2019年3月初周 内部威胁主客观特征融合检测框架研究

二〇一九年三月六日星期三

下午2时11分

至今为止，自己已经就行为特征树构建了针对内部攻击者异常行为的检测框架（18-TrustCom），同时使用CPB特征刻画了信息窃取与内部破坏两类典型内部攻击的内在动机模型，并采用KMeans+OCSVM的方式构建了主观高危用户检测器（《计研发》在投），接下来作为自己博士毕业研究的总结，将研究如何结合使用内部用户的行为异常与主观风险协同识别内部恶意用户。

上述研究的初心在于：内部恶意用户，一方面要具有恶意性，一方面要表现出恶意行为。自己之前的工作分别从两个方面开展了研究，并且通用检测框架中设置了多个阈值以供风险数值进行作用，需要注意的是，自己提出的误报过滤方法适用于正常行为数量远大于恶意行为的情况，在低阈值情况下更多正常行为参与到误报过滤中，可以进一步提升误报过滤效果。

今天上午初步进行了思考，提出了一种基于用户层面的融合检测方法，即融合点在于表现出异常行为的异常用户集合UsersAD与识别为高风险的高危用户集合UsersHR的三种关联。

1. 用户层面融合框架

无论是处于Static/Dynamic模式，假定获取了相同时间节点/窗口的异常用户集合与高危用户集合ADU与HRU，那么依据集合关系有三种关联：

1. 若用户A属于ADU∩HRU，则A既具有攻击动机又有异常行为，作为最终恶意内部用户报警，输出到MUS(Malicious Users Set)
2. 若用户属于HRU-ADU，则A具有攻击动机却尚未表现出当前阈值下的异常行为，故依据其动机数值一定降低异常阈值，重新检测已有行为数据，若发现了异常行为，则添加到MUS中（提升了恶意用户的召回率），若依旧无异常行为，则作为可疑用户持续以新的低阈值进行后续检测；
3. 若用户属于ADU-HRU，则A表现出异常行为但是没有明显的攻击动机，故作为可疑用户持续以当前阈值监测；

上述方法融合后的效果应该至少有两点：

1. 对于HR检测Recall=1的攻击场景（如CERT4.2的场景三），可以使用HRU来交叉过滤ADU，即同时提升ADU的召回率且降低误报率；
2. 对于HR检测Recall<1的攻击场景（如CERT4.2的场景一/二）