David Colombo Follow
Jan 24 · 22 min read · Listen

Save

How I got access to 25+ Tesla's around the world. By accident. And curiosity.

David Colombo.

My journey into cyber security:

- Started programming at the age of 10
- Got into cyber security at the age of 13
- Dropped out of school at the age of 15
  I asked myself, "Why should I sit here and learn Latin or do poem analysis if I could be out there and protecting critical infrastructure?"
- Started own company at the age of 17
- Published globally recognized cyber security research at age 19
  As seen on Bloomberg, TechCrunch, CNN and more
- Invited speaker and thought leader at the World Government Summit
-

In short: It's my passion

Cyber Security is one of the most pressing challenges of tomorrow and a key threat to a fully digitalized future. For me personally it isn't just a job, but my passion.

Topics in this talk:

We will take a look at three main topics including how I managed to hack multiple Teslas, how the automotive ecosystem is changing and why cyber security in mobility will be one of the most pressing challenges of tomorrow.

How to hack Teslas

- What I was able to do
- The vulnerability behind it
- The vulnerability reporting process
- The key learnings from the experience

Why the Automotive Eco-system needs to be secure

- How the automotive attack surfaces are expanding
- Why the holistic approach to security is important

Cyber Security in Mobility

One of the most pressing challenges of tomorrow

- Outlook into the future of mobility cyber security
- What is needed to ensure a secure future

How to hack Teslas:

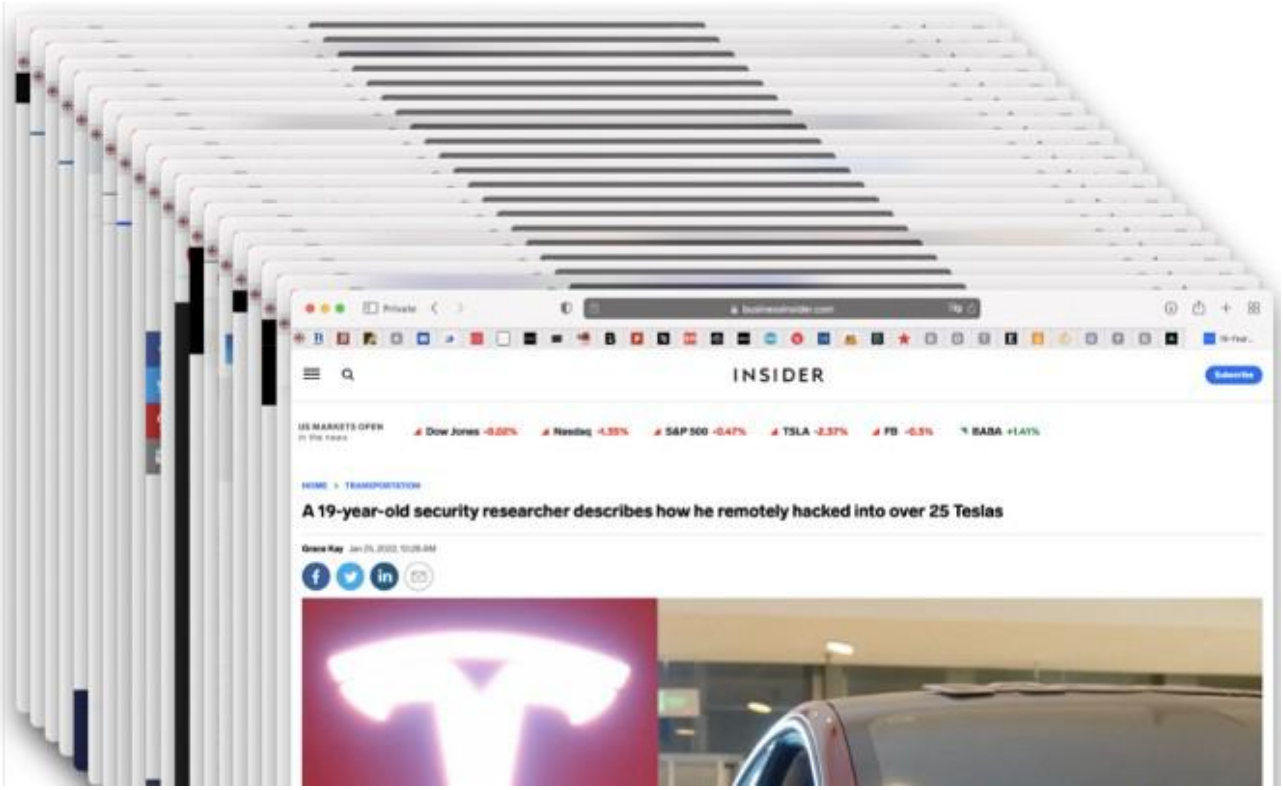
Let's deep dive into how I managed to hack into 25+ Teslas all around the world through a critical vulnerability in a third-party application.

Talking Points Include:

- (Third Party) Applications for Modern Vehicles
- API Security
- Responsible Disclosure
- Critical Vehicle Features Hacked

4

David Colombo



5

What features I was able to control:

I had full control over multiple vehicle features, including critical ones (marked with *).

Querying accurate vehicle location*	Turning off Sentry Mode*	Unlocking / Locking the vehicle doors*	Starting Keyless Driving*
Flashing the lights*	Controlling certain infotainment features	Controlling temperature settings	A lot more...

6

David Colombo

How did this happen? By accident. And curiosity.

Port Scan results of interesting backup. domain

```
Screen Shot Port Scan
Not shown: 996 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
4000/tcp open  remoteanything
5555/tcp open  freeciv

Nmap done: 1 IP address (1 host up) scanned in 4.16 seconds
david@Tuxedo-DX1507:~$
```

Basic enumeration steps of infrastructure environment	1

7

How did this happen? By accident. And curiosity.

Port Scan results of interesting backup. domain

```
Not shown: 996 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
4000/tcp open  remoteanything
5555/tcp open  freeciv

Nmap done: 1 IP address (1 host up) scanned in 4.16 seconds
david@Tuxedo-DX1507:~$
```

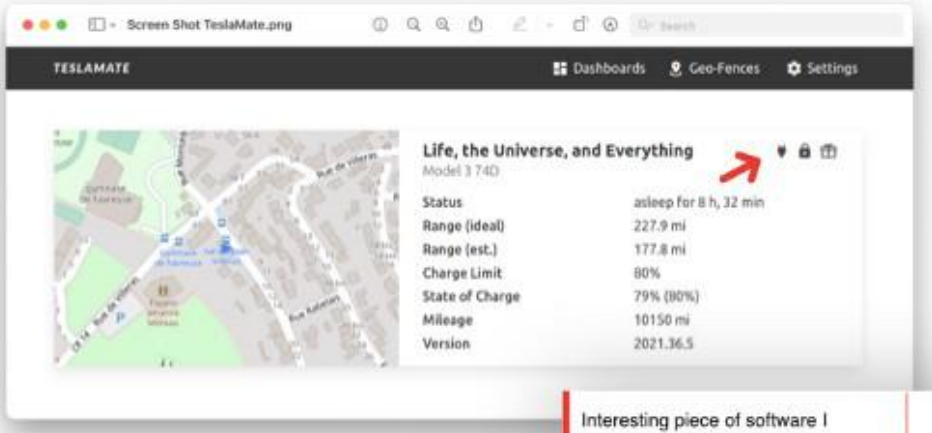
Failed try to connect via telnet

```
david@Tuxedo-DX1507:~$ telnet backup.
Trying
Connected to backup.
Escape character is '^]'.
Connection closed by foreign host.
david@Tuxedo-DX1507:~$
```

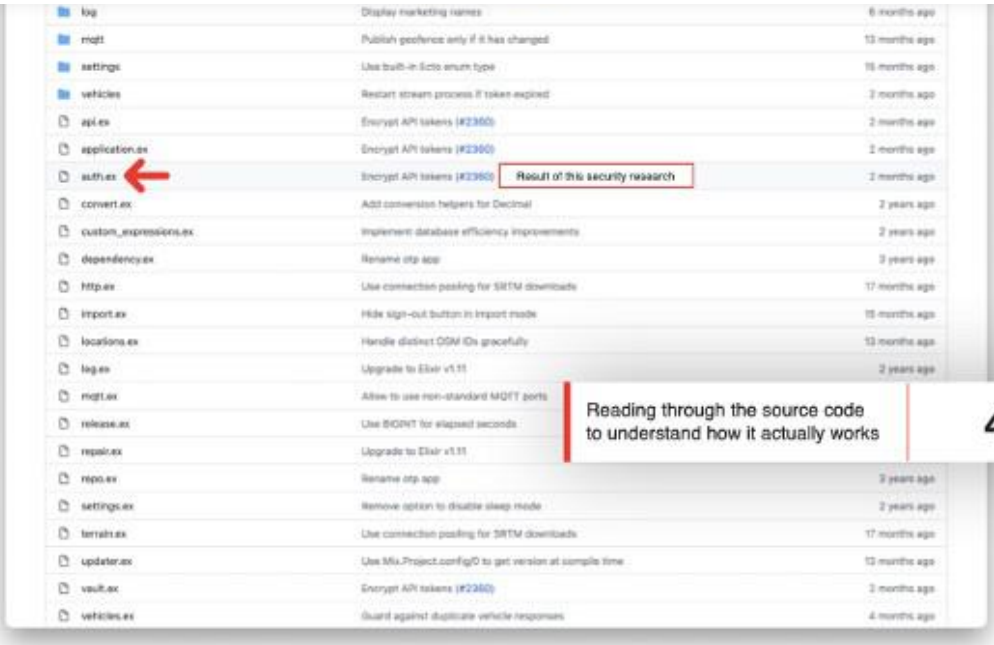
Basic enumeration steps of infrastructure environment	1	→ Figuring out what services and applications are running	2

David Colombo

How did this happen? By accident. And curiosity.



Interesting piece of software I wanted to learn more about	3	

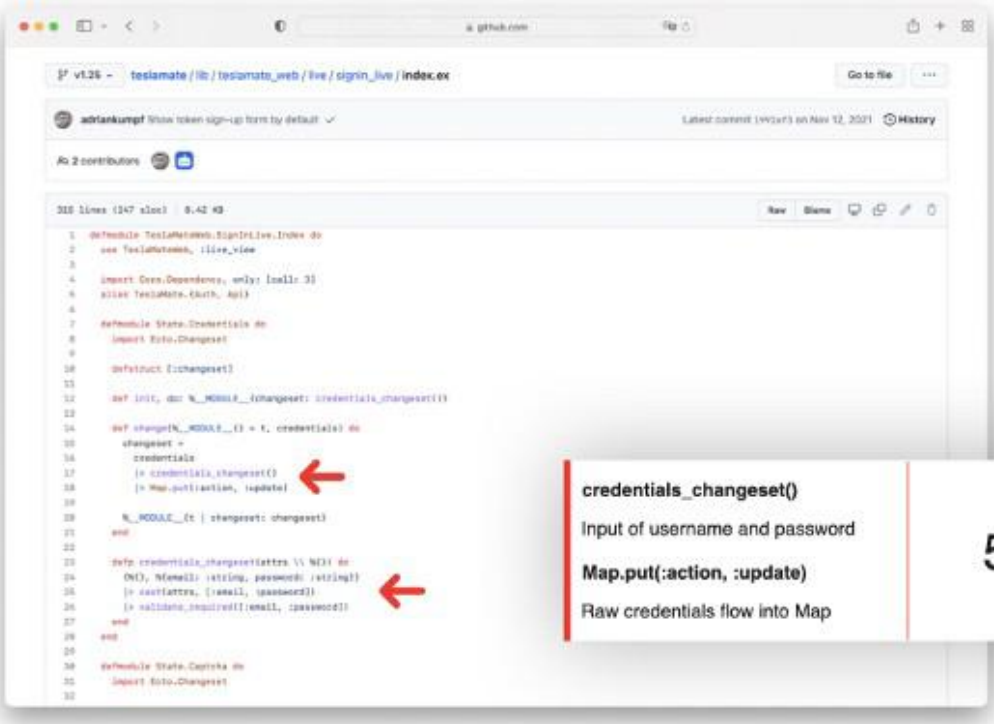


Reading through the source code to understand how it actually works

4

10

David Colombo



```
credentials_changeset()
Input of username and password
Map.put(:action, :update)
Raw credentials flow into Map
```

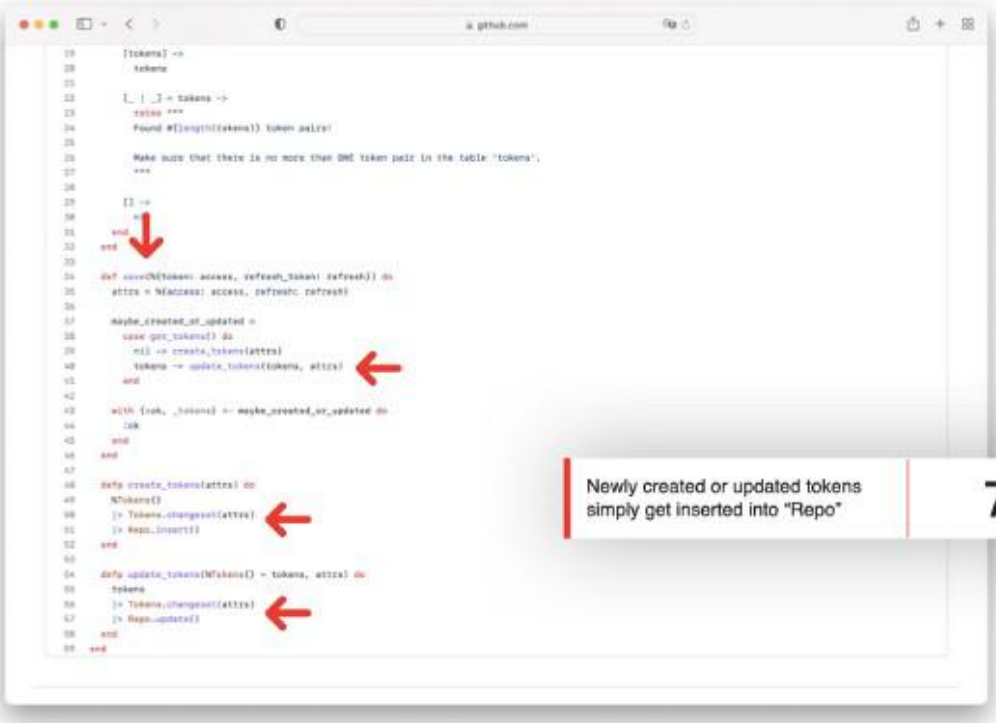
5

11

Sign in with credentials in exchange for token 6

12

David Colombo



Newly created or updated tokens simply get inserted into "Repo" 7

13

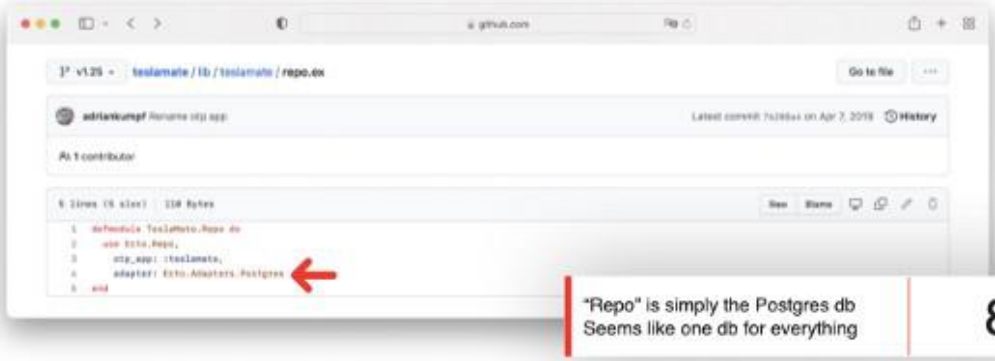
Tokens get inserted into "Repo" without encryption

The software exchanges the credentials for API tokens and then stores those tokens in "Repo" without ever encrypting them. I originally thought, if that's the case then "Repo" itself must be some kind of secure storage method that takes care of encryption.

What did we discover so far?

14

David Colombo



"Repo" is simply the Postgres db
Seems like one db for everything

8

15

Tokens get inserted into "Repo" without encryption

The software exchanges the credentials for API tokens and then stores those tokens in "Repo" without ever encrypting them. I originally thought, if that's the case then "Repo" itself must be some kind of secure storage method that takes care of encryption.

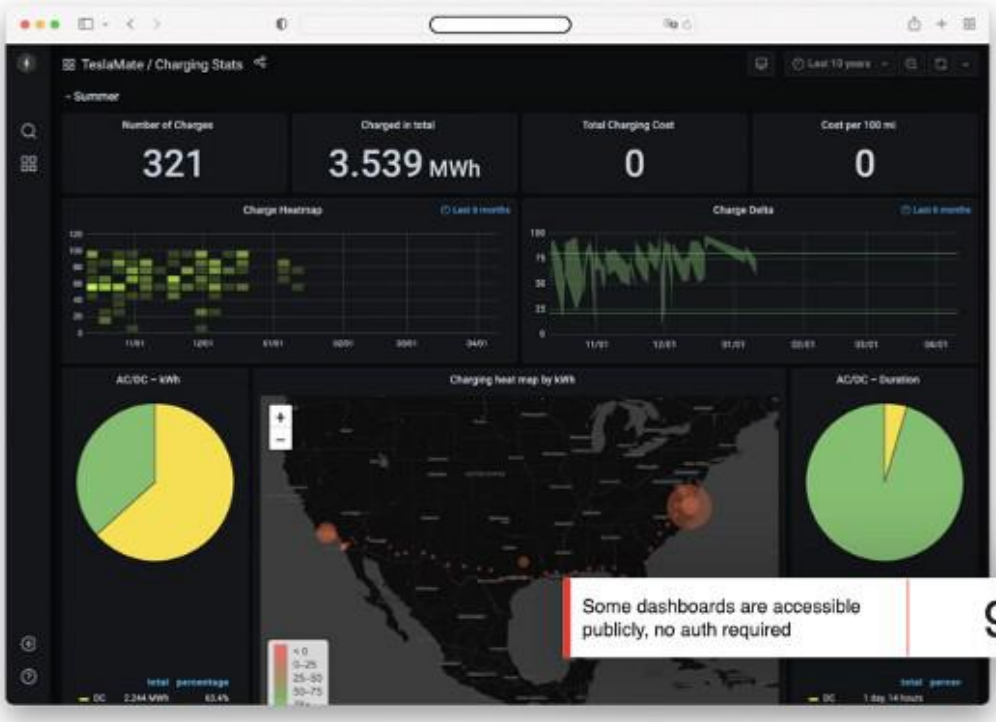
What did we discover so far?

Tokens get stored next to all other data in the database

As it turns out "Repo" is simply the connector to a normal Postgres database stored on the system. Since the Postgres database is the default storage location for all collected data, then the sensitive Tokens simply get stored in a table next to all other data.

16

David Colombo



17

What did we discover so far?

Tokens get inserted into "Repo" without encryption

The software exchanges the credentials for API tokens and then stores those tokens in "Repo" without ever encrypting them. I originally thought, if that's the case then "Repo" itself must be some kind of secure storage method that takes care of encryption.

Tokens get stored next to all other data in the database

As it turns out "Repo" is simply the connector to a normal Postgres database stored on the system. Since the Postgres database is the default storage location for all collected data, then the sensitive Tokens simply get stored in a table next to all other data.

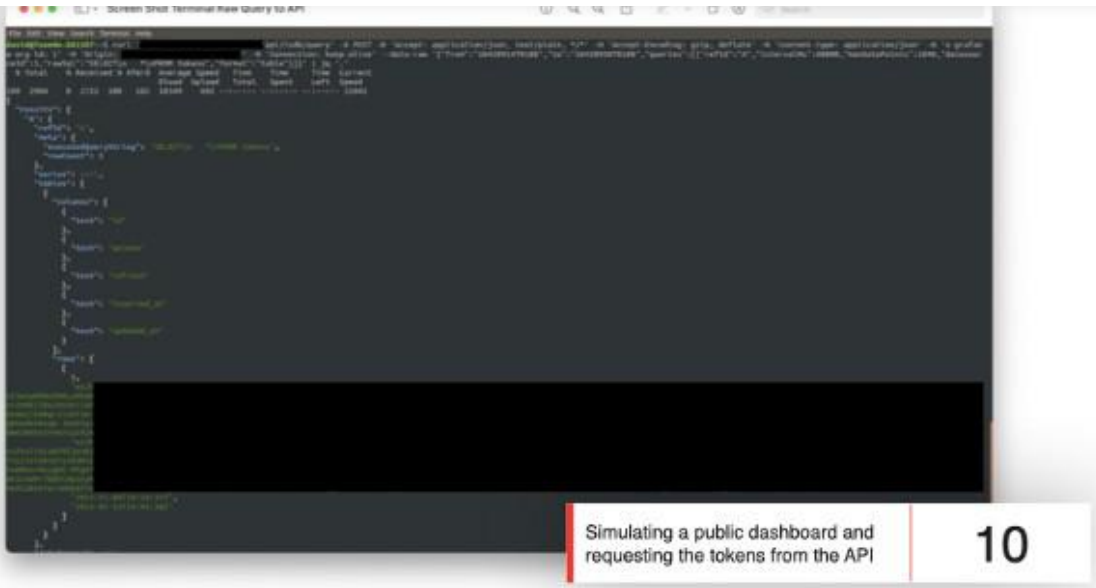
Certain data dashboards are accessible publicly

If you investigate what happens with the vehicle data stored in the database then you will find dashboards, such as the ones with charging statistics, that are accessible without auth. In short, you can access some data in the database publicly through that.

David Colombo

What if I could tell the API I'm a public dashboard and bring it to read me the tokens?

Let's just try it →



Simulating a public dashboard and requesting the tokens from the API 10

20

David Colombo

Tesla API Tokens = Digital Car Keys

the keys to the kingdom

with extended remote control functionality

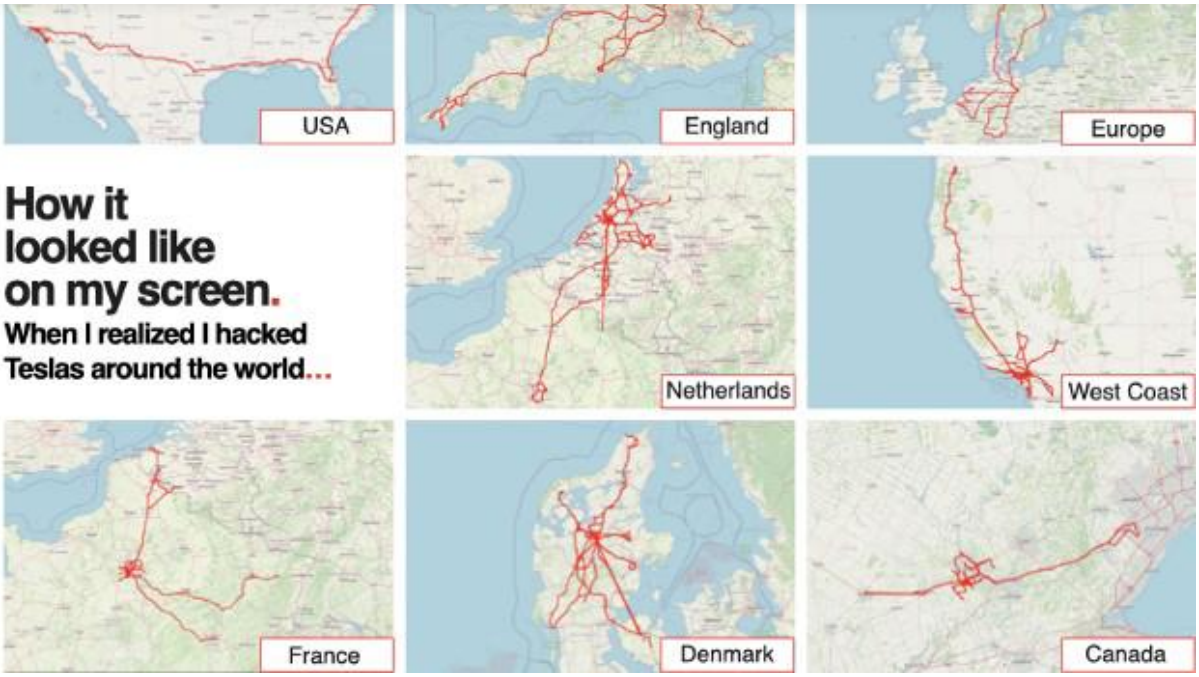
Querying accurate vehicle location*

Turning off Sentry Mode*

Unlocking / Locking the vehicle doors*

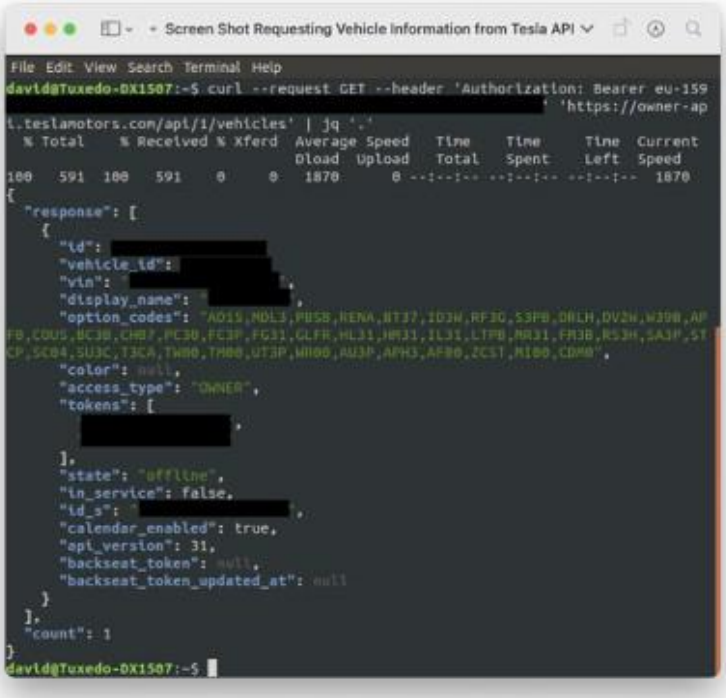
Starting Keyless Driving*

21

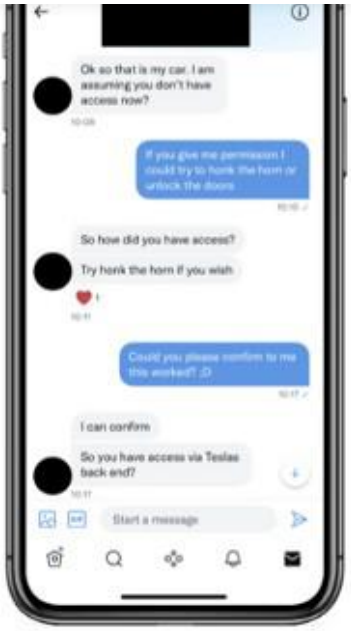


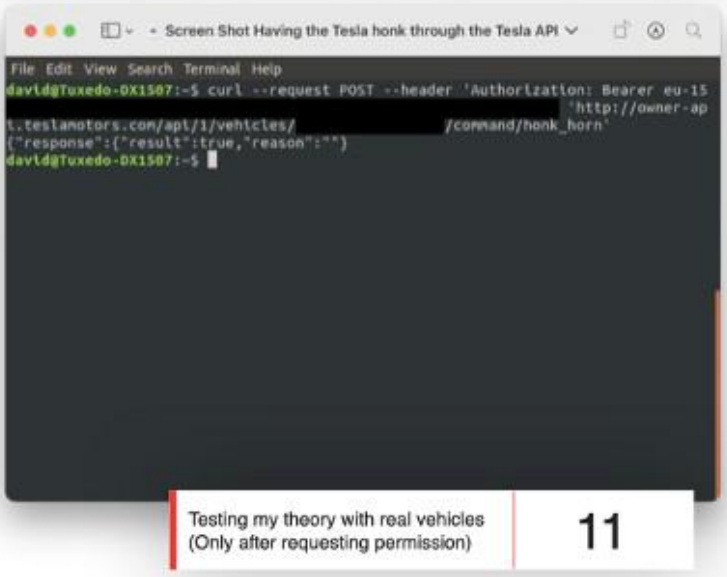
22

David Colombo



23





24

David Colombo

Vulnerability Disclosure Process

Third-Party Developer Directly

Sent my report and the all the vulnerability details directly to the developer in order to get the critical vulnerability patched as soon as possible.

Tesla Product Security Team

Talked with the Tesla Security Team in order to notify affected owners and revoke any access to Teslas that might be affected.

Affected Owners & Media

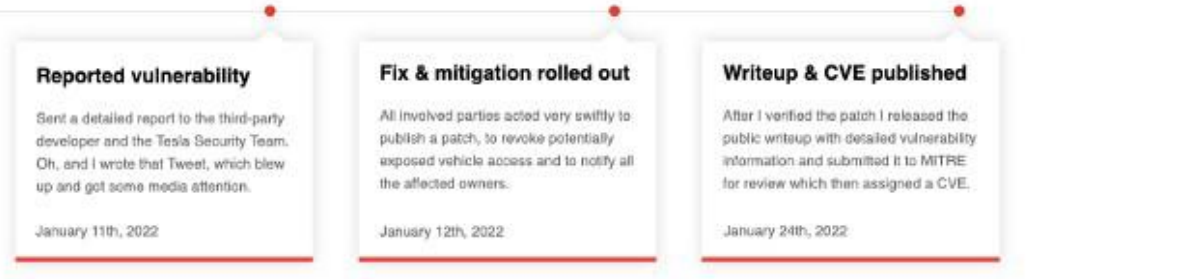
The public response and media interest to the initial announcement of the findings was massive and I tried to handle this as efficient as possible through the process.

25

Vulnerability Research and Disclosure Timeline.

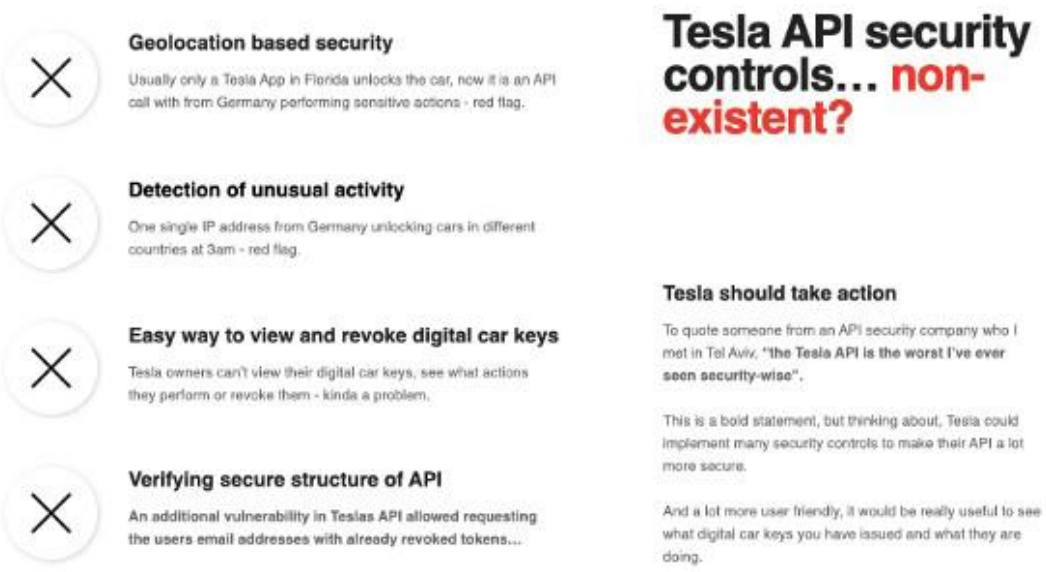
David Colombo

Vulnerability Research and Disclosure Timeline.



28

David Colombo



29

30

Key Learnings for me

About Automotive Cyber Security

You don't have to hack a car to hack a car

The future **ecosystem** will be one of the main attack vectors when it comes to automotive security.

Security research is becoming more important

Especially in automotive. If we don't find vulnerabilities in the vehicles of tomorrow, threat actors will.

There are substantial entry-level barriers

It, unfortunately, is really hard to get into automotive security research, since you need substantial resources aka a car.

David Colombo

31

Key Learnings for me

About Automotive Cyber Security

You don't have to hack a car to hack a car

The future **ecosystem** will be one of the main attack vectors when it comes to automotive security.

Security research is becoming more important

Especially in automotive. If we don't find vulnerabilities in the vehicles of tomorrow, threat actors will.

There are substantial entry-level barriers

It, unfortunately, is really hard to get into automotive security research, since you need substantial resources aka a car.

Key Learnings for me

About Automotive Cyber Security

You don't have to hack a car to hack a car

The future **ecosystem** will be one of the main attack vectors when it comes to automotive security.

Security research is becoming more important

Especially in automotive. If we don't find vulnerabilities in the vehicles of tomorrow, threat actors will.

There are substantial entry-level barriers

It, unfortunately, is really hard to get into automotive security research, since you need substantial resources aka a car.

32

David Colombo

33

Why the Automotive Ecosystem needs to be secure:

The automotive landscape is changing very fast, so is the automotive ecosystem. We have to keep an eye on the increasing attack surfaces.

Talking Points Include:

Increasing Attack Surface

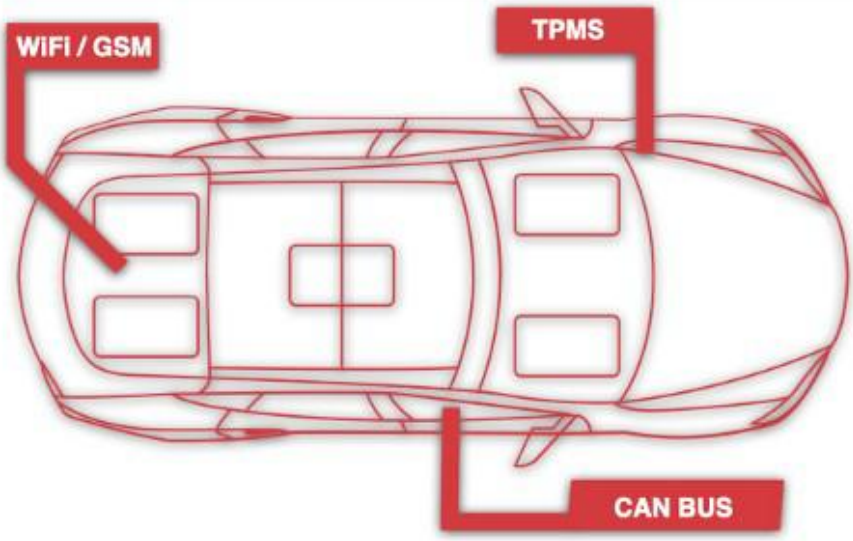
Dangers of the Automotive Ecosystem

34

David Colombo

80 years ago, no digital technology involved.

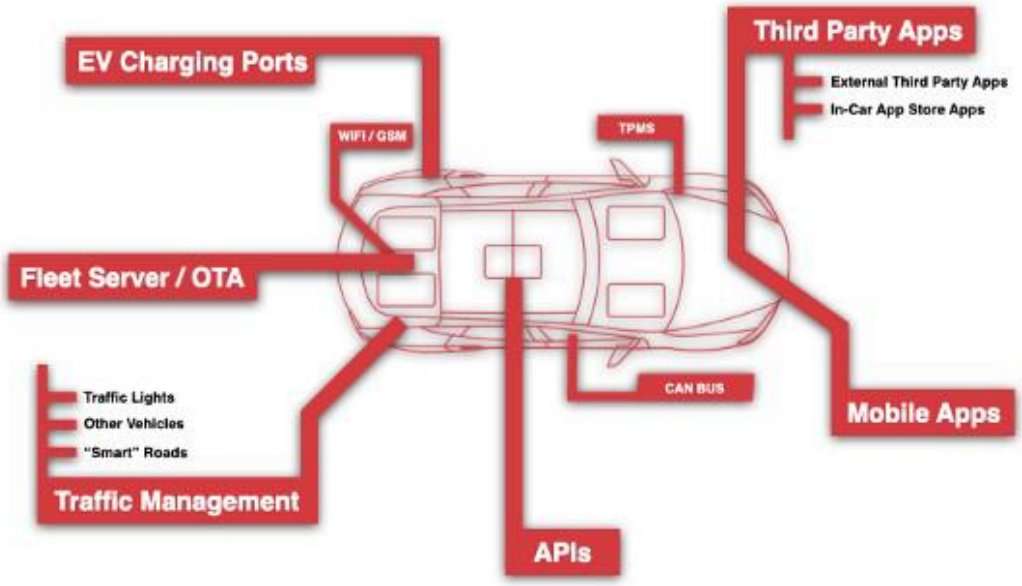
35



36

David Colombo

Future attack surface.



37

38

David Colombo

The risks of automotive cyber attacks in 2022

There is a wide range of critical risks

Malicious cyber attacks on vehicles and/or the automotive ecosystem can have disastrous outcomes affecting not just the public image of automakers and OEMs, but also having direct impact on human lives, infrastructure and other physical aspects.

A fleet hacked by a threat actor with malicious intent would be a worst-case scenario which should be avoided at all costs.

Luckily hacks like this only have been demonstrated by security researchers, but it shows that this is already technically possible.

Vehicles can have physical impact on human lives

Cyber Security for vehicles is not a nice to have but an absolute must have

39

Ever thought about a **hacked government motorcade?**

What if a threat actor such as an international terrorist organization gains the capability to hack the vehicles in a government motorcade transporting VIPs ranging from ministers to heads of state…

This might sound like it's from a new action movie, but if you take a look at the developments and published research in the automotive security research space this is absolutely a risk we should take into consideration.

The IT infrastructure of the Germany's military-run transport fleet already got hacked in 2020 showcasing that threat actors are indeed interested in this vector.

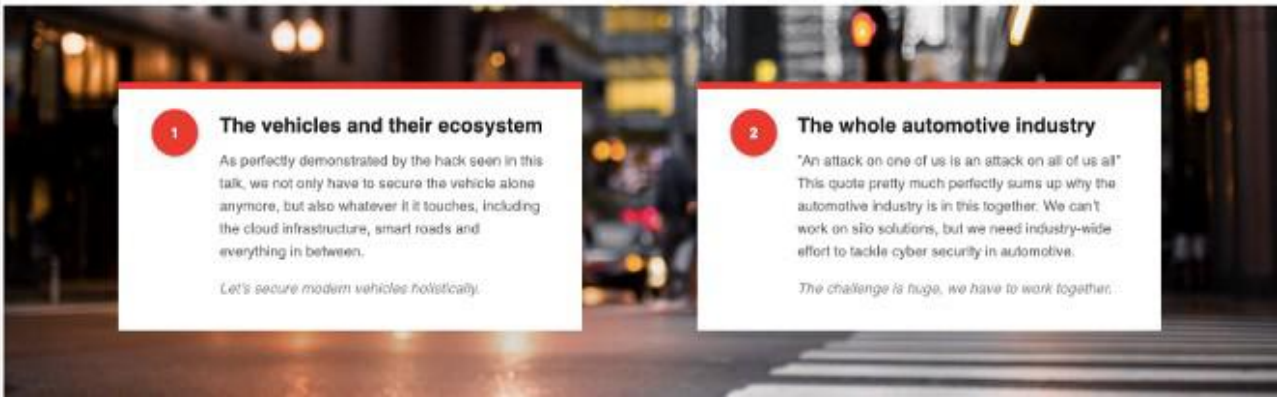
Copyright David Colombo

Copyright David Colombo

40

We need a more holistic approach!

Cyber Security in Mobility is a huge and extensive topic involving a lot of different parties, technologies and things to take into consideration. That's why need to tackle the topic with a holistic approach rather than silo solutions.



41

Cyber Security in Mobility.

Cyber Security in Mobility is a topic that already affects hundreds of millions of lives and yet we are still at the beginning of it. There are a number of things that we have to discuss, including the massive skills and talent shortage.

42

David Colombo

Future of mobility is… massive growth

Source: BNEF

Automotive

Including ICE and EV

Growth until 2050

Source: RB

Drones

For passenger transportation

Growth until 2050

Source: Statista

Airplanes

In service worldwide

Growth until 2050

43

What we have to do? To ensure a secure future

Collaborate together

In the mobility cyber security space we shouldn't have silos, but join collaboration. The ASRG and Auto-ISAC are great examples.

Create future talents

Without creating the next-generation of mobility cyber security talent we already failed the huge challenge that is in front of us before starting.

Enhance capabilities

Since cyber security in mobility is going to be a complex challenge we have to enhance capabilities to create solutions for all the various stakeholders.

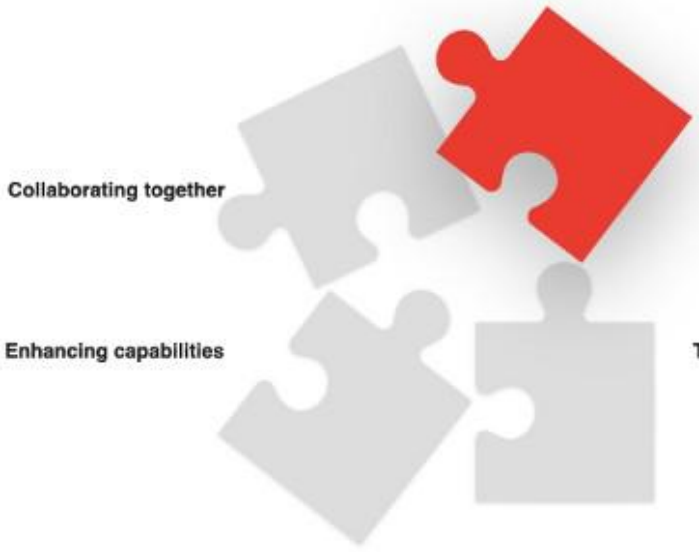
Take action fast

This isn't something we have 30 years for, we have to start now and act very fast in order to ensure the vehicles of the future are in a secure ecosystem.

44

David Colombo

Without talent in mobility cyber security we won't succeed!



45

Without talent in mobility cyber security we won't succeed!

Collaborating together

Enhancing capabilities

Creating future talent

Talent is the key puzzle piece that enables all the others

Taking action fast

46

David Colombo

We all have to work together
To secure tomorrow's mobility

OEMs & Global Organizations

OEMs are primarily responsible for securing their vehicles and infrastructure, but they need specialized mobility cyber security companies and the community to fulfill that.

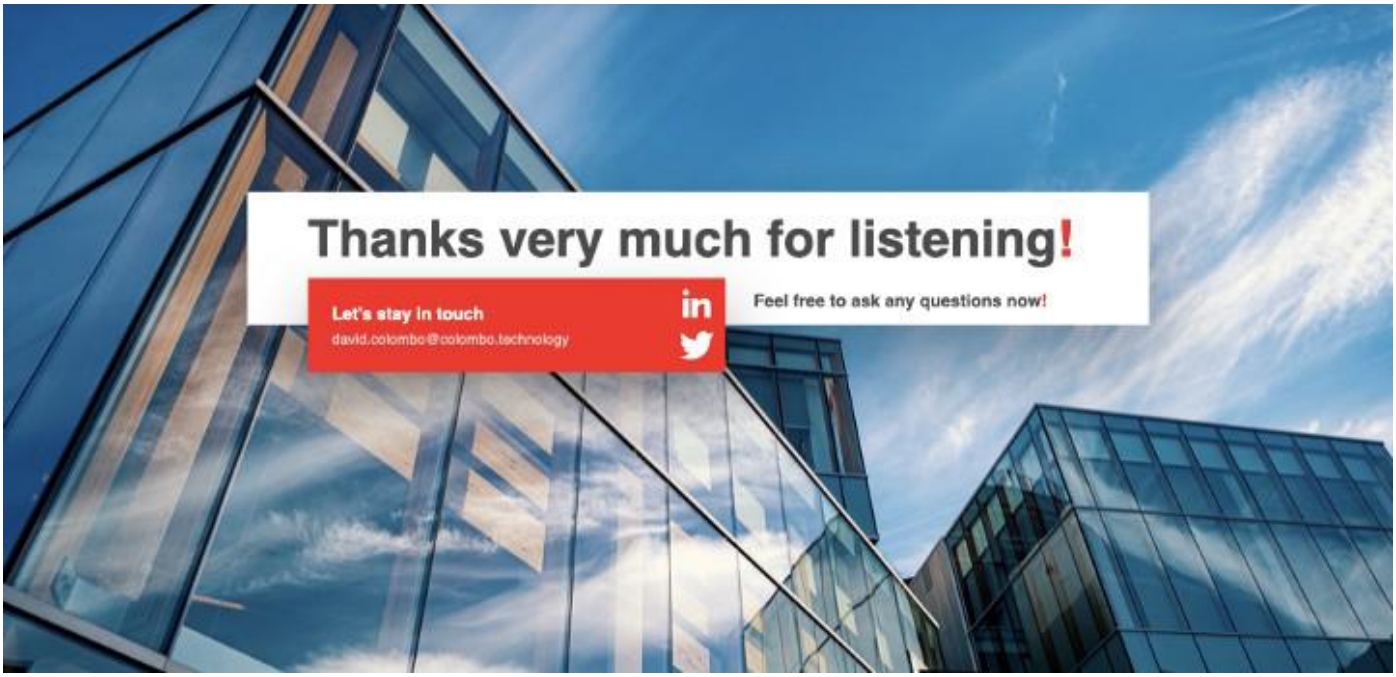
Cyber Security Companies

Mobility cyber security companies are hubs for cutting-edge research and solutions to enhance capabilities for all involved parties like OEMs and auditors.

Cyber Security Community

The mobility cyber security community will be crucial to tackle the huge challenge in front of us, to exchange knowledge and train the next generation of talents.

48



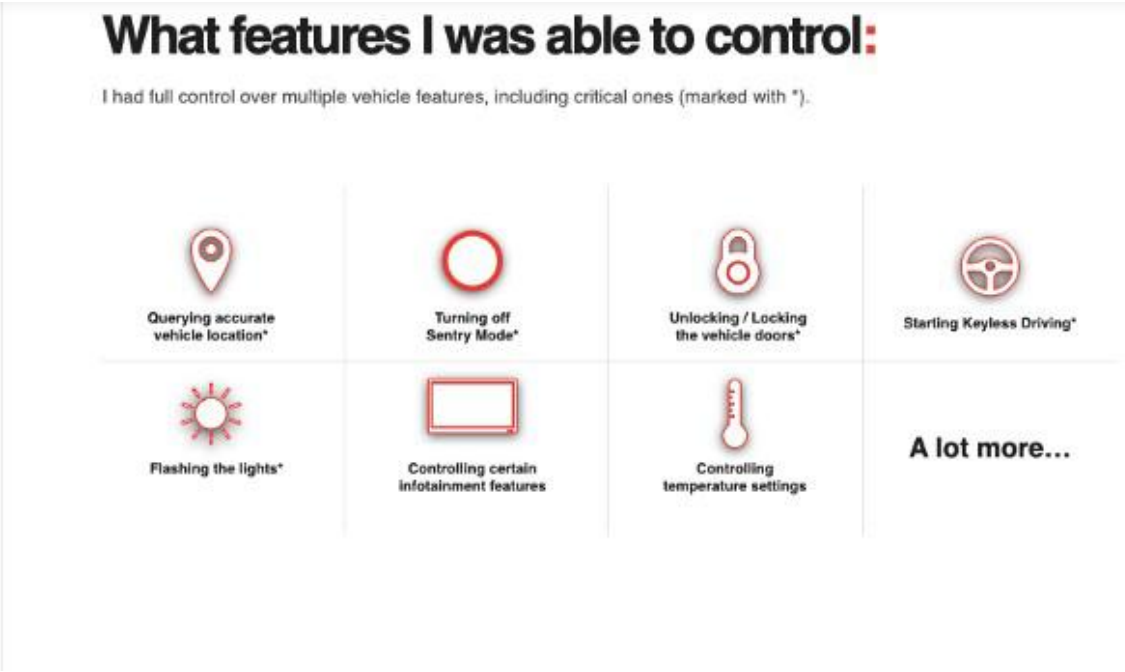
How the heck did a 19 year old from Germany manage to be able to take over more than 25 Tesla's around the world?

This is quite a story so buckle up and get in for a good read!

> **Important: This is not a vulnerability in Tesla's infrastructure directly, but Tesla is still responsible for many security shortcomings.**

What am I even talking about?

In short: I was able to run remote commands such as "disable Sentry Mode", "unlock the doors", "open the windows" and even "start Keyless Driving".



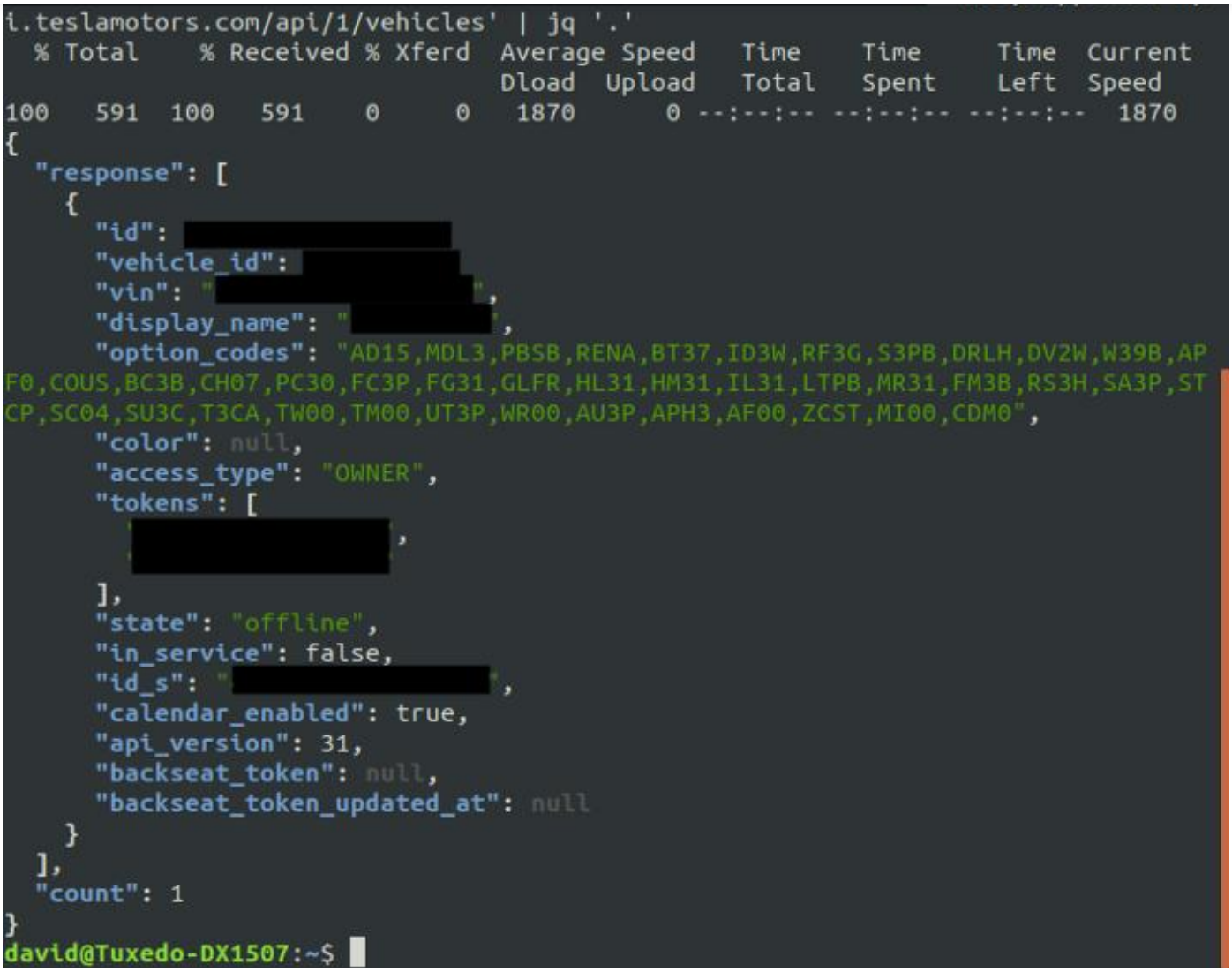
You see where this is going? Someone with malicious intent could even steal the car.

I, fortunately, did not have any access to the steering, accelerator & brakes and any other driving safety critical feature (*although I might have been able to use the summon feature to get the car moving, but I cannot confirm if this would have been possible*).

Nonetheless, there should be no way at all that someone could literally walk up to some Teslas they do not own and take them for a drive.

I also think it potentially could result in some dangerous situations on the road. For example, if someone with remote access starts blasting music on max volume while the driver is on the highway, or randomly and uncontrollable remotely flashing the lights of the Teslas at night.

I would prefer that not to happen.



Feel free to ignore this image. It is only here to be displayed in thumbnails.

> *Legal Disclaimer, before I proceed: This is all part of Security Research and I purely have good intent. As soon as I can confirm a vulnerability exists I immediately report it to the affected and involved parties. This writeup is part of responsible disclosure to the third-party maintainer and the Tesla Security Team.*

Full Timeline

To get a quick overview of all important events. Detailed report below.

2021–10–29: Contacted the owner.

2021–11–01: Got the instance taken down.

2022–01–09: Searched internet-wide for affected third-party instances.

2022–01–10: Found more than 20+ in 12 countries.

2022–01–10: Tried to find owner-identifying information.

2022–01–10: Reported this to two Tesla owners I was able to find.

2022–01–10: Tweeted about it, because I was frustrated that I couldn't identify more Tesla owners.

2022–01–10: The Tweet exploded.

2022–01–10: Number of found instances grew to 25+ in 13 countries.

2022–01–10: I talked to the renowned cyber security export John Jackson, who recommended I get a CVE-ID assigned for this, so the issue can be handled more efficiently.

2022–01–11: Requested a CVE-ID from MITRE. Providing preliminary information.

2022–01–11: Prepared this detailed writeup to describe the full situation.

2022–01–11: Contacted the Tesla Product Security Team to get the affected owners notified asap.

2022–01–11: Contacted the third-party maintainer to possibly get a patch ready.

2022–01–11: Shared additional information regarding affected owners with the Tesla Product Security Team.

2022–01–11: MITRE granted the CVE-ID request. CVE-2022–23126 pending.


2022–01–12: The third-party maintainers released version 1.25.1 with a partial fix.

2022–01–12: Tesla revoked thousands of potentially affected API tokens at 6:30 UTC / 7:30 CET.

2022–01–12: Tesla actively forced some affected users to reset their passwords.

2022–01–12: Waiting on further response from the Tesla Product Security Team.

2022–01–12: Worked with the third-party maintainer to explore potential further patches (encrypting the critical access tokens).

2022–01–13: The Telsa Security Team confirmed they revoked all affected API access tokens and all the affected Tesla owners have been notified by email and push notification.

2022–01–13: Some of the previous affected Tesla owners still seem to be affected.

2022–01–18: In contact with Tesla again, waiting on clarification from the Tesla Security Team.

2022–01–19: Tesla revoked another batch of access tokens.

2022–01–19: Discovered and reported an additional vulnerability, this time affecting Teslas API directly.

2022–01–22: Tesla confirmed the additional vulnerability and rolled out a fix into production.

2022–01–24: Public Release of this Writeup.

2022–01–24: Provided all information to MITRE / the CVE assignment team.

2022–01–24: CVE-2022–23126 published.


But now: Who even am I?

I'll keep it short, I promise.

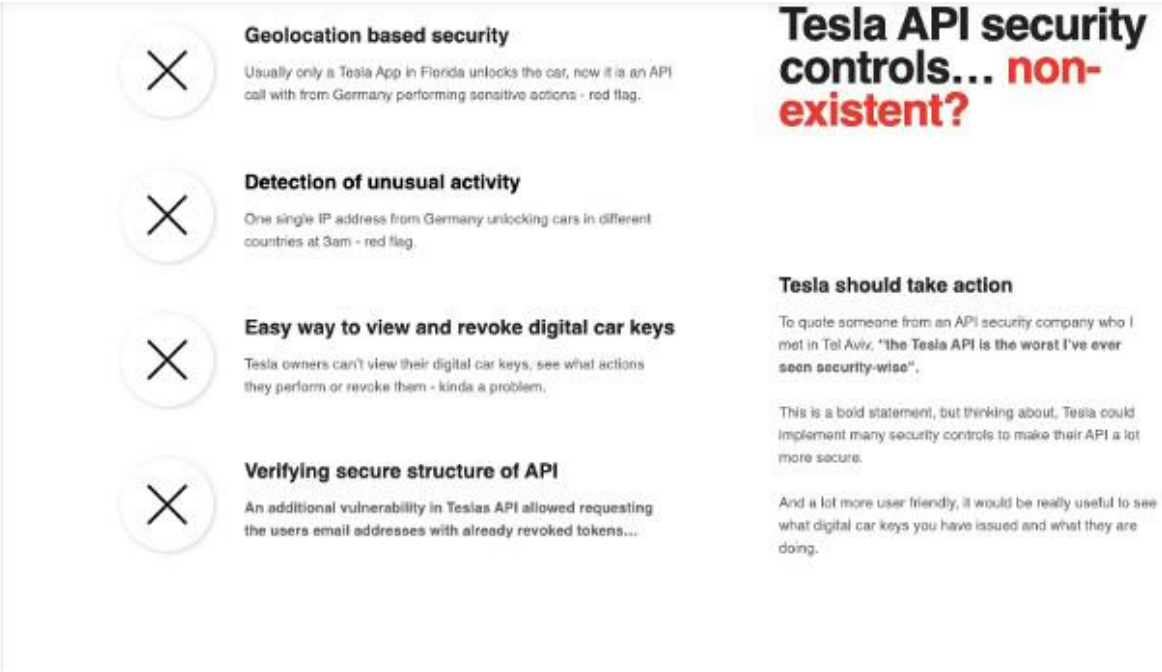
So, I'm David Colombo, 19 years and from the beautiful state of Bavaria in Germany (to be a bit more exact, around 2 hours from Munich).

I started coding back when I was around 10 and then somehow dived into cyber security (my school wasn't very happy when their info screens didn't display school information anymore).

With 15 I basically dropped out of school (with special permission from the German chamber of commerce to only go to school 2 days a week) to educate myself even more in that area and start a company with the goal to improve the current cyber security landscape. The company is now known as Colombo Technology, providing Security Audits, Penetration Tests & Cyber Security Consulting among other services.

Since then I've found various security vulnerabilities at e.g. RedBull, the U.S. Department of Defense and numerous more organizations under NDAs.

Now, what's the issue with the Tesla's? The fun part.

When did I get aware of this for the first time?

That's the fun background story about how I initially got aware of this issue. Feel free to skip this, the more recent events are further below.

It started last year actually. I was about to get in contact with a client for my company regarding a Security Audit. A pretty cool SaaS company from Paris.

And then, you know how it is, curiosity kicked in. I already wanted to take a peek look at their infrastructure to get some basic information about what services and platforms they use, I didn't even start a full fledged Security Audit yet. Maybe, I thought, I'd even very quickly find some outdated software or exposed backup database that I could show them in the next meeting. Oh boi, was I wrong. It was about to get much better.

When doing some basic subdomain enumeration, I found a backup.redacted.com domain. Looks interesting, right?

But there wasn't anything running besides a plain "this works" page.

The end.

A very light nmap scan produced some results, but did only find remoteanything and some “game server” ports. Strange enough.

The, for a backup server, weird namp scan

Connecting via telnet didn’t work.

Telnet didn’t quite work

But… simply accessing those ports now in the browser brought up something interesting.

Let me introduce you to TeslaMate:

This already looked a lot more interesting now.

But trying to access the Dashboards or anything didn't work.

Accessing Dashboards only gave me an error.

So I thought yeah, this is nice, I can see where this Tesla is parked. Let's go and report this.

But once again, curiosity came in to play. I must say, I am a huge Tesla fan myself. So I

> *It's only intended for pulling data and storing as well as displaying them. You can not run any commands like unlocking doors using the TeslaMate Dashboard. (We'll get to how running commands is still possible later.)*

By taking a look into the Dockerfile you'll see it also brings a Grafana installation with it. Hah — the inaccessible Dashboards.

The port 5555. Let's try to access that.

Upsie, I know where you went on vacation. It's definitely not freeciv as nmap claimed.

Me after seeing that: *sorry what? 0.o*

I was able to see a large amount of data. Including where the Tesla has been, where it charged, current location, where it usually parks, when it was driving, the speed of the trips, the navigation requests, history of software updates, even a history of weather around the Tesla and just so much more.

Update: Unauthorized guest access to the Grafana dashboards containing these sensitive information is now disabled. Fixed with TeslaMate release v1.25.1, that got

year.

But now curiosity strikes for the third time. Or the fourth time?

I really wanted to know how TeslaMate works. Because... if it is able to pull all the vehicle data it might also have a way to send commands to the Tesla?

After that thought I spent some time reading the TeslaMate source code in order to figure out how the authentication works, how the Tesla credentials flow through the app and where it stored the user's API key.

Long story short, it does save the API key where it also stores all the other data. The API key is neither stored separate nor is it encrypted.

So, if Grafana can access the vehicle data, and the API key is stored next to the vehicle data, can Grafana read and output the API key?

Well, there is Grafana Explore to run custom queries. This needs authentication tho. What a bummer.

Ever heard about this distant cyber security issue called... "default passwords"? Yep, TeslaMate Docker's Grafana installation comes with default credentials.

> ***It also is possible to query the tokens as an unauthorized anonymous user without logging in through a Grafana endpoint (see CVE-2022–23126 further below as well as TeslaMate patch v1.25.1 released after private disclosure and the screenshot that is included further below).***
>
> For that please watch the webinar released in cooperation with the Automotive Security Research Group: https://www.youtube.com/watch?v=fG9ySnNQVxI

I took the shot and tried logging in with admin:admin which, kinda unsurprisingly, but still hilariously it worked.


over the CTO's Tesla.

Which I deemed a high to critical security issue. No one should be able to unlock the SaaS company's CTO's Tesla doors... So I immediately stopped there and contacted the organization and get this resolved.

With that the whole thing was done for me. Last year.

This weekend a random thought crossed my mind.

TeslaMate is basically Insecure-By-Default, that means if it is deployed with it's default Docker configuration or the docker image with default configuration is used then TeslaMate is exposed and vulnerable to this.

CWE-1188 has a perfect description for it:

> *The software initializes or sets a resource with a default that is intended to be changed by the administrator, but the default is not secure.*
>
> *Developers often choose default values that leave the software as open and easy to use as possible out-of-the-box, under the assumption that the administrator can (or should) change the default value. However, this ease-of-use comes at a cost when the default is insecure and the administrator does not change it.*

What if... there are more of such exposed instances on the internet?

I was pretty busy and didn't have time for it but I couldn't get rid of the thought. So I had to take a look. And I searched the internet for exposed stuff once again, yay. Just that it this time was exposed access to vehicles.

Another thing that made me start searching for this again was, that you apparently no longer need the users password to issue a Keyless Driving API call.

As of Dec 1, 2021 you apparently no longer need a password to start Keyless Driving.

How to gain access to random Tesla's all the around the world:

- Run an internet-wide search for TeslaMate instances (search e.g. for the MQTT brokers).
- Make sure they run with the insecure default Docker configuration (this should be fixed by now, as user please pull the latest version asap).
- Go to port 3000 to access the Grafana dashboard.
- Login using default credentials *(of course only do that with explicit authorization)*.
- Go to the Explorer tab.
- Use the Query Builder to extract the API and refresh tokens.
- Have fun playing around with a Tesla (of course only with vehicles you own).

> ***Alternatively to logging in, if for example the owner changed the admin password (as they should have), you could also run arbitrary requests to the TeslaMate data source as unauthorized anonymous Grafana user through a Grafana API endpoint. See CVE-2022–23126. This only affects the TeslaMate docker and is patched by now. See the screenshot below.***

28

Querying the Tesla API token from Grafana without submitting credentials or login cookies.

> ***Regarding details of the critical vulnerability in the code please watch my session which will be released by the Automotive Security Research Group on May 12th 2022.***

- Opening the windows.
- Starting Keyless Driving.
- Sharing videos to the Tesla.
- Changing heater/cooler settings.
- Honking the horn & flashing the lights.

> *Funfact: It even is / would have been possible to open and close some garage doors (if the garage doors are connected to the exposed Teslas, see https://tesla-api.timdorr.com/vehicle/commands/homelink).*

A full list can be found here: https://tesla-api.timdorr.com/

As you can see it's a long list of possible data to query or commands to run.

You could run commands that annoy the shit out of the Tesla owner (imagine music blasts at max volume and every time you want to turn it of it just starts again or imagine every time you unlock your doors they just lock again), you could watch every move the Tesla owner does (it's kinda strange watching people driving to get groceries or knowing exactly where they live and yet there's no way you can report that to them) and you could even steal the Tesla as already mentioned in the introduction of this writeup.

And there I was... sitting in front of substantial remote access capabilities to those Tesla vehicles (in one of the later screenshots you'll see the access_type will be "owner" since it's the Owner API).

But first let's take a look at some of these beautiful (exposed) Teslas all around the world!

Tesla Model Y driving in California.

Tesla driving in Europe.

Tesla Model 3 driving in (mainly) in Belgium

Tesla Model 3 driving in the UK


Tesla Model Y driving in Florida.

Tesla Model 3 driving in Denmark.

Model Y driving in and around Kitchener (Canada).

I actually found 25+ Tesla's from 13 countries within hours. Including Germany, Belgium, Finland, Denmark, the UK, the US, Canada, Italy, Ireland, France, Austria and Switzerland. There were about at least an additional 30+ from China, but I really did not want to mess with China's cyber security laws so I left them completely untouched.

My initial scan resulted in 300+ found instances, but I haven't been able to confirm whether all of these were vulnerable since the Tesla Security Team asked me to not access any more instances until further notice.

> *Update: Since Tesla revoked thousands of keys this might have been an even more widespread issue.*

If you find any confirmed affected instance, please immediately notify the rightful owner or the Tesla Security Team (vulnerabilityreporting@tesla.com).

How did this whole thing unfold?

Well, what do you do if you find such vulnerabilities?

You report it to the responsible owner.

luckily managed to find the guy on Twitter. Greetings to Michael and his Model 3 at this point!

But what do you do if you can't find the responsible owner?

Tweet about it ¯_(ツ)_/¯

First public Tweet regarding this matter

Jokes aside, I actually posted that Tweet solely because I got frustrated. After a full day of finding exposed Teslas I was only able to find two Tesla owners to report it to them. Remember, two out of more than two dozen Teslas.

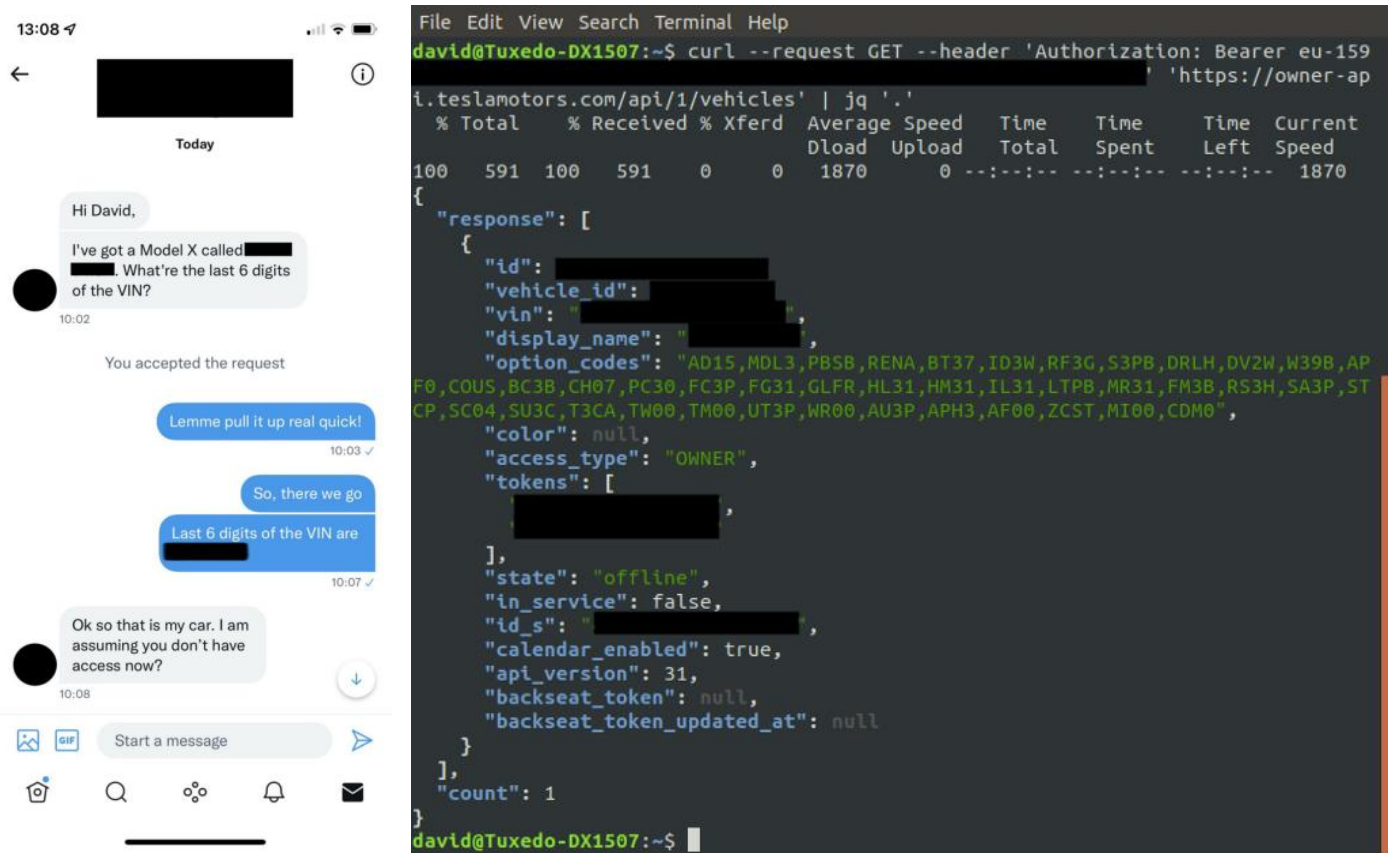
And I'm very sorry for all the confusion and/or speculations that this Tweet might have caused. Next time I'll definitely coordinate this differently.

And then... the Tweet blew up.

> *To respect the privacy of the affected Tesla owner I have modified the following section*

I actually found another affected Tesla owner from Ireland thanks to the Tweet. I commented about one specific name of a Tesla called “Blue Giant” and after some time later I woke up to this:



Verifying it is his Tesla using the VIN.

Turns out the Blue Giant from Ireland on my list actually is his Blue Giant.

Having Blue Giant honking.

Scary Throw-In:

The API tokens that allowed for this kind of access to “Blue Giant” stayed active and did not get revoked even after the owner explicitly and multiple times reset his Tesla Account password.

4 hours later we finally managed to figure out a way to get the Tesla API to revoke the keys through an undocumented API endpoint (see further below).

Coordinated disclosure with the Tesla Security Team

After I figured out there’s no (legal) way I’d be able to find the contact details of the affected owners (and I really didn’t want to put a “you’re hacked” video on the screen of random Teslas, as some folks on Twitter recommended), I talked to the Tesla Product Security Team.

They confirmed they are investigating the issue and then following on that revoked all affected and legacy tokens shortly after.

As of now 13. January 2021 all of the affected users also should have been notified by email, according to the Tesla Security Team.

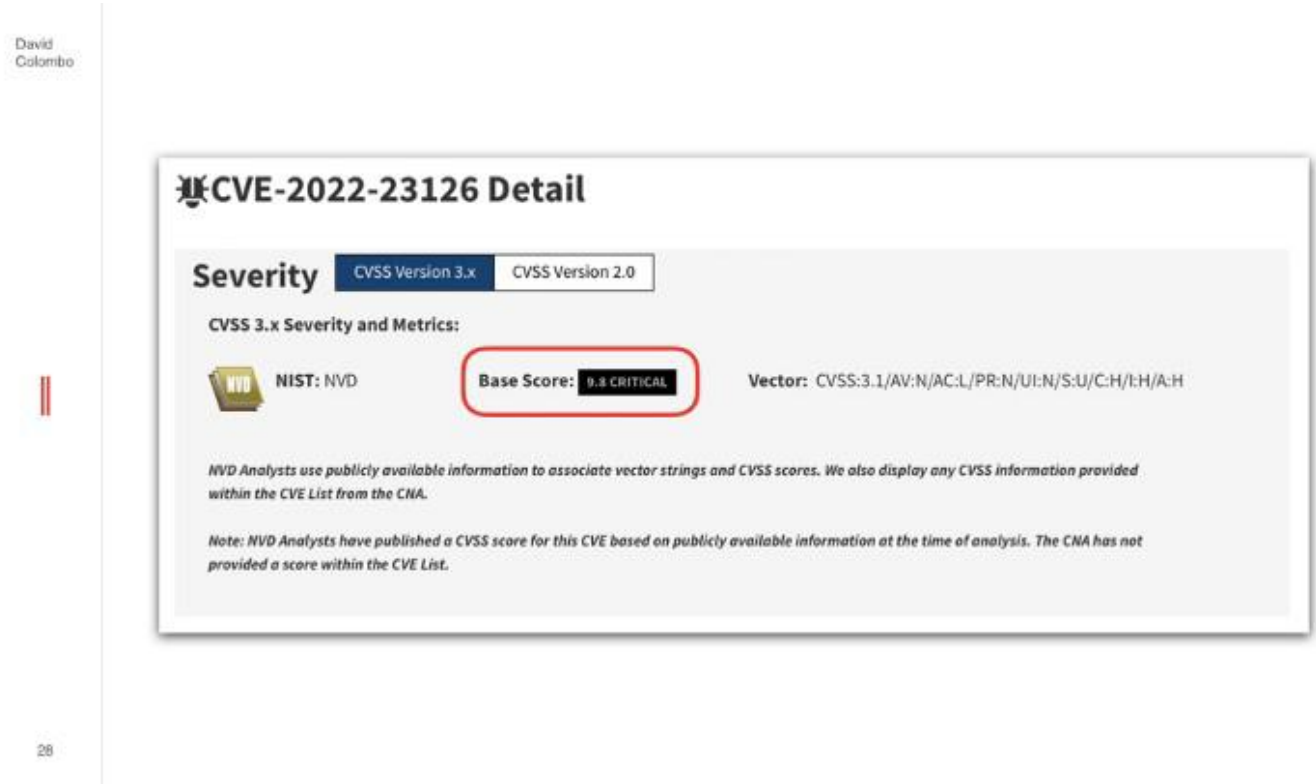
token revocation of the Tesla Security Team, probably because the users signed in to the vulnerable TeslaMate instances again.

So I built a quick Python script to automatically revoke exposed access tokens from vulnerable instances myself.

> Bad news, there doesn't seem to be a way to revoke version 3 tokens.

If I'll find a way to revoke version 3 tokens, I could simply pipe the internet-wide scans into this script to automatically and continuously revoke any further exposed access tokens from vulnerable instances.

RE: CVE-2022–23126 with CWE-1188



Since there was quite a number of affected Tesla owners and it would be very useful to be able to share a CVE-ID with all TeslaMate users (and because CWE-1188 fits so perfectly here), I requested a CVE number for this vulnerability.

> *"TeslaMate's default Docker configuration prior version 1.25.1 allows for an attacker to obtain a victim's generated token, giving them the ability to perform unauthorized actions via Tesla's API such as controlling certain critical features of the vehicle or disclosing sensitive information."*

Released patches for CVE-2022–23126:

Release v1.25.1 · adriankumpf/teslamate

Disable anonymous logins to Grafana by default (when using the teslamate/grafana Docker image) The first time you visit...

github.com

Note: This is not the personal fault of the maintainer! It's an open source project, that grew over time and something like this can happen.

Please watch the ASRG webinar so learn more about this: https://www.youtube.com/watch?v=fG9ySnNQVxI

Recommendations for mitigating this CVE

Just... don't... connect critical stuff to the internet. It's very simple.

And if you have to then *make very sure it is set up securely and not with insecure defaults*. Here are the TeslaMate Docs to setup more advanced auth: https://docs.teslamate.org/docs/guides/traefik

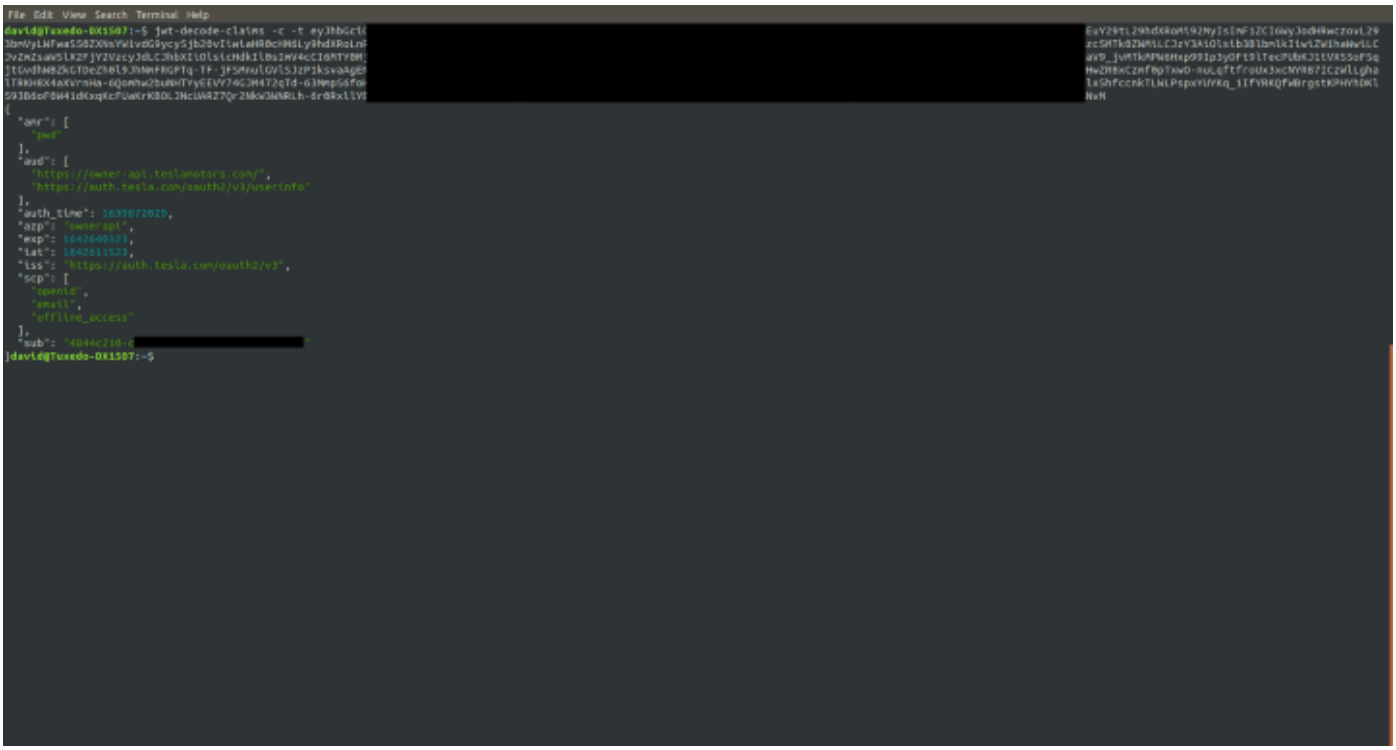
Oh, and please built solid APIs. An API with security in mind could have prevented this with ease.

Update: A patch has been released. Please update to at least version 1.25.1

tokens, I started searching for that endpoint.

It actually was pretty easy to find it in retrospect. Although there is no official Tesla OAuth documentation, Tesla was nice enough to add the endpoint somewhere else.

Version 3 access tokens, other than version 2 access tokens, are JWTs. And if you decode them you can see this:



Decoding a version 3 access token for the Tesla API.

Additionally to the *https://owner-api.teslamotors.com/* endpoint for the vehicle commands it also shows *https://auth.tesla.com/oauth2/v3/userinfo* for, well, user information. Yay, finally a way to get the owners email addresses. (Tesla has asked me *not* to use those email addresses to notify owners of exposed Teslas.)

But, to my very surprise, I noticed **I could query the email addresses of Tesla owners using tokens that got already revoked by the Tesla Security Team**. See here:

Querying the emails of Tesla owners using tokens that are revoked by Tesla.

At the beginning of the story I didn't have any way to find owner-identifying information and now I can query email address even with revoked access. Kind of ironic!

I reported this issue to the Tesla Security Team immediately. They confirmed the vulnerability and rolled out a fix into production shortly after. This one is also eligible for bug bounty from Tesla :D (I hope this pays for all my coffees of the past two weeks.)

Addition on January 26th, regarding Pin-to-Drive

I originally suggested the following to all Tesla owners:

- Enable Pin-to-Drive to prevent anyone from stealing your Tesla even with valid API access tokens or account credentials.

But apparently **Pin-to-Drive gets bypassed by the Keyless Driving API call**.

What should be done to prevent this from happening again?

(Affected) Tesla Owners:

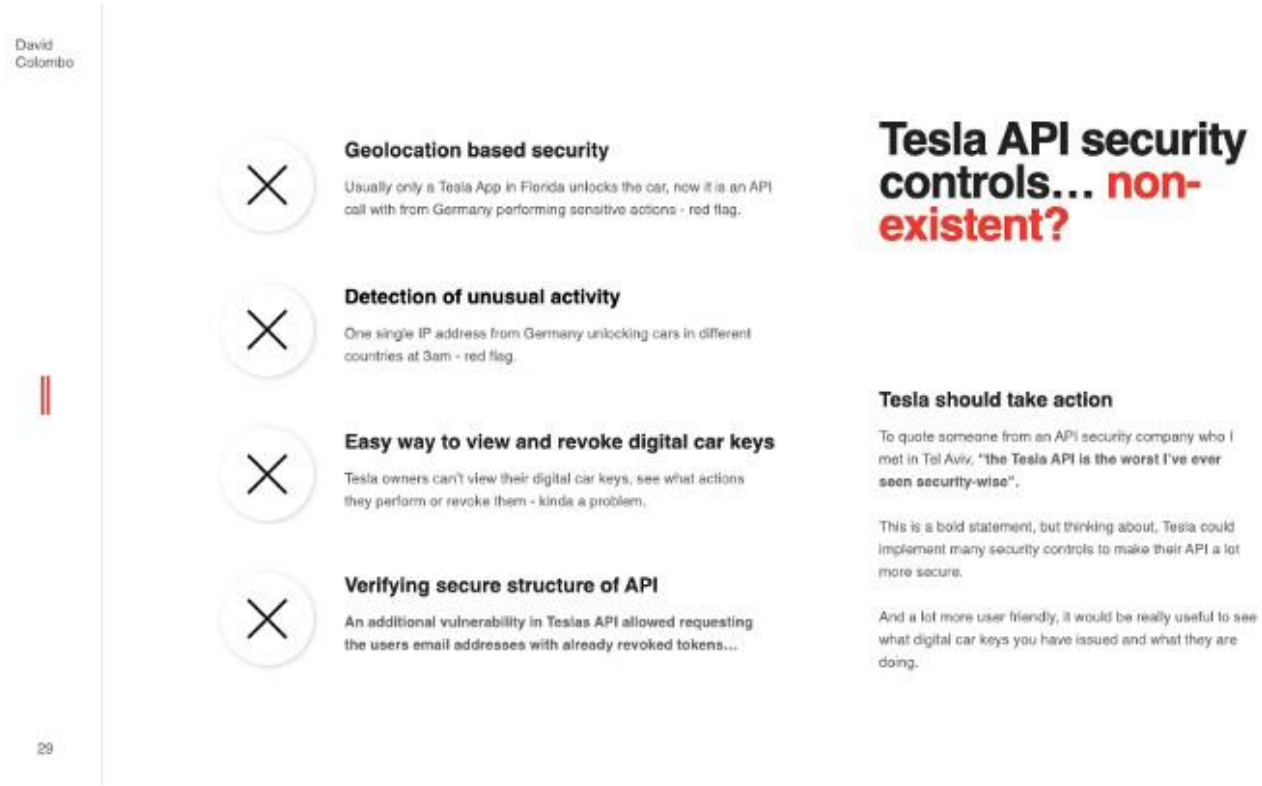
- Be very very careful who you give your credentials to.
- Update TeslaMate (and any other third-party Tesla software you use) to the latest version and keep an eye on further security updates.
- **Do not put random stuff on the internet.**
- We found a way to revoke potentially compromised API tokens (see the image below). ***This unfortunately only works with version 2 tokens which are deprecated now. There doesn't seem to be a way to revoke version 3 tokens yet.***

Third-Party Maintainers:


quickly released after I shared this writeup privately with the maintainer.)

- **Do not store critical access tokens accessible.** Store it in a way it's not accessible via external access. At best encrypted. (This is currently under consideration for TeslaMate. See https://github.com/adriankumpf/teslamate/pull/2360)

Tesla:



Yes, I do think Teslas security measures are okay, but there is room for some major improvement:

- Add multiple scopes to the API! People are going to use it anyways make it secure for them. Just **add multiple scopes** like: Read-Only Scope (for third-party software that only needs to collect data), Non-Critical Scope (seat heater, etc), Critical Scope (unlocking doors, keyless driving, etc).
- Require the password for the Keyless Driving API endpoint again (I have no idea why

- Since Tesla API tokens are basically car keys, but can be generated easily, copied and used multiple times in multiple places, Tesla should/could implement an easy way to keep inventory of & track Tesla API tokens.
- Finally add the “press in case of hacked to cut cloud connectivity” button to the cars that Elon Musk mentioned in 2017 ;)

Why did this happen?

Why the Automotive Ecosystem needs to be secure:

The automotive landscape is changing very fast, so is the automotive ecosystem. We have to keep an eye on the increasing attack surfaces.

Talking Points Include:

Increasing Attack Surface

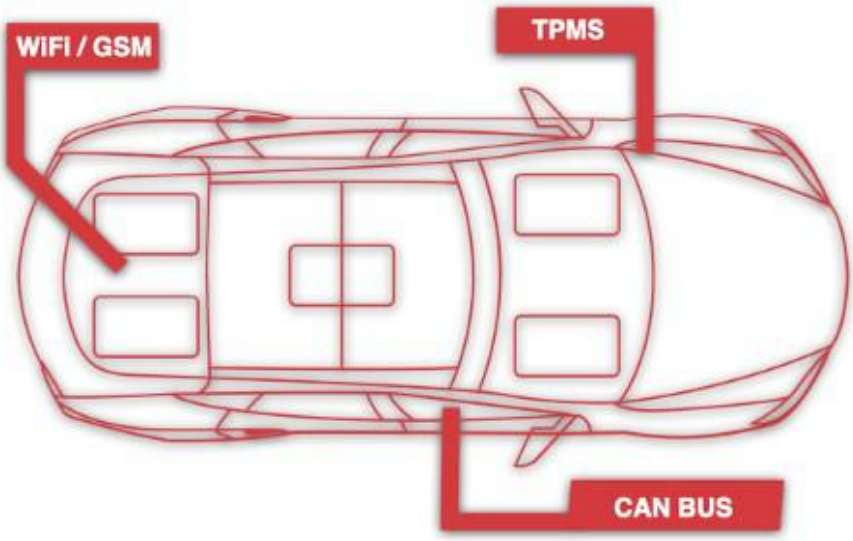
Dangers of the Automotive Ecosystem

34

David Colombo

80 years ago, no digital technology involved.

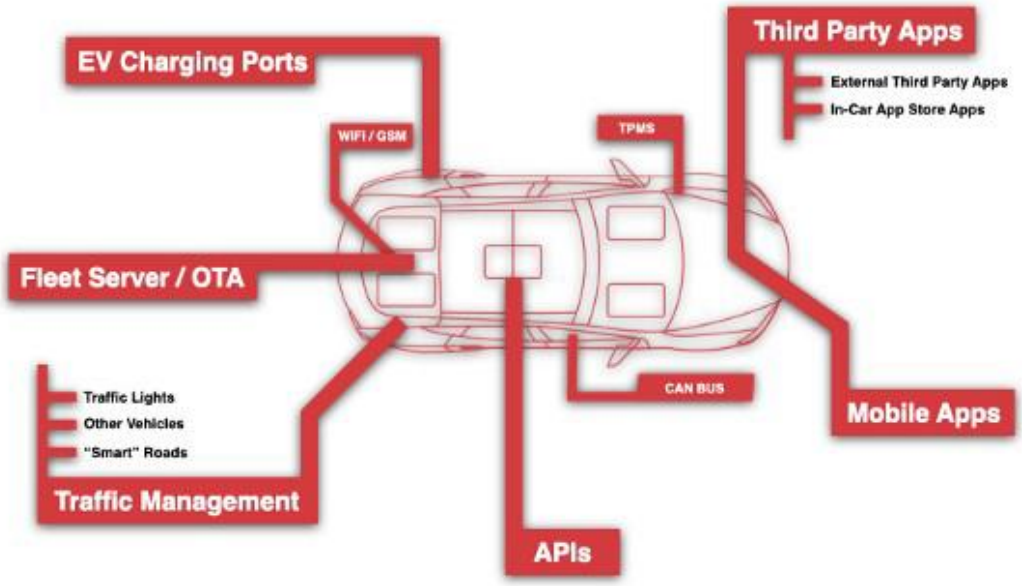
35



36

David Colombo

Future attack surface.



37

FAQ

Whose fault is that?

It basically is a concatenation of issues that in the end lead to me being able to have control over those cars. The owners, the third-party maintainer as well as Tesla itself could have done steps to prevent this all from happening.

Would I have been able to move the car?

Not as far as I know, but renowned cyber security researcher John Jackson who had insights on this issue pointed out that it might have been possible to utilize the “summon” feature to get the car moving and potentially even hit something.

Why didn't I tell Tesla first?

Tesla is not responsible for owner or third-party issues. Luckily they still helped in remediating this and protecting the affected Tesla owners. And maybe they'll even implement some recommendations to give their users and even more secure experience.

Is there an issue with the initial Tweet?

Kind of, it should have said "remote control over certain (critical) features (including being able to turn off Sentry Mode, unlocking doors and starting Keyless Driving)" rather than simply "full remote control".

Although I clarified it in the following Tweets and did my best to get the facts to all media who reported on this, I'm sorry for any confusion caused.


Why did it take so long to release the Writeup after the initial Tweet?

Since this is still part of responsible disclosure, I had to talk to the Tesla Security Team as well as the third-party maintainer first and I also had to make sure all of the exposed Teslas (that I was aware of) are no longer affected by the issues.

Is TeslaMate bad software in general?

No! It is an amazing piece of software with an awesome maintainer. And I do not want to put any blame on the maintainer, since he is interested in making it secure for all users as much as I am. Furthermore are primarily the Docker installations affected and every user using the great Advanced Setup Guides (https://docs.teslamate.org/docs/guides/apache) should not be affected.

What's next?

I'll definitely continue researching security related to Tesla, since I want Tesla owners and their cars to be as secure as possible. I'd love to get my hands on a Tesla hardware and/or a Tesla MCU.

Automotive security is a very important topic, especially as other automakers, such as VW, join in digitizing their fleets.

If you need to contact me personally, feel free to send me a DM on Twitter (https://twitter.com/david_colombo_) or contact me on LinkedIn (https://linkedin.com/in/david-colombo).

To contact the Colombo Technology Cyber Security Team, please email cybersecurity@colombo.technology or go to our contact form here.

Let's make the internet out there more secure for everyone!

Special Thanks to: John Jackson (Security Researcher), Adrian (TeslaMate Maintainer),