未来网络安全，靠“信誉”计算

今天的网络安全威胁，正迫使我们不得不从惯用的亡羊补牢，转向防微杜渐的安防策略。这也使得“信誉计算”成为未来网络安全的新希望。

当您生病就医时，医生如何确诊您的病症呢？通常，医生会遵循一系列常规步骤，先问您哪儿不舒服，然后测量体温。基于这两项结果，医生可以大致了解您的病情。不过，单凭这些信息医生还不足以找出确切病因，他们还必须将这些信息与几十项其他数据（如血压等）关联起来进行分析，这样医生才能非常自信的确保诊断准确、对症下药。

同样，网络安全信誉系统也依赖于大量数据间的关联关系。多年来，从医生诊断疾病到数学家为金融工具评级等诸多领域都在借助这些系统评估状况、制定决策。

如今，随着越来越多的用户借助更多设备访问在线工具，同时与同事、朋友和陌生人在越来越多的在线平台上保持交流互动，信誉计算工具对网络安全越发重要。信誉为基于互联网的人物和业务的真实身份的可靠性和完整性提供了令人安心的保证，这在物理环境下是无法实现的。

什么是信誉？

维基百科将信誉定义为“一个人、一群人或一个组织根据某一特定标准对一组实体的看法（技术上称为“社会评价”）。我们在这里所讨论的信誉与电子实体有关，例如，文件、发件人和网站等。

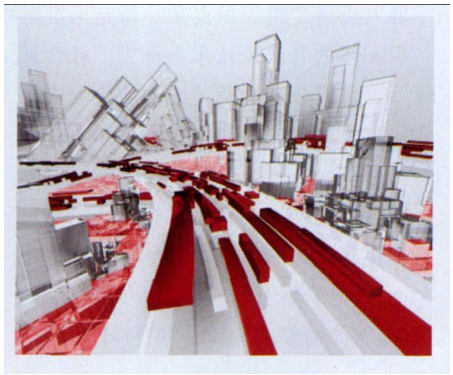
首先，信誉是动态、暂时的。例如，以前合法的网站受到恶意软件感染后就会被迅速揪出来，标记为危险网站，也就是说信誉必须与内容保持同步更新。其次，实体信誉很少出现“绝对好”或“绝

对差”的情况，而是介于这两者间广阔的“灰色地带”。信誉与策略相结合有助于安全决策者制定明智决策。最后，可信度是计算信誉时一个重要的考量因素。可信度是指我们估算的置信区间或可靠性。分析时考虑的数据点和评价标准越多，计算出的信誉越准确。有利于提高信誉可靠性的四大因素是：数据量、数据寿命、数据可信度和广泛的数据关联性。

信誉计算以数以亿计的电子实体为基础，包括文件、网站、Web 域、邮件、DNS 服务器和网络连接。同时采用高度细化的评分系统，该系统是以各种实体行为、特性相关信息以及人们对类似实体表现的过往经验为基础的。

信誉不仅是安全系统的重要组成部分，而且是必要部分。当前的威胁攻击太迅速、太隐匿，以致无法依靠传统技术（例如基于签名的保护和黑名单等）进行拦截。如果威胁意在攻击更多计算机，那么它的传播速度要比编写和部署签名的速度快得多，而且黑名单解决方案无法像信誉评分那样发现细微差别。另一方面，我们看到攻击性强、有针对性威胁的目的不单单是迅速蔓延，而且要规避检测、降低影响，以实现隐蔽、目标更明确的攻击。为抵御这两种极端威胁（以及介于两者间的任何威胁），安全专业人士以及解决方案供应商都认识到，当前的威胁态势要求系统必须能够根据所采集的实体智能信息实时计算实体信誉，并基于信誉采取适当措施。

2009 年末和 2010 年初，对 Google 和其他 20 多家企业发起攻击的极光行动（Operation Aurora）就是以特定人群为目标的有针对性威胁。攻击者使用复杂的规避技术潜入这些用户的机器，进而窃取公司宝贵的信息和知识产权。尽管诸如极光行动这样的威胁会竭力逃避检测并且隐匿颇深，但它们总会使用一些相关实体（例如，从临时有害 IP 地址发出旨在诱骗毫无戒心的用户打开受恶意软件感染的网站的电子邮件），这些实体的信誉会不断变化。



确保信誉计算具有高置信度的四大要素

除了作为可靠信誉系统的基础，对于以下列方式增强置信度，遥测数据同样十分有用：

- **数据量。**可将其想象为望远镜的光圈：数据量（进光量）越多，观察者看到的空间越远。这使我们能够迅速察觉威胁活动，更准确地识别威胁。
- **数据寿命。**长期采集数据有助于增强系统成熟度，可确保信誉系统有一个扎实的基础，有助于基于实体过去的行为来预计实体可能的行为方式。这不仅有助于及时检测到异常行为，而且还有助于基于公认的模式识别攻击。
- **数据可信度。**处理信誉系统时，数据可信度是一个需要认真考虑的要素。强大的信誉系统必须具备验证所收到的数据并调整数据源可信度的机制。诸如位置、配置和数据源过去行为等因素会影响源数据在整体信誉计算中的权重。
- **数据关联性。**强大信誉系统的核心要素是能够采集并关联来自代表所有威胁载体的广泛源的遥测数据。数据能够关联代表了威胁方方面面的数据就如同拥有了完成拼图的所有图块。

信誉的威力

从所有载体采集数据可以帮助我们了解威胁，更准确地计算任何涉及威胁的实体信誉。基于信誉的安全理念已流行多年，但今天我们不得不应对数量激增的威胁，包括快速传播的病毒、目标明确且规避性强的 IP 劫持等各类攻击。应对这些挑战需要一个统一的、客观的安全框架，以了解并评估不断动态变化的实体的安全状态。高度可信地了解实体状态（源自一组可信的关联遥测数据）是提供全面保护的基石。

警惕 Android 扣费门

近期，360 手机安全中心接到大量用户反馈，称下载了免费 Android 软件后，莫名被扣走了大量的话费。经过手机安全专家分析和排查发现，目前 Android 平台最新出现的扣费恶意软件采用将恶意代码植入正常软件的方式，此前发现的比塞班（Symbian）扣费程序更加隐蔽，整个扣费过程均在后台完成，普通用户完全无法感知。

据悉，目前 Android 平台恶意软件开始采用 SP 吸费的模式来非法获利，被植入扣费代码的软件在安装后，或立即发作或定时发作，私自向 SP 号发送业务定制信息，屏蔽 10086 的扣费确认短信并自动回复，完成扣费后自动删除短信记录，整个过程完全暗箱操作，用户无法看出任何痕迹。所以特别提醒广大用户加以小心，随时检查消费记录，一旦遇到异常，及时联系相关运营商部门进行核查。Android 平台的恶意软件目前已形成一条完整产业链，并借鉴了流氓软件在 PC 端的做法，扣费很隐蔽，手段则无所不用其极。