OEM Cyber Security Layout Report, 2020

December 2020

ResearchInChina
www.researchinchina.com

STUDY GOAL AND OBJECTIVES

This report provides the industry executives with strategically significant competitor information, analysis, insight and projection on the competitive pattern and key companies in the industry, crucial to the development and implementation of effective business, marketing and R&D programs.

REPORT OBJECTIVES

- To establish a comprehensive, factual, annually updated and cost-effective information base on market size, competition patterns, market segments, goals and strategies of the leading players in the market, reviews and forecasts.
- To assist potential market entrants in evaluating prospective acquisition and joint venture candidates.
- To complement the organizations' internal competitor information gathering efforts with strategic analysis, data interpretation and insight.
- To suggest for concerned investors in line with the current development of this industry as well as the development tendency.
- To help company to succeed in a competitive market, and

METHODOLOGY

Both primary and secondary research methodologies were used in preparing this study. Initially, a comprehensive and exhaustive search of the literature on this industry was conducted. These sources included related books and journals, trade literature, marketing literature, other product/promotional literature, annual reports, security analyst reports, and other publications. Subsequently, telephone interviews or email correspondence was conducted with marketing executives etc. Other sources included related magazines, academics, and consulting companies.

INFORMATION SOURCES

The primary information sources include Company Reports, and National Bureau of Statistics of China etc.

Abstract

Research into automotive cyber security: server and digital key are the ports vulnerable to attacks, for which OEMs have stepped up efforts in cyber security.

With advances in the CASE (Connected, Autonomous, Shared, and Electrified) trend, cars are going smarter ever with functional enrichment. Statistically, the installation rate of telematics feature to new cars in China is over 50% from January to October of 2020, a figure projected to rise to 75% or so in 2025. In terms of functionality, intelligent cockpit and advanced automated driving become trending, and the features such as multi-modal interaction, multi-display interaction, 5G connectivity, V2X, OTA and digital key finds ever broader application alongside the soaring number of vehicle control codes and more port vulnerabilities to safety threat.

Currently, the automotive cyber security events arise mainly from attacks on server, digital key, mobile APP, OBD port among others.

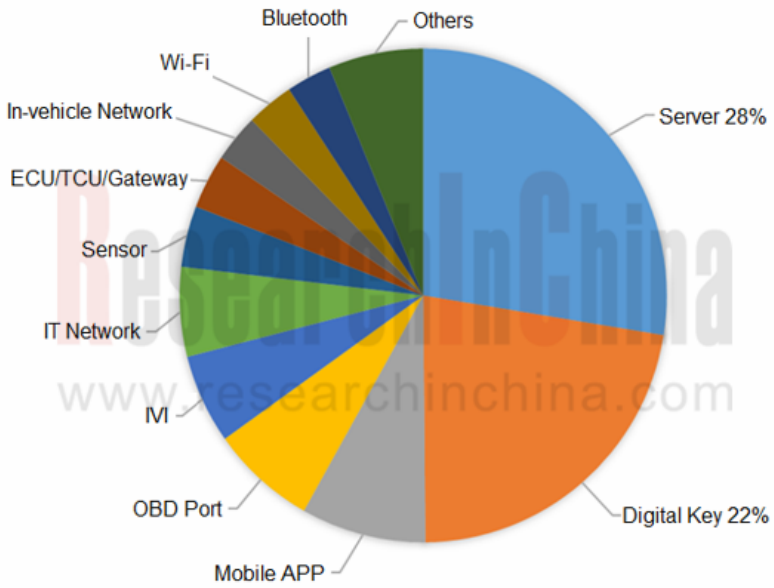
Server acts as the most important port for cyber security, which is exposed to the attack by hackers on operating system, database, TSP server, OTA server and the like, thus issuing in data tampering, damage and vehicle safety accidents. Most tools of assault on servers are remotely accessible with lower costs, while the data storage over servers is of paramount importance, all of which lead to often a rather high share of attacks on servers.

Digital key, as the second port that matters most to cyber security, is a common media subject to vehicle intrusion and theft. In 2020, there will be 300,000 Bluetooth digital key installs in China, coupled with an installation rate at about 4%, with such more functionalities besides lock/unlock & start as account log-in, key sharing, vehicle trajectory record, and parcel delivery to cars, which has ever more implications on vehicle safety.

Different auto brands are subject to varied attack on vehicle security.

The smarter a car is, the more vulnerable to security attacks will be. Amid the intelligence trend, all OEMs, whatever Mercedes-Benz, BMW, Audi, VW, Toyota, Honda or Hyundai, have varied exposure to security attacks.

Global Automotive Cyber Security Incidents by Ports as of 2020



Source: upstream.auto; ResearchInChina

Cyber Security Incidents of Some OEMs, 2018-2020

OEM	Time	Field	Event
Mercedes-Benz	2019	APP	Car2Go App was hacked, and some 100 cars were stolen.
	2019	User data security	User data leaked due to security vulnerabilities of APP program over IOS platform.
	2020	Communication security	A recall of 9,765 Benz cars from the Chinese market due to communication module software problem.
BMW	2019	Server	Vietnamese APT Group hacked the networks of BMW, which led to shutdown of the compromised computer.
Audi	2018	IVI	Security researchers have found several vulnerabilities in the infotainment system of some Audi models, allowing them to remotely access the system.
	2019	Car club website	Vulnerabilities in car club website resulted in car owner information leakage.
VW	2018	IVI	White hat hacker found remote code execution vulnerabilities in MIB module of IVI of VW Golf GTE.
	2020	IVI	Security company found vulnerabilities in traction control module of VW Polo SEL TSI manual 1.0L.
Toyota	2019	Server	Toyota data breach in Australia branch and Japan exposed personal information on 3.1 million customers.
	2019	AVN (Audio Video Navigation)	Keen Security Lab of Tencent discovered four security breaches in 2017 Lexus NX300.
	2020	DST80 encryption system	White hat hacker obtained car key via Digital Signature Transponder.
Honda	2018	Server	Honda Car India stored customer data on two unsecured AWS servers, exposing personal details of 50,000 users to data theft.
	2020	Server	Honda suffered an Ekans ransomware attack, which inflicted Honda's global operations.
Hyundai	2020	DST80 encryption system	Researchers found that it was able to access car key via Digital Signature Transponder.

Source: ResearchInChina

In March 2020, key encryption approaches of OEMs like Toyota, Hyundai and KIA were reported to have limitations with a possibility of intrusions and thefts largely due to the vulnerabilities of TI's DST80 encryption system employed by them. A hacker just stands near the car that packs DST80 remote control key, using the inexpensive Proxmark RFID reader/transmitter for the 'identity theft' of the key and thus getting the encrypted information.

Make	Period	Model
Toyota	2009-2013	**Auris (2011)**
	2010-2013	Camry
	2010-2014	Corolla
	2011-2016	FJ Cruiser
	2009-2015	Fortuner
	2010+	Hiace
	2008-2013	Highlander
	2009-2015	**Hilux (2014)**
	2009-2015	Land Cruiser
	2011-2012	RAV4
	2010-2014	Urban Cruiser
	2011-2013	Yaris
Tesla	06/2018-07/2019[1]	**Model S (2018)**

Make	Period	Model
Kia	2012+	**Ceed (2016)**
	2014	**Carens (2014)**
	2011-2017	Rio
	2013+	Soul
	2013-2015	Optima
	2011+	Picanto
Hyundai	2008+	I10
	2009+	I20
	2009+	I20
	2010+	Veloster
	2016	**IX20 (2016)**
	2013	**I40 (2013)**

OEM quicken their presence in cyber security

To address serious challenges in automotive cyber security, the OEMs are sparing no efforts in security improvement in many aspects: a) information management inside the company and optimization of R&D process; 2) to build a team intended for cyber security; 3) cyber security protection of telematics.

➢ **European and American OEMs: Diversified deployments of cyber security protection**

The automakers from Europe and America are pushing ahead with cyber security construction roundly with technical superiorities, with a tightened control on information security management inside the company apart from improvements in cyber security protection of telematics. As concerns team construction, the majority of European and American OEMs as usual set up either an independent cyber security division or a subsidiary to ensure information security during a vehicle lifespan.

Mercedes-Benz, for instance, has such actions for cyber security in the three below:
Cloud computing: vehicle data protection enabled by a cloud platform through which the car owner takes control of data openness to the outside while driving, and at the same time relevant information will be eliminated automatically after the car owner leaves his/her car;
Factory: partnership with telecom carriers and equipment vendors to set up intelligent vehicle manufacturing factories with production data safety enabled by 5G mobile network;
Vulnerability protection: joins forces with third-party cybersecurity providers to test and repair the potential vulnerabilities of intelligent connected vehicle.

> Japanese and Korean OEMs: with a more focus on cyber security protection and management inside the company

Nissan Motor, for example, proceeds with intro-company management on information security and perfects the regulations concerned. Over the recent years, Nissan has been improving its R&D management system and cyber security platform, with its Tel Aviv-based joint innovation laboratory and collaborations with Israeli start-ups on cyber security testing and study. As yet, Nissan has more than ten cooperative joint prototype projects.

> Chinese OEMs: the emerging forces go ahead of the rest

The emerging carmakers are commendable in cyber security protection. Cases include XPENG Motors that boast concurrent deployments over cloud, vehicle and mobile phone by building a security team on its own and the partnerships with Aliyun, Irdeto, and Keen Security Lab of Tencent in order for a proactive protection system; and NIO that has built a X-Dragon multi-dimensional protection system through a self-owned security team and multi-party cooperation.

Also, the time-honored Chinese automakers follow suit, such as Dongfeng Motor, SAIC, GAC and BAIC that all prioritize the security stewardship during their life cycle. As concerns its overall deployment, SAIC, for example, incorporates its subordinates into the group's cyber security protection and management system and applies the data encryption software (GS-EDS system) with one accord for data safety as a whole; secondly, SAIC builds a cloud platform independently and a proprietary cloud computing center delivering cloud-based security services; last, SAIC founded SAIC Lingshu Software Co., Ltd in charge of developing basic technology platform and sharpening software R&D competence.

Cyber Security Layout of Chinese OEMs

Region	OEM	Cyber Security Layout	Highlights
China	Xpeng Motors	Establish its own security team; multi-dimensional security field	1. Establish protection system against 80% attack attempt; other 20% effective attack is processed by active protection system primarily being machine learning. 2. Digital car key **meeting IFAA financial level standard**
	NIO	Establish security team, security engineering methodology, safety protection technology, safety guarding system, and security response system	**X-Dragon** multi-dimensional protection system
	Lixiang	Establish a comprehensive security team; partner with security vendor; roll out security emergency response center	Safety protection for full life cycle of data
	WM Motor	Establish a well-rounded security protection strategy; partner with security vendor to enhance security protection capability; focus on parts and chip security protection position	**OTA updates**
	Dongfeng Motor	Establish full life cycle safety management; set automotive cyber security level evaluation standard; establish technology framework	Enterprise network protection architecture
	SAIC	Unify data encryption software for the group; form a cloud computing center; establish SAIC Lingshu Software Co., Ltd.	SAIC wholly funded Shanghai FinShine Technology Co., Ltd. to provide application safety evaluation, intelligent probe, DDOS protection and other cloud-based security services.
	GAC	Establish unified identity authentication platform; synchronously plan three systems -- cloud platform, OTA, and cyber security	Security protection for autonomous driving
	BAIC	Establish a subsidiary named BAIC Data; partner with cyber security companies	BAIC BJEV **OTA technology** is a proprietary core technology, already iterated to 2nd Gen.

OEMs have ever broader cooperation in cyber security.

In addition to security enhancement, OEMs are vigorously seeking for external collaborations on vehicle, communication, platform, data, and application, to name a few.

Cyber Security Partners of Some OEMs

Region	OEM	IoV Security	Vehicle Security Protection	Communication Security Protection	Platform Security Protection	Data Security Protection	Application Security Protection
Europe	BMW		CRITICAL Software	CAICT	Keen Security Lab of Tencent	Aliyun	APPLE
	Audi			Deutsche Telekom, Huawei, American Tower, Qualcomm		IOTA foundation	
	Ford		Qualcomm Technologies. In, Baidu, Microsoft	Autonomic	Microsoft		Amazon Web Services (AWS)
	GM	GVSC, Honda	Verizon		HackerOne, AT&T		
Japan and South Korea	Toyota			NTT	UI Evolution, 360	Amazon Web Services (AWS)	INGEEK, Alipay, UI Evolution
	Honda	Tencent			Amazon Web Services (AWS), Evenote	NationSky, Boston University	Continental
	Nissan	SafeRide Technologies		Continental, Ericsson, NTT, DOCOMO, OKI, Qualcomm	Lan-You Technology, 360, Cybellum	Amazon Web Services (AWS)	Tsinghua University
	Hyundai		Tencent, DeepGlint	Cisco, Autotalks	NVIDIA, eCloud InterConnect, CertiK		
China	Xpeng Motors		NXP&ST, Keen Security Lab of Tencent		Aliyun		Irdeto, G+D mobile security
	NIO		AutoChips		Paraview Software	Acronis	
	WM Motor		Tsinghua Unigroup, 360, BlackBerry, Abupdate		Tencent	Tencent	SenseTime
	GAC		NXP, Tsinghua Unigroup	Huawei	Tencent, Baidu	Tencent, Huawei	
	BAIC	Huawei, CATARC	NXP, CEC Industrial Internet, Qianxin	Beijing Yesway	Baidu Cloud		

Table of contents

Table of contents

Table of contents

ResearchInChina

The Vertical Portal for China Business Intelligence

How to Buy

You can place your order in the following alternative ways:

1.Order online at www.researchinchina.com

2.Fax order sheet to us at fax number:+86 10 82601570

3. Email your order to: report@researchinchina.com

4. Phone us at +86 10 82600828

Party A:			
Name:			
Address:			
Contact Person:		Tel	
E-mail:		Fax	

Party B:			
Name:	Beijing Waterwood Technologies Co., Ltd (ResearchInChina)		
Address:	Room 2-626, 6th Floor, No.1, Shanyuan Street, Haidian District, Beijing, 100080		
Contact Person:	Liao Yan	Phone:	86-10-82600828
E-mail:	report@researchinchina.com	Fax:	86-10-82601570
Bank details:	Beneficial Name: Beijing Waterwood Technologies Co., Ltd Bank Name: Bank of Communications, Beijing Branch Bank Address: NO.1 jinxiyuan shijicheng,Landianchang,Haidian District,Beijing Bank Account No #: 110060668012015061217 Routing No # : 332906 Bank SWIFT Code: COMMCNSHBJG		

Title	Format	Cost
Total		

Choose type of format

PDF (Single user license) ……..3,200 USD

Hard copy …… 3,400 USD

PDF (Enterprisewide license)…..... 4,800 USD

※ Reports will be dispatched immediately once full payment has been received. Payment may be made by wire transfer or credit card via PayPal.

ResearchInChina

www.researchinchina.com