Quantum Computing – A Real Threat to the Automobile – Are We Prepared?

Kevin Link, Chief Strategy Officer, M2MD Technologies, Inc.

Defining a practical solution to the security challenges in the automotive industry is critical today as automakers continue to roll out remote control features like locking/unlocking and remote start. Security becomes even more paramount for the success of the autonomous car and related over-the-air software updates. Accordingly, the future vehicle communications will require un-hackable security that does not end up on the nightly news. Breaches and hacks will set the industry back and struggle to gain the required owner confidence for autonomous driving adoption. And now, research by some of the most prestigious and qualified cryptographers in the world is suggesting a new security threat is on the horizon – Quantum Computing. The U.S. National Security Agency (NSA) recently warned that the most common cryptography used today will soon be made obsolete by quantum computing. Is this a real threat to the automotive industry and are we prepared?

Quantum Computing Defined

The strength of any cryptographic algorithm is based on how computationally difficult the algorithm is and how long it would take to crack. In place of ordinary bits used by today's computers, quantum computers use 'qubits' that behave more efficiently by performing selected mathematical algorithms exponentially faster than a classical computer.[1] Quantum computers can tackle the most daunting of mathematical problems in less time and therefore leave most cryptographic algorithms insecure.

There is little doubt among the experts that quantum computing is coming and therefore a real threat to currently used cryptography methods - the debate is when. Experts from the NSA, U.S. Department of Defense Central Security Service (CSS), the U.S. National Institute of Standards and Technology (NIST), and Massachusetts Institute of Technology among others, have suggested dates as early as 2025. The NIST published a report on Post-Quantum Cryptography in April 2016 and concluded that organizations 'be prepared to transition away from these algorithms [public-key] as early as 10 years from now"[2] (see table below).

Security Basics

To understand the problem, we need to start with the basics on how the most common security standard – Transport Layer Security (TLS) using Public Key Infrastructure (PKI) and certificates is used to establish a secure session on the Internet. TLS and its predecessor Secure Sockets Layer (SSL) were established by various public, private, and governmental organizations to ensure the privacy and data integrity between two previously anonymous communicating

[1] Information Assurance Directorate, National Security Agency (NSA), MFQ U/00/815099-15, January 2016

[2] Report on Post-Quantum Cryptography (NISTIR 8105), National Institute of Standards and Technology, April 2016

applications/devices on the Internet. The TLS protocol is composed of two layers: (1) the TLS Handshake Protocol and (2) the TLS Record Protocol for transmission of data records.

The TLS Handshake Protocol typically allows the client to authenticate the server, agree on the exact cipher suite and generate cryptographic keys that will be used to protect the data that will be exchanged through the TLS Record Protocol. Optionally, adding a client certificate to the Handshake Protocol allows the server to authenticate the client, but this option is rare for secure Internet sessions. To facilitate the handshake process, the client encrypts a random secret using the server's public key and the server decrypts the random secret using the associated private key (known as public-key cryptography or asymmetric cryptography). Applications and devices that are anonymous to each other, such as your laptop and a banking website, must use public-key cryptography since neither have previous knowledge of each other prior to the session establishment. In this example, the bank's server provides a public key to every client device that attempts to securely communicate with it, and each client device uses that key to encrypt a secret message, which is a symmetric key used during the record portion, which transmits the data. Only the bank's server with its associated private key can decrypt this secret message. The strength of this public-key cryptography methodology relies on the computational difficulty for a private key to be determined from its corresponding public key – thus the threat quantum computing presents. Quantum computers can efficiently solve the cryptographic algorithms to determine the private key rendering all public key solutions vulnerable.

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	----------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Impact of Quantum Computing on Common Cryptographic Algorithms[2]

From the table published by NIST (above), the three-cryptographic algorithms that use public keys (as listed in the bottom three rows of the table) would no longer be secure given that "sufficiently large quantum computers will be built to break essentially all public key schemes currently in use."[2]

Given the potential availability of quantum computing as early as 2025, any industry with assets with long useful lives, e.g. an automobile, must address this threat now. Accordingly, an

automobile placed in service in 2018 with today's public key security becomes a target within its useful life.

Automotive Security Today

The automotive industry has received unfavorable attention of late given the recent vehicle hacks and the risk these security breaches pose to both driver and passengers. With the significant growth in the connected car and the investment in autonomous vehicles, the cellular connection found in an embedded telematics control unit (TCU) of a vehicle is the most vulnerable and largest attack surface. According to well-known security researchers Charlie Miller and Chris Valasek, this "telematics system is the holy grail of automotive attacks"[3] since the range is quite broad (i.e. the car's cellular connection has global reach). Another automotive security expert, Samy Kamkar, demonstrated his discovery of public-key cryptography deficiencies with the mobile app of four major automakers in August 2015.[4]

As a result of these weaknesses, the U.S. FBI, in coordination with the Department of Transportation and NHTSA issued a public service announcement in March 2016 "warning the general public and manufacturers – of vehicles, vehicle components, and aftermarket devices – to maintain awareness of potential issues and cybersecurity threats related to connected vehicle technologies in modern vehicles."[5] Automakers are responding to these threats and associated announcements but continue to rely on public-key cryptography methods in vehicles sold today – not solutions that address the long-term threats of quantum computing. This is a problem!

Consider the Facts

The research appears clear:

1. Quantum computing could be here as soon as 2025.
2. The NSA has advised that public key methods will not be secure after the advent of quantum computing.
3. The NSA is encouraging vendors to develop quantum-resistant protocols.

[3] Car & Driver, Hacking Duo Explores Scary Potential for Wireless Car Hacking, Names "Most and Least Hackable Cars", August 8, 2014

[4] DrivingSales.com, "Security Researcher Modifies Device to Hack BMW, Mercedes-Benz and Chrysler Vehicles", August 18, 2015.

[5] FBI Public Service Announcement, Motor Vehicles Increasingly Vulnerable to Remote Exploits, Alert I-031716-PSA, March 17, 2016

Solving the Security Problem

Symmetric cryptography is the oldest and best-known technique and is used by TLS Record Protocol, the transmission of data records (i.e., once the session initiation handshake is complete). For the TLS Handshake Protocol to use symmetric cryptography, both the client and the server must have prior knowledge of each other to have shared-secret keys. Symmetric encryption uses the same cryptographic material for encrypting and decrypting data. While symmetric-key methods can be used in the handshake process, experts are quick to point out that using symmetric-keys have one major challenge – the logistics of distributing, storing, and updating shared-secret keys over a potentially insecure communications channel, something impossible for two anonymous parties on the Internet. But automotive telematics systems are different and always have prior knowledge of each other.

The mobile phone industry has solved this problem. Today, mobile phones use symmetric-key cryptography to secure the network connection, with the keys generated and distributed by a SIM card. The SIM card has proven to be a very secure hardware element that cannot be physically or logically attacked for purposes of extracting the secret keys without destroying them. The secret key, also known as subscriber authentication key, is loaded securely in the SIM card at the time of manufacture and then loaded into the mobile network authentication center. This secret key is never used directly but is used to derive shared-secret working keys that are used in the session initiation handshake. These shared-secret keys are periodically updated to ensure ultimate security. If ever compromised, the subscriber authentication key can be updated using a separate secure side channel. Further, if any algorithm weakness is ever discovered, the cryptographic algorithms and even the operating system of the SIM card can be securely and remotely updated through the secure side channel to keep the application data secure. (The standards for wireless network security are defined by the collaboration of international telecom associations and documented as 3rd Generation Partnership Project (3GPP)).

Why has the automotive industry not followed the cellular industry in adopting symmetric-key cryptography methods? Enter M2MD Technologies.

The team at M2MD Technologies, previously the founders of Hughes Telematics (now Verizon Telematics), have created a method that provides the best of both TLS and 3GPP standards. The process is far more complicated than can be covered in this article, but the takeaway is that the process uses SIM-based symmetric secret-keys that can dynamically generate sufficiently large (by NIST's standards) shared-secret working keys as needed without the keys or other cryptographic inputs being transmitted across the network – thus, solving the only material challenge researchers describe with symmetric cryptography. In addition, the M2MD solution uses 1/20th of the data and simpler computations that increase server efficiency 23 to 1 over currently used public-key methodologies. To clarify, the M2MD solution does not use any credentials that belong to the Mobile Network Operator (MNO) and the solution does not require the MNO to share any secret data with either M2MD or the telematics operator.

The NEW Security Opportunity

As the largest segment of the IoT, the automotive industry has an opportunity to be both a pioneer and leader in security by introducing the first solution protected from the post quantum

computing era. The threat is real, and with the extended life of the automobile, which currently averages 11.5 years[6], the time is now.

Consider the new facts:

- Quantum Computing is real and on the horizon – as reported by the NSA.
- Symmetric Key Cryptography is the best choice for securing both the handshake and the record layer.
- Symmetric Key Cryptography is faster and less processor intensive than asymmetric (PKI) cryptographic methods.
- A SIM based approach to distribute and manage the secret keys solves the only downside to using symmetric cryptography.

The research is convincing, and the models have been built. M2MD Technologies has partnered with Giesecke & Devrient (G&D) to demonstrate the benefits of this solution. ***The first phase of testing is complete, and the results have confirmed there is a better method for security allowing the industry to be prepared for quantum computing.***

# # #

About the Author

Mr. Link is the Chief Strategy Officer for M2MD Technologies, Inc., a position he has held since joining M2MD in late 2016. Previously, Mr. Link was Co-Founder of Hughes Telematics and Senior Vice President and General Manager of China for Verizon Telematics. As a member of the Executive Team since its inception in 2006, Mr. Link served in various Strategic roles within the company. His most recent role included serving as Senior Vice President of Corporate Marketing and PR as well as the General Manager of the China operation. In these capacities, he was responsible for building the Hughes Telematics brand and served as the global spokesman for the company. Mr. Link was inducted into the TU Automotive Hall of Fame in 2016 and was also recognized as the Telematics Professional of the Year in China in 2015.

www.m2mdtech.com
Twitter: @M2MDTECH
LinkedIn: M2MD Technologies, Inc.
Media Contact: PR@m2mdtech.com

[6] Average Age of Automobile Breaks Record, USA Today, July 29, 2015.