SGX security background

Monday, April 10, 2017 4:10 PM

3个基本概念

Confidentiality	消息不会被其他人读取	通过加密来保证	AES-GCM, AES-CTR	RSA with PKCS #1 v2.0
Integrity	消息的完整性不会被破坏，或者被破坏后能意识到被攻击了	MAC/signature	HMAC-SHA-2 AES-GCM	DSS-RSA, DSS-ECC
freshness	在integrity的基础上，接收者总是能收到最新的消息，或者能意识到攻击。	Nonces+integrity		

每个加密原语都需要通过一个随机数来生成独一无二的key，而随机数的生成是通过（CSPRNG）来做到的，他的值不应该被预测到。

Confidentiality
对称加密：双方使用同样的key加密和解密，因此key的分发必须能够保证confidentiality 和integrity
非对称加密：使用public key进行加密，private key进行解密。Public key的分发不用保证confidentiality，只需要有integrity。

对称加密中比较有名的有AES，将一个128bit的block转换为另一个128bit的block，最近要求使用256 bit长的key。
非对称加密的RSA.通常非对称加密算法比对称加密算法需要的计算量要大得多，因此通常发送者先用非对称加密的公钥加密一个一次使用的key发送给接收者。如下图所示：

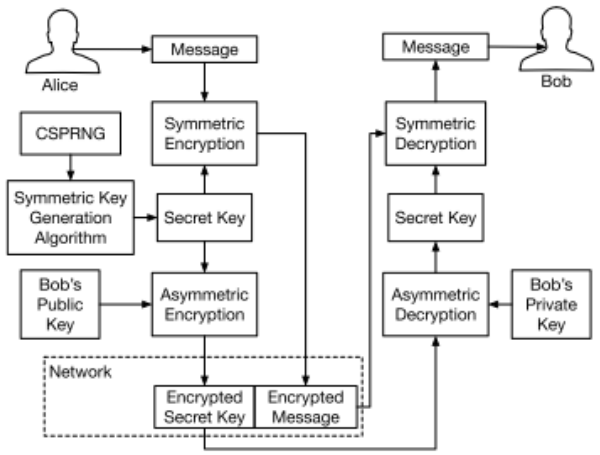
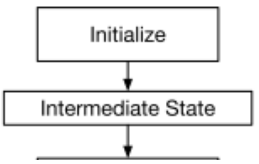


Figure 40: Asymmetric key encryption is generally used to bootstrap a symmetric key encryption scheme.

Integrity
通过 secure hashing functions提供。SHA-2 256 bits
Sha-2 将message 分为block，通过不停的extend block到中间状态，最后得出最终状态。其中，message block 和中间状态的长度是不变的。如下图：



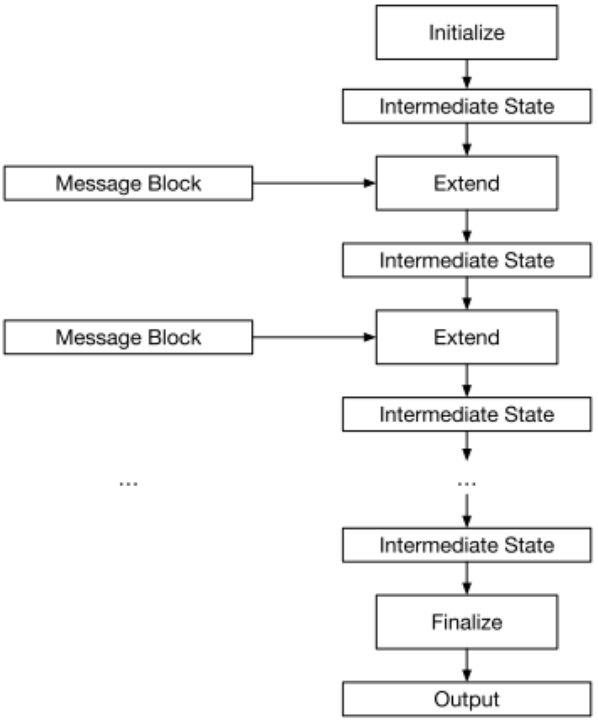
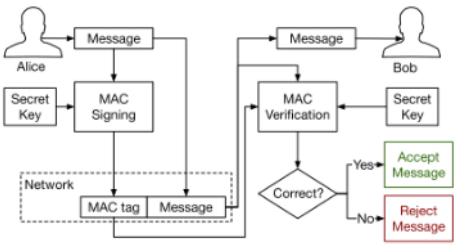


Figure 41: A block hash function operates on fixed-size message blocks and uses a fixed-size internal state.



在对称加密算法中，Message Authenitication code （ MAC ）用来保证integrity。
通常MAC没有特殊的算法，直接使用对应的对称加密算法来解密MAC
HMAC（Hash MAC)可以使用任何secure hash算法来生成MAC。

非对称密钥的原语可以提供个integrity保证是signatures 。sender用自己的私钥进行签名算法。

Freshness

CA 机制

Key agreement protocols