第21话

网络攻击和防御

简单是最终的复杂。

– 达芬奇

这里没有安全措施 继续前进!

– 理查德克莱顿

21.1 简介

在本章中,我将尝试将安全的网络方面整合到一个连贯的框架中。这并不简单,因为很多网络安全都是实际工程;计算机科学的纯粹主义者可能会将这个领域视为一个堆在另一个堆上的堆垛机。网络安全对许多开发人员来说可能并不那么重要:如果您为 Android 和 iPhone 编写与 AWS 或 Azure 上的服务通信的应用程序,那么您可以将大部分的担心留给亚马逊或微软。

但许多组织需要关注网络安全,并且有一些可见的战略趋势。二十年来,人们普遍认为公司将拥有受信任的内部网络或 Intranet,并通过防火墙保护免受 Internet 的影响;虽然拥有机密内部网络的国防和情报组织采取了极端做法,但大多数普通公司都认为较温和的版本是最佳做法。有些行业没有可行的替代方案。例如,工业控制系统中使用的协议 DNP3 和 Modbus 不支持加密或身份验证,因为它们是在租用线路和专用无线电链路时代发展起来的。到 1990 年代后期,控制系统工程师将传感器和执行器连接到 IP 网络,因为它们更便宜 然后意识到世界上任何知道传感器 IP 地址的人都可以读取它,并且任何知道执行器 IP 地址的人都可以激活它。这导致销售理解这些协议的防火墙的专业公司的增长;能源公司有数千个。一个典型的电

变电站可能有来自多个供应商的 200 台设备,在性能至关重要的 LAN 上,因此改造加密是不切实际的;但它只有一个与外界的连接,所以你必须在那个地方进行保护。这称为重新周边化。同样的方法也适用于车辆,内部 CANBUS 无法受到保护,因此与外界的无线电接口必须受到保护。

但在许多公司中,趋势坚定地朝着另一个方向发展,即去边界化。一位思想领袖是谷歌,它推广一种没有防火墙的架构,它称之为零信任安全模型:“通过将访问控制从网络边界转移到个人用户和设备,Beyond Corp 允许员工、承包商和其他用户更安全地工作从几乎任何位置无需传统 VPN。”谷歌的经验是,向移动和云技术的转变使得网络边界变得越来越难以定义,更不用说警察了,如果一家公司足够大以至于一些内部妥协是不可避免的,那么边界是放置主要保护的错误位置[1984]。仍然存在一些外围防御,最显着的是针对拒绝服务攻击,但内部网络在其他方面没有特权,重点是对用户和设备进行严格的身份验证和授权:每项服务都有一个面向互联网的访问代理。

人们可能会将其视为按服务提供的防火墙,而不是按建筑物提供的防火墙,但它在敏感度层、设备清单服务和访问控制引擎 [1479] 方面还有很多。您还需要非常好的 HR 数据,这样您就可以将员工和承包商与允许他们使用的设备和服务联系起来。其他运营大型数据中心的公司正在采用几乎相同的架构,零信任安全现在是 NIST [1618] 标准草案活动的主题。毫无疑问,由于在家工作的大量增加,它会从大流行中得到提振。

其他组织可能会采用混合方法。例如,我工作的大学在外围有一些防御措施,但主要是让部门做我们自己的事情;计算机科学系与人文系或财务部门的要求截然不同。

为了探讨选项和限制,我首先要讨论网络工作协议,例如 BGP、DNS 和 SMTP,以及滥用它们可能导致的服务拒绝攻击。然后,我将仔细研究恶意软件,然后是过滤和入侵检测等防御技术,以及防御者如何协调它们。然后,我将调查广泛使用的加密协议(如 TLS、SSH 和 IPsec)的局限性,以及认证机构特别棘手的角色。最后我将回到网络架构。许多诉讼都很复杂且相互关联,有一些重要的权衡取舍。例如,各种端到端加密可以带来好处 尤其是在对抗批量监控方面 但会妨碍我们为网络安全而进行的监控。

本章将讨论固定网络,我将讨论有什么不同 erer
关于移动网络在下一章。

21.2 网络协议和拒绝服务

我假设您对基本网络协议有所了解。电报摘要如下。互联网协议 (IP) 是一种无状态协议,可将分组数据从一台机器传输到另一台机器； IP 版本 4 使用 32 位 IP 地址,通常写为 0-255 范围内的四个十进制数字,例如 172.16.8.93。 ISP 正在迁移到 IP 版本 6,因为 40 亿个可能的 IPv4 地址即将分配； IPv6 使用 128 位地址。大约 10-15% 的流量现在是 IPv6;在许多国家/地区,新的宽带订阅将为您提供一个适用于所有普通消费者用途的 IPv6 地址。

本地网络主要使用以太网,其中设备具有唯一的以太网地址（也称为 MAC 地址）,这些地址使用地址解析协议 (ARP) 映射到 IPv4 地址。动态主机配置协议 (DHCP) 用于根据需要为机器分配 IP 地址,并确保每个 IP 地址都是唯一的。网络地址转换 (NAT) 还使网络上的多个设备能够使用相同的面向 Internet 的 IP 地址,通常具有不同的端口号;大多数移动网络运营商和许多 ISP 都使用它。因此,如果您想追踪一台做了坏事的机器,您通常需要获取将设备的 MAC 地址映射到 IP 地址的日志。可能有不止一个日志,而且很多地方都可能出错 例如错误的时间戳,以及无法理解时区。

最基本的问题之一是预防和缓解拒绝服务 (DoS) 攻击。这些有很多口味。对手可能会尝试窃取您的部分 IP 地址空间或您的一个或多个域,以发送垃圾邮件;即使您取回它,您也可能会发现它已被广泛列入黑名单。对手可以从许多受感染机器的僵尸网络中向您发送大量流量;分布式拒绝服务 (DDoS) 攻击。

他们可以滥用 DNS 等各种在线服务向您发送大量数据包流量。让我们依次解决这些问题。

21.2.1 BGP 安全

互联网是一个互连的网络网络:它的组成部分是自治系统 (AS),例如 ISP、电信公司和大型组织,每个系统都控制着一系列 IP 地址。将它们结合在一起的粘合剂,即 Internet 的核心路由协议,是边界网关协议 (BGP)。

路由器 在网络上交换数据包的专用计算机 使用 BGP 来交换有关哪些路由可用于到达特定 IP 地址块的信息,并维护路由表以便它们可以选择要使用的有效路由。 AS 可以通过从大型传输提供商那里购买服务来将 trac 路由到其他 AS,但通常会通过在本地互联网交换 (IX) 上相互对等来降低成本,其中大多数国家至少有一个,而大国家可能有几个。

互联网互连是一个复杂的生态系统,具有许多相互依赖的层次。其开放和去中心化的组织对于互联网的成功和弹性至关重要,这意味着卡特里娜飓风等自然灾害和 9/11 等恐怖袭击的影响已得到缓解

时间和空间有限,还有各种技术故障。然而,由于一级供应商的整合,互联网正慢慢变得更加集中,并且容易受到共模故障（如断电)和破坏性攻击的影响。

我们可以合理预见的最严重的攻击将涉及攻击者在数以千计的路由器上植入恶意软件,以便它们通告大量虚假路由,阻塞路由表并破坏路由结构。已经以事件和事故的形式出现了几起警告。 2008 年,在巴基斯坦政府试图通过宣布虚假路线在当地对其进行审查后,YouTube 在几个小时内无法访问； 2010年中国电信发布无效路由10万余条,劫持15%的互联网地址18分钟。一些人将其归因于意外,而另一些人则认为中国一直在测试“网络核武器”,其中一些放射性尘埃逃逸了。大多数路由器现在只接受来自每个对等体的有限数量的路由,可能是几十条,也可能是几百条;如此大规模的破坏将需要数以千计的破坏路由器。中国和（最近)俄罗斯一直在努力使他们国家的互联网可分离,这样理论上可以发起重大的破坏性攻击,而不会对当地服务和设施造成不可接受的附带损害。

有报道称 BGP 劫持被中国用于情报收集;例如,从 2016 年 2 月开始,从加拿大到韩国政府网站的流量通过中国路由了六个月 [533]。还存在犯罪滥用,从垃圾邮件发送者劫持 IP 地址空间,到 2018 年 8 位数的广告欺诈,其犯罪者隐藏在从美国空军窃取的地址空间中 [791]。最后,2019-20 年关于是否应允许华为在与美国结盟的国家大规模（或完全)销售路由器的政治斗争愈演愈烈。

退一步说,互联网的弹性很难定义和衡量;它与效率之间存在紧张关系,并且随着少数非常大的网络开始占据主导地位,它可能会减少。这些范围从占主导地位的传输提供商 Level 3 到由 Google、Akamai、Cloudflare 和其他公司运营的内容交付网络 (CDN)。弹性与效率、可达性和拥塞、流量优先级与商业敏感性、复杂性和规模之间存在许多复杂的相互作用。没有机制来检查通过 BGP 分发的路由信息的有效性。 ISP 和政府之间普遍存在的不信任使得监管变得困难。缺乏关于该系统如何运作的良好信息也使得理性讨论变得困难。

迄今为止,韧性一直取决于产能过剩和快速增长,但这不可能永远持续下去。 2011 年,我和同事为欧洲网络和信息安全局撰写了一份重要报告,详细探讨了这些问题 [1906]。

目前主要的技术 BGP 安全机制是资源公钥基础设施（RPKI),它使注册机构能够证明“自治系统 X 公布 IP 地址范围 Y”。这不会阻止有能力的攻击者,因为恶意路由公告只会在中间攻击者的路由末尾拥有正确的 AS;但它会检测到导致大部分中断的胖指错误。它是否会使已经脆弱的 BGP 系统更加健壮,以重新获得大量证书

可见的电源;当 RIPE 的证书于 2020 年 2 月到期时,出现了短暂的中断,直到它被修复。对于未来,人们正在研究 Peerlock,通过这种方式,立交桥上的主要 AS 可以共享有关他们将和不会宣布哪些路线的信息;这有可能为交换成员带来足够的本地利益,使其能够实际部署。

21.2.2 DNS 安全

域名系统 (DNS) 允许助记名称,例如 ross-anderson。 com 映射到任何一种 IP 地址;有一个层次结构的 DNS 服务器可以执行此操作,从数百个顶级服务器到 ISP 和本地网络上的机器,这些服务器缓存 DNS 记录以提高性能和可靠性。它确实偶尔会受到攻击:2016 年 10 月,Mirai 僵尸网络攻击了 DynDNS,在美国东海岸摧毁了 Twitter 五个小时。但是 DNS 已经成为一个大规模的分布式系统,许多非常快的机器连接到非常高容量的网络,因此对它的服务拒绝攻击很少见。

劫持确实时有发生,而且发生在不同层面。一些州拦截和重定向 DNS 查询作为审查手段;一些 ISP 已经这样做了,作为一种用他们从中获得收益的广告替换网页中的广告的方法; ISP 的 DNS 服务器可能会被黑客攻击,将客户带到恶意网站。这被称为域欺骗,在一种称为路过式域欺骗的变体中,骗子将您引诱到一个包含 javascript 的网页,该网页将您的家庭路由器的 DNS 服务器从您的 ISP 处的服务器更改为他们控制的服务器 [1816]。下次您尝试访问 www.citibank.com 时,您可能会被引导至模拟它的网络钓鱼站点。这就是更改家庭路由器默认密码的原因之一 即使它只能从您的网络内部访问。

为了防止 DNS 劫持,DNSSEC 在 DNS 名称记录中添加了数字签名。通过验证这样的签名,您可以检查记录是否来自权威服务器并且在途中没有被更改。接受度参差不齐：.gov 中的所有美国政府域都应该签名,而瑞典的大多数域都已签名,因为注册商使签名域更便宜。

然而,出于对密码学使系统更加脆弱的担忧,一些像谷歌这样的大公司不会签署他们的 DNS 记录;如果出了什么问题,你就可以消失。其他公司避免使用 DNSSEC,因为他们不希望竞争对手“走动”并枚举他们所有的子域; NSEC3 扩展使公司能够使用哈希来避免这种情况,但许多公司（或其服务提供商)尚未构建基础设施。

DNSSEC 的另一个问题是它在拒绝服务攻击中被滥用。一种常见的技术是,爱丽丝通过向查理发送一条消息来攻击鲍勃,“嘿,你能告诉我这个小问题的非常大的答案吗?你的,鲍勃!”由于签名的 DNS 记录要大得多,租用 DDoS 服务可以使用 DNSSEC 作为放大器,Alice 可以将声称来自 Bob 的 IP 地址的数据包发送到许多 DNS 服务器,然后这些服务器用回复轰炸目标。 （厚颜无耻的罪犯将 FBI 用作查理,因为 fbi.gov 有两把漂亮的大钥匙。）

2020 年有争议的问题是 DNS-over-https (DoH)。主要的浏览器维护者 Chrome 和 Mozilla 建议与其以明文形式发送 DNS trac,不如通过 https 将其加密到 DoH 解析器。据称这对保护隐私有好处,因为您的 ISP 将获得较少的有关您浏览的信息（但除非您使用 Tor,否则它仍然会有很多）。缺点是许多企业安全产品会监控 DNS 以检测滥用情况。如果恶意软件危害了您车队中的一台机器,您可能会在它试图联系命令和控制服务器时发现它,因此企业购买威胁情报源并监控列入黑名单的域名（和 IP 地址）。系统管理员还喜欢监控 DNS 劫持,并阻止某些不适合工作的域。 DoH 将使这一切变得更加困难,并且是有问题的架构,因为在应用程序上运行核心网络服务意味着它“不再是互联网”[428]。在商业方面,DoH 可能会巩固谷歌对广告市场的控制,同时在路由、负载平衡等方面给 Akamai 和 Cloudflare 等内容交付网络带来问题。它还将停止 ISP 为移动用户转码视频以节省带宽。专家们更愿意通过 TLS 运行 DNS。

21.2.3 UDP、TCP、SYN泛洪和SYN反射

在广域网上,大多数数据在使用无连接的用户数据报协议 (UDP) 或在端点之间建立持久连接的传输控制协议 (TCP) 的机器之间移动。让我们从 Alice 用于启动与 Bob 的 TCP 连接并为后续数据包跟踪设置序列号的 3 次握手开始。

一个！ B:同步;我的号码是XB!答:确
认;现在 X+1 SYN;我的号码是 YA!背
部;现在Y+1（开始说话）

图 21.1 – TCP/IP 握手

该协议已被多种方式利用。经典的拒绝服务攻击是 SYN 泛洪。 Alice 只是简单地发送了很多 SYN 数据包并且从不确认任何回复。 Bob 积累的 SYN 数据包记录超过了他的软件可以处理的数量。 1996 年,第一批分布式拒绝服务攻击之一使用了这种方法,导致纽约 ISP Panix 瘫痪数日。

技术修复是“SYNcookie”:B 不保留传入 SYN 数据包的副本,而是简单地将 X 的加密版本作为 Y 发送出去。这样,Bob 就不必保留很多关于半开的状态会议。尽管如此,SYN 泛滥仍然持续了很多年,尽管速度有所下降。一般原则是,当您设计一个任何人都可以调用的协议时,不要让恶意用户强迫诚实的用户工作。

现在比较常见的攻击是SYN反射。爱丽丝给鲍勃一个数据包

据称来自查理。 Bob 回复 Charlie,在实践中,系统最多发送五个 ACK 以响应每个 SYN 作为稳健性度量,因此仍然存在有用的放大效果 。

21.2.4 其他放大器

除了 DNS 和 TCP [1503],许多其他协议已被用于服务拒绝攻击。早期的最爱是玩蓝精灵;这利用了 Internet 控制消息协议 (ICMP),该协议使用户能够向远程主机发送回显数据包以检查它是否处于活动状态。如果 Alice 向广播地址发送一个声称来自 Bob 的 ICMP 数据包,则子网上的所有机器都会向他发送响应。协议已更改,因此广播地址不会回复。坏人改用 NTP 和 DNS 等协议,仍然可以找到放大器。

随后将对基于数据包放大的攻击进行更彻底的修复。
大多数可用的放大器使用 UDP 数据包,包括 ICMP 和 NNTP 但不包括 SYN 反射;所以从 2000 年代中期开始,宽带 ISP 开始过滤掉带有伪造源地址的 UDP 数据包。微软还改变了他们的网络堆栈,使受感染的机器更难发送带有欺骗性 IP 地址的数据包;您现在需要破解操作系统,而不仅仅是任何旧应用程序。因此,必须从托管中心的服务器运行利用 UDP 数据包放大器的攻击。在 2010 年代后期,此类攻击越来越多地成为 DDoS 雇佣运营商的专利,对付他们最有效的对策是突袭并逮捕他们。

21.2.5 其他拒绝服务攻击

随着创建拒绝服务攻击的巧妙方法被一个接一个地关闭,坏人越来越多地转向蛮力,通过从受感染的机器发送大量数据包。第一次分布式拒绝服务 (DDoS) 攻击可能是 80 年代的 Morris 蠕虫,而 1990 年代第一次蓄意攻击是在 Panix 上提到的攻击。如今,僵尸网络利用各种漏洞进行组装,地下市场让一些人专门从事黑客机器并将其出售给以各种方式获取价值的其他人。自 2016 年以来,最常用于 DDoS 攻击的机器是闭路电视摄像机等物联网设备,这些设备现在大量连接到具有合理带宽的家庭 WiFi 网络,但它们往往具有已知的默认密码 而且通常无法修补。 Mirai 僵尸网络于 2016 年 10 月出现以利用此机会,此后已经出现了 1000 多个变体（其源代码已发布到 Hackforums）。

拒绝服务攻击的动机多种多样。大多数是由学生发起的 通常是想要摧毁对方团队的团队对话服务器的玩家。多年来,DDoS 黑市一直存在 供租用,美国和其他地方的当局一直试图关闭它。已经发生了一些勒索事件（例如在线博彩公司）,并且越来越多地使用这种技术来压制政治对手 - 开始

也许是对吉尔吉斯斯坦反对党服务器的攻击,即使这些服务器已迁移到北美 [1613]。我们在第 2 章中讨论了国家在冲突中的使用。

也就是说,我们不能忘记在线行动主义。如果十万人向白宫发送电子邮件抗议某项政策或其他政策,这是 DDoS 攻击吗?抗议者不应被视为重罪犯;但抗议很容易变成滥用职权,而在立法上做出区分可能很困难。

21.2.6 电子邮件 从间谍到垃圾邮件发送者

电子邮件的 SMTP 标准在防止批量拦截和防止大量不需要的邮件方面存在特殊问题。

默认情况下,电子邮件既不加密也不经过身份验证,几十年来任何可以监控网络或访问邮件服务器的人都可以使用。
可以使用 PGP/GPG 等程序来加密邮件,但这从未在小型社区之外流行起来。首先,这样的程序使用起来会很痛苦,其次,它会产生强大的网络效应 :如果您的朋友都不使用,那么使用电子邮件加密就毫无意义。更重要的是,如果只有一小部分人使用加密,这可能只会引起当局的注意;正如我们在第 20.4 节中讨论的那样,颠覆团体、间谍等确实需要匿名而不仅仅是保密。因此,PGP/GPG 倾向于由专家使用,例如系统管理员和反病毒研究人员。

批量拦截有两种主要的对策。首先,大多数邮件服务器在交换邮件时使用 starttls 与其他邮件服务器建立加密通信,尤其是自斯诺登泄密以来。加密交换可能会被中间人攻击所阻止,一些不那么民主的国家已经报道了这些情况。目前针对此类攻击的对策 MTA 严格传输安全 (MTA-STS) 得到了 Microsoft、Google 和 Yahoo [1220] 的支持:它允许邮件服务提供商指定邮件只能通过经过认证的 TLS 会话传递给他们您从他们的网站下载的适当证书。这可以防止对进出大公司的电子邮件进行降级或拦截攻击,还允许对其他服务器进行机会主义的、首次使用时信任的加密。 MTA-STS 通常取代了早期的标准,即基于 DNS 的命名实体身份验证 (DANE),后者将 starttls 的 TLS 证书放入邮件服务器的 DNS 记录1。

第二个对策是现在大约 95% 的个人电子邮件帐户都在五大网络邮件提供商处,许多公司也在使用它们。在这种情况下,电子邮件的机密性由 TLS 确保,并通过我们稍后讨论的证书固定和证书透明度得到加强。但是,虽然批量访问可能会被阻止,但网络邮件会受到授权访问,就像企业外包的其他服务一样。

大量不需要的邮件或垃圾邮件有两个组成部分。第一种是完全合法但不受欢迎的营销传播。由于营销人员可能会厌倦

1DANE 在德国仍然被广泛使用,但谷歌拒绝使用它,因为它依赖于谷歌认为不够可靠的 DNSSEC。

选择退出,用户会发现一旦某个报价或供应商不再感兴趣,按下“报告垃圾邮件”按钮会更方便。

第二种是由僵尸网络发出的大量通常不需要的 trac,通常带有明显的犯罪意图。这在某些方面类似于 DDoS 攻击:正如 DDoS 机器人可能会伪造 IP 地址一样,垃圾邮件机器人可能会伪造发件人的电子邮件地址。这是由具有四个主要机制的大型供应商进行的。

1. 域密钥识别邮件 (DKIM) 通过使用签名密钥将电子邮件与发送域联系起来,签名密钥的公共验证密钥保存在发送域的 DNS 记录中。尽管在传输过程中添加了标头,但仍选择已签名的材料来明确识别消息,但要阻止坏人添加额外的“From: PayPal”标头。没有太多改动的邮件可以转发。垃圾邮件发送者通过 Gmail 发送他的垃圾邮件,Gmail 对其进行签名,然后再转发,这是一种重放攻击;所以邮件服务器缓存 DKIM 签名并丢弃带有已经出现过几次的签名的邮件。

2. 发件人策略框架 (SPF) 类似,但将邮件绑定到源 IP 地址。同样,这可以根据域 DNS 记录中的密钥进行验证。
   SPF 不允许邮件转发;邮件列表服务器应该使用一个名为 Authenticated Received Chain (ARC) 的相关协议来重新签署他们转发的邮件。

3. 域的 DNS 还可以包含基于域的消息身份验证、报告和一致性 (DMARC) 记录,这使它的所有者可以建议收件人应该如何处理看似来自所有者域但使用 DKIM 进行身份验证失败的电子邮件和防晒系数。

4. 机器学习系统用于根据身份验证结果和其他标准过滤邮件,并根据用户是否将邮件报告为垃圾邮件来获取大部分基本事实。用户对营销材料的偏好会随着时间的推移而变化,从而使这变得更加复杂。

垃圾邮件的非法部分现在是一个高度专业化的行业,由几个大团伙经营。自 2000 年代中期以来,其统计数据一直“不稳定”,而且这种情况越来越明显。截至 2020 年,这些团伙通常使用恶意 BGP 路由公告窃取 IP 地址空间,注册数千个域,并在机器学习过滤器启动并阻止它们之前从每个域发送数百个垃圾邮件。

21.3 恶意软件动物园 特洛伊木马、蠕虫和 RAT

恶意代码的第一个例子是特洛伊木马 以希腊人留给特洛伊木马的马命名,据说是作为礼物,但其中包含

向希腊军队打开特洛伊城门的士兵 [1129]。多年来一直存在关于命名法的宗教战争,这就是为什么许多人更喜欢只使用恶意软件一词。我的用法是,特洛伊木马是一种在不知情的用户运行时会执行恶意操作(例如捕获密码)的程序。蠕虫是一种在其他系统上自我复制的恶意程序,而通过将自身挂接到其他程序的代码中来进行复制的则是病毒。远程访问木马 (RAT) 是一种软件,可以以 root 用户身份运行,也可以不以 root 用户身份运行,但它可以让远程方访问运行它的设备,而 rootkit 是一种以 root 用户身份安装在设备上的软件,它可以让第三方秘密地访问控制它。可能不需要的软件 (PUS) 可能已被公开或通过欺骗安装,但会执行用户不想要的操作(如果他们完全理解)。

这些类别不是相互排斥的,边界可以是上下文相关的。例如,跟踪软件 使一个人能够跟踪另一个人的手机位置和使用情况的软件 分为不同的类别,具体取决于它是秘密安装的,还是由一个控制他的伙伴的人安装的,或者是由法院命令它作为保释条件。即使是隐蔽的恶意软件也不总是非法的,因为它可以被执法机构用来将嫌疑人的手机和笔记本电脑变成窃听设备,也可以被欺诈者用来远程控制银行账户2。

恶意软件通常使用隐蔽技术来隐藏,但最终它被识别出来并编写了删除它的工具。围绕恶意软件有一个完整的生态系统:恶意软件编写者、受感染机器的僵尸网络,以及一系列提供从威胁情报到防病毒软件的一切服务的安全公司。

(甚至有公司出售恶意软件 尤其是向政府机构。)
除了正规经济之外,还有一个由网络骗子组成的地下经济,他们出售从银行木马到 DDoS 出租服务等各种东西。

21.3.1 恶意软件的早期历史

在 20 世纪 60 年代初期,机器速度很慢,而且它们的 CPU 周期是配给的 学生经常排在队列的尾部。学生们发明了一些技巧,例如编写带有特洛伊木马程序的电脑游戏,以检查程序是否以 root 用户身份运行,如果是,则创建一个具有已知密码的特权帐户。到 20 世纪 70 年代,大学的分时系统成为越来越多涉及木马的恶作剧的目标。开发了各种技巧。 1978 年,Xerox PARC 的 John Shoch 和 Jon Hupp 编写了一个他们称为蠕虫的程序,该程序通过网络自我复制以寻找空闲处理器,以便为它们分配任务 [1724]。

1984 年,肯·汤普森 (Ken Thompson) 在接受计算机科学最高奖项图灵奖时,发表了一篇经典论文《Reflections On Trusting Trust》。他表明,即使系统的源代码经过仔细检查并且已知没有漏洞,仍然可以插入活板门 [1883]。他的技巧是在编译器中构建陷门。如果这认识到它是

2另一方面,某些防病毒产品在各种方面表现得像恶意软件,包括在“免费试用”后很难删除,或引入不安全因素。2019 年 12 月,一款品牌的 AV 软件因泄露过多个人信息而被 Chrome、Firefox 和 Opera 下架[358]。

编译登录程序时,它会插入一个适用于任何帐户的主密码3。当然,有人可能会检查编译器的源代码,然后从头开始重新编译。因此,如果编译器识别出它正在编译自己,它就会插入漏洞,即使它不存在于源代码中。因此,即使您可以购买具有可验证的安全硬件、操作系统和应用程序的系统,编译器二进制文件仍然可能包含木马。其寓意是,为了完全信任一个系统,仅构建所有系统是不够的,在软件工程师使用“构建”一词的意义上,即从源代码编译它。您必须创建所有这些,包括工具链和硬件。

恶意软件接下来变成了移动设备。 1981 年,一名九年级学生为 Apple II 编写了有史以来第一个计算机病毒 [1216]。 1984 年,弗雷德·科恩 (Fred Cohen) 获得了该主题的博士学位;他对不同操作系统的实验展示了代码如何将自身从一台机器传播到另一台机器,正如我在第 9.6.4 节中提到的,从多级系统的一个部分传播到另一个部分。在大约三年内,我们开始在野外看到第一个真正的活病毒:当用户在软盘上或通过公告板共享程序时传播的 PC 病毒4。

一个早期的创新是“Christma”病毒,它于 1987 年 12 月在 IBM 大型机周围传播。它是一个用大型机命令语言 REXX 编写的程序,它的标题写着“不要读我,执行我”和代码,如果执行后,在屏幕上画了一棵圣诞树然后将自己发送给用户联系人文件中的每个人。这是一个恶作剧,而不是出于恶意;并通过使用网络(IBM 的 BITNET)进行传播,并邀请用户运行它,它领先于时代。

21.3.2 网络蠕虫

1988 年 11 月,媒体和公众开始意识到互联网蠕虫病毒的恶意软件。这是 1988 年 11 月由 Robert Morris Jr 编写的一个程序,该程序利用多个漏洞从一台机器传播到另一台机器 [617]。它在猜测攻击中尝试了 432 个常用密码,寻找被它感染的机器信任的任何机器,并且还尝试利用 Unix 中的漏洞(包括 6.4.1 节中提到的 fingerd 错误)。它还采取措施伪装自己:它被称为 sh 并加密了它的数据字符串(尽管使用凯撒密码)。

它的作者声称他的代码不是对互联网的蓄意攻击 只是一个实验,看看代码是否可以从一台机器复制到另一台机器。但它有一个错误。它应该识别出已经被感染的机器,而不是再次感染它们,但这个功能没有用。结果是大量的 trac 完全阻塞了 Internet(或者更准确地说,它的前身 Arpanet),尽管事实上它当时只影响了 Arpanet 上 60,000 台机器中的大约 10%。一节课

3 这发展了 Paul Karger 和 Robert Schell 在 1974 年 [1019] 的 Multics 评估中首先提出的想法。

4在互联网向公众开放之前,在线服务大多是独立的;公告板通常由爱好者操作,并允许订阅者甚至匿名用户拨入以共享信息和文件。

是那些保持紧张并且没有断开网络连接的站点可以更快地恢复,因为他们可以找出正在发生的事情并获得修复。

21.3.3 进一步的恶意软件演变

到 20 世纪 90 年代初,PC 病毒已经成为一个问题,它们催生了整个反病毒软件行业。整个 1990 年代,操作系统获得了更好的访问控制,使恶意软件编写者的工作变得更加困难,但解释语言的传播提供了大量新机会。

到 21 世纪初,主要载体是 Word 等产品中的宏语言,主要传输机制已成为互联网 [298]。

恶意软件进化的下一阶段是让用户成为传播机制。 2000 年的“Love Bug”是一种蠕虫病毒,它会将自己发送给受害者通讯录中的每个人,主题行“我爱你”旨在让人们打开它5。这一事件告诉我们通过过滤来阻止此类事情的困难;一家拥有 85,000 名员工 的加拿大公司在防火墙处删除了所有 Windows 可执行文件,但他们的许多员工 都有个人网络邮件帐户,所以 Love Bug 还是进来了。该公司在他们的地址簿中为每位员工提供了公司目录的副本,结果崩溃了,因为 85,000 个邮件客户端每个都试图对 85,000 个地址中的每一个说“我爱你”。 Love Bug 之后出现了类似的蠕虫病毒,这些蠕虫病毒通过提供布兰妮·斯皮尔斯和帕丽斯·希尔顿等名人的照片说服人们点击它们。

下一个发展是 flash 蠕虫,它通过扫描整个 Internet 来寻找容易受到某种攻击或其他攻击的机器并接管它们来传播; Code Red 和 Slammer 等示例在几小时甚至几分钟内感染了所有易受攻击的机器,并推动了对哪种自动防御可能会及时做出反应的研究 [1821]。

2000 年代初期还见证了间谍软件和广告软件的兴起。间谍软件在未经所有者授权的情况下从您的计算机(现在是您的手机)收集和转发信息,或者充其量只是一个模糊的弹出窗口,它并没有真正告诉您您同意什么。它也可能由其他人安装,例如父母或伴侣;间谍软件越来越多地涉及亲密伴侣虐待。广告软件可能会用广告弹出窗口轰炸用户,并可能与间谍软件捆绑在一起。此类产品的供应商甚至起诉了将其产品列入黑名单的防病毒公司。有些间谍软件是故意安装的,无论是公司想要监视员工,父母想要查看孩子在做什么,还是施虐者想要监视和控制他们的伴侣。界限是模糊的,不同的人可能有不同的观点。

2004-6 年发生了翻天覆地的变化。在那之前,大多数恶意软件编写者这样做是为了好玩或给他们的朋友留下好印象 基本上,他们都是业余爱好者。从那以后,地下市场和犯罪论坛的出现使得

5 它可以被视为 1987 年“圣诞节”蠕虫病毒的一种更致命的变种,但 Love Bug 的作者是马尼拉的一名小学生,他可能从未听说过那个。

整个业务更加专业。恶意软件编写者现在可以通过软件获得报酬来招募机器,这些机器可以出售给僵尸网络牧民以换取现金并用于其他攻击。

在业余时代,大多数病毒都是片状的;实际上很少在野外传播。如果代码没有足够的传染性,它就不会传播,但如果你让它的传染性太强,那么在几个小时内,世界上的反病毒供应商就会升级他们的产品来检测和删除它。既然恶意软件编写者关注的是金钱而不是吹牛的权利,他们往往会避免自我复制的蠕虫病毒,转而支持更可控的漏洞利用活动。 （主要的例外是利用无法修补的物联网设备。）

到 2000 年代后期,最大的僵尸网络使用专业的在线营销技术来发展他们的网络。各种故事被用来诱使人们点击一个链接并运行一个木马程序,该木马程序会将 rootkit 放到他们的机器上。

受害者必须点击几个警告才能安装软件;但是 Windows 会弹出许多烦人的对话框,大多数人只需单击它们即可。
Storm 是最早的大型公司之一,靠拉高出货的经营者和药房骗子谋生 [1090]。安全研究人员试图通过找到并关闭他们的命令和控制服务器来禁用大型僵尸网络； Storm 使用点对点架构消除了这种单点故障 [1835]。最终被微软列为下架目标。同样的游戏还在玩； 2020 年 3 月,微软关闭了 Necurs,这是一个拥有 900 万台机器的僵尸网络,它已经增长了八年,分发银行木马以及勒索软件和垃圾邮件 [349]。

自 2016 年 10 月以来,Flash 蠕虫以 Mirai 蠕虫及其变体卷土重来。 Mirai 最初接管了带有已知 root 密码和无法升级软件的 wifi 连接闭路电视摄像机;可以在一个小时左右的时间内找到并招募 IPv4 地址空间中的所有此类设备。

从那时起,已经有超过一千个 Mirai 变种攻击各种物联网设备。

21.3.4 恶意软件如何工作

恶意软件通常有两个组件 一个复制机制或投放器,以及一个有效负载。蠕虫在运行时只是简单地在其他地方制作自己的副本,可能是通过密码猜测或使用远程代码执行漏洞（两者都被 Internet 蠕虫使用）侵入另一个系统。病毒在其他软件中传播,可能作为文档中的宏,而特洛伊木马通常由受害者执行。

病毒的第二个组成部分是有效负载。激活后,这可能会做一件或多件坏事：

- 泄露您的机密数据；
- 使用银行恶意软件或间谍软件直接攻击您；
- 加密您的数据并要求赎金；
- 攻击他人,例如当 GCHQ 的 Operation Socialist 在 sec 中描述时

2.2.1.9 破坏 Belgacom 并在其中安装软件,以监控通过比利时到其他国家的手机流量;

- 执行一些其他恶意任务,例如使用 CPU 来挖掘 cryp
  货币;
- 安装rootkit 或远程访问特洛伊木马,使其控制器能够执行上述任何操作,协调对其他机器的恶意软件攻击,并更新自身以响应任何反制措施。

如果目标不是个人而是公司（如 Belgacom 案例）,则攻击可能需要数周至数月的工作。一旦攻击者控制了目标网络上的设备,他们就会想横向移动以映射网络并找到身份验证服务器和邮件服务器等关键资产,从而扩大危害范围并安装远程访问木马以获得永久存在。有很多可能性。

1. 在过去,攻击者会安装 packet snier 软件来获取密码并破坏其他帐户,最终包括 sysad min 的帐户。现在的良好做法是使用双因素身份验证或使用 Kerberos 或 SSH 等协议来阻止此类攻击,以确保明文密码不会通过 LAN。

2. 其他技术以文件服务器等共享资源为目标。例如,Linux 服务器可能使用网络文件系统 (NFS) 协议;当一个卷第一次被挂载时,客户端从服务器获得一个根文件句柄 一个不依赖于时间并且不能被撤销的访问权证。

   我们在自己的实验室使用 Kerberos 对客户端和服务器进行身份验证来阻止这种情况。Windows 文件共享也有类似的问题,尽管细节有所不同； WannaCry 和 NotPetya 蠕虫使用的 EternalBlue 漏洞利用了此类文件共享。

3. SSH 等安全机制带来了更多漏洞,大型组织中的机器可能有成千上万个 SSH 密钥相互通信,入侵者可以利用它们和它们创建的信任结构四处移动。

要了解当今有能力的攻击者可用的工具范围,我建议您浏览埃德·斯诺登发布的 NSA 文件和在 Vault 7 披露中泄露的 CIA 工具包。网络战士拥有一系列漏洞利用工具包、投放器、RAT 和用于秘密渗漏情报产品的软件。

要点是,您网络上的入侵者接管其他机器的难易程度取决于您将网络锁定的严密程度,而任何破坏后可能造成的损害将取决于您网络中其他机器的信任程度,或容易受到受损机器的攻击。这是不信任本地网络,而是始终坚持客户端和服务器之间强身份验证的论点之一。

21.3.5 对策

在 1987 年第一个 PC 病毒出现后的几个月内,就出现了销售防病毒软件的初创公司。这导致了一场军备竞赛,病毒和反病毒开发人员试图以智取胜。

早期的防病毒软件基本上有两种类型 扫描程序和检查程序。扫描程序在可执行文件中搜索妥协指标 (IoC),通常是来自特定病毒的字节串。恶意软件开发人员以各种方式做出回应,而主导技术变成了多态性。这个想法是在每次恶意软件复制时更改代码,以使其更难找到稳定的 IoC。通常的技术是加密代码,并有一个包含解密代码的小头。每次复制时,恶意软件都会使用不同的密钥重新加密自身,并通过替换等效的指令序列来调整解密代码。现代恶意软件可能会依次运行六个这样的加壳程序,并在运行时递归地自行解压。 AV 公司通过在虚拟机中运行代码进行反击,因此恶意软件开发人员包括 VM 检测代码。 AV 公司至少可以将解压后的代码用作 IoC,只要他们能够破解到最后的解压操作即可。

Checksummers 保留系统上所有授权可执行文件的白名单列表,以及原始版本的校验和,通常使用哈希函数计算。恶意软件开发人员的主要对策是隐身,在这种情况下,这意味着恶意软件会监视校验和所使用的那种操作系统调用,并在进行检查时隐藏自己。

要提供针对恶意软件的强大防御,您必须将工具、激励措施和管理结合起来。我们在过去了解到基于 DOS 的文件病毒可以为所有事件提供中央报告点,并控制组织机器上加载的所有软件。主要风险是在家中用于工作和其他用途(例如孩子玩游戏)的机器,以及来自其他组织的文件。同样的原则仍然适用。

然而,企业现在需要比以前更加协调的响应。原因之一是防病毒软件的效果越来越差。

僵尸网络和机器利用的商业化意味着恶意软件编写者像公司一样运作,设有研究和测试部门。

当前的防病毒产品在首次推出时几乎无法检测到所有漏洞利用(如果其编写者对它们进行了适当的测试),并且其中许多漏洞都没有引起防病毒行业的注意就招募了目标数量的机器。最终效果是,虽然防病毒软件可能在 2000 年代初期检测到几乎所有流通的漏洞利用程序,但到 2010 年,典型产品可能只检测到其中的三分之一,而到 2020 年,您预计会在事后检测到感染并必须清理。这意味着拥有良好的工具支持、记录网络流量并根据最新的威胁情报对其进行分析。更重要的是,rootkit 供应商提供售后服务;如果运送了移除工具包,rootkit 供应商将迅速运送对策。

如今,许多攻击者 尤其是有能力的攻击者 不会将恶意软件文件留在身边,而是“生活在这片土地上”;他们可能只是将他们的 ssh 密钥添加到您的其中一台服务器上的授权密钥列表中,这样他们就可以在需要时弹出,而不会留下任何遗留 AV 可以找到的东西。

21.4 防御网络攻击

在防御恶意软件和网络攻击方面,本书 2008 年第二版的观点是您需要三样东西:足够好的管理以保持您的系统打上最新补丁并正确配置;阻止已知特洛伊木马和网络攻击的防火墙;和入侵检测来监控您的网络和机器以寻找妥协指标,这样您就可以捕获通过的 stu 并在之后进行清理。

原则在 2020 年保持不变,但现在的现实要复杂得多,因为任务的规模和复杂性使自动化几乎变得必不可少。大型 Windows 商店可能有类似以下内容:

1. 在每个端点上运行的代理,向云服务报告,让您完全了解哪些软件在何处运行,并使您能够推送更新;

2. 持续探测网络已知漏洞的漏洞扫描器
   漏洞;

3. 各种边界控制设备,可能包括防火墙、过滤所有访问网站 URL 的代理服务器,以及关键应用程序的代理;

4. 供员工远程工作的 SSL 网关;

5. 自带设备 (BYOD) 经理,负责控制员工使用但公司不拥有的笔记本电脑、电话和其他设备;

6. 数据泄露防护 (DLP) 系统,用于识别试图泄露的人员
   删除公司文件或代码;

7. 一个威胁情报平台,整合了来自多个供应商的信息,提醒您各种妥协指标,包括错误的 DNS 名称和 IP 地址;

8. 一个日志分析工具,让您可以在出现问题时返回并进行计算
   妥协最先发生,它传播了多远;

9. 安全编排和响应 (SOAR) 系统,如果您注意到网络中的某些设备正在与错误地址通信,例如已知恶意软件的命令和控制服务器,它可以帮助您快速响应。

让所有这些一起工作需要系统集成,否则您的网络安全中心将有数十名员工,他们的工作是将坏域、坏 IP 地址和其他危害指标的列表从一种工具复制到另一种工具。

就是说,让我们沿着这个列表往下看。

认真对待 IT 安全的组织 因为它们是国家行为者(如大型服务公司)的目标,或者具有严格的合规性要求

（如银行），或有很多损失（如军队） 旨在从源头上阻止所有漏洞。这意味着让所有补丁都保持最新，这反过来又意味着自动补丁管理。但这样的策略比看起来更难。它带来了许多困难的子问题，例如维护网络上所有设备的准确清单。如果你对注册新设备施加严格的官僚主义，人们将不得不想办法绕过它来完成他们的工作。因此，您还需要扫描您的网络，看看那里有什么以及它是否容易受到攻击。即使是勤奋的组织也可能会发现一次修复所有安全漏洞的成本太高；补丁可能会破坏关键应用程序，而一个组织最关键的系统通常运行在最不安全的机器上，因为管理员不敢升级它们，因为担心失去服务。

这与操作安全相互作用。在第 2 章和第 8 章中，我们讨论了培训人员不通过愚蠢行为暴露系统的实践和局限性。到 2000 年代中期，主要的攻击媒介是鱼叉式网络钓鱼 诱使人们点击电子邮件中下载并安装 rootkit 的链接。我们从埃德·斯诺登那里了解到，这是美国国家安全局在 2013 年攻击一家公司的标准方式：他们将监控外部流量以识别系统管理员，进行一些背景研究以识别个人目标，并制作令人信服的网络钓鱼诱饵。或者，他们会将目标定向到他们可以欺骗的网站或他们可以发起中间人协议攻击的网站。

您可能会尝试教育您的员工 不要点击可疑邮件中的链接，但有能力的攻击者会创建看起来并不可疑的邮件。如此多的企业希望他们的客户和供应商点击链接，您的员工必须点击一些链接才能完成工作。我们在第 3 章和其他地方讨论过，指责受害者是不适应的；如果你的安全系统不可用，你必须修复它们而不是责怪可怜的用户。

许多公司通过在云服务而不是本地机器中打开所有邮件附件来降低风险，为员工提供 Chromebook、iPad 或 Mac 等非 Windows 机器，或者使用防火墙或邮件过滤器来去除可疑内容。

21.4.1 过滤：防火墙、审查软件和窃听

防火墙是位于专用网络和互联网之间的机器，可以过滤掉可能有害的流量。它以将汽车或轻型飞机的乘客舱与发动机舱隔开的金属舱壁命名，以保护乘员免受燃料火灾。防火墙在 20 世纪 90 年代中期出现时引起了争议。纯粹主义者说公司中的所有机器都应该受到保护，而防火墙倡导者则说这是不切实际的。从那以后，争论就来回摇摆。

防火墙只是检查数据包流并执行过滤或日志记录操作的系统的一个例子。损坏的数据包可能会被丢弃，或以使其无害的方式进行修改。它们也可以复制到日志或审计跟踪中。非常相似的系统也用于互联网审查和执法窃听；我将在本节中讨论的几乎所有内容也适用于这些应用程序。任何方面的发展

这些领域可能会影响其他领域;实际系统可能具有重叠的 ping 功能。例如,许多公司的防火墙或邮件过滤器会屏蔽色情内容,有些甚至会屏蔽脏话,而审查儿童色情内容或异议政治言论的 ISP 系统可能会自动向当局举报肇事者。许多过滤器还保留日志,以便事后调查攻击;在部分金融部门,所有员工通信都必须记录在案,以便监管机构可以调查任何对内幕交易或洗钱的怀疑。

过滤器基本上分为三种类型,具体取决于它们是否运行
在 IP 数据包级别、TCP 会话级别或应用程序级别。

21.4.1.1 包过滤

最简单的过滤器只检查数据包地址和端口号。
此功能在路由器、Linux 和 Windows 中作为标准提供。
您可以通过确保只有“本地”数据包离开网络并且只有“外部”数据包进入网络来阻止 IP 欺骗。也很容易阻止来自“已知不良”IP 地址的 trac。例如,IP 过滤是中国防火墙审查机制的主要组成部分;可以在路由器硬件中保存一个坏 IP 地址列表,这样可以快速完成数据包过滤。

基本数据包过滤通常用于阻止所有流量,除了到达特定端口号的流量。您可能最初允许电子邮件和 Web trac 等常见服务使用的端口,然后根据需要打开更多端口。随着我们转向软件定义网络 (SDN),用商品服务器上的软件控制的廉价交换机取代昂贵的路由器,数据包过滤规则仅成为 SDN 控制器中的访问控制规则。

然而,数据包过滤器可以被许多技巧击败。例如,数据包的分段方式可能是初始分段通过了防火墙的检查,但随后被后续分段覆盖,将源地址替换为违反安全策略的地址。另一个限制是维护黑名单很困难,尤其是当它不是您要专门阻止的 IP 地址,而是解析为 IP 地址的内容时,尤其是在瞬态基础上。例如,网络钓鱼者使用 fast-flux 之类的技巧,站点的 IP 地址每小时更改几次。

21.4.1.2 电路网关

下一步是电路网关,它重新组合并检查每个 TCP 会话中的所有数据包。这比简单的数据包过滤更昂贵,但也可以提供虚拟专用网络 (VPN) 的附加功能,从而使通过 Internet 的公司流量在防火墙之间进行加密。我将在本章的最后一节讨论用于此目的的 IPSEC 协议。

TCP 级别的过滤可以用来做更多的事情,例如 DNS 过滤。
但是,这样的过滤器无法在应用程序级别筛选出不良内容,从恶意代码到儿童性虐待材料。因此,它可以被编程为将某些类型的 trac 定向到应用程序过滤器。

21.4.1.3 应用代理

第三种防火墙是应用程序代理,它了解一种或多种服务。例如,尝试清除垃圾邮件的邮件过滤器,以及阻止或删除不良内容的 Web 代理。经典目标是剥离代码,无论是简单的可执行文件、网页中的活动内容,还是来自传入 Word 文档的宏。转向基于 Web 的邮件服务和 https 的采用大大减少了邮件过滤器要做的工作,并且随着服务公司采用证书透明度等技术措施来防止代理,过滤需要转移到端点。

应用程序代理也可能成为瓶颈。一个例子是中国的防火墙,它在 2000 年代一直试图阻止涉及被禁主题的邮件和网络内容 [448]。自从主要服务提供商采用 https,以及也可用于通信的 Google Docs 等服务的可用性,中国干脆阻止了大多数公民使用 Gmail 和 Facebook 等服务。

在谷歌推广的新兴 BeyondCorp 模型中,代理位于应用程序服务器本身的前面,因此不需要信任内部网络。

21.4.1.4 入口过滤与出口过滤

大多数防火墙向外看并试图将坏东西挡在外面,但有些防火墙向内看并试图阻止坏东西离开。先驱者是军事邮件系统,它监视传出的流量以确保没有任何机密信息以明文形式发送出去。 2005 年左右,一些 ISP 开始查看外发邮件跟踪以尝试检测垃圾邮件 [442];到目前为止,大多数消费者 ISP 都会阻止他们的客户发送带有欺骗性源地址的数据包。这种源地址验证意味着使用 UDP 反射攻击的 DDoS 运营商不能再使用僵尸网络,而需要租用数据中心的服务器。

2020 年出口过滤增长最快的用途是防止数据泄漏 (DLP)。 “打电话回家”的软件,无论是出于版权保护还是营销目的,都可能泄露高度敏感的材料,谨慎的组织越来越希望监视和控制这种行为。但是 https 的广泛使用意味着 DLP 系统通常需要在端点上安装软件,而不是使用中间件。

21.4.1.5 架构

多年来,许多公司都购买了防火墙来取悦他们的审计员。如果那是你的痛点,一个简单的过滤路由器不需要太多维护,也不会太碍事。在另一个极端,国防承包商的一个严格的防火墙系统可能包括一个将外部世界连接到一个屏蔽子网的数据包过滤器,也称为非军事区 (DMZ),它又包含许多应用程序服务器或代理以过滤邮件、网络和其他服务。您可能还希望找到数据二极管来分隔以不同许可级别运行的网络,以确保机密信息不会泄露

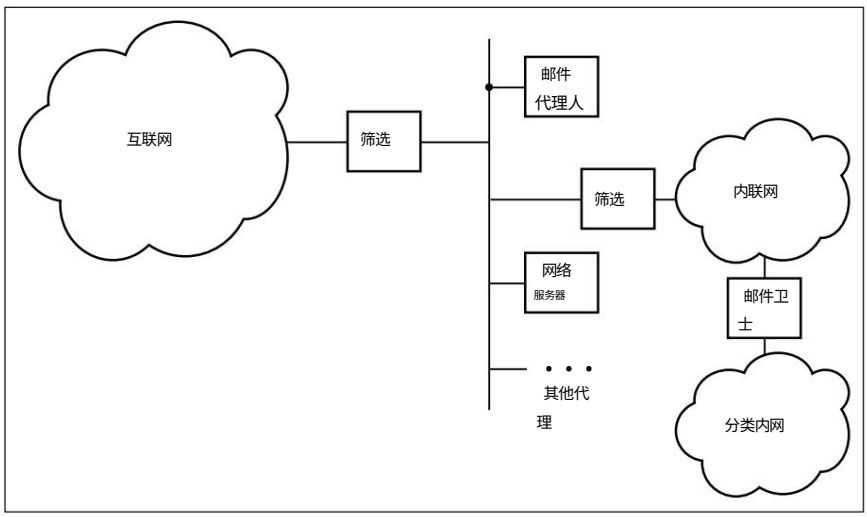

图 21.2:MLS 网络的复杂防火墙

向外或向下（图 21.2）。

另一种方法是拥有更多但更小的网络。在我们的大学，我们有防火墙来分隔部门，尽管我们有一个共享的网络骨干网和一些共享的中央服务，例如日志记录。

学生和财务系没有理由应该在同一个网络上，计算机科学系与神学系的要求截然不同。将每个网络保持在较小的范围内可以限制任何妥协的范围，并有助于激励系统管理员保护它。

网络安全架构设计中的考虑因素包括简单性、可用性、去边界化与重新边界化、欠阻塞与过度阻塞、可维护性和激励。

首先，由于防火墙只做少量的事情，所以可以使它们简单地消除漏洞和错误的来源。如果您的组织拥有不同种类的机器，那么将尽可能多的安全任务加载到少量简单的机器上是有意义的。另一方面，如果您运行的是呼叫中心之类的东西，拥有一千台配置相同的 PC，那么努力保持此配置紧凑是有意义的。这些大致是上面介绍中讨论的能源公用事业和谷歌模型。

其次，复杂的中央安装不仅会增加运营成本，而且会妨碍人们安装后门（例如绕过防火墙的电缆调制解调器）来完成工作。我将在 ?? 部分讨论当外交官的社交系统无法使用时，他们如何通过使用私人电子邮件摆脱困境。许多经营良好的公司都有开放的访客网络，我们部门也是如此；总会有一些有用的东西。谨慎的系统管理员会监控实际的网络配置，而不仅仅是依赖“策略”。

第三,防火墙只有在人们找到绕过它们的方法时才会起作用。早期的防火墙只允许邮件和网络通过;因此,从计算机游戏到匿名代理的应用程序的编写者重新设计了他们的协议,以使客户端-服务器 trac 看起来尽可能像普通的 web trac。然后一切都转移到 Web 2.0,这样的过滤器在很大程度上变得无效。

接下来是去边界化 正如谷歌的 BeyondCorp 指出的那样,由于电话和 PDA 的激增被用于以前在台式计算机上完成的功能,以及通过改变业务涉及更多功能外包的方法 无论是正式外包给分包商还是非正式外包给广告支持的网络应用程序。如果您组织的某些部分无法控制(例如销售团队和研发实验室)而其他部分必须控制(财务办公室),那么您可能需要单独的架构。 Web 应用程序的激增伴随着在外围做事的动力减弱,因为有用的事情变得更难做。代码和数据之间的差异被新的脚本语言逐渐削弱。许多公司在 2000 年代初期试图阻止 JavaScript,但被需要它的流行网站击败。如今,可能无法阻止您的员工连接大量根本无法保护的物联网设备 [1254]。

然后是我们的老朋友接受者操作特征或 ROC 曲线。没有一种过滤机制具有完全的精度,因此不可避免地需要在欠块和过度块之间进行权衡。如果你正在运行一个审查系统来阻止孩子们在公共图书馆访问色情内容,当一些图片通过时,你是否会阻止并惹恼父母和教会,或者你是否会阻止并因侵犯言论自由权而被起诉?更糟糕的是,用于过滤性、暴力和脏话 Web 内容的防火墙系统也往往会阻止言论自由网站(因为其中许多批评防火墙供应商 还有一些提供技术建议如何以规避阻塞。)

正如我们一再指出的那样,安全对激励的依赖至少与对技术的依赖一样多。一个管理由他们认识的一百个人使用的部门网络,并且必须亲自清理由入侵或配置错误造成的任何混乱的系统管理员,比那些只是大团队中的一个成员的人更有动力经过数千台机器。

21.4.2 入侵检测

攻击会发生,阻止某些攻击并检测其余攻击通常比试图阻止所有攻击的成本更低。用于检测不良事件发生的系统通常称为入侵检测系统 (IDS)。我之前讨论的防病毒软件产品就是一个例子;但该术语最常用于位于您网络上并寻找正在进行的攻击或受损机器的迹象的盒子 [1636]。例子包括:

- 一台机器试图联系一个“已知的坏”服务,例如用于控制僵尸网络的 IRC 频道,或一个已知的坏 IP 地址 或试图

解析已知的错误 DNS 名称；

- 具有伪造源地址的数据包 例如声称是
  来自子网外部但实际上源自子网；
- 来自网络中机器的垃圾邮件。

在这种情况下，IDS 通常会告诉系统管理员需要查看特定机器。这可能只是调查的第一步，该调查涉及查看日志以了解它是如何发生的，以及攻击者可能还感染了什么。

我们在前面的章节中看到的其他入侵检测示例包括检测支付卡欺诈的机制和寻找内幕交易的股票市场系统，例如通过在价格敏感公告之前增加交易量。现在这是一个活跃的研究领域：自 2012 年以来人工智能的繁荣催生了许多寻找模式匹配问题的初创公司。

21.4.2.1 入侵检测的类型

最简单的入侵检测方法是在超过阈值时发出警报。三次或更多次登录失败、信用卡支出是过去三个月移动平均数的两倍以上，或者一次手机通话持续时间超过六个小时，都可能会引起注意。更复杂的系统通常分为两类。

误用检测系统使用入侵者可能行为的模型进行操作。如果用户连续三天从自动提款机提取最大允许金额，银行系统可能会发出警报；如果以前天真的用户突然开始使用像编译器这样的复杂工具，Unix 入侵检测系统可能会发出警报来寻找用户帐户接管。简单的误用检测系统（例如防病毒扫描程序）会寻找签名 特定攻击的已知特征。这可以在数据中是明确的（例如将其标记为特定恶意软件的可执行文件的子字符串）或在行为中（例如联系已知僵尸网络命令和控制服务器的 IP 地址的机器） .更复杂的滥用检测系统将大量签名视为信号，然后训练机器学习分类器来做出决定。正如我在第 12.5.4 节中讨论的那样，用于检测卡欺诈的系统使用数十种信号，因为考虑到现代支付系统的规模，它们需要低误报率才能发挥作用。

在没有明确的攻击者作案手法模型的情况下，异常检测系统会尝试更艰巨的工作来寻找异常行为。希望是检测以前未被识别和分类的攻击。这种类型的系统自 1990 年代以来就使用了人工智能技术，尽管一些公司避开了它们；例如，谷歌的政策是避免尝试学习阈值或自动检测因果关系的系统，而是使用简单的系统来检测最终用户请求率的变化 [236]。

滥用和异常检测之间的分界线有些模糊。
一个边界案例是本福德定律，它描述了数字在

随机数。人们可能认为以数字“1”、“2”、...“9”开头的数字同样常见。但是当数字来自随机的自然资源并且跨度超过一个数量级时,因此它们的分布独立于表示它们的数字系统,分布是对数的:大约 30% 的十进制数以 1 .

那些想出数字来伪造账本,甚至在不知道本福德定律的情况下使用随机数生成器的不诚实的职员,经常被这样抓到 [1247]。

另一个边缘案例是蜜罐 留下一些诱人的东西来吸引注意力。例如,我提到过,一些医院有带有名人姓名的虚拟记录,以诱骗忽视患者隐私的工作人员 。在网络环境中,蜜罐模拟多种类型的设备,以便攻击者扫描互联网寻找(比如)特定升级状态的 DSL 调制解调器,从而找到一个进行攻击;这可能包含一个简单的仿真器,或者具有更新的设计,即在 VM [1955] 中运行的实际调制解调器固件。

结果是蜜罐操作员可以看到谁在攻击什么以及如何攻击。

21.4.2.2 入侵检测的一般限制

有些入侵是显而易见的。如果您担心激进分子会破坏您的网站,那么可以在某处安装一台机器,该机器可以频繁获取页面并在页面发生变化时发出警报。但在一般情况下,入侵检测是很难的。病毒先驱 Fred Cohen 证明检测病毒(在决定一个程序是否会做坏事的意义上)与停止问题一样困难,所以我们永远不能指望一个完整的解决方案 [450]。

还有一个定义问题。一些入侵检测系统被配置为阻止某些类型的可疑行为。但这将入侵检测系统变成了一种访问控制机制,同时也为拒绝服务攻击打开了大门。我更喜欢将入侵检测系统定义为监视日志并引起对可疑事件的注意的系统。

然后是误报的成本。学术机器学习研究人员通常认为,当他们将分类器训练为具有 0.1% 的误报率时,他们已经做得很好了。但是,如果您是 Gmail 团队的一员,并且每天要与 10 亿用户进行身份验证打交道,那就太过分了。大型系统需要非常低的误报率。

最后,机器学习分类器存在三个普遍问题:它们不太擅长检测新攻击,人们玩弄它们,以及它们吸收了训练数据的偏见。我们将在 25.3 节中更详细地讨论这些。

21.4.2.3 检测网络攻击的具体问题

现在转向检测网络入侵的具体问题,它比支付欺诈更难发现。网络入侵检测产品仍然存在较高的漏报率和误报率。事后才检测到实际的入侵是很常见的。性能不佳的原因包括以下,在

没有特别的顺序。

- 互联网是一个非常嘈杂的环境 不仅在内容层面如此,在数据包层面也是如此。大量随机垃圾到达任何实质性站点,并且足够多的垃圾可以被解释为具有敌意以提供显着的误报率。许多坏数据包是由软件错误引起的;其他是过时或损坏的 DNS 数据的错误;还有一些是逃脱的本地数据包,环游世界并返回[213]。

- “攻击太少”。如果每百万会话有 10 次真实攻击 这几乎肯定是高估了 那么即使系统的误报率低至 0.1%,误报与真实报警的比率也将是 100。我们讨论过类似的问题防盗警报器;对于运行 HIV 等疾病筛查计划的医务人员来说,这也是一个众所周知的问题,在这种情况下,测试错误率超过了疾病流行率。在信号远低于噪音的地方,警卫会感到疲倦并且错过真正的警报。

- 虽然银行盗窃会导致不正确的状态 钱在错误的地方,以及审计线索中的证据 但许多网络入侵旨在避免这种情况,例如,如果他们的任务是泄露机密数据。

  编写软件来检测错误比检测稍微奇怪的行为要容易得多。

- 许多网络攻击特定于特定版本的软件,因此您需要一个庞大且不断变化的攻击特征库。

  然而,许多公司购买入侵检测系统以满足保险公司或审计师的要求,而且产品并不总是保持最新。

- 随着越来越多的trac 被加密,它不能轻易地进行内容分析或过滤出恶意代码。如果 DNS-over-https 成为常态,依赖于分析您的 DNS trac 的工具将变得不那么有效 ective。

- 我们在防火墙背景下讨论的问题在很大程度上也适用于入侵检测。可以在包层过滤,速度快但漏掉的多;或者您可以代理您的应用程序,这很昂贵 – 并且需要不断更新以应对新的应用程序和攻击。

- 您可能需要在本地和全局进行入侵检测。由于加密的网络会话,越来越多的事情必须在本地机器上完成;但有些攻击是隐蔽的 对手每天向大约 100,000 台主机中的每台发送 1-2 个数据包,您需要一个中央监视器来按源地址和目标地址以及端口对数据包进行计数。

如今,入侵检测系统涉及网络和端点设备群中不同级别的多种监控机制和产品的协调。正如我之前在第 21.4 节中讨论的那样,拥有数万名使用 Windows 的员工的大公司通常会有几十种产品。集成和自动化监控和

响应越来越成为 CISO 的工作。因此,增长领域包括用于安全事件和事件管理 (SIEM)、安全编排和响应 (SOAR) 以及指标的集成工具。

21.5 密码学:参差不齐的边界

网络安全以多种方式与密码学相互作用。我们已经提到过关于 DNS over https 的争论;现在我将简要描述加密的其他五个方面。它们是 SSH; WiFi、蓝牙和 HomePlug 提供的本地链路保护 ; VPN 中使用的 IPSec 机制;传输安全协议;以及用于支持其中许多的公钥基础设施 (PKI)。在上一章中,我们讨论了试图用密码学构建更值得信赖的组件的尝试如何遇到许多现实世界的工程和经济限制。我们用来在网络上设置边界并在其中转化信任的工具并没有什么不同 。

新出现的主题是问题中分布最广的部分是难以管理的,因为供应商不关心;特别是作为“物联网”的一部分销售的数千种设备类型没有可供用户使用的远程管理工具,供应商通常不升级软件,并且缺少用户界面意味着身份验证是随意的最好的。与此同时,问题中最集中的部分 PKI 经常被政府指令所破坏。

21.5.1 SSH

当我使用我的笔记本电脑访问台式机上的文件,或与我们实验室中的任何其他机器做任何事情时,我使用安全外壳 (SSH),它提供 Unix 和 Windows 主机之间的加密链接。因此,当我在家工作时,我的 trac 受到保护,当我从办公桌上的 PC 登录实验室的另一台机器时,我使用的密码不会明文通过 LAN。

SSH 最初是在 1995 年由赫尔辛基科技大学的研究员 Tatu Yl¨onen 编写的,当时那里发生了一次密码窃听攻击 [2058]。它在机器之间建立加密连接,这样登录密码就不会在网络上明文传输,并支持其他有用的特性,从而使其得到迅速采用 [1617]。

有多种配置选项,但在最直接的配置选项中,每台机器都有一个公私密钥对。私钥受用户在键盘上键入的密码保护。为了从我的笔记本电脑连接到实验室的服务器,我将我的笔记本电脑公钥安装在相关服务器上的一个文件中。当我想登录服务器时,系统会提示我输入密码;两台机器设置了一个 Die-Hellman 密钥;私钥用于签署临时公钥,以阻止中间人攻击;因此,后续的 trac 既被加密又被验证。手动密钥安装很直观,但扩展性不是特别好。还有使用 Kerberos 的选项,无论是验证使用 Die-Hellman 设置的会话密钥,还是设置

直接设置会话密钥。 （在后一种情况下,SSH 退化为 Kerberos 的变体,因为它现在是一种受信任的第三方协议,警方可以让 Kerberos 服务器解密 trac。）

可能的问题包括,如果您一次在键盘上键入一个字符,那么每个字符都会在其自己的数据包中发送,并且数据包到达间隔时间可能会泄露有关您正在键入的内容的大量信息 [1803] .然而,最糟糕的可能是大多数用于服务器到服务器通信的 SSH 密钥都是明文存储的,根本没有密码保护。因此,如果一台服务器受到威胁,同样的事情也会发生在所有其他信任安装在其上的 SSH 密钥的机器上。

SSH 通常用作简单的登录机制;许多物联网设备运行 Linux,并允许任何知道适当密码的人远程登录。这使他们容易受到密码猜测攻击,并且在存在弱密码或已知默认密码的情况下,会被招募到基于 Mirai 和类似工具的僵尸网络中。这里的对策是蜜罐。

21.5.2 外围无线网络

许多网络在边缘使用无线技术从接入点到设备或从一台设备到另一台设备的最后几英尺。 WiFi、蓝牙和 Homeplug 等协议都提供加密功能,以防止服务滥用和窃听。然而,大多数都容易受到难以完全阻止的本地攻击,因为许多设备没有打补丁,缺少用户界面,或两者兼而有之。

21.5.2.1 无线网络

WiFi 支持无线局域网,无论是在家中将电话和其他设备连接到家庭路由器,还是通过企业连接支付终端和库存控制设备以及 PC。自 1997 年推出以来,它附带了一系列加密协议。第一个被广泛使用的协议 WEP（用于有线等效隐私)被证明相当容易破解,因为美国出口管制要求的密码较弱,而且性能不佳协议设计 [299, 1873]。自 2004 年以来,名为 WPA2 的改进系统使用 AES 加密。每个接入点的密钥通常印在一张卡上,该卡可以放入路由器背面。

WiFi 网络应该被视为不受信任吗?设置密码的原因更多是为了防止第三方使用您的带宽或配额,而不是域名欺诈的风险。英国或美国的许多人都觉得有一个开放的网络供客人使用很方便,这样您和您的邻居就可以使用彼此的网络作为备份。在您为下载带宽付费的国家/地区,家庭路由器密码大多已设置。在某些国家,例如印度,运行开放式 WiFi 接入点是违法的（2008 年在孟买发动袭击的恐怖分子使用它们悄悄地给家里打电话）。将钥匙放在卡上是可用安全设计的一个巧妙示例:户主可以通过将卡别在墙上或将其锁起来,使他们的网络尽可能开放或安全。

WiFi 安全性仍然有些脆弱。通用即插即用 (UPnP) 允许网络中的任何设备通过路由器的防火墙打孔;自 2013 年以来,国土安全部一直建议人们将其关闭 。然而,现在许多设备和家用电器都带有附加的云服务,这很难。它与 WiFi 保护设置 (WPS) 一起使用,让您只需按一下按钮即可在网络上注册设备。您可以设置 PIN,但已发现针对该机制的一些攻击。

企业可能需要多加小心。 2007 年 3 月,零售连锁店 TJ Maxx 报告其系统中约有 4570 万个信用卡号码被盗; 《华尔街日报》报道说,明尼苏达州圣保罗的一个不安全的 WiFi 连接是罪魁祸首 [1509]。银行起诉该公司,并最终以 4100 万美元 [788] 和解。

打补丁是个问题。例如,在 2020 年 3 月,我们了解到 Broadcom wifi 芯片中的 Kr00k 漏洞,该漏洞将在 Mac 和 iPhone 中得到修补,但可能不会在无线路由器或旧版 Android 手机中得到修补 [799]。至于绝大多数物联网设备,从玩具到家用电器,它们永远不会得到修补。

21.5.2.2 蓝牙

蓝牙是另一种短距离无线协议,旨在用于个人区域网络,例如将耳机连接到电话,或将口袋中的电话连接到汽车的免提接口。它还用于将相机和电话连接到笔记本电脑,将键盘连接到 PC 等。与 WiFi 一样,该协议的第一个版本被证明存在缺陷 [2015、1713、1101]。从 2.1 版(2007 年发布)开始,蓝牙支持安全简单配对 [1169],它使用椭圆曲线 Die-Hellman 来阻止被动窃听攻击。中间人攻击更难;通过生成一个六位数字进行数值比较来处理它们。但是,由于其中一台或两台设备可能缺少键盘或屏幕(或两者都缺少),因此也有可能在一台设备上生成数字并在另一台设备上作为密钥输入;并且有一种“正常工作”模式无法防止中间人攻击。更重要的是,数据可能会或可能不会被签名,总共有大约十种不同的保密性、完整性和抵抗中间人攻击的组合;并且已经发现了许多攻击,其中一些受到斯诺登披露 [1635] 中列出的 NSA 工具的启发。同样,修补是一个问题。 2018 年,Eli Biham 发现许多实现可能被中间人向身份验证协议提供无效椭圆曲线 [244] 所愚弄,而在 2020 年,Daniele Antonioli 及其同事发现了 mig-in-中间攻击,你只是将来自蓝牙设备的挑战反射回它,声称你现在是挑战者而目标设备是响应者 [124]。因此,如果您的设备带有未打补丁的蓝牙芯片,则它可能容易受到攻击。

21.5.2.3 家庭插件

HomePlug 是一种用于通过电源线进行通信的协议。
HomePlug AV 广泛用于 wifi 扩展器:您将一个站插入您的

路由器或电缆调制解调器,另一个在您房子的另一端提供远程 wifi 接入点。 （利益声明:我是该协议的设计者之一。）我们面临着与蓝牙团队相同的设计限制:并非所有设备都有键盘或屏幕,我们需要保持低成本。我们决定只提供两种操作模式:安全模式,用户手动向其网络控制器输入印在设备标签上的唯一 AES 密钥,以及“简单连接”模式,在这种模式下,无需身份验证即可交换密钥.在这种模式下,密钥甚至没有加密;它的目的不是提供安全性,而是防止错误的关联,例如当设备错误地与隔壁的网络配对时 [1436]。然而,许多供应商仅支持“简单连接”模式,并在首次使用时采用信任策略,如第 14.3.3.3 节所述。其他人成对出售扩展器,并已安装密钥。智能电表可以与变电站通信,电力公司可以通过电力线为家庭提供宽带（尽管由于射频干扰而没有广泛使用）。供应商还以各种方式定制产品,使其与竞争对手不兼容。由于这种混乱,几乎不能依赖密钥管理。

21.5.2.4 VPN

虚拟专用网络 (VPN) 通常使用称为 IPsec 的协议套件在 IP 层进行加密和身份验证。这将安全关联定义为用于保护特定数据包流的密钥、算法和参数的组合。受保护的数据包可能只是经过身份验证,或者也被加密;在前一种情况下,添加了一个身份验证标头以保护数据完整性,而在后一种情况下,数据包也被加密并封装在其他数据包中。还有一个用于设置密钥和协商参数的 Internet 密钥交换 (IKE) 协议,我们可以从 Ed Snowden 的披露中推断出该协议的标准默认设置（使用 1024 位 Die-Hellman)是不安全的。

VPN 由防火墙供应商提供,因此通过在本地 LAN 和路由器之间的每个分支中安装一个他们的盒子,所有内部流量都可以通过 Internet 加密。如果有适当的软件,个别员工的笔记本电脑和家用 PC 也可以加入 VPN。 VPN 也可用于商业用途,例如伊朗和中国等国家的个人和公司使用它来绕过国家防火墙。

21.6 CA 和 PKI

正如我们在 5.7.4 节中讨论的那样,公钥密码学的先驱们开发了一种证书愿景,将公钥绑定到控制相应私钥的组织、人员或设备的名称或角色。最初认为政府或电话公司会这样做,但他们太慢了。在互联网繁荣时期,企业家们设立了证书颁发机构 (CA),微软和 Netscape 等软件公司将他们的公钥嵌入到他们的浏览器中。随之而来的是淘金热

CA 相互购买并合并;投资者希望每个设备都需要一个公钥证书,所以你需要每两年向 Verisign 支付 10 美元来更新你的烤面包机上的证书,否则它就不会与你的冰箱通信。

一旦这种愚蠢行为平息下来,世界各国政府便开始将他们自己的 CA 的根证书放入浏览器中,以用于情报和监视目的。随着人们转向 Gmail 等网络服务,安全机构开发了进行中间人攻击的工具,并且由于 TLS 用于加密密码输入(以及后来的整个会话),这意味着拥有一个 CA在 www.gmail.com 上为目标浏览器接受的安全机构公钥生成证书。事实上,在 Financial Cryptography 2011 的小组讨论中,我问 Mozilla 的人,当我前一天更新 Firefox 时,为什么它放回了我为土耳其情报组织 Tubitak 删除的证书。这时,一名男子站在观众席上大喊:“你怎么敢侮辱我的国家!” Tubitak 不是情报机构 它是一个研究机构! Mozilla 的人耸了耸肩,苦笑道:“现在你知道证书管理有多难了吧。”

那年晚些时候发生了 DigiNotar 丑闻。 DigiNotar 是一家荷兰 CA,被发现为 Gmail 颁发了通配符证书。伊朗特工入侵它以监控伊朗的 300,000 名 Gmail 用户;制裁意味着,与土耳其不同,他们不能只是让他们的政府证书在主要浏览器中停滞不前。 Mozilla 和谷歌通过删除根证书迅速将 DigiNotar 处死;微软和苹果紧随其后。

这在荷兰造成了真正的破坏,其中许多在线政府服务使用 DigiNotar 证书,并且不得不争先恐后地获得其他证书。
事实证明,另一家 CA Comodo 此前曾遭受过攻击,但该公司声称已撤销其所有错误颁发的证书。从那时起,来自浏览器根存储的 CA 和审核员的压力越来越大。

“公共(密钥基础设施)”和“(公钥)基础设施”之间经常存在语义混淆。首先,无论出现什么新应用程序,都可以使用基础架构;我将其称为开放式 PKI。第二,它不能;我将其称为封闭式 PKI。如果您正在构建政府机构可能会攻击的服务,那么最好关闭您的 PKI,并使用在您自己的场所运行的 CA 这样您就可以了解任何搜查令。我建议维护安装在数百万台机器上的软件的公司使用私有 CA 作为他们的代码签名密钥。

PKI 有许多内在的局限性,我们在分布式系统一章中讨论了其中的许多局限性。命名是一件很麻烦的事情,应用对证书的依赖程度越高,证书的使用寿命就越短。有时您可以通过删除不必要的名称来简化事情:与其在一张证书上写着“Ross Anderson 的密钥是 KR”,另一张说“Ross Anderson 有权管理 x.foo.com”,您可能只说“KR 有权管理x.foo.com.

这是“一个关键还是多个”争论的一个方面。我是否应该期望有一个单一的数字凭证来取代我目前随身携带的每一个金属钥匙、信用卡、刷卡门禁卡和其他令牌?或者应该每个

它们会被不同的 erent credential取代吗?多把钥匙保护客户:我不想必须使用一把钥匙来抵押我的房子来买我的午餐三明治。正如我们在有关银行业务和簿记的章节中看到的那样,很容易通过让设备显示另一条消息来欺骗人们签署一条消息。

现在,标准的 PKI 机制(X.509 协议套件)的开发是为了提供电话簿的电子替代品,因此它首先假设每个人在开放的 PKI 架构中都将拥有唯一的名称和唯一的密钥。

这反过来会导致信任问题,其中有很多。

- 如果您从 Firefox 中删除数百个根证书中的一个,Mozilla 会默默地替换它; Windows 附带了更多的根证书 但您根本无法删除它们。在每种情况下,您都必须知道如何将证书标记为不受信任。

- 有一些有趣的效果 ,政府在 Windows 中拥有证书但在其他浏览器中没有(例如泰国,在 2014 年军事政变后)不得不对 Mac 用户采取不同的监视方法 [1554] .

- 许多公司使用过时的证书,或者与错误的公司相对应的证书,通常是因为公司的营销部门找了承包商来进行促销或其他活动。结果,用户被训练忽略安全警告,只有一小部分人习惯于关注它们 [841]。最近,Firefox 等浏览器使得点击过去的警告变得更加困难。

- 证书将公司名称绑定到 DNS 名称,但它们的供应商通常不是这两个名称的授权机构;他们在检查申请人是否可以回复发送到该域的电子邮件,或者是否可以发布带有 CA 质询的网页后颁发证书。使用“扩展验证”证书6 情况稍微好一些,但即使它们也不是万无一失的。

- 在他们的“认证实践声明”中,CA 竭力否认所有责任。

- 证书撤销是一个问题。最初的想法是任何依赖证书的人都可以从 CA 下载证书撤销列表 (CRL) 并检查他们将要依赖的任何证书。然而,这要求在线操作以获得高保证,从而损害了公钥密码学的大部分优势。此外,某些系统(尤其是美国政府系统)的用户每次启动系统时都必须下载大型 CRL,从而导致延迟和网络拥塞。大约从 2013 年开始,人们转向在线证书状态协议 (OCSP),这是一种更有效的在线状态检查协议。

像往常一样,在所有这些混乱的背后是安全经济学。在 1990 年代的互联网繁荣时期,SSL 协议(当时的 TLS)赢得了更多

6这些用于在您的浏览器中显示一个绿色的挂锁,尽管现在已停止使用
在 Chromium 于 2020 年从第 76 版开始,经过研究表明没有人给予任何关注。

称为 SET 的复杂且重量级的协议,因为它减轻了开发人员的负担 [110]。合规成本转嫁给了用户 他们通常无法应对 [524]。从那时起,许多围绕 CA 和证书的工程一直在迎头赶上。

在撰写本文时,最大的问题是证书的生命周期;让我们加密;和证书透明度。

如果要被主要浏览器接受,证书的最长允许生命周期已经从 8 年稳步减少到 3 年,再到 27 个月。

2017 年和 2019 年的投票提议将期限缩短至 13 个月 [1581],而在 2020 年,Apple 宣布从 9 月开始,其设备将不再接受任何有效期超过 398 天的证书 [1446]。这将迫使许多网站刷新他们的证书;看看公司如何清除 DNS 中的所有证书将会很有趣。 (这还将扩大具有年度证书的系统与一些工业和物联网系统之间的差距,在这些系统中,由于软件升级困难,证书必须持续多年。)

过去获取证书很困难,因为您必须去购买一个证书,证明您控制了您的域,获取证书,将其上传到您的服务器,更改配置,然后进行所有测试。这里的变革者是一个非营利组织,互联网安全研究小组 (ISRG) 免费提供证书,到 2020 年 2 月已经颁发了 10 亿个证书。免费提供证书允许完全自动化,从而降低成本:他们的“LetsEncrypt”CA 以每年 300 万美元的预算支持 1 亿个站点。 LetsEncrypt 着手简化证书部署,其影响是实实在在的:20% 的浏览器连接仍然是明文,但这比四年前的 60% 有所下降。这项服务于 2015 年开始,也就是斯诺登事件曝光两年后。他们的自动化证书管理环境现已标准化为 RFC8555,因此商业 CA 也在使用它。有一个透明度日志,系统没有手动覆盖,因此可以保证他们从未被迫颁发证书。 (事实上,美国国家安全局使用他们的证书。)2019 年 11 月,他们是最大的 CA,为 1.88 亿个域提供了 1.12 亿个证书;他们拥有前 100 名网站的 5%,但占前 100 名网站的 35%。他们的规模意味着错误会影响很多网站; 2020 年 3 月,他们软件中的一个错误意味着必须更换涵盖 1200 万个服务器名称的 300 万个证书 [590]。

21.6.1 证书透明度

在对 Comodo 和 DigiNotar 的攻击之后,开始研究阻止恶意颁发证书的机制。证书透明度旨在通过维护每个域在野外看到的所有证书的日志来做到这一点,以便域所有者可以快速发现不应为其域颁发的证书。谷歌在 2013 年推出了第一个证书透明度日志,而 Chrome 在 2015 年开始坚持使用此类日志来扩展验证证书。谷歌发现赛门铁克在域所有者不知情的情况下为许多域(包括它们自己的域)颁发了证书 [1786],并且2018 年,所有 CA 都强制要求证书透明度。

21.7拓扑

网络拓扑是其节点连接的模式,这可能是安全架构的重要组成部分。

- 一个公用事业可能有多个孤岛,每个孤岛包含一个发电机或变电站,在受信任的网络上有数十到数百个设备,依次通过专门的防火墙和 VPN 连接到网络控制中心。

- 云服务提供商的数据中心可能有数万台机器,提供商及其租户颁发的证书层次结构决定了哪些虚拟机或哪些机器上的容器可以相互通信。虽然内部网络可能不受信任,但从某种意义上说,网络位置在访问控制决策中不起作用,它可能会免受前端系统的 DDoS 攻击。

- 政府使用的机密系统可能有相当大的可信网络在较高级别运行,建筑物中有单独的局域网。

可以找到更复杂的拓扑,其中节点是用户,边缘是它们在彼此的地址簿中的存在。社会网络分析已被应用到从流行病学到犯罪学和新技术如何扩散的研究,再到研究直接在用户之间传播的危害,例如宏病毒 [1433]。社交网络可以通过具有顶点顺序的幂律分布的图来建模;少量连接良好的节点有助于使网络对随机故障具有弹性,并且易于导航。然而,它们也使此类网络容易受到有针对性的攻击。移除连接良好的节点,网络很容易断开[36]。独裁者凭直觉知道这一点;斯大林通过杀害富裕农民巩固了他的统治,波尔布特杀害了知识分子,而征服者威廉则杀害了撒克逊绅士。现在我们有了定量模型,它们有助于解释为什么革命者倾向于将自己组织成细胞 [1373];通过仅针对几个关系密切的组织者进行 trac 分析,警察部队可以识别数量惊人的持不同政见者组织的成员 除非持不同政见者首先以细胞结构组织起来 [510]。

21.8 小结

预防和检测通过网络发起的攻击是现代 CISO 工作的核心。这很困难,因为它涉及范围广泛的攻击类型和安全技术。它可能导致具有新闻价值的失败。不太可能有任何神奇的解决方案,尽管很多事情都可以提供帮助。每一项新的进步都会带来新的担忧;例如,云服务可能会将大部分网络安全任务转移给提供商,但会使配置管理变得更加关键。总的来说,这些问题是如此复杂和混乱,以至于管理它们需要一种自动化的全系统方法。

黑客技术部分取决于对主要供应商意外引入的漏洞的机会性利用,部分取决于通过社会工程让人们运行不可信代码的技术。然而这些已经发展成为一个完整的坏人生态系统,这也是安全工程师需要研究和理解的。

研究问题

2000 年,网络安全研究的重心是技术:随着拒绝服务攻击的可能性开始变得清晰,我们正忙于寻找对协议和应用程序的新攻击。到 2010 年,关于经济和政策的讨论更多:关于改变责任规则如何让事情变得更好 [97]。到 2020 年,将有更多关于指标的工作:衡量实际发生的邪恶行为,并将其不仅用于政策辩论,还用于执法。在操作层面,游戏是关于自动化和集成 让大公司能够处理大量威胁情报和网络监控信息,将其转化为可操作的情报,并衡量网络安全团队的工作效率。

进一步阅读

早期的互联网安全经典由 Steve Bellovin 和 Bill Cheswick 撰写,Avi Rubin 加入了他们的第二版 [221]。关于病毒的开创性工作是由 Fred Cohen [450] 完成的,而 Li Gong（设计它的人)[783] 讨论了 Java 安全性。对于 BGP 安全,请参阅我们的 2011 年 ENISA 报告:完整的 Monty 超过 200 页,专为开始攻读网络安全博士学位的人设计,但也有较短的执行摘要 [1906]。

有关恶意软件的更详细概述,我可能会推荐 Wenke Lee 的 Cybok 调查论文 [1137]; Sanjah Jha 的 Cybok 网络安全调查提供了 IPSEC 以及以太网和基于端口的安全性的更多细节 [983]。

我不知道关于证书颁发机构生态系统的任何好的概述。您可以从 2004 年对 Verisign 创始人 Jim Bidzos 的口述历史采访开始 [240]。 Microsoft 和 Netscape 的最初目标是在万维网上快速启动电子商务;证书的使用然后传播到密码和软件更新,当 Javascript 出现时,同源原则将信任转移到网站。许多其他参与者加入进来,一些政府机构试图破坏 CA 生态系统,而另一些则试图加强它。技术安全目标与法律目标之间存在冲突,审计人员与监管机构之间也存在冲突。因此,来自 WebTrust（美国和加拿大会计师)和 ETSI（最相关的欧洲标准机构)对 CA 安全的看法截然不同。有关更多详细信息,Ryan Sleevi 关于生态系统问题的演讲 [1785] 为那些想要深入研究当前问题（包括技术和运营)及其背景的人提供了很多建议。