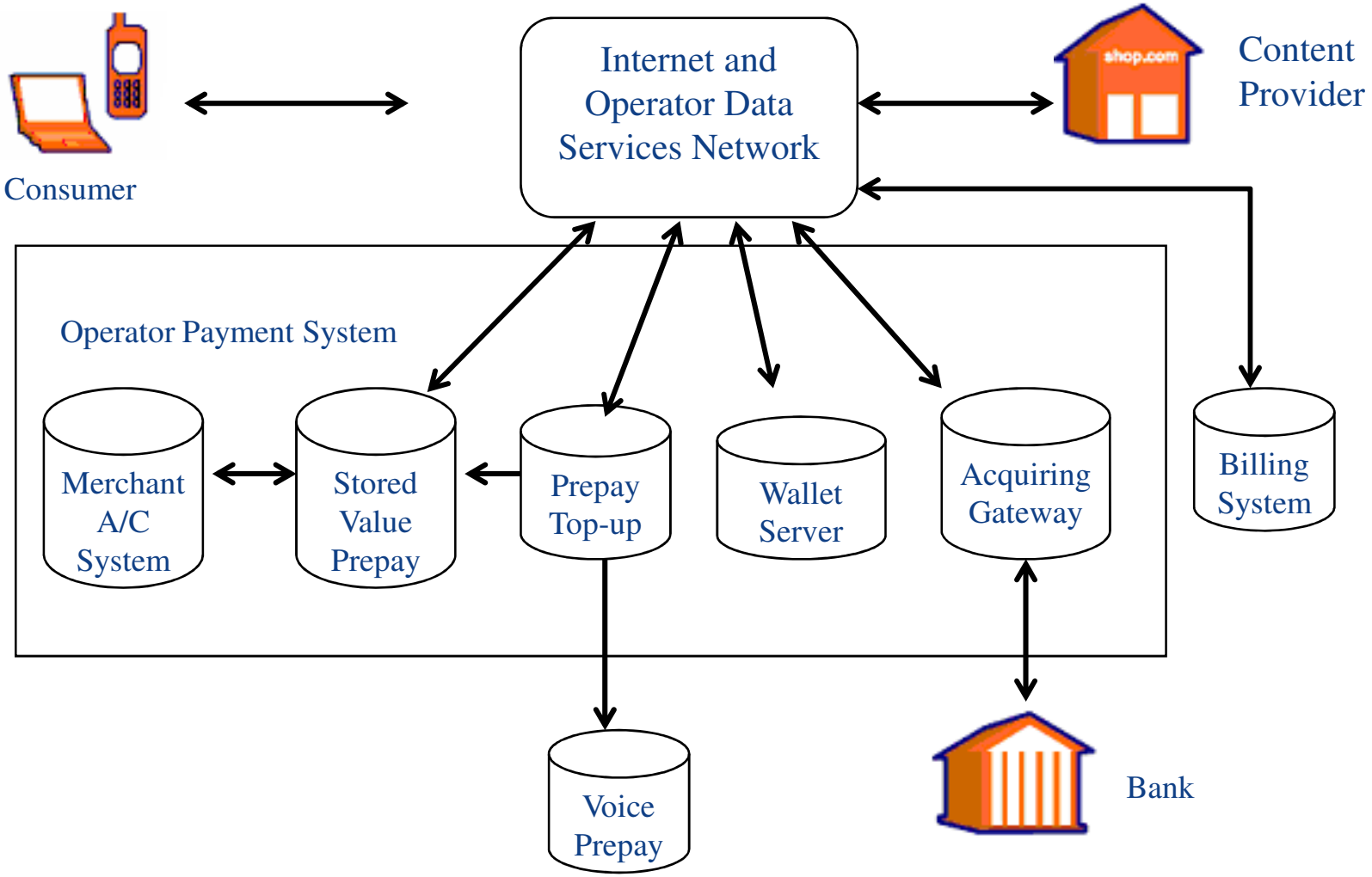
ارائه دهنده:
دکتر شاه حسيني
مهندس افهامي

بازیگران پرداخت همراه



بازیگران پرداخت همراه

ارائه دهنده:
ثر شاه حسینی
هندس افهامی



بازیگران پرداخت همراه

مشتری کسی است که یک وسیله همراه دارد و می خواهد از طریق آن هزینه خدمت یا محصول را بدهد.

- مشتری خرید همراه را راه اندازی می کند
- مشتری به فراهم کننده پرداخت رجیستر می شود.
- مشتری مجوز پرداخت را می دهد.

یک فراهم کننده محتوا یا بازرگان محصولات را به مشتری می فروشد.

- در پرداخت همراه، محتوا می تواند از اخبار یا سرویس‌ها، خرید و سرویسهای بلیط یا خدمات سرگرمی و خدمات مالی باشد.
- فراهم کننده محتوا یا بازرگان درخواستهای خرید را به فراهم محتوا کننده خدمت ارسال می کند.
- برگشت درخواستهای دریافت مجوز را به مشتری رله می کند
- مسئول دریافت محتوا می باشد.

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

بازیگران پرداخت همراه

❖فراهم کننده سرویس پرداخت

✓مسئول کنترل جریان تراکنش میان مشتریان همراه ، فراهم کنندگان محتوا و شخص سوم مورد اعتماد.

✓فراهم کننده سرویس همراه می تواند اپراتور موبایل، بانک یک شرکت کارت اعتباری یا یک شرکت پرداخت مستقل باشد.

❖شخص سوم مورد اعتماد (TTP)

✓شخص سوم مورد اعتماد می تواند اپراتوررها، بانکها و شرکتهای کارت اعتباری باشد.

✓نقش اصلی TTP احراز اصالت و مجازشناسی تراکنشات و توافق پرداخت می باشد.

❖اپراتورهای موبایل

اپراتورهای موبایل مسئول استاندارد سازی و تعامل با سیستم های پرداخت دیگر هستند.

چرخه زمانی پرداخت همراه

ثبت نام (*Registration*)

مشتری یک حساب با فراهم کننده سرویس پرداخت برای سرویس پرداخت از طرق یک روش پرداخت خاص باز می کند.

تراکنشات (*Transaction*)

1. مشتری درخواست خرید خود را با فرستادن یک درخواست (برای مثال اس ام اس) به فراهم کننده محتوا می فرستد.
2. فراهم کننده محتوا درخواست را به فراهم کننده سرویس پرداخت ارسال میکند.
3. فراهم کننده خدمت، پرداخت از شخص سوم مورد اعتماد برای احراز اصالت و مجازشناسی درخواست میکند.
4. فراهم کننده خدمت پرداخت، فراهم کننده محتوا را از وضعیت احراز اصالت و مجازشناسی آگاه می سازد. اگر مشتری به طور موفقیت امیز احراز اصالت و مجازشناسی شده باشد فراهم کننده محتوا، محتوای درخواستی را میدهد.

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

ارائه دهنده:
دكتر شاه حسيني
مهندس افهامي

چرخه زمانی پرداخت همراه

تسویه حساب (*Payment settlement*)

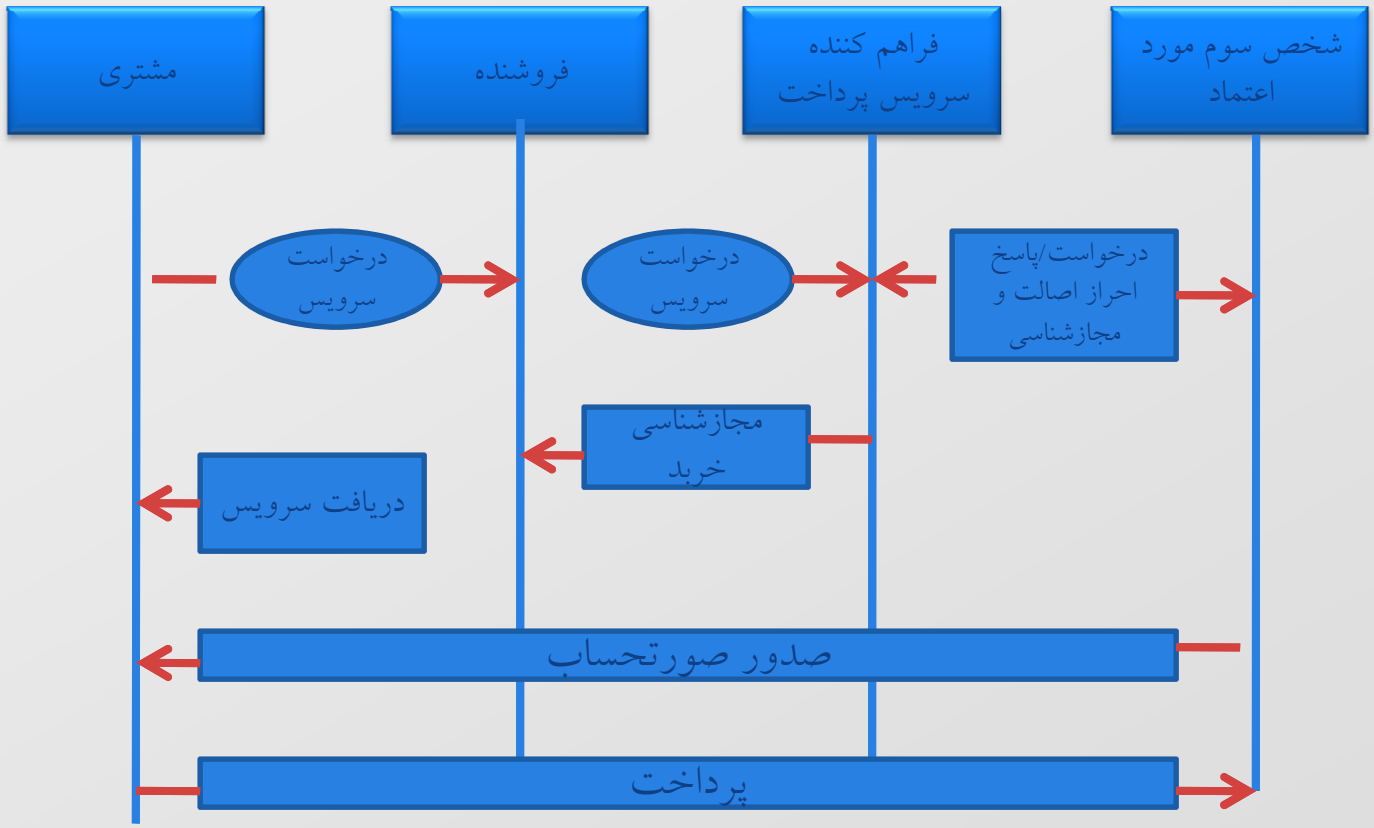
تسویه حساب می تواند به سه صورت زیر باشد.

- ✓ روش پرداخت بلادرنگ
- ✓ روش پیش پرداخت
- ✓ روش پس پرداخت

پروتکلهاي
ارتباطي در
پرداخت همراه و
امنيت آنها

ارائه دهنده:
دکتر شاه حسيني
مهندس افهامي

چرخه زمانی پرداخت همراه



پرداخت همراه

پرداخت همراه یک روش پرداخت به جای پرداخت از طریق پول نقد، چک، کارتهای اعتباری است که از یک تلفن همراه برای پرداخت یک رنج وسیع از کالاهای دیجیتال یا سخت استفاده می شود.

- کالاهای دیجیتال همانند موزیک، ویدئو، آهنگها، بازیهای آنلاین و....
- هزینه حمل و نقل، پارکینگ و...
- کتابها، مجله، بلیط

چهار روش برای پرداخت همراه وجود دارد:

- پرداخت از طریق SMS
- صدور صورتحساب مستقیم
- پرداخت وب همراه
- پرداخت بی تماس

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

پروتکلهاي
ارتباطي در
پرداخت همراه و
امنيت آنها

ارائه دهنده:
دکتر شاه حسيني
مهندس افهامي

پرداخت همراه از طریق SMS

- مشتری یک درخواست پرداخت از طریق پیام اس ام اس یا یک USSD از طریق یک کد کوتاه به صدور حساب تلفن یا کیف انلاین فروشنده ارسال می شود.
- روش پرداخت از طریق اس ام اس در کشورهای اروپایی و آسیایی رایج می باشد.
- با ارایه روشهای پرداخت دیگر همانند پرداختهای وب موبایل، پرداخت موبایل کلاینت (اندروید) و صدور حساب پرداخت موبایل زیاد مورد توجه نیست.

ارائه دهنده:
دکتر شاه حسيني
مهندس افهامي

پرداخت همراه از طریق SMS

۱- قابلیت اعتماد پایین

تراکنشات پرداخت می تواند به سادگی از بین رود.

۲- سرعت پایین

فرستادن اس ام اس برای مشتری و فروشنده زمانبر است.

۳- امنیت

رمزنگاری SMS/USSD تا رابط رادیویی می باشد.

۴- هزینه بالا

هزینه های زیادی برای این روش پرداخت وجود دارد.

۵- نرخ payoutپایین

۳۰٪ الی ۵۰٪

صورتحساب همراه مستقیم

مشتری از گزینه صورتحساب همراه در هنگام بازدید از یک سایت بازرگانی الکترونیکی استفاده میکند.

- ✓ در این روش پرداخت مشتری، از احراز اصالت دو عامله شامل یک PIN و کلمه عبور یکبار مصرف استفاده می کند.
- ✓ حساب همراه مشتری برای خرید شارژ می‌شود.
- ✓ صورت حساب همراه مستقیم یک راهکار ارائه شده برای پرداخت است که نیازی به کارتهای اعتباری/بدهکاری یا پیش ثبتنام در یک پرداخت آنلاین نیست.

این روش پرداخت بیشتر در آسیا رایج می باشد و دارای مزایای زیر می باشد.

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

ویژگیهای صورتحساب همراه مستقیم

❖**امنیت**

احراز اصالت دوعامله و ماشین مدیریت خطرپذیری (ریسک) از تقلب جلوگیری میکند.

❖**راحتی**

هیچ پیش ثبت نام و نرم افزار همراه مورد نیاز نیست.

❖**سرعت**

بیشتر تراکنشات در کمتر از ده ثانیه انجام می شود.

❖**توسعه یافتگی (آزمایش شده)**

۷۰ درصد خریدهای برخط دیجیتال در برخی از مناطق آسیا از این روش استفاده میکنند.

پروتکلهای ارتباطی در پرداخت همراه و امنیت آنها

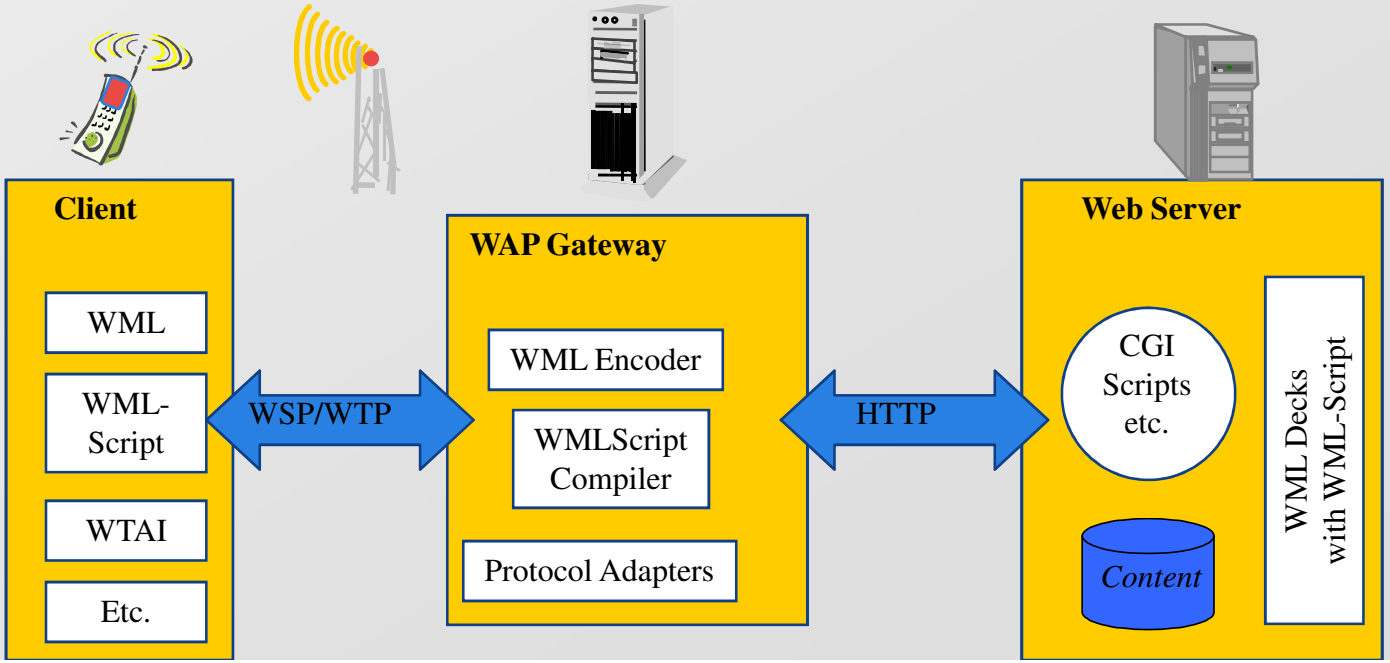
ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

پرداختهای وب همراه

مشتریان از صفحات نمایش شده یا برنامه های کاربردی دانلود و نصب شده بر روی تلفن همراه برای پرداخت استفاده میکنند.

پرداخت وب همراه از پروتکل کاربرد بیسیم WAP استفاده میکنند در نتیجه مزایا و معایب آن شبیه WAP است.

- استفاده آسان: مشابه خرید از صفحات وب
- رضایت بالای مشتری: سرعت بالا



ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

پرداختهای بدون تماس

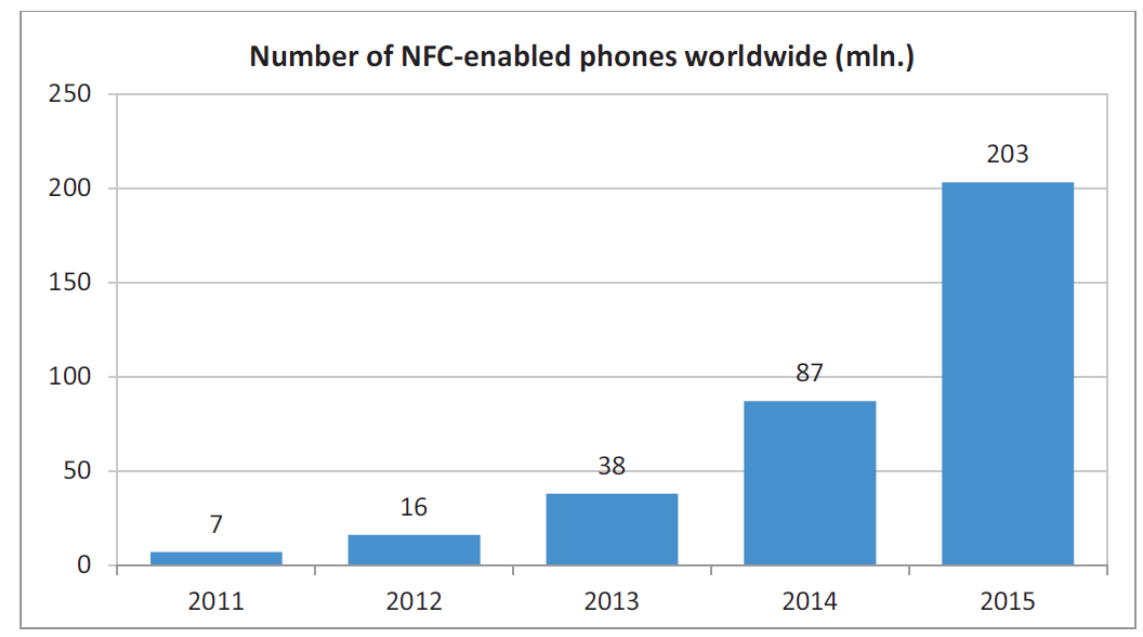
- ارتباطات میدان نزدیک یا NFC برگرفته از فناوری برگرفته از فناوری RFID می‌باشد
- محدودیت عمده RFID ارتباط یک طرفه آن است که از کد به READER است.
- این محدودیت در سال ۱۹۹۰ میلادی برای اولین بار توسط فیلیپس و سونی مطرح شد.
- این دو شرکت یک استاندارد برای ارتباط دو طرفه تماسی ارایه کردند. این استاندارد ارتباط میدان نزدیک یا NFC نامگذاری شد.

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

پرداختهای بدون تماس

❖ این استاندارد از سال ۱۹۹۰ میلادی مطرح شد و در سال ۲۰۰۳ میلادی توسط موسسه ISO مطرح شد که به عنوان یک استاندارد باز برای ارتباطات دو طرفه است.

❖ همراه با توسعه ارتباط دو طرفه تماس، پیشرفت های زیادی در سرعتی که با آن داده ها منتقل شده و امنیت داده های منتقل شده از طریق رمز گذاری انجام شده است.



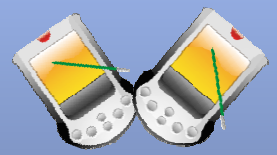
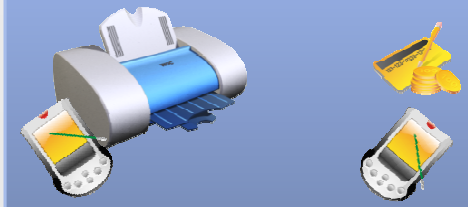
پروتکلهای ارتباطی در پرداخت همراه و امنیت آنها

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

پروتكلهاي
ارتباطي در
پرداخت همراه و
امنيت آنها

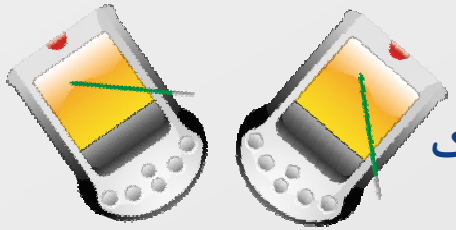
ارائه دهنده:
دكتر شاه حسيني
مهندس افهامي

دسته بندی روشهای پرداخت همراه براساس ابعاد

	P2P	C2P
فناوری نزدیک	پرداختهای بی تماس 	پرداختهای بی تماس تلفن موبایل به عنوان POS 
فناوری راه دور	انتقال پول همراه 	پرداخت برخط همراه 

روشهای پرداخت بدون تماس نزدیک

در روشهای پرداخت بدون تماس، پرداختها به صورت نزدیک کردن بدون تماس صورت می‌گیرد.



کاربردهای پرداخت بدون تماس نزدیک

- پرداخت با دستگاه pos با نگه داشتن تلفن موبایل به صورت نزدیک
- انتقال پول به دوستتان از طریق حرکت دادن تلفن به همدیگر
- پرداختن بلیط مترو با نزدیک کردن به دستگاه reader
- پرداخت های بدون تماس می تواند میلان مشتریان (P2P) و میان مشتریان و بازرگانـان (C2B) انجام شود.

فناوری بدون تماس نیز به دو دسته زیر تقسیم بندی می شود:

- در حومه (Vicinity): این فناوری بیشینه مسافت خواندن را بین ۱ تا ۱.۵ متر قرار میدهد.
- نزدیک (Proximity): این فناوری برای مسافتهای خیلی نزدیک برابـر بـا ۷.۵ سـانتی متـر قـرار میدهد.

ارائه دهنده:
دكتر شاه حسيني
مهندس افهامي

روشهای پرداخت بدون تماس نزدیک

تلفن همراه همانند POS

در سالهای اخیر استفاده از تلفن همراه به عنوان یک pos (point of sale) برای گرفتن جایگاه کارتهای پرداخت مرسوم شده است.

کاربردها

- پرداخت کردن به تاجر در رستوران یا فست فود

- با استفاده از یک وسیله اضافی و یک برنامه کاربردی برای سخت‌افزار، تلفن همراه می تواند کارتهای پرداخت را قبول کند.

- کارت خوان خارجی، پرداختها به صورت معمولی میان مشتری و شرکتهای کوچک برقرار میکند. هدف این دستگاه برای شرکتهای نه انچنان بزرگ به جای وسایل pos قدیمی می باشد.

ارائه دهنده:
دكتر شاه حسيني
مهندس افهامي

روشهای پرداخت همراه دور

انتقال پول همراه

یک انتقال پول همراه وجوه از یک مشتری به دیگری در راه دور می باشد:

- **پرداخت ها میان مشتریان در یک کشور می باشد. در کشورهای توسعه یافته میان مردم در یک شهر و شهرهای دیگر کشور میباشد. بنابراین یک کشور همانند چین یک بازار بزرگ برای انتقال پول همراه میان p2p وجود دارد که برای مثال توسط خدمات PayPal پشتیبانی شده است.**

- **اکثریت انتقالات پول همراه شامل مشتریان در سرتا سر جهان می باشد. این محدوده remittances نامیده می شود.**

براساس گزارش اخیر بانک جهانی پول منتقل شده با این روش حدود ۳۲۵ بیلون در سال ۲۰۱۰ بوده و انتظار می رود که به ۴۰۴ بیلون در سال ۲۰۱۳ میلادی برسد.

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

روشهای پرداخت همراه دور

ارائه دهنده:
دكتر شاه حسيني
مهندس افهامي

پرداختهای برخط همراه

پرداختهای آنلاین همراه پرداختهایی هستند که از طریق مرورگر وب یا از طریق یک برنامه کاربردی بر روی تلفن همراه انجام میشود.

پرداختهای برخط همراه وجود دارد که هر دو برای B2C کاربرد دارد:

- بازرگانی همراه
- کالاهای دیجیتال

✓ بازرگانی همراه برای خرید برخط برای کالاها یا وسایل بر روی تلفن همراه می‌باشد.
✓ خریدن کالاهای دیجیتال بر روی تلفن همراه از طریق بسترهای همراه می باشد.

✓ پرداختهای همراه معمولا توسط کارتهای پرداخت ذخیره شده و لینک شده به اکانت کاربر بر روی تلفن همراه یا کارتهای اعتباری پیش پرداخت شده به حساب کاربر انجام میشود.

استقبال فراهم آورندگان سرویس‌های پرداخت همراه

- اپراتورهای شبکه همراه
- موسسات مالی
- تولید کنندگان گوشی
- فراهم کنندگان فناوری
- بازرگانان
- مصرف کنندگان

اولین همایش بین‌المللی
بانکداری الکترونیک و
نظام های پرداخت
(اول اسفند 1390 ــ برج میلاد)

پروتکلهای
ارتباطی در
پرداخت همراه و
امنیت آنها

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

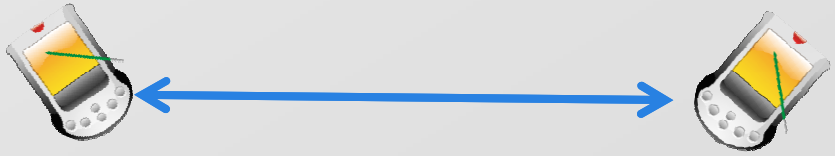
فناوری NFC

❖ ارتباط میدان نزدیک یا NFC (near field communication) یک فناوری ارتباطی بی سیم با فرکانس بالا و دامنه کوتاه می باشد.

❖ انتقال داده بین دستگاه را تا فاصله ای در حدود ۱۰ سانتیمتر با فرکانس 13.56 مگاهرتز و بدون نیاز به تنظیمات کاربر، امکان پذیر می نماید.

❖ برای اینکه دو دستگاه بتوانند با هم ارتباط برقرار کنند کافیست آنها را در نزدیکی یکدیگر قرار داد گیرد.

❖ رابط NFC موجود در دستگاه ها بصورت خودکار تنظیمات مورد نیاز را انجام می دهد و ارتباط اغلب بصورت peer-to-peer بین دو دستگاه برقرار می گردد



ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

فناوری NFC

- این فناوری مبتنی بر RFID بوده و نمونه ساده توسعه یافته ای از استاندارد ISO 14443 که استانداردی برای سیگنال های RFID و کارت های بدون تماس میباشد.
- NFC ترکیبی رابط کارت های هوشمند و خواننده (reader) در یک دستگاه تشکیل شده است.
- این فناوری قادر است با سایر دستگاه های NFC ارتباط برقرار نماید.
- این فناوری می تواند با readerهای و کارت های هوشمند منطبق با استاندارد ISO 14443 ارتباط برقرار کنند.
- هزینه راه اندازی آن بسیار پایین و بصرفه می باشد.
- نرخ تبادل اطلاعات آن به 424 Kb/s می رسد که همین امر قابلیت آن را برای پرداخت ها با حجم بالا بسیار مناسب ساخته است.

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

کاربرد فناوری NFC

کاربردهای فناوری NFC

- تبادلات و پرداخت های سیار با امنیت بالا
- ارتباطات بصورت Peer-to-Peer
- دسترسی به اطلاعات در حین حرکت

- در حال حاضر در بیشتر کشورهای توسعه یافته و برخی کشورهای در حال توسعه بصورت pilot در حال استفاده می باشد.
- تعداد زیادی از شرکت های سازنده گوشی های همراه نظیر Philips, Sony, Nokia, Motorola و ... در حال فعالیت در زمینه این فناوری می باشند تا بتوانند از این طریق سهم بیشتری را در بازار رقابتی امروز از آن خود کنند.

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

بررسی فناوری NFC

NFC مبتنی بر تکنولوژی RFID بوده و از قوانین مشابهی پیروی می نماید.
سامانه های RFID متشکل از دو قسمت زیر می‌باشد:

- ❖ حمل کننده سیگنال (contact less tag) یا Tag
- ❖ دریافت کننده – دستگاه خوانده/نوشتن (read-write-device)

✓ NFC با استفاده از این روش رمزنگاری و همچنین الگوهای رمزنگاری مجزا توانسته سطح بالایی از امنیت را به کاربران ارائه دهد.

✓ این فناوری می تواند از زیرساخت های بی سیم موجود استفاده نماید که همین عدم نیاز به ساختار مجزا منجر به صرفه جویی در هزینه ها و افزایش تمایل به استفاده از این فناوری گردیده است.

✓ با استفاده از NFC می توان بسیاری از فرآیند های بانکی از قبیل دریافت موجودی حساب، پرداخت قبوض و ... را توسط تلفن همراه انجام داد.

پروتکلهای ارتباطی در پرداخت همراه و امنیت آنها

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

ارائه دهنده:
دكتر شاه حسيني
مهندس افهامي

استانداردهای فناوری NFC

نام استاندارد	مشخصات
ISO 18092 (NFCP-1)	رابط NFC و پروتکل-۱ استاندارد شبکه بیسیم برد کوتاه مدهای کاری NFC شباهتهای با استاندارد RFID بیان نرخ های داده
ISO 21481 (NFCIP-2)	رابط NFC و پروتکل-۲
ISO 22536 (NFCIP-1)	رابط و پروتکل NFC نسخه یک روشهای تست رابط فرکانس رادیویی
ISO 23917 (NFCP-1)	روشهای آزمون پروتکل
ISO 28361 (NFC-WI)	رابط سیمی NFC

جریان پروتکل NFC

برای عملکرد صحیح NFCIP-1 باید یک مجموعه عملیات را به ترتیب انجام شود:

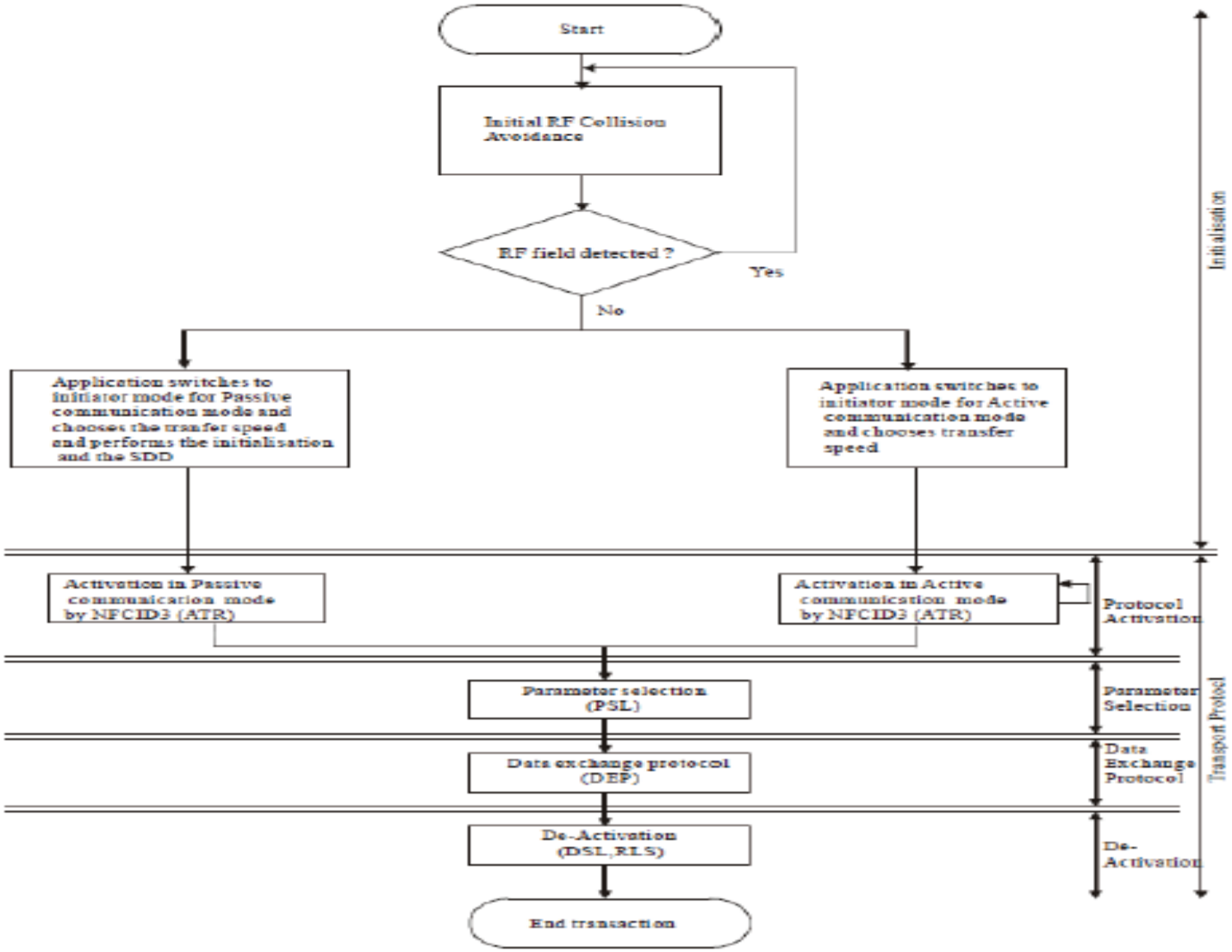
- ✓هر وسیله NFCIP-1 به صورت پیش فرض در مد هدف قرار دارد.
- ✓هر وسیله NFCIP-1 باید به مد آغازگر سویچ کند اگر توسط کاربرد مورد نیاز باشد.
- ✓کاربرد می تواند مد فعال یا غیر فعال خود و سرعت انتقال را انتخاب کند.
- ✓آغازگر باید وجود میدان RF را شناسایی کند اگر میدانی فعال باشد نباید میدان خود را فعال کند.
- ✓اگر میدان خارجی فعال نباشد آغازگر میدان RF را فعال می کند.
- ✓هدف باید توسط میدان RF یا آغازگر فعال شود.
- ✓انتقال اطلاعات در مد فعال یا غیر فعال باید در سرعت انتقال انتخاب شده باشد.
- ✓مد انتقال و سرعت باید متناسب با مد انتقال و سرعت اغازگر باشد.

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

پروتكلهاي
ارتباطي در
پرداخت همراه و
امنيت آنها

ارائه دهنده:
دكتر شاه حسيني
مهندس افهامي

راه اندازی NFC

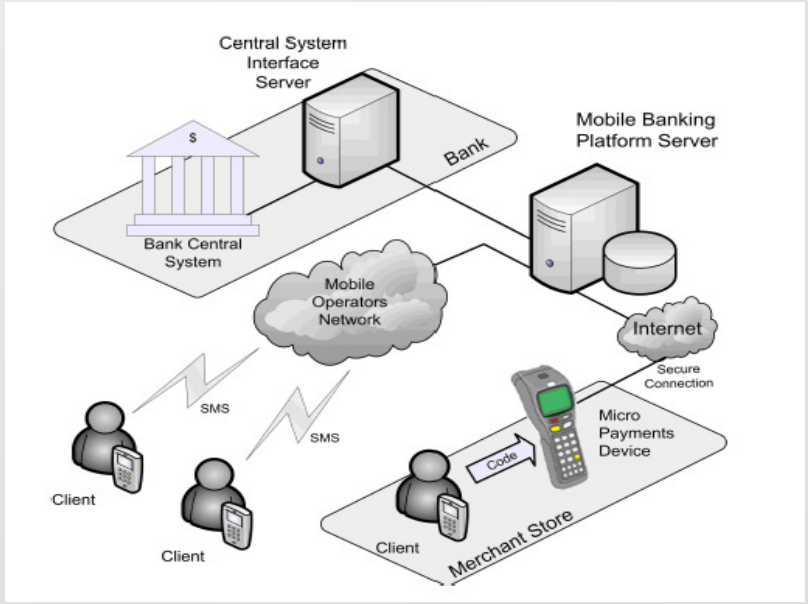


پروتكلهاي
ارتباطي در
پرداخت همراه و
امنيت آنها

ارائه دهنده:
دكتر شاه حسيني
مهندس افهامي

پرداخت توسط NFC

- در فناوری NFC کاربر گوشی همراه خود را که مجهز به فناوری NFC است در نزدیکی دستگاه خواننده (reader) قرار دهد.
- در این صورت دستگاه با ایجاد سیگنال های الکترونیکی تراشه موجود در گوشی را فعال کرده و می تواند اطلاعات مربوط به حساب مشتری و موجودی او را بهمراه اطلاعات هویتی کاربر را از تراشه موجود بدست آورد.



مزایای استفاده از پروتکل NFC در بانکداری

- برقراری ارتباط آسان با دستگاهای همراه مجهز به فناوری NFC
- استفاده از پروتکل WAP
- استفاده از لایه WTLS ، اضافه شدن امکانات امنیتی همانند رمزنگاری و امضای دیجیتال و پروتکل SSL
- توانایی انقال حجم بالا اطلاعات
- NFC می تواند یک فناوری مکمل برای Bluetooth و 802.11 که برد وسیعی دارند
- با استفاده از این فناوری کاربر می تواند بصورت همزمان چندین نوع کارت یا Debit کارت را در تلفن همراه خود داشته باشد

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

انواع مختلف انتقال داده توسط NFC

- NFC وابستگی زیاد به اتصال الکتروستاتیک / مغناطیسی (magnetic/electrostatic) میان وسایل به جای پخش امواج رادیویی همانند فناوری WI-FI دارد.

- وسایل NFC می تواند بر روی قدرت میان الکتریکی و مغناطیسی کم کار کند که منجر به رنج کوتاه ارتباط می شود.

رابط NFC در دو وضعیت مختلف می‌تواند داده‌ها را منتقل کند:

- فعال (Active)
- غیرفعال (Passive)

یک دستگاه فعال (Active) قادر است میدان رادیویی خود (RF) را تولید و به محیط اطراف ارسال کند.

یک دستگاه غیرفعال (Passive) توانایی تولید این امواج را نداشته و از میدان تولیدی دستگاه مقابل استفاده می‌کند.

پروتکلهای ارتباطی در پرداخت همراه و امنیت آنها

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

انواع مختلف انتقال داده توسط NFC

- بهتر است دستگاه‌هایی که از باتری داخلی بهره می‌گیرند، در حالت غیرفعال قرار داشته باشند تا نیازی به مصرف انرژی داخلی نباشد.
- از این رو پروتکل موجود در NFC می‌تواند حتی در زمان‌هایی که تلفن همراه خاموش است نیز کار خود را ادامه دهد.
- ارتباط بین دو دستگاه فعال را یک تبادل فعال می نامند
- ارتباط بین دو دستگاه که یکی فعال و دیگری غیرفعال است را تبادل غیرفعال می‌نامند.
- یک واسط NFC مانند یک تلفن همراه اطلاعات یک کارت غیرفعال را می‌خواند
- اطلاعات یک واسط NFC مانند یک تلفن همراه، توسط یک واسط فعال همچون یک دستگاه فروش بلیت، خوانده می‌شود
- NFC به عنوان یک رابط دوطرفه بین دو تلفن همراه عمل می‌کند

پروتکلهای ارتباطی در پرداخت همراه و امنیت آنها

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

انواع مختلف انتقال داده توسط NFC

وسیله الف	وسیله ب	
فعال	فعال	هر دو وسیله میدان تولید میکنند
غیر فعال	فعال	فقط وسیله ب میدان تولید میکند
فعال	غیر فعال	فقط وسیله الف میدان تولید میکند

	آغازگر	هدف
فعال	ممکن	ممکن
غیر فعال	غیر ممکن	ممکن

پروتکلهای ارتباطی در پرداخت همراه و امنیت آنها

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

مدهای انتقال فناوریNFC

- سبک نوشتن و خواندن
- سبک تقلید برچسب
- سبک انتها به انتها

❖در سبک نوشتن/خواندن گوشی های NFC میتوانند بر روی برچسب ها بنویسند یـا از روی آنها اطلاعات دریافت کنند. مانند پوسترهای هوشـمند. ارتباطـات بـدون تمـاس ایـن سبک را پشتیبانی میکنند.

❖در سبک تقلید برچسب گوشی-های NFC مانند کارتهای هوشمند عمل میکنند. بـرای مثال به عنوان کیف پول.

❖در سبک انتها به انتها سطوح مختلف ارتباطی بین دو گوشـی- NFC ایجـاد مـی-شـود. مانند مبادله کارتهای تجاری.

پروتکلهای ارتباطی در پرداخت همراه و امنیت آنها

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

اولين همايش بين‌المللي
بانكداري الكترونيك و
نظام هاي پرداخت
(اول اسفند 1390 ــ برج ميلاد)

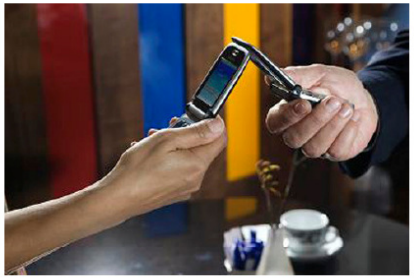
پروتكلهاي
ارتباطي در
پرداخت همراه و
امنيت آنها

ارائه دهنده:
دكتر شاه حسيني
مهندس افهامي

حالتهای کاری NFC

تلفن به وسیله

تلفن به تلفن



تلفن به خواننده

تلفن به برچسب

قالب مبادله داده NFC (NFC Dat)

- قالب ذخیره داده بر روی تگهای NFC می‌باشد.
- از یک استاندارد مشخص و واحد برای ذخیره اطلاعات استفاده میکند.
- مستقل از نوع تگ می باشد.
- یک تعداد از انواع داده خاص را تولید میکند:
  - URI, TextRecord, and SmartPoster
- توسط انجمن های NFCاستاندارد شده است.

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

قسمت دوم: چالش‌های امنیتی سامانه‌های پرداخت الکترونیکی همراه

اهداف امنیتی مدیریت شبکه

- ✓ **محرمانگی:** یعنی این ویژگی که اطلاعات برای افراد غیرمجاز، موجودیت های غیر مجاز یا فرآیندهای غیرمجاز نمایان نشود و یا در اختیار ایشان را نگیرد.
- ✓ **جامعیت داده:** یعنی این ویژگی که داده به طریق غیرمجاز تغیر نیافته و از بین نرود.
- ✓ **دسترس پذیری:** یعنی این این ویژگی که به محض در خواست یک موجودیت مجاز در دسترس و قابل استفاده باشد.

سه هدف فوق به اختصار CIA نامیده میشوند و در کنار این سه هدف اصلی یک هدف دیگر نیز مطرح است که استفاده قانونی یا Legitimate use نامیده شده و در مجموع CIA+ نامیده میشوند.

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

سرویسهای امنیتی

- ✓ **سرویس احراز هویت:**
  - ✓ احراز هویت موجودیت نظیر
  - ✓ احراز هویت مبدا داده:
- ✓ **سرویس کنترل دسترسی:** جلوی دسترسی های غیر مجاز را میگیرد.
- ✓ **سرویس محرمانگی:**
  - ✓ محرمانگی اتصال گرا
  - ✓ محرمانگی بدون اتصال
  - ✓ محرمانگی میدان محدود
  - ✓ محرمانگی جریان ترافیک

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

سرویسهای امنیتی

- ✓ **سرویس جامعیت داده :**
  - ✓ جامعیت داده اتصال گرا با ترمیم
  - ✓ جامعیت داده اتصال گرا بدون ترمیم
  - ✓ جامعیت داده اتصال گرا میدان محدود
  - ✓ جامعیت داده بدون اتصال
  - ✓ جامعیت داده بدون اتصال با میدان محدود

- ✓ **سرویس عدم انکار:**
  - ✓ عدم انکار مبدا
  - ✓ عدم امکار تحویل

پروتکلهای ارتباطی در پرداخت همراه و امنیت آنها

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

سازوکارهای امنیتی

سازوکارها یا مکانیزمهای امنیتی به دو دسته خاص و فراگیر تقسیم میشوند.

- ✓ **ساز و کارهای خاص:**

  فقط برای برخی از سرویسها قابل استفاده هستند.

- ✓ **سازو کارهای فراگیر**

  ارتباطی به سرویس امنیتی ندارند و به طور کلی در شبکه قابل استفاده هستند.

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

ساز و کارهای خاص

۸ سازو کار خاص عبارتند از:

- ✓ رمزنگاری
- ✓ امضای رقمی
- ✓ کنترل دستیابی
- ✓ جامعیت داده
- ✓ احراز هویت تبادلی
- ✓ پرکردن ترافیک
- ✓ کنترل مسیریابی
- ✓ گواهی

پروتکلهای
ارتباطی در
پرداخت همراه و
امنیت آنها

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

ساز و کارهای خاص

۱- رمزنگاری:

- به دو دسته کلی تقسیم میشود:
  - متقارن (کلید محرمانه)
  - نامتقارن (کلید عمومی و کلید خصوصی)

در درس رمزنگاری به طور مفصل بحث شده است.

۲- امضای رقمی

- فرستنده و گیرنده کلیدها را برعکس رمزنگاری نامتقارن استفاده میکنند
  - امضای یک واحد واحد داده (با کلید خصوصی)
  - وارسی امضا (با کلید عمومی)

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

ساز و کارهای خاص

۳- کنترل دستیابی

- این مکانیزم از مشخصه های احراز شده یک موجودیت یا اطلاعات خاص (نظیر عضویت در یک مجموعه شناخته شده) استفاده میکند تا حقوق دستیابی را تشخیص و مورد اجرا گزارد. اگر یک موجودیت بخواهد از یک منبع غیرمجاز استفاده کند یا از یک منبع مجاز به صورت نامناسبی استفاده کند، تابع کنترل دستیابی جلوی آن دستیابی را میگیرد و حتی امکان ارائه گزارش به عنوان قسمتی از دنباله ممیزی امنیتی را نیز دارد.

- مکانیزم های کنترل دستیابی براساس یک یا چند تا از موارد زیر انجام میشود:
  - پایگاه داده کنترل دستیابی.
  - اطلاعات احراز هویت برای مجاز شناسی هستارها.
  - قابلیت هائی که حق دستیابی به منابع را تعین میکند.
  - برچسب های امنیتی که به یک موجودیت متصل است و برای دستیابی یا عدم آن (معمولا براساس سیاستهای امنیتی) استفاده میشود.
  - زمان دستیابی مورد درخواست.
  - مسیرهای دستیابی مورد درخواست.
  - دوره یا طول زمان دستیابی.

- مکانیزم های کنترل دستیابی میتواند در دو انتهای ارتباط یا هر نقطه دیگری اعمال شود.

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

ساز و کارهای خاص

۴- مکانیزم جامعیت داده

- دو جنبه جامعیت داده عبارتست از:
  - جامعیت یک بسته
  - جامعیت جریان داده

در عمل مکانیزمهای مختلفی برای فراهم آوردن این دو جنبه استفاده میشود اگرچه مکانیزمهای دومی نیاز به اولی دارد.

- در دوطرف ارتباط باید عملیات انجام شود. فرستنده اطلاعات اضافی به دنبال اطلاعات اصلی میچسباند و در طرف گیرنده همان عملیات انجام میشود و اضافات با هم مقایسه میشوند.
  - این مکانیزم جلوی ارسال مجدد را نمیگیرد.
  - میتواند شامل ترمیم هم باشد (با ارسال مجدد یا با تصحیح)

- در حالت اتصال گرا شامل عدم جابجائی ترتیب بسته ها، از بین رفتن اطلاعات، ارسال مجدد، تغیر و میان گذاری اطلاعات است که نیاز به استفاده از شماره سریال برچسب زمانی و رمزنگاری زنجیری دارد.

- برای ارتباطات بدون اتصال برچسب زمانی به طور محدود با حمله Replay مقابله میکند.

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

ساز و کارهای خاص

۵- احراز اصالت تبادلی

احراز اصالتی است که با تبادل اطلاعات بین طرفین انجام میشود.

- ✓ برخی فنون لازم برای احراز اصالت تبادلی
  - ✓ استفاده اطلاعات احراز اصالت مثل رمز عبور توسط موجودیت فرستنده
  - ✓ روشهای رمزنگاشتی
  - ✓ اطلاعات موجودیتها و حقوق آنها
- ✓ در خصوص احراز اصالت موجودیت ها بعدا (در فصل ۵ درس) بیشتر بحث میشود.
- ✓ هر تخطی از آن منجر به قطع ارتباط و ثبت در دنباله ممیزی(Audit Trial) میشود.
- ✓ وقتی که از روشهای رمزنگاشتی استفاده میشود از پروتکل دستدهی برای اطمینان از زنده بودن و مقابله با حمله Replay استفاده میشود.
- ✓ انتخاب روشها در احراز اصالت تبادلی به شرایط محیطی بستگی دارد که باید به موارد زیر اشاره شود:
  - ✓ برچسب زمانی
  - ✓ دستدهی دومرحله ای یا سه مرحله ای
  - ✓ عدم انکار

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

ساز و کارهای خاص

۶- پرکردن ترافیک

- ✓ جلوی تحلیل ترافیک را توسط مهاجم میگیرد.
- ✓ تحلیل ترافیک یعنی اطلاعات ناشی از مشاهده ترافیک (وجود، عدم وجود و فرکانس تکرار ترافیک)
- ✓ پرکردن ترافیک اگر با رمزنگاری محافظت شود کارا خواهد بود.

۷- کنترل مسیریابی

- ✓ انتخاب مسیر های فیزیکی امن (با الگوریتمهای پویا یا مسیر از قبل تعین شده).
- ✓ داده های با برچسب امنیتی خاص به دلیل سیاستهای امنیتی از زیرشبکه ها رله ها یا مسیرهای خاص عبور نکند.

۸- گواهی

- ✓ اطمینان از خواص داده انتقال یافته (مثل جامعیت، مبدا، زمان، مقصد) توسط سازوکارهای گواهی تامین میشود.
- ✓ اطمینان توسط گواهی نفر سوم که طرفین به آن اعتماد دارند یعنی TTP فراهم میشود.

ارائه دهنده:
دكتر شاه حسيني
مهندس افهامي

ساز و کارهای فراگیر

سازو کارهای فراگیر در استاندارد عبارتند از:

- ✓ کارکردهای قابل اعتماد
- ✓ برچسب های امنیتی
- ✓ تشخیص رویداد
- ✓ دنباله ممیزی امنیتی
- ✓ ترمیم امنیتی

چند نکته در خصوص سازو کارهای فراگیر:

- ✓ ازآنجائیکه این مکانیزم ها مخصوص سرویس خاصی نمیباشند، به طور صریح در لایه ای ارائه نمیشوند.
- ✓ برخی از آنها به جنبه های مدیریت شبکه مربوط میباشند. در حالت کلی اهمیت این مکانیزمها مستقیما به سطح امنیتی مورد نیاز مرتبط است.

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

ساز و کارهای فراگیر

کارکردهای قابل اعتماد:

- ✓ کارکردی است که براساس قاعده (نظیر آنچه توسط سیاستهای امنیتی تعین شده) درست تشخیص داده شود.
- ✓ کارکردهای قابل اعتماد میتواند برای گسترش محدوده یا تاثیر بیشتر سایر سازوکارهای امنیتی استفاده میشود.
- ✓ هرکارکردی که مستقیما مکانیزمهای امنیتی را فراهم آورده یا دستیابی به آنها را فراهم میکند باید قابل اعتماد باشد.
- ✓ روندهائی که تضمین میکند که سخت افزارها و نرم افزارها قابل اعتماد باشند خارج از حوزه بحث ما است.

ارائه دهنده:
دكتر شاه حسيني
مهندس افهامي

ساز و کارهای فراگیر

برچسب های امنیتی:

- منابع شامل بسته های داده میتواند برچسب امنیتی داشته باشند که حساسیت امنیتی آنها را نشان میدهد.
- برچسب های امنیتی هنگام انتقال استفاده میشوند.
- برچسب ها میتوانند صریح یا ضمنی باشند.

ارائه دهنده:
دكتر شاه حسيني
مهندس افهامي

ساز و کارهای فراگیر

تشخیص رویداد:

- ✓ مکانیزم های تشخیص رویداد، تشخیص تخطی های امنیتی است. البته میتواند رویدادهای عادی را نیز تشخیص دهد (مثل دستیابی های موفق)
- ✓ مشخصات آنکه چه چیزی رویداد است در بخش مدیریت رسیدگی به رویدادها در توصیه نامه X800 بیان شده است.
- ✓ تشخیص وقایع امنیتی مختلف میتواند باعث یک یا برخی از فعالیتهای زیر شود:
  - ✓ گزارش رویدادهای محلی
  - ✓ گزارش از راه دور رویدادها
  - ✓ Log کردن رویدادها
  - ✓ فعالیتهای ترمیم
- ✓ نمونه هائی از رویدادها عبارتند از
  - ✓ یک نوع تخطی امنیتی خاص
  - ✓ یک رویداد خاص منتخب
  - ✓ سریز دفعات رخداد یک رویداد

ارائه دهنده:
دكتر شاه حسيني
مهندس افهامي

ساز و کارهای فراگیر

دنباله ممیزی امنیتی :

- ✓ یک ملاحظه و بازرسی مستقل از فعالیتهای ثبت شده سیستم برای آزمون کافی بودن کنترل ها است تا از انجام روندهای عملیاتی براساس سیاستهای بنا نهاده شده اطمینان حاصل شود، و از خرابی دارائی ها جلوگیری کند، و برای هر تغیری در کنترل ها، روندها، و سیاستها پیشنهاد ارائه نماید.

- ✓ این امر نیاز به ضبط اطلاعات مربوطه و تحلیل آنها دارد.

- ✓ جمع آوری و ضبط اطلاعات در حوزه این مکانیزم است ولی توابع مربوط به تحلیل اطلاعات مربوط به مدیریت امنیت است و مربوط به این سازو کارها نیست.

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

ساز و کارهای فراگیر

اولين همايش بين‌المللي بانكداري الكترونيک و نظام هاي پرداخت
(اول اسفند 1390 ــ برج ميلاد)

پروتكلهاي ارتباطي در پرداخت همراه و امنيت آنها

ارائه دهنده:
دكتر شاه حسيني
مهندس افهامي

ترمیم امنیتی :

- ترمیم امنیتی با درخواستهائی از مکانیزم هائی مثل توابع رسیدگی ومدیریت رویدادها سروکار دارد و فعالیت ترمیم را با اعمال مجموعه ای از قوانین انجام میدهد.
- این فعالیتها میتواند از سه نوع زیر باشد:
  - بلادرنگ: مثل قطع ارتباط
  - موقت : مثل بی اعتبار کردن یک موجودیت
  - بلندمدت: مثل قراردادن در فهرست سیاه

ارائه دهنده:
دكتر شاه حسيني
مهندس افهامي

نگاشت سازوکارهای خاص و سرویسهای امنیتی

TABLE 1/X.800

Illustration of relationship of security services and mechanisms

Service \ Mechanism	Encipherment	Digital signature	Acces control	Data integrity	Authenti-cation exchange	Traffic padding	Routing control	Notari-zation
Peer entity authentication	Y	Y	·	·	Y	·	·	·
Data origin authentication	Y	Y	·	·	·	·	·	·
Access control service	·	·	Y	·	·	·	·	·
Connection confidentiality	Y	·	·	·	·	·	Y	·
Connectionless confidentiality	Y	·	·	·	·	·	Y	·
Selective field confidentiality	Y	·	·	·	·	·	·	·
Traffic flow confidentiality	Y	·	·	·	·	Y	Y	·
Connection Integrity with recovery	Y	·	·	Y	·	·	·	·
Connection integrity without recovery	Y	·	·	Y	·	·	·	·
Selective field connection integrity	Y	·	·	Y	·	·	·	·
Connectionless integrity	Y	Y	·	Y	·	·	·	·
Selective field connectionless integrity	Y	Y	·	Y	·	·	·	·
Non-repudiation. Origin	·	Y	·	Y	·	·	·	Y
Non-repudiation. Delivery	·	Y	·	Y	·	·	·	Y

· The mechanism is considered not to be appropriate.

Y Yes: the mechanism is considered to be appropiate, either on its own or in combination with other mechanisms.

Note – In some instances, the mechanism provides more than is necessary for the relevant service but could nevertheless be used.

ارائه دهنده:
دكتر شاه حسيني
مهندس افهامي

امنیت در فناوری NFC

- از آنجا که فناوری NFC یک استاندارد بی‌سیم است، مشخص است که در این زمینه بحث امنیتی جلوگیری از Sniffing یا استراق سمع امواج رادیویی از اهمیت بالایی برخوردار خواهد بود.
- دو دستگاه مجهز به این فناوری توسط امواج رادیویی یا RFها با یکدیگر تبادل اطلاعات می‌کنند.
- در چنین مواردی هکرها قادر هستند با استفاده از آنتن‌های قوی، سیگنال‌های انتقالی را دریافت کنند.
- در حال حاضر تجهیزات بسیاری برای دریافت و رمزگشایی سیگنال‌های رادیویی وجود دارند و دسترسی به آنها کار سختی نیست.

سوال مهم:

برقراری ارتباط مبتنی بر NFC بین دو دستگاه نزدیک به هم (حداکثر فاصله ۱۰ سانتی‌متر) صورت می‌گیرد. سوالی که پیش می‌آید این است که با این وجود چگونه یک نفوذگر قادر خواهد بود سیگنال‌های قابل استفاده را دریافت کند؟

عوامل تاثیر گذار در استراق سمع NFC

- مشخصه امواج رادیویی دستگاه فرستنده (هندسه و شکل و شمایل آنتن، محیطی که در آن امواج منتشر می‌شوند و...)

- مشخصات آنتن مهاجم (شکل هندسی و امکان تغییر موقعیت در کلیه ابعاد)
- کیفیت گیرنده مهاجم
- کیفیت رمزگشای سیگنال مهاجم
- انتخاب محل حمله توسط نفوذگر
- .....

- در مجموع زمانی که یک دستگاه فعال در حال ارسال داده‌هاست استراق سمع می‌تواند تا فاصله ۱۰ سانتی‌متری انجام پذیرد.
- برای یک ارتباط غیرفعال این فاصله به یک متر هم می‌رسد.

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

تقسیم بندی حملات بر روی پروتکل NFC

سرویس امنیتی	تهدیدات
تهدیدات جامعیت	تهدیدات جامعیت داده
	حملات اصلاح داده
	حملات خرابی داده
	حملات مرد میانی
	حملات ترزیق داده
	تهدیدات جامعیت مبدا
	حملات فیشینگ
	حملات relay
تهدیدات در دسترسی بودن	حملات اخلال در سرویس
تهدیدات محرمانگی	حملات استراق سمع
تهدیدات عدم انکار	حملات عدم انکار

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

ارائه دهنده:
دكتر شاه حسيني
مهندس افهامي

تهدیدات جامعیت داده

- اعتماد به داده و منبع به نام جامعیت اطلاعات شناخته میشود.
- جامعیت اطلاعات دارای دو نوع جامعیت داده و جامعیت مبدا می باشد.
- انواع حملات جامعیت داده
  - حمله اصلاح داده ها
  - حمله تغییر داده ها
  - حمله مرد میانی
  - حمله ترزیق داده ها

تهدیدات جامعیت مبدا اطلاعات که NFCبا آن مواجه است عبارتند از:

- حمله فیشینگ
- حمله رله

تهدیدات اصلاح داده ها

- مهاجم می تواند داده هایی را که توسط دستگاه NFCفرستاده شده تغییر دهد.
- با توجه به استاندارد NFCIP-1 در حالت فعال روی ۱۰۶ کیلوبیت/ثانیه داده انتقالی عملیات انجام می-دهد و از کلید شیفت دامنه (ASK)۱۰۰٪ همراه با کدنویسی ویرایش میلر استفاده می کند.
- برای نرخ بیت بالاتر ASK 10٪ با ترکیبی از کدنویسی منچستر استفاده می شود.
- با استفاده از کد ویرایش میلر سیگنال بعد از '۰' توقف ندارد وقتی بیتهای ترکیبی '۱۰' فرستاده می شود.
- در حالی که دو بیت سیگنال '۰' مکث دارد وقتی که بیت-های ترکیبی '۰۰' فرستاده می شود.
- تغییر مکث را به سیگنال برای مهاجم با استفاده ازکدنویسی ۱۰۶ کیلوبیت/ثانیه آسان است
- اما تغییر سیگنال به توقف غیر ممکن است.
- اصلاح داده ها در NFCزمانی امکان پذیر است که در آن نرخ بیت بالاتر از ۱۰۶ کیلوبیت / ثانیه باشد.

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

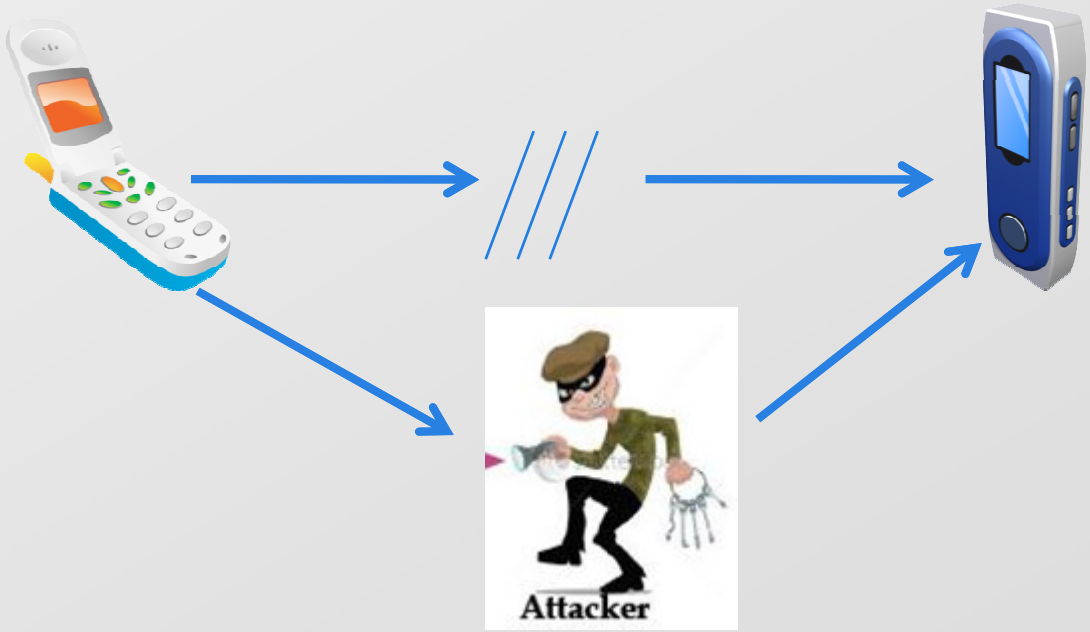
تهدیدات خرابی دادها

- به جای مشاهده داده، مهاجم می تواند سعی کند آن را تغییر دهد.
- مهاجم می تواند به سادگی داده ها را مختل کند، تا گیرنده قادر به درک آن نباشد.
- اگر مهاجم دقیقا زمان ارتباط و فرکانسهای انتقال معتبر درآن زمان خاص را بداند، تنها می تواند داده ها را مخدوش نماید.
- مهاجم می تواند با دانستن این که چه مدولاسیون و طرح کدگذاری استفاده می شود، زمان درست برای ارسال فرکانس های معتبر را محاسبه نماید.
- در این حالت، مهاجم نمی-تواند داده ها را بخواند، تنها میتواند سیگنالها را مخدوش کند به طوری که گیرنده ممکن است آن-ها را درک نکند

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

تهدیدات مرد میانی

- در چنین حملاتی هر دو طرف (فرستنده و گیرنده) تصور میکنند که آنها درحال برقراری یک ارتباط امن هستند. اما مهاجم در میان فرستنده و گیرنده قرار گرفته است.



ارائه دهنده:
دكتر شاه حسيني
مهندس افهامي

تهدیدات مرد میانی

❖مهاجم سیگنال پیام قربانی را میخواند وسپس روی لینک ارتباط با وب سرور قرار میدهد.

❖ بعد از آن حمله کننده پیام پاسخ را از سرور وب دریافت میکند و با تغییر این پاسخ با توجه به خواست خود، آن را به قربانی می فرستد.
❖مهاجم اطمینان حاصل می-کند که وقتی یک طرف داده هارا می فرستد ، طرف دیگر آن را نمی داند. او داده-ها را ره-گیری کرده ، تغییر می-دهد و به گیرنده می فرستد.

❖در NFC، هر دو طرف، داده ها را همان زمان انتقال میدهند. بنابراین، برخورد بین ارتباطات به راحتی با مقایسه سیگنالهای دریافتی وانتقالی شناسایی می شود
❖حملات MITMقابل پیاده سازی روی NFCنیستند، چرا که دامنه ارتباطات کوچک شده است.
❖حمله MITMدشوار به نظر می رسد، این سناریو ممکن است در هنگام استفاده از این فناوری در بانکداری و دیگر مناطق حساس ، تهدیدات امنیتی به وجود آورد.

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

ارائه دهنده:
دکتر شاه حسيني
مهندس افهامي

تهدیدات ترزیق داده

- مهاجم می تواند داده هایی را در خلال پیام های فرستاده شده از دستگاه ارسال به دستگاه دریافت و بالعکس قرار دهد.
- حمله ترزیق داده ها هنگامی امکان پذیر است که دستگاه بیش از حد زمان برای پاسخ دهی صرف میکند.
- مهاجم می-تواند اطلاعات خود را قبل از داده های گیرنده واقعی ارسال کند.
- اگر جریان اطلاعات فرستاده شده از گیرنده و مهاجم همپوشانی داشته باشد، داده خراب خواهد شد.

ارائه دهنده:
دکتر شاه حسيني
مهندس افهامي

حملات رله

- در تراکنشات بی تماس حملات رله تهدیدات امنیتی جدی هستند.
- مهاجم در این مورد می تواند رمزنگاری و اقدامات امنیتی دیگر را دور بزند.
- هیچ سخت افزار و کد گذاری سیگنال برای این حمله مورد نیاز نیست.
- JSR 257 و JSR 82، ابزارهای API است که به راحتی در دسترس است، و برای چنین حملاتی مورد استفاده قرار گیرند.

حملات رله

- این حمله به عنوان "حمله کرم چاله ی" نیز شناخته شده است.
- مهاجم می تواند پروتکل های امنیتی مربوط به چالش-های رله و پاسخ بین دو طرف را دور بزند.
- مهاجم همیشه پاسخ صحیح را با استفاده از حمل و نقل پیام اصلی که او از طرف دیگر دریافت نموده است، ایجاد میکند و پاسخ را ثبت می-نماید، پروتکل با موفقیت اجرا می-شود
- هر دو طرف ارتباط غافل از حضور مهاجم بین آنها در حال ارتباط باقی میمانند.
- در این سناریو حمله نیاز به دانستن ساختار و اجرای پروتکل، الگوریتم مورد استفاده، داده ها یا کلید نیست. مهاجم تنها ارتباط کامل بین هر دو طرف را بدون وقفه ذخیره میکند.

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

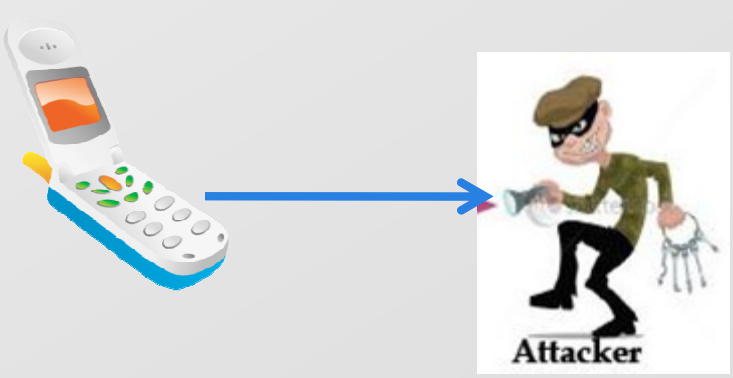
ارائه دهنده:
دكتر شاه حسيني
مهندس افهامي

تهدیدات قابلیت دسترسی

توانایی استفاده از اطلاعات یا منابع مورد نظر، قابلیت دسترسی نامیده می شود.

از دیدگاه امنیتی:

اگر کسی عمدا باعث غیر قابل دسترس شدن سیستم یا جلوگیری از دسترسی کاربر به سیستم برای مدت زمان خاص شود، تهدیدات قابلیت دسترسی رخ می‌دهد.



ارائه دهنده:
دكتر شاه حسيني
مهندس افهامي

تهدیدات قابلیت دسترسی

- به عنوان مثال، مهاجم سرور وب سایت فروش برخط را با خرید سرور ثانویه به خطر می اندازد. هنگامی که فرد دیگری درخواست اطلاعات از سرورنماید،
- مهاجم می تواند هر گونه اطلاعاتی که او می خواهد را فراهم کند.
- مشتریان برای کسب اطلاعات می-توانند با خریدار اولیه سرور بگیرند. اگر خریدار اولیه در پاسخ دهی با شکست مواجه شود، از سرور ثانویه خواسته خواهد شد که به ارائه اطلاعات بپردازد.
- مهاجم از تماس مشتریان با خریدار اولیه سرور جلوگیری به عمل می-آورند، به طوری که همه مشتریان به سرور دوم که در حال حاضر توسط مهاجم کنترل می-شود، رجوع کنند.
- در این سناریو، مشتری نمی-تواند هیچ چیزی از این وب سایت خریداری نماید.

ارائه دهنده:
دكتر شاه حسيني
مهندس افهامي

حملات اخلال در سرویس

- ✓این حمله می تواند به سادگی با جمع کردن سیگنال انجام شود.
- ✓ NFC به راحتی می تواند چنین حمله هایی را تشخیص دهد.

حملات اخلال در سرویس

- یکی از نمونه های حمله اخلال در سرویس، جایگزینی تگ اصلی با یک تگ خالی است.
- هنگامی که یک دستگاه NFC این تگ خالی را لمس میکند، در پاسخ به آن یک پیام خطا تولید می شود و دستگاه را اشغال میکند .
- تلفن همراه هر زمان که با یک تگ خالی مواجه شود راه اندازی دوباره (Reboot) میشود.
- این نوع از حمله با استفاده از تگ های چسبنده با پیام ناقص (malfunctioned)و قرار دادن این تگ در بالای تگ اصلی پیاده سازی می-شود.

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

تهدیدات محرمانگی

- محرمانگی پنهان نمودن اطلاعات و منابع از دسترسی های غیر مجاز می باشد.
- اگر مدیریت بالاتر تقاضای دیدن اطلاعات را دارد، باید آن را کشف رمز کند.
- مدیریت عالی باید کلید رمزنگاری برای کشف داده را داشته باشد. با این حال، اگر مهاجم کلید کشف رمز را به دست آورد اطلاعات محرمانه به خطر میافتد

ارائه دهنده:
دكتر شاه حسيني
مهندس افهامي

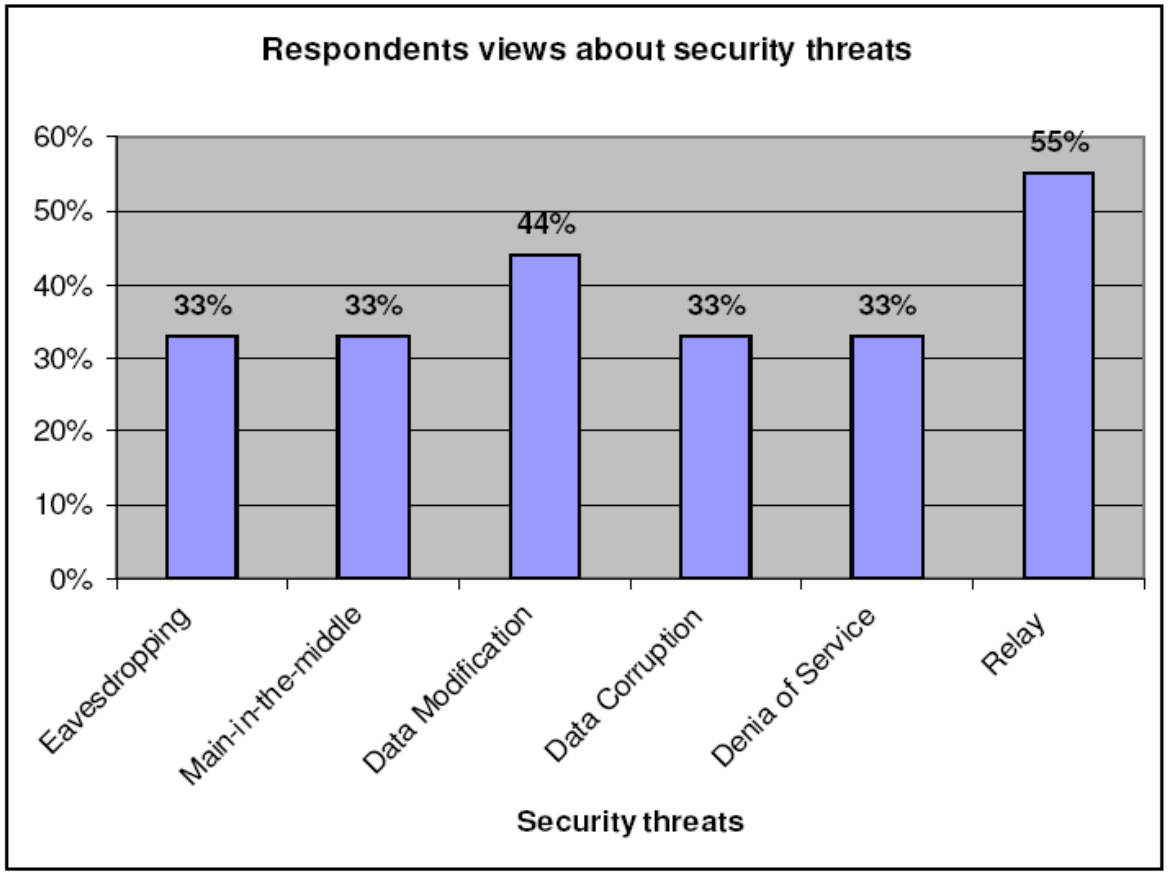
استراق سمع

- در ارتباطات بی سیم آشکار ترین حمله سرقت و استراق سمع است. مهاجم می تواند به هر گونه داده بین دو دستگاه را با استفاده از آنتن و ابزار تجزیه و تحلیل، شنود کند.
- با توجه به قدرت کم و فاصله نزدیک ارتباطی دستگاه های NFC، میتوان اظهار داشت که استراق سمع در این زمینه در مقایسه با دامنه بزرگتر دیگر فناوریهای ارتباطی مشکل است.
- استراق سمع حالت غیر فعال نسبت به حالت فعال سخت تر است،
- دستگاه در حالت فعال در محدوده ۱۰ متر و دستگاه در حالت غیر فعال در محدوده ۱ متر میتواند شنود شود.
- سرقت و مشاهده در NFCعملا بعید است. اما NFCداده ها را با سرعت زیاد انتقال می-دهد. بنابراین انتقال داده ها از داخل به خارج در یک سازمان میتواند یک مسئله باشد.

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

ارائه دهنده:
دكتر شاه حسيني
مهندس افهامي

مقایسه درصد انجام حملات در NFC



پروتکلهای ارتباطی در پرداخت همراه و امنیت آنها

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

روشهای مقابله با انواع حملات

استراق سمع
- استفاده در مد غیر فعال

خرابی داده
حملات خرابی داده براحتی قابل کشف می باشد با مقایسه توان دریافتی

اصلاح داده ها
- ارسال بسته با نرخ 106k Baud در مد فعال
- بررسی میدان RF
- استفاده از کانال امن

ترزیق داده
- پاسخ داده به دستگاه فرستنده بدون هیچ تاخیر
- گوش دادن دستگاه به کانال
- کانال امن

مرد میانی
- استفاده از ارتباط فعال-غیر فعال
- گوش داده به کانال

راه اندازی کانال امن

- راه اندازی کانال امن بهترین روش برای مقابله با حملات استراق سمع و اصلاح داده میباشد.
- یک پروتکل توافق کلید همانند دیفی کلید بر روی RSA یا منحوی بیضوی برای تسهیم راز میان دو دستگاه می تواند استفاده شود.

- تسهیم راز می تواند با استفاده از کلید متقارن همانند 3DES یا AES باشد که برای محرمانه کردن کانال امن می تواند استفاده شود.

توافق کلید برای فناوری NFC

- استفاده از رمزنگاری کلید نامتقارن برای فناوری NFC با محاسبات بالا به صرفه نیست
- از نقطه نظر تئوری، استفاده از کلید نامتقارن امنیت صد در صد فراهم میکند.
- در برخی از مقالات ارائه شده طرح استفاده از کلید نامتقارن متناسب با فناوری NFC ارائه شده است

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

ارائه دهنده:
دکتر شاه حسینی
مهندس افهامی

نتیجه گیری

۱- مبانی پرداخت الکترونیکی معرفی شد

- ✓ بررسی معماری روشهای پرداخت همراه
- ✓ بررسی مزایا و معایب روشهای پرداخت موجود

۲- فناوری NFC معرفی شد

- ✓ بررسی استانداردهای فناوری NFC
- ✓ بررسی مدهای انتقال NFC

۳- مهمترین چالشهای امنیت پرداخت با فناوری NFC

- ✓ بررسی حملات ممکن بر روی NFC (استراق سمع و اصلاح داده و ....)
- ✓ ارائه راهکارهایی برای مقابله با حملات

زمینه های دیگر برای بحث های آتی:

- ✓ بررسی رمزنگاری کلید نامتقارن برای بهبود امنیت NFC
- ✓ پیاده سازی حملات ممکن بر روی NFC با سخت افزارها و نرم افزارهای موجود