网络安全第一周报告

这周我浏览了几个老师推荐的网站如 www.cert.org.cn,www.infrosec.org.cn 等，了解了国内外有关网络安全的事件，在国际上国家，组织之间通过黑客间谍互相攻击，窃取对方资料，如美国网络攻击伊朗，黑客攻破土耳其国家警察服务器等等。也了解了在国内黑客通过各种手段窃取个人隐私的手段，如“相册”系列 Android 恶意程序，Android 平台窃取用户短信和通讯录的恶意程序等等 ,使我进一步认识到网络安全危机的无处不在和网络安全的重要性。

除此之外，我还阅读了老师提供的有关攻击手法的资料如 Buffer Overflow Exploits，在这片文章中，我初步了解了黑客如何通过缓冲区溢出来攻击用户电脑和蠕虫病毒的历史。通过 buffer overflow 来攻击 VAX 系统是蠕虫病毒在之前的攻击手法之一，他通过发送特定的字符串给用户的守护进程，蠕虫使进程执行代码来使蠕虫繁殖。而在当代，超过 50%的网络安全事件都与 Buffer overflow 有关，其攻击手法包括 stack buffer overflow,off-by-one overflow,heap overflow,function pointer overflow,exploiting of format string 等等。在 stack buffer overflow 中当用户的缓冲区被攻击者的 string 占领，函数返回地址被改写，当函数被调用，就会给攻击者套上一层伪装，这个问题的主要原因是没有范围检测，但有时范围检测也会出现问题，并非万全之策。而 heap overflow 将会改写原有的指针，使其指向重要但无法正常访问的文件。函数指针的溢出将会使程序调用非法函数。格式化字符串也会被利用来改写地址内容。除此之外，如果网络服务器在存储 RUL 的缓冲区溢出，那么攻击者可以通过提供畸形 URL 来获得控制权。

既然 Buffer overflow 如此常见，那么必然有对应他的方法。最简单的方法就是用相对安全的语言如 java。除此之外的方法还有 Non-Executable Stack，Run-Time Checking，StackGuard Dereference，PointGuard Dereference。然而，就算有这么多方法还是无法阻挡 buffer overflow 的发生，毕竟 We Will Never Achieve a Perfectly Secure System!