道和邦-用户智能令牌 ECToken 服务

#V1.3.0
#author:walksing
#cdate 2022-04-16
#last 2023-07-20
#密级:*****

业务甲方：
项目乙方：道和邦（广州）电子信息科技有限公司

目录

一 背景

道和邦，以道和天下，协和万邦为理念

本项接口服务用于对用户智能识别 ECtoken（服务端免内存）智能认证，智能拦截服务

本项是技术产生是基于 SMG-iSBS 可迭代超级商城身份智能识别，级 DOBHON-DP-SFTV 动态代理网关打通实现动态抓取影视信息，可实现基于 DP 网关实现 js 反编程拦截破除广告；实现动态基于源网站信息实现可预期展现有价信息过程；如影视剧信息，有价信息是搜索，列表，详情-播放，剧集；可定向针对性实现信息的资源聚会，打通一站式影视信息孤岛，含智能分润结算。

ECToken 是基于加密 Cookie 缓存在浏览器客户端，每次请求动态传 token 被服务器解密进行身份识别；服务端无需建立缓存省却大量硬件。

本方案实施的必要前提条件，必须是洛数超算加密支撑，传统加密算法部署会耗费大量 CPU 计算时间。本算法较传统 AES/BASE64 算法快 120 倍。

本服务，可智能抵抗反爬虫攻击；登录端无需手机验证码；其原理是通过分段无痕加密 js 组合；只有真正的浏览器内核方可正确解析；真正内核浏览器 js 解析器开发工作量巨大；密钥一次一密钥；保障信息安全。

本服务为一系列技术生态组合产生新的技术。可将网络攻击由业务攻击转向代理网关 DPG 的攻击，而 DPG 攻击第一步就是 ECToken 校验，没有先注册登录，这样会自动拦截机器人账户；业务系统按本业务接口做好技术对接，将鉴权统一委托给代理网关；相当于给业务增加网盾保护。

本服务尤其适合广大各类企业服务使用；解决信息安全；业务接口改造过程采用最省时省力的方案；通过代理网关完成 ECToken 智能解读；而又不参与核心业务系统的研发；保护企业业务系统独特性，安全性；同时也保护 ECToken 密钥，颁发，组装的安全性；因为 ECToken 为 SAAS 服务；不对外发布 API.

本服务采用自己实现的洛数 hash（杂凑）算法：Luoshu81Encrypt.hashLuoshu

其性能较 MD5/sha 系列 快 5-10 倍；生存 32 位数字，也是超算加密密码学的基石。

二 本项技术支撑

2.1 ECToken 智能令牌颁发

2.2 Msession Cookie 读写

2.3 AFS 可迭代并行存储（超存储）

2.4 Luoshu81Encypt 洛数超算加密系列套件

2.5 IPSC 轻量级 IP 无痕登录校验器

2.6 dproxy 动态代理网关服务

三 预期效果

3.1 网盾效用，反爬虫攻击

3.2 无需短信验证码，体验性强

3.3 ECToken 加密令牌，智能识别身份

3.4 http 无状态认证 ,可随时重启 web 服务，业务不中断

3.5 基于 IP 绑定认证

3.6 服务端无内存，节省大量内存硬件资源

3.7 支持大用户量访问

3.8 支持动态刷写加密 KV 到 ECToken

四 业务系统整改规则

4.0 先选一个简单的业务系统做整改测试

4.1 备份业务系统源码，重新 clone 一份业务系统以做整改

4.2 公告模块调用

4.2.0 Wresposne 代理输入、输出类

入参智能过滤：
Eg:Wresponse 代替标准 response 类（以 java 为例）
Wresponse out=new Wresponse(request,response);
原：
主键类型 String usrid=request.getParameter(“usrid”);
非主键类型 String content=out.getParameter (“content”);

改：
主键类型 String usrid=out.getParameterPK(“usrid”);
非主键类型 String content=out.getParameterNPK(“content”);
getParameterPK, getParameterNPK 都做了攻击性参数过滤
其功能可自动屏蔽 sql 注入漏洞，url 注入漏洞

4.2.1 提交鉴权域名

如:mbs.xxx.com dns 指向:cname:mbs.dohbon.com
如果无法提供域名，默认以 mbs.dohbon.com 代替 mbs.xxx.com

4.2.2 删除所有原业务中调内存读用户信息的代码逻辑

如：String usrid=Msession.mget(request,“usrid”) 本段代码是取内存 session usrid ;
改造如下：String usrid=Msession.get(request,”usrid”); 该方法是取 Cookie
等同于 Wcookie.get(request,”usrid”)

4.2.3 禁用 web 服务下的自动 session 功能

如：session.get(“”) 因他们不支持大用户访问

4.2.4 鉴权成功标志

1）http header:
2）Cookie:islogin=1;siptk=xxxx;

4.2.4.1 通过 ua.jsp 读取

https://mbs.dohbon.com/mbs/dproxy.jsp?u=https://mbs.dohbon.com/mbs/ua.jsp

islogin:1
siptk: == 配置值
则校验通过

cgate:hw.hk.51　这里是一级网关代理

cip:120.230.111.8　这里可读取用户端真实 ip

usrid:$usrid　来自 ECToken 当前 usrid

sname:mbs.xxx.com

sip: 182.160.9.206 服务端 IP

siptk: 357634677635323587669711446143 81 服务端 IPtoken

islogin:1　这里标识鉴权 OK 且判断请求者 sname 与实际请求域名一致性验证,siptk==357634677635323587669711446143 81,则无条件放行访问业务子系统，不然，则重定向到 mbs.xxx.com 进行登录

注：此 siptk=357634677635323587669711446143 81 为定值基于 182.160.9.206

测试用例如下：

https://mbs.dohbon.com/mbs/dproxy.jsp?u=https://mbs.dohbon.com/mbs/ua.jsp

referer:https://mbs.dohbon.com/mbs/ua.jsp

host:mbs.dohbon.com

x-real-ip:117.80.6.81

remote-host:117.80.6.81

cgate:hw.hk.51

cip:117.80.6.81

sch:https

x-forwarded-for:117.80.6.81

connection:close

accept:application/xml,application/xhtml+xml,text/html;q=0.9,
text/plain;q=0.8,image/png,*/*;q=0.5

user-agent:SMG-DPG3.3.0/ (mbs.dohbon.com)

content-type:application/x-www-form-urlencoded

usrid:walksing

sname:mbs.dohbon.com

sip:182.160.9.206

siptk:3576346776353235876697114461438 1

islogin:1

cache-control:no-cache

pragma:no-cache

4.2.4.2 通过 cookie:islogin=1；siptk=xxx;

校验 siptk 配置值相等可认为鉴权通过,改参数禁止业务系统对其写

仅在登录网关由网关改写状态

4.2.5 dproxy 代理访问模式

所有业务访问模式通过 dproxy 动态代理网关访问

动态代理网关会智能解密 ECToken 并完成鉴权，业务子系统访问格式如下：

https://mbs.xxx.com/mbs/dproxy.jsp?u=https://service.xxx.com

以下为影视剧代理调用模式参考

4.2.6 eget 智能令牌读取当前访问者信息

https://mbs.xxx.com/mbs/dproxy.jsp?act=eget&dn=mbs.xxx.com&dntk=xxxx

act:eget 读令牌

dn:当前访问者域名

dntk:域名令牌（需要事先向乙方申请颁发）

返回解密后的信息

格式如下：&$key1=$val1&$key2=$val2&...

注：该接口，请控制调用频率，仅在必要获取用户详情信息时调用；否则会被智能网关拦截

4.2.7 eset 写入 ECToken 指令功能

写入指令有效期依赖于 ECToken 有效期，默认有效期 30 天；直到令牌重新登录颁发，自动续期。
调用参数：/mbs/dproxy.jsp?act=eset&dn=mbs.xxx.com&dntk=xxxx&$key1=$val1&key2=$val2
规则约束：当$key=roles 时,禁止$val=S,其他值通过
本指令可对当前用户设定若干加密信息键值对写入 ECToken,建议包括字段总长度小于 2K 字节；用于加密 session 会话共享，比如加密存储指纹信息，写入 cookie，
仅服务端解密测试用例:
https://mbs.xxx.com/mbs/dproxy.jsp?act=eset&dn=mbs.xxx.com&dntk=xxxx&nickname=天一

4.2.8 登录

https://mbs.xxx.com/mbs/index.jsp
输入:usrid,passwd 自动登录，登录成功后自动颁发加密令牌存入 cookie:user 字段
登录成功后
自动重定向到
https://mbs.xxx.com/mbs/dproxy.jsp?u=https://service.xxx.com/
进入业务入口

4.2.9 注册

https://mbs.xxx.com/mbs/register.jsp
提交基本信息完成注册，需要牢记邮箱
注册成功后自动重定向到
https://mbs.xxx.com/mbs/index.jsp?u= https://service.xxx.com/

进行登录

----------（完）----------