M2MD Technologies, Inc.

Securely Connecting Machines to Mobile Devices

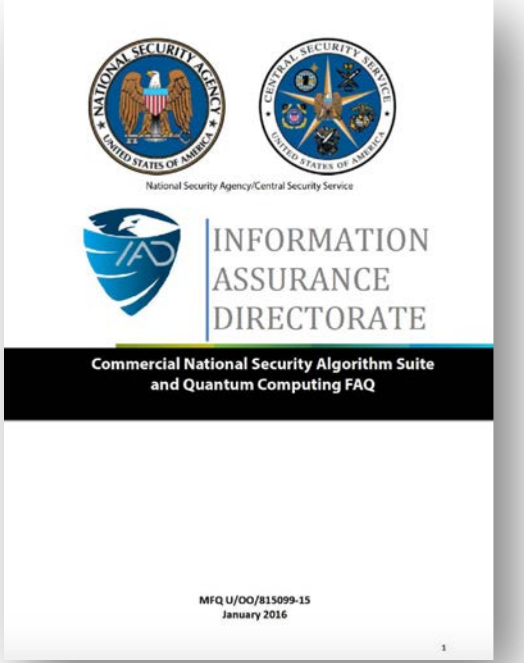
Security Facts Worth Knowing

June 2017

Security Facts Worth Knowing - A “Must Read” for Every Automotive Security Professional!

NSA’s Recent Security Directorate

“…sufficiently large quantum computers will be built to break essentially all public key schemes currently in use.”



National Security Agency/Central Security Service

INFORMATION
ASSURANCE
DIRECTORATE

Commercial National Security Algorithm Suite
and Quantum Computing FAQ

MFQ U/OO/815099-15
January 2016

1

[Link To Website - Search Quantum Computing FAQ]

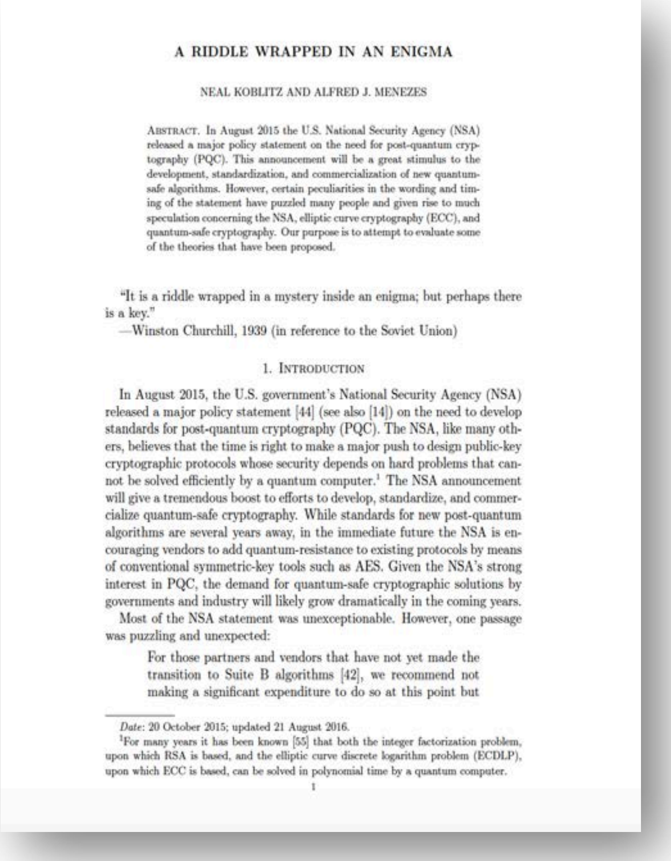
The research clearly warrants that everyone in the security business should evaluate the threat of Quantum Computing and make sure they are on the right course.

Recent Expert Research

Neal Koblitz
- Co-Creater of Elliptic Curve Cryptography (ECC)

Alfred Menezes
- Chairman of Centre for Applied Cryptographic Research
- Author of “Handbook of Applied Cryptography”

“The NSA seemed to be suggesting that practical quantum computers were coming so soon that people who had not yet upgraded from RSA to ECC should not bother to do so, and instead should save their money for the future upgrade to post-quantum protocols.”



A RIDDLE WRAPPED IN AN ENIGMA

NEAL KOBLITZ AND ALFRED J. MENEZES

Abstract. In August 2015 the U.S. National Security Agency (NSA) released a major policy statement on the need for post-quantum cryptography (PQC). This announcement will be a great stimulus to the development, standardization, and commercialization of new quantum-safe algorithms. However, certain peculiarities in the wording and timing of the statement have puzzled many people and given rise to much speculation concerning the NSA, elliptic curve cryptography (ECC), and quantum-safe cryptography. Our purpose is to attempt to evaluate some of the theories that have been proposed.

“It is a riddle wrapped in a mystery inside an enigma; but perhaps there is a key.”
—Winston Churchill, 1939 (in reference to the Soviet Union)

1. Introduction

In August 2015, the U.S. government’s National Security Agency (NSA) released a major policy statement [44] (see also [14]) on the need to develop standards for post-quantum cryptography (PQC). The NSA, like many others, believes that the time is right to make a major push to design public-key cryptographic protocols whose security depends on hard problems that cannot be solved efficiently by a quantum computer.[1] The NSA announcement will give a tremendous boost to efforts to develop, standardize, and commercialize quantum-safe cryptography. While standards for new post-quantum algorithms are several years away, in the immediate future the NSA is encouraging vendors to add quantum-resistance to existing protocols by means of conventional symmetric-key tools such as AES. Given the NSA’s strong interest in PQC, the demand for quantum-safe cryptographic solutions by governments and industry will likely grow dramatically in the coming years.

Most of the NSA statement was unexceptionable. However, one passage was puzzling and unexpected:

> For those partners and vendors that have not yet made the transition to Suite B algorithms [42], we recommend not making a significant expenditure to do so at this point but

---

Date: 20 October 2015; updated 21 August 2016.

[1] For many years it has been known [55] that both the integer factorization problem, upon which RSA is based, and the elliptic curve discrete logarithm problem (ECDLP), upon which ECC is based, can be solved in polynomial time by a quantum computer.

[Link To Article](#)

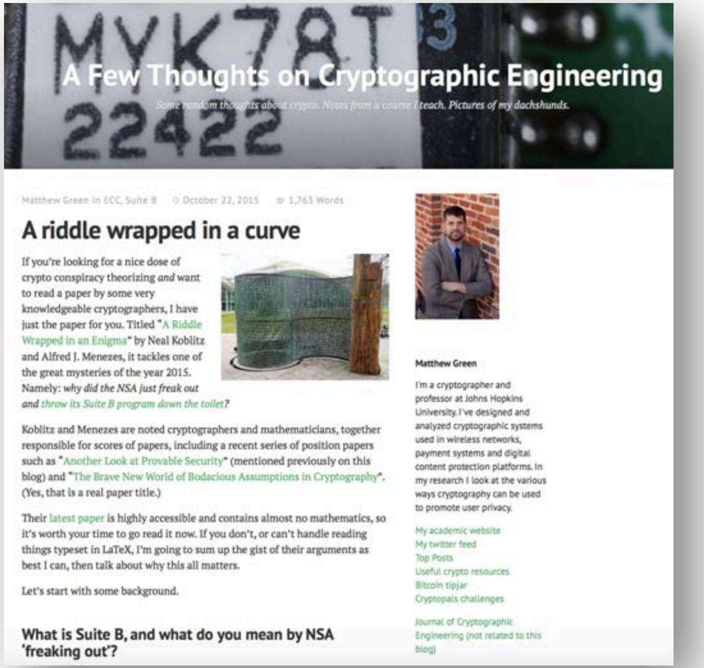
Does the NSA know something we don’t?

Recent University Research

Michael Green

- Cryptographer and Professor at Johns Hopkins University

“The NSA is freaking out…[perhaps] the NSA isn’t worried about quantum computers at all, but rather, that they’ve made a major advance in classical cryptanalysis of the elliptic curve discrete logarithm problem — and panic is the result.”



A Few Thoughts on Cryptographic Engineering

Some random thoughts about crypto. Notes from a course I teach. Pictures of my dachshunds.

Matthew Green in ECC, Suite B · October 22, 2015 · 1,763 Words

A riddle wrapped in a curve

If you're looking for a nice dose of crypto conspiracy theorizing *and* want to read a paper by some very knowledgeable cryptographers, I have just the paper for you. Titled "A Riddle Wrapped in an Enigma" by Neal Koblitz and Alfred J. Menezes, it tackles one of the great mysteries of the year 2015. Namely: *why did the NSA just freak out and throw its Suite B program down the toilet?*

Koblitz and Menezes are noted cryptographers and mathematicians, together responsible for scores of papers, including a recent series of position papers such as "Another Look at Provable Security" (mentioned previously on this blog) and "The Brave New World of Bodacious Assumptions in Cryptography". (Yes, that is a real paper title.)

Their latest paper is highly accessible and contains almost no mathematics, so it's worth your time to go read it now. If you don't, or can't handle reading things typeset in LaTeX, I'm going to sum up the gist of their arguments as best I can, then talk about why this all matters.

Let's start with some background.

What is Suite B, and what do you mean by NSA 'freaking out'?

Matthew Green

I'm a cryptographer and professor at Johns Hopkins University. I've designed and analyzed cryptographic systems used in wireless networks, payment systems and digital content protection platforms. In my research I look at the various ways cryptography can be used to promote user privacy.

My academic website
My twitter feed
Top Posts
Useful crypto resources
Bitcoin tipjar
Cryptopals challenges

Journal of Cryptographic Engineering (not related to this blog)

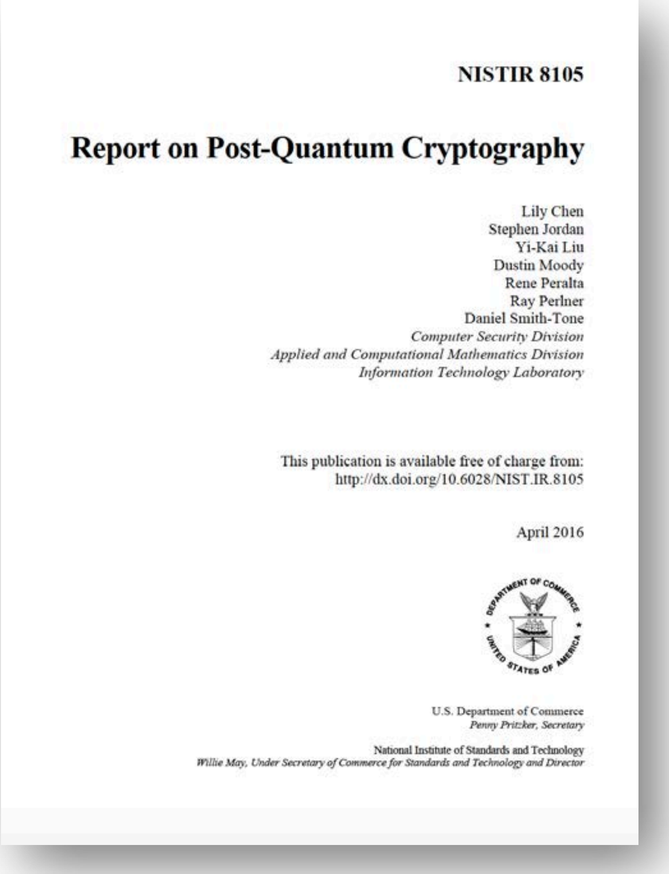
Link To Article

Regardless of the expressions used (Freaking Out) it is clear the NSA seems concerned.

Timing of Quantum Computing

National Institute of Standards and Technology
U.S. Department of Commerce

"…regardless of whether we can estimate the exact time of the arrival of the quantum computing era, we must begin now to prepare our information security systems to be able to resist quantum computing."



NISTIR 8105

Report on Post-Quantum Cryptography

Lily Chen
Stephen Jordan
Yi-Kai Liu
Dustin Moody
Rene Peralta
Ray Perlner
Daniel Smith-Tone
Computer Security Division
Applied and Computational Mathematics Division
Information Technology Laboratory

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.IR.8105

April 2016

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

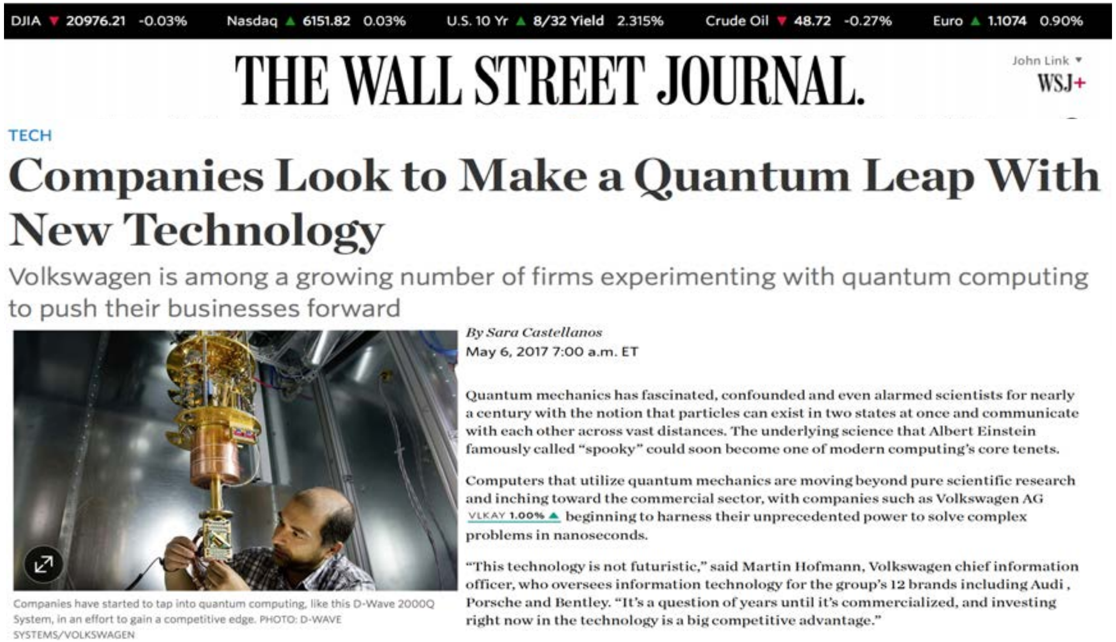
[Link To Publication](http://dx.doi.org/10.6028/NIST.IR.8105)

Given the average lives of vehicles, the industry should consider evaluating this threat now.

Timing of Quantum Computing

- “This technology is not futuristic,” said Martin Hofmann, Volkswagen chief information officer, who oversees information technology for the group’s 12 brands including Audi , Porsche and Bentley. “It’s a question of years until it’s commercialized, and investing right now in the technology is a big competitive advantage.”

- Companies including D-Wave Systems Inc. and IBM have been pioneering quantum computing, and experts say that within five years the technology could be powerful enough to solve new classes of problems that are currently beyond the grasp of even supercomputers.



DJIA ▼ 20976.21 -0.03% Nasdaq ▲ 6151.82 0.03% U.S. 10 Yr ▲ 8/32 Yield 2.315% Crude Oil ▼ 48.72 -0.27% Euro ▲ 1.1074 0.90%

THE WALL STREET JOURNAL.

TECH

Companies Look to Make a Quantum Leap With New Technology

Volkswagen is among a growing number of firms experimenting with quantum computing to push their businesses forward

By Sara Castellanos
May 6, 2017 7:00 a.m. ET

Quantum mechanics has fascinated, confounded and even alarmed scientists for nearly a century with the notion that particles can exist in two states at once and communicate with each other across vast distances. The underlying science that Albert Einstein famously called “spooky” could soon become one of modern computing’s core tenets.

Computers that utilize quantum mechanics are moving beyond pure scientific research and inching toward the commercial sector, with companies such as Volkswagen AG VLKAY 1.00% ▲ beginning to harness their unprecedented power to solve complex problems in nanoseconds.

“This technology is not futuristic,” said Martin Hofmann, Volkswagen chief information officer, who oversees information technology for the group’s 12 brands including Audi , Porsche and Bentley. “It’s a question of years until it’s commercialized, and investing right now in the technology is a big competitive advantage.”

Companies have started to tap into quantum computing, like this D-Wave 2000Q System, in an effort to gain a competitive edge. PHOTO: D-WAVE SYSTEMS/VOLKSWAGEN

[Link To Publication]

Even a top automaker believes Quantum Computing is a real threat.

What security methods are at risk?

M2MD
Technologies, Inc.

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

From the table published by NIST, Public Key Cryptographic Algorithms (e.g. Certificates) will no longer be secure with Quantum Computing.

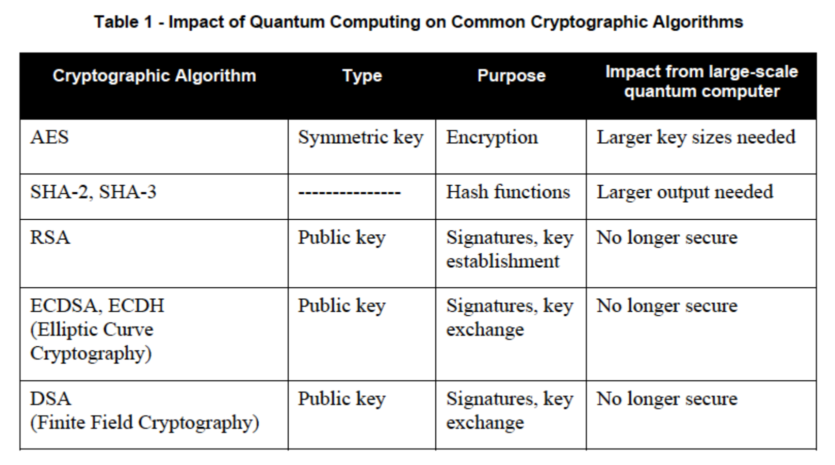


Table 1 - Impact of Quantum Computing on Common Cryptographic Algorithms

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

[Link To Report]

What security methods are at risk?

Information Assurance Directorate
MFQ U/OO/815009-15
January 2016

"The NSA stated that organizations that run classified or unclassified national security systems (NSS) and vendors that build products used in NSS…. should no longer use:"

- ECDH and ECDSA with NIST P-256
- SHA-256
- AES-128
- RSA with 2048-but keys
- Diffie-Hellman with 2048 keys

Link To Website - Search Quantum Computing FAQ

If the NSA is declaring that Public Key Cryptographic Algorithms are no longer secure– should we be worried?

Evaluation of Current Methodologies

“**Breaking News:** The cryptography that we all know and use, such AES-128, SHA-1 and SHA-256, RSA/DH, and the most commonly used elliptic curve P-256 (a.k.a. secp256r1) are NO LONGER wholeheartedly supported by the NSA. In fact most of these, if not all, are not quite recommended anymore. Link

“The industry’s usual recipe of waiting for catastrophe and then fixing it is very risky.” ~ MIT Technology Review, January 2017 Link

“For those partners and vendors that have not yet made the transition to Suite B elliptic curve algorithms, we recommend not making a significant expenditure to do so at this point but instead to prepare for the upcoming quantum resistant algorithm transition”. Link

NSA Says It “Must Act Now” Against the Quantum Computing Threat
~ *February 2015* Link

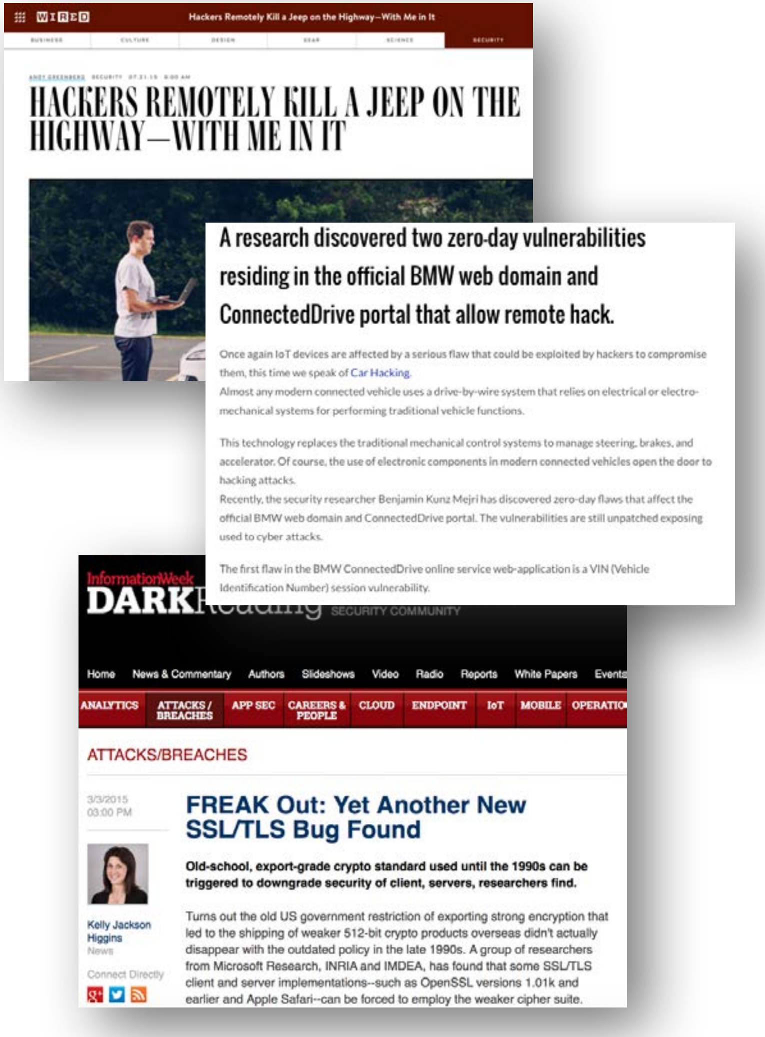
NSA advisory sparks concern of secret advance `ushering in cryptoapocalypse
~ *October 2015* Link

NSA Plans To Retire Current Cryptography Standards
~ September 2015
Link To Website - Search Quantum Computing FAQ

Experts are suggesting methods other than Public Key Infrastructure (PKI).

Security Headlines

- PKI and certificate operations were designed to secure two anonymous parties and are inefficient when the server knows the device.
- Certificate operations are computationally intensive, slow, and difficult on constrained devices.
- Certificate operations consume significant data and increase cost at every cellular session establishment.
- Certificates are susceptible to “private key” discovery, certificate expiration and certificate authority breaches. Revoking certificates on a private network is nearly impossible. If a certificate is compromised, the vehicle may have to be recalled.
- For IoT devices, certificates are typically stored insecurely in main-processor memory
- On average, a top-of-the-line server supporting certificate based security can support only 15,000 devices driving higher hardware costs and impacting scalability.


WIRED
Hackers Remotely Kill a Jeep on the Highway—With Me in It
BUSINESS
CULTURE
DESIGN
GEAR
SCIENCE
SECURITY
ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

A research discovered two zero-day vulnerabilities residing in the official BMW web domain and ConnectedDrive portal that allow remote hack.

Once again IoT devices are affected by a serious flaw that could be exploited by hackers to compromise them, this time we speak of Car Hacking.
Almost any modern connected vehicle uses a drive-by-wire system that relies on electrical or electro-mechanical systems for performing traditional vehicle functions.

This technology replaces the traditional mechanical control systems to manage steering, brakes, and accelerator. Of course, the use of electronic components in modern connected vehicles open the door to hacking attacks.
Recently, the security researcher Benjamin Kunz Mejri has discovered zero-day flaws that affect the official BMW web domain and ConnectedDrive portal. The vulnerabilities are still unpatched exposing used to cyber attacks.

The first flaw in the BMW ConnectedDrive online service web-application is a VIN (Vehicle Identification Number) session vulnerability.

ATTACKS/BREACHES

3/3/2015
03:00 PM

FREAK Out: Yet Another New SSL/TLS Bug Found

Kelly Jackson Higgins
News

Connect Directly

Old-school, export-grade crypto standard used until the 1990s can be triggered to downgrade security of client, servers, researchers find.

Turns out the old US government restriction of exporting strong encryption that led to the shipping of weaker 512-bit crypto products overseas didn't actually disappear with the outdated policy in the late 1990s. A group of researchers from Microsoft Research, INRIA and IMDEA, has found that some SSL/TLS client and server implementations--such as OpenSSL versions 1.01k and earlier and Apple Safari--can be forced to employ the weaker cipher suite.

PKI and Certificates have major issues.

Certificate Authority News

"Google, Apple and Mozilla will not recognize SSL/TLS certificates from WoSign and its affiliate StartCom in 2017."

"Google found that the certificate issuance policies and practices of Symantec (which acquired VeriSign's authentication division) from past several years are dishonest that could threaten the integrity of the TLS system used to authenticate and secure data and connections."

eWEEK

Why Browser Vendors Chose to Distrust 2 Certificate Authorities
~ *November 2016* Link

ars TECHNICA

Google Chrome to Distrust Symantec HTTPS Credentials after being caught miss-issuing 30,000 certificates.
~ *March 2017* Link

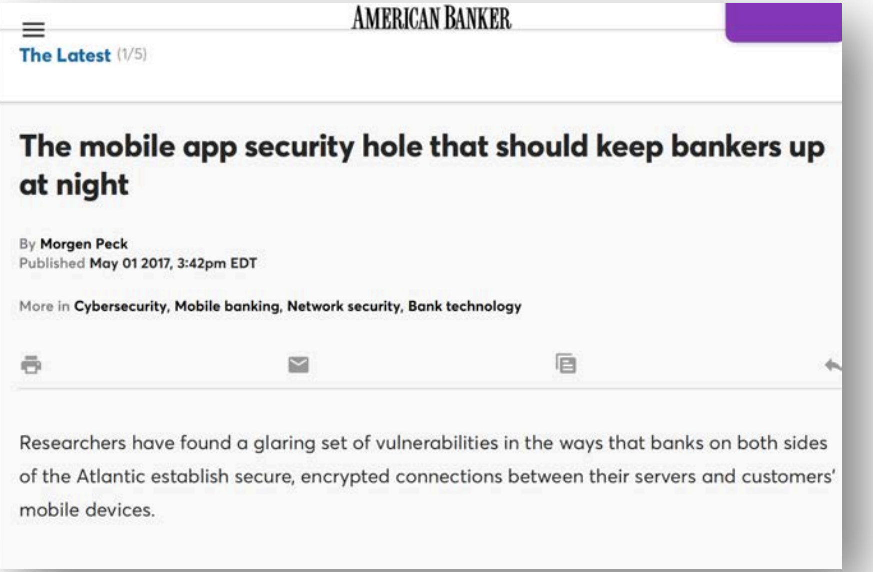
ZDNet

Google says a future update in Chrome will remove trust for all certificates from China's main root certificate authority ~ *April 2015* Link

Should we be worried if Google no longer trusts Symantec - which is the world's largest certificate authority with 38% market share?

Certificate Pinning in the News

The transport layer security, or TLS, protocols banks use to secure online banking sessions are as baffling as they are essential. They involve the participation of multiple entities—a bank's server, client-side validators, and security certificate authorities—all of which provide necessary reputational and cryptographic checks on the system. As complex as it is, TLS gets the job done, at least on web browsers. But mobile applications are another story altogether. The developers who build these apps are increasingly opting for simplified implementations, and recent blunders suggest that modifying TLS for mobile financial applications is much more difficult than it seems.



AMERICAN BANKER

The Latest (1/5)

The mobile app security hole that should keep bankers up at night

By **Morgen Peck**
Published **May 01 2017, 3:42pm EDT**

More in **Cybersecurity, Mobile banking, Network security, Bank technology**

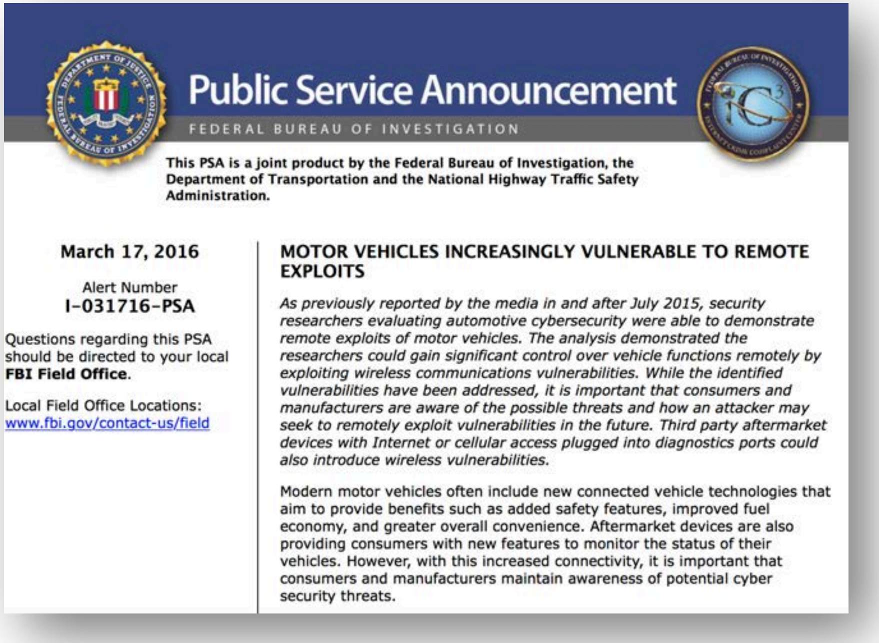
Researchers have found a glaring set of vulnerabilities in the ways that banks on both sides of the Atlantic establish secure, encrypted connections between their servers and customers' mobile devices.

"Google and Apple have lagged in their support and saddled developers with clumsy platforms."

Government Warnings

M2MD Technologies, Inc.

"…an attacker making a cellular connection to the vehicle's cellular carrier – from anywhere on the carrier's nationwide network – could communicate with and perform exploits on the vehicle…." Link



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

This PSA is a joint product by the Federal Bureau of Investigation, the Department of Transportation and the National Highway Traffic Safety Administration.

March 17, 2016

Alert Number
I-031716-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office.**

Local Field Office Locations:
www.fbi.gov/contact-us/field

MOTOR VEHICLES INCREASINGLY VULNERABLE TO REMOTE EXPLOITS

As previously reported by the media in and after July 2015, security researchers evaluating automotive cybersecurity were able to demonstrate remote exploits of motor vehicles. The analysis demonstrated the researchers could gain significant control over vehicle functions remotely by exploiting wireless communications vulnerabilities. While the identified vulnerabilities have been addressed, it is important that consumers and manufacturers are aware of the possible threats and how an attacker may seek to remotely exploit vulnerabilities in the future. Third party aftermarket devices with Internet or cellular access plugged into diagnostics ports could also introduce wireless vulnerabilities.

Modern motor vehicles often include new connected vehicle technologies that aim to provide benefits such as added safety features, improved fuel economy, and greater overall convenience. Aftermarket devices are also providing consumers with new features to monitor the status of their vehicles. However, with this increased connectivity, it is important that consumers and manufacturers maintain awareness of potential cyber security threats.

Link to Announcement

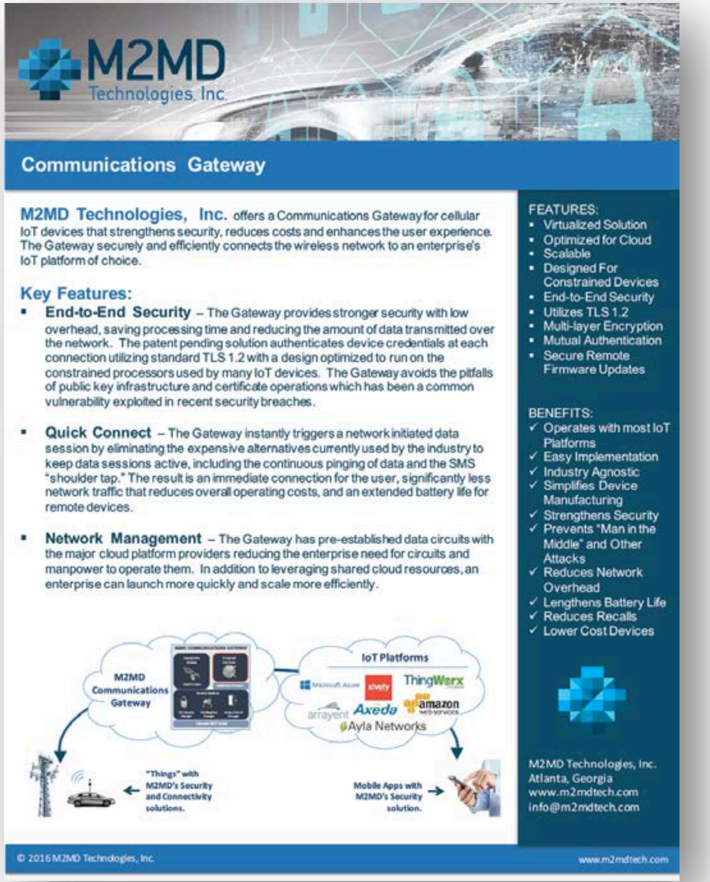
Even the FBI has issued announcements about cybersecurity threats.

As suggested by the U.S. National Security Agency – now is the time to look beyond traditional security methods for IoT devices.

A Proven Solution is Here.

Industry veterans, M2MD Technologies, have developed an innovative security solution using the best of 3GPP and TLS 1.2.

- ✓ Solid Security without pitfalls of Certificates
- ✓ Protected from Quantum Computing
- ✓ 23 times more server efficient
- ✓ 20 times more data efficient
- ✓ No Public Keys
- ✓ Works with any Hardware/TCU
- ✓ Works with any telematics platform
- ✓ Works with any carrier (Mobile Network Operator)



M2MD Technologies, Inc.

Communications Gateway

M2MD Technologies, Inc. offers a Communications Gateway for cellular IoT devices that strengthens security, reduces costs and enhances the user experience. The Gateway securely and efficiently connects the wireless network to an enterprise's IoT platform of choice.

Key Features:

- **End-to-End Security** – The Gateway provides stronger security with low overhead, saving processing time and reducing the amount of data transmitted over the network. The patent pending solution authenticates device credentials at each connection utilizing standard TLS 1.2 with a design optimized to run on the constrained processors used by many IoT devices. The Gateway avoids the pitfalls of public key infrastructure and certificate operations which has been a common vulnerability exploited in recent security breaches.
- **Quick Connect** – The Gateway instantly triggers a network initiated data session by eliminating the expensive alternatives currently used by the industry to keep data sessions active, including the continuous pinging of data and the SMS "shoulder tap." The result is an immediate connection for the user, significantly less network traffic that reduces overall operating costs, and an extended battery life for remote devices.
- **Network Management** – The Gateway has pre-established data circuits with the major cloud platform providers reducing the enterprise need for circuits and manpower to operate them. In addition to leveraging shared cloud resources, an enterprise can launch more quickly and scale more efficiently.

M2MD Communications Gateway
IoT Platforms
Microsoft Azure
xively
ThingWorx
arrayent
Axeda
amazon web services
Ayla Networks
"Things" with M2MD's Security and Connectivity solutions.
Mobile Apps with M2MD's Security solution.

FEATURES:
- Virtualized Solution
- Optimized for Cloud
- Scalable
- Designed For Constrained Devices
- End-to-End Security
- Utilizes TLS 1.2
- Multi-layer Encryption
- Mutual Authentication
- Secure Remote Firmware Updates

BENEFITS:
- ✓ Operates with most IoT Platforms
- ✓ Easy Implementation
- ✓ Industry Agnostic
- ✓ Simplifies Device Manufacturing
- ✓ Strengthens Security
- ✓ Prevents "Man in the Middle" and Other Attacks
- ✓ Reduces Network Overhead
- ✓ Lengthens Battery Life
- ✓ Reduces Recalls
- ✓ Lower Cost Devices

M2MD Technologies, Inc.
Atlanta, Georgia
www.m2mdtech.com
info@m2mdtech.com

www.m2mdtech.com

Link to Details

Related M2MD Technologies Articles:

- ➢ Security – Where Do You Focus   Link to Article
- ➢ Quantum Computing – A Real Threat to the Automobile   Link to Article

About M2MD Technologies

Our Story

- Significant experience in cellular IoT – specifically with the connected car.
- Realized that many IoT applications lacked adequate security.
- Saw the need for faster and cheaper cellular data connectivity techniques.
- Experienced the need for seamless cellular data connectivity allowing for multiple party billing when roaming.
- Appreciated automakers request for a global solution.

Our Company

- ✓ Developed solutions that address multiple cellular IoT challenges: security, cost, user experience and automotive data heavy applications.
- ✓ Unique security application leveraging TLS while avoiding pitfalls of certificates (where the hacks have occurred).
- ✓ Cellular connectivity techniques that are faster and don’t depend on SMS or continuous device pinging.
- ✓ Global Data System allowing consumers to add their automobile to their existing data plan.

Comprehensive Security

Efficient Use of Resources

Enhanced User Experience

Contact Information

M2MD
Technologies, Inc.

www.m2mdtech.com

#M2MDTech

Linkedin/m2mdtech