安全小课堂第138期【浅谈电子邮件安全】

JSRC 京东安全应急响应中心 5月14日

自1982年互联网诞生至今，电子邮件一直是各大互联网公司核心的沟通方式。全球每小时发送的邮件数量超过30亿封，邮件也是黑客最为青睐的获取个人or公司机密的途径，如何保护邮件的安全？

JSRC小课堂第**138期**，邀请到**京东安全攻防实验室redteam负责人**，**超级无敌大菠菜**师傅，就电子邮件安全为大家进行分享，同时感谢白帽子们的精彩讨论。

为什么要讨论电子邮件（EMAIL）安全，而不是即时通讯（IM）安全？

对于个人和企业来说，IM和EMAIL安全都很重要，两者都要考虑账号安全和消息内容安全的问题。之所以今天强调EMAIL安全，主要是因为以下几点：

1. IM比EMAIL与生俱来的安全优势。

A. 交互的封闭性，如微信不能和whatApp聊，每种IM都需要单独注册，下载特定App；

B. 相对实名制，国内外IM基本清一色采用/支持手机号登录；

C. 协议自定义，whatapp的端对端加密等。

D. 社交圈概念更浓。

2. EMAIL在安全上有更多的可操作性，国际标准。

A. SMTP/POP3/IMAP/Exchange ActiveSync/CalDAV/CardDAV over TLS。

B. 基于邮件客户端配置的PGP 或者 S/MIME 端对端加密。

C. SPF/DKIM/DMARC 等国际安全协议。

D. 各种邮件安全网关产品，防病毒、钓鱼等等。

3. EMAIL相当于IM的一些优势。

A. 匿名性，邮件是国内为数不多的不要求实名的通讯工具。

B. 正式性，尤其是企业级邮箱，是合作伙伴沟通、客服与客户沟通的最佳途径。

C. 国际通用协议，只要知道email address就可以投递，没有交互门槛。

D. 邮箱协议得到了扩展，更方便办公，如Exchange ActiveSync、CalDAV/CardDAV 实现了同步日历事项和联系人的功能。

电子邮件安全的国际标准有哪些?

在上面的问题有提到相关的安全协议，主要有以下几个：

1. 保障EMAIL传输层安全的协议，EMAIL Protocals over TLS，目前市面上提供邮箱服务的厂商都支持。

2. S/MIME（Secure Multipurpose Internet Mail Extensions），提供端对端加密通讯。

3. SPF（Sender Policy Framework），用来鉴别发送邮件的服务器或者IP，是否为该域允许的范围。基于DNS配置的，防止发信人伪造某个域名的邮件地址。

4. DKIM （Domain Keys Identified Mail），用来确保发件人地址真实存在，邮件内容未被篡改。

5. DMARC（Domain-Based Message Authentication, Reporting & Conformance非IETF国际标准），依赖SPF和DKIM，属于为收件人提供的认证上报协议，当收到某个伪造域名的邮件事可以上报给该域名（或者拒绝等处理方式）。

S/MIME：https://tools.ietf.org/html/rfc5751

SPF：https://tools.ietf.org/html/rfc4408

DKIM：https://tools.ietf.org/html/rfc4871

DMARC：https://dmarc.org/

非国际标准的邮件安全实践还有哪些?

1. PGP（Pretty Good Privacy）端对端加密。

2. 配置邮件客户端一次一密/应用专用密码，GMail/QQ邮箱

3. 基于账号安全层面的考虑更多些，账号安全不是今天讨论重点，简单举例：QQ邮箱（QQ），企业邮箱（Exchange/AD/ERP），GMail(Google凭证)

A. MFA二次认证

B. 基于移动端设备的二次认证

C. 管理邮件客户端/邮件客户端协议（POP3/IMAP/Exchange）

D. 审计账号登录信息

PGP可以使用开源版本：https://www.openpgp.org/

安全电子邮件有哪些使用场景?

这里的安全电子邮件是指，同时开启TLS和S/MIME（或PGP）的方式（SPF/DKIM/DMARC因为需要运维配置）。

A. 国家大选、民主人士、国家涉密单位、银行、证券等

B. 企业信息安全部门，如MSRC与白帽子在漏洞方面的互动，

C. 企业财务部门，尤其是上市企业，财报等

D. 企业高管，公司的战略规划等

E. 企业运维、DBA等

F. 其他对邮件安全有特殊需求的人群

怎么才能做到绝对的安全?

1. 没有绝对的安全，只能比"别人"做的更好
2. 采用S/MIME或PGP 加密邮件
3. 关于EFAIL，EFAIL攻击可以让攻击者有可能读取到PGP和S/MIME电子邮件的内容。

前提1，已经搞定了你的邮件账户/邮件服务器。

前提2，搞定了你的TLS证书，并且可以监听你的网络。

前提3，搞定了你的装有邮件证书的计算机。

客户端不配置证书，通过命令行解密。参考 https://efail.de/

哪种方式最适合我?

因人而异，对号入座。

企业用户

1. 开启SPF/DKIM/DMARC协议
2. 强制开启Mail Protocols over TLS
3. 邮件安全网关，实现邮件病毒扫描和垃圾邮件识别
4. 信息安全部、财务部门、高管、运维等上S/MIME

个人用户

1. 选择一个合适的EMAIL服务提供商，国际建议Gmail，国内建议QQ
2. 账号安全的配置尽可能全部开启，如MFA，短信验证，一客户端一密，账号安全检查等。Mail Protocols over TLS开启。
3. 邮件内容的加密，启用PGP或者S/MIME，comodo。
4. 邮件客户端的管理，删除长登录的邮件客户端认证；关闭掉不用邮件收取协议，如POP3/IMAP/Exchange选一个即可。
5. 定期审计个人邮件的登录等信息
6. 网络环境和终端等安全

这是JSRC小课堂陪伴你的

第3年63天

如果有你希望出现在安全小课堂内容暂时未出现

欢迎留言告诉我们

如果有所收获欢迎将它分享

让更多的人加入JSRC安全小课堂

交流

开课时间：周五下午15:30

QQ开课群：464465695

留言：针对本期主题内容，你还有什么疑问吗？欢迎留言交流~

JSRC