Wireless Attack Vectors Against Automobiles

Written by Elijah DiGregorio 4/12/2024 Published by GainSec

Wireless based attacks have been and continue to be a major avenue for compromising the internal systems of vehicles. Attacks were first theorized in the early 2000s, but it wasn't until around 2010 that they began appearing in the wild, and it wasn't until 2015 or so that they had become truly widespread. These attacks account for an ever increasing percentage of both vehicle thefts and thefts from vehicles, as well as present other potential risks and dangers as both the systems and the attacks become more advanced. Modern automobiles present a uniquely challenging security landscape. A central issue is that most of the internal technologies of many vehicles' systems lack any real security, possessing neither authentication nor validation mechanisms. The continual addition of new technological features and assets are far outpacing the rate at which relevant security features are implemented, exacerbating the issue. Additionally, as technology becomes more readily available and more affordable, the likelihood and relative risk of attacks increase. There are currently a few common attacks used against automobiles, as well as several that are seen less often.

A vast majority of wireless attacks against vehicles target Remote Keyless Entry Systems, also known as RKES. RKES have been and continue to be a major attack vector for thieves, and it's happening for many reasons. They have become a common feature on automobiles over the past 15 or 20 years. RKES have significant security weaknesses, and as time progresses, the technology required to bypass their security has become much more affordable and available. Some of the tools are of legitimate use to a locksmith, and many of other tools are often advertised similarly. It's been a growing problem for almost 15 years, with attacks targeting RKES accounting for more and more vehicle theft as time goes on.

Attacks over time:

- 2014: Dominic Tobin, The Sunday Times:
  How Hi-Tech Thieves Are Defeating Keyless Car Security Systems
- 2016: Claims Journal:
  NICB Uncovers Abilities of Relay Attack Units Increasingly Used in Auto Thefts
- 2017: RTL-SDR.com:
  Using an RTL-SDR and RPITX to Defeat the Rolling Code Scheme Used on Some Subaru Cars
- 2018: KU Leuven, Research Group COSIC:
  Fast, Furious and Insecure: Passive Keyless Entry and Start in Modern Supercars
- 2021: WILX10; Onondaga, Michigan:
  Car thieves programming new key fobs
- 2022: CBS News:
  Security experts, police offer advice on how to prevent keyless car thefts

- 2022: Christopher Boyd, Malwarebytes:
  Car owners warned of another theft-enabling relay attack
- 2024: WUSA9, DC Metro Area:
  Thieves could use a key fob programming device to steal your car, police warn
  (references Autel tools, starts at 1:03)

Tools being sold:

- 2020: Motherboard (VICE):
  Meet the Guy Selling Wireless Tech to Steal Luxury Cars in Seconds

Places to buy tools:

- evanconnect.com
- keylessrepeatersonline.com
- Keylessrepeater.shop
- keylessgorepeater.com

"Tools for Locksmiths":

- Autel Scan Tool vendors:
  autel.com/us/where-to-buy/
- NitroScan Tools Diagnostic Systems vendors:
  nitroscantool.com/find-a-distributor/
- locksmithkeyless.com

Attacks on Locksmiths for tools:

- WREG Memphis Local News:
  Accused thieves target locksmiths, steal key programming machines
- CBS News:
  Chicago Car Thieves Now Target Locksmiths For Key Fobs and Programming Devices

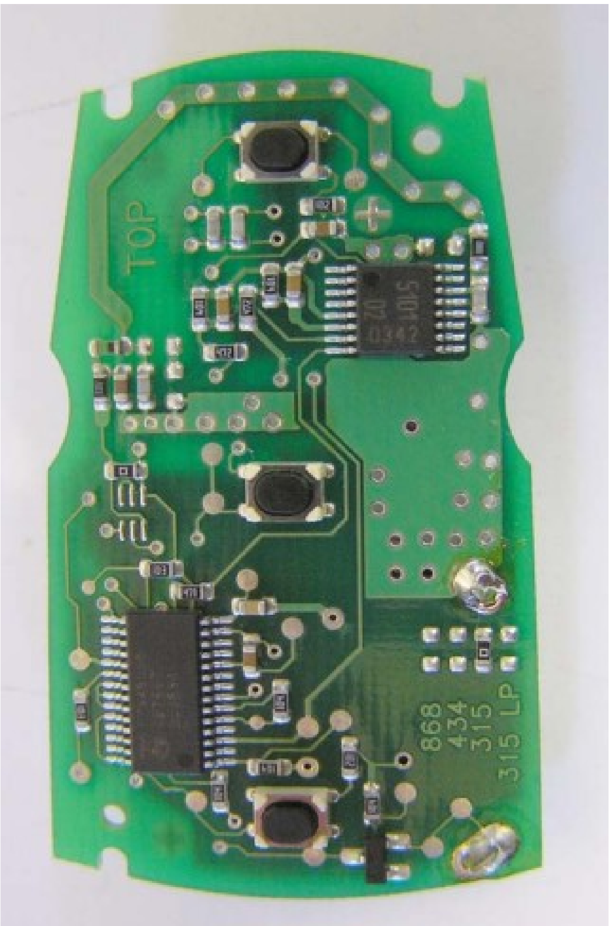
RKES have gone through many iterations. The first RKES was first patented in 1981 by Neimans, now called Valeo, a supplier in the automobile industry. Its first commercial release was on the 1982 Renault Fuego. It did not use Radio Frequency (RF) signals to unlock the vehicle, but instead it used an infrared (IR) data stream. The first implementation of an RF based key fob would come a few years later in 1985, with Rover being the first major brand to adopt the technology. However, the industry didn't switch over to RF key fobs as a whole until the 1990s. Additionally, they didn't implement rolling codes until 1990, and it wasn't until the mid 90s that they began to implement encryption. In 1998, Mercedes released the first RKES that added a keyless start function as standard equipment on their S-Class series of vehicles. This technology was developed by Siemens VDO, and prior to its release RKES could only unlock vehicles. An important note is that up until 2012, most key fobs could be easily reprogrammed by the user. In 2013 a change was made to require key fobs to be reprogrammed via the use of a computer and specialized software, usually through a dealership or a locksmith. In 2016 some companies began to opt to use Ultra Wide Band (UWB) by using cellphones in place of the traditional RKES key fobs, but that has not become a standard at the point of writing.

There are two types of RKES, Passive and Active, but they share some commonalities. When considering programming, all RKES use sets of predetermined rolling codes to try and avoid replay attacks. The validity of these codes is based on the code sent from the key fob itself. If the key fob and the vehicle end up at different positions on the list, the vehicle will verify the code sent from the key fob and then sync its position on the list to that of the key fob. Additionally, all RKES work on various challenge-response protocols, sending RF signals between the Body Control Module (BCM) in the vehicle and an RFID in the key fob. Most RKES key fobs contain similar hardware within their casings. They consist of a printed circuit board (PCB) with pre-programmed buttons, a microcontroller chip, button cell battery, a short-range radio transmitter, and varying combinations of different RFID chips. Nearly every RKES key fob will have an LF RFID chip, and any key fob that allows push button or passive start will also possess an RF RFID chip.

1: Example of Remote Keyless Entry System Key Fob

1a: Exterior

1b: Circuit Board Top Interior



1c: Circuit Board Bottom Interior

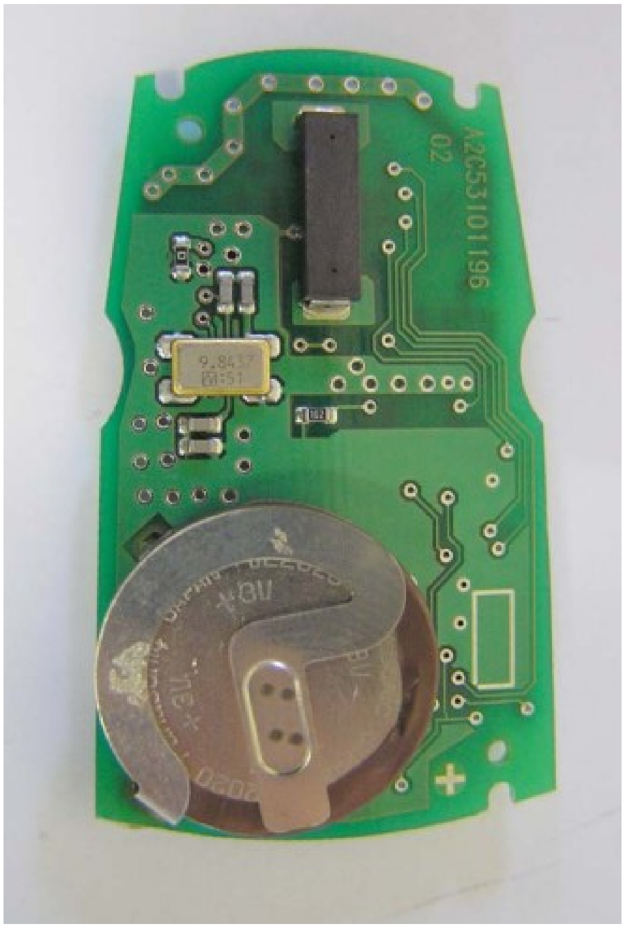
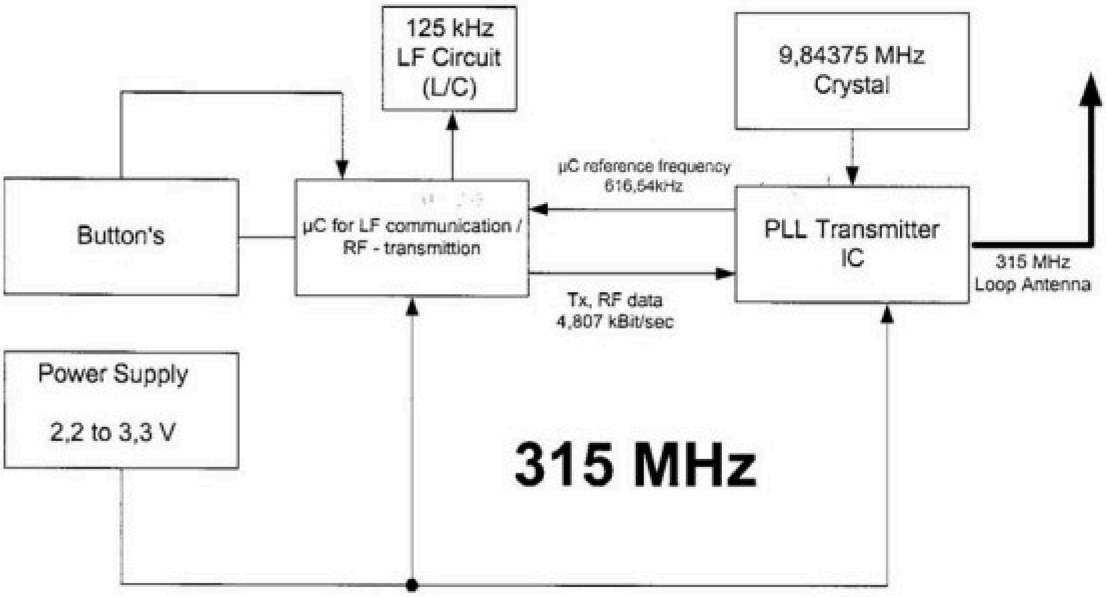


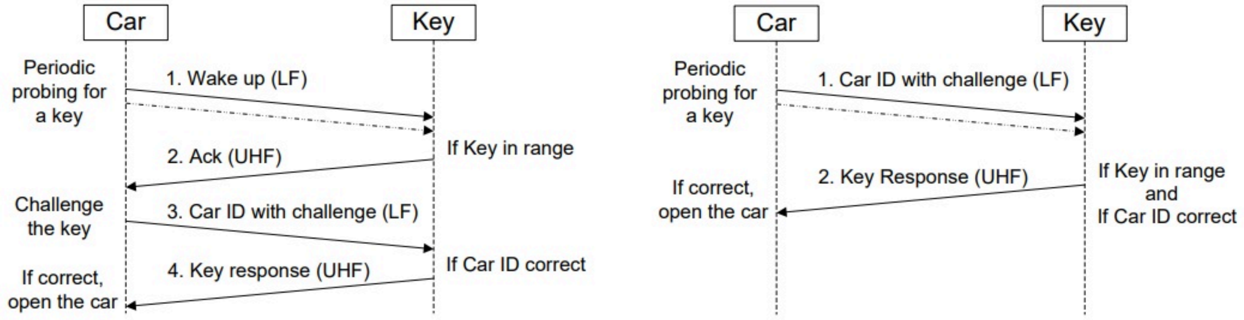
Fig 2: Technical Diagram of RKES Key Fob



Oscillator frequencies
generated or used
in the device: :   9.84375MHz / 315 MHz

The first kind of attack to discuss is the one that targets Passive Keyless Entry Systems (PKES). These systems are sometimes also called Passive Access Secure Entry (PASE). There are different PKES protocols, but they are all challenge-response protocols, and the end step of each protocol remains the same. The vehicle challenges with a Low Frequency (LF) RF signal and the key fob responds with the appropriate Ultra High Frequency (UHF) RF signal. Once the vehicle receives the signal, it unlocks the doors and turns off the engine immobilizer. The door systems are intended to work when the devices are within five meters or less of one another, and the ignition system is intended to work when the devices are within 30cm or less of one another. Included in this category are PKES that have a Passive Keyless Ignition System (PKIS). A PKIS allows for the ignition of the car to be started when a key fob is within proximity of the ignition. A PKES that includes PKIS is often referred to as Passive Entry Passive Start (PEPS) or Keyless Entry/Go.

Fig 3: PKES Challenge-Response Protocol Examples



The attack targeting PKES is called a Relay Attack or Two-Thief Attack, and the majority of PKES are vulnerable to it. It is the most common attack against vehicles, both currently and historically. These attacks use paired, full-duplex Software Defined Radio (SDR) transceivers to extend the functional range between vehicle and key fob to distances of up to 300 meters. In this scenario, one attacker is near the vehicle with the emitter, while another attacker is near the victim key fob with the receiver. The emitter takes the LF signal from the vehicle and upconverts the signal to increase the range, sending it to the receiver. The receiver then downconverts the signal back into its original LF signal and presents it to the key fob. The UHF signal response from the RFID within the key fob is then sent back to the vehicle, making the vehicle believe that the key fob is within the appropriate range.

Fig 4: PKIS Vehicle Ignition Challenge-Response Protocol Example

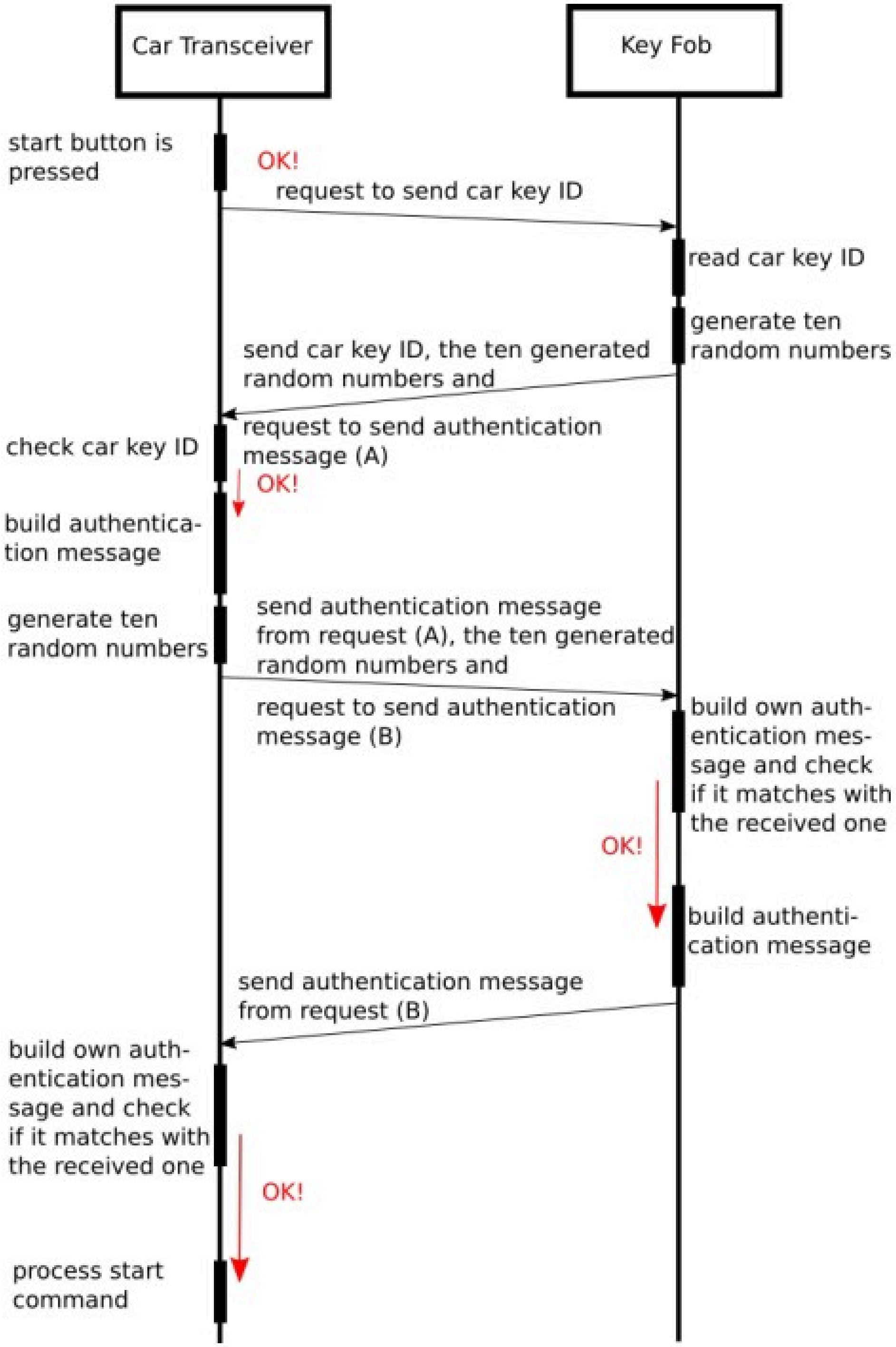
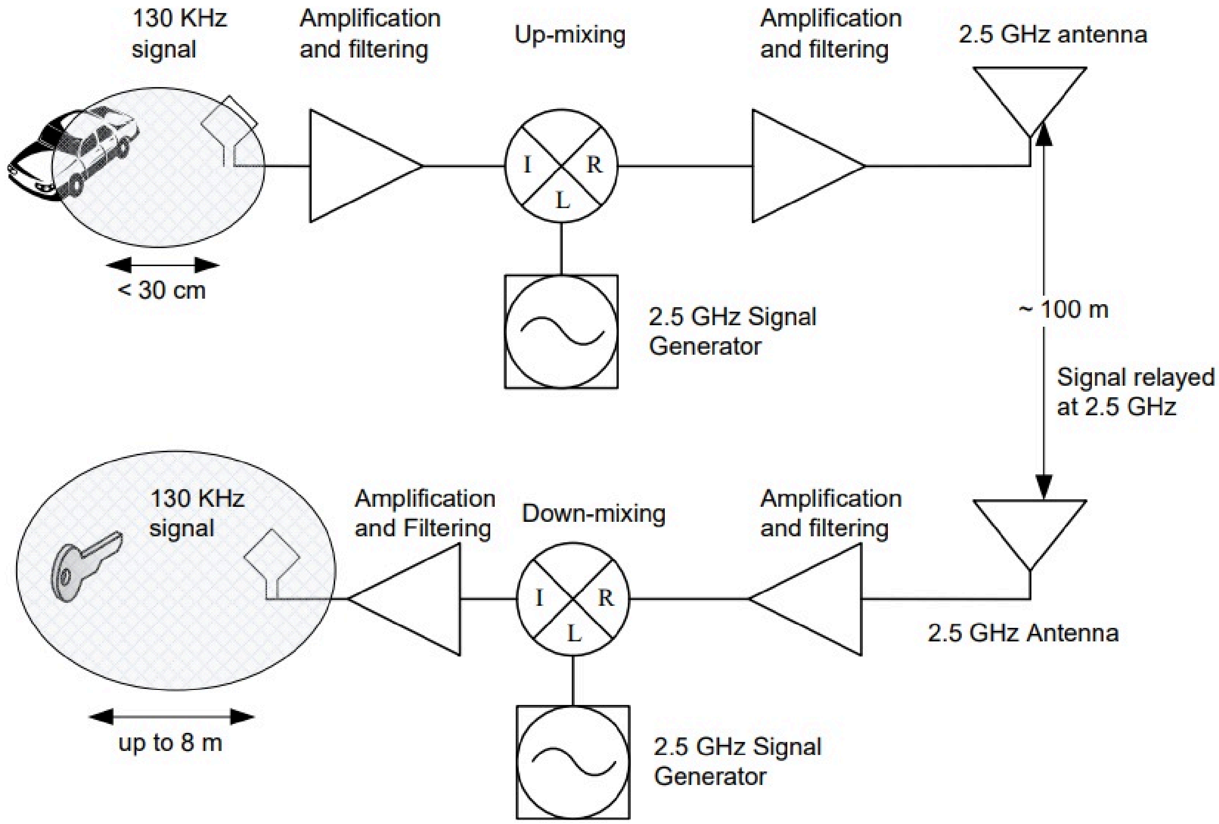
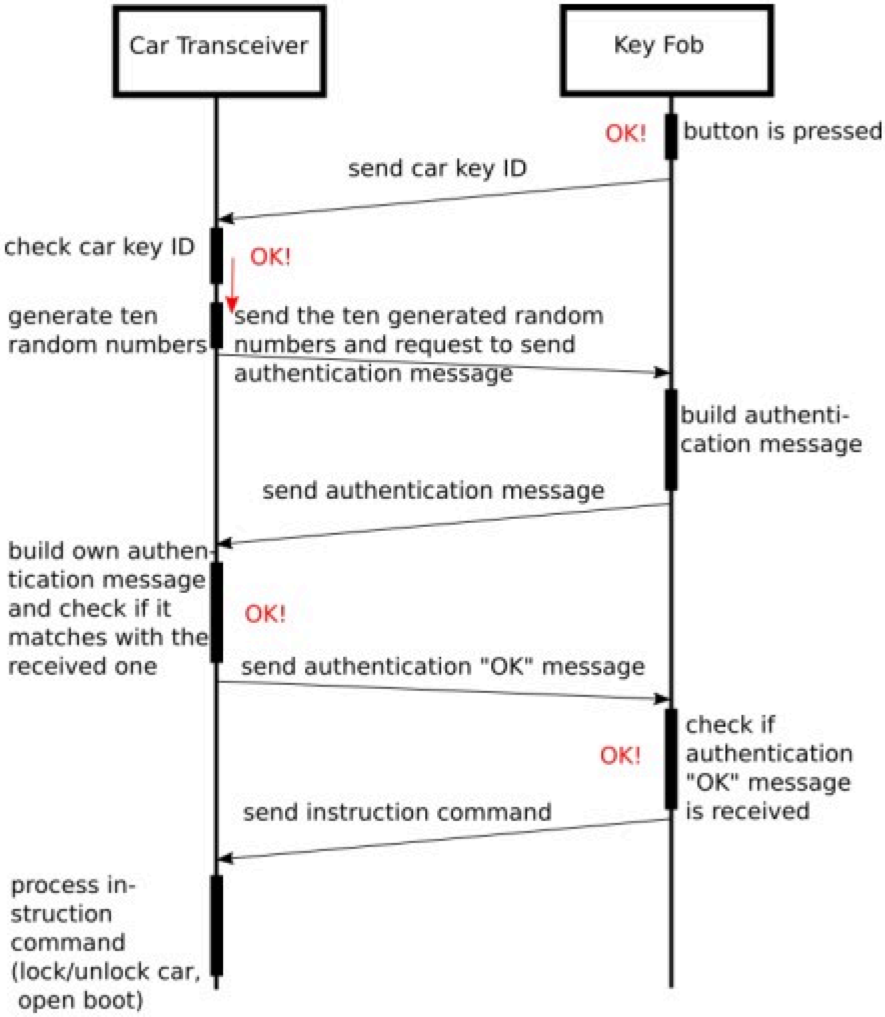

Car Transceiver
Key Fob
start button is pressed
OK!
request to send car key ID
read car key ID
generate ten random numbers
send car key ID, the ten generated random numbers and
request to send authentication message (A)
check car key ID
OK!
build authentication message
generate ten random numbers
send authentication message from request (A), the ten generated random numbers and
request to send authentication message (B)
build own authentication message and check if it matches with the received one
OK!
build authentication message
send authentication message from request (B)
build own authentication message and check if it matches with the received one
OK!
process start command

Fig 5: Diagram of Relay Attack against PKES



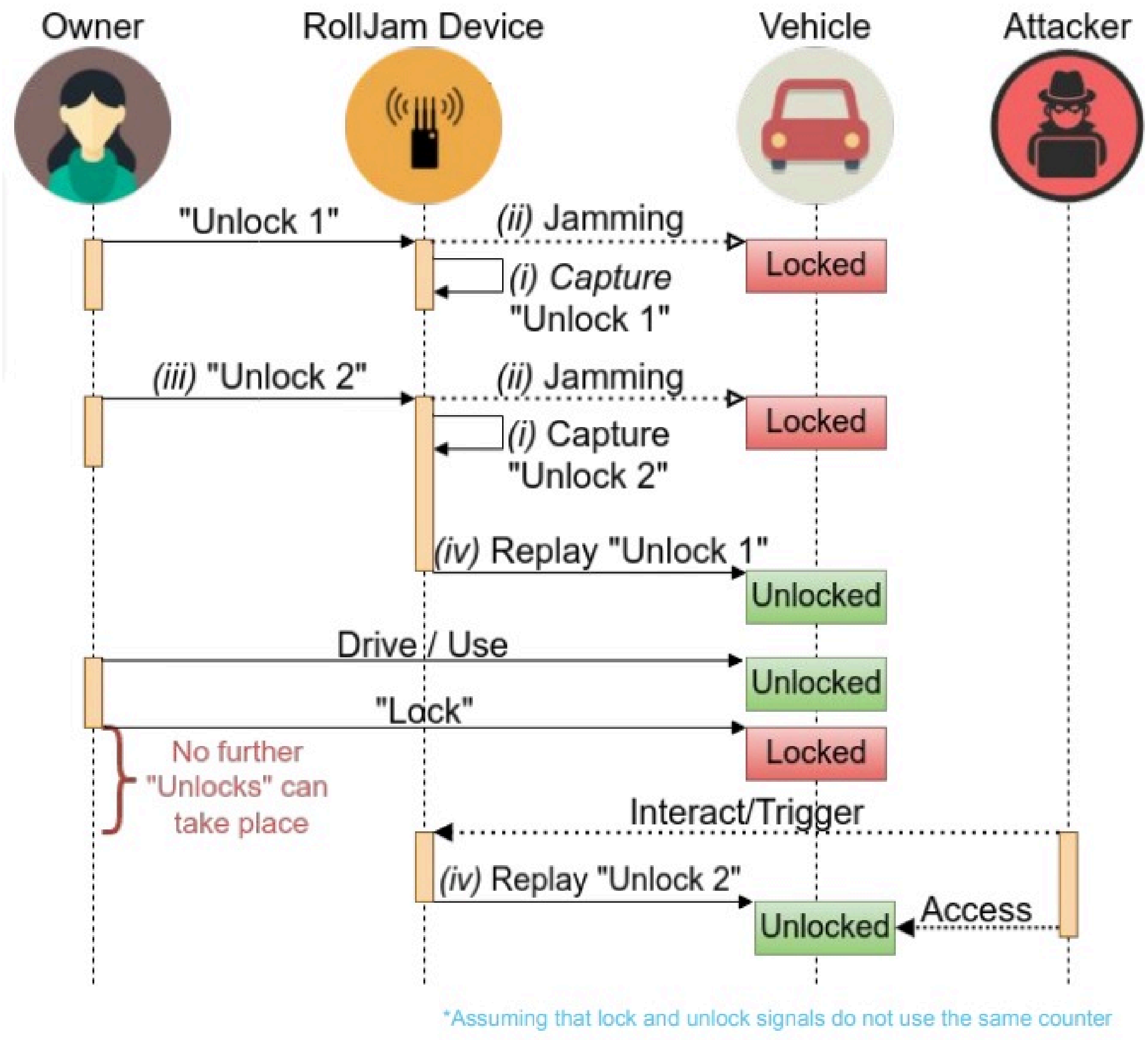
The second type of attacks to discuss are those targeting Active Keyless Entry Systems (AKES). AKES protocols function in a manner similar to PKES, but with the initial communication beginning with the press of a command button on the key fob. Following that, a series of messages are sent between the vehicle and the key fob to validate that the messages are legitimate. This authentication occurs on both sides of the exchange, and once complete, the instruction code is sent from the key fob to the vehicle. The codes are generally transmitted as [rolling code + command], with each button having its own set of rolling codes. Both of these attacks require either a full-duplex or two (2) half-duplex devices. Additionally, many modern AKES also include PKIS systems. This means that while the AKES themselves are not vulnerable to Relay Attacks, an attacker can potentially execute a Relay Attack against the ignition system if they manage to gain entry through other means

Fig 6: AKES Challenge-Response Protocol Example


Car Transceiver
Key Fob
OK!
button is pressed
send car key ID
check car key ID
OK!
generate ten random numbers
send the ten generated random numbers and request to send authentication message
build authentication message
send authentication message
build own authentication message and check if it matches with the received one
OK!
send authentication "OK" message
check if authentication "OK" message is received
OK!
send instruction command
process instruction command (lock/unlock car, open boot)

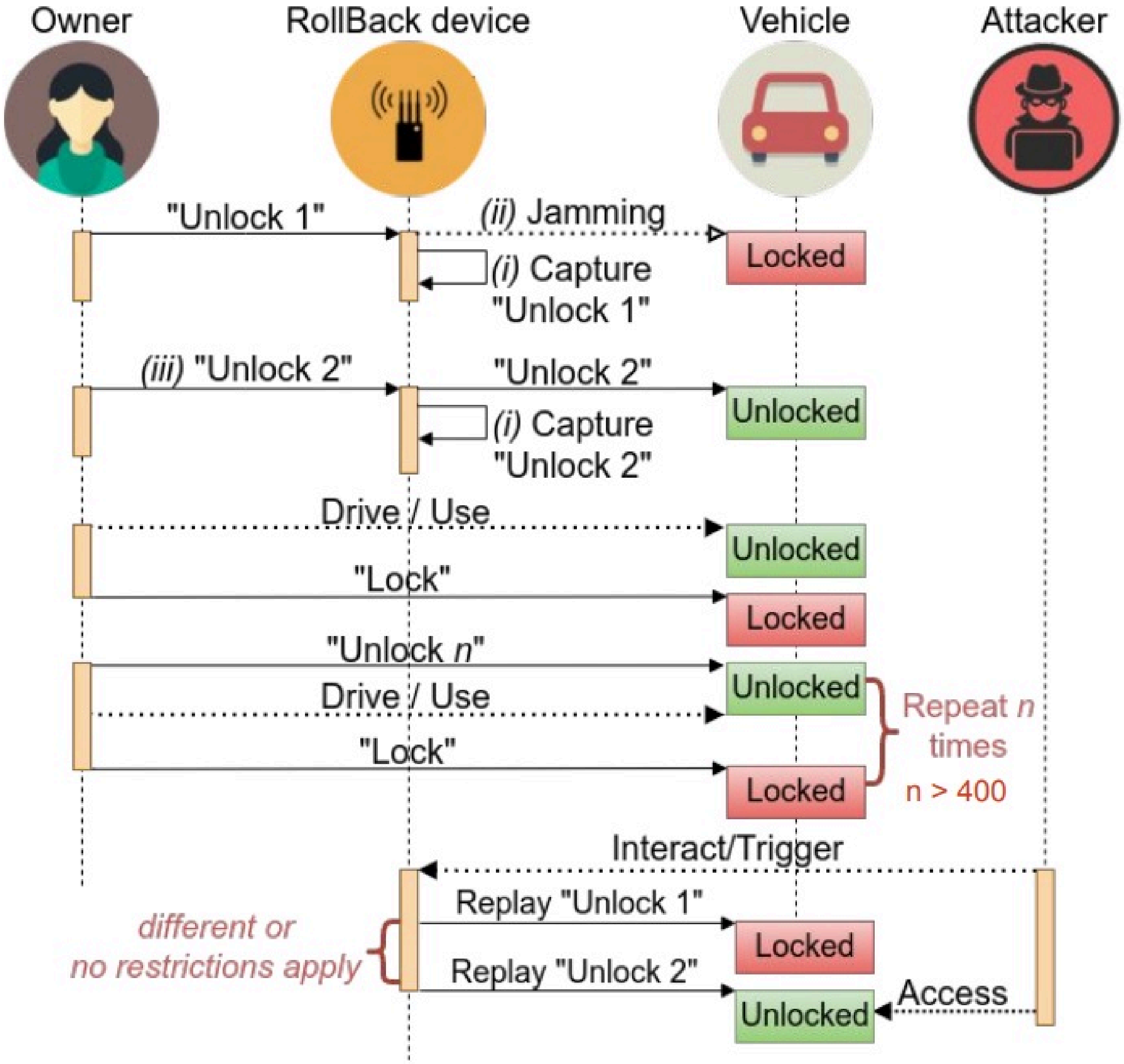
The first attack targeting AKES is RollJam, first introduced by Samy Kamkar in 2015. RollJam is a MitM type of replay attack, but it is an exploit of the safety provisioning, not an actual hack. It functions by using a device to jam the frequency used by a key fob while also recording the signal being sent by the key fob. By jamming the frequency, the vehicle cannot receive the signals from the key fob. After recording several button presses, the device then broadcasts the first message it intercepted to the vehicle. The car unlocks with the first code and the attacker now has several “future” codes that are still valid, but only as long as that key fob button is not pressed again before they are used.

Fig 7: RollJam Attack Diagram



The second attack is called RollBack, and it uses similar tooling and initial steps as RollJam, but much more effectively. RollBack was created in 2022 by Levente Csikor and Hoon Wei Lin, and they have called it a Time-Agnostic Re-Synchronization Attack. In this attack, multiple codes from the key fob are recorded for future use. In this example, an attacker will jam a key fob and collect a number of codes, but only the very last code collected will be sent prior to the exploit. At a later time the attacker can replay the series of codes in quick succession, starting with the first code collected. This will trigger the vehicle to reset its position on the list of rolling codes. The number of codes required to trigger this reset varies between manufacturers, but it is generally between two and five codes. The remaining codes that were collected and unused in the RollBack reset are once again valid. This attack is particularly effective because it can be done at any point in time, and can be reused multiple times, but only as long as the key fob has not been pressed more than 400 times since the collection of the codes.

Fig 8: RollBack Attack Diagram



There have recently been some stronger efforts to remediate these vulnerabilities, but the implementations are not consistent across the industry. There are many companies working on various solutions, but none of their works have truly come to the forefront as the de facto solution. Some companies have added sleep modes to PKES key fobs to prevent relay attacks by only allowing the RFID chip to respond to requests from the vehicle if the key fob is in motion. Some have added physical switches to their key fobs, allowing them to be turned off by the owner when not in use. A few companies have added MFA such as biometrics and keypads. Others have begun to switch their keyfobs from UHF frequencies to UWB frequencies, which is supposed to provide security through distance-bounding protocols. However, switching to UWB may prove to have its own shortcomings. UWB struggles to strike a balance between effective distance and security. There are already several potential attacks against UWB being discussed, as well as a few methods of improving security. One proposed method of preventing relay attacks was put forth by Wonsuk Choi, Minhye Seo, and Dong Hoon Lee in 2017. Their proposed system used sound comparisons between the vehicle and the user for proximity confirmation. Another approach to preventing relay attacks that was put forth in a patent designed by Lawrence Amadi and applied for by Ford in 2022. Amadi's patent uses a dual gait authentication to determine if the gait of the key fob holder matches the gait of the person approaching the vehicle, preventing access if the data does not correlate.

Since 2020, many companies have also begun to offer a Digital Key. Digital Keys utilize cellphones in place of the traditional key fob. Some Digital Keys mitigate the risk of relay attacks by using UWB frequencies paired with Bluetooth Low Energy (BLE) to measure secure ranging with Time of Flight (ToF) measurements. However, many Digital Keys just use BLE for communication. And while UWB with BLE is more resilient to relay attacks, BLE alone is very weak against relay attacks. Additionally, these keys are intended to be easily shared by the owner, and the strength of their security is predicated on the security settings of the cellphone and the awareness of the end users. It is quite obvious that using a cellphone instead of a key fob or car key introduces a multitude of new attack vectors, and potentially creates more issues than it solves.

There are also aftermarket solutions available to consumers. One of these is a simple pouch for the key fob that blocks RFID signals. Another system, manufactured by Firstech, is called the Secure Push-to-Start system (SPTS-U) and it acts as a type of 2FA for Push-to-Start vehicles. The SPTS-U is installed in a vehicle's wiring harness and blocks signals from the key fob to the ignition until the user validates themselves through an aftermarket remote. The major downside of the SPTS-U is that it requires all OEM alarms to be disabled for it to function properly, but it does not stop an attacker from using a relay attack to enter your car.

There is not a consensus on what the best solution is within the industry. While it will still take time to see widespread implementation of these security measures, the majority of cars on the road today are still vulnerable to these attacks. Looking at the potential solutions, I think that the simplest solutions are the best. A passive sleep mode or physical switch are fairly straightforward and effective, limiting the access to the vehicle by attackers. After that, I think that adding some form of MFA is probably the next best option, although it would most likely have an impact on the convenience of the RKES system. A programmable keypad with a lockout after a certain number of failures would be well-suited to the task, providing a reasonable level of supplemental security to the RKES system. While a fingerprint or retinal scan sounds good, the issue of balancing false positives against false negatives alone could create some very serious issues, either allowing unauthorized people access or denying legitimate users access to the vehicle.

The following are additional examples of attacks against vehicles using different avenues than the already discussed RKES vectors, though they are not currently as prevalent as the previously mentioned exploits. There are many systems, designs, and configurations and it is not widely known which peripheral systems and communications systems are currently exploitable. These systems may include Bluetooth, BLE, cellular (GSM) , WiFi, GPS, OnStar, or even the somewhat neglected V2X protocol

There is the 2020 hack of a Tesla Model 3 through its WiFi by researchers Ralf-Philipp and Benedikt Schmotzle. They used an attack dubbed 'TBONE' at PWN2OWN 2020. This attack allowed full control over the infotainment center, including doors, windows, stereo, and climate control. It also allowed modifications to 'steering and acceleration' modes, but did not result in driving control. Additionally, they say that if they had included a privilege escalation exploit, such as CVE-2021-3347, they would have been able to upload modified firmware and infect nearby Teslas in a manner similar to a worm. This error existed within the ConnMan service, which is a Connection Manager program made by Intel. When asked about the issues within ConnMan, Intel said they would not be making any changes to the program, indicating that they believed it was an issue with the implementation of the program. While Tesla has since fixed the issue, ConnMan is still used in other infotainment systems across the industry.

- 2021: Security Week: Tesla Car Hacked Remotely From Drone via Zero-Click Exploit

Another method of attack against Tesla PKES was discovered in 2022, this time using a traditional relay attack against Tesla's Bluetooth Low Energy (BLE) Phone-as-a-Key system. UK-based NCC Group discovered a new method of relay attacks against the BLE link-layer. Tesla acknowledged the existing weaknesses of their PKES system, but did not issue any updates or other statements. NCC Group recommended that vehicle owners disable their passive entry systems and use the PIN to Drive feature present in Teslas, which require a 4 digit PIN code to be entered inside the car before it can be started. This issue seemingly persists even today. In early 2024, security researchers Talal Haj Bakry and Tommy Mysk used an EvilTwin access point that mimicked a common Tesla network to perform a MitM attack on the Phone-as-a-Key system, allowing them to unlock and steal a Tesla.

- 2022: Tech Crunch: New Bluetooth attacks can remotely unlock Tesla vehicles and smart locks
- 2022: NCC Group: Technical Advisory - Tesla BLE Phone-as-a-Key Passive Entry Vulnerable to Relay Attacks
- 2024: BleepingComputer: MitM phishing attack can let attackers unlock and steal a Tesla

Another instance, occurring in 2022, involves specific year Mazdas (2014-2017) having their infotainment systems stuck in a repeating reset loop. This occurred to drivers in the Seattle area listening to 96.9 KUOW, and was apparently due to poor fault tolerance and a lack of ability to clear cached files. It is reported that the issue was caused by extensionless image files being transmitted via HD radio to the vehicles' Radio Data Systems (RDS). The system couldn't determine how to open the files, causing it to freeze and reboot. Upon rebooting, the extensionless files were still present and still unable to be processed, leading to a continuous cycle of death and rebirth. According to available reports, Mazda did not have a method to clear the data and simply opted to replace the Connectivity Master Units (CMU) of the affected vehicles. It is unclear whether there was ever a software update issued in response to this discovery. While this incident was not an intentional attack, it highlights the sensitivities and vulnerabilities that may exist in the underlying systems of our vehicles.

- 2022: The Verge: Mazdas head units are getting bricked by a local NPR station in Seattle

When looking at all the wireless attack vectors that have been exploited, and how those exploits have continued to both increase in frequency and evolve, it becomes clear that this is not a minor issue. The ever increasing amount of communications technology being added onto vehicles, and how that may add to the attack surface of a vehicle is worth taking note of as well. Finally, knowing that even unintentional or erroneous communications may have substantial impacts highlights the sensitivity and vulnerability of these technologies and how they are implemented in vehicles. Taking all of that into account, I think it is unlikely these attacks will stop being relevant any time soon unless serious effort, thought, and care are put into either solving or substantially mitigating them.

Other Common Tools:

- Fcc.io: Used to lookup FCC standards of devices. Can give frequency ranges and device schematics.
- HackRF One (Great Scott Gadgets): half-duplex transceiver; can be used to view, record, and replay signals; 1MHz - 6 GHz; requires computer connection for control and use
- HackRF One Portapack H2 (aftermarket)+: half-duplex transceiver; can be used to view, record, and replay signals; 1MHz - 6 GHz; fully contained device
- Flipper Zero: half-duplex transceiver; can be used to view, record, and replay signals; 300 MHz - 928 MHz (core)
- YARD Stick One (Great Scott Gadgets): half-duplex transceiver;can be used to view, record, and replay signals; *most* sub 1GHz frequencies; requires computer connection for control and use
- RTL-SDR + rtl_fm: SDR is the physical receiver and rtl_fm is the software used to record the signals; 500 KHz - 1766 MHz
- Ettus Research Devices: Top of the line transceivers; considered top notch in SDR
- GNU Radio (EttusResearch): Free & Open-source SDR software

Relevant Frequencies:

- RFID: Typical LF frequency is 125 KHZ; May range from 30 KHz to 500 KHz
- NFC: Typical RF frequency is 13.56 MHz; May range from 3MHz to 30 MHz
- Key Fobs: US: 315 MHz, 433.92 MHz - uses Amplitude Shift Keying (ASK)
  JP: 434.79 MHz - uses Frequency Shift Keying (FSK)
  EU: 868 MHz - uses Amplitude Shift Keying (ASK)
- UWB: 3.1 GHz -10.6 GHz
- Bluetooth/BLE: 2.4GHZ (2400 MHz - 2483.5 MHz)
- WiFi: 2.4 GHz, 5 GHz, 6 GHz
- RDS: RDS Data Stream: 57 KHz
  Monophonic Audio Signal: 15KHz
  Stereophonic Audio Signal: 23KHz to 53 KHz
- OnStar: System: 824 MHz - 855 MHz
  Base Transmitter: 824 MHz - 900 MHz
- Global System for Mobile Communications (GSM): 900 MHz - 1800 MHz
- GPS: Always transmits on at least 2 frequencies
  L1: 1575.42 MHz
  L2: 1227.6 MHz
  L5: 1176 MHz
- V2X (Vehicle-to-Everything): part of the 5.9 GHz Safety Band
  The 5.9 GHz Safety Channel

References:

Diagrams:

- Fig 3 & 5: ”Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars” Aurelien Francillon et al
- Fig 4 & 6: “A Protocol for a Secure Remote Keyless Entry System Applicable in Vehicles using Symmetric-Key Cryptography” Tobias Glucker et al
- Fig 7 & 8: “RollBack, A New Time Agnostic Replay Attack” Levante Csikor & Hoon Wei Lin; BlackHat USA 2022

Papers:

- "Requirements of Remote Keyless Entry (RKE) Systems" Analog.com
- ”Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars” Aurelien Francillon et al
- “A Protocol for a Secure Remote Keyless Entry System Applicable in Vehicles using Symmetric-Key Cryptography” Tobias Glucker et al
- "Tbone - A Zero-Click Exploit For Tesla Mcus" Ralf-Philipp Weinmann & Benedikt Schmotzle
- "Designing Next-Generation Key Fobs" Paul Lepek, Atmel
- “RollBack, A New Time Agnostic Replay Attack” Levante Csikor & Hoon Wei Lin; BlackHat USA 2022
- "Some Attacks Against Vehicles' Passive Entry Security Systems and Their Solutions" Ansaf Ibrahem Alrabady & Syed Masud Mahmud
- ”Cybersecurity challenges in vehicular communications” Zeinab El-Rewini et al
- "Roadmap for Cybersecurity in Autonomous Vehicles" Vipin Kumar Kukkala et al
- "Sound-Proximity: 2-Factor Authentication against Relay Attack on Passive Keyless Entry and Start System" Wonsuk Choi et al
- "Passive Entry Passive Start Verification with Two-Factor Authentication" Lawrence Amadi et al
- "United States Frequency Allocation: The Radio Spectrum" United States Depart of Commerce & National Telecommunications and Information Administration
- “The 5.9 GHz Safety Band” US Department of Transportation

Videos:

- DEF CON 23 - Samy Kamkar - Drive it like you Hacked it: New Attacks and Tools to Wireless
- RollBack - A New Time-Agnostic Replay Attack Against the Automotive Remote Keyless Entry Systems

Articles & Posts:

- "I Had No Idea The Renault Fuego Was The Car With This Huge Automotive First" Jadon Torchinsky, Jalopnik
- "Keyless Wonder: How Did We End Up With 'Smart' Wireless Keys For Our Cars?" James Mills, The Sunday Times
- "HOW IT WORKS; Remote Keyless Entry: Staying a Step Ahead of Car Thieves" Matt Lake, New York Times
- "The wireless design evolution of keyless entry systems in vehicles" Brian Fernandes, EDN
- Bypassing Rolling Code Systems" Andrew Nohawk
- "Reverse engineering a car key fob signal (Part 1)" Sami Alaoui Kendil, 0x44.cc
- "Hacking Car Key Fobs with a HackRF One Software-Defined Radio" Luciano Ferrari, LufSec

- ”Applying Ultra-Wideband Wireless Technology for Security and Automation” Deb Spitler, HID Global
- "Cybersecurity: who are the leaders in vehicle relay attack prevention for the automotive industry?" GlobalData
- "Digital Car Keys Step into Era of UWB" Shenzhen RF-star Technology Co., Ltd.
- "How secure is your vehicle with digital key technology?" Amber Pollick, Car Connectivity Consortium
- "Cars That Use Digital Keys in 2024" Chantel Wakefield, Kelley Blue Book
- "What’s the state of C-V2X?" Mark Lowenstein, Fierce Network
- "First Patent! Shuts the Door on Relay Attacks and Prevents Grand Theft Auto" Lawrence Amadi