数据安全的“七寸”是数据“在途”的 HTTPS 加密

最近发生了两个与数据相关的事情，一个是大事—**国家数据局**正式挂牌，将从国家层面统筹协调数字中国、数字经济、数字社会的规划和建设，能够更好统筹数据资源整合共享和开发利用，推动互联网、大数据、云计算、人工智能、区块链等数字技术加速创新融合，实现数字技术与实体经济的深度整合，是抓抢数字经济发展先机、打造经济发展新动能的重要举措。另一个看起来好像不是大事但实际上也是大事的数据安全问题，这就是“谁泄露了我的航班信息”。笔者看了许多相关的文章认为都没有分析到点子上，本文从密码技术方面来分析这个数据安全问题，希望能帮助大家真正明白到底是谁泄露了用户的航班信息和用户隐私信息，真正了解什么是保护数据安全的关键。

现在是大数据时代，大家都能理解数据是需要流通的，这就是数据资源整合共享和开发利用。航班数据从用户端生产后从用户端传输到数据处理的云端系统，也就是航空公司的服务器上，然后再流通到票务公司、旅游服务公司、交通服务公司等等多个服务提供商的服务器和工作人员的电脑上。所以，正如有关文章所写的，的确很难界定到底是哪个环节泄露了用户数据，这可能是一个无法理清的无头案。

但是，无论谁拥有过数据，笔者认为最大的泄露可能是数据在传输途中被非法窃取，因为数据“在岸”时各大航空公司和相关公司都一定是有相关的严格管理制度和安全防护措施的，我国各种管理信息系统建设已经经过了四十多年的建设和完善，这一点大家还是应该有信心的。

但是，在当下的云计算和大数据时代，信息系统建设者还停留在传统的基于城堡防护的思路上，仅投资建设了各种安全防护系统和各种数据安全管理制度，能保证数据的“在岸”安全，但是却忽视了数据的“在途”安全，数据离开了城堡到用户手中和到合作伙伴系统中是明文传输的，非常容易被非法窃取，这才是数据泄露的根本原因。

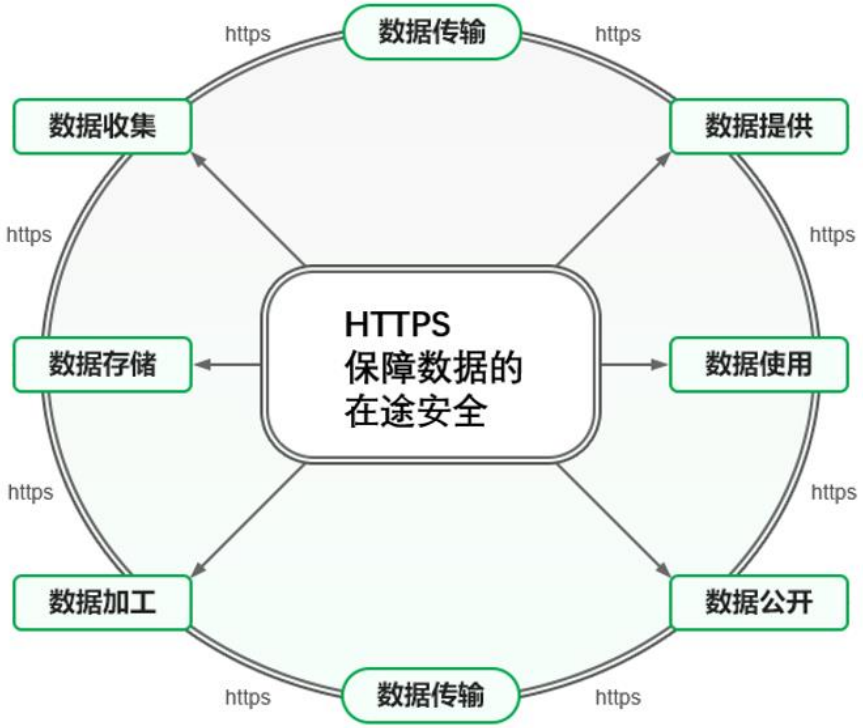
为了印证这个观点，笔者检索了国际证书透明日志系统，统计了我国前十大航空公司的域名的 SSL 证书申请量，同时实际检查了各个航司的官网及订票系统是否启用了 SSL 证书实现 HTTPS 加密，具体数据如下表所示，数据并不乐观，其中有两家航司没有实现全站 HTTPS 加密，要求用户输入个人机密信息的注册页面居然有不支持 HTTPS 加密或者不强制支持 HTTPS 加密的，那么用户在这些页面输入的个人信息就非常容易被非法窃取，而笔者更加不能接受的是居然登录页面也不支持 HTTPS 加密，也就是说用户在航司系统中用户名和口令非常容易被

非法窃取，这如何保障用户的航班信息安全？全站 HTTPS 是不仅仅是官网 HTTPS 加密，登录系统和注册系统都必须是 HTTPS 加密，用户登录后的系统也必须是 HTTPS 加密，只有这样才能用户数据的“在途”安全。

排名	航空公司	检索域名	证书数	国外CA%	国密证书	官网HTTPS	注册页HTTPS	登录页HTTPS	HTTPS合规
1	南方航空	csair.cn	5	100.00%	无	否，支持HTTPS	是	否，支持HTTPS	否
2	国航(中国站)	airchina.com.cn	28	100.00%	无	否，支持HTTPS	否，支持HTTPS	是，但支持HTTP	否
	国航(美国站)	airchina.us	1	100.00%	无	是	是	是	**是**
3	东方航空	ceair.com	21	61.90%	无	是	是	是	**是**
4	海南航空	hnair.com	8	75.00%	无	是	是，但支持HTTP	是，但支持HTTP	否
5	厦门航空	xiamenair.com	2	100.00%	无	是	是	是	**是**
6	深圳航空	shenzhenair.com	1	100.00%	无	是	否	否	否
7	四川航空	sichuanair.com	4	100.00%	无	是	是	是	**是**
8	春秋航空	ch.com	1	100.00%	无	是	是	是	**是**
9	吉祥航空	juneyaoair.com	1	100.00%	无	是	是	是	**是**
10	山东航空	sda.cn	3	100.00%	无	是	是	是	**是**

笔者也检查了全球十大航司的官网，没有发现一个网站系统不是全站全业务系统都实现 HTTPS 加密的，排名第一位的美国航空(aa.com)申请了 **1612** 张 SSL 证书，是我国申请证书最多的国航的 28 张的 57 倍多，这个数字就能说明所有美航的信息系统都实现了 HTTPS 加密，这一点非常值得我国航司学习。很有意思的是，排名靠后的几个航司已经实现官网、登录和注册页全都 HTTPS 加密，笔者为这些航司点赞。

依据《数据安全法》第三条对“数据处理”的定义，数据处理包括数据的收集、存储、使用、加工、传输、提供、公开等。在这个七个数据处理环节中，其他六个环节都离不开数据传输，所以，数据安全的“七寸”是数据传输，必须保护数据的传输安全，不做好这个安全保护，其他安全保护都是空中楼阁，这就是数据的“在途”安全，唯一可靠的技术方案就是 HTTPS 加密，数据在全生命周期中的流通传输都必须是通过 https 加密通道传输，当然，依据《密码法》必须采用商密算法的 https 加密，也就是必须部署国密 SSL 证书来实现 HTTPS 加密，只有这样才能有效保障每一个数据处理过程中的数据处于有效保护中，使得数据从生产到销毁的全生命周期都处于持续安全状态。这也是《数据安全法》所定义的“数据安全”要求，“指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。”



回到本文话题“到底谁泄露了用户的航班信息”，笔者只列出了航司的网站系统的 SSL 证书申请情况和部署情况，并没有时间去遍历其它相关航班数据流通使用单位的官网，所以，仍然无法回答这个问题。但是，相信大家通过分析航班信息的源头的 HTTPS 加密情况就能看到这个问题的关键在哪，关键在所有航班信息流通环节都必须实现 HTTPS 加密。航司必须实现不仅自己的所有系统都是 HTTPS 加密，而且航班信息交换 API 也必须是 HTTPS 加密方式提供给合作伙伴，并要求所有合作伙伴都必须所有系统实现 HTTPS 加密。

所有与航班信息相关的单位不能只是保护自己业务系统服务器的安全，不能只是保护数据的“在岸”安全，必须同时保障航班数据的“在途”安全，只有同时保障了数据的“在岸”安全和“在途”安全，才能真正保障用户数据的安全，这也是所有互联网服务数据安全的最低要求，不仅仅是航班信息。至于如果实现 HTTPS 加密，当然首选自动化实现 HTTPS 加密解决方案，以确保各种业务系统能不间断地自动化实现 HTTPS 加密，不间断地保障业务数据的“在途”安全。

有诗为证：

数据安全七环节，在途安全是关键。
打蛇就要打七寸，保障数据在传输。
传输加密为必须，加密算法用商密。
数据流通多环节，在途加密保安全。

王高华

2023 年 10 月 27 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。