
بسم الله الرحمن الرحيم

پردیس بین الملل دانشگاه گیلان

رشته مهندسی فناوری اطلاعات (تجارت الکترونیک)

تحلیل امنیتی پروتکل های پرداخت سیار مبتنی بر WAP

از

مجتبی ایوبی مبرهن

استاد راهنما:

دکتر اسدالله شاه بهرامی

استاد مشاور:

دکتر رضا ابراهیمی آتانی

شهریور ماه ۱۳۹۱

تقدیم به

پدر و مادر عزیزم، که همیشه پشتیبان و همراه من در زندگی هستند.

تشکر و قدردانی

از خداوند بزرگ شکرگذارم. بزرگترین افتخار من این است که خالقی چون او دارم.

از دکتر اسدالله شاه بهرامی استاد راهنمای پایان‌نامه ام تشکر فراوان می کنم. اگر بخواهم در یک جمله ایشان را وصف کنم باید بگویم: او به من اندیشیدن را آموخت نه اندیشه ها را.

از جناب آقای دکتر رضا ابراهیمی مشاور پایان نامه که در این راه مرا یاری نمودند تشکر فراون دارم.

فهرست مطالب

فصل پنجم (راه حل های پیشنهادی) ٦٦

فهرست اشکال

فهرست جداول

فهرست حروف اختصاری					
AuC	Authentication Center	HTTP	Hypertext Transfer Protocol	SMS	**Short Message Service**
B2B	Business To Business	HTML	Hyper Text Markup Language	SSL	**Secure Sockets Layer**
B2C	Business To Consumer	HMAC	Hash-based Message Authentication Code	SIM	**Subscriber Identity Module**
B2G	Business To Government	ITTP	Intelligent Terminal Transfer Protocol	SHA	**Secure Hash Algorithm**
C2C	Consumer To Consumer	ISP	Internet Service Provider	SS7	**Signaling System 7**
C2G	Consumer To Government	IP	Internet Protocol	TTML	**Timed Text Markup Language**
CDMA	Code Division Multiple Access	IE	Internet Explorer	TCP/IP	**Transmission Control Protocol/Internet Protocol**
CDPD	Cellular Digital Packet Data	IDEA	International Data Encryption Algorithm	TCP	**Transmission Control Protocol**
CA	Certificate Authority	ITU	International Telecommunication Union	TLS	**Transport Layer Security**
DLP	Discrete Logarithm Problem	IMT2000	International Mobile Telecommunication 2000	UMTS	**Universal Mobile Telecommunications System**
DES	Data Encryption Standard	ICMP	Internet Control Message Protocol	UDP	**User Datagram Protocol**
3DES	Triple DES	IPS	Intrusion Prevention System	UA	**User Agent**
DoS	Denial of Service	IDS	Intrusion Detection System	URL	**Uniform Resource Locator**
EMS	Enhanced Messaging Service	KDC	Key Distribution Center	WAP	**Wireless Application Protocol**
EDGE	Enhanced Data rates for GSM Evolution	LDAP	Lightweight Directory Access Protocol	WML	**Wireless Markup Language**
ECMA	European Computer Manufacture Association	MAC	Message Authentication Code	WDP	**Wireless Datagram Protocol**
ECDH	Elliptic Curve Diffie Hellman	ME	Mobile Equipment	WTLS	**Wireless Transport Layer Security**
ECC	Elliptic Curve Cryptography	MD5	Message Digest 5	WTP	**Wireless Transaction Protocol**
ECDLP	Elliptic Curve Discrete Logarithm Problem	MiM	Man In the Middle	WSP	**Wireless Session Protocol**
ECDSA	Elliptic Curve Digital Signature Algorithm	MSP	Mobile Service Providers	WPKI	**Wireless Public Key Infrastructure**
ETSI	European Telecommunications Standards Institute	OSI	Open Systems Interconnection	WIM	**WAP Identity Module**
FTP	File Transfer Protocol	PDA	Personal Digital Assistant	WTLSK	**Improved WTLS by means of Kerberos**
GSM	Global System for Mobile Communications	PKI	Public Key Infrastructure	WBIPS	**WTLS Based on IPS**
GPRS	General Packet Radio Service	PIN	Personal Identification Number	WBVPN	**WTLS Based on VPN**
GTP	GPRS Tunneling Protocol	PRF	Pseudo Random Function	XML	**Extensible Markup Language**
HDML	Handheld Device Markup Language	RSA	Rivest, Shamir, Adleman	XHTML	**Extensible Hyper Text Markup Language**

تحلیل امنیتی پروتکل های پرداخت سیار مبتنی بر WAP

مجتبی ایوبی مبرهن

چکیده :

در دنیا امروز، تجارت الکترونیک بخش مهمی از زندگی انسان ها شده است. تجارت الکترونیک مدل ها و انواع مختلفی دارد ولی تمام این مدل ها صرف نظر از تفاوت های اساسی که در ویژگی های خود دارند از بخش های کلی تقریبا مشابه ای مانند پرداخت، حمل ونقل و تبلیغات تشکیل شده اند. یکی از مهم ترین بخش ها در هر مدل از تجارت الکترونیک قسمت پرداخت الکترونیکی هزینه کالا یا خدمات خریداری شده است. پرداخت الکترونیکی را می توان از دیدگاه های متفاوتی بررسی کرد. یکی از مدل های پرداخت، پرداخت الکترونیکی بوسیله دستگاه های سیار مانند گوشی های همراه و از طریق شبکه های بی سیم می باشد. در این پروژه انواع پرداخت سیار بررسی شده و سیستم WAP به عنوان سیستم پرداخت سیار انتخاب می شود. ساختار پروتکل WAP و لایه های تشکیل دهنده آن را بیان کرده و روی ویژگی های امنیتی آن تمرکز می کنیم. مکانیزم های امنیتی WTLS، WIM و WPKI توضیح داده و مشکلات و ضعف های امنیتی سیستم WAP بیان می شود. در پایان راه کار ها و روش های مناسب برای بالا بردن سطح امنیت پرداخت سیار توسط مکانیزم WAP را ارائه می دهیم.

کلمات کلید :

دستگاه های سیار، شبکه های بی سیم، پروتکل کاربردی بی سیم، پرداخت سیار، احراز هویت، حملات امنیتی و تجارت الکترونیک

Security Analysis of Mobile Payment Protocols based on WAP

Mojtaba Ayoubi Mobarhan

Abstract:

Nowadays, electronic commerce is the important part of people life. Electronic commerce has different types and models. All of these models have same parts like payment, transportation and advertisement. One of the most significant sections of any model in the electronic commerce is the payment of goods and services purchased. Electronic payment can be examined from different perspectives. One of the models of payment is mobile payment by mobile devices like cell phones and the wireless network. In this project, two types of payment systems are studied and WAP system is selected as mobile payment system. We explain WAP structure and layers. Then, we focus on security specification of WAP system. The WAP security mechanisms like WTLS, WIM and WPKI are described. In addition, security weaknesses, problems and attacks are presented in this system. Therefore, some solutions and ways are proposed to increase security level of mobile payment with WAP mechanism.

Keywords:

Mobile Device, Wireless Network, Wireless Application Protocol, M Payment, Authentication, Security Attacks and Electronic Commerce.

فصل اول

مقدمه

۱-۱- مقدمه

اکنون که در عصر پیشرفت تکنولوژی اطلاعات و ارتباطات قرار داریم، ملت ها، شرکت ها و دولت ها برای کسب موفقیت در میدان رقابت و افزایش درآمد خود ناگزیر از مجهز شدن به ابزارهای تکنولوژی و روی آوردن به تجارت الکترونیک می‌باشند. تجارت الکترونیک از مزایا و پیامد های اقتصادی مهمی از قبیل گسترش بازار، کاهش قیمت منابع تولید، ارتقای بهره‌وری، کاهش هزینه های مبادلاتی، ایجاد اشتغال و کاهش تورم برخوردار بوده و در رشد اقتصادی جامعه نقش محوری ایفا می کند. یکی از مهم ترین بخش ها در هر مدل از تجارت الکترونیک قسمت پرداخت الکترونیکی هزینه کالا یا خدمات خریداری شده است. اهمیت این بخش به این علت است که عملیات مالی و جابجایی پول الکترونیکی بین حساب های بانکی در این بخش صورت می گیرد. روش های مختلفی برای پرداخت بر حسب نوع کاربرد و شرایط وجود داردکه می توان تمام این روش ها را با معیارهایی مثل راحتی، امنیت، سرعت، توان و انرژی مصرفی بررسی و ارزیابی کرد. یکی از روش های پرداخت، پرداخت الکترونیکی به وسیله دستگاه های سیار مانند گوشی های همراه و از طریق تکنولوژی های بی سیم مانند شبکه های سلولی دیجیتال می باشد. تجارت سیار امروزه مورد توجه و کاربرد بیشتر مردم دنیا قرار گرفته است بنابراین در راستای آن اهمیت پرداخت سیار نیز روز به روز افزایش می یابد.

در تجارت الکترونیک سیستم های مختلفی برای انجام پرداخت سیار وجود دارد. کاربران می توانند متناسب با نیاز و شرایط خود سیستم پرداخت الکترونیکی مناسب را انتخاب و از آن استفاده کنند. یکی از سیستم های پرداخت که امروزه مورد توجه اکثر کاربران قرار گرفته است استفاده از سرویس اینترنت سیار برای انجام امور بانکی است. برای استفاده از اینترنت در دستگاه های سیار ما نیازمند به پروتکل کاربردی بی سیم یا Wireless Application Protocol (WAP) هستیم. پروتکل WAP[1] یک پروتکل استاندارد ارتباطات برای استفاده از اینترنت در دستگاه های سیار است که توسط ۴ شرکت بزرگ دنیا در سال ۱۹۹۷ طراحی و ساخته شد. در واقع می توان گفت که این پروتکل همان پروتکل اینترنت بهینه شده برای ارتباطات بی سیم است. ما در این پروژه تکنولوژی WAP را به عنوان سیستم پرداخت سیار انتخاب کردیم.

۱-۲- ضرورت انجام پروژه

در تراکنش های تجارت الکترونیک، مخصوصا در پرداخت الکترونیک حفظ امنیت داده های ارسالی دارای اهمیت بسیار زیادی است. شبکه های بی سیم با وجود مزیت های زیادی که برای کاربران خود دارند، از امنیت کمتری نسبت به شبکه های با سیم

[1] . Wireless Application Protocol (WAP)

برخور دارند. از یک طرف دسترسی به شبکه های بی سیم برای متجاوزان بسیار راحت است چون شبکه های بی سیم مانند شبکه های با سیم دارای ناحیه و محدوده مشخصی نیستند و از طرف دیگر به علت محدودیت های موجود در دستگاه های سیار و شبکه های بی سیم مانند پهنای باند ضعیف، حافظه کم، قدرت پردازش پایین و توان مصرفی بالا نمی توان از سیستم های امنیتی و الگوریتم های رمزنگاری قوی به راحتی در محیط بی سیم استفاده کرد. از این رو، امنیت شبکه های بی سیم و کاربرد های خاص آن مثل پرداخت سیار بسیار حائز اهمیت است.

۱-۳- اهداف پروژه

همان طور که در بخش قبل گفته شد امنیت پرداخت سیار به خاطر ویژگی های خاص شبکه های بی سیم دارای اهمیت بسیار زیادی است. در این پروژه پروتکل WAP به عنوان سیستم پرداخت سیار انتخاب و روی معیار امنیت این سیستم تمرکز می شود. پارامترهای مختلف امنیتی این سیستم را بررسی کرده و مکانیزم های مناسب برای فراهم کردن این پارامترها را تحلیل می کنیم تا بتوانیم نقاط ضعف و محدودیت های امنیتی موجود در این سیستم را درک کنیم. در پایان راه حل های مناسبی برای بهبود امنیت این سیستم در پرداخت سیار پیشنهاد خواهد شد.

۱-٤- مراحل انجام پروژه

در این پایانامه ابتدا روی تجارت الکترونیک، تجارت سیار و پرداخت سیار مطالعه ای جامع صورت می گیرد. سپس روی پرداخت الکترونیک به وسیله پروتکل WAP متمرکز می شویم. ساختار پروتکل WAP و لایه های تشکیل دهنده آن را بررسی نموده و با مطالعه دقیق روی مکانیزم های امنیتی آن، نقاط ضعف و حملات صورت گرفته روی این سیستم را تحلیل می کنیم. در پایان، راه حل های مناسب برای بهبود امنیت این سیستم ارائه می شود. ترتیب مراحل انجام پروژه به شرح زیر است.

۱. مطالعه جامع و گسترده روی مفهوم تجارت الکترونیک و مدل های مختلف آن و تمرکز روی تجارت سیار
۲. تحقیق و بررسی روی پرداخت سیار و روش ها و سیستم های پرداخت به وسیله دستگاه های بی سیم
۳. بررسی ساختار پروتکل کاربردی بی سیم WAP
۴. مطالعه مکانیزم های امنیتی پروتکل WAP و الگوریتم های رمزنگاری مورد استفاده در این مکانیزم ها
۵. تحلیل و آنالیز ضعف های موجود در مکانیزم های امنیتی و حملات صورت گرفته در سیستم WAP