

基于内核的商用密码基础设施

全软件栈商用密码操作系统解决方案





张天佳 阿里云商密软件栈负责人

在阿里云操作系统团队担任安全技术开发,主要研究方向为OS安全,包括可信计算,机密计算。目前专注于国内商用密码的技术开发以及推广工作,主导开发了Linux内核,libgcrypt等多个项目的商用密码工程化以及优化实现,也是国内主流商密基础库解决方案BabaSSL的技术委员会委员,同时负责Anolis社区商密软件栈项目。



商用密码简介及现状

标准自主制定

密码算法国产化

一致用户体验

商业应用空白

生态碎片化

国际技术封锁



商密算法与对应的主流算法

类型	国际算法	商密算法		
对称算法	DES, AES	SM4		
公钥算法	RSA, ECDSA, ECDH	SM2 SM3		
消息摘要	SHA256, MD5			
传输层安全协议	SSL, TLS	TLS1.3 + 商密算法套件 (RFC8998) GM/T 0024和TLCP商密双证书协议		
证书	sha*WithRsaEncryption	SM2-with-SM3		

4



商密基础设施架构

应用生态 NGINX, Tengine, curl BabaSSL, libgcrypt, Gnulib 算法基础库 内核 linux, grub, shim CPU,加速器,UEFI 硬件固件

HTTPS, TLCP应用

sm3sum, TLS 1.3 + 商密套件

modsign, IMA

SecureBoot



Babass

主打商密的密码算法库,与OpenSSL 1.1.1保持兼容

蚂蚁阿里内部项目合并,主要发起者杨洋,OpenSSL Maintainer 完全以社区方式动作,BabaSSL技术委员会决策项目发展方向

BabaSSL已于2020.10开源:

https://www.babassl.cn/

https://github.com/BabaSSL/BabaSSL

当前最新stable版本: 8.2.1



BabaSSL 场景



存储服务



网络服务



1OT嵌入式 移动端设备



BabaSSL 功能特性

当前稳定版本 (BabaSSL 8.2.1) 的特性:

- 基于OpenSSL 1.1.1,具备OpenSSL 1.1.1的全部能力并且保持兼容
- 支持商密SM2, SM3和SM4, SM4 GCM/CCM模式算法
- 更加完善的SM2算法支持,比如X.509证书签发、验签的支持,这是OpenSSL 1.1.1欠缺的能力
- GM/T 0024 和 TLCP 商密双证书TLS协议
- 支持RFC 8998: TLS 1.3+商用密码算法套件
- 提供了对IETF正在标准化过程中的Delegated Credentials
- 支持 IETF QUIC API 底层密码学能力
- 正在申请软件密码模块一级资质



BabaSSLX寸比OpenSSL

特点	BabaSSL	OpenSSL		
IETF新密码技术 (Delegated Credentals, Compact TLS)	快速跟进	相对保守		
商密算法支持	深度支持	有限支持		
商密协议支持	支持TLCP和RFC 8998	无		
商密算法技术合规	软件密码模块1级*			
开源社区	完全国内可控开源社区	国际开源社区		
API易用程度	简易API *	API比较复杂		
国产硬件支持	默认支持	默认不支持		
云厂商集成	深度集成阿里云	无		
嵌入式设备友好	是	9 否 (不在发展路线上)		



开源软件对商密的支持情况以及社区回馈统计

开源软件名称	SM2	SM3	SM4	SM4- avx/avx2	PKCS#7	x509	commit数量	修改行数
gnulib	-	▼	_	_	_	_	5	-5/+1046
libgcrypt	V	V	V	Υ	-	-	13	-64/+1630
linux	$\overline{\checkmark}$	Υ	Υ		开发中	V	26	-301/+6936
OpenSSL	V	$\overline{\checkmark}$	✓	×		V	123	-3391/+11958
coreutils	-	Υ	-	-	-	-	1	-1/+1
RustCrypto	×	V	Υ	×	-	-	1	-0/+851
ima-evm- utils	✓	✓	-	-	-	-	5	-13/+97
tpm2-tools	-	~	-	-	-	-	21	-52/+982

- V 表示由OpenAnolis开发并已经贡献到开源软件中的特性
- "开发中"表示由OpenAnolis开发中的、或是开源软件正在进行review的特性
- "Y"表示开源软件已经支持且不是由OpenAnolis开发的
- 🗙 表示开源软件尚未支持
- "-"表示开源软件无需支持



商密软件栈主要成果

- Gnulib库中实现了SM3算法的基础实现,Gnulib是GNU软件栈中一个通用的基础库
- 实现了libgcrypt中基础的商密算法SM2/3/4
- 实现了Linux内核里SM2算法,以及支持了使用SM2/3算法的pkcs#7签名,X509证书
- 使用x86 AVX2指令集优化内核的SM4算法,相比于纯软件实现,有接近8倍的性能提升
- Linux内核Kernel TLS支持使用SM4 GCM/CCM算法
- IMA场景支持使用SM2/3算法组合,包括内核和用户态工具ima-evm-utils的支持
- 在Rust生态中主流算法库RustCrypto中实现了SM3算法
- 支持coreutils社区实现sm3sum工具,目前以 cksum -a sm3 方式在上游社区支持
- OpenSSL的KTLS支持以及商密实现上的若干问题修复



Anolis商密版OS

操作系统层面内置商用密码的解决方案

内置商密

兼容开放

开箱即用



Anolis 商密版OS - 特色功能

全链路支持商用密码基础设施

下载地址: <u>https://mirrors.openanolis.cn/anolis/8.2/isos/ShangMi/</u>

- 使用BabaSSL替代OpenSSL作为系统默认的基础密码算法库
- linux kernel支持完整的SM2/3/4算法以及使用商密算法的PKCS#7签名和X509证书
- 提供给开发者SM2/3/4商密算法基础库以及使用商密算法的X509证书以及SM2签名能力
- 提供GM/T 0024和TLCP国密双证书协议基础库
- 支持RFC 8998协议开发,在TLS 1.3中使用商密算法套件



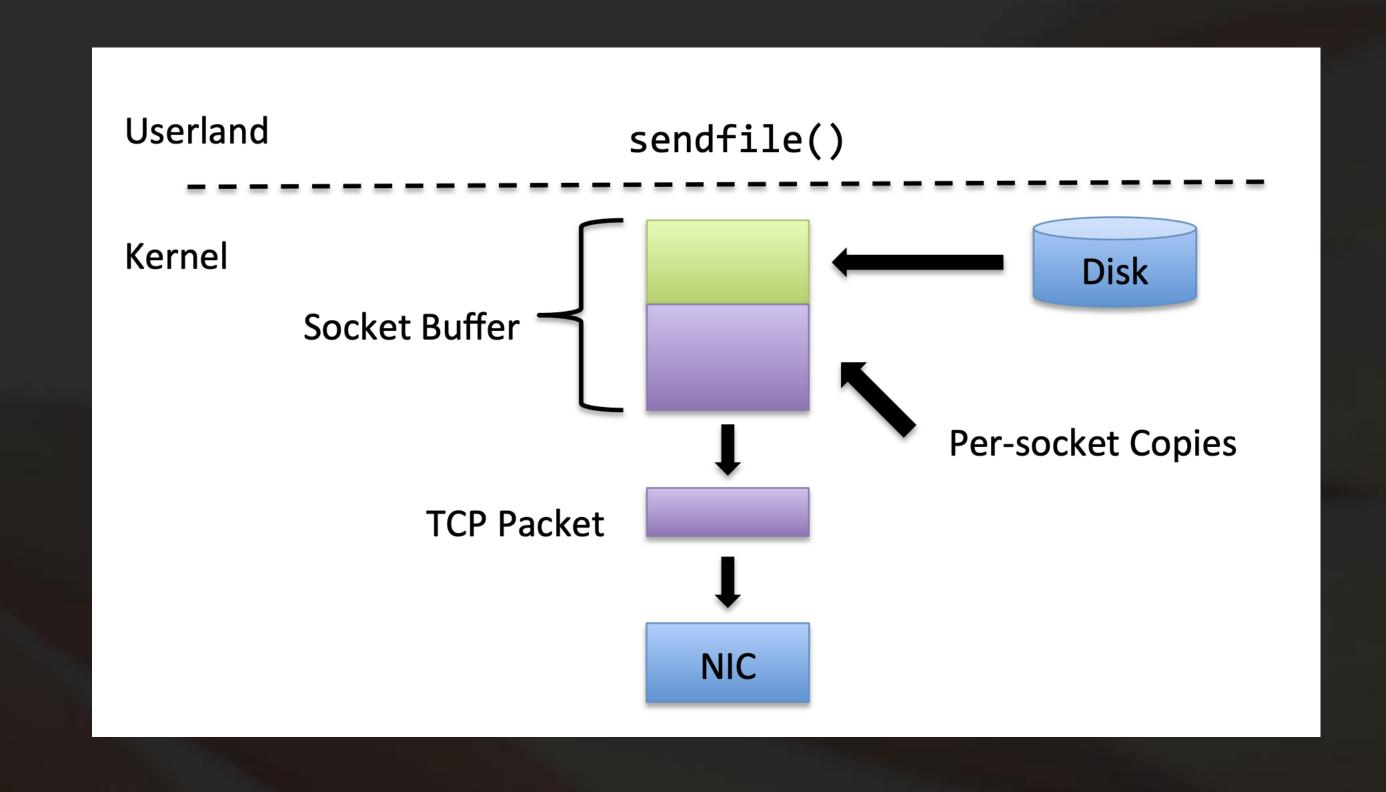
商用应用场景 - HTTPS (RFC8998 TLS 1.3 + 商密套件)

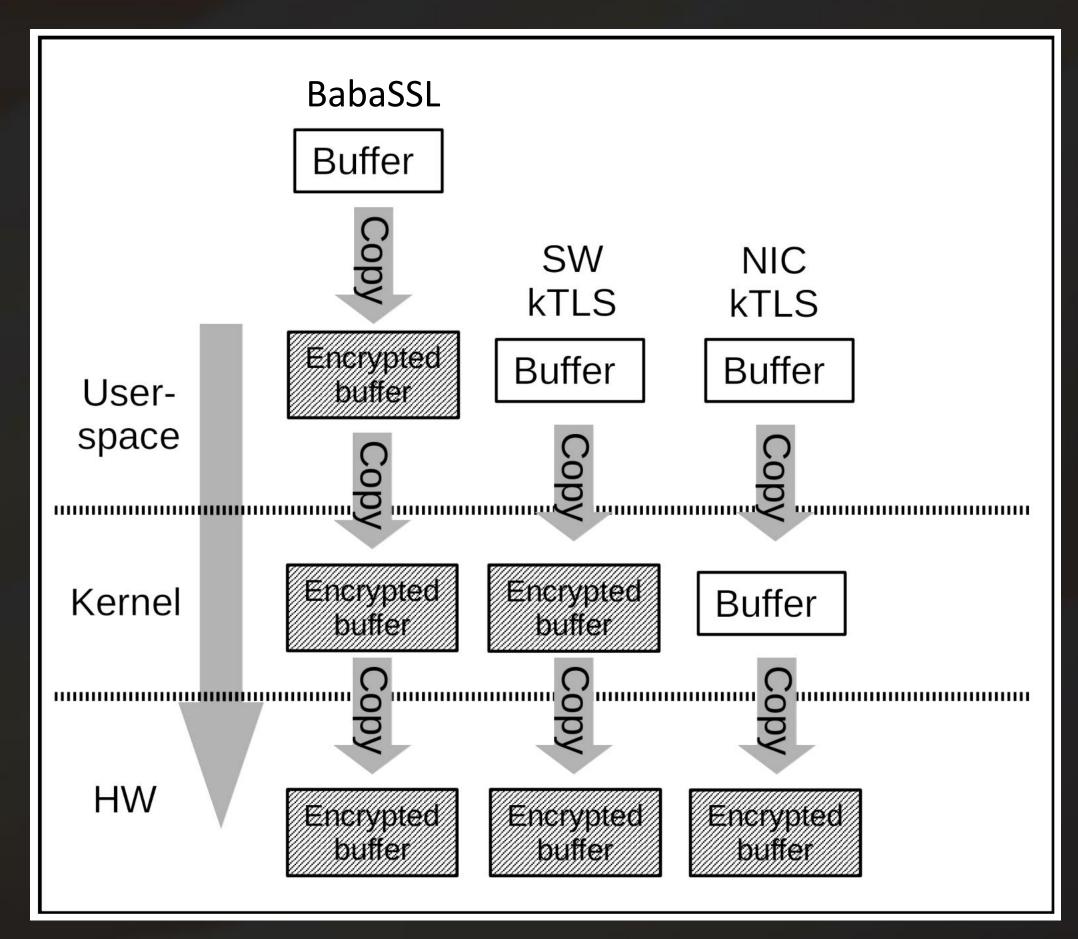
```
Transport Layer Security
TLSv1.3 Record Layer: Handshake Protocol: Server Hello
     Content Type: Handshake (22)
     Version: TLS 1.2 (0x0303)
     Length: 155

→ Handshake Protocol: Server Hello
       Handshake Type: Server Hello (2)
       Length: 151
       Version: TLS 1.2 (0x0303)
       Random: b684cb5bcbfb60a1778ae611f1d9a4548f8ccdb73c29400f8ab1ddf36048ca91
       Session ID Length: 32
       Session ID: 9ff00a72a24e6d52cf9934080ff2b9752a5cfdec1f45939d017bb96e26ac3477
       Cipher Suite: TLS_SM4_GCM_SM3 (0x00c6)
       Compression Method: null (0)
       Extensions Length: 79
     Extension: supported_versions (len=2)
          Type: supported_versions (43)
          Length: 2
          Supported Version: TLS 1.3 (0x0304)
     v Extension: key_share (len=69)
          Type: key_share (51)
                                                    SM2
          Length: 69
        Key Share extension
          V Key Share Entry: Group: Unknown (41), Key Exchange length: 65
               Group: Unknown (41)
               Key Exchange Length: 65
               Key Exchange: 0445561d23e04fa9ca96679d60c2366b4b593bc6c44f4594f62608df6ce39d2483fd5bd1...
```



商用应用场景 - HTTPS (Kernel TLS)







商密应用场景 - IMA和modsign商密化





Anolis商密软件栈SIG

基于Anolis OS发行版构建商密基础设施及解决方案生态 致力于为行业提供基于商密的信息安全标准

SIG开发运作相关链接
SIG地址

https://openanolis.cn/sig/crypto

代码库

https://codeup.openanolis.cn/codeup/crypto





致谢

张天佳: tianjia.zhang@linux.alibaba.com