**EMCS2010: Applied Cryptography and Data Privacy**

Assignment: Vulnerabilities in the News

Brian Russel Davis, [brian\_davis@brown.edu](mailto:brian_davis@brown.edu)

(July 21, 2019 Sunday). Hyundai Motor Company (A005380) issued patent titled "Method of providing security for controller using encryption and apparatus thereof". News Bites - Asia: South Korea. Retrieved from <https://advance-lexis-com.revproxy.brown.edu/api/document?collection=news&id=urn:contentItem:5WM8-B0B1-JB4F-Y3JX-00000-00&context=1516831>.

This news story deals with a long and enduring vulnerability in cars. Most automotive operating systems are constructed in a way that are insecure and based on very old architecture. This patent by Hyundai seems to be a first step towards solving a long ignored problem.

According to the patent:

“A method of authenticating a controller by a gateway in a vehicle, comprising: transmitting a first symmetric key to the controller; generating a first one-time authentication value (OTAV), encrypting the first OTAV with the first symmetric key and delivering the encrypted first OTAV to the controller; sending a request for authentication using the first OTAV to the controller; receiving a hash value from the controller in response to the request, wherein the first symmetric key is encrypted using a third symmetric key corresponding to a session prior to a session in which authentication using the first OTAV is performed, and wherein the method further includes: determining a hash value using the first OTAV; comparing the received hash value with the determined hash value; and generating a second symmetric key when the received hash value is identical to the determined hash value; and authenticating the controller using a prestored certificate and public key when the received hash value differs from the determined hash value.”

It seems like the technology is pretty simplistic, but may be effective. By using three levels of symmetric encryption and hashing the controller which facilitates security leverages a very simple system to provide layers of protection. Just like the example we studied in class, it doesn’t take complex sophistication to create solid security. Many times it is the simple tried and testing techniques, applied in a modern context that make the best solution. At NASA there was a deep respect for these type of solutions. Consider for a moment that the first man on the moon was put there not by computers, but by the work of amazingly talented African American women using pencil and paper.

“Approximating a pathway made up of infinitely many points, by linking together a finite number of calculations, is an example of something called a numerical approach in mathematics. That's what Johnson's character in the movie means when she says Euler's Method works "numerically."

Euler's Method is one of the simplest of many numerical methods that now exist for solving differential equations.”[[1]](#footnote-0)

This “numerical” approach to math can be applied to cryptography. Simple, clean, solid state. I think the Hyundai patent is an example of this approach in action.

1. Meyers, C. (2017, March 03). Exploring the Math in 'Hidden Figures'. Retrieved July 21, 2019, from https://www.insidescience.org/news/exploring-math-hidden-figures [↑](#footnote-ref-0)