

سیستم های پرداخت الکترونیکی

و

امضای دیجیتالی

www.ketab.ir

تالیف: دکتر سید نوراله واله

عضو هیأت علمی دانشگاه آزاد اسلامی

(واحد تهران شرق)

۱۳۹۲

بسم الله الرحمن الرحيم

سرشناسه	: واله، سیدنوراله ، ۱۳۲۹
عنوان و نام پدیدآور	: سیستم‌های پرداخت الکترونیکی و امضای دیجیتالی / تالیف سیدنوراله واله.
مشخصات نشر	: تهران : سیدنوراله واله ، ۱۳۹۲.
مشخصات ظاهری	: ۱۱۹ ص . مصور، نمودار
شابک	: 978-964-04-9689-3
وضعیت فهرست نویسی	: فیا
عنوان اصلی	: Electronic Payment Systems and Digital Signature
موضوع	
موضوع	: انتقال الکترونیکی وجوه
موضوع	: امضای الکترونیکی
موضوع	: بازرگانی الکترونیکی
رده بندی کنگره	: ۱۳۹۲ س ۹/۲ و ۱۷۱۰ HG
رده بندی دیویی	: ۳۳۲/۱۷۸
شماره کتابشناسی ملی	: ۳۱۹۹۳۶۵

نام کتاب	: سیستم‌های پرداخت الکترونیکی و امضای دیجیتالی
تالیف	: دکتر سید نوراله واله
ناشر	: دکتر سید نوراله واله
نوبت چاپ	: اول
تیراژ	: ۵۰۰ نسخه
چاپ	: مهدی
قیمت	: ۴۰۰۰۰ ریال
شابک	: ۹۷۸-۹۶۴-۰۴-۹۶۸۹-۳

* کلیه حقوق برای مولف محفوظ است.

شابک: ۹۷۸-۹۶۴-۰۴-۹۶۸۹-۳

ISBN: 978-964-04-9689-3

تلفن: ۸۸۲۵۴۳۰۰ - ۰۹۱۲۴۴۳۰۸۴۰

تکنیک‌های کنترل و محافظت در (سیستم‌های پرداخت الکترونیکی و امضای دیجیتالی) از مهمترین عواملی می‌باشند که می‌بایستی در شبکه‌های کامپیوتری اعمال گردد. در این مجموعه ابتدا کنترل محیط‌های کامپیوتری و کنترل‌ها در سیستم‌های کامپیوتری و ایمنی سیستم اطلاعات (IS) و سپس نرم افزار پرداخت‌ها و دریافت‌های عمومی (GAS) و سایر نرم افزارهای کنترل مربوط به آنها (CAPS) مورد بررسی قرار گرفته‌اند.

بطور کلی در فصل اول ابزار و تکنیک‌های پرداخت و دریافت‌ها با کمک کامپیوتر با توضیح (CAATTS) عنوان گردیده است و در فصل‌های بعدی تمرکز اصلی بر روی فاز امنیت (Security) بوده که با تشریح سیستم‌های پرداخت الکترونیکی، کاربرد روشهای امنیتی در سیستم‌های پرداخت الکترونیکی و امضای دیجیتالی مورد بررسی قرار گرفته‌اند. محافظت از پولهای الکترونیکی در تجارت از طریق وب یا (Ecommerce) و پروتکل (kerberos) که یکی از ابزارهای امنیت در اینترنت می‌باشد نیز بررسی شده است.

در فصل آخر، مفهوم امضای دیجیتالی (Digital Signature) و عملکرد (E-Signature) و (DSS) و الگوریتم‌های امضای دیجیتالی و نقش (Hash) و (SHA) و الگوریتم (DSA) دقیقاً مورد بررسی قرار گرفته‌اند.

امید است این مجموعه موثر و مفید واقع گردد.

دکتر سید نوراله واله

عضو هیأت علمی دانشگاه آزاد اسلامی

(واحد تهران شرق)



فهرست مطالب

صفحه

عنوان

فصل اول: ممیزی محیط کامپیوتری شده

۲	مقدمه
۷	کنترل‌ها در سیستم‌های کامپیوتری
۱۸	امنیت در سیستم اطلاعات (IS)
۲۴	نرم افزار حسابرسی عمومی (GAS)
۲۸	دیگر نرم افزارهای ممیزی
۳۳	ابزار و تکنیکهای حسابرسی با کمک کامپیوتر (CAATs)

فصل دوم: امنیت در سیستم‌های پرداخت الکترونیکی

۴۴	سیستم‌های پرداخت الکترونیکی
۴۵	سیستم‌های پرداخت الکترونیکی
۴۵	اجزای یک سیستم پرداخت الکترونیکی
۴۶	انواع سیستم‌های پرداخت الکترونیکی
۴۶	۱- Offline در مقابل Online
۴۷	۲- Debit (نقدی) در مقابل Credit (اعتباری)
۴۷	۳- Macro در مقابل Micro
۴۸	ابزارهای پرداخت در یک سیستم پرداخت الکترونیکی
۴۸	۱- کارتهای اعتباری (Credit Cards)
۴۹	۲- پول الکترونیکی
۵۰	۳- چک الکترونیکی



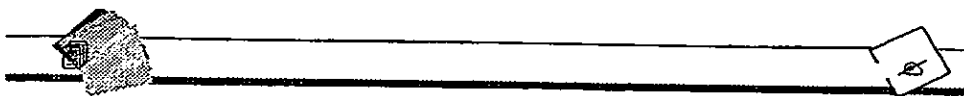
صفحه	عنوان
۵۱	امنیت پرداختهای الکترونیکی.....
۵۳	سیستم‌های امنیتی پرداخت.....
۵۷	در دسترس بودن و قابلیت اطمینان.....
۵۷	خلاصه‌ای از چند روش امنیتی.....
۵۹	سیستم FV (First Virtual).....
۶۰	امنیت پولهای الکترونیکی.....
۶۰	۱- عملیات پرداخت غیر قابل ردیابی.....
۶۱	۱-۱ امضای گمنام (Blind signature).....
۶۱	۱-۲ مبادله سکه‌ها (Exchanging coins).....
۶۲	حفاظت از مصرف دوباره سکه‌ها.....
۶۲	۲-۲ امضای مبهم.....
۶۳	۲-۳ معاوضه سکه‌ها.....
۶۳	۲-۴ نگهبان (Guardian).....
۶۳	۲-۵ امضای نگهبان.....
۶۴	۲-۶ امضای بانک منتشرکننده پول.....
۶۴	۳- محافظت در برابر جعل سکه‌ها.....
۶۴	۴- محافظت در برابر دزدیده شدن سکه‌ها.....
۶۵	۴-۱ حقوقی کردن سکه‌ها (Customize Coins).....
۶۵	۴-۱-۱ مشتری خاص در حالی که هنوز سکه‌ها گمنام هستند.....
۶۶	۴-۱-۲ سکه‌های خاص برای مشتری.....
۶۷	۴-۱-۳ سکه‌های خاص مشتری و فروشنده.....
۶۷	پروتکل Kerberos.....

فصل سوم: امضای دیجیتالی

۷۳	امضای دیجیتالی
۷۴	مقدمه
۷۵	امضاها و قانون
۷۸	چگونگی عمل امضا دیجیتالی
۸۲	گواهینامه‌های کلید عمومی
۸۴	رقابتها و موقعیها

فصل چهارم: استاندارد امضای دیجیتال (DSS)

۸۷	استاندارد برای DSS
۹۱	شاخص قسمتهای دیگر
۹۶	فرآیند استاندارد اطلاعات
۹۶	ویژگیهای استاندارد امضاء دیجیتال DSS
۹۶	مقدمه
۹۶	کلیت
۹۷	استفاده از الگوریتم DSA
۹۸	پارامترهای DSA
۹۹	تولید امضاء
۹۹	نظم دادن امضاء
۱۰۳	۲-۲ - تولید پایه‌ها



صفحه	عنوان
۱۰۶	شاخص ^۳ تولید شماره تصادفی برای DSA
۱۰۷	۳-۱. الگوریتم برای محاسبه ^m ارزشهای ^x
۱۰۸	۳-۲. الگوریتم برای محاسبه یک یا بیش از یک ارزش ^r و ^k
۱۱۰	۳-۳. ساخت نقش ^G از SHA
۱۱۰	۳-۴. ساخت نقش ^G از DES
۱۱۲	شاخص ^۴ . تولید دیگر نقشها
۱۱۷	خلاصه
۱۱۸	منابع و مأخذ

www.ketaboo.ir