<u>=Q</u>

下载APP



加餐 | 密码学, 心底的冷暖

2020-12-11 范学雷

实用密码学 进入课程》



讲述: 范学雷 时长 05:12 大小 4.77M D

你好,我是范学雷。

今天是我们的一次加餐,我们不讲知识,我要跟你分享一点关于密码学的小感慨。

2011 年的时候,因为要参与解决 BEAST 安全漏洞的国际合作,我得以和一些顶尖的密码学家一块儿工作。当时,幸运的是,我提议的解决方案被广泛采纳,成为了事实上的标准,给 TLS 1.0 续了十年的命。

不幸的是,十多年来,我对密码学一直都很崇拜,但是,它的很完美的印象在我的心底。 彻底击碎了,这也彻底改变了我对密码学应用市场的认识。 为了更好地帮助我找到解决方案,当时的一位密码学家分享给我一些他的调查数据。这些数据研究了全球最知名的几十万家公司的公开网站,帮助他们发现了很多和密码学相关的安全问题。

问题很严重,国内公司的问题尤其严重。按理说,大公司有钱有人有技术,能够养得起、请得动密码学专业领域的工程师,信息系统应该没有突出的密码学问题。

很遗憾的是,2011年的数据表明,那时候的国内大公司,虽然有钱有人有技术,却依然霸占了问题最突出、威胁最严峻的榜单前列。

现实和理想

这是我第一次被密码学现实和理想之间的差距震撼到了。因为这些问题,其实都不是什么 技术门槛的问题。技术都是公开的,也都是随手可取的。大部分的安全问题,都来源于这 些应用的设计者和实现者没有意识到这些麻烦的存在。

他们没有意识到问题的存在,当然也就不可能解决掉这些问题。在密码学业者眼里的常识,也许是普通软件工程师意识之外的存在。更严重的现实是,由于意识不到这些安全问题,这个公司当然也就不知道这些安全漏洞。

什么时候,他们能知道这些问题呢?要么有善意的研究者告诉他们,要么有恶意的攻击者警告他们。更多的时候,恶意的攻击者已经击破了系统,盗取了数据,也没有留下痕迹,当然也没有敲响警钟。这些被盗取的数据,随时都会是威力巨大的暗雷,不知道什么时候就会引爆!

从 BEAST 安全漏洞开始,随后的几年里,我的工作时间几乎就被不断颠覆的密码算法霸占了。三五年的时间里,几乎所有的主流密码学算法都爆出了或多或少的漏洞。昨天还占据主流地位的算法,今天就被宣布有破解办法,明天就要被扫进历史的垃圾箱了。

大家都忙着给算法打补丁,找替代品,更新产品。这种连环式的暴雷,过了五六年才算消停。但是,能够消停,也是因为业界几乎把 2010 年之前主流的密码学算法都换了一个遍。

隐忧依然存在

2020年,一切似乎算是可以喘口气了。可是,隐忧依然存在。

第一个隐忧就是,大家都知道老算法有问题,那使用新算法了吗?答案是令人难堪的:并没有。比如,2020年,Zoom就被研究者披露使用了二三十年前就已经不安全的加密算法。

第二个隐忧是,如果使用新算法,数据就安全了吗?答案还是令人难堪的:也不一定安全。如果有心者记录了历史数据,如果加密历史数据的算法有一天被破解,历史数据还是有可能被破解。历史数据里有价值的信息,比如用户名和密码,再比如知名人士的行程。尴尬的是,有人认为,不仅存在这样的有心者,而且还有钱有权有势。

第三个隐忧是,如果是新系统、新算法,数据就安全了吗?答案稍微让人欣慰:还有一点风险。这点需要防范的风险就是,如果新算法未来被破解,加密数据能不能被解密?我们要确保即使未来算法被破解,特别是量子时代到来后,数据也没有办法解密。要做到这一点,还是需要有点密码学领域的专业知识积累的。

看看这些隐忧,我心里只有凉凉两个字。因为,大部分的软件工程师还没有掌握密码学的基础知识,当然也不会担心这些问题。不担心这些问题,当然就更不会有人去想解决问题的方法。

不过,我还是听说,有很多学校,在大学一二年级,开设了类似于"密码学 101"这样的基础课,即便学生的专业并不是计算机。但令人欣慰的是,即使不是软件工程师,像密码学 101 这样的基础课程,也可以帮助我们更好地保护自己的隐私,保护自己。

十年后,也许有一个新模样。

极客时间的《实用密码学》这个专栏,就是我为十年后的新模样,添的一块砖。

提建议

© 版权归极客邦科技所有,未经许可不得传播售卖。 页面已增加防盗追踪,如有侵权极客邦将依法追究其法律责任。

上一篇 08 | 该怎么选择初始化向量?

下一篇 09 | 为什么ECB模式不安全?

精选留言 (6)



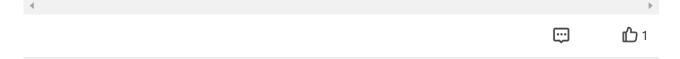


sugar

2020-12-13

我曾担任过BAT某业务部门的安全接口人,受理各类安全技术相关的case和后续跟进。从我的视角来看,信息安全这个领域 老师本节提到的问题,本质上需要靠政策和立法去推动。我不知道在硅谷是怎样的,但至少国内大厂我很清楚,2017年网安法出台后,是有明显改变的。举个例子: 法规要求服务端log至少保留3个月或者6个月,那么公司会推动相应的机制确保自己是"合法"的,因为如果遇到重大安全攻击比如APT,网警介入发现…

作者回复: 哎,不说了,谈起背后的原因,能吐一江水。我们能做的,就是在现有条件下,尽力去推动信息系统安全,创造一个多赢的局面,同时让自己越来越有价值。





Ender0224

2020-12-12

"我期待的另外一个结果,就是希望你能够对常见算法心中有数。需要使用算法的时候,能够有意识,可以通过查阅资料和相关规范,快速跟上"

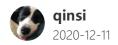
针对老师谈到的第二点,我的疑问是,即使做了很多查阅资料和相关规范的工作,最终可能还是会找一个知名开源软件,参考其对新安全协议的实现,直接抄过来用,这就让我感觉就算不查阅直接抄过来也是ok的,那这部分工作的价值是什么?

展开~

作者回复: 抄作业也有不同: 有的抄的明白, 有的抄不明白; 有的抄的起, 改的动; 有的抄不起, 改不动。不知道基本的密码学算法, 作业超过来, 以后的维护怎么办呢? 毕竟, 任何作业随着时间的推移, 都是漏洞百出的。而且, 让别人抄你的作业, 不香吗? 老抄作业, 啥时候是个头呢?

我觉得2011年的是时候,国内公司的安全状况不容乐观的原因,可能就和没能力抄作业有关系。





很多样例代码都是错的,被复制粘贴到各种工程中 展开~

作者回复: 是的, 很遗憾样例代码会过时的。样例代码的维护是一个很大的问题。 这是一个很棒的角度!





runner

2020-12-11

期待老师关于密码学更多干货, 理论附带工程实践!

展开٧

作者回复: 我加油!





罗乾林

2020-12-11

突然有个想法:

如果我们积累足够多的历史数据,用现在流行的深度学习能不能训练一个模型能够破解密码

作者回复: 2^128的安全强度,现在的计算能力应该没有办法,深度学习也不行。量子计算时代, 2^128的安全强度,就不敢说还安全了。





孜孜

2020-12-11

我倒是有点疑惑,日常工作,凡事有人和我讨论安全和漏洞,我基本上来就是一句话,保持framework和package更新。。对于加密,目前我们都上了https,其他的也都在tls上。对于我来说,就是紧跟业界推荐,让我disable或者升级什么,我就干什么。 其实我不认为我有实现加密算法的能力,甚至我也没有使用加密算法能力,我充其量就是个配置

者。。其实我对这门课程的期待就是,当我去做升级和disable某些算法时候,能心中有… 展开~

作者回复: 能主动地跟上业界推荐,及时更新,其实就解决了大部分问题了。这是我期待的结果之一。我期待的另外一个结果,就是希望你能够对常见算法心中有数。需要使用算法的时候,能够有意识,可以通过查阅资料和相关规范,快速跟上。

