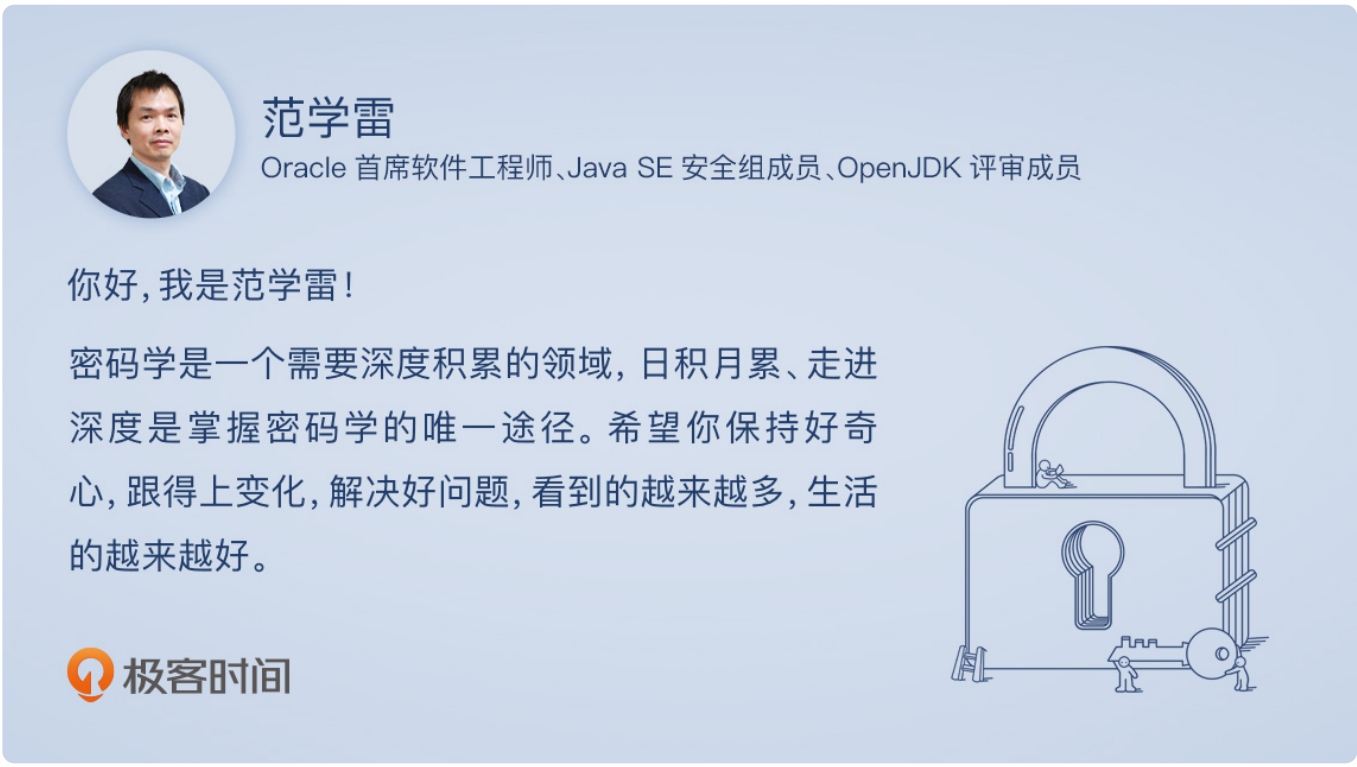
结束语 | 深挖坑、广积粮

2021-01-11 范学雷

实用密码学 进入课程 >



讲述：范学雷
时长 04:24 大小 4.05M

你好，我是范学雷。

我觉得自己是一个写字还算快的程序员。

从第一段文字开始，到着手写这一篇结束语，也有八九个月的时间了，还包括利用了近两个月的休假。如果当初我能够想象得到，每一讲的文章，都要写一两个星期的话，我是断断不敢有写这个专栏的一星一点的想法的。2020 年初，我一不小心给自己挖了一个大坑。

不过，现在回头看看，所有的付出时间都是有收获的。2020 年初挖的坑，我在 2020 年还是给填上了。

珍惜踩过的坑

其实，**我们踩过的每一个坑，最后都会变成我们脚底的一块砖**。在我想着怎么把我记忆里的东西表达成文字的时候，在我想着怎么把复杂的东西用简单的形式叙述出来的时候，在我想着怎么呈现技术背后的基本原理和基础逻辑的时候，我都在积攒着对密码学更深的理解和认识。

对于我自己而言，密码学具有神奇的魔力。

我在这个领域已经工作了二十多年，一点儿也没有感到厌倦。密码学领域的工程实践，依然对我有巨大的诱惑力；其中的很多问题，也一直吸引着我继续在这个领域里去摸索。

我每一年都要看很多论文，每一年都要解决很多新问题，每一年又会发现很多新问题，几乎每一年都有完全不一样的挑战。也许，这就是密码学和密码学工程实践的魔力所在吧。

其实，**别人踩过的每一个坑，也都可以变成我们脚底的一块砖**。

不过，这需要我们去寻找，去分析，去汲取。相比较而言，密码学本身并不难学，困难在于追踪密码学的最新进展，了解密码分析的最新动向，知道什么时候该抛弃，知道什么问题该避免。

信息安全危机和数据泄漏的代价是巨大的，我们不能等着掉进坑里后，再去想怎么从坑里爬出来。所以，我们要关注、珍惜别人踩过的坑。如果说学习密码学有捷径的话，就是去深挖别人踩过的坑，让每一次公开的信息安全危机，都成为你脚底的一块砖。

积累学过的粮

珍惜自己和别人踩过的坑，还不够，我们还要给自己积累更多的粮。

比如说，看到了 Zoom 安全问题的报道，就不能仅仅把它当作一个故事，我们要去寻找更多的材料，去了解这个安全问题的技术细节，以及解决这个问题的具体方案。

我们可以创建自己的“禁止清单”和“爬坑清单”，在我们要去检查我们自己的产品有没有类似的问题时，**给自己的“禁止清单”添加新的条目，给自己的“爬坑清单”添加新的场景和解决办法**。

如果我们每一年都读很多论文，每一年都分析很多安全事故，每一年都解决很多新问题，每一年都遇到新挑战，毫无疑问地，我们的“禁止清单”就会越来越厚，“爬坑清单”也会越来越实用。

只要我们没有丧失兴趣，在这个领域的积累就会越来越多。我们站的越高，我们就有越多的机会看到更多的风景，包括很少人才能看到的风景。

深挖坑，广积粮，这是我送给你的学好密码学的一个小建议。

送君千里，终须一别

终于还是到了要说再见的时候了，但是这只是这个专栏的结束，却是你新的开始。希望这个专栏里提出的问题，给你思路和启发，让你在之后的密码学学习中，发现新的问题。

我说过，密码学就是在一个又一个的问题里蓬勃发展的，不管你以后遇到多么艰深的困难，我都希望你可以停下来思考一小会儿，看看自己有没有什么想法，有没有更深入的见解。

送君千里，终须一别。希望这一路走来，曾有文字和观点可以让你开心和愉悦，也许只是一个小思路的点拨，也许只是一个新的知识点，还有可能是那只喝茶吃酒的喜鹊。

无论怎样，都是你与我的宝贵回忆，有幸与你相遇在这个专栏，走过这样一段路。写的文字有人读，然后才能有想法的传递。谢谢你阅读我写的文字！

如果他日有缘相遇，我们再叙衷肠。

《实用密码学》课程结束了，这里有一份毕业问卷，题目不多，希望你能花两分钟填一下。十分期待能听到你说一说，你对这个课程的想法和建议。

提建议

上一篇 20 | 综合案例：如何解决约会难题?

下一篇 结课测试 | 这些密码学的知识，你都掌握了吗?

精选留言 (2)

写留言

25ma
2021-01-11

感谢老师倾壤相授，让我对密码学知识有了一个新的认识和提高

1

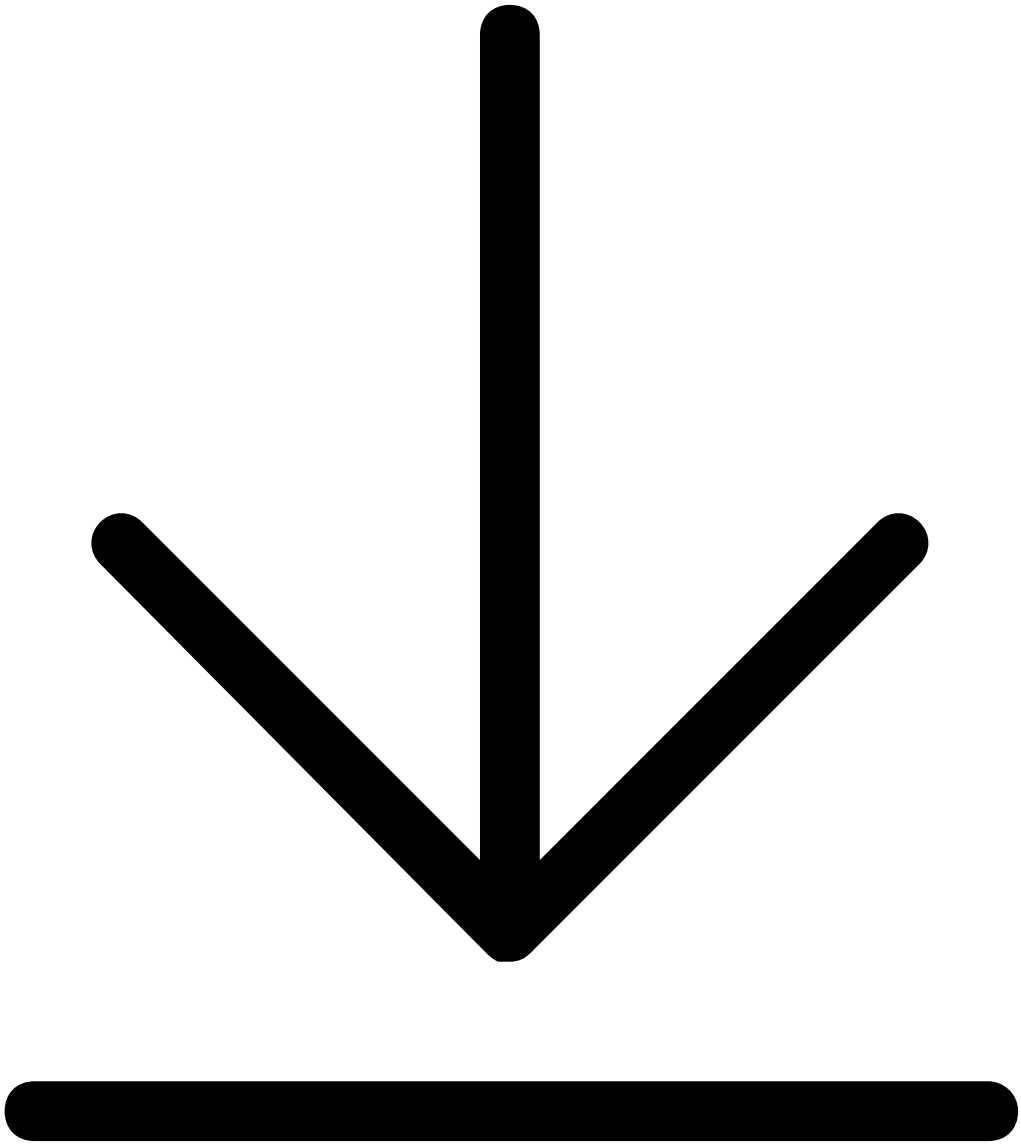
孜孜

2021-01-11

有什么好的网站可以看到别人的坑呢?

展开

作者回复: 来源比较零散，关注世界性的信息安全大会，以及信息安全的新闻。https://thehackernews.com/可能是信息比较密集的一个网站。



拖拽到此处
图片将完成下载