

Security Lab

jiangkun@fmsh.com.cn

Kun Jiang, Xinyi Xie, Rui Dai

Introduction

How does it work

More technical description

Impact and demo

Possible countermeasures

Is Phone



Key

Secure

Compromising

Keyless

Entry for

Tesla

Model 3

Exploit:

Authentication

Bypass by

Spoofing

Data: 2022-03-

06

Exploit Authors:

Kun Jiang, Xinyi

Xie, Rui Dai, Jun

Lu



Security Lab

jiangkun@fmsh.com.cn

Kun Jiang, Xinyi Xie, Rui Dai

Introduction

How does it work

More technical description

Impact and demo

Possible countermeasures



Affected

Product: Tesla

Model 3

Version: Tesla

Model 3: V11,

Tesla Mobile

App: V4.23 (test

on Motorola

Edge S Android

11)

CVE: CVE-

2022-37709



Security Lab

jiangkun@fmsh.com.cn

Kun Jiang, Xinyi Xie, Rui Dai

Introduction

How does it work

More technical description

Impact and demo

Possible countermeasures

The Tesla app has a feature called Phone Key that turns a smartphone into a key. Locking and unlocking even starting Model 3 with your phone key is conveniently hands-free. As



you approach,
your phone's
Bluetooth signal
is detected and
doors unlock.
Further, you can
start and drive
the car without
ever taking the
phone out of a
pocket.
However, this
passive entry
and start
feature are not
secure enough.
Authentication
can be bypassed
by spoofing. It
allows attackers
to open a door
and drive the car
away by
leveraging
access to a



Security Lab

jiangkun@fmsh.com.cn

Kun Jiang, Xinyi Xie, Rui Dai

Introduction

How does it work

More technical description

Impact and demo

Possible countermeasures



legitimate
Phone Key.



Security Lab

jiangkun@fmsh.com.cn

Kun Jiang, Xinyi Xie, Rui Dai

How does it work?

The phone key communicates with Model 3 using Bluetooth in plain. The Bluetooth Phone Key reconnects to the Model 3 depending on the vehicle's MAC address

Introduction

How does it work

More technical description

Impact and demo

Possible countermeasures



only. Since the MAC address of the car is static, an adversary can fake the Model 3 easily. The Phone Key will reconnect to the device with the specific MAC automatically. In this case, the adversary forwards the messages to both sides as an intermediary. Model 3 authenticates the key by two attestations. The Phone generates the second attestation



Security Lab

jiangkun@fmsh.com.cn

Kun Jiang, Xinyi Xie, Rui Dai

Introduction

How does it work

More technical description

Impact and demo

Possible countermeasures



based on a token from the vehicle. According to our experiments, the update of the token is not related to the connection status and happens over hours. It allows the adversary to complete the attack with one attack device. The adversary needs to approach the owner and the Model 3 in turn to forward messages. By spoofing the Phone key and the vehicle, the



Security Lab

jiangkun@fmsh.com.cn

Kun Jiang, Xinyi Xie, Rui Dai

Introduction

How does it work

More technical description

Impact and demo

Possible countermeasures



attack device
can bypass the
authentication.
Finally, the
Model 3 unlocks
the door and can
be started.



Security Lab

jiangkun@fmsh.com.cn

Kun Jiang, Xinyi Xie, Rui Dai

More Technical Description

Here is a more
detailed
explanation of
the exploit:
The Phone Key
and Model 3 will
generate a

Introduction

How does it work

More technical description

Impact and demo

Possible countermeasures



shared secret by

ECDH . The

shared key is

used to

authenticate

attestations.

The attestations

are calculated

by AES-GCM .



Security Lab

jiangkun@fmsh.com.cn

Kun Jiang, Xinyi Xie, Rui Dai

1. Get the MAC

address

BD_ADDR of

the Model 3

according to

advertisements

broadcasting.

2. Change the

MAC

address of

the attack

device same

as Model 3

3. Approach

the owner to

Introduction

How does it work

More technical description

Impact and demo

Possible countermeasures



get the first
attestation

A.

4. Approach
Model 3 to
get the token
G

5. Approach
the owner to
get two
attestations

A', B

6. Back to the
vehicle. The
vehicle
unlocks.

The figure below
shows the entire
process of
exploiting the
vulnerabilities.



Security Lab

jiangkun@fmsh.com.cn

Kun Jiang, Xinyi Xie, Rui Dai

Introduction

How does it work

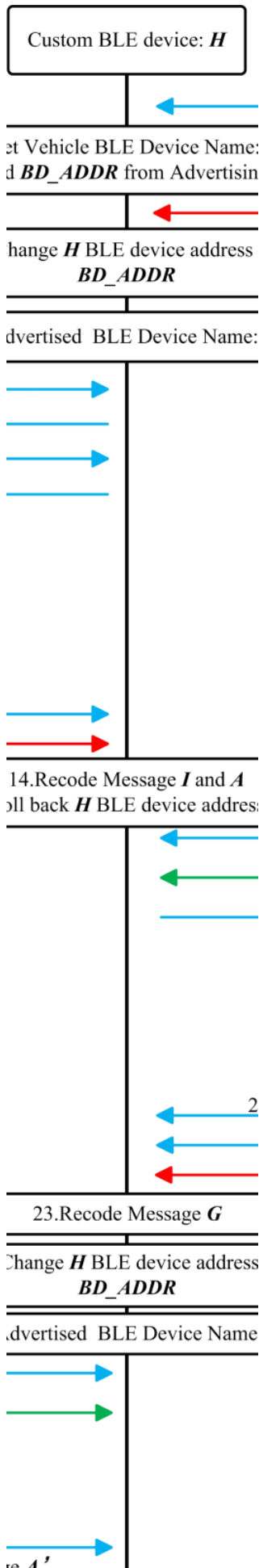
More technical description

Impact and demo

Possible countermeasures

Adversary





Security Lab

jiangkun@fmsh.com.cn

Kun Jiang, Xinyi Xie, Rui Dai

Introduction

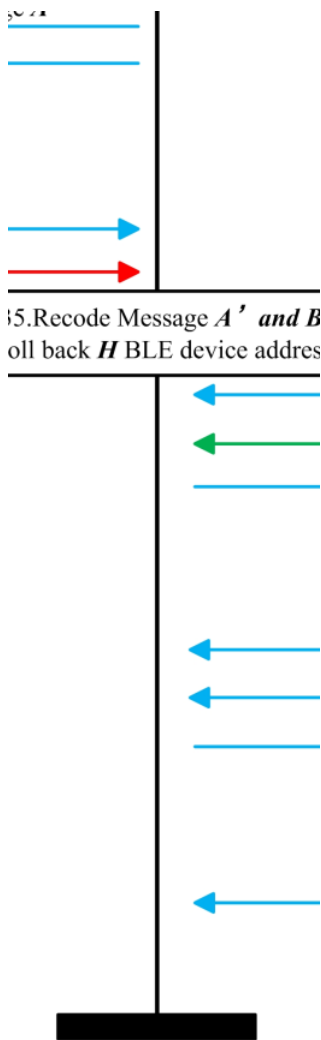
How does it work

More technical description

Impact and demo

Possible countermeasures





Security Lab

jiangkun@fmsh.com.cn

Kun Jiang, Xinyi Xie, Rui Dai

Introduction

How does it work

More technical description

Impact and demo

Possible countermeasures

**Impact
and
Demo**



1. The whole process is out of the awareness of the car owner. People can drive your car without your permission.

2. Because the token G remains fixed for several hours, the attacker



Security Lab

jiangkun@fmsh.com.cn

Kun Jiang, Xinyi Xie, Rui Dai

Introduction

How does it work

More technical description

Impact and demo

Possible countermeasures



has
plenty
of time
to
complete
the Man
in the
Middle
Attack.
The
parking
lot near
Starbucks
or
supermarkets
appears
to be a
great
place to
perform
the
attack.

3. Since
most of
the
communicatic



Security Lab

jiangkun@fmsh.com.cn

Kun Jiang, Xinyi Xie, Rui Dai

Introduction

How does it work

More technical description

Impact and demo

Possible countermeasures



data on
the
Bluetooth
channel
is in
plaintext,
it is
easy for
an
attacker
to
replay
some
fixed
data,
such as
request
commands
and
vehicle
status
information.

4. Any
devices
that
support



Security Lab

jiangkun@fmsh.com.cn

Kun Jiang, Xinyi Xie, Rui Dai

Introduction

How does it work

More technical description

Impact and demo

Possible countermeasures



*BLE 5
can
exploit
this
vulnerability
to
complete
the
attack.*



Security Lab

jiangkun@fmsh.com.cn

Kun Jiang, Xinyi Xie, Rui Dai

Our results
show that
attackers can
break into Tesla
Model 3 and
drive it away in
one minute
without the
awareness of
the car owner. It
brings into
question the
security of
Passive Keyless

Introduction

How does it work

More technical description

Impact and demo

Possible countermeasures



Entry and Start
(PKES) and
Bluetooth
implementations
in security-
critical
applications.



Security Lab

jiangkun@fmsh.com.cn

Kun Jiang, Xinyi Xie, Rui Dai

We created an
app named
TesMla for
Android device
to conduct the
attack.

You can check
the demo video
for attack on the
Youtube.

More
information for
the app is on the
Github.

Introduction

How does it work

More technical description

Impact and demo

Possible countermeasures



Possible countermea



Security Lab

jiangkun@fmsh.com.cn

Kun Jiang, Xinyi Xie, Rui Dai



BLE
on encryption
PIN
2 Tesla
Drive can
Car enable
owners secure
can BLE
enable communication.
this The
multi- communication
factor between
authentication end
countermeasure. devices.
It will
allows be
owners protected
to by
program this
a session
key

Introduction

How does it work

More technical description

Impact and demo

Possible countermeasures



personal key.
identification Enabling
number. BLE
This encryption
feature will
forces improve
the the
owner difficulty
to of
enter the
these analysis.

numbers
into
the
screen
to
drive
the
car.



Security Lab

jiangkun@fmsh.com.cn

Kun Jiang, Xinyi Xie, Rui Dai

Introduction

How does it work

More technical description

Impact and demo

Possible countermeasures



F h ToF-
Token based
frequently secure
ranging
Tesla The
can UWB
update



update the token every time the Model 3 establishes a BLE connection. The adversary has to use two attack devices connecting to the Phone Key and Model
utilizes the ToF technique to measure the distance. Messages of measurement or synchronization require encryption or signature by a trusted module, Secure Element (SE) for example.



Security Lab

jiangkun@fmsh.com.cn

Kun Jiang, Xinyi Xie, Rui Dai

Introduction

How does it work

More technical description

Impact and demo

Possible countermeasures



3

simultaneously.

To

a

certain

degree,

refreshing

the

token

fast

enough

will

reduce

the

attack

window.



Security Lab

jiangkun@fmsh.com.cn

Kun Jiang, Xinyi Xie, Rui Dai

Introduction

How does it work

More technical description

Impact and demo

Possible countermeasures



Tesla has been
notified over 6
months ago
(March/2022)
and has not
replied yet.

© All rights
reserved.



Security Lab

jiangkun@fmsh.com.cn

Kun Jiang, Xinyi Xie, Rui Dai

Introduction

How does it work

More technical description

Impact and demo

Possible countermeasures

