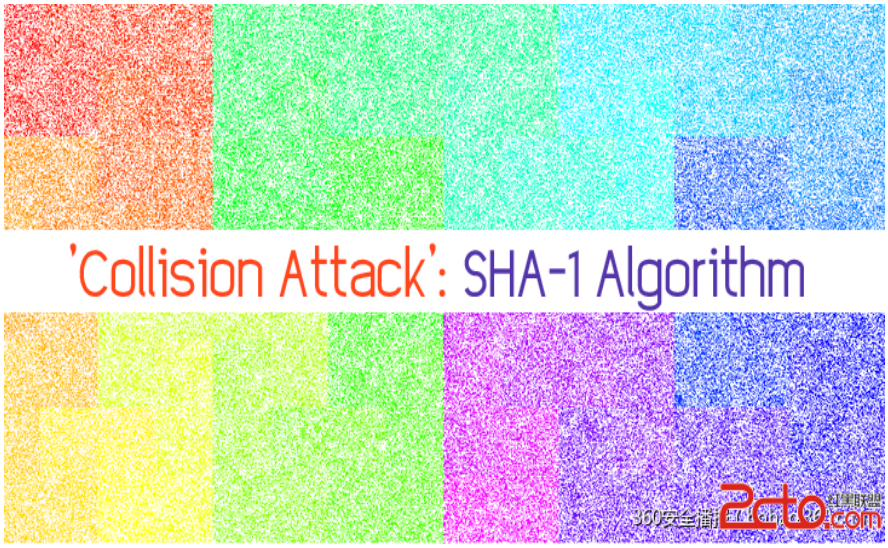
冲突攻击：广泛使用SHA-1散列算法将被立即停用

发布时间：2015-10-12 16:40:00 来源：论坛 作者：红黑联盟

关键字：新闻



SHA-1——互联网被广泛采用加密散列函数中的一个—— 已经要被停用了。

是的，破解SHA1算法所需要的时间和成本远远没有此前预期的那么多。

根据一组研究人员所说，SHA-1薄弱到完全可能会被破解，并且是在未来三个月内被黑客攻破。

该SHA-1算法是在1995年由美国国家安全局(NSA)设计的，作为电子签名算法的一部分。和其他散列函数一样，SHA-1将任何输入的信息转换成一个由数字和字母组成的长字符串，即把这条信息变成一个加密的指纹信息。

这和指纹很相似，因为只要它们时独一无二的，它们就是唯一的所得散列。如果两个不同的输入产生了相同的散列时(也可以称为冲突)，这可以用来为黑客提供各种各样的可乘之机，黑客可以利用这个破坏银行交易，软件下载，或任何网站通信的网络安全。

对SHA-1算法的冲突攻击

来自荷兰的Centrum Wiskunde&Informatica，法国的INRIA和新加坡南洋理工大学的研究人员发表了一篇论文，表明SHA-1算法很容易受到相同冲突的攻击，这被他

最新报道

贵阳再发“英雄帖” 邀君5月共赴大
“雾霾”中的朋友圈,那些打码的照
爱数签约国家教育部备份项目
《太子妃》新春喜乐会,第三个结局
Chinapex创略：用定制化程序化平
酷6四季度首度盈利 VR战略引关注
小屏iphone5SE要回归,竟有这些良
应用号或把微信变成“互联网操作系

专题 视频

监控真实用户访问体验，企业需要借一双“慧眼”
在互联网环境下，企业面临各种竞... 详细

2015联想开放架构大会比特网直播
2015惠普软件DevOps大会专题
融所有,变所需 华为云化数据中心网络SDN
H3 BPM正在掀起一场自上而下的管理创新浪潮

比特焦点

贵阳数博会 utm安全网关 下一代防火墙 统一安全网关 硬件防火墙 企业级防火墙 企业IT采购引擎 热点新闻 网宿互联网大会 第六届CIO年会 软交会 IDF 2013 爱普生 MWC CES 云计算 虚拟化 vmware 企业IT采购 oracle 微软 Windows8 大数据 CMO CIO ThinkServer ARM Windows Server 2012 BI hadoop 超级本 移动信息化

邮件订阅

☐ 软件信息化周刊 ☐ 商务办公周刊
☐ 网络周刊 ☐ 服务器周刊

们称为Freestart 冲突(Freestart Collision)。

冲突攻击出现在以下情况：当相同的散列值(指纹)产生了两个不同的信息时，就可以被利用并伪造电子签名，从而使攻击者破解使用SHA-1算法编码的通信。

破解SHA1算法目前需要$75,000到$120,000的成本

早在2012年，著名的安全研究员布鲁斯预计，到2015年，开展SHA1冲突攻击将花费$ 700,000，而到2018年，仅仅需要$ 173,000。

然而，根据新的研究，这样的攻击可能会在今年进行，花费$75,000到$120,000——而这多亏了一项新的显卡技术的发明的“自食其果”，冲突攻击是从中发现的。

研究论文中这样说道：“我们的新的基于GPU的预测更加精确了，而且这些是显著低于施奈尔估算的。更令人担忧的是，他们已经在理论上从今天的犯罪集团的资源进行了施奈尔估算，比此前预期的早了2年，SHA-1算法在1年之前就被标记为不安全。”

在一切都来不及了之前推进SHA-2或者 SHA-3

从已公布的调查结果来看这些都是理论上的，并不会造成任何即时的危险，但我们强烈建议管理员从SHA-1算法，尽快迁移到安全的SHA-2或SHA-3散列算法。

管理员应考虑SHA-1散列算法对于他们的组织和规划所带来的影响：

1.SHA-2/SHA-3的硬件兼容性

2.服务器软件更新是否支持SHA-2/SHA-3

3.客户端软件是否支持SHA-2/SHA-3

4.自定义应用程序代码是否支持SHA-2/SHA-3

SHA-2算法是由美国国家安全局开发的，而SHA-3由一组独立的研究人员开发。

返回比特网首页>>

相关文章：

为什么Google急着杀死加密算法SHA-1
破解MD5和SHA-1不意味密码破解
浅谈MD5和SHA-1被破解和应用改进策略
专家观点:破解MD5和SHA-1不意味密码破解(图)
专家观点:破解MD5和SHA-1不意味密码破解(图)
ASP.NET中MD5和SHA1加密的几种方法

[责任编辑：小石潭记] [我要挑错]