Acyclica White Paper:
RoadTrend does not Capture PII

Submitted to:
Daniel Benhammou
President, CEO
Acyclica
PO Box 4062
Frisco, CO 80443
(303)859-4216
djb@acyclica.com

Submitted by:
Collette Thepenier
IT Security Consultant
Coalfire Systems, Inc.
11000 Westmoor Circle
Suite 450
Westminster, Colorado 80021
(303)554.6333 x7051
cthepenier@coalfire.com

Date
December 18, 2015

Confidentiality Notice:
This document contains confidential information relating to Client Name. It is provided for the sole use of Client Name and is not for public distribution.

Table of Contents

Intro

Acyclica is the leading provider of high resolution, real-time traffic congestion information. They are the fastest growing ITS company providing congestion management solutions. Its suite of traffic analytics software and sensor devices are currently being used by over 50 agencies both domestic and international to help to monitor and improve traffic congestion. Acyclica works with cities, municipalities and Departments of Transportation to aggregate and analyze data to bridge gaps in traditional traffic data services. Acyclica also provides data to organizations and businesses in need of relevant travel information services ranging from origin and destination information to travel-times.

Based on the data Acyclica captures, their customers/client then have information that can be provided to travelers and traffic engineers, such as a calculated average speed for different monitored roadway segments, duration of traffic/turn signals, and average progress time along different monitored roadway segments, representative of travel and stop time and delays. This then allows traffic engineers to correct traffic signal length, set sensors and traffic lights to be shorter/longer, and provide information to travelers about traffic signals or other pertinent information around delays.

Applications of Acyclica technology include: Signal Timing & Coordination, Traffic network optimization, Street parking congestion analysis, Congestion mapping, Route planning, Workzone congestion enforcement, Variable message signs, Incident Detection, Emergency responder routing and Route Utilization.

Acyclica technology anonymously collects media access control (MAC) address information and send the data to the cloud using WiFi technology through the use of their RoadTrend Sensor. This sensor is a proprietary Linux-based device that is discreetly installed inside of traffic control cabinets for their clients/customers. The devices are Ethernet connected and have a WiFi adapter capturing the MAC addresses of all devices within its range. Based upon the design and configuration, Acyclica believes that they are able to be exponentially more accurate, capturing several hundred times more data than normal mobile apps or traffic pattern analyzers.

Commented [D1]: Wifi is not used for communication. All communication is over wired networks with data transmission either over encrypted cellular networks or a hard line.

Using WiFi detection of MAC addresses, Acyclica is able to identify and differentiate vehicle movement as it approaches, stops and leaves an intersection. From the aggregated data, Acyclica is able to extract and provide actionable information to their clients/customers to make informed choices on the traffic service enhancements and resolution of traveler challenges.

Summary/Intended Message

Acyclica technology anonymously collects media access control (MAC) address information and send the data to the cloud using WiFi technology through the use of their RoadTrend Sensor. Using WiFi detection of MAC addresses, Acyclica is able to identify and differentiate vehicle movement as it approaches, stops and leaves an intersection.

MAC address is a media access control address which uniquely identifies a device connected to a network. MAC addresses are usually assigned by a manufacturer and the information is hard-coded to the device and stored in its hardware. MAC addresses are independent of device ownership such that there is no immediate connection to the device owner/user. A MAC address thus does not represent any personally identifiable information (PII). If device ownership changes, the device MAC address remains unchanged. Within the product and services provided by Acyclica, the applicable device is a mobile device. The only way to connect a MAC address to the mobile device owner/user is to work with a mobile carrier to associate the MAC address to an active mobile phone number listed on mobile customer's account. In this case, the PII resides with the mobile carrier who maintains the details of a mobile customer's account.

Even though this information is not PII, since it not inherently tied to an individual mobile device owner/user, Acyclica still does protect the data using encryption technology embedded within proprietary code that secures the non-PII MAC address at the device prior to transmission to the Acyclica's backend infrastructure for analysis. Other methods of securing the non PII data include specific design and configuration of the backend infrastructure components, as well as industry standard security practices for access controls and logging/monitoring and alerting.

Acyclica's clients/customers are agencies both domestic and international, including cities, municipalities and Departments of Transportation. Depending upon the contracted service(s), these clients/customers may have access to the aggregated data through a web portal. Since no PII is captured, there is no PII shared with Acyclica's clients/customers through this portal. However, Acyclica still does protect the data using encryption technology for data encryption across the internet providing an encrypted web portal using a third party encryption certificate.

Question/Concern

What information does Acyclica collect? Is this information PII?

Mobile device MAC address data is collected by Acyclica for their analytics, however there is no PII captured that could identify an individual mobile device owner/user, such as name or mobile device number. The captured MAC address cannot be tied to an individual mobile device owner/user unless done so by the mobile carrier, which is outside of the purview of Acyclica.

Mobile device MAC address data collected by Acyclica and provided to their customers/clients is very minimal, and includes only a hashed value of the MAC address (never a full, unhashed version), in addition to timestamp, strength (of signal) and serial number (of sensor device). This information is provided to the customer/client by way of an access controlled web portal, which can also permit an export to csv. And API is also made available for customers/clients to integrate the data into digital signage for real-time communication to travelers in determined areas.

Why is it important to protect the non-PII data that is collected?

While not PII, if data from a mobile carrier were to be made available, by means either accidental or nefarious, a third party may be able to correlate the data and use the analysis to track the movements and activities of the mobile device owner/user. In these cases, the movements and activities of the mobile device owner/user could reveal addresses of personal residence or workplace, as well as those dates and times when the mobile device owner/user was regularly present or absent at either location. The likelihood of this occurrence can vary and there are many other variables that contribute to the overall level of risk.

How does Acyclica secure the collected non-PII data?

Regardless of risk likelihood and level, Acyclica employs industry-standard measures to secure the data itself as it is captured at the device, retained in the backend infrastructure components and made available to the customer/client, as well as during data transmission from the device to the backend infrastructure components and the presentation of the data in a web portal. Acyclica ensures also that there are configuration standards and industry-accepted hardening criteria incorporated into the design and implementation of their sensor devices and backend infrastructure components, as well security practices that enforce strong access controls, configuration management procedures and methods of being aware of the state of the systems at all times.

Specifically, the following security measures are in place to secure the non-PII MAC address:

1. Limited data capture of MAC address
    - The intended design of the sensor devices limits the collection of MAC address data based upon the signal strength that is broadcasted to the WiFi antenna within the designated traffic cabinets range (500-700 feet). This means that there is a focused effort to only capture data within the predetermined range which will provide the most relevant data.

2. Encryption technology at device prior to transmission
    - Acyclica has created proprietary code that incorporates encryption technology using industry standard algorithm and cipher strengths, as well as inclusion of the use of a cryptographic hash function with a generated salt value. A cryptographic hash function is a way to easily validate that a string of data corresponds to a specific hash value. If the original data string is unknown, but the stored hash value is known, by design, the cryptographic hash function makes it challenging to recreate the original data string. Utilization of hash function is intended to assure the integrity of data in transmission. In cryptography, a salt is random piece of data that is used, in addition to a string of data, in the creation of a hash value through use of a hash function.
    - The primary function of salts is to prevent retro calculation of the hashed value if the hash function is known. Use of a salt precludes the effectiveness of using a list of possible pre-computed values since the salt is randomly generated. With Acyclica's proprietary technology solutions, the salt rotates every 24 hours on the actual sensor device. The salt value is determined by timestamp which enables the hash to be dynamic. This encryption methodology is in sync with industry standard protocols. Additionally, there is proprietary code that is running on the sensor device that performs the encryption function. The proprietary nature of the code strengthens to nature of the encryption methodology. The methodology of transmission to the cloud is a direct post to the back end systems, versus an HTTPS transmission or broadcast over open, public networks which is considered less secure.

3. Secure transmission to Acyclica's backend environment –
    - Acyclica avoids the use of HTTPS transmission or broadcast of data over open, public networks.

4. Encryption technology in the backend environment –
    - [More information is needed here if it is to be included]

5. Database schema design and repository in AWS environment –
   - Information such as address, name, race and gender is not captured, only MAC address. All other data capture corresponds to needed data which would be publically available and which is relevant specifically for traffic analysis.

6. Secure presentation to customers/clients in an encrypted (HTTPS) web portal –
   - The web portal (https://cr.acyclica.com) uses industry-accepted encryption by way of a third-party certificate.

7. Secure configuration and hardening of device –
   - Acyclica uses of a pared down proprietary Linux installation with a specific embedded processor, chosen for processing optimization. Minimal storage is available on this device to enable only intended functionality and to also limit data retained. Additionally, there are specific access controls set to ensure restricted logical access to the device.

8. Secure configuration and hardening of backend infrastructure –
   - [Unsure of how much technical information is appropriate here if it is to be included]

9. Industry standard security practices –
   - Acyclica employs logical access controls to ensure minimally assigned access and privileges, based upon a need-to-know. Vulnerability of systems are managed with patch procedures and change management processes, and logs are captured and monitored for maximum security awareness of the state of the devices and systems

10. Security language built into the contractual agreement with customers/clients –
    - Acyclica has built specific security language into their contracts to clearly delineate the responsibilities between Acyclica and the customer/client for security of data and associated regulatory requirements.

Validation

In order to validate the design and operational effectiveness of Acyclica's security program which protects the non PII MAC address data that it collects for analysis, Coalfire reviewed Acyclica's proprietary encryption code, as well as their documented processes. Additionally, configuration settings were validated with demonstrations and real-time observations with administrate personnel. Coalfire also investigated data repositories to look for any PII, as well as validate that the non PII that is captured is appropriately secured when made available to the customer/client.

Results

Based upon the results of the evaluation efforts, Coalfire was able to confirm the operation effectiveness of Acyclica's device and systems design such that there is no PII retained in any data repository, nor is the non PII MAC address ever presented to customer/clients in an unencrypted, unhashed format. Design effectiveness was confirmed with review, observation and interviews of configuration and code implementation with administrative personnel. Documented processes were also validated as effectively designed and operational as demonstrated by supporting evidence assessed during review of data repositories and device and system configurations.

Conclusion

Acyclica sensor device technology anonymously collects media access control (MAC) addresses data from mobile devices through the use of a WifF connection on their RoadTrend Sensor. The sensor detects the MAC address on mobile devices within a specific broadcast range of signal strength. With this proprietary device, Acyclica is able to be more accurate, capturing significantly more data than traditional mobile apps or traffic pattern analyzers.

Since MAC addresses are hard-coded to a mobile device, they are independent of device ownership such that if device ownership changes, the MAC address on that device remains unchanged. This solution design thus precludes any direct connection to the device owner and cannot indicate any personally identifiable information (PII). The only way to connect a MAC address to a mobile device owner/user is to work with the associated mobile carrier to associate the MAC address to an active mobile phone number listed on mobile customer's account. In this case, the PII resides with the mobile carrier who maintains the details of a mobile customer's account.

This methodology of data collection for vehicle movement is a more secure alternative to the traditional capture of license plate information. Capture of this information can reliably identify the identity of the driver based upon associated vehicle registration information. As a result, license plate data should be considered PII. While this information may not be immediately available to the general public, whomever has access to the data has the ability to retroactively connect the license plate directly to the registered owner of the vehicle.

Even though MAC address data is not PII, if account data from a mobile carrier were to be made available, by means either accidental or nefarious, a third party may be able to correlate the data and use the analysis to track the movements and activities of the mobile device owner/user. In these cases, the movements and activities of the mobile device owner/user could reveal addresses of personal residence or workplace, as well as those dates and times when the mobile device owner/user was regularly present or absent at either location. The likelihood of this occurrence can vary and there are other variables that outside Acyclica that would contribute to the overall level of risk.

Regardless of risk likelihood and level, Acyclica takes active steps to employ industry-standard security measures to protect the non-PII MAC address data itself as it is captured at the device and retained in the backend infrastructure components using a proprietary encryption and hashing methodology. Acyclica also secures both their front end sensor devices, as well as their back end supporting infrastructure components with specific design parameters. Also, the presentation of the data to the customer/client is intentionally pared back to preclude the availability of unhashed, unencrypted MAC address data; instead only the encrypted and hasted data is made available and only through a secure web portal. Finally, Acyclica has incorporated industry standard security practices that enforce strong access controls, configuration management procedures and methods of being aware of the state of the systems at all times.

This comprehensive approach to securing non PII MAC address data was evaluated by Coalfire through review of code and documented processes, as well as validation of configuration settings and investigation retained data. Through this evaluation, Coalfire was able to confidently conclude that PII data is not captured, nor retained and the intended security measures implemented to secure the non PII MAC address data were in place and operating as intended.