THEFT OF KEYLESS ENTRY/STARUP CARS

A presentation by
John Krout
For PATACS Arlington
April 7, 2021

Why this topic is relevant to you

- Today, hybrids and electric vehicles use this same keyless entry/startup behavior; some by default, some offer it as an option.
- Your next car may be a hybrid or electric
- All keyless entry/startup cars face the same risk of theft
- Some of today's cars also face a risk due to digital security flaws in the car's fob

Use the QR code

online article about car fob cloning

Agenda

- My own experience with Toyota Prius
- How keyless entry/startup works
- Fob foibles
- How thieves use tech to steal a keyless entry/startup car
- Ways to minimize the risk of theft

My Toyota Prius experience

- I bought a Prius in 2005.
- That car had the keyless entry/startup feature.
- I bought a 2015 Prime Plug-In, with the same feature.
- In 2020, my son told me of reported car thefts of keyless entry/startup cars.
- Like any skeptical parent, I checked online.
- I found a Popular Mechanics article published in September 2019 detailing the theft method and the tech involved.

How keyless entry/startup works

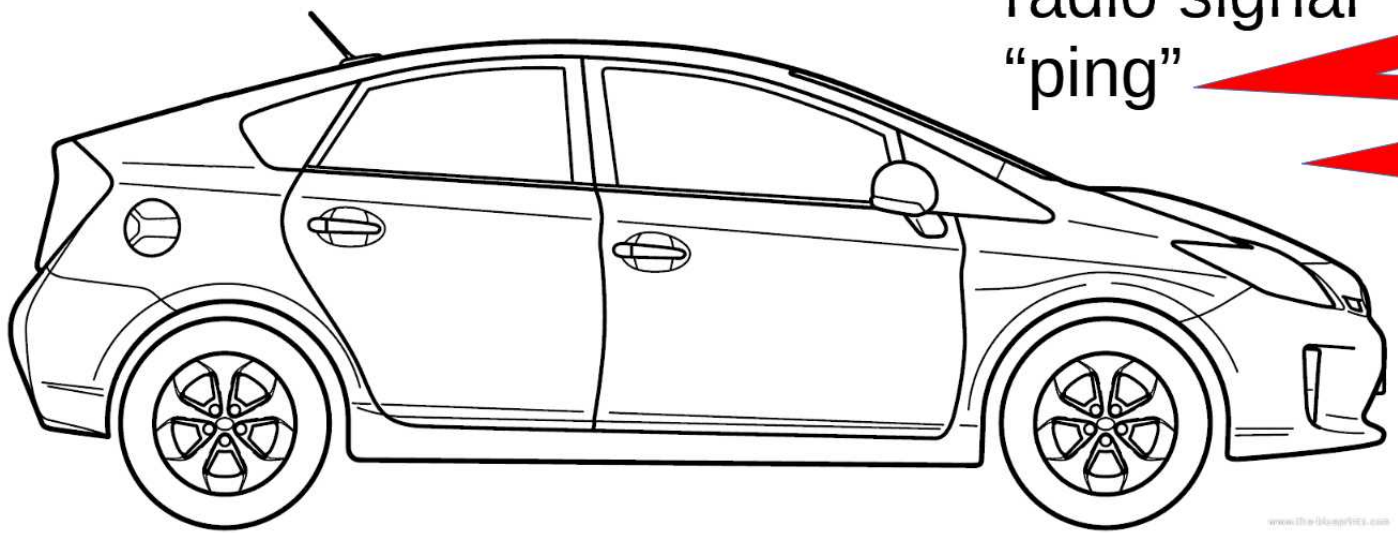
How keyless entry/startup works

- The car comes with a **fob** powered by a button battery.
- Each fob has a unique 128-bit digital ID.
- Fob proximity to car auto-unlocks the driver door.
- Pushing the Prius Power button on the dash also involves the fob in authorization to start the car.

How car and fob work together

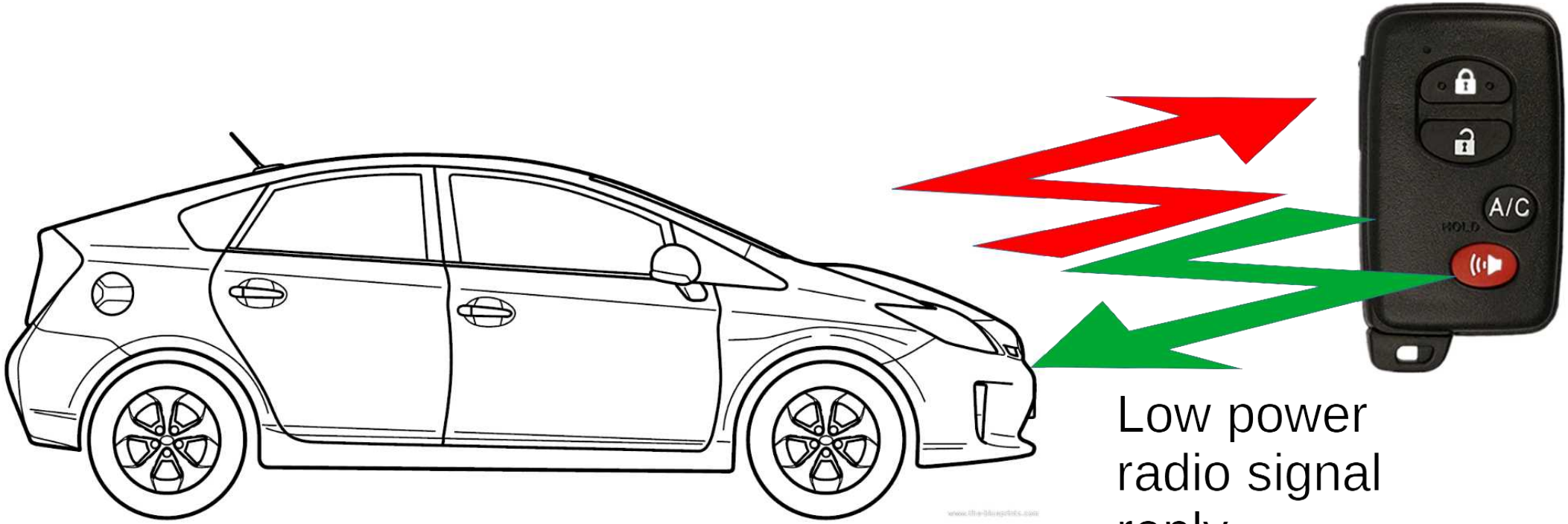
- The fob and car communicate automatically using low power radio signals.
- Low power means automatic communication works only when the fob is within roughly 2 feet of the car.
- Every hybrid has a very high capacity battery, and can send low power pings to detect the fob for many days without significant loss of car battery power.
- Fob receives ping and then replies, sending its 128-bit digital ID, pre-registered with the car.
- Car verifies fob digital ID is registered, turns on interior lights, and unlocks driver door.

Car sends ping



Low power
radio signal
“ping”

Fob responds



Low power radio signal reply

What does the car do next?

- If ping results in no response from fob, then fob is not nearby
- Car repeats ping
- If fob responds, then fob is close to car
- If fob digital ID is recognized by car, then car unlocks driver door and turns on interior lights

Car startup behavior

- Press Power button for a moment, while depressing brake pedal
- Car repeats the ping and awaits response, possibly at lower power, to ensure fob is inside car.
- Fob receives ping, and sends reply including digital ID
- Car receives reply, verifies digital ID, and starts the engine.
- In my Prius Plug-In, that starts ***only*** the electric motor. A separate button starts the internal combustion engine.

Fob foibles

Fob buttons

- All work up to 30 feet away from car
- Lock
- Unlock
- A/C ($2000 option)
- Sound the horn

When the fob battery is dead

- Fob includes a small key that can be removed from fob for unlocking doors the old-fashioned way.
- Gen 2 Prius (including my 2005 Prius) had a dashboard slot to power a fob containing a dead battery, for car startup
- Gen 3 Prius dashboard reports to driver when fob battery is low

Fob registration with car

- Fob digital ID can be registered with car
- Used fobs are available online
- Registration process is convoluted for consumers, due to lack of a car app or computer interface
- Registration process is not documented in owner manual or tech manual
- Registration processes ***are*** documented on **Priuschat.com**
- Each fob can be registered with many cars

Use the QR code

Car thieves and tech

Inexpensive Relay Attack

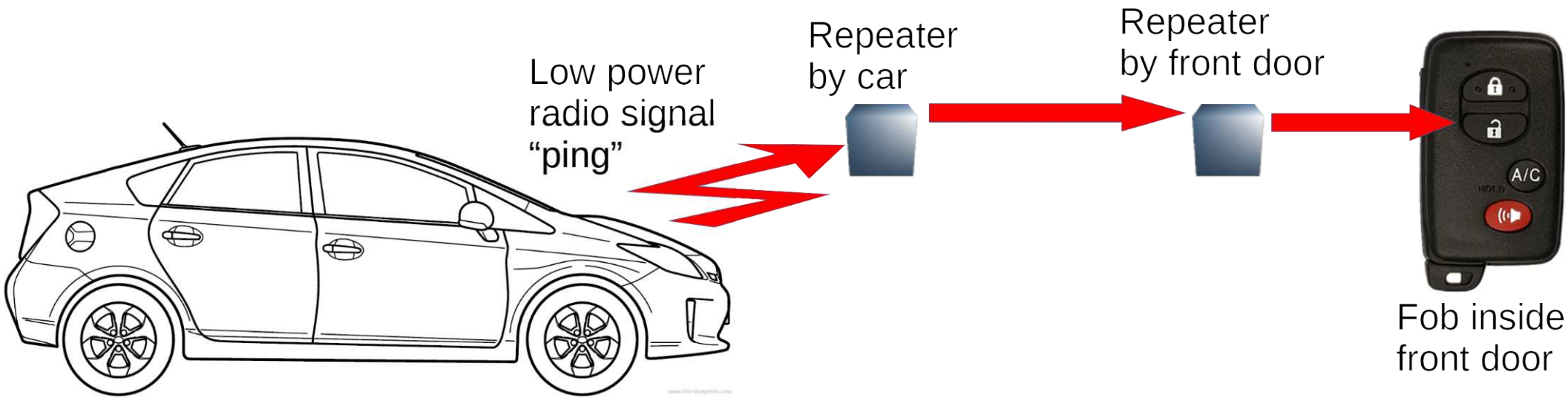
- This scheme was reported by **Popular Mechanics** in September 2019:

  https://www.popularmechanics.com/technology/security/a29835980/technology-theft-rfid-bluetooth/

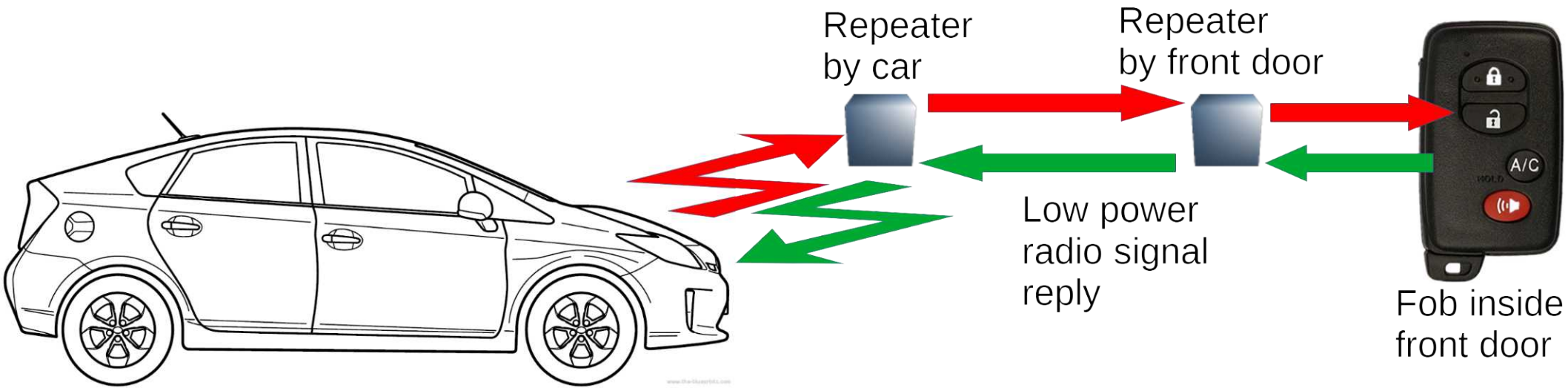
Use the QR code

- Context: night time, fob is close to front door of house, car is on street close to house.
- Car thief brings two $10 battery-powered **radio repeaters**

How a thief unlocks the car



How a thief unlocks the car



How a thief starts the car

- Thief enters car, taps the Power button.
- Car pings again, *through the repeaters.*
- Fob responds again, *through the repeaters.*
- Car verifies fob digital ID, and starts.
- Thief picks up repeaters, and drives away.

Next steps for thief

- With internal combustion engine tuned off, electric motors in car make very little noise.
- Owner and neighbors will not hear the car start up.
- Thief may need to refuel the stolen car.
- Gas station staff may believe stolen car is turned off.
- Thief may register another fob with the stolen car.
- Toyota branded parts are expensive!
- Drive to chop shop, where stolen car is disassembled for parts.

Minimize risk of theft

Various risk mitigations

- Put car inside a locked residential garage.
- Use a steering wheel lock.
- Store fobs at home inside a **Faraday Cage**.

  $12 steel cash box on Amazon

  $9 metal envelope on Amazon

  Any metal box you have on hand.

THE END