Neusoft东软

NetEye Event Language 技术简介

（第一版）

沈阳东软软件股份有限公司

2006 年 5 月

NEL（NetEye Event Language）是东软自主研发成功的一种通用攻击描述语言，包括 NEL 语言规范及相应的开发环境。NEL 为不同类型的入侵检测防御产品（如网络 IDS/IPS、主机 IDS/IPS、应用防火墙、应用安全增强模块等）的开发提供了一个具有强大描述能力、高度的可扩展性和很高代码执行效率的语言平台。

NEL 是一种过程型编程语言，提供了很多高级语言中才有的过程性手段，具有强大的描述复杂攻击的能力。NEL 引入了事件这一新的语言元素，同时引入了事件逻辑约束关系，使得 NEL 具有强大的攻击描述能力的同时，提供了攻击检测防御所必须的抽象性和概括性。NEL 平台具有良好的可扩展性，采用 NEL 开发的产品可以快速开发出针对新的漏洞和攻击的防护方案。

开发人员可以采用 NEL 基于协议异常、漏洞特征或攻击特征等来定义攻击检测防御规则。基于协议异常或漏洞的 NEL 规则更准确地描述了攻击的本质特征，因此具有极强的攻击抽象力和检测效率，往往一条规则就可以检测数十种攻击，并有效阻止 0-day 攻击。下面以 SMTP 协议为例，简单介绍一下如何采用 NEL 编写攻击检测防御规则。

RFC 中对各种协议的状态转换、交互过程都是有严格限定和规范的，如果协议的交互过程偏离了协议规范，就是一种协议异常，而这往往意味着攻击。下面是一个通过检查协议状态转换异常来检测抵御攻击的例子。

```
BAD_DATA_REQ: data_req($0->mail_state < SMTP_MAIL_STATE_RCPT_TO )
{
    smtp_deny($0, "Haven't seen RCPT TO command before this DATA command!\n");
}
;
```

说明：根据 RFC 2821，在一个合法的 SMTP 连接过程中，只有在客户端至少发送过一个“RCPT TO”请求命令之后，客户端发送“DATA”请求命令才是合法的，*$0->mail_state < SMTP_MAIL_STATE_RCPT_TO* 即代表着在 SMTP 连接过程中，客户端尚未发送过“RCPT

TO”请求命令，因此通过这条规则可以阻挡住所有不符合 SMTP 协议标准交互过程的“DATA”请求命令，同时也将所有利用直接发送“DATA”请求命令进行的攻击拦截下来。

基于 NEL 的安全产品具有非常强的客户化和定制化能力。以 Web 应用为例，通过在规则中引入应用环境相关的信息（如 Web 应用所允许使用的参数数量、参数名、数据类型、页面语言、通信协议等），可以开发出定制化的 NEL 规则，增强其适应性和准确性，更好地抵御各类缓冲区溢出攻击、SQL 注入、URL 攻击等等。

下表是 NEL 与 SNORT、BRO 这两种目前比较流行的攻击描述语言的对比。

		NEL	SNORT	BRO
开发模式		语言平台/协议分析/攻击检测防御规则的开发可分别由三个小组分别完成，层次清晰，彼此的工作不会互相影响	语言平台与攻击检测防御规则的开发可由两个小组分别完成，彼此的工作不会相互影响；协议分析与攻击检测防御规则紧藕合在一起，检测规则中必须包含协议分析过程	语言平台与攻击检测防御规则的开发可由两个小组分别完成，彼此的工作不会相互影响； 语言平台与协议分析紧藕合在一起，必须由同一个小组完成
规则开发人员的要求		无需了解协议分析和语言平台的内部细节	需要了解协议分析的内部细节	需要了解语言平台的内部细节
协议扩展性		强	弱	强
检测准确性		高	低	高
检测能力	协议分析能力	强	弱	强
	漏洞描述能力	强	弱	强
	抵御变形攻击能力	强	弱	强
运行效率		编译模式，运行效率高	编译模式，运行效率高	解释模式，运行效率低
利用已有 C 代码的能力		具备	不具备	不具备

表 1　NEL 与其它攻击描述语言的对比

由上表可以看出，NEL 平台具有强大的攻击描述能力、优异的可扩展性和卓越的运行效率，同时具有无缝调用 C 语言实体的能力。因此基于 NEL 平台可以很方便地针对不同的安全需求开发相应的安全产品，NEL 平台的主要应用领域包括：

1. 专注网络安全领域的厂商、科研院所和组织机构等，可以采用NEL平台开发IDS/IPS、应用防火墙、蠕虫检测系统、垃圾邮件防护系统、DOS/DDOS防护系统、异常流量监控系统、P2P 应用（BT、MSN、QQ、SKYPE 等）控制/过滤系统、安全服务器（如WEB/MAIL/FTP/ DNS/文件服务器）等等。
2. 操作系统开发商可以采用 NEL 平台对操作系统常用的服务和协议进行安全性增强，开发安全操作系统。
3. 数据库及数据库应用开发商可以采用 NEL 平台增强数据库通信协议的安全性，加强对数据库通信过程的审查，及时发现对数据库的非法访问与恶意攻击，保障数据库自身的安全性。
4. 应用系统开发商可以采用 NEL 平台对应用（如 web 访问、web service 服务等）流量进行过滤和检查，及时发现利用应用服务进行的攻击、窃密等行为。
5. 网络设备供应商可以采用 NEL 平台增强路由协议、SIP 协议、H.248 协议的安全性，检测针对语音/视频服务系统的攻击，增强电信运营网络的安全性。
6. 移动软件开发商可以采用 NEL 平台开发手机等移动设备的安全模块，检测手机病毒等新的威胁。

NEL 作为一种具有中国自主知识产权的攻击描述语言，东软希望 NEL 能够在信息安全领域得到广泛应用。为此，东软推动成立了“NEL 开发联盟”。作为一个知识互享和经验交流的平台，国内外信息安全领域的厂商、组织机构、技术人员可以通过“NEL 开发联盟”随时了解 NEL 平台最新的功能特性、技术进展、应用领域和发展方向，合作开展基于 NEL 平台的安全技术和产品的研究开发，将 NEL 打造成为象 JAVA 在企业级计算领域一样的，在网络安全计算领域“遍在”的语言平台。

如您希望了解更多NEL技术和“NEL开发联盟”的相关信息，可以访问东软NetEye网站，http://neteye.neusoft.com，点击“NEL开发联盟”栏目，获取您感兴趣的信息。或者发邮件到xusq@neusoft.com，邮件主题请包括“NEL开发联盟”字样。

期待您的关注与参与！