

# امنیت در بانکداری اینترنتی

تالیف:

دکتر شهریار محمدی

(عضو هیات علمی دانشکده مهندسی صنایع،

دانشگاه صنعتی خواجه نصیرالدین طوسی)

زینب زارع حسینی

بهار ۱۳۸۹

سرشناسه : محمدی، شهریار، ۱۳۴۰ -

عنوان و نام پدیدآور : امنیت در بانکداری اینترنتی/تالیف شهریار محمدی، زینب زارع حسینی.

مشخصات نشر : تهران: دانشگاه صنعتی خواجه نصیرالدین طوسی، ۱۳۸۹.

مشخصات ظاهری : ۲۸۰ص.، مصور، جدول، نمودار.؛ ۱۷×۲۴سم.

فروست : ۳۶۸.

شابک : ۶۰۰۰۰ ریال: 978-964-8703-82-5

وضعیت فهرست : فیبا

نوبسی

یادداشت : کتابنامه

یادداشت : واژه نامه

موضوع : بانکداری اینترنتی -- اقدامات تأمینی

موضوع : بانک و بانکداری -- ایران -- اقدامات تأمینی

شناسه افزوده : زارع حسینی، زینب، ۱۳۶۳ -

شناسه افزوده : دانشگاه صنعتی خواجه نصیرالدین طوسی

رده بندی کنگره : ۱۳۸۹ الف۸/۱۷۰۸/۷HG

رده بندی دیویی : ۳۳۲/۱۰۲۸۵

شماره : ۳۹۲۸۷۰۲

کتابشناسی ملی

نام کتاب: امنیت در بانکداری اینترنتی

مولف: دکتر شهریار محمدی، عضو هیئت علمی دانشکده مهندسی صنایع، دانشگاه صنعتی خواجه

نصیرالدین طوسی، زینب زارع حسینی

ناشر : انتشارات دانشگاه صنعتی خواجه نصیرالدین طوسی

نوبت چاپ : اول

تاریخ چاپ : مرداد ۱۳۸۹

تیراژ : ۱۲۰۰ جلد

قیمت : ۶۰۰۰ تومان

کد کتاب : ۲۶۸

ISBN: 978-964-8703-82-5

شابک : ۹۷۸-۹۶۴-۸۷۰۳-۸۲-۵

لیتوگرافی: نشر نماد

چاپ و صحافی: نشر نماد

تلفن مرکز پخش : ۸۸۷۷۲۲۷۷ (۰۲۱)

(حق چاپ برای ناشر محفوظ است)

## فهرست مطالب:

۱	پیشگفتار
۳	فصل اول: مقدمه
۵	۱.۱ پیدایش پول
۵	۱.۱.۱ کالا، واسطه مبادله
۶	۲.۱.۱ مسکوک فلزی
۸	۳.۱.۱ پول کاغذی
۹	۲.۱ بانکداری
۱۰	۱.۲.۱ تاریخچه پیدایش بانکداری
۱۰	۱.۱.۲.۱ دوره قدیم (از ... تا قرن پنجم میلادی)
۱۰	الف . بابل
۱۰	ب . یونان
۱۱	ج . ایران
۱۱	د . رم
۱۲	ه . چین
۱۲	۲.۱.۲.۱ در قرون وسطی (از قرن پنجم تا پانزدهم میلادی)
۱۳	۳.۱.۲.۱ دوره رنسانس (از قرن پانزدهم تا سال ۱۹۲۱)
۱۴	۴.۱.۲.۱ دوره جدید بانکداری
۱۴	۵.۱.۲.۱ بانکداری اسلامی
۱۵	۶.۱.۲.۱ نخستین بانک جهان از آن ایرانیان بود
۲۰	۳.۱ اینترنت
۲۲	۱.۳.۱ پروتکل‌های اینترنت
۲۳	۴.۱ تجارت
۲۸	۵.۱ تجارت الکترونیک در اینترنت
۳۱	۱.۵.۱ تاریخچه تجارت الکترونیک
۳۵	۲.۵.۱ امنیت تجارت الکترونیک
۳۸	۳.۵.۱ موفقیت در تجارت الکترونیک
۴۳	۶.۱ بانکداری الکترونیک
۴۶	۱.۶.۱ تاریخچه بانکداری الکترونیک در جهان

۵۱	۲.۶.۱ تاریخچه بانکداری الکترونیک در ایران
۵۲	۳.۶.۱ بانکداری متمرکز الکترونیکی
۵۴	۴.۶.۱ مدیریت ریسک و بانکداری الکترونیکی
۵۶	۷.۱ پرداخت الکترونیکی
۵۷	۱.۷.۱ ویژگی‌های سیستم‌های پرداخت الکترونیکی
۵۷	۸.۱ پول الکترونیکی
۵۹	۱.۸.۱ ویژگی‌های پول الکترونیکی
۶۱	۲.۸.۱ انواع پول الکترونیکی
۶۱	۱.۲.۸.۱ پول الکترونیکی شناسایی شده
۶۱	۲.۲.۸.۱ پول الکترونیکی غیرقابل شناسایی
۶۲	۹.۱ روش‌های مختلف ارائه خدمات بانکداری الکترونیک
۶۲	۱.۹.۱ کانال‌های بانکداری الکترونیک
۶۳	۲.۹.۱ شاخه‌های بانکداری الکترونیک
۶۳	۱.۲.۹.۱ استانداردها و پروتکل‌های مورد استفاده در بانکداری تلفن همراه
۶۴	۱.۱.۲.۹.۱ نسل اول تلفن همراه
۶۵	۲.۱.۲.۹.۱ نسل دوم تلفن همراه
۶۶	۳.۱.۲.۹.۱ نسل ۲.۵ تلفن همراه
۶۷	۴.۱.۲.۹.۱ نسل ۲.۷ تلفن همراه
۶۷	۵.۱.۲.۹.۱ نسل سوم تلفن همراه
۶۸	۱.۵.۱.۲.۹.۱ فناوری‌های سازگار با نسل سوم
۶۸	۱.۱.۵.۱.۲.۹.۱ بلوتوث
۶۹	۲.۱.۵.۱.۲.۹.۱ WML/WAP۵
	۱۰.۱ طبقه بندی خدمات بانکداری الکترونیک از نظر جنبه‌های مختلف
۷۰	ریسک
۷۰	۱.۱۰.۱ اطلاعات عمومی
۷۰	۲.۱۰.۱ اطلاعات مربوط به مشتری
۷۰	۳.۱۰.۱ دستورالعمل‌های وکالت مشتری
۷۱	۴.۱۰.۱ تعاملات مربوط به مشتری (تعاملات انفرادی)
۷۱	۵.۱۰.۱ ثبت مشخصات و ثبت نام مشتری
۷۲	۱۱.۱ مزایای بانکداری الکترونیک

۷۳	۱۲.۱ بانکداری الکترونیک ؛ فرصت‌ها و تهدیدها
۷۵	فصل دوم: اینترنت، بانکداری اینترنتی و امنیت (مرور کلی)
۷۷	۱.۲ بانکداری اینترنتی
۷۸	۲.۲ مسائل امنیتی در بانکداری اینترنتی
۷۸	۱.۲.۲ معماری و نیازمندی‌های امنیت
۷۸	۱.۱.۲.۲ معماری اینترنت
۷۹	۲.۱.۲.۲ نیازمندی‌های امنیت
۸۰	۳.۱.۲.۲ هزینه در ازای امنیت
۸۱	۴.۱.۲.۲ خدمات سیستم بانکداری اینترنتی
۸۲	۲.۲.۲ امنیت مخابرات میان کاربر و بانک
۸۲	SSL/ TLS ۱.۲.۲.۲
۸۲	۱.۱.۲.۲.۲ کانال ایمن
۸۳	۲.۱.۲.۲.۲ توافق و انتقال داده
۸۴	SSLV۲/SSLV۳/TLS ۲.۲.۲.۲
۸۵	۳.۲.۲.۲ مسایل پیاده‌سازی
۸۶	۴.۲.۲.۲ تکیه‌گاه‌های اعتماد
۸۷	۵.۲.۲.۲ محدودیت‌های صادراتی
۸۸	۳.۲.۲ اعتبارسنجی کاربر
۸۸	۱.۳.۲.۲ اعتبارسنجی موجودیت در برابر اعتبارسنجی تراکنش
۸۸	۲.۳.۲.۲ مکانیزم تصدیق
۸۸	۱.۲.۳.۲.۲ رمز با طول ثابت
۸۹	۲.۲.۳.۲.۲ رمز پویا
۹۰	۳.۲.۳.۲.۲ پرسش / پاسخ
۹۰	SSL/TLS ۴.۲.۳.۲.۲
۹۱	۵.۲.۳.۲.۲ امضای دیجیتالی
۹۱	۶.۲.۳.۲.۲ مجوزهای سخت‌افزاری
۹۲	۴.۲.۲ محافظت و امنیت داده‌ها
۹۲	۱.۴.۲.۲ کدگذاری و رمز کردن داده‌ها
۹۲	۱.۱.۴.۲.۲ تعاریف

۹۳	۲.۱.۴.۲.۲ پیشینه
۹۴	۳.۱.۴.۲.۲ بانک‌ها چگونه رمزگذاری را بکار می‌برند؟
۹۴	۲.۴.۲.۲ مراجع تأیید کننده و گواهی‌های دیجیتال
۹۵	۳.۴.۲.۲ روترها و دیواره‌های آتش
۹۸	۴.۴.۲.۲ امنیت فیزیکی
۹۸	۵.۲.۲ مطالب بیشتر راجع به امنیت
۹۸	۱.۵.۲.۲ ثبت‌نام
۹۹	۲.۵.۲.۲ وکالت و نمایندگی
۱۰۰	۳.۵.۲.۲ بسترهای امن
۱۰۱	۴.۵.۲.۲ عامل انسانی
۱۰۱	۵.۵.۲.۲ ورود به کامپیوتر و کنترل عملیات
۱۰۳	فصل سوم: محافظت و امنیت داده‌ها
۱۰۴	۱.۳ رمزنگاری
۱۰۵	۲.۳ تاریخچه رمزنگاری
۱۱۲	۳.۳ اصطلاحات رایج رمزنگاری
۱۱۴	۴.۳ اصول ششگانه کرکف
۱۱۶	۵.۳ سرویس رمزنگاری
۱۱۷	۶.۳ پروتکل رمزنگاری
۱۱۸	۷.۳ الگوریتم‌های رمزنگاری
۱۲۰	۱.۷.۳ الگوریتم‌های بدون کلید
۱۲۰	۱.۱.۷.۳ توابع درهم‌ساز
۱۲۱	۱.۱.۱.۷.۳ تصادم هش
۱۲۲	۲.۱.۷.۳ جایگشت یک‌طرفه
۱۲۲	۲.۷.۳ الگوریتم‌های مبتنی بر کلید
۱۲۲	۱.۲.۷.۳ الگوریتم‌های رمزنگاری کلید متقارن
۱۲۴	۱.۱.۲.۷.۳ الگوریتم‌های رمزنگاری DES, ۳DES
۱۲۷	۱.۱.۱.۲.۷.۳ الگوریتم Key Schedule
۱۲۷	۲.۱.۱.۲.۷.۳ امنیت DES
۱۲۹	۳.۱.۱.۲.۷.۳ الگوریتم‌های جایگزین DES

- ۱۳۰ ۲.۱.۲.۷.۳ الگوریتم رمز دنباله‌ای
- ۱۳۱ ۱.۲.۱.۲.۷.۳ مزایا، معایب و کاربردهای رمزهای دنباله‌ای
- ۱۳۲ ۲.۲.۱.۲.۷.۳ نمونه‌های رمزهای دنباله‌ای پیاده‌سازی شده
- ۱۳۳ ۳.۱.۲.۷.۳ رمز قطعه‌ای یا بلوکی
- ۱۳۶ ۱.۳.۱.۲.۷.۳ کاربردهای رمزهای قطعه‌ای
- ۱۳۷ ۲.۳.۱.۲.۷.۳ طراحی الگوریتم رمز قطعه‌ای
- ۱۳۹ ۴.۱.۲.۷.۳ توابع تصدیق پیام (MAC)
- ۱۴۰ ۲.۲.۷.۳ الگوریتم‌های رمزنگاری کلید نامتقارن
- ۱۴۲ ۱.۲.۲.۷.۳ الگوریتم RSA
- ۱۴۸ ۲.۲.۲.۷.۳ الگوریتم‌های مبتنی بر لگاریتم گسسته
- ۱۴۹ ۱.۲.۲.۲.۷.۳ مثال عددی توابع لگاریتم گسسته
- ۱۴۹ ۲.۲.۲.۲.۷.۳ مسأله لگاریتم گسسته
- ۱۵۰ ۳.۲.۲.۲.۷.۳ الگوریتم‌های محاسبه
- ۱۵۱ ۴.۲.۲.۲.۷.۳ کاربرد در رمزنگاری
- ۱۵۱ ۳.۲.۲.۷.۳ الگوریتم‌های مبتنی بر منحنی‌های بیضوی
- ۱۵۲ ۳.۲.۷.۳ امضای دیجیتالی
- ۱۵۲ ۱.۳.۲.۷.۳ مقدمه
- ۱۵۳ ۲.۳.۲.۷.۳ مشخصات امضای دیجیتال
- ۱۵۸ ۳.۳.۲.۷.۳ معایب امضای دیجیتال
- ۱۶۰ ۴.۳.۲.۷.۳ مزایای امضای دیجیتال
- ۱۶۱ ۵.۳.۲.۷.۳ چگونه یک امضای دیجیتالی درست کنیم؟
- ۱۶۲ ۸.۳ مراجع تأیید کننده و گواهی‌های دیجیتال
- ۱۶۳ ۱.۸.۳ زیرساخت کلید عمومی (PKI)
- ۱۶۴ ۱.۱.۸.۳ مولفه‌های زیرساخت کلید عمومی
- ۱۶۵ ۱.۱.۱.۸.۳ سیاست‌های صدور گواهی (CP)
- ۱۶۵ ۲.۱.۱.۸.۳ مرجع صدور گواهی (CA)
- ۱۶۷ ۳.۱.۱.۸.۳ مرجع ثبت گواهی (RA)
- ۱۷۰ ۴.۱.۱.۸.۳ مرجع الصاق زمان (TSA)
- ۱۷۲ ۵.۱.۱.۸.۳ پایگاه نگهداری گواهی‌ها (LD)
- ۱۷۳ ۶.۱.۱.۸.۳ سیستم توزیع گواهی (CDS)

۱۷۴	۲.۸.۳ گواهی‌های دیجیتال
۱۷۴	۱.۲.۸.۳ انواع مختلف گواهی
۱۷۵	۲.۲.۸.۳ انواع کلاسهای گواهی دیجیتال
۱۷۵	۳.۲.۸.۳ ساختار گواهی
۱۷۸	۴.۲.۸.۳ ساختارهای دیگر گواهی
۱۷۸	SPKI ۱.۴.۲.۸.۳
۱۷۹	PGP ۲.۴.۲.۸.۳
۱۷۹	SET ۳.۴.۲.۸.۳
۱۸۰	۵.۲.۸.۳ گواهی‌های اختیاری
۱۸۰	۶.۲.۸.۳ مدیریت گواهی
۱۸۱	۷.۲.۸.۳ صدور گواهی
۱۸۱	۸.۲.۸.۳ ابطال گواهی
۱۸۲	۹.۲.۸.۳ انتشار یک لیست از گواهی‌های باطل شده
۱۸۲	۱۰.۲.۸.۳ وارد و صادر کردن گواهی
۱۸۳	۱۱.۲.۸.۳ تنظیمات Active Directory برای گواهی‌ها
۱۸۵	<b>فصل چهارم: امنیت بانکداری اینترنتی</b>
۱۸۷	۱.۴ امنیت بانکداری اینترنتی
۱۸۸	۲.۴ مفهوم اعتماد
۱۸۹	۳.۴ یک چارچوب امنیتی نمونه از بانکداری اینترنتی
۱۹۰	۱.۳.۴ مراحل روند عملیات چارچوب
۱۹۲	۴.۴ محیط بانکداری اینترنتی
۱۹۲	۱.۴.۴ توصیف فضاهای موجود در محیط بانکداری اینترنتی
۱۹۵	۲.۴.۴ عملیات مستقل در تراکنش‌های بانکداری اینترنتی
۱۹۵	۳.۴.۴ تحلیل تصمیم امنیتی
۱۹۸	۴.۴.۴ مطالعه موردی
۲۰۰	۵.۴ احراز هویت و اهمیت آن در سیستم بانکداری اینترنتی
۲۰۳	۱.۵.۴ ارزیابی ریسک
۲۰۵	۲.۵.۴ متدولوژی‌ها، فرایندها و تکنیک‌های احراز هویت
۲۱۷	۶.۴ پروتکل‌های امنیتی مورد استفاده در سیستم بانکداری اینترنتی

۲۱۷	۱.۶.۴ پروتکل امنیتی SSL
۲۱۹	۲.۶.۴ پروتکل امنیتی لایه انتقال امن
۲۲۰	۳.۶.۴ پروتکل امنیتی فرایندهای الکترونیکی امن
۲۲۴	۴.۶.۴ پروتکل امنیتی سه بعدی
۲۲۷	<b>فصل پنجم: تهدیدهای موجود در سیستم بانکداری اینترنتی</b>
۲۲۹	۱.۵ تهدیدها و حمله‌ها در سیستم بانکداری اینترنتی
۲۳۱	۲.۵ حمله‌های موجود در سیستم بانکداری اینترنتی
۲۳۲	۱.۲.۵ حمله‌ی راه دور
۲۳۲	۱.۱.۲.۵ حمله‌ی فیشینگ
۲۳۷	۲.۱.۲.۵ حمله‌ی سرویس نام دامنه
۲۳۷	۳.۱.۲.۵ حمله‌ی استراق سمع
۲۳۸	۲.۲.۵ حمله‌ی محلی
۲۴۳	۳.۲.۵ حمله‌ی چندگانه
۲۴۶	۳.۵ نمونه‌هایی از رشد سریع حملات اینترنتی
۲۴۶	۱.۳.۵ رشد چشمگیر حملات فیشینگ در اینترنت
۲۴۹	۲.۲.۵ تروجان اینترنتی Ransom-A
	۳.۳.۵ ویروس رایانه‌ای جدید اقدام به نصب مرورگر تقلبی و پخش موسیقی
۲۵۰	گوش خراش می‌کند
۲۵۱	۴.۳.۵ آدوب کاربران نرم افزار فلش را به دانلود وصله اصلاحی فراخواند
	۵.۳.۵ یک شرکت اینترنتی ۲۹ ایراد امنیتی نرم افزارهای شرکت‌های
۲۵۲	معروف را فاش می‌کند
۲۵۳	۶.۳.۵ ویروس رایانه‌ای با نام "سانتا"
۲۵۵	<b>فصل ششم: روش‌های حفاظتی در برابر حملات اینترنتی</b>
۲۵۷	۱.۶ روش‌های حفاظتی
۲۵۸	۱.۱.۶ کد اعلان بر اساس پیام کوتاه
۲۶۰	۲.۱.۶ روش تأیید تصویر
۲۶۵	۳.۱.۶ پوسته‌ی امنیتی پویا
۲۶۶	۴.۱.۶ روش‌های مقابله با فیشینگ

۲۶۷	۵.۱.۶ رمز عبور هش شده به همراه نام دامنه
۲۶۸	۶.۱.۶ راه حل نرم افزاری براساس PKI
۲۷۱	۷.۱.۶ توکن‌های سخت افزاری براساس PKI

## فصل هفتم: تهدیدهای موجود در عملیات احراز هویت

۲۷۵	در بانکداری اینترنتی
۲۷۷	۱.۷ تهدیدهای موجود در عملیات احراز هویت
	۱.۱.۷ تهدیدهای موجود در عملیات احراز هویت در بانکداری اینترنتی
۲۷۷	بصورت کلی
۲۷۷	۱.۱.۱.۷ حمله سرقت اطلاعات محرمانه بصورت برون خطی
۲۷۸	۲.۱.۱.۷ حمله سرقت کانال اینترنتی
	۲.۱.۷ تهدیدهای موجود در عملیات احراز هویت در بانکداری اینترنتی
۲۸۰	بصورت جزئی
۲۸۰	۱.۲.۱.۷ حمله پسورد کرکر
۲۸۰	۱.۱.۲.۱.۷ حمله بروت فورس
۲۸۰	۲.۱.۲.۱.۷ حمله دیکشنری
۲۸۱	۲.۲.۱.۷ حمله فیشینگ
۲۸۱	۳.۲.۱.۷ حمله فریب دهنده سرور
۲۸۲	۴.۲.۱.۷ حمله کشف فایل رمزعبور
۲۸۳	۵.۲.۱.۷ حمله شولدر سرفینگ
۲۸۴	۶.۲.۱.۷ تروجان ربودن پسورد
۲۸۴	۱.۶.۲.۱.۷ تروجان ثبت کننده کلید
۲۸۴	۲.۶.۲.۱.۷ تروجان هدایت کننده
	۲.۷ رده بندی روش‌های احراز هویت براساس مقاومت آنها
۲۸۴	نسبت به مهاجمان

## فصل هشتم: پروتکل‌های پیشنهادی برای افزایش امنیت

۲۸۷	احراز هویت در بانکداری اینترنتی
	۱.۸ پروتکل‌ها و روش‌های پیشنهادی حفاظتی در مسئله
۲۸۹	احراز هویت در بانکداری اینترنتی

۲۸۹	۲.۸ پروتکل‌های پیشنهادی برای عمل احراز هویت
۲۸۹	۱.۲.۸ راه‌حل رمز عبور کوتاه مدت
۲۹۲	۲.۲.۸ راه حل براساس گواهی نامه دیجیتالی
۲۹۵	۳.۲.۸ احراز هویت بر اساس تولید کلید پویا
۳۰۰	۴.۲.۸ احراز هویت با استفاده از رمز عبور ساده با کمک توابع هش
۳۰۲	۳.۸ روش احراز هویت مورد استفاده در دو بانک خارجی (HSBC, ING)
۳۰۵	۴.۸ مقایسه روش‌های احراز هویت موجود

۳۰۹	<b>فصل نهم: امنیت بانکداری اینترنتی در بانک‌های ایران</b>
۳۱۱	۱.۹ اینترنت بانک در ایران
۳۱۲	۲.۹ بانکداری اینترنتی در بانک ملت
۳۱۴	۱.۲.۹ امنیت اینترنت بانک ملت توسط پروتکل SSL
۳۱۶	۳.۹ بانکداری اینترنتی در بانک سامان
۳۱۷	۱.۳.۹ امنیت سامان کارت
۳۱۸	۴.۹ بانکداری اینترنتی در بانک پاسارگاد
۳۲۰	۵.۹ بانکداری اینترنتی در بانک کشاورزی
۳۲۳	۶.۹ بانکداری اینترنتی در بانک اقتصاد نوین
۳۲۴	۷.۹ بانکداری اینترنتی در بانک صادرات
۳۲۵	۱.۷.۹ نکات مهم به هنگام استفاده از اینترنت بانک صادرات
۳۲۷	۸.۹ بانکداری اینترنتی در بانک تجارت
۳۲۸	۱.۸.۹ نکات امنیتی در هنگام استفاده از اینترنت بانک تجارت
۳۲۹	۹.۹ بانکداری اینترنتی و بانک پارسیان
۳۲۹	۱.۹.۹ نکات امنیتی مربوط به اینترنت بانک پارسیان
۳۳۱	۱۰.۹ بانکداری اینترنتی در بانک ملی
۳۳۱	۱.۱۰.۹ عضویت در سبا و مسائل امنیتی موجود
۳۳۳	۲.۱۰.۹ مقررات و شرایط فعال‌سازی شناسه کاربری
۳۳۵	۱۱.۹ بانکداری اینترنتی بانک سرمایه
۳۳۷	۱۲.۹ بانکداری اینترنتی بانک سینا
۳۳۸	۱۳.۹ ملاحظات ایمنی در سیستم بانکداری اینترنتی
۳۳۸	۱.۱۳.۹ ملاحظات ایمنی پیش بینی شده در سیستم بانکداری اینترنتی

۳۳۸	۱.۱.۱۳.۹ موارد امنیتی در نظر گرفته شده در سطح شبکه
۳۳۹	۲.۱.۱۳.۹ موارد امنیتی در نظر گرفته شده در سطح سیستم
۳۴۰	۳.۱.۱۳.۹ موارد امنیتی در نظر گرفته شده در انجام تراکنش‌ها
۳۴۰	۲.۱۳.۹ مواردی امنیتی که مشتری باید رعایت کند
۳۴۰	۱.۲.۱۳.۹ امنیت سیستم عامل
۳۴۱	۲.۲.۱۳.۹ امنیت مرورگر وب
۳۴۲	۳.۲.۱۳.۹ امنیت در مقابل ویروس‌های شناخته شده
۳۴۲	۴.۲.۱۳.۹ امنیت پست الکترونیکی
۳۴۳	۵.۲.۱۳.۹ سایر موارد
۳۴۷	مراجع
۳۵۳	واژه نامه

## پیشگفتار

با رشد روز افزون تجارت الکترونیکی و به تبع آن بانکداری اینترنتی و در مقابل افزایش ریسک و پیچیده شدن حمله‌های موجود در سیستم‌های الکترونیکی، مسئله امنیت عملیات و تراکنش‌های اینترنتی پررنگ‌تر شده و از مسائل بنیادین هر سیستم الکترونیکی در نظر گرفته می‌شود. علیرغم اینکه با رشد و گسترش تجارت الکترونیکی و تمامی بخش‌های مرتبط با آن از جمله بانکداری اینترنتی، جنبه‌های امنیتی مربوط به آن‌ها در نظر گرفته شده و توجه زیادی از جانب سازمان‌ها و سیستم‌های الکترونیکی شده است، اما باز هم شاهد تخلف‌های زیادی در سیستم‌های الکترونیکی مخصوصاً در بخش بانکی و به تبع آن ضرر و زیان هنگفتی در این بخش‌ها هستیم. علاوه بر زیان‌های مالی وارده به این سیستم‌ها، این موضوع سبب کم شدن ارتباط مشتری و همچنین سلب اعتماد آن‌ها از سیستم اینترنتی بانک‌ها می‌شود. بانک‌های زیادی در سطح دنیا از این موضوع در سیستم اینترنتی خود رنج می‌برند و روز به روز مقادیر مالی به سرقت رفته از حساب‌های مشتریان در این بانک‌ها افزایش می‌یابد. دلیل این موضوع می‌تواند افزایش پیچیدگی روز افزون حمله‌ها و تهدیدهای موجود برای بانک‌ها، و در مقابل ضعف مکانیزم‌های امنیتی در این سیستم‌ها، مخصوصاً در مسئله احراز هویت و ورود مشتریان به سیستم بانکی باشد. در این کتاب سعی شده است به بیان ساده و روان به مفاهیم امنیت بانکداری اینترنتی، حفاظت و امنیت اطلاعات، مفاهیم بنیادین و پروتکل‌های امنیتی مرتبط پرداخته شود. همچنین آسیب‌پذیری‌ها، تهدیدها و حمله‌های

اینترنتی موجود در سیستم‌های بانکداری اینترنتی، مخصوصاً در مسئله احراز هویت و نیز روش‌های محافظت در برابر این حملات بیان شده است. در ادامه به روش‌ها و پروتکل‌های پیشنهادی در سطح مقالات برای افزایش امنیت در مسئله احراز هویت در سیستم بانکداری اینترنتی پرداخته شده است. و در انتها امنیت بانکداری اینترنتی در سطح بانک‌های داخل کشور بررسی شده است. امید است این کتاب بتواند گامی هر چند کوچک در زمینه فرهنگ استفاده، مخصوصاً دقت در استفاده از سیستم‌های بانکداری اینترنتی برداشته و مورد توجه و علاقه دانشجویان، مدیران و کارشناسان IT و امنیتی ادارات و سازمان‌ها واقع شود.

زمستان ۱۳۸۸

دکتر شهیار محمدی

زینب زارع حسینی