SQUIRE PATTON BOGGS

无人驾驶汽车和相关网络安全问题
Autonomous Vehicles and Cybersecurity Concerns

在过去十年间，企业在开发无人驾驶汽车方面投入了大量的时间和资源。谷歌公司在2016年8月的月度报告中宣称，在过去七年里，其开发的无人驾驶车辆在“自动驾驶”模式下已累计行驶了将近两百万英里。

Over the last decade, companies have devoted considerable time and resources to the development of autonomous vehicles. In its August 2016 monthly report, Alphabet Inc.'s Google Inc. reported that its self-driving vehicles had logged nearly two million miles in autonomous mode over the last seven years.

减少交通拥堵、增加安全性、提高人口流动性、甚至增加数字媒体收入的可能性——无人驾驶汽车对社会的诸多潜在好处是不言而喻的。全球每年都有130万人因交通事故死亡，5000万人受伤，而人为因素一直是道路交通事故的罪魁祸首（占比达93%）。因而专家们预计，运用技术能力替代人类驾驶将大大降低碰撞率。2012年发布的一份独立报告估计，无人驾驶车辆技术的广泛应用还可以将公路运载能力提高五倍。鉴于潜在利益驱动和飞速的技术进步，可以清楚地预见在不久的将来，无人驾驶车辆将飞入寻常百姓家。而消费者对于无人驾驶车辆的诸多疑问中最重要的一条是：无人驾驶车辆是否安全，或者无人驾驶车辆的使用是否会威胁我们的安全?

The potential benefits that autonomous vehicles offer society are numerous: from less traffic congestion and increased safety, to greater mobility for the population and possibly even increased digital media revenue. Human error is the cause of 93 % of road traffic accidents, with 1.3 million fatalities and 50 million injuries globally every year. Experts estimate that replacing human drivers with capable technology will substantially decrease collision rates. An independent report in 2012 estimated that widespread adoption of autonomous vehicle technology could also increase highway capacity fivefold. In light of the potential benefits and the rapid technological progress, it is clear that autonomous vehicles will be available to regular consumers in the not-so-distant future. Among the many important questions on the minds of consumers is: will autonomous vehicles be safe, or will the use of autonomous vehicles threaten our security?

在美国，一些消费者团体和立法者已对有关无人驾驶汽车的安全和信息隐私问题方面的立法缺失提出了关注，而这也可能对从事该领域研发和生产的所有国际汽车制造商和技术公司产生重大影响。在这里，我们将对全球汽车制造商下一步亟需了解的，最新颁布的准则和拟议立法进行分析。

In the US, consumer groups and some legislators have voiced concern about the lack of legislation addressing security and information privacy issues in connected cars, which could have a significant impact on all international car manufacturers and technology companies working in this space. Here, we will analyze recent guidelines and proposed legislation, which global automotive manufacturers will need to be keenly aware of going forward.

美国国家公路交通安全管理局（下称NHTSA）和美国交通部（下称DOT）于9月20日发布了关于无人驾驶车辆的指南。该指南旨在通过提出对某些网络安全问题的解决办法来帮助无人驾驶车辆相关企业更好地理解其在保护消费者的隐私和安全、同时也包括保护自身免受未来诉讼方面应该采取的下一步措施。

The US National Highway Traffic Safety Administration (NHTSA) and US Department of Transportation (DOT) guidelines on autonomous vehicles were released September 20. These guidelines address some of these cybersecurity concerns so assist autonomous vehicle companies to better understand the steps they should take to protect the consumers' privacy and security, and of course protect themselves from future litigation.

黑客技术：控制你的汽车和数据

Hacking: Taking Control of Your Vehicle and Your Data

说起无人驾驶汽车，以及更普遍意义上的车联网汽车，我们最常听到的顾虑就是黑客的威胁和第三方控制汽车的风险。已有多项报告显示车辆控制系统极易受黑客攻击，尤其是无人驾驶汽车，因其包含有更多互联的内部组件，使得黑客更容易侵入汽车的计算机系统。虽然迄今为止大多数黑客都被汽车制造商聘用的，专门研究防范未来风险的计算机安全专家制止，但据报道称，最近几个月来已有偷车贼运用黑客技术潜入了机动车的计算机控制系统。

The concerns heard most often about autonomous cars – and, indeed, in connected cars more generally – are the threat of hacking and fear that a third party will take control of consumers' cars. There are numerous reports showing vehicle controls are vulnerable to hacks and since autonomous vehicles consist of more interconnected components, this increases the ability for a hacker to infiltrate a car's computer system. To date, most hacks have been undertaken by security experts hired by the carmakers for research purposes so as to reduce future threats. However, in the last few months there have been reports of car thieves hacking into vehicles' computer control systems.

许多评论家对如今汽车行业广泛使用的专用短程通信技术（DSRC）表示担忧。该技术在未来将会被运用在无人驾驶汽车和车联网汽车中，以帮助避免车辆碰撞事故，并且可以用来提供商业服务。但是消费者组织担心该技术的使用会创造出一个“轮子上的计算机系统”，而且会伴随网络联动性的增强带来更多的网络安全问题。一旦该系统被黑客侵入，入侵者将可以篡改汽车安全信息或切断设备联络，从而导致严重的后果。

Many commentators have expressed grave concerns about Dedicated Short-Range Communication (DSRC) technology incorporated into many cars today. The DSRC technology, which will form part of all autonomous and "connected cars" in the future, helps to avoid collisions and offers commercial services. A number of consumer organizations fear DSRC technology will create a "Computer on Wheels" and that the increased connectivity will present significant cybersecurity issues. If a DSRC system was hacked, the perpetrator could falsify vehicle safety messages or disable the communication of the device, which might have catastrophic consequences.

联邦和州政府法规均未顾及消费者对网络安全的担忧

Neither State nor Federal Laws Address Consumers' Cybersecurity Concerns

尽管公众和各行各业都已意识到了风险所在，并且业内也对信息隐私权保护的最佳实践达成了协议，但大多数国家依然还未采取相关立法措施。

While the public and the industry recognize the risks, and there is industry agreement on information privacy best practices, the vast majority of states have yet to adopt legislation related to autonomous vehicles.

目前还没有针对无人驾驶汽车安全和隐私问题展开的州立法，但从联邦一级来看，已经有相关法案被提出。2015年7月，《汽车安全和隐私法案》诞生。这部法案启动了对汽车网络安全问题的跨部门调查。该法案的内容之一就是NHTSA将负责制定和发布相关条例，要求具备可访问数据或控制信号的汽车同时必须装备用于检测、报告及阻止任何试图截获数据或控制汽车的行为的设施。同年11月，《汽车安全和隐私学习法案2015》和《无人驾驶汽车隐私保护法案2015》相继出台。前者要求NHTSA开展为期一年的学习调研，通过咨询其他政府机构、行业精英、高等院校等部门，最终起草一个有关无人驾驶汽车软件安全、网络安全和隐私安全规制的草案框架。而后者要求美国总审计长制作一份公开报告，对DOT应对无人驾驶汽车技术的准备工作的充分性（包括消费者隐私保护方面）作出评估。以上法案都已提交委员会，目前正处于审查阶段。

There are currently no state laws in place addressing the security and privacy issues stemming from autonomous vehicles. At the federal level, several bills have been proposed that relate to autonomous vehicles and security. In July 2015, the Security and Privacy in Your Car Act (SPY Car Act) was introduced. The SPY Car Act seeks to launch a cross-sector investigation into vehicle cybersecurity. Among other things, under the SPY Car Act, the NHTSA would be responsible for issuing regulations that would require that vehicles with accessible data or control signals be equipped to detect report and stop any attempts to intercept driving data or control the vehicle itself. In November 2015, the Security and Privacy of Your Car Study Act of 2015 and the Autonomous Vehicle Privacy Protection Act of 2015 were proposed. The Car Study Act would require NHTSA to conduct a one-year study, consulting with other government agencies and industry leaders as well as universities, to recommend a framework for regulating car automated software safety, cybersecurity and privacy regulations. The Autonomous Vehicle Act would require the US Comptroller General to provide a public report that assesses the readiness of the DOT to address vehicle technology challenges, including consumer privacy protection. All of these bills were referred to committees, where they are currently undergoing review.

NHTSA和汽车行业网络安全指南

NHTSA and the Auto Industry Cybersecurity Guidelines

美国联邦法律已要求NHTSA发布《联邦机动车安全标准（FMVSS）》和供机动车生产商遵守并保证合规的规章制度。NHTSA和无人驾驶汽车行业均已认识到网络安全的重要性，并在过去的几年里投入了大量资源用于开发值得推荐的网络安全实践方法。

Federal law already requires NHTSA to issue Federal Motor Vehicle Safety Standards (FMVSS) and regulations to which manufacturers of motor vehicles must conform and certify compliance. NHTSA and the autonomous vehicle industry recognize the importance of cybersecurity and in the last several years have devoted considerable resources to developing recommended cybersecurity practices.

2016年3月，美国联邦调查局、DOT和NHTSA联合发布了一则公告，就有关汽车中现存和潜在的网络安全漏洞向公众和汽车行业发出警示。2016年1月，DOT和NHTSA对《无人驾驶汽车的初步政策声明》进行了更新，对包括开发无人驾驶汽车配置的最佳实践及无人驾驶汽车的州示范政策在内的某些举措进行了确认。如今，为了促进各州制定法律的统一性，NHTSA又提出了一项供各州采纳的示范政策，并确定了无人驾驶汽车规定中可由各州自由裁量的范围。

In March 2016, the FBI, DOT and NHTSA put out a public service announcement warning the public and the automobile industry of cybersecurity vulnerabilities that exist in cars today and in the future. In January 2016, the DOT and NHTSA issued policy guidance updating the Preliminary Statement of Policy Concerning Automated Vehicles, identifying certain initiatives that include the development of a best practices guide for the deployment of autonomous vehicles and a model state policy on automated vehicles. NHTSA has now proposed a model policy for the states to adopt so as to promote uniformity among state laws as they develop and has identified which aspects of autonomous vehicle regulation should be left to the states' discretion.

与此同时，汽车制造商们在2015年成立了"汽车信息共享和分析中心"（Auto-ISAC）以帮助分享那些具有威胁性的信息。7月，为提高汽车网络安全性，Auto-ISAC发布了一份《汽车网络安全最佳实践》的综述。虽然经过了五个月的酝酿，该文件却并没有给出具体的技术或管理方案，而只是推荐了诸如国际标准化组织（ISO）和国家标准与技术研究院（NIST）等一些组织制定的网络安全资源和标准。行业领头企业相互合作的角色不应被打折扣。的确，最新发布的NHTSA指南对Auto-ISAC以促进学习和信息交流的组织的身份来促进各个部门和各个角度之间更紧密的合作提出了更高的要求。

Meanwhile, automakers established an Automotive Information Sharing and Analysis Center (Auto-ISAC) in 2015 to assist in the sharing of threat information. In July, the Auto-ISAC released an overview of comprehensive Automotive Cybersecurity Best Practices (Best Practices) to improve vehicle cybersecurity. Developed over a five-month period, the Best Practices do not prescribe specific technical or organizational solutions and are only recommendations that incorporate established cybersecurity resources and standards from organizations such as the International Organization for Standardization (ISO) and National Institute of Standards and Technology (NIST). The role of industry led collaboration should not be discounted. Indeed, the newly released NHTSA guidelines outline the need for ever-greater collaboration within the sector and points to Auto-ISAC as a group to promote learning and information exchange.

就DSRC技术而言，DOT也已作出了开发可提高公路安全性的先进技术的承诺。自2014年起，NHTSA就致力于制定一项规则用于设定车辆与车辆之间的通信技术标准，其中包含了安全、隐私和安全等方面的问题。 目前白宫管理和预算办公室正在审查这项规定。

In relation to concerns raised about DSRC technology, the DOT announced a commitment to developing advanced technologies that could enhance highway safety. Since 2014, NHTSA has been working on a rule addressing vehicle-to-vehicle communications technology standards, including safety, privacy and security issues. That rule is currently under review by the White House Office of Management and Budget.

NHTSA和DOT于9月20日联合发布的，备受期待的《无人驾驶汽车指南》中给出的是一个框架而非一套既定的安全规则。该指南指出，“识别、保护、检测、响应和恢复功能应该被用于实施风险管理决策、解决风险和威胁，以及能够快速响应网络安全事件并从中吸取教训。”DOT将运用15项安全标准来对每辆车进行独立评估，而其中涉及到数据隐私和网络安全的就有三项数据，即数据记录和共享、隐私和汽车网络安全。

In the highly anticipated NHTSA and DOT guidelines for autonomous vehicles released September 20, the agency set out a framework rather than a prescribed set of safety regulations. The guidelines note that the ''identification, protection, detection, response and recovery functions should be used to enable risk management decisions, address risks and threats and enable quick response to and learning from cybersecurity events.'' DOT will utilize a 15-point security standard to independently evaluate each vehicle. Three of these points relate exclusively to data privacy and cybersecurity: data recording and sharing, privacy and vehicle cybersecurity.

在新指南的解释性说明中，DOT和NHTSA明确指出了覆盖设计和开发阶段整个供应链过程的网络安全要求。由此看来，不仅无人驾驶汽车制造商必须证明其符合了上述15项标准，有可能其供应商也必须符合这些标准的规定。 这些新指南的发布虽然提供了进一步指导，但还只是跨出了制定制造商及供应商所需要遵循的一套完整网络安全实践的第一步。 DOT还将在不久的将来针对整个汽车行业发布更明确、具体且有补充性的网络安全最佳实践指南。

In the explanatory notes of the new guidelines, the DOT and NHTSA make clear that the cybersecurity requirements relate to the entire supply chain in the design and development stages. Autonomous vehicle manufacturers will therefore have to set out that they have met such standards within the 15-point standard but also potentially that their suppliers have as well. These new guidelines, while providing further guidance, are just the beginning to defining an exact set of cybersecurity practices that manufacturers and their suppliers will need to follow. The DOT will also be releasing more specific but complementary cybersecurity best practices for the whole automobile industry in the near future.

在10月24日，DOT和NHTSA以提供自愿指导的形式发布了期待已久的《网络安全最佳实践指南》（CBP）。该指南的范围覆盖了无人驾驶汽车从供应环节到发电机和调节器的全部范畴。在CBP中，NHTSA鼓励制造商、供应商和其他利益相关者携手合作，以共同支持对技术和非技术劳动力的教育工作。该文件列举了NHTSA和业界在网络安全方面已经采取的一些步骤，并提供这一指南作为补充现有标准、原则和最佳实践的资源。

On October 24, the DOT and NHTSA released their anticipated Cybersecurity Best Practices (CBP) in the form of voluntary guidance. The scope of the guidance covers the entire autonomous vehicles supply chain down to alternators and modifiers. In the CBP, NHTSA encourages manufacturers, suppliers and other stakeholders to work together to support educational efforts for both the technical and non-technical workforce. The document lists a number of steps both NHTSA and the industry have already taken in relation to cybersecurity and supply this guidance as a resource to supplement current standards, principles and best practices.

CBP在汽车网络安全方面提出了以下建议：（1）安全的分层方法；（2）使用现行IT安全现场行业标准；（3）在车辆的整个生命周期中考虑隐私和网络安全风险；（4）确保网络安全成为管理层承诺的优先事项；（5）积极参与Auto-ISAC，分享与网络安全风险和事件有关的信息；（6）为外部网络安全研究人员制定漏洞报告/披露政策；（7）编制有关处理事件和漏洞流程的文档；（8）自我审核的风险、记录、定期保留和修订；和（9）渗透测试。

The CBP promotes the following in vehicle cybersecurity: (1) a layered approach to safety; (2) use of current IT security site industry standards; (3) consideration to privacy and cybersecurity risks through the lifecycle of the vehicle; (4) management commitment to ensuring cybersecurity is a priority; (5) active involvement in Auto-ISAC to share information related to cybersecurity risks and incidents; (6) creation of vulnerability reporting/disclosure policies for external cybersecurity researchers; (7) documentation of its process for handling incidents, vulnerabilities and exploits; (8) self-auditing of risks which are documented, retained and revised regularly; and (9) penetration testing.

CBP还确认了某些应该使用的基本网络安全保护措施，包括但不限于：（1）限制开发者访问系统；（2）将诊断特征限于在某些条件下实现预期目的的特定操作；（3）采用良好的安全编码实践，减少第三方在软件更新期间获得未加密固件的任何机会；（4）限制固件修改的能力将使得安装恶意软件更具挑战性；（5）将车辆ECU上的网络服务器的使用限制为基本功能，同时移除任何不必要的网络服务；（6）分割关键安全信息；（7）在外部服务器和车辆之间的任何基于IP的操作通信中采用已被接受的加密方法。

The CBP also identifies a number of fundamental cybersecurity protections that should be used including, but not limited to: (1) limiting developer access to systems; (2) limiting diagnostic features to specific operations that accomplish the intended purpose in certain conditions; (3) employing good security coding practices that reduce any opportunity for a third party to obtain unencrypted firmware during software updates; (4) limiting the ability for firmware modification would make it more challenging for malware to be installed; (5) limiting the use of network servers on vehicle ECUs to essential functionality, with any unnecessary network services being removed; (6) segmenting critical safety information; (7) employing accepted encryption methods in any IP-based operational communications between the external servers and vehicle.

结论

Conclusions

消费者对自动驾驶车辆所带来的潜在安全问题的担心是理所应当的。幸运的是，美国政府的相关决策者和活跃于该行业的企业正在认真对待这些问题，并致力于制定能够适用于未来发展的网络安全准则和隐私原则，以减轻公众在这方面的担忧。

Consumer fears about the potential security issues that autonomous vehicles pose are valid. Fortunately, key US government stakeholders and companies active in the autonomous vehicle industry are taking such concerns seriously and are working towards cybersecurity guidelines and privacy principles that could shape future regulations to alleviate such concerns.

当然，这并不意味着无人驾驶车辆迈入寻常生活领域之后就不会受到黑客的攻击，但这意味着相关程序已经到位，并向着将这种风险最小化的方向迈进。虽然现在看起来似乎各方都在齐心协力，然而时间将最终证明联邦和州政府是否能够赶在无人驾驶汽车投入实际应用之前通过立法来充分解决这些网络安全问题，还是会步其他新兴技术之后尘，美国和其他地方的政府最终沦为法律制度方面的追赶者？让我们拭目以待。

This does not mean autonomous vehicles will not be hacked once they are available to the public, but it does mean that a process is in place and moving forward to minimize such risks. Though there appears to be a concerted effort, time will tell whether federal and state governments can pass legislation that adequately addresses these cybersecurity concerns before autonomous vehicles become available to the public or if, as with other emerging technologies, lawmakers in the US and elsewhere will be playing catch-up.

联系人

Contact

Daniel Roules 陆大安
Partner, Shanghai Office
上海分所合伙人
T +86 21 6103 6309
E daniel.roules@squirepb.com

Gretchen Ramos
Partner, San Francisco Office
旧金山分所合伙人
T +1 415 743 2576
E grentchen.ramos@squirepb.com