Sending out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways

利用公共网关的 SMS 生态系统的安全性描述

Bradley Reaves, Nolen Scaife, Dave Tian, Logan Blue,
Patrick Traynor and Kevin R.B. Butler

{reaves, scaife, daveti, bluel}@ufl.edu

{traynor, butler}@cise.ufl.edu

Florida Institute for Cybersecurity Research (FICS)
University of Florida

November 6, 2019

目录

目录

引言

研究背景

- 短信息 (SMS) 成为现代通讯的重要组成部分
- 很多组织或网站使用短信息作为身份验证的辅助通道
- 现代短消息的发送，在抵达终端之前不接触蜂窝网络

主要工作

- 对 SMS 数据进行迄今为止最大的挖掘分析
- 评估良性短消息服务的安全态势
- 刻画通过 SMS 网关进行的恶意行为

目录

短消息服务中心 (SMSC)

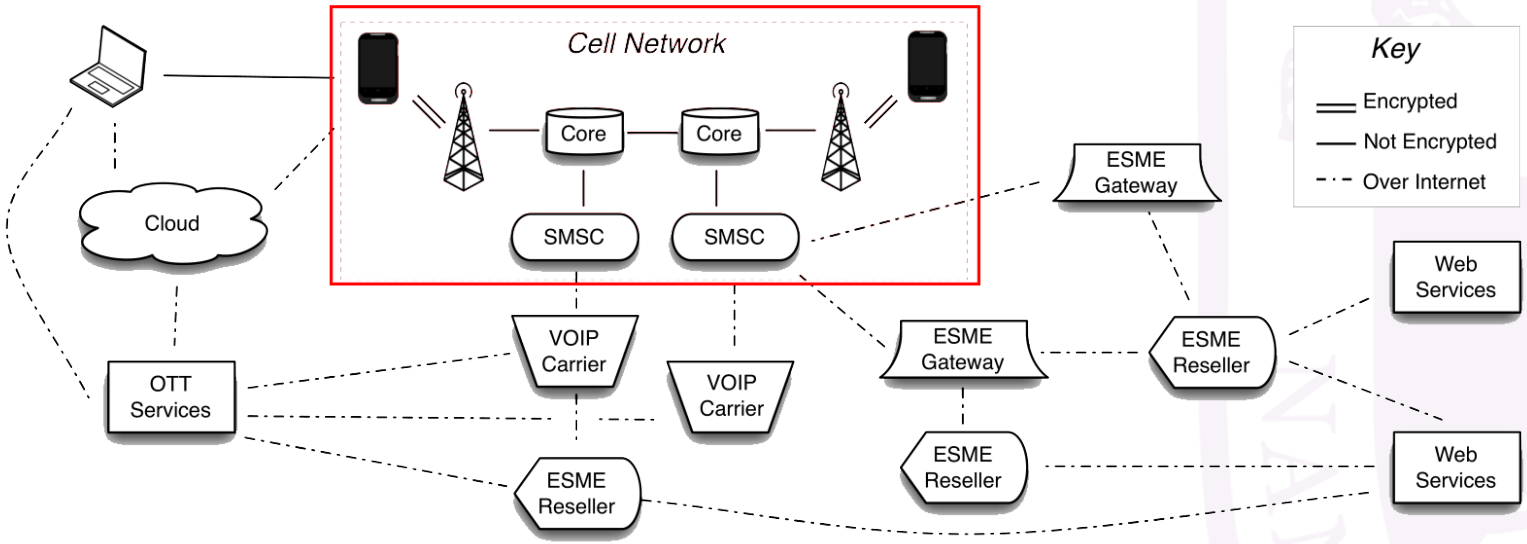


图 1: 短消息服务中心

短消息服务中心通过运营商网络路由消息，是 SMS 系统的核心。SMSC 接受文本消息，并将消息转发到蜂窝网络中的移动用户。

外部短消息实体 (ESME)

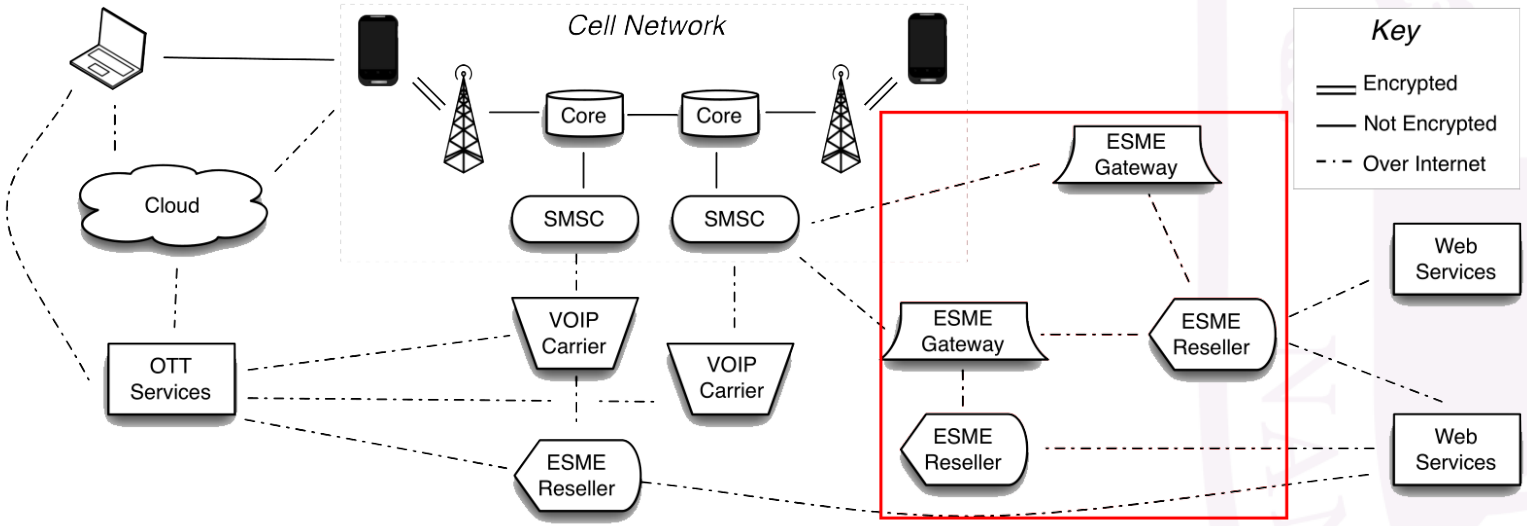


图 2: 外部短消息实体

外部短消息实体为外部组织提供针对运营商网络的短消息接入服务。ESME 可以用于紧急通报、慈善捐款、或接受一次性验证码等功能。

OTT 服务

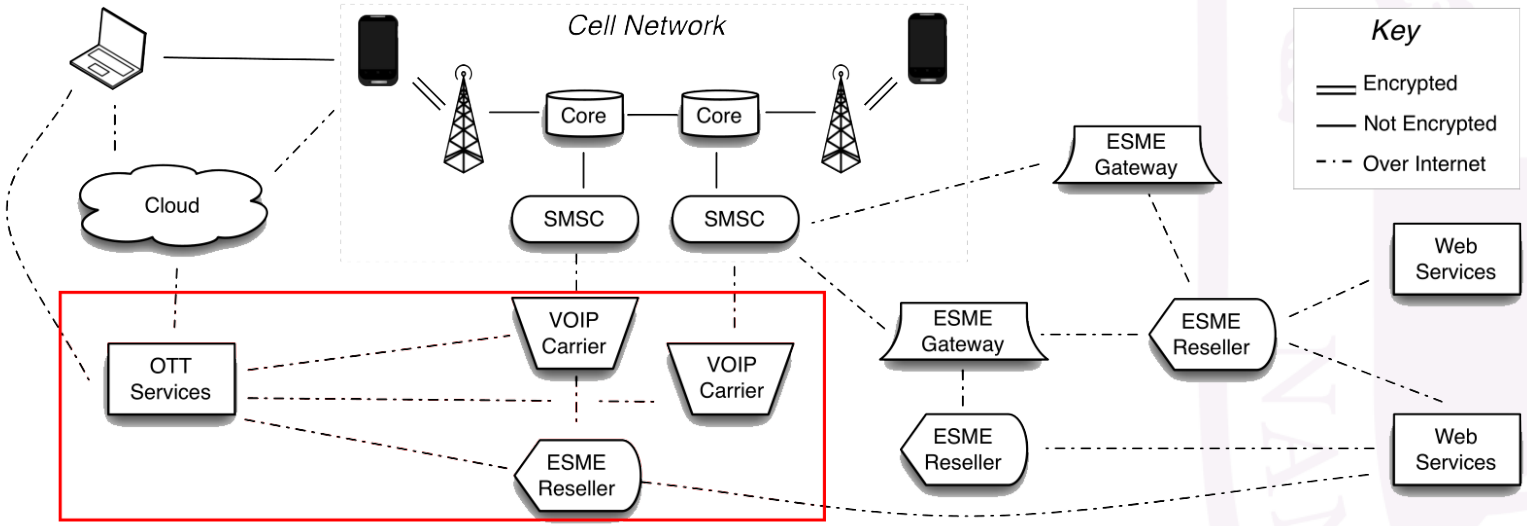


图 3: OTT 服务

OTT 服务支持在数据网络上提供短信和语音等第三方服务。
OTT 可以使用云服务来存储和同步 SMS 到用户的其他设备。

目录

爬取公共短消息网关

- 使用 Scrapy 框架爬取公共网关
- 收集 8 个公共短信网关在 14 个月的数据
- 共抓取 386,327 条数据

表 1: 公共网关及抓取的信息数

Site	Messages
receivesmsonline.net	81313
receive-sms-online.info	69389
receive-sms-now.com	63797
hs3x.com	55499
receivesmsonline.com	44640
receivefreesms.com	37485
receive-sms-online.com	27094
e-receivesms.com	7107

消息聚类分析

基本思路

- 使用编辑距离矩阵将类似的消息归于一张连通图中。
- 使用固定值替换感兴趣的消息，如代码、email 地址。
- 查找归一化距离小于阈值的消息，并确定聚类边界。

实现步骤

1. 加载所有消息。
2. 用固定的字符串替换数字、电子邮件和 URL 以预处理消息。
3. 将预处理后的信息按字母排序。
4. 通过使用编辑距离阈值 (0.9) 来确定聚类边界。
5. 手动标记各个聚类，以确定服务提供者、消息类别等。

消息分类结果

- **账户创建确认信息**：向来自服务提供者的用户提供了一个代码，该服务提供者需要在新帐户创建期间进行 SMS 验证。
- **活动确认信息**：向来自服务提供者的用户提供了请求授权进行活动的代码 (例如，付款确认)。
- **一次性密码**：包含用户登录的代码的短信息。
- **用于绑定不同设备的一次性口令**：将消息发送给用户，以绑定一个新的电话号码或启用相应的移动应用程序。
- **重置密码口令**：包含密码重置密码的短信息。
- **其他**：其他未被指定为某种特定功能的消息。

消息分类结果

- 账户创建和移动设备绑定占比最大，占 51.6%
- 一次性密码信息占 7.6%
- 密码重置消息占 1.3%
- 包含“测试”关键词的消息占 0.8%

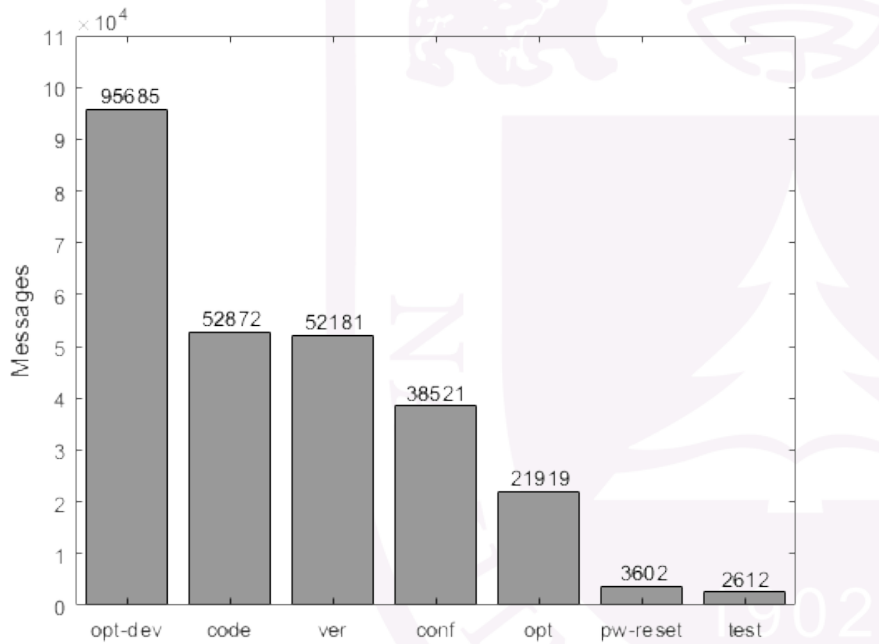


图 4: 消息的聚类

目录

使用 SMS 作为安全信道

PII 和其他敏感信息

- 财务信息
- 用户名和密码
- 重置密码口令
- 其他个人识别信息 (PII)
- 敏感程序的 SMS 活动

使用 SMS 作为安全信道

SMS 编码熵

使用 χ 方检验测试每组编码的熵。χ 方检验是一个零假设的显著性检验，用于测试 SMS 服务的编码是否是从低位到高位均匀分布的。若 p 值小于 0.01，则表明观测值和理想均匀分布之间存在统计学上的显著差异。检验结果表明，65% 的 SMS 服务的编码熵较低，容易被预测和攻击。

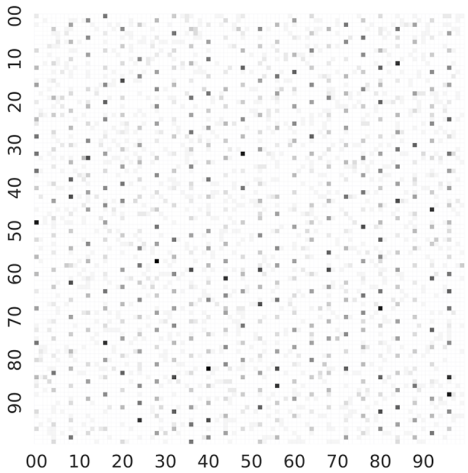


图 5: WeChat

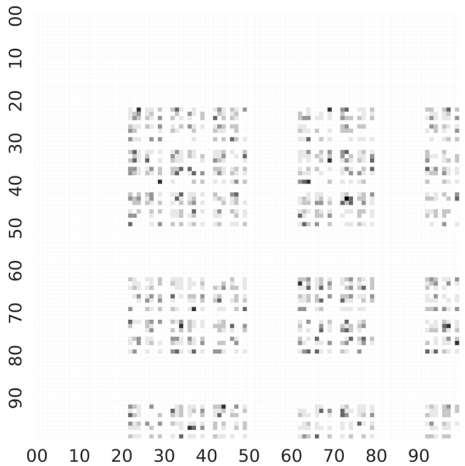


图 6: Talk2

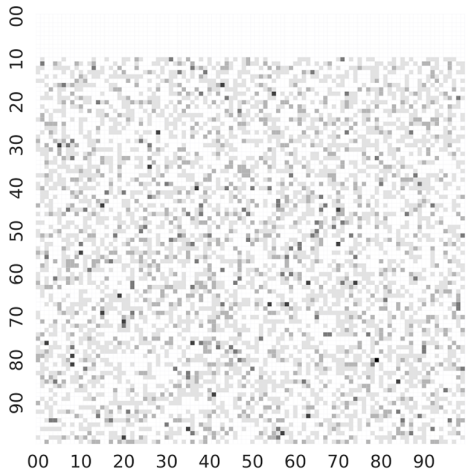


图 7: Google

SMS 的恶意应用

公共网关检测到的恶意信息

- **泄露用户位置信息**：短 URL 可以用于确定消息的源和目的地，即会泄漏用户的位置信息。
- **垃圾邮件宣传广告**：在公共网关服务中比例较低，约为 1.0%。
- **网络钓鱼活动**：试图欺骗用户，使其相信自己正与合法网站通信。

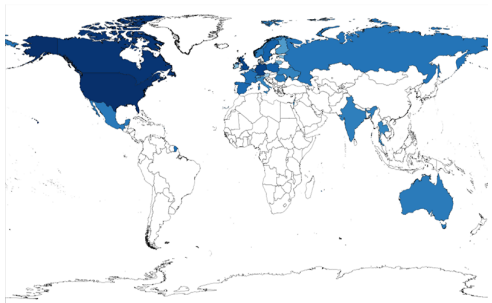


图 8: SMS 地址分布

```
Apple Customer,
Your lost iPhone has been found \
    and temporarily switched ON.
To view iPhone map location
lostandfounds-icloud*com
Apple
```

图 9: 钓鱼短信实例

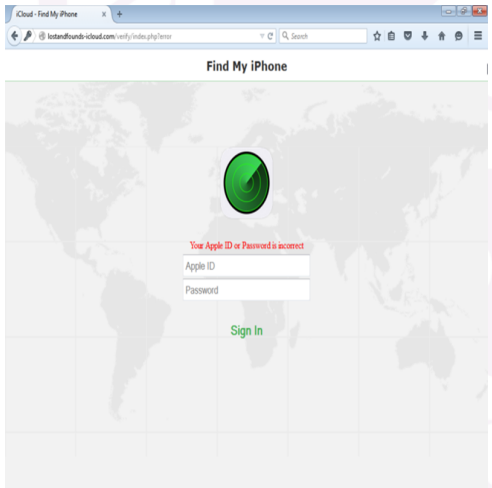


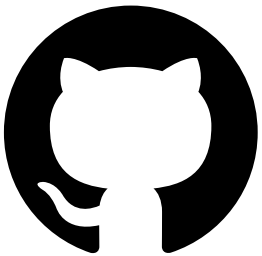
图 10: 钓鱼网站

目录

结论

- SMS 生态系统在智能手机时代出现了新的发展，加入了更多新的设备和参与者。
- 公共网关为用户提供了基于 SMS 的各种安全解决方案。
- 根据该研究，将 SMS 作为安全信道传递敏感信息存在一定的危险性。一些一次性的消息传递机制亟待改进。
- 至于短信滥用，公共网关可以用于规避一些安全性较差的认证机制，或进行 PVA 欺诈行为。

Thanks for Listening.



LaTeX Beamer template is opensource on Github now!

`https://github.com/shellqiqi/NJU-Beamer-Slide`

Welcome Star and Fork.