OWASP

Open Web Application Security Project

应用安全领域的关键趋势—RASP技术

王青龙

RASP技术简介

RASP

(Runtime application self-protection)

“运行时应用自我保护”

Gartner 在2014年应用安全报告里将 RASP 列为 **应用安全** 领域的 **关键趋势**，并将其定义为:

> *Applications should not be delegating most of their runtime protection to the external devices. Applications should be capable of self-protection (i.e., have protection features built into the application runtime environment).*
>
> （应用程序不应该依赖外部组件进行运行时保护，而应该具备自我保护的能力，也即建立应用运行时环境保护机制。）

RASP技术产生

未知攻击

攻击商业化演变越来越多组织
研究的未知攻击方式层出不穷

防护精度

大多防护类产品基于规则的方
式进行防护防护精度远远不够

体验极差

现有防护产品对于攻击的判断
比较粗暴带来的防护体验极差

边界模糊

云计算给用户带来的大量迁移
导致防护的边界模糊甚至消失

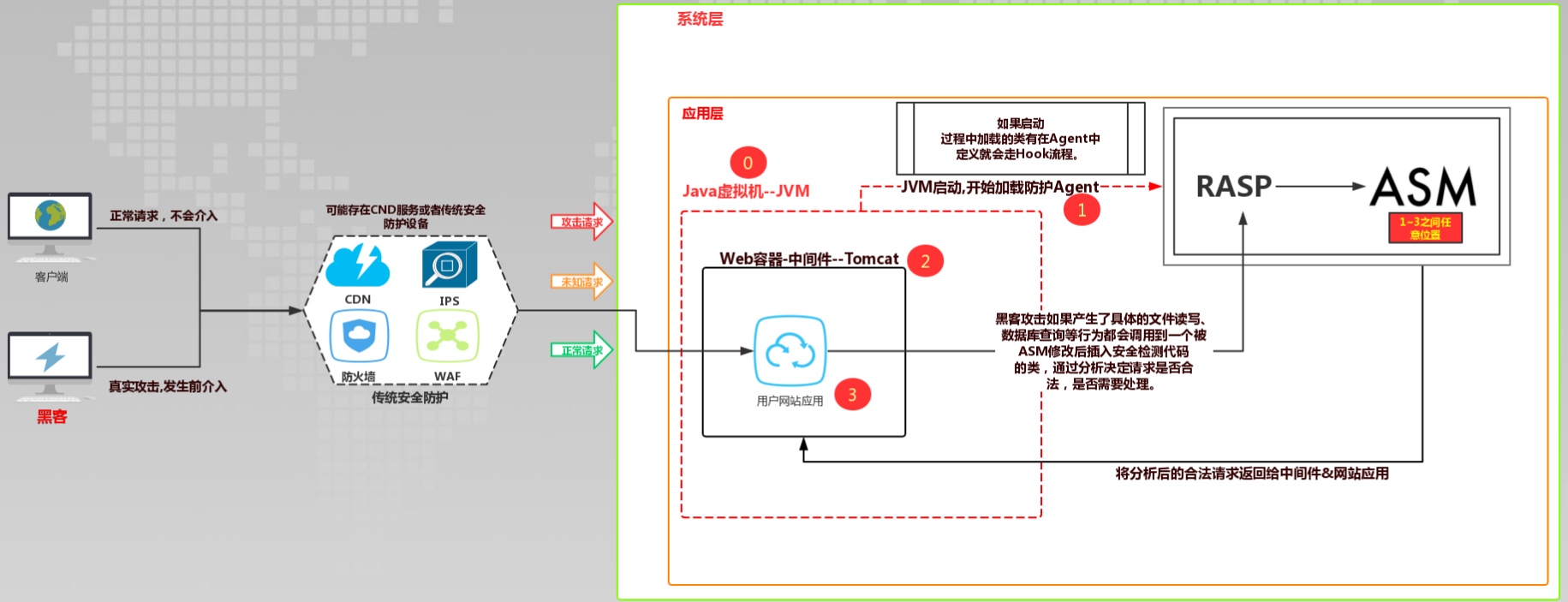
数据多样

随着业务的不断线上运用各类
数据随之增多给防护带来挑战

环境复杂

用户的应用系统的运行环境多
样性给防护体系带来极大困扰

RASP技术逻辑



RASP技术亮点

防御更广

应用程序一起运行，了解应用的上下文和运行逻辑，在运行中可以精确掌握攻击请求并进行实时拦截。

误报更低

无需借助规则，对应用的结构及请求最终执行实时完全的掌握对无法达成的攻击不在进行判断或告警。

兼容更好

与应用程序完全融合，不仅了解应用程序的实现更能够有效的兼容应用所有API可做到无缝完美融合.

效率更高

对攻击请求能够精准的识别与判断，实时对攻击请求进行拦截和处理，能够第一时间对事件告警和处置。

RASP技术能力

OWASP Top 10 2017	
A1 – 注入	A6 – 安全配置错误
A2 – 失效的身份认证	A7 – 跨站脚本 （xss）
A3 – 敏感信息泄露	A8 – 不安全的反序列化
A4 – XML外部实体（XXE）	A9 – 使用已知漏洞组件
A5 - 失效的访问控制	A10 – 不足的日志记录与监控

RASP技术能力

expression(表达式执行)

scanner(扫描器攻击)

filemode(恶意文件访问)

webshell(后门拦截及检测)

upload(文件上传攻击)

spring(Spring框架增强)

patch(动态补丁)

cmd(本地命令执行)

Server-Side Request Forgery(SSRF攻击)

webserver(畸形文件攻击、未授权路径访问拦截)

RASP vs WAF 技术对比 部署

RASP

- 嵌入在应用程序内部，应用代码无感知
- 简单到可以一键部署
- 无需配置与学习
- 开发语言强相关

WAF

- 外部边界入口统一部署
- 支持透明(串联)、旁路、反向代理三种方式
- 需要配置与学习
- 无开发语言限制

RASP vs WAF 技术对比 能力

RASP

- 防护已知攻击和未知攻击
- 基于规则&行为判断
- 支持虚拟补丁修复
- 误报率极低

WAF

- 防护已知攻击
- 基于规则判断
- 不支持虚拟补丁
- 误报率较高

RASP vs WAF 技术对比 性能

RASP

- 关键点检测
- 消耗cpu及内存
- 性能消耗在<10%
- 请求延迟小

WAF

- 规则越多，性能越低
- 无cpu及内存消耗
- 无性能消耗
- 请求延迟大

RASP全球厂商

waratek

OpenRASP

Prevoty
Now Part of IMPERVA

RASP全球厂商

- Arxan:
- Avocado
- BrixBits
- CA Technologies-Veracode
- CIX Software
- Checkmarx
- Contrast Security
- Hdiv
- Hewlett Packard Enterprise (HPE)
- Pradeo
- Promon
- Signal Sciences
- Synopsys
- tCell
- Vasco
- Virsec
- Immunio

OWASP

Open Web Application
Security Project

感谢聆听，谢谢大家！