针对移动设备的 FREAK 攻击

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	FREAK Out on Mobile		
原文作者	Yulong Zhang, Hui Xue, Tao Wei, Zhaofeng Chen	**原文发布日期**	2015 年 3 月 17 日
作者简介	Yulong Zhang 是火眼公司的高级软件研究工程师。www.linkedin.com/pub/yulong-zhang/22/385/b05/en Tao Wei 是火眼公司的高级研究科学家。在加入火眼公司前，他担任北京大学的副教授和加州大学伯克利分校的来访项目科学家。www.linkedin.com/pub/tao-wei/26/60/25/en		
原文发布单位	火眼公司		
原文出处	https://www.fireeye.com/blog/threat-research/2015/03/freak_out_on_mobile.html		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
免责声明	本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。		

针对移动设备的 FREAK 攻击

Yulong Zhang, Hui Xue, Tao Wei, Zhaofeng Chen

2015 年 3 月 17 日

自心脏出血漏洞后，最近披露的 FREAK 攻击[1]再一次引发了人们对 TLS（安全传输层协议）实现的安全性的关注[2]。然而，致力于客户端安全检查的 freakattack.com 只检查各种浏览器。在这篇博客中，我们研究 iOS 和 Android 应用程序在 FREAK 攻击下的安全状态。

FREAK 攻击允许“攻击者拦漏洞客户端与服务器之间的 HTTPS 连接，迫使它们使用弱加密，攻击者可以破解加密并窃取或操纵敏感数据。”[1] 为使 FREAK 攻击获得成功，服务器需要接受 RSA_EXPORT 密码套件，而客户端需要在非出口密码套件中允许临时的 RSA 密钥。因此，攻击者可能会降低连接的加密强度，便于窃取数据。

截至 3 月 4 日，Android 和 iOS 平台的最新版本都容易受到 FREAK 攻击 [3]。因为 iOS 和 Android 应用程序可能包含 OpenSSL 库的漏洞版本，所以 FREAK 既是平台漏洞又是应用程序漏洞。即使厂商修复了 Android 和 iOS 系统的漏洞，当它们连接到接受 RSA_EXPORT 密码套件的服务器时还是会遭受 FREAK 攻击。苹果公司于 3 月 9 日修复了 iOS 8.2 的 FREAK 漏洞，但是一些 iOS 应用程序仍然容易受到 FREAK 攻击，原因就在于此[4]。

我们扫描了 10,985 个流行的、下载量超过 100 万的 Google Play Android 应用程序，发现其中的 1228 个（11.2%）容易受到 FREAK 攻击，因为它们使用有漏洞的 OpenSSL 库连接到漏洞 HTTPS 服务器。这 1228 个应用程序的下载量已经超过了 63 亿。在这 1228 个 Android 应用程序中，664 个采用 Android 的捆绑 OpenSSL 库，564 个使用自己编译的 OpenSSL 库；所有这些 OpenSSL 版本都容易受到 FREAK 攻击。

iOS 方面，14,079 个流行 iOS 应用程序中的 771 个（5.5%）连接到有漏洞的 HTTPS 服务器。在低于 iOS 8.2 的版本上，这些应用程序很容易受到 FREAK 攻击。771 个应用程序中的其中 7 个具有自己的 OpenSSL 版本，在 iOS 8.2 上仍然容易受到攻击。

漏洞统计

攻击者可能利用中间人（MITM）技术发动 FREAK 攻击，来截取并修改移动应用程序和后端服务器之间的加密流量。攻击者可以使用公知的技术，例如 ARP 欺骗或 DNS 劫持。攻击者不必实时破解加密，他们每周记录弱加密的网络流量，将其解密并访问内部敏感信息。

表 1 呈现了有漏洞的、属于安全和隐私敏感类别的 Android 和 iOS 应用程序的数量。不太敏感的类别，如体育和游戏，则不包含在内。表中的红色柱状代表应用程序开发人员修复的 FREAK 漏洞。对于 Android 应用程序，我们进一步绘制了同样类别的漏洞应用程序的下载量，如表 2 所示。蓝色柱状代表截止 3 月 10 日漏洞应用程序的下载量。

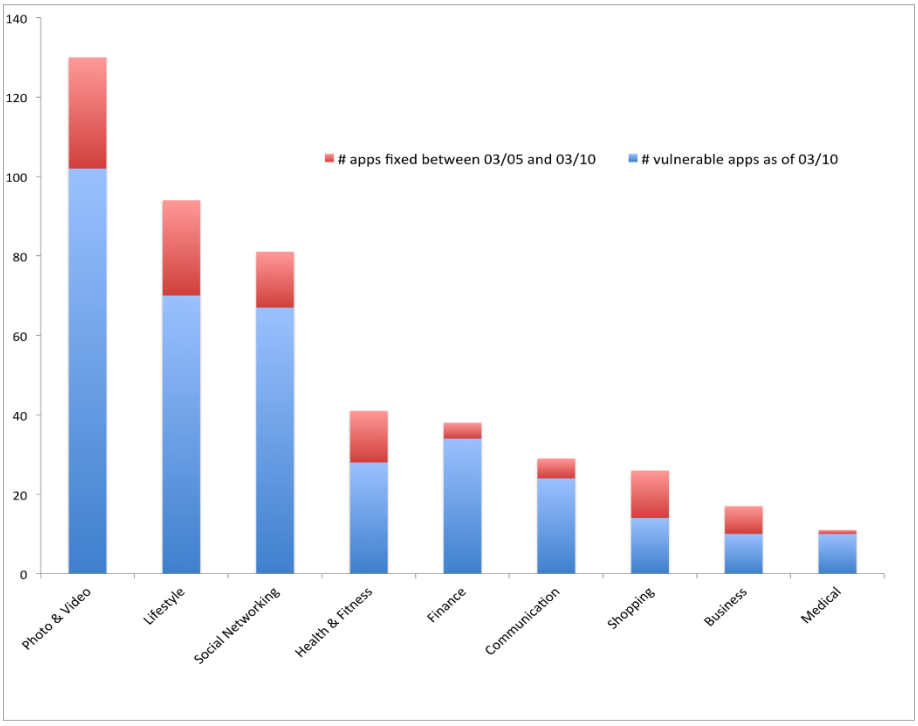

表 1：易受 FREAK 攻击的应用程序的数量

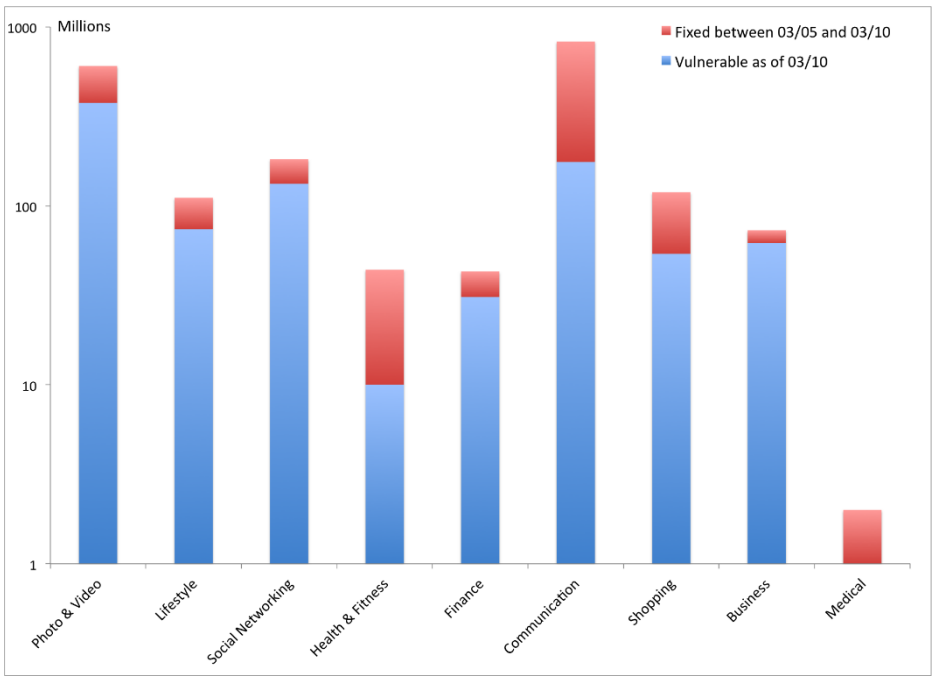

表 2：易受 FREAK 攻击的 Android 应用程序下载量（对数刻度）

攻击场景

举例来说，攻击者可以对一个流行的购物应用程序发动 FREAK 攻击，窃取用户的登录凭据和信用卡信息。其他敏感的应用程序包括医疗、生产和金融应用程序。图 1 和图 2 显示了被攻击者破解后的漏洞应用程序和相应服务器之间的明文通信。

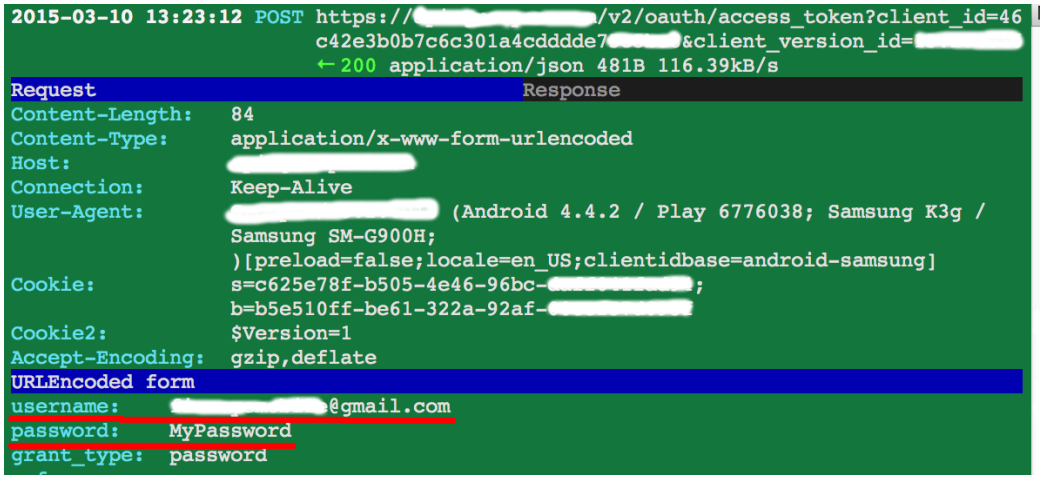

图 1：解密的登录凭据

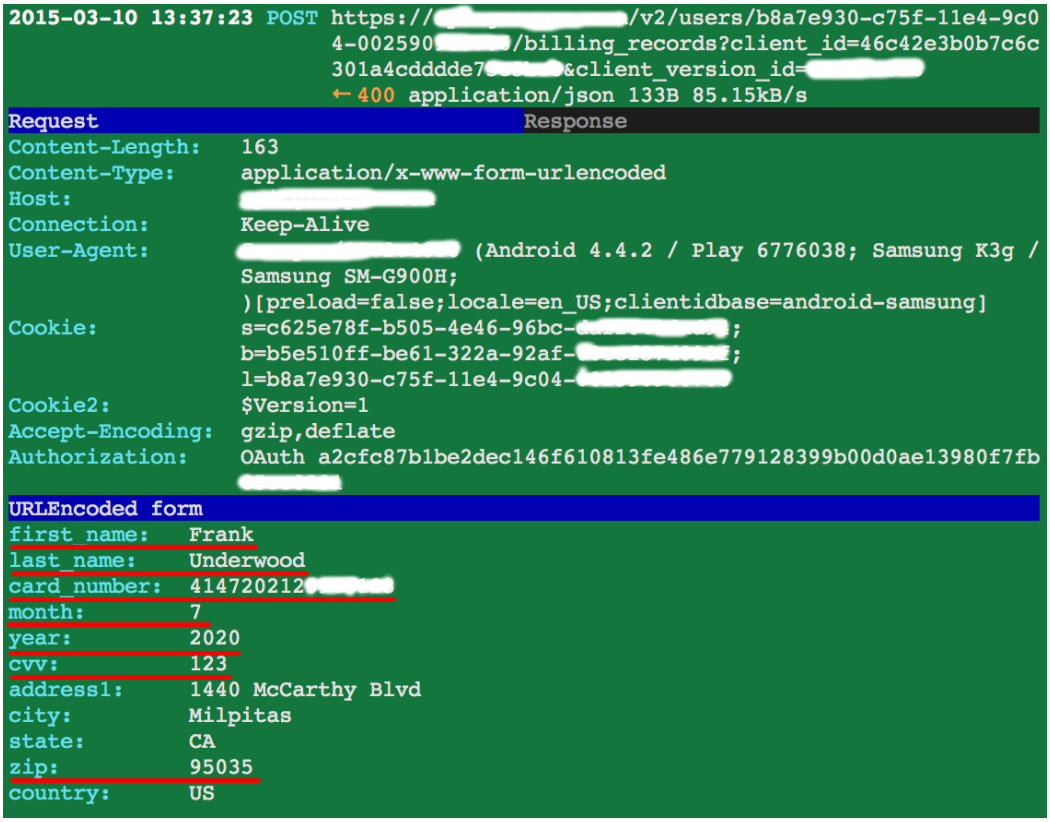

图 2：解密的信用卡信息

移动应用程序已经成为攻击者的重要前端和有价值的目标。FREAK 攻击对移动应用程序的安全和隐私带来了严重威胁。我们呼吁应用程序开发人员和网站管理员尽快解决这个问题。

参考文献

[1] https://freakattack.com/

[2] http://heartbleed.com/

[3] http://www.engadget.com/2015/03/04/freak-flaw-ios-android-ssl-bug/

[4] https://support.apple.com/en-us/HT204423