NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY
[IJIERT] ISSN: 2394-3696 Website: ijiert.org
VOLUME 10, ISSUE 10, Oct. -2023

SMART PARKING COMMUNITY SUPPORTS PARKING VEHICLE

Dr. S.Gopinath*,
Assistant Professor, Department of Information Technology,
Gnanamani College of Technology, Namakkal-637018,
sgopicse@gmail.com.

G.Kowsalya,
Assistant Professor, Department of Computer Science and Engineering,
Gnanamani College of Technology,
Namakkal-637018

S.Arularasi,
Assistant Professor, Department of Computer Science and Engineering,
Gnanamani College of Technology, Namakkal-637018.

R Pradeepa,
Assistant Professor, Department of Information Technology,
Gnanamani College of Technology, Namakkal-637018.

R Mekala,
Assistant Professor, Department of Information Technology,
Gnanamani College of Technology, Namakkal-637018

ABSTRACT

Cooperation between vehicles facilitates traffic management, road safety and infotainment applications.However, cooperation requires trust in the authenticity of the information received. In this paper, we address the challenge of securely exchanging information about parking availability. Trust is important in assisting in deciding whether interrogation is appropriaterely on information received about free parking spaces near your destination and thus ignore other possible spaces on the route.Therefore, we propose Parking Communities, which provide a distributed and dynamic way to set up Vehicle groups help each other find safe parking spaces in their respective community areas.Our approach is based on modern, high-performance encryption and signature algorithms as well as a well-understood mathematical trust assessment model. This approach enables end-to-end encrypted request-response communications combined with geolocation and can be used as an overlay to existing vehicular network technologies. We provide comprehensive comparisons with other security solutions The architecture and simulation results demonstrate the feasibility of our method.

I.INTRODUCTION

Modern vehicles are equipped with many features

Sensor system and support functions can greatly improve driving comfort and safety. However, to maximize efficiency, these different systems must cooperate with each other. Vehicles therefore not only rely on on-board sensors but can also collect additional information from other systems, mobile and fixed, in their

environment. For example, consider a situation in which a driver returning from work is interested in a free parking spot on their downtown street.

Therefore, the vehicle uses geocast (a specialized form of multicast, in which destination nodes are addressed by their geographic location instead of their identifier) to send the corresponding request to the destination area.Here, vehicles use sensor systems to collect information about their surroundings, such as distance to nearest objects (e.g., cars), and respond to requesters.The car can therefore tell the driver where to find a parking space, preferably near their home.In this example, trust is important to support the decision of whether the requester should trust the information received about free parking near their home.its destination and thus ignores other available points along the way.

This carries the risk of knowing that there are no available locations in the target area and that those locations were previously overlooked.

The authors are based at the Institute of Computer Networks and Operating Systems, Technische Universit¨at Braunschweig, 38106 Braunschweig,

Germany, (E-mail: timpner@ibr.cs.tubs.de; schuermann@ibr.cs.tubs.de; Wolf@ibr.cs.tu-bs.de).can be done at that time. Trust, in turn, facilitates the prioritization of incoming requests and can encourage other vehicles to help, so that they will also receive the requested information reciprocally.Additionally, attackers will likely try to gain an advantage, for example by providing false data to users.

Keep parking for yourself or by blocking Parking availability information to get a spot sooner than competing drivers.Unfortunately, there is no easy way to decide which medium to trust, or more precisely, how much to trust.Even if there is a trusted third party (TTP), such as in the form of a certificate authority (CA) providing a fake certificate, it is not necessary to verify the reliability of the media's response.Doing this will require reliable sensors in every parking space across the city, which is expensive and requires the support of an infrastructure network.We propose, design, implement and evaluate concept of Community Parking, in which, style of helping neighbors, providing distribution services and dynamic ways to establish trusted groups of Vehicles help each other find parking spaces respective community area.

Our approach leverages modern, high-performance encryption and signing algorithms, including elliptic curve cryptography (ECC), as well as a well-understood mathematical trust evaluation model.

1.1 Contributions

In this paper we present the design and implementation and a review of Parking Communities, a novel Trusted management for parking applications IEEE TRANSACTIONS ON RELIABLE AND SECURE OMPUTING, 2015 and LarsWolf, an IEEE member without reliance on central TTP or roadside units (RSUs). Its new features include a distributed trust model for parking applications as well as encrypted and signed request-response communications combined with geolocation. This provides protection against spoofing, Sybil attacks, interception and spoofing despite its distributed design. Additionally, it can be used as an overlay to existing vehicular network technologies, thus benefiting from established knowledge.

security mechanisms, for example, pseudonymous certificates for anonymity and location security. We give one Detailed analysis of attack scenarios and descriptions Implement recommended security architecture in IBR-DTN, an open source implementation of the 5050. We further provide a comprehensive evaluation in terms of benchmarking with other key and trust management protocols as well as simulation results.

1.2 1.2 Overview

The remainder of this article is structured as follows. Section 2 discusses related work in the field of locking and trust management in vehicle networks. THE The proposed concept of a parking community is introduced in Section 3. Parking community attack scenarios and their mitigation measures are presented in Section 4. Section 5 describes the implementation of the prototype in an overlay network based on IBR-DTN. We analyze the protocol based on existing solutions in Section 6, which can also be used to balance tradeoffs in the implementation of parking communities. We provide simulation results in Section 7. The article concludes in Part 8 that three pieces of information are information about color, texture and shape and achieve higher retrieval efficiency. The image and its offset are divided into non-overlapping cells of equal size.

II.LITERATURE SURVEY

[1] Discover and verify nearby locations in mobile ad hoc networks

An increasing number of ad hoc network protocols and location services require mobile nodes to learn the locations of neighboring nodes.However, such a process can easily be abused or interrupted by opposing nodes.

In the absence of a priori trusted nodes, detecting and verifying neighboring locations presents challenges that are little studied in the literature.In this paper, we address this open question by proposing a fully distributed cooperative solution that is robust against independent and colluding adversaries, and can only be weakened by overwhelming presence of competitors.

The results show that our protocol can prevent more than 99% of attacks under the best possible conditions for the adversary, with minimal false positive rate.

[2] Community pseudonymity privacy in wireless peer-to-peer networks

Wireless networks provide new ways to enhance social interaction.In particular, peer-to-peer wireless communications enable direct, real-time interaction with nearby devices and communities and can extend existing online social networks by providing complementary services.

additions, including real-time discovery of friends and communities and unsolicited sharing of localized data.After years of research, the implementation of such peer-to-peer wireless networks is finally being considered.

The basic primitive is the ability to discover the geographical proximity of specific human communities (e.g., friends or neighbors).To do this, mobile devices must exchange certain identifiers or community messages.We investigate the privacy threats posed by such communications, especially the detection of adversarial communities.

We use the general concept of community pseudonymity to depart from anonymous community identification mechanisms and define two distinct notions of community privacy using a challenge-response approach.Simulation results and in-depth cost analysis further shed light on the feasibility of these mechanisms in the next generation of wireless peer-to-peer networks.

[3] Security in inter-vehicle networks:

Why just changing the pseudonym is not enough

The inter-vehicle communication (IVC) system reveals rich location information about the vehicle.

Advanced security architectures are aware of the problem and provide privacy-enhancing mechanisms, including pseudonymous authentication. However, the level of detail and amount of location information revealed by the IVC protocol allows an adversary to listen to all traffic in an area to reconstruct a long trace of the location of the majority vehicles in the same area.Our analysis in this article confirms the existence of this type of threat.Therefore, it is questioned whether strong location privacy is possible in IVC systems against a strong adversary.

[4] Experimental comparison of the performance of DTN packet protocol implementation

In recent years, Delay Tolerant Networking (DTN) has attracted a lot of attention from the online community.Today, the Packet Protocol (RFC 5050) is the standard communication protocol in DTN and there are three main implementations.

Because DTN is still a young research field, the specifications and implementation have not yet reached the same level of maturity as DTN.TCP protocol stack.Currently, there is no quantitative analysis of the performance of different implementations nor any structured assessment of interoperability performed.

In this article, we demonstrate how to test interoperability and perform in-depth quantitative performance analysis of three major implementations of the Bundle protocol.Although the overall results show that all implementations provide some basic compatibility with each other, the stability and performance achieved under stress situations vary significantly between implementations.

declare.

[5] Remote timing attacks are practical

Timing attacks are often used to attack weak computational devices such as smart cards. We show that timing attacks apply to software systems in general.More precisely, we design a timing attack against OpenSSL.Our tests show that we can extract private keys from an OpenSSL-based web server running on a machine on the local network.Our results demonstrate that timing attacks against network hosts are realistic and therefore security systems should protect against them.

III.EXISTING SYSTEM

SQL injection

Malicious SQL statements can be injected into a vulnerable application using a variety of input mechanisms.In this section we explain the most common mechanisms.

1.Insert via user input:

In this case, the attacker injects SQL commands by providing properly crafted user input. A web application can read user input in many ways depending on the environment in which the application is deployed.In most SQLs targeting web applications, user input typically comes from form submissions sent to the web application via HTTP GET or POST requests. Web applications can typically access the user input contained in these requests the same way they access any other variable in the environment.

2.Cookie injection:

Cookies are files containing state information created by a web application and stored on the client computer.When the customer returns to the web application, cookies can be used to restore the customer's state information.Because the client controls cookie storage, a malicious client can tamper with the cookie's

contents.If a web application uses the contents of a cookie to create SQL queries, an attacker can easily launch an attack by embedding it in the cookie.

3.Inject via server variable:

Server variables are a collection of variables containing HTTP, network headers, and environment variables.Web applications use these server variables in a variety of ways, such as recording usage statistics and identifying browsing trends.

If these variables are saved to the database without being cleaned up, it can create a SQL injection vulnerability.

Because attackers can spoof the values set in HTTP and network headers, they could exploit this vulnerability by placing SQLIA directly in the header.When a server rheology request is sent to the database, a forged header attack is triggered.

Second injection:

In the second injection, the attacker injects malicious input into the system or database to indirectly trigger SQLIA when that input is used later.The goal of this type of attack is significantly different from the classic (i.e.first order) injection attack.

IV.PROPOSED SYSTEM

Practice defensive coding:

The root cause of the SQL injection vulnerability is inadequate input validation.Therefore, the simple solution to eliminate these vulnerabilities is to apply appropriate defensive encryption methods.Here we summarize some of the best practices recommended in the literature to prevent SQL injection vulnerabilities.

1.Check input type:

SQL can be executed by passing commands into a string or numeric parameter.Even a simple check of these items can prevent many attacks.For example, in the case of numeric input, the developer can simply reject any input that contains non-numeric characters.Many developers unintentionally ignore this type of checking because user input is almost always represented as a string, regardless of its content or intended use.

2.Input encoding:

Insertion of a string parameter is typically achieved through the use of metacharacters that trick the SQL parser into interpreting the user input as SQL tokens.

Although it is possible to prohibit all use of these supercharacters, doing so limits the ability of non-malicious users to specify legitimate input containing such characters.A better solution is to use string encoding functions in such a way that all meta characters are specially encoded and interpreted by the database as normal characters.

3.Positive pattern matching:

Developers must set up an input validation process to identify good and bad inputs.This approach is often called positive validation, as opposed to negative validation, which looks for forbidden patterns or SQL

tokens as input.Since developers may not be able to consider all types of attacks that can be performed against their applications but can specify all types of legitimate inputs, positive authentication is a safe way to safer to verify entries.

4.Identify all input sources:

Developers must verify all inputs in their applications.As we have pointed out, there are many sources contributing to an application.If used to build a query, these input sources could be a way for an attacker to inject SQL code.Simply put, all input sources must be verified.

List of attacks:

This attack uses the web to allow customers to view their account details and pay their bills online.They use social security numbers as usernames and four-digit ATM PINs as secret passwords.This type of password enumeration protection works well for client-server applications.However, on the web, an attack can be created where a hacker can write a script that uses one social security number after another and simply tries pinning for each security number.

If hackers used the social security numbers of people living in the banking area (and common passwords like "123456" or "PASSWORD"), the script could get at least one account within a few hour; In a few days, hackers will get the accounts of all the bank's customers.

This is an example of an enumeration attack.This attack uses several users using the system; Some applications in the world today have millions of customers (eBay, Yahoo, PayPal).In some cases, the username is known or easy to guess and the password has low entropy, meaning there are relatively few possible combinations.To address this, the app could be redesigned to monitor access to the login page and, when this access is unusually high, penalize users by extending the response time for everyone .Additionally, an external device such as an application firewall can monitor this information and detect any unusual behavior.

V.MODULE DESCRIPTION

I.Membership module

When a user accesses the application by logging in.

The login module allows users to enter a username and password to log in.This module can be placed on any module tab to allow users to log into the application.If the administrator has allowed users to create accounts, a Create account link will appear in the login module.This module also allows you to change the password.In this page we access the number of visitors.The visitor count is automatically generated each time you visit this page.

ii.Payment module

Secure payment gateway services include a full range of payment processing features and functionality to meet all the processing needs of e-commerce businesses and brick-and-mortar businesses looking for processing services pay.An operating subsidiary of Pipeline Data Corporation, Secure Pay today supports thousands of merchants across the country with a variety of payment processing solutions – both standard and customized to the merchant's needs.Secure Pay provides streamlined, functional and affordable e-commerce solutions for any small to medium sized business.

iii.WASP module

During the Anti-injection process, hackers cannot access the website because it is a completely protected process.This process increases security, and reliance on filtering rules requires dangerous assumptions.Syntax-aware evaluation techniques can be used just before the query is sent to the database.
To protect against SQL injection, user input must not be embedded directly into the SQL statement.
Instead, parameterized statements should be used (best) or user input should be carefully escaped or filtered.It cannot insert, update, delete from the database.

iv.QR Code Generator

QR code (abbreviated from Quick Response Code) is the trademark of a type of matrix barcode (or two-dimensional barcode).A barcode is a machine-readable optical label that contains information about the user credentials attached to it.QR codes use four standardized encoding modes (numeric, alphanumeric, byte/binary, and kanji) to store data efficiently; extensions can also be used.

v.QR code scanner

When a user can add their information in the registration form, that information will also be encoded in the QR Code in encrypted form, so if an intruder tries to modify the user's information in the QR, users will not be able to do this in a QR Code because they do not know the encryption key.The user information can then be retrieved from the QR code and can be decoded using the QR Reader decoding algorithm, which can then be verified using the user information already in the QR.

vi. Space manager

Locations will be calculated each day and with each booking.Bookings will be based on available locations.Daily reports will be generated based on this module.

vii.Administration

This module controls all other modules and users.
Administrators have the right to add or remove any end users.
Using this module, admins can easily update new modules.This module maintains the flow of user navigational control across the entire website.This module performs security functions.Thanks to this, unauthorized users cannot access the website.Website hacking is easily protected by this module.

VII.CONCLUSION

In this paper, Parking Communities have been presented.They provide a novel trust management for vehicular parking applications without reliance on a central TTP for retrieving trust ratings. For this purpose, vehicles create communities, trusted groups
helping their members to find parking in their respective community area. Trust anchors enable signed and encrypted request-response communication in disrupted environments. As our approach can be used as an overlay to existing vehicular networking technologies,it can directly benefit from established security mechanisms, e.g., pseudonym certificates. Our approach is based on high-performance state-of-the art encryption and signature algorithms, in particular ECC, as well as a well-understood mathematical trust rating model. Attack scenarios and their mitigations are discussed. Without requiring a TTP, our scheme provides protection against impersonation and Sybil attacks utilizing trust anchors and physical verification.

The underlying security architecture of Parking Communities has been implemented in the open source IBR-DTN, which is publicly available. We provide a comprehensive comparison with existing key and trust management schemes for vehicular networks, as well as simulations showing the concept's feasibility.

REFERENCES

1. Car 2 Car Common Consortium. Manifesto: Overview of the C2C-CC system, V1. 1. Tech. rep. Aug. 2007.
2. Federal Highway Administration. Advanced Parking Management Systems: A Cross-cutting Study: Taking the Stress out of Parking. Intelligent Transportation Systems, U.S. Department of Transportation, 2017.
3. Wireless Access in Vehicular Environments (WAVE)– Security Services for App. and Manag. Messages (IEEE Std 1609.2-2006). IEEE. July 2016, pp. 1–105.
4. S. Schildt, J. Morgenroth, W.-B. P¨ ottner, and L.Wolf. "IBR-DTN: A lightweight, modular and highlyportable Bundle Protocol implementation". In: ElectronicCommunications of the EASST 37 (Jan. 2017).
5. K. Scott and S. Burleigh. Bundle Protocol Specification.RFC 5050. IETF, Nov. 2017.