SDCC
中国软件开发者大会
SOFTWARE DEVELOPER CONFERENCE CHINA

从SSL协议谈起

- 加密是安全的基石

- 信息明文传输的风险
  - 窃听风险：第三方可以获知通信内容
  - 篡改风险：第三方可以修改通信内容
  - 冒充风险：第三方可以冒充他人身份参与通信

潜在攻击方式

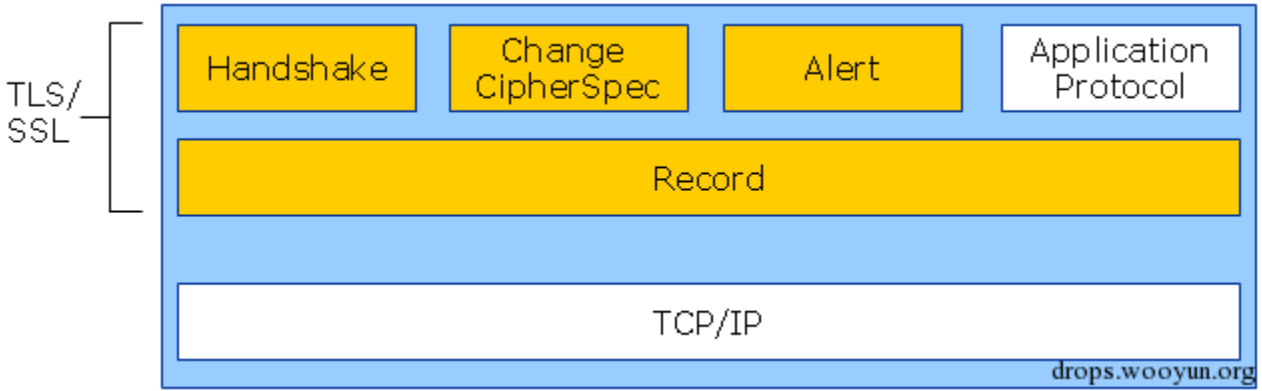
- 网络攻击方式
  - Arp欺骗
  - 路由器
  - DNS
  - BGP
  - 。。。

- 目标
  - 如何在不可信的网络环境中传输数据
- 解决明文传输的风险
  - 所有信息都是加密传播，第三方无法窃听
  - 具有校验机制，一旦被篡改，通信双方会立刻发现
  - 配备身份证书，防止身份被冒充
- 历史
- 最新版本 SSL3.3/TLS1.2

SSL应用范围

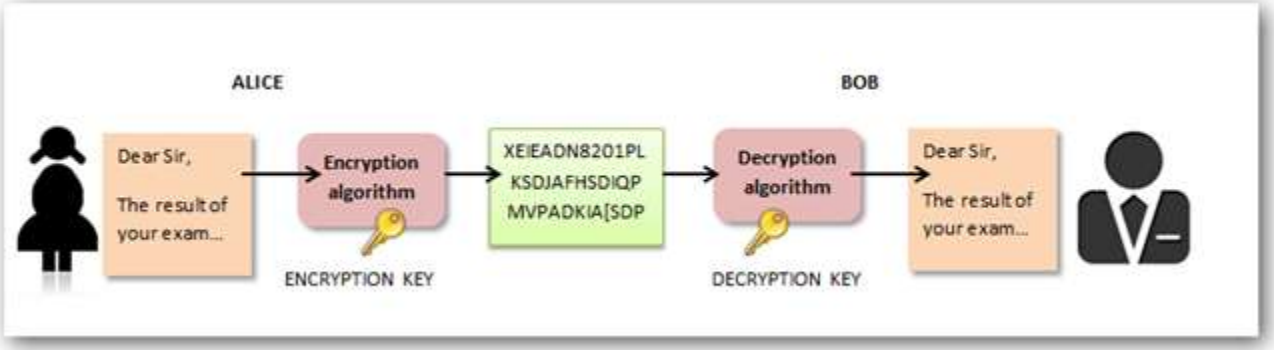
- 针对传输层的加密
- 可以应用到的应用层协议
  - http
  - ftp
  - smtp
  - 。。。

- 网络层级


TLS/
SSL
Handshake
Change
CipherSpec
Alert
Application
Protocol
Record
TCP/IP
drops.wooyun.org

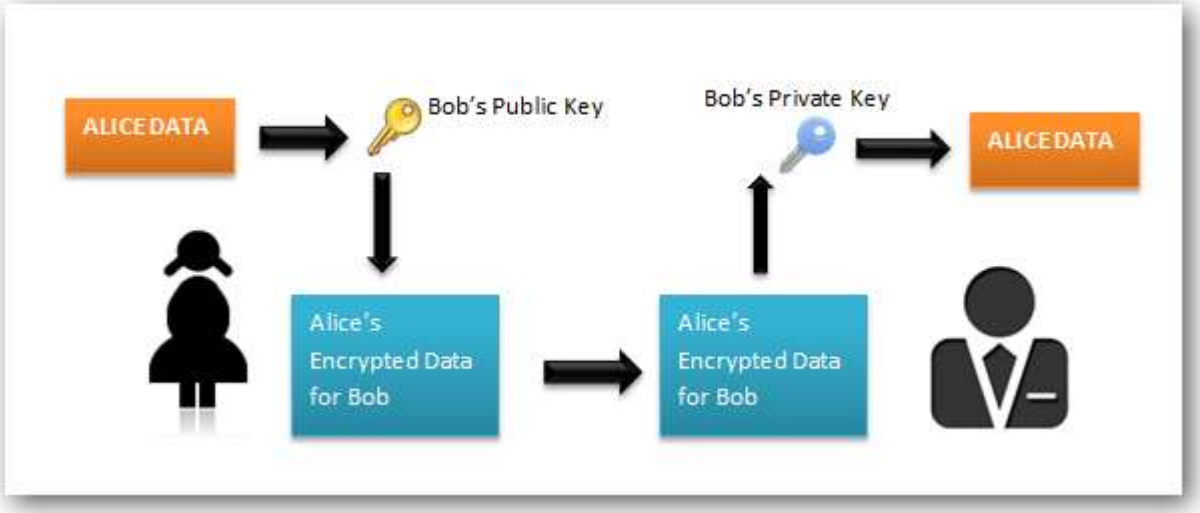
- SSL协议分为握手阶段和应用阶段
  - 握手阶段也称协商阶段，在这一阶段，客户端和服务器端会认证对方身份(依赖于PKI体系，利用数字证书进行身份认证)，并协商通信中使用的安全参数、密码套件以及MasterSecret。后续通信使用的所有密钥都是通过MasterSecret生成
  - 在握手阶段完成后，进入应用阶段。在应用阶段通信双方使用握手阶段协商好的密钥进行安全通信

- 对称加密


ALICE
BOB
Dear Sir,
The result of your exam...
Encryption algorithm
ENCRYPTION KEY
XEIEADN8201PL
KSDJAFHSDIQP
MVPADKIA[SDP
Decryption algorithm
DECRYPTION KEY
Dear Sir,
The result of your exam...

- 起源
  - Xor
- DES
- AES

- 非对称加密



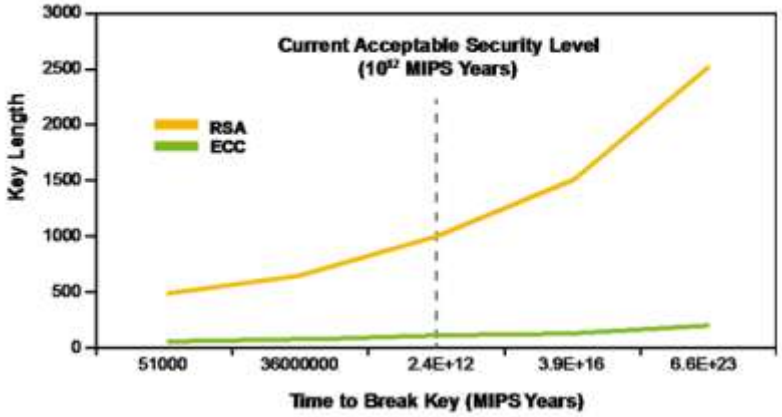
- 解决了密钥保存和交换的难题

非对称加密算法

- RSA
  - 给定两个质数p、q 很容易相乘得到n，对n进行因式分解却相对困难
- ECC-椭圆曲线
  - K=kG 给定K和G，很难求k

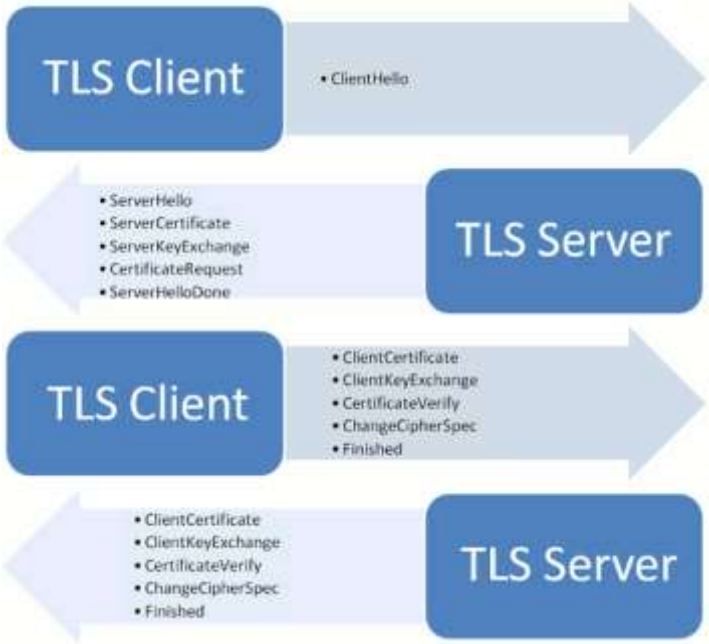
- 破解ECC和RSA所需的计算量对比
  - http://www.atmel.com/ <RSA vs ECC Comparison for Embedded Systems>

Figure 1. RSA and ECC Performance (Source: RSA)[8]



This chart presents another way to look at the performance of RSA and ECC. It compares what key lengths of each algorithm will provide a level of security measured in the time in MIPS-years to break the security. It is clear that ECC is more efficient.

- 图解


TLS Client
• ClientHello
• ServerHello
• ServerCertificate
• ServerKeyExchange
• CertificateRequest
• ServerHelloDone
TLS Server
TLS Client
• ClientCertificate
• ClientKeyExchange
• CertificateVerify
• ChangeCipherSpec
• Finished
• ClientCertificate
• ClientKeyExchange
• CertificateVerify
• ChangeCipherSpec
• Finished
TLS Server

- 图解


Hello! Let's start a encrypted conversation using TLS 1.2.
I want to talk to bank.com
I know the following cipher suites:
- ECDHE and RSA with 128bit AES in GCM mode and SHA256
- RSA with 128bit AES in GCM mode and SHA256
Here's a randomly chosen number:
3d86a5..04
Hi there, I think we can chat.
Let's use the cipher:
RSA with 128bit AES in GCM mode and SHA256
Here's my random number:
ca35f0..13
Here's my certificate chain:
[bank.com's certificate]
This certificate checks out: it was issued to bank.com and digitally signed by a certificate authority I trust.
Here's a secret encrypted with the RSA public key I took from your certificate:
[encrypted pre-master secret]
We can both derive the same key using this secret and the random numbers we exchanged.
I have decrypted the secret and derived the key.
From now on let's use the key to encrypt what we say.
[It's so great to speak privately]
[Can you get me the current balance of my checking account?]
[Sure thing, you have $12.05 left in that account]

- 会话密钥源于三个随机数
  - ClientHello
  - ServerHello
  - Pre-master key

- 完成了对SSL的了解
- 对于智能设备从中可以得到哪些启示

- 非对称加密
- 密钥的选择

- 使用场景
  - 通信
  - 固件校验

- 非固定
- 非可预测

- http://drops.wooyun.org/tips/10450

网络拓扑

- 和其他在线服务的对比
  - 用户对象数量可控

- 开启通信协议提供的加密方式
  - Wi-Fi
  - 蓝牙
  - ZigBee
- 对于密钥的选取
  - 不可预测性

- 不可信的不只是通信环境
- 可以被逆向的对象
  - 移动控制App
  - 智能设备本身
- 实时的选择非对称加密

- 认证是安全的另一块基石
  - 验证用户或设备是否是声称的身份
  - 结果只有两种，符合或者不符合
- ACL
  - 多用户，不同控制等级的需求

- 认证
  - 需前置，有足够的覆盖度
  - 与后续控制的关联性
  - 时效性

- 去控制中心化的设计
  - 内网穿透？
  - 将云端服务器看成一个传输节点，而非控制节点

- 将认证推至接近设备端
  - 云端决定是否可以建立转发通道
  - 具体控制由近设备端决定

- 覆盖度不足
- 某路由器配置文件下载漏洞
  - http://www.wooyun.org/bugs/wooyun-2010-0110062

1.漏洞1，任意下载config.bin[路由器配置文件] 例如：http://192.168.1.1/config.bin

2.openssl enc -d -des-ecb -nopad -K 478DA50BF9E3D2CF -in config.bin

提取配置信息。

3.找到首行

code 区域

```
authKey 0rZily4W9TefbwK
```

此为加密过的用户后台登陆密码。

- 认证信息可预测
- http://drops.wooyun.org/tips/10109

SDCC
中国软件开发者大会
SOFTWARE DEVELOPER CONFERENCE CHINA

sdcc.csdn.net