

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

سمنار

عنوان سمنار
امنيت پرداخت الكترونيكي

توسط:

چکیده

پرداخت الکترونیکی بخش بسیار مهمی از سیستم کسب و کار الکترونیکی است، که باید امنیت آن تضمین شود. سیستم‌های پرداخت الکترونیکی از اجزای اصلی نظام مالی هر کشور هستند که نقش موثری در انتقال سریع، کارآمد و ایمن در میان بازارها و فعالان مختلف نظام مالی و نیز، ارتقای کارایی نظام مالی کشور ایفا می‌نمایند همچنین، توسعه نظام‌های پرداخت با تسهیل مبادلات اقتصادی و ایجاد بستر مناسبی برای اجرای سیاست‌های پولی می‌تواند به توسعه مالی و اقتصادی کشور کمک کند. همانطور که می‌دانیم، پرداخت از طریق شبکه‌ها به خصوص اینترنت امنیت بالایی می‌طلبد، زیرا ارسال داده‌ها و اطلاعات مالی از قبیل، شماره کارت اعتباری، شماره حساب، ارسال اطلاعات محرمانه مالی، ارسال کد رمز و کلمه عبور و هزاران اطلاعات محرمانه دیگر نگرانی‌های زیادی به دنبال می‌آورد و با توجه به رشد و گسترش تجارت الکترونیک و افزایش حجم مبادلاتی که در این حوزه صورت می‌گیرد یکی از موضوعات مهم، سیستم پرداخت و امنیت آن در شبکه جهانی اینترنت است. هدف این سمینار ارزیابی ویژگی‌های سیستم‌های پرداخت الکترونیک همچون ایمنی، گمنامی، قابلیت اعتماد و غیره از دیدگاه مختلف است. همچنین ضمن بررسی انواع تهدیدات امنیتی در عرصه پرداخت الکترونیکی به طبقه‌بندی و ارزیابی آنها می‌پردازد. و روش‌های افزایش امنیت در سیستم پرداخت الکترونیکی را مورد مطالعه و ارزیابی قرار می‌دهد.

کلمات کلیدی: پرداخت، پرداخت الکترونیکی، امنیت، اینترنت، گمنامی

فهرست مطالب

| صفحه | عنوان |
|--|---------------------------------------|
| ۱ | چکیده |
| فصل اول: مقدمه | |
| ۸ | ۱-۱- مقدمه |
| فصل دوم: مروری بر امنیت پرداخت الکترونیکی | |
| ۱۰ | ۱-۲- مقدمه |
| ۱۱ | ۲-۲- تعریف امنیت |
| ۱۱ | ۳-۲- انواع حملات بر روی سیستم ناامن |
| ۱۱ | ۱-۳-۲- حملات شبکه |
| ۱۱ | ۱-۱-۳-۲- جاسوسی (استراق سمع غیر فعال) |
| ۱۱ | ۲-۱-۳-۲- Spoofing |
| ۱۲ | ۳-۱-۳-۲- Hijacking |
| ۱۲ | ۴-۱-۳-۲- ضبط و پخش |
| ۱۲ | ۵-۱-۳-۲- حمله حدس زدن-PIN |
| ۱۲ | ۲-۳-۲- حملات رمزنگاری |
| ۱۲ | ۱-۲-۳-۲- حمله متن اصلی |
| ۱۳ | ۲-۲-۳-۲- حمله متن آشکار |
| ۱۳ | ۳-۲-۳-۲- حمله با متن اصلی منتخب |
| ۱۳ | ۴-۲-۳-۲- حمله متن رمز شده انتخابی |
| ۱۴ | ۴-۲- تهدیدات امنیتی |
| ۱۴ | ۱-۴-۲- مشکلات احراز هویت |
| ۱۴ | ۲-۴-۲- مشکلات حفظ حریم شخصی کاربران |
| ۱۵ | ۵-۲- پول الکترونیکی |
| ۱۶ | ۶-۲- کیف الکترونیک |
| ۱۷ | ۱-۶-۲- قابلیت های کیف پول الکترونیکی |
| ۱۸ | ۲-۶-۲- کیف پول الکترونیکی و چالش جدید |
| ۱۹ | ۷-۲- چک الکترونیکی |
| ۱۹ | ۸-۲- امضاء دیجیتال |
| ۱۹ | ۱-۸-۲- امضاء کردن |

| | |
|----|---|
| ۱۹ | ۲-۸-۲- تصدیق کردن |
| ۱۹ | ۲-۹- امضاء کور براساس RSA |
| ۱۹ | ۲-۹-۱- کور کردن پیام |
| ۲۰ | ۲-۹-۲- امضاء کردن |
| ۲۰ | ۲-۹-۳- بازگشایی کوری |
| ۲۰ | ۲-۹-۴- تصدیق کردن |
| ۲۰ | ۲-۱۰- شمای کلی از سیستم‌های پرداخت |
| ۲۱ | ۲-۱۰-۱- ملزومات اساسی سیستم پرداخت الکترونیکی |
| ۲۱ | ۲-۱۰-۱-۱- کارایی |
| ۲۱ | ۲-۱۰-۱-۲- امنیت |
| ۲۱ | ۲-۱۰-۱-۳- خواص جانبی |
| ۲۲ | ۲-۱۱- گمنامی در سیستم‌های پرداخت |
| ۲۲ | ۲-۱۱-۱- الزامات مورد نیاز برای فسخ (لغو) سیستم‌های پرداخت گمنام |
| ۲۲ | ۲-۱۱-۲- تکنیک‌های گمنامی |
| ۲۳ | ۲-۱۲- نیازهای امنیتی مهم یک سیستم پرداخت موفق |
| ۲۳ | ۲-۱۲-۱- کنترل دسترسی |
| ۲۴ | ۲-۱۲-۲- محرمانه بودن اطلاعات |
| ۲۴ | ۲-۱۲-۳- یکپارچگی داده |
| ۲۴ | ۲-۱۲-۴- احراز هویت شرکت کنندگان |
| ۲۴ | ۲-۱۲-۵- انکارناپذیری |
| ۲۴ | ۲-۸- جمع‌بندی |

فصل سوم: مطالعه و بررسی روش‌های امنیت سیستم‌های پرداخت الکترونیکی

| | |
|----|--|
| ۲۶ | ۳-۱- مقدمه |
| ۲۷ | ۳-۲- تهدید امنیتی و امنیت تکنیک‌های پرداخت الکترونیکی |
| ۲۸ | ۳-۳- پروتکل پرداخت الکترونیکی امن |
| ۲۹ | ۳-۴- سیستم پرداخت الکترونیکی امن با استفاده از تونل ارتباطات امن |
| ۲۹ | ۳-۴-۱- تونل ارتباطی امن |
| ۲۹ | ۳-۴-۲- کار تونل |
| ۳۰ | ۳-۵- فناوری پرداخت ایمن |
| ۳۰ | ۳-۵-۱- پروتکل SSL |
| ۳۱ | ۳-۵-۲- پروتکل SET |

| | |
|----|---|
| ۳۱ | ۳-۵-۲-۱- مزایای استفاده از پروتکل SET |
| ۳۲ | ۳-۵-۲-۲- سرویس‌های SET |
| ۳۲ | ۳-۵-۲-۳- اجزای SET |
| ۳۳ | ۳-۵-۲-۴- رمزنگاری در پروتکل SET |
| ۳۳ | ۳-۵-۲-۱- مباحث مربوط به رمزنگاری |
| ۳۳ | ۳-۵-۲-۲- سیستم رمزنگاری متقارن |
| ۳۳ | ۳-۵-۲-۳- سیستم رمزنگاری نامتقارن (کلید عمومی) |
| ۳۴ | ۳-۵-۲-۵- سناریوی SET |
| ۳۵ | ۳-۵-۲-۶- مسائل و مشکلات حل نشده‌ی SET |
| ۳۵ | ۳-۵-۲-۱- امکان ارتباط متقابل |
| ۳۶ | ۳-۵-۲-۲- ادغام سیستم‌ها |
| ۳۶ | ۳-۵-۳- پروتکل iKP |
| ۳۸ | ۳-۵-۳-۱- گام‌های پروتکل iKP |
| ۳۸ | ۳-۵-۴- پروتکل 3D Secure |
| ۳۹ | ۳-۵-۴-۱- مراحل تراکنش در پروتکل 3D Secure |
| ۴۱ | ۳-۵-۵- بحث و بررسی پروتکل‌های پرداخت اینترنتی و تراکنش الکترونیکی امن |
| ۴۳ | ۳-۴- جمع بندی |

فصل چهارم: نتیجه گیری و پیشنهادات

| | |
|----|-----------------------------------|
| ۴۵ | ۴-۱- نتیجه گیری و پیشنهادات |
|----|-----------------------------------|

فهرست اشکال

- شکل ۱-۲- فرآیند استفاده از پول الکترونیکی ۱۵
- شکل ۲-۲- مفهوم e-wallet ۱۶
- شکل ۱-۳- حمله غیرفعال ۲۷
- شکل ۲-۳- حمله فعال ۲۷
- شکل ۳-۳- تونل ارتباطات امن شامل SSL و تونل رمزنگاری تودر تو ۲۹
- شکل ۴-۳- تونل ارتباطی امن بین مشتری، بازرگان و دروازه پرداخت ۲۹
- شکل ۲-۳- جریان پیام iKP ۳۷

فصل اول

مقدمه

با توجه به موج جهانی شدن، بسیاری از مفاهیم و تعاریف در زندگی اجتماعی- اقتصادی بشر امروز تغییر کرده است. افراد هر جامعه بسیار سهل و آسان به اطلاعات دسترسی دارند. تغییراتی که به واسطه ظهور اینترنت یا به طور اعم فناوری اطلاعات و ارتباطات در زندگی یکایک افراد جوامع مختلف ایجاد شده، باعث گردیده که سرعت نشر مفاهیم، فناوری نوین و نیز خدمات تازه افزایش چشمگیری یابند. در این بین تجارت الکترونیکی به عنوان موتور محرکه اقتصاد دانائی محور قرن بیست و یکم از جایگاهی ممتاز برخوردار است. از مهمترین مؤلفه‌های اثر گذار در عینیت یافتن تجارت الکترونیکی، مبادلات مالی است. با رشد سریع اینترنت، بانکداری آنلاین نقش بسیار مهم و اساسی در پرداخت‌های الکترونیکی پیدا کرده و درحقیقت بستر مناسبی را برای تراکنش‌های مالی ایجاد نموده است [1]. یکی از مهم‌ترین مواردی که در سیستم‌های پرداخت، به کرات مورد بررسی قرار گرفته است امنیت می‌باشد. از آن جایی که اینترنت یک شبکه‌ی باز است که هیچ‌گونه کنترل متمرکزی بر آن اعمال نمی‌گردد، ضروری است که زیرساخت‌ها و عوامل پشتیبانی و به ویژه سیستم‌های پرداخت موجود در آن از مقاومت کافی در مقابل حملات اینترنتی در امان و مصون باشند. از دو دیدگاه می‌توان به موضوع امنیت نگاه کرد. از یک سو کاربران در زمان انجام پرداخت آنلاین دوست دارند که پولشان در امان باشد و از سوی دیگر بانک‌ها و سازمان‌های خدماتی در زمینه‌ی پرداخت نسبت به موقعیت خود در قبال حفظ وجوه خودو مسائل مالی و اطلاعات شخصی افراد حساس هستند. برای مثال می‌توان به امنیت سیستم‌های وجه نقد الکترونیکی اشاره کرد که در این زمینه دچار مشکلاتی شده است. زیرا براساس قانون هیچ فردی اجازه‌ی ضرب سکه‌های الکترونیکی را ندارد و در صورت بروز چنین مسأله‌ای دولت و بانک‌های ذی صلاح، در قبال ضرب سکه‌های تقلبی مسئول می‌باشند. یکی از مشکلات دیگر وجه الکترونیکی، استفاده‌ی مجدد از آن می‌باشد.

آنچه در یک معامله‌ی طبیعی صورت می‌گیرد این است که بابت کالا یا خدمات ارائه شده از پول موجود یک بار استفاده می‌شود، اما در محیط الکترونیکی و در جایی که کپی اطلاعات و تغییر رکوردها عمل آسانی است چالش‌های فراوانی را برای مهندسان ایجاد می‌کند. اپراتور سیستم پرداخت الکترونیک باید از این مسأله اطمینان حاصل کند که از وجه الکترونیک دو بار استفاده نشده است. از این منظر معمولاً جنبه‌هایی مانند گمنامی، رمزنگاری و unforgeability (ناتوانی در ایجاد "پول تقلبی" در سیستم) در مسأله‌ی امنیت مد نظر قرار می‌گیرد.