日本车联网信息安全发展现状与分析

中国科学院信息工程研究所 印曦 魏冬 黄伟庆 韦迪

日本是全球车联网的先行者。经过几十年的发展，日本已经是全球车联网最发达的国家之一。

日本是全球车联网的先行者。1981年，本田汽车公司与日本消费电子厂商阿尔派合作共同研发，推出了世界第一款陀螺仪车载导航，并在此基础上率先推出了车联网服务，与移动互联网相融合，增强汽车用户的黏性。经过几十年的发展，日本已经是全球车联网最发达的国家之一。然而，近年来，日本频繁发生攻击轮胎压力监测系统、使用广域网攻击车载LAN和解析防盗器密钥等恶意事件。针对此情况，日本显示出了对汽车信息安全的高度重视，并制订了相应的对策和管理方针。

汽车联网技术的潜在威胁

日本信息处理推进机构（IPA，Information-technology Promotion Agency）主要致力于研究汽车信息安全。根据该机构已公布的资料，汽车联网技术的潜在威胁呈两大趋势。

第一个趋势：以智能手机为中心，汽车与互联网联动越来越普遍。

智能手机与传统手机的一大差异在于客户可以开发应用，比较自由地向任何人提供。从简单应用到实用类型，市面上流通的应用种类繁多。然而，在这些应用中，有一些应用的可靠性很差。黑客有可能通过其中的漏洞，以智能手机为跳板，给车载设备和车载导航仪系统造成损害，或是经由智能手机泄露车内信息，侵犯驾驶员的隐私。而且，使用智能手机意味着汽车随时都与外部网络连接。因此，经由外部网络和智能手机，能够对正在行驶的汽车发起攻击。

除了智能手机之外，自动收费系统、智能车钥匙等通过无线与外部连接的功能，以及纯电动汽车经由充电插头连接车载网络的功能也在逐渐普及。随着汽车开始接入车外网络的便捷化，或许，攻击者无需靠近汽车，就可以跨越网络，攻击全世界的汽车。即使不是随时随地接入网络，用户误下载的智能手机恶意应用也有可能危害到汽车。

第二个趋势：车载软件、车载LAN对于汽车的“行驶、转弯、停车”等基本控制功能的影响正在增大。

汽车厂商使用通信或信息终端来提供门锁控制、调整发动机功率、更新软件等服务。这些功能一旦被黑客成功入侵，很容易产生重大危害。而且，为了在降低成本的同时确保通用性，部分车载系统开始使用Linux之类的通用操作系统。汽车用户使用起各项服务来越来越方便，但是，解析或攻击操作系统的难度也随之越来越低。

不只是操作系统，车载LAN的通用性也在提高。过去，以CAN（控制器区域网络）为代表，车载LAN的通信方式虽然在电路层级实现了标准化，但是，请求指令、响应机制等具体内容大多是因企业而异的，构成了实际运用中的障碍。从信息安全的角度来看，这样的障

碍其实是一道防火墙。

如今，市场上已经出现了使用近距离无线通信“蓝牙”、WLAN 等网络提供车载 LAN 通信内容的适配器。随着越来越多的车载 LAN 采用互联网标准，车内外的众多设备和信息系统都将与汽车紧密连接，连接车载 LAN 的操作也会越来越简单，因此，与此相关的防护措施，包括防火墙等，被攻破也将变得轻而易举。

IPA Car 模型与攻击途径

IPA 通过分析与汽车信息安全相关的攻击方法，设想出了三种攻击途径。

第一，直接攻击。

汽车不同于个人电脑和手机，由于其较大的体积及某些特性，用户很难始终监视车辆。恶意攻击者比较容易直接接触到汽车。在进行年检等检测的时候，汽车必须交由检查人员管理，有可能会受到装扮成检查人员的第三方攻击。用户在自行改造时，也可能无意识地解除汽车的安全功能。

第二，从便携式产品入侵。

除了汽车厂商提供的功能之外，用户通过汽配市场等途径购买并安装在车上的产品也种类繁多。拆装这些产品时，来自外部的病毒等威胁有可能进入车内。尤其是智能手机，一方面很容易就能获得面向汽车的通用应用，另一方面，也容易获得掺杂着大量山寨应用和包含恶意代码的应用。因此，研发人员在开发阶段，就必须要考虑到用户可能携带进入车内产品的种类，包括智能手机、平板电脑等。

第三，从外部网络攻击。

汽车上有很多使用通信的装置，例如智能钥匙、轮胎压力监测系统、路车间通信等，这些使用短距离无线通信的功能的装置，有可能受到通信被窃听、被恶意中断等威胁。而且，智能手机与车载系统联动的使用越来越普遍，汽车连接外部网络的机会越来越多，车载信息服务也逐渐普及，因此，从外部网络实施攻击的威胁已成为现实。

根据这三种攻击方式，IPA 从汽车需要的可靠性等角度出发，设想了按照车辆功能群进行分类的汽车模型——“IPA Car”，如图 1 所示。

IPA Car 模型将车载 LAN 最大限度地抽象化，假设用 1 条总线连接全部功能，把所有功能分成实现“行驶、停止、转弯”的“基本控制功能”、提升舒适性和便利性的“扩展功能”、用户带入车内

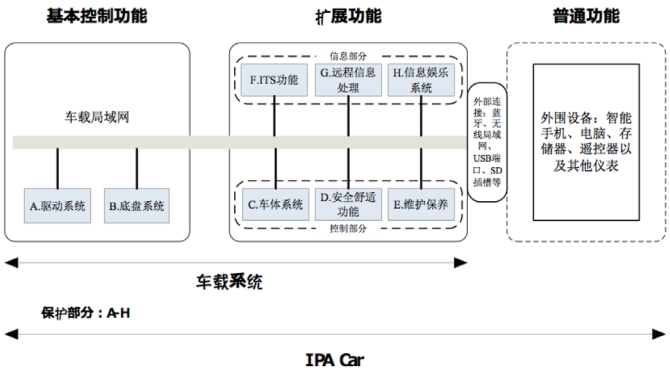

图 1　IPA Car 的模型

的产品等“一般功能”。所以，容易成为攻击入口的外部接口可能包含在各项功能中。IPA Car 将外部接口其整理到“扩展功能”与“一般功能”之间的连接部分。另外，“基本控制功能”与“扩展功能”合称为“车载系统”，这两个功能群又细分为“驱动类”、“信息娱乐类”这样的形式。“扩展功能”大致可以分成两类。一是包括“车体系统”、“安全舒适功能”、“诊断及维护”在内的“控制相关功能”，主要与行驶、停止、转弯等汽车的物理功能密切相关。另一类是包含“ITS（Intelligent Transport System）功能”、“通信与信息”、“信息娱乐”等在内的“信息相关功能”，是有关向驾驶员提供信息的功能。这两类功能的相关服务一旦发生安全问题，产生的风险截然不同。在发生信息安全问题时，需根据该模型理清系统与功能的联动机理和信息的种类来采取对策。

原因、对策与管理

根据 IPA Car 模型，IPA 将联网汽车信息安全产生威胁的原因分成两类。一类是“用户偶然引发的失误”，另一类是“攻击者故意引发”。按照不同的发生原因，相应的威胁分别如表 1 和表 2 所示。

目前，汽车信息安全领域的研究人员正在逐年增加。除 IPA 之外，部分汽车研究机构已经开始探讨自己特有的安全对策。各领域的研究人员也在不断改进攻击技术和对策技术，积累新的思路。针对前面提到

威胁	说明
设置错误	用户经由汽车内的用户接口，错误实施操作和设置。
感染病毒	通过用户从外部带入的产品和记录介质，车载系统感染病毒和恶意软件。

表 1　用户操作造成的威胁

威胁	说明
非法利用	无正当权限者通过伪装和攻击产品漏洞，利用汽车系统功能。
非法设置	无正当权限者通过伪装和攻击产品漏洞，非法变更汽车系统设置数据。
信息泄漏	汽车系统中应当受到保护的信息落入非法人员之手。
窃听	车载设备之间的通信、汽车与周边系统的通信遭到窃听、截取。
Dos 攻击	通过非法或过多的连接要求造成系统瘫痪、服务受阻。
虚假消息	攻击者通过发送虚假消息，使汽车系统执行非法动作和显示。
记录丢失	删除或篡改操作记录等，使用户无法查看。
非法传播	通过控制通信途径，劫持正规通信、夹杂非法通信。

表 2 攻击者干扰引发的威胁

的威胁，IPA 采取了合理的安全对策，如表 3 所示。

按照汽车的生命周期（策划、开发、使用、废弃），IPA 在迎合大部分企业需要的基础上，整理出了相应的安全管理方针，如表 4 所示。

就管理来说，在汽车生命周期的任何阶段，产品提供商都必须要实施安全对策。制定整体方针，并按照这一方针，在各个阶段实施连贯的安全对策。如果每次开发产品和服务时都从零开始制定安全对策，不仅会造成大量浪费，还有可能让组织的安全对策出现偏差。在管理方面，尤为重要的是培养精通信息安全的人才、制定贯穿整个开发体制的基本规则、不断收集与更新攻击方式相关的信息。

策划阶段。从进入实际的开发之前的策划阶段开始，就要结合安全对策，这一点非常重要。因为在策划阶段，经常要讨论汽车整个生命周期的预算。在这一阶段，需确定汽车的理念和配备的功能。另外，还需要考虑各项功能的安全性的重要程度，并为相应的对策分配预算。

开发阶段。在汽车企业及部件企业设计硬件和软件并安装到汽车上的这一阶段，须做到准确安装

要件、杜绝漏洞。此外，如果预算充裕，还需购置漏洞评估设备。

使用阶段。这是用户购买汽车，实际使用的阶段。在车辆使用期间，位置信息、用户下载的软件、用户的操作记录和行驶记录等大量的信息将存储在车辆和数据中心之中。虽然安全对策要配合用户使用的场景来实施，但是，也要注意保护隐私。另外，如果在车辆售出后发现漏洞，还必须考虑构筑能将相关信息通知用户和车主、与销售店和维修厂等构建合作应对的体制。

废弃阶段。在用户因换购、故障等原因废弃汽车的阶段，人们往往容易忽视安全对策，因此，在这一阶段尤其要注意。废弃的方式包括通过二手车销售店等渠道转让给其他用户、注销后报废等。不同的情况必须采取不同的对策。

类别	安全对策		说明
安全要件定义	要件管理工具		要件管理工具是能够整理复杂的程序要求，使要件与设计、功能相对应，并对其进行管理的工具。整理安全要件有助于防止漏装安全功能。
安全功能设计	安全架构设计		在明确系统的使用案例和模型的前提下，分析威胁和风险，根据安全方针，设计应对方法和应对位置的方法。能够防止对策略疏漏引发的漏洞等。
安全功能设计	利用安全功能	加密	加密包括保护信息资产本身的内容加密，以及防止通信遭到窃听的通信通道加密两类。根据加密方式不同，处理速度、数据量等也存在差异，因此，根据要求选择加密方式非常重要。
		认证	对用户、通信对象以及追加的程序等是否合法、是否遭到了篡改进行认证的方法。除了密码、哈希值等软件处理之外，还包括 IC 芯片等使用专用硬件的方法。
		访问控制	对使用者的操作权限、功能机通信的范围等实施管理。通过恰当地设定使用者及功能的影响范围，防止设想外的利用，并保护主要功能不被其他功能发生的问题影响。
安全安装	安全编程		防止缓冲区溢出等已知漏洞的编程技术。包括禁止利用存在漏洞的函数、禁止容易产生误解的密码表述等。
安全评估	安全测试		确认系统成品是否存在漏洞的方法。包括检测已知漏洞的工具、调查未知漏洞的模糊测试等方法。
其他措施	制定指南		通过指南等书面形式，向用户传达正确的使用方法和发生安全问题时的应对方法非常重要。而且，工厂出货时的设置也要注意防范安全问题。

表 3　针对威胁的安全对策

汽车的生命周期很长，要想确保安全，除了企业采取措施之外，汽车用户的协助同样不可或缺。今后，汽车企业对用户的安全启蒙活动数量，可能会大幅增加。

生命周期	安全举措	概要
管理	制定安全规则	设定安全相关组织的规定和规则。
	实施安全教育	对参与开发和使用的人员，实施安全基础概念和安全技术的培训。
策划阶段	安全信息的收集和发布	收集可能与自己的组织开发的系统有关的漏洞信息、事件信息、标准化动向等，向相关人员发布。
	定义安全要件	对于将要开发的系统，结合其使用方法和使用的信息，定义安全要件。
	确保安全相关预算	为开发阶段的安全对策费、使用阶段实施的安全升级等制定预算。
	外包开发时的安全措施	确定外包开发时的签约规则、能担保人员和委托品的安全品质的规则及筛选方法。
	应对与新技术相关的威胁	探讨今后汽车可能采用的新技术的威胁和风险。
开发阶段	设计	结合安全功能的安装方式和日志收集方式等进行设计。
	安装时的安全对策	利用可防止漏洞出现的安全编码和编码标准。
	安全评估和调试	在测试环节利用源代码的复查和模糊测试等方式检验。
	准备向用户提供信息所需内容	汇总有助于用户正确利用系统的信息。
使用阶段	安全问题的应对	构筑发生事件时能够快速采取应对措施的联络体制，实施训练等。
	向用户和汽车相关人员提供信息	探讨在发现漏洞时向用户发布安全补丁和信息的方法。
	充分利用漏洞相关信息	合理使用漏洞相关信息，防止已经发现的漏洞再发、减少漏洞对于相关系统的危害。
废弃阶段	制定废弃策略	在汽车废弃时提供信息删除功能，防止用户信息等落入他人之手，并公开删除方法。

表 4　汽车生命周期的安全管理策略

结语

综上所述，日本一直以来大力发展民用技术，对于汽车信息安全技术的投入呈逐年上升趋势。一方面，日本成立了多个相应的研究机构，从技术上提高汽车联网的安全性。另一方面，日本制定了高效的安全对策和管理方针，降低汽车信息泄漏的风险。同时，日本鼓励研究机构与企业合作，将技术和管理手段有机调配，促成汽车信息安全的最佳效果。

（本栏责编：王丹娜）