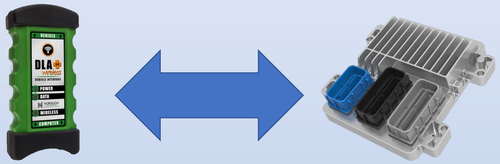
Seed-Key Security Exchange

Students: JOHN MAAG CHRISTOPHER REDING KELLY HOWELL
Advisor: DR. JEREMY DAILY

THE UNIVERSITY of TULSA
Student CyberTruck Experience

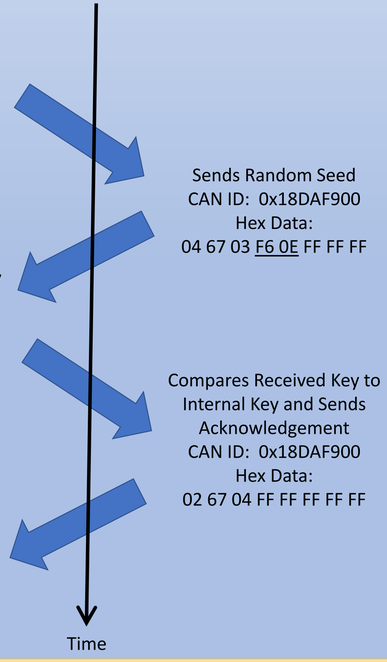
What is a Seed-Key Exchange?

A seed-key exchange is a sequence of network messages used in the automotive industry to verify a diagnostic device is communicating with an Electronic Controller Unit (ECU). The seed-key exchange process is used when diagnostic software wants to modify safety or emissions related features of the ECU.



Vehicle Diagnostics Adapter

Electronic Control Unit

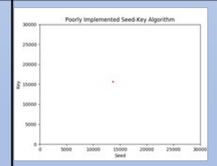
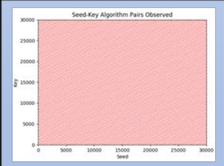
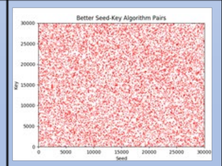


Shortcomings of Current Seed-Key Exchanges

A brute force attack may be possible because the range of the seeds was only 65,535 values. This is too few and the entire seed-key exchange can be determined in a matter of days using diagnostic computers.

Some instances of vehicles and products on the road today have an even smaller range, such as a single seed-key pair.

The some seed-key pairs show linear trends when graphed. However, good implementations of security algorithms produce keys that do not show patterns.

	Worst	Better	Ideal
Seed-Key Pairs Plotted			
Level of Security	• Only one seed key pair • Can be hacked in matter of minutes using a guess and check method. • Vulnerable to replay attacks.	• Current Industry Standard • This has a pattern, so the algorithm can be analyzed. • 16 bit pairs can be brute forced to collect pairs the 65,535 pairs.	• Theoretical look at how a good algorithm's pairs should look like. • No general pattern for analysis • More points = *Longer* to brute force
How To Improve	• Multiple seed-key pairs stops replay attacks.	• A longer seed and key would prevent easy brute forcing • Software stops generating keys after a number of failed attempts. • More sophisticated algorithm	• With enough time and resources, any device is hackable • Look to other industries for inspiration for solutions.

Seed-Key Improvements

A relatively easy way to increase the security of these exchanges would be to create a larger range of seed-key pairs. This would make brute forcing the algorithm a longer process, requiring more resources such as time and computing power.

The algorithm itself should be improved upon. Today, in computer security, there are many methods to creating secure, pattern less algorithms that would take supercomputers to derive. For example, basing an algorithm on the elliptic curve increases randomness.

Cracking an ECU's Seed-Key Exchange

Goal: Try to build a look-up table that contains all the seed-key pairs.

First, we impersonate an ECU and continuously send seeds, while recording keys from the diagnostics software.

Once all the seed-key pairs have been recorded, an external device can use the recorded pairs in a lookup table.

The external device, with the knowledge of the correct keys, now impersonate a diagnostic tool and affect the electronic control unit.

Experimental Hardware

- Beagle Bone – University of Tulsa Truck Cape
- RP1210 Compliant Vehicle Diagnostics Adapter Tool
- Heavy Vehicle ECM
- External 12v Power Supply