网络攻防技术前沿进展

崔宝江
北京邮电大学
cuibj@bupt.edu.cn

目录

- 一、传统网络攻击技术
- 二、后斯诺登时代的网络攻击技术

目录

一、传统网络攻击技术

- 效果不佳的传统攻击
  - 蠕虫攻击
  - U盘感染
- 仍然有效的传统攻击技术
  - 水坑式攻击--访问挂马网页
  - 鱼叉式攻击--电子邮件的附件和链接
  - 诱骗式攻击--网站下载

theguardian

News | Sport | Comment | Culture | Business | Money | Life & style

News › World news › Edward Snowden

Edward Snowden's explosive NSA leaks have US in damage control mode

White House refers Snowden's case to Justice Department while Republicans in Congress call for whistleblower's extradition

Dan Roberts and Spencer Ackerman in Washington and Tania Branigan in Beijing
theguardian.com, Monday 10 June 2013 19.43 BST

Jump to comments (840)

Daniel Ellsberg called Snowden's leak the most important leak in American history
Link to video: NSA whistleblower Edward Snowden: 'I don't want to live in a society that does these sort of things'

目录

- 二、后斯诺登时代的网络攻击技术
  - 数字签名的神话被打破
  - 直捣黄龙式的网络溯源技术

目录

- 二、后斯诺登时代的网络攻击技术
  - 数字签名的神话被打破
  - 直捣黄龙式的网络溯源技术

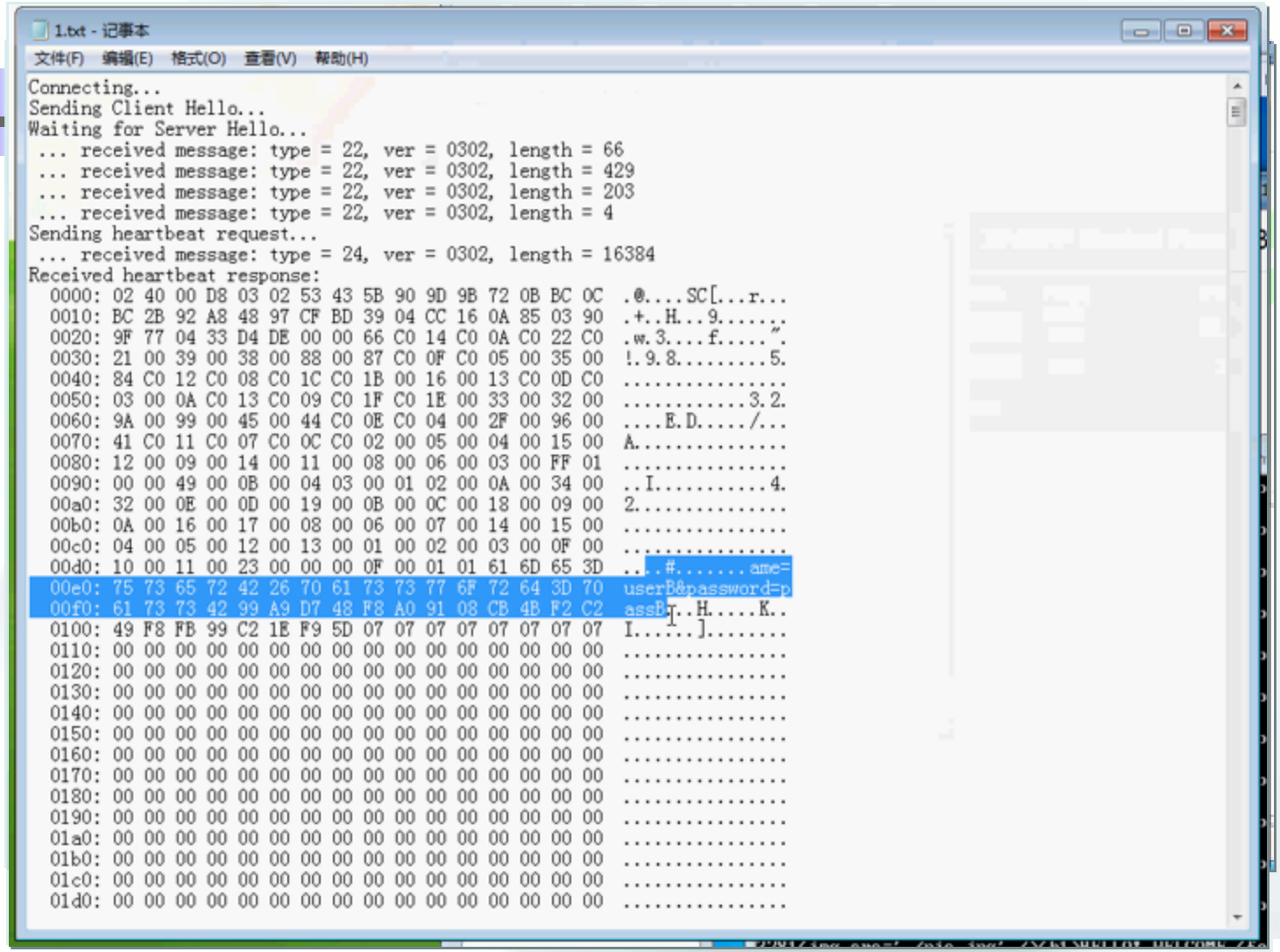
目录

二、后斯诺登时代的网络攻击技术

- 数字签名的神话被打破
  - 从传统的安全协议软件漏洞利用
  - 发展到未公开的数字签名破解方法

OpenSSL漏洞分析

- OpenSSL官网2014年4月7日发布公告
  - OpenSSL “heartbleed”漏洞（CVE-2014-0160）
  - 由安全公司Codenomicon的研究人员和Google安全小组的Neel Mehta相互独立地发现的
  - 黑客可获取与OpenSSL服务端程序毗邻的内存中64K字节的内容
    - 主要是保存在内存中解密后的登录用户名、口令、cookie等


1.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
Connecting...
Sending Client Hello...
Waiting for Server Hello...
... received message: type = 22, ver = 0302, length = 66
... received message: type = 22, ver = 0302, length = 429
... received message: type = 22, ver = 0302, length = 203
... received message: type = 22, ver = 0302, length = 4
Sending heartbeat request...
... received message: type = 24, ver = 0302, length = 16384
Received heartbeat response:
0000: 02 40 00 D8 03 02 53 43 5B 90 9D 9B 72 0B BC 0C .@....SC[...r...
0010: BC 2B 92 A8 48 97 CF BD 39 04 CC 16 0A 85 03 90 .+..H...9.......
0020: 9F 77 04 33 D4 DE 00 00 66 C0 14 C0 0A C0 22 C0 .w.3....f.....".
0030: 21 00 39 00 38 00 88 00 87 C0 0F C0 05 00 35 00 !.9.8.........5.
0040: 84 C0 12 C0 08 C0 1C C0 1B 00 16 00 13 C0 0D C0 ....
0050: 03 00 0A C0 13 C0 09 C0 1F C0 1E 00 33 00 32 00 ....3.2.
0060: 9A 00 99 00 45 00 44 C0 0E C0 04 00 2F 00 96 00 ....E.D...../...
0070: 41 C0 11 C0 07 C0 0C C0 02 00 05 00 04 00 15 00 A...............
0080: 12 00 09 00 14 00 11 00 08 00 06 00 03 00 FF 01 ....
0090: 00 00 49 00 0B 00 04 03 00 01 02 00 0A 00 34 00 ..I...........4.
00a0: 32 00 0E 00 0D 00 19 00 0B 00 0C 00 18 00 09 00 2...............
00b0: 0A 00 16 00 17 00 08 00 06 00 07 00 14 00 15 00 ....
00c0: 04 00 05 00 12 00 13 00 01 00 02 00 03 00 0F 00 ....
00d0: 10 00 11 00 23 00 00 00 0F 00 01 01 61 6D 65 3D ....#.......ame=
00e0: 75 73 65 72 42 26 70 61 73 73 77 6F 72 64 3D 70 userB&password=p
00f0: 61 73 73 42 99 A9 D7 48 F8 A0 91 08 CB 4B F2 C2 assB...H.....K..
0100: 49 F8 FB 99 C2 1E F9 5D 07 07 07 07 07 07 07 07 I.......]........
0110: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0120: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0130: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0140: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0150: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0160: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0170: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
01a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
01b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
01c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
01d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....

MS14-066 破窗漏洞

- 2014年11月，Windows安全通道（Secure Channel，Schannel）惊报漏洞，微软日前发布列为重大等级的MS14-066信息安全公告
  - 此漏洞影响带有SSL的IIS服务器，以及远程桌面。
  - 黑客可以构造特定的数据包在Schannel中远程执行恶意代码，并藉此漏洞入侵系统。

目录

二、后斯诺登时代的网络攻击技术

- 数字签名的神话被打破
  - 从传统的安全协议软件漏洞利用
  - 发展到未公开的数字签名破解方法

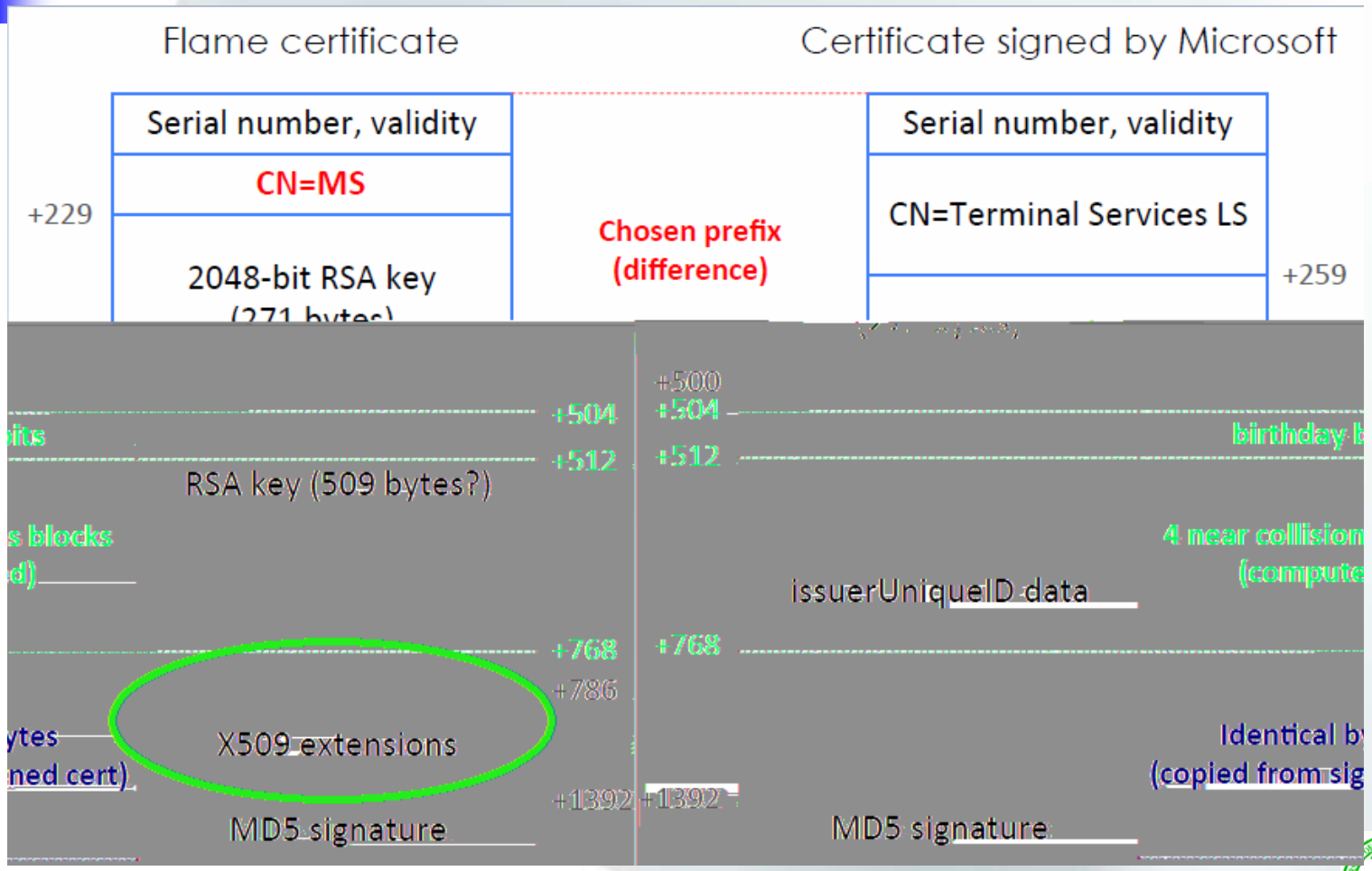
数字签名的神话被打破

- 2011年1月16日，美国《纽约时报》发表文章称，美国和以色列当初联合研制的名为“震网”的电脑蠕虫病毒，成功袭击的伊朗纳坦兹铀浓缩工厂等核设施。
  - 震网Stuxnet病毒于2009年7月被发现，可以通过移动存储介质和局域网进行传播，根据科学和国际安全研究所的统计，“震网”病毒造成位于纳坦兹的大约8000台离心机里有1000台已在2009年底和2010年初被换掉。

数字签名的神话被打破

- 2012年5月，卡巴斯基率先宣布发现攻击伊朗、以色列等多个中东国家的恶意程序，并将其命名为Flame（火焰）
- Flame是迄今发现为止程序最大的网络武器，Flame程序庞大却能隐藏得难以被发现。尽管Flame早在2010年3月就开始活动，但直到卡巴斯基实验室发现之前，没有任何的安全软件将其检测到
- Stuxnet（震网）病毒及Duqu病毒，同Flame（火焰）病毒有着深层次的关联。

数字签名的神话被打破


Flame certificate
Certificate signed by Microsoft
Serial number, validity
CN=MS
2048-bit RSA key
+229
Chosen prefix
(difference)
Serial number, validity
CN=Terminal Services LS
+259
+504
+512
RSA key (509 bytes?)
+768
+786
X509 extensions
MD5 signature
+500
+504
+512
issuerUniqueID data
+768
+1392
+1392
MD5 signature

数字签名的神话被打破

The bit differences in the near collision blocks can be used to determine what technique produced them

Using our forensic tool, we have indeed verified that a chosen-prefix collision attack against MD5 has been used for Flame. More interestingly, the results have shown that not our published chosen-prefix collision attack was used ,but an entirely new and unknown variant. This has led to our conclusion that the design of Flame is partly based on world-class cryptanalysis.

Marc Stevens, CWI.nl

小结

- 数字签名的神话被打破
  - 安全协议的应用是互联网安全的基础
  - 数字签名和加密算法的破解，将振动整个安全的基石
  - 尤其关键的是，已经大大超越学术界的最新成果
  - 数字签名一旦可被伪造，直接造就了一批防无可防的攻击手段

目录

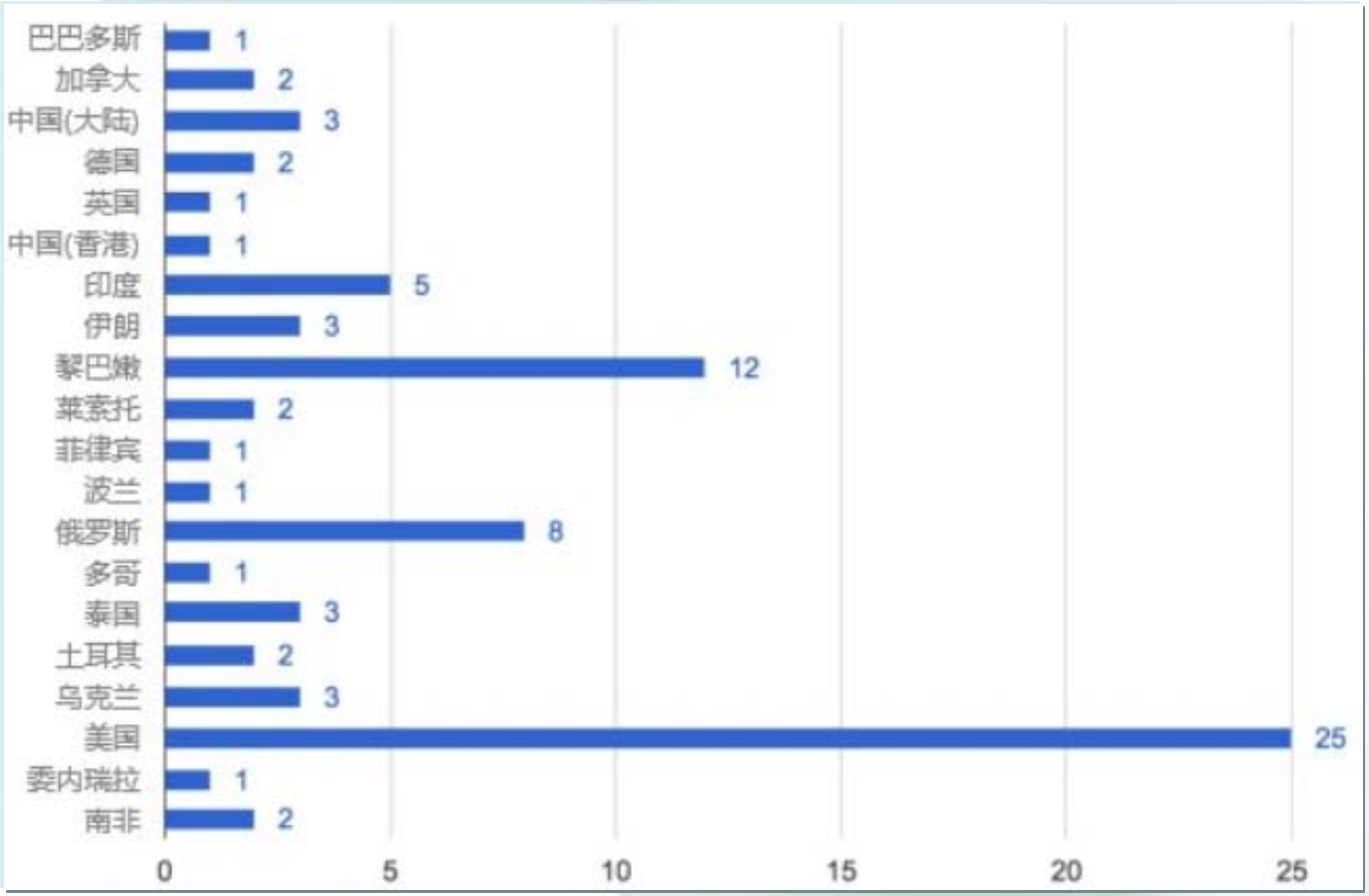
二、后斯诺登时代的网络攻击技术

- 数字签名的神话被打破
- 直捣黄龙式的网络溯源技术

直捣黄龙式的网络溯源技术

- 2015年9月份，安全公司FireEye发布报告称在19个国家的79台思科路由器上发现SYNful Knock后门程序。
- 植入的后门每次路由器重启时都会加载。它可支持高达100个模块，攻击者能够根据特定目标加载不同功能的模块。

直捣黄龙式的网络溯源技术



直捣黄龙式的网络溯源技术

- 如何获得网络设备的控制权
  - 基于黑盒的漏洞挖掘、漏洞利用、远程控制
    - 难度高，工作量大，投入大，漏洞覆盖面难以保证
  - 基于白盒的漏洞挖掘、漏洞利用、远程控制
    - 难以获得白盒环境

直捣黄龙式的网络溯源技术

- 美国《纽约时报》和德国《明镜》周刊披露斯诺登提供的材料显示
  - 美国国家安全局侵入中国华为公司在深圳总部的服务器，监控华为高管的通讯，并试图寻找华为产品的技术漏洞来监控使用华为产品的其他国家。

直捣黄龙式的网络溯源技术

- 行动代号为“猎巨人”(Shotgiant)，始于2007年
  - 首先潜入华为公司的主服务器，获取华为路由器及其他硬件的工作信息
  - 由NSA的黑客精英团队——“特定入侵行动办公室”直接在华为的网络中植入自己的后门，窃取源代码，监控那些使用华为硬件设备的网络。
  - 一份来自NSA的内部文件显示，“我们目前可以对相关网络进行正常访问，并获取了大量不知如何处置的数据。”

直捣黄龙式的网络溯源技术

- 华为被入侵的原因
  - 一是意图通过入侵华为来监控华为的产品动态；
  - 二是华为的光纤布局对其全球监视网络产生了威胁；

直捣黄龙式的网络溯源技术

- 网络设备入侵
  - 难度最高的入侵技术
  - 效果最好的入侵技术
    - 溯源直捣黄龙
    - 攻击防无可防

总结

- 倡议：共同构建“高校网络安全威胁大数据预警分析平台”
  - 北邮将提供网络安全威胁检测分析预警软件
  - 攻击数据汇总到有条件高校的大数据平台
  - 对全国高校的网络攻击提供实时攻击预警

总结

- 网络攻防，技术为王
  - 鼓励创新，崇尚探索
  - 弯道超车，容纳失败
  - 百花争鸣，遍地开花
  - 教学改革，培养特长

Q & A