



GoSSIP Summer School, 2017. 7. 12

软件中密码系统的安全测评

刘慧

密码与计算机安全实验室 (LoCCS)



Outline



- 密码与密码测评
- 身份鉴别
- 安全通信

JOSS'19

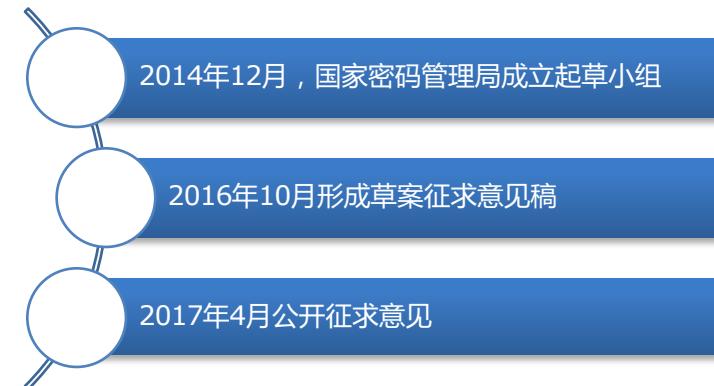
密码与密码测评



国家对于密码的管理上升到立法的高度

2017年4月13日，国家商用密码管理办公室发布《中华人民共和国密码法（草案征求意见稿）》公开征求意见的通知

- 密码领域综合性、基础性的法律
- 网络与信息安全是国家安全的重要组成部分
- 密码是保障网络与信息安全的核心技术和基础支撑
- 密码工作直接关系国家政治安全、经济安全、国防安全和信息安全，直接关系公民、法人和其他组织的切身利益。



第十二条 关键信息基础设施应当依照法律、法规的规定和密码相关国家标准的强制性要求使用密码进行保护，同步规划、同步建设、同步运行密码保障系统。

第十八条 国家对关键信息基础设施的密码应用安全性进行分类分级评估，按照国家安全审查的要求对影响或者可能影响国家安全的密码产品、密码相关服务和密码保障系统进行安全审查。

密码与密码测评



国家对于密码的管理上升到立法的高度

本法所称密码，是指使用特定变换对数据等信息进行**加密保护**或者**安全认证**的物项和技术

密码分类保护要求

- **核心密码、普通密码**可以用于保护国家秘密信息，**商用密码**用于保护不属于国家秘密的信息

密码应用

- 强调国家积极规范和促进密码应用
 - 充分发挥密码在网络空间中**身份识别、安全隔离、信息加密、完整性保护和抗抵赖性**等方面的重要作用
- 规定了关键信息基础设施密码使用要求
- 规定了商用密码产品、服务管理制度 - 规定了电子政务电子认证服务管理制度

密码检测认证管理制度

第十七条 国家推进密码检测认证体系建设，制定**密码检测、**
认证规则。密码检测、认证机构应当依法取得相关资质，并依照
法律、法规的规定和密码检测、认证规则开展密码检测、认证。

密码与密码测评



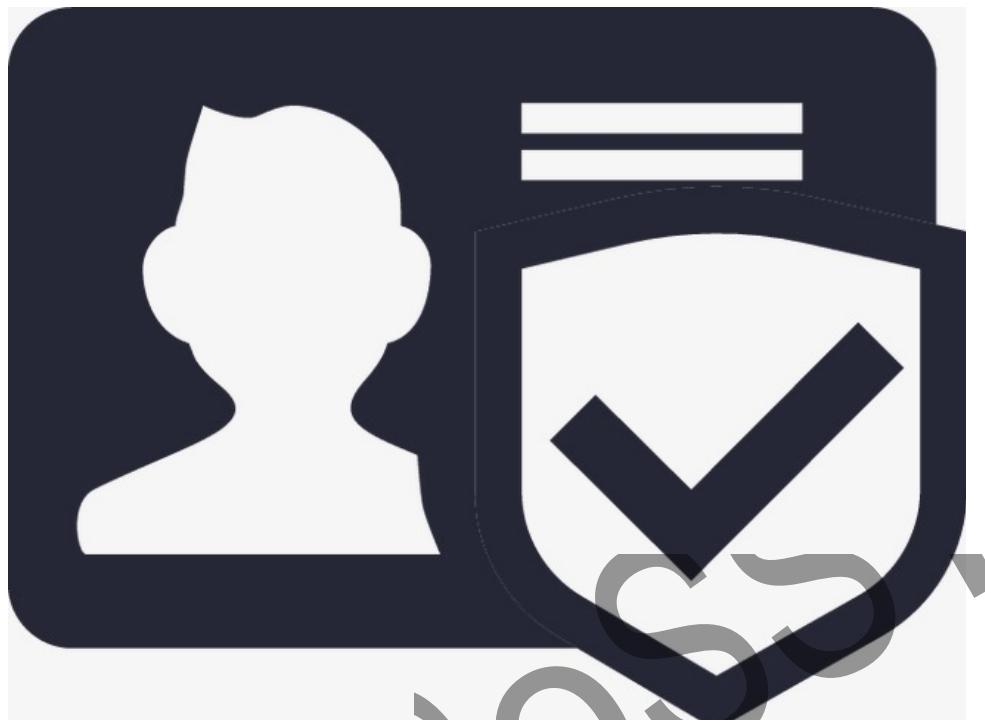
商用密码技术实施要求

2009年3月，国家密码管理局发布《信息安全等级保护商用密码技术实施要求》

2015年9月，国家密码管理局发布《信息安全等级保护商用密码测评机构审批服务指南》

测评标准《信息系统密码应用基本要求（草稿）》正在进行中





jos

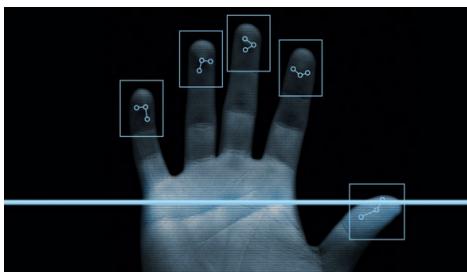
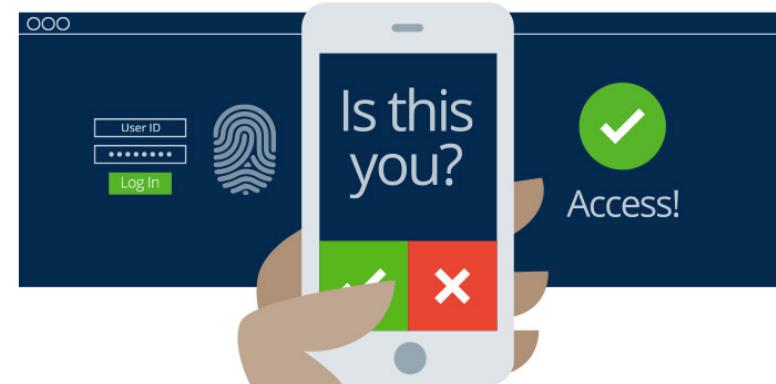
身份鉴别

身份鉴别



从安全测评角度来看，身份鉴别的安全要求反映在以下指标

- 提供单一、两种或两种以上的身份鉴别方式
- 身份鉴别信息具备不易被冒用的防范能力
- 身份鉴别信息具备不可伪造性



身份鉴别



身份鉴别测评的关键——基于密码的身份认证

- 认证消息的抗重放、抗泄露

安全建议：

- 使用安全传输协议（如SSL）
- 若将密码作为后续通信的双方预共享秘密信息（密钥材料），那么使用pbkdf对密码进行处理

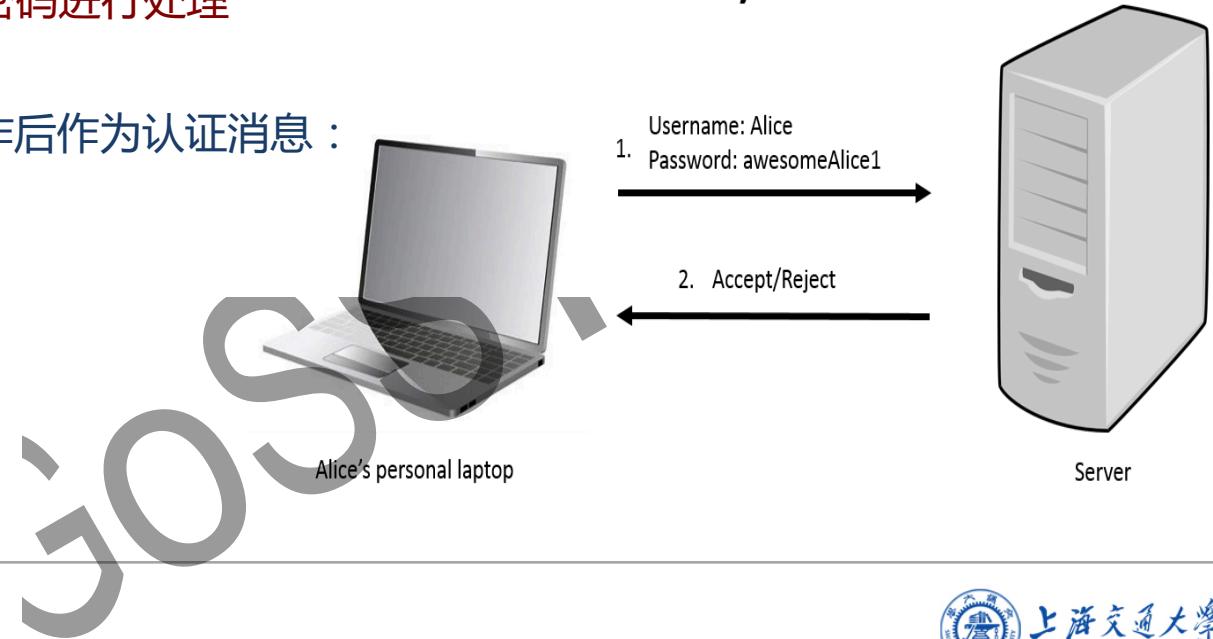
绝对避免对密码做以操作后作为认证消息：

- None
- 哈希/带盐哈希
- 对称加密算法加密

密码认证协议(PAP)

Password Authentication Protocol

PAP two-way handshake



身份鉴别

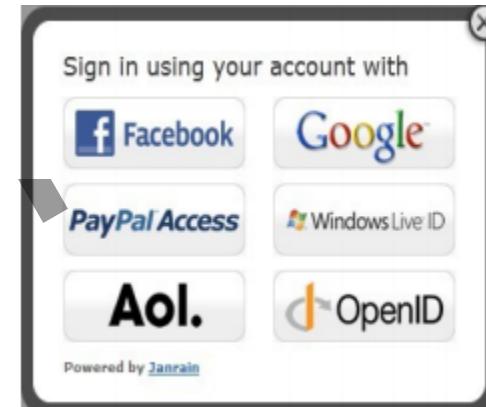


基于第三方的身份鉴别——多方认证协议

- 多方认证协议是帮助一个应用利用第三方应用的认证系统认证用户的一种安全协议

协议分为两个阶段：

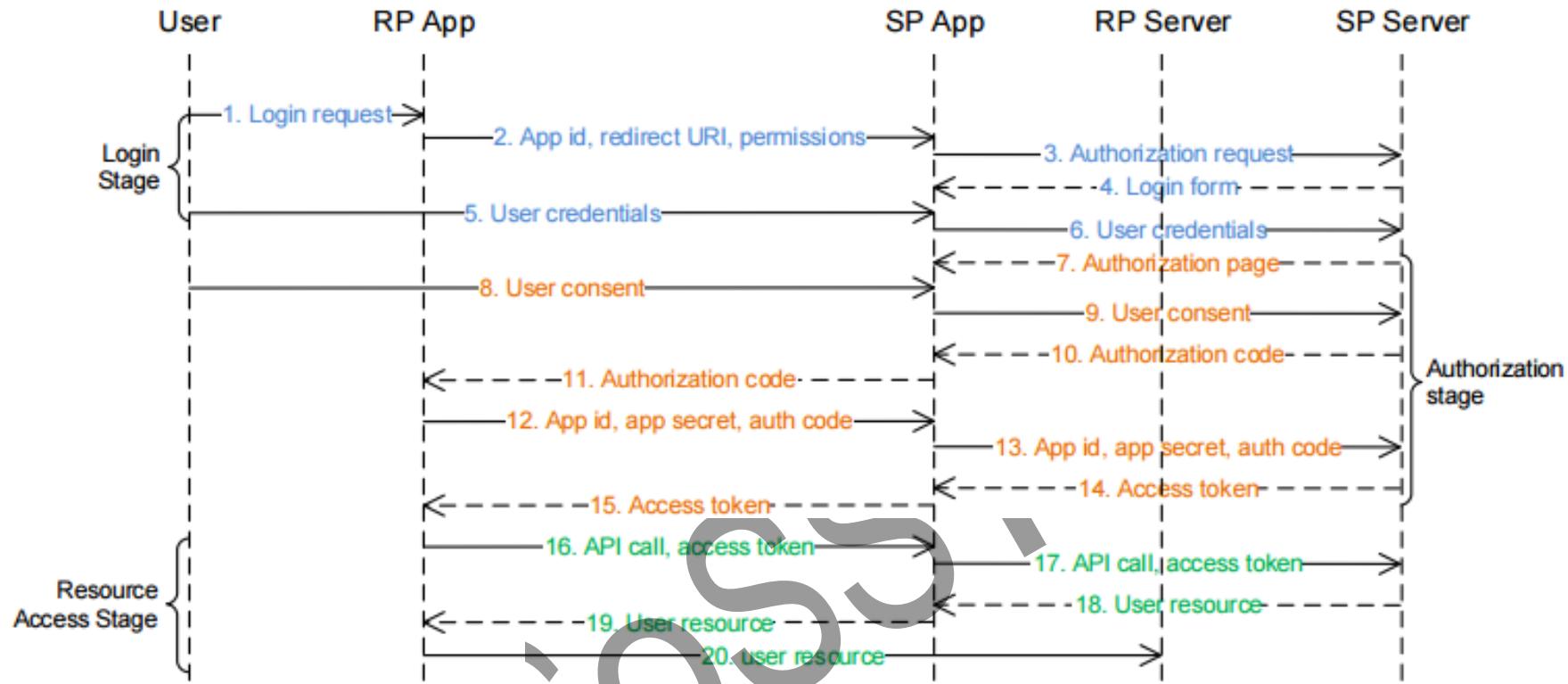
- 当前应用请求用户授权，允许它访问用户在第三方应用中存储的数据。
- 获得授权后，凭借访问令牌请求用户在第三方应用的身份信息认证用户。



身份鉴别



基于第三方的身份鉴别——多方认证协议



身份鉴别



基于第三方的身份鉴别——多方认证协议

- 错误的实现可导致第三方身份鉴别的机制失效

在Google的实现中，应用向Google的服务器请求
email , name , phone等信息以及它们的签名：

- 需要签名的参数的list可写，即可以被攻击者篡改
- 很多网站依赖email来认证用户的身份



```
BRM1:src=RP dst=http://IdP/accounts/o8/ud↓  
Arguments:  
openid.ns [WORD] ↓ & openid.claimed_id [UU] ↓ &  
openid.identity [UU] ↓ &  
openid.return_to [URL] {RP/b/openid} ↓ &  
openid.realm [URL] {RP/b/openid} ↓ &  
openid.assoc_handle [BLOB] ↓ &  
openid.openid.ns.ext1 [WORD] ↓ &  
openid.ext1.type.email [WORD] ↓ &  
openid.ext1.type.firstname [WORD] ↓ &  
openid.ext1.type.lastname [WORD] ↓ &  
openid.ext1.required [LIST] ↓  
    (email,firstname,lastname)  
  
BRM2:src=IdP↓ dst=http://IdP/openid2/auth  
Arguments: st [MU] [SEC] ↓  
  
BRM3: src=!IdP dst=https://RP/b/openid↓  
Arguments:  
openid.ns [WORD] ↓ & openid.mode [WORD] &  
openid.response_nonce [SEC] &  
openid.return_to [URL] ↓ &  
openid.assoc_handle [BLOB] ↓ &  
openid.identity [UU] & openid.claimed_id [UU] &  
openid.sig [SIG] &  
openid.signed [LIST] ↓ &  
openid.opEndpoint [URL] {IdP/accounts/o8/ud} ↓ &  
openid.ext1.type.firstname [WORD] ↓ &  
openid.ext1.value.firstname [UU] &  
openid.ext1.type.email [WORD] ↓ &  
openid.ext1.value.email [UU] &  
openid.ext1.type.lastname [WORD] ↓ &  
openid.ext1.value.lastname [UU]  
protected by  
openid.sig
```

Figure 8: GoogleID+Smartsheet trace for scenario (A)

身份鉴别



身份鉴别在特殊场景下的困难

- 对于物联网设备，因设备本身能力受限，导致身份认证安全性的削弱甚至缺失
- 手机与设备的通信协议：BLE (Bluetooth Low Energy) 低功耗蓝牙
 - 受限于BLE设备的能力（功耗低、没有输入输出设备等）
BLE协议本身所提供的安全性往往不能满足身份认证的需要



配对模式：

- Just Works
- Passkey Entry
- OOB (Out Of Band)

BLE协议的基本信息



低功耗蓝牙设备的身份认证

□ BLE协议的工作过程

- 运行在2402MHz-2480MHz
- 2MHz spacing, 40个信道（其中37，38，39为广播信道）

- 通信范围小于100m

```
Advertising Address: AmiccomE_48:34:ed (18:7a:93:48:34:ed)
▽ Advertising Data
  ▷ Flags
  ▷ 16-bit Service Class UUIDs
  ▽ Device Name: 187A934834ED
    Length: 13
    Type: Device Name (0x09)
    Device Name: 187A934834ED
```

□ 广播-连接-配对

- 广播：

- ADV_IND、ADV_DIRECT_IND、ADV_NONCONN_IND、AND_SCAN_IND

- SCAN_REQ、SCAN REP

- 连接：

- CONN_REQ

```
Access Address: 0x8e89bed6
▷ Packet Header: 0x2245 (PDU Type: CONNECT_REQ, TxAdd=false, RxAdd=false)
Initiator Address: 43:e7:93:95:a7:5f (43:e7:93:95:a7:5f)
Advertising Address: AmiccomE_48:34:eb (18:7a:93:48:34:eb)
▽ Link Layer Data
  Access Address: 0xaf9a8caf
  CRC Init: 0x59ef79
  Window Size: 3
```

BLE协议的基本信息



低功耗蓝牙设备的身份认证

□ 配对

- 交换配对信息 : IO Capability , MITM flag

□ 认证链接

- BLE特有的密钥交换算法

TK (Temporary Key)



STK = AES128 (TK,
Srand || Mrand)

STK (Short Term Key)



LTK (Long Term Key)

- 分发密钥

Opcode: Pairing Request (0x01)
IO Capability: Keyboard, Display (0x04)
OOB Data Flags: OOB Auth. Data Not Present (0x00)
▼ AuthReqBonding, MITM
..... .01 = Bonding Flags: Bonding (0x1)
..... .1.. = MITM Flag: 1
Max Encryption Key Size: 16
► Initiator Key DistributionLTK IRK CSRK
► Responder Key DistributionLTK IRK CSRK

Opcode: Pairing Response (0x02)
IO Capability: No Input, No Output (0x03)
OOB Data Flags: OOB Auth. Data Not Present (0x00)
▼ AuthReqBonding, No MITM
..... .01 = Bonding Flags: Bonding (0x1)
..... .0.. = MITM Flag: 0
Max Encryption Key Size: 16
► Initiator Key DistributionCSRK
► Responder Key DistributionLTK

配对模式 :

- Just Works : 000000
- Passkey Entry : 6位数字
- OOB (Out Of Band) : 128bit

BLE配对过程

低功耗蓝牙设备的身份认证



Pairing Method	Temporary Key (TK)	MITM Protection	Notes
Just Works	0 (zero)	NO	<ul style="list-style-type: none">No authentication
Passkey Entry	0 ... 999999 (six decimal digits) The rest of the key is padded with zeroes.	YES	<ul style="list-style-type: none">AuthenticatedInterface allows displaying or entering values
Out Of Band	Usually a full 128 bit key.	YES	<ul style="list-style-type: none">Authenticated

JOSS

BLE配对过程

低功耗蓝牙设备的身份认证



		Initiator			
		OOB Set	OOB Not Set	MITM Set	MITM Not Set
Responder	OOB Set	Use OOB	Check MITM		
	OOB Not Set	Check MITM	Check MITM		
	MITM Set			Use IO Capabilities	Use IO Capabilities
	MITM Not Set			Use IO Capabilities	Use Just Works

gossy

Take Home



低功耗蓝牙设备的身份认证

- 受限于BLE设备的能力（功耗低、没有输入输出设备等），BLE协议本身所提供的安全性往往不能满足身份认证的需要

- 不配对，连接后直接通信
- 在BLE协议之上添加简单的机制

- “Token不算智能，必须双向通信才算”





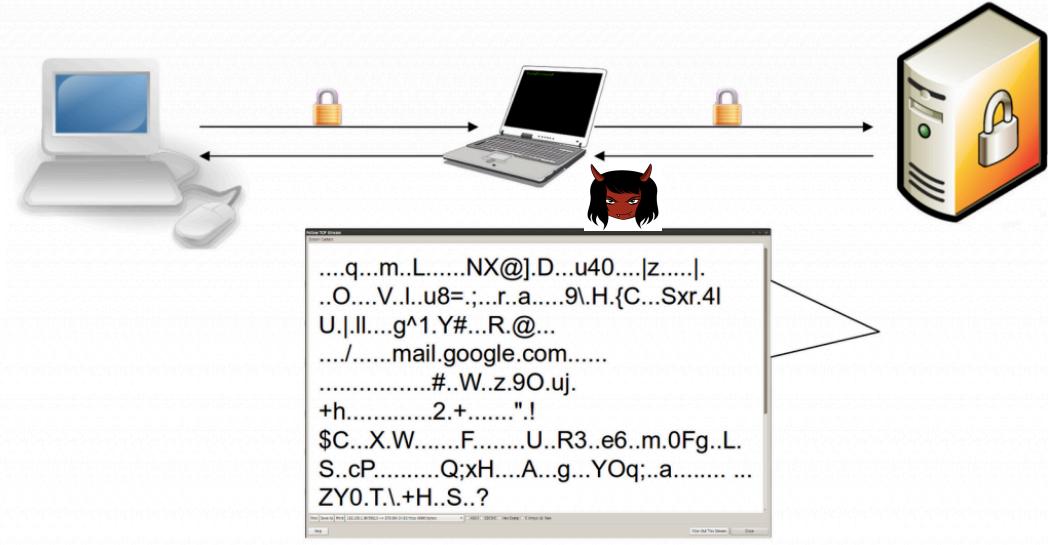
3GSS、
安全通信

安全通信

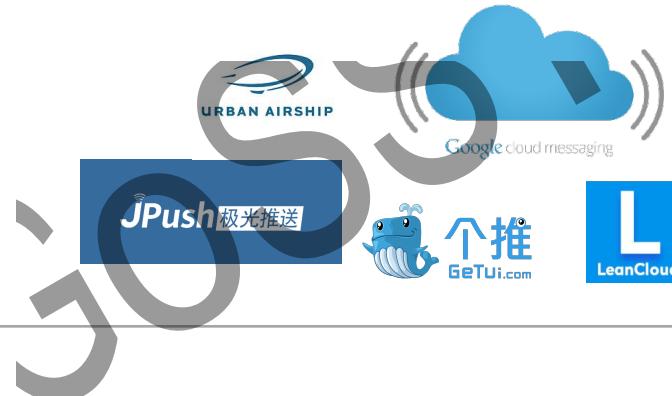
使用安全协议为网络通信数据传输提供**机密性和完整性**



✓ SSL/TLS 协议



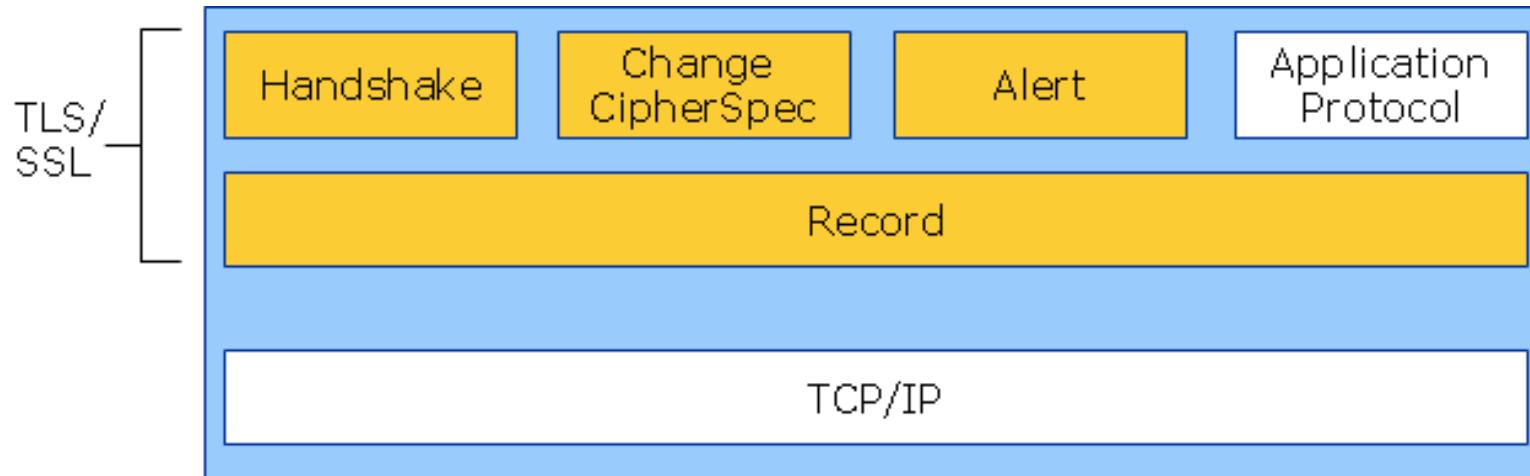
✓ 私有通信协议



SSL协议简介

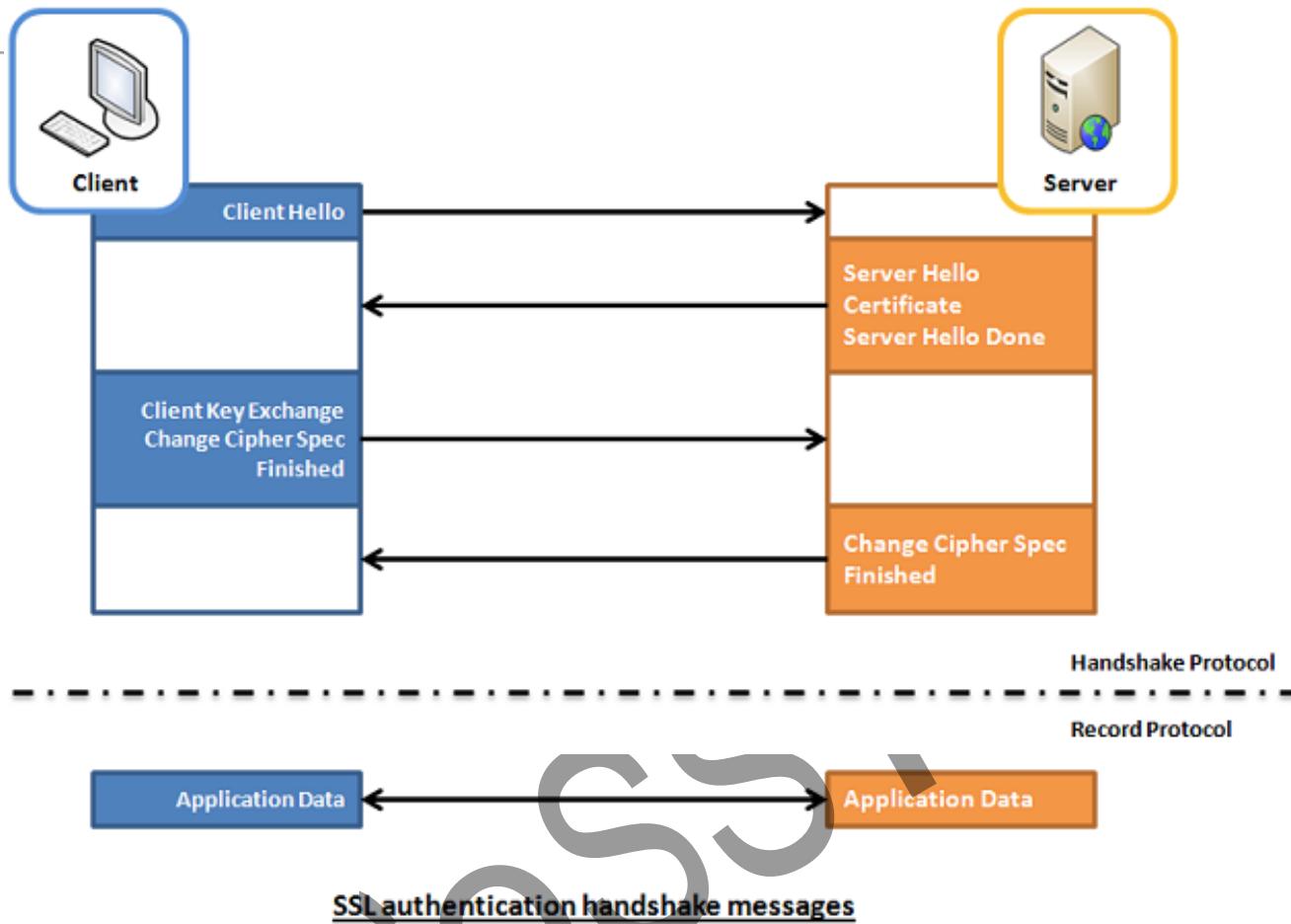


SSL协议包含握手、交换密码规范、警告和记录层四个子协议



- Handshake : 协商安全参数和密码套件、身份认证、密钥交换
- ChangeCipherSpec : 一条消息，表明握手已完成
- Alert : 对握手协议中一些异常的错误提醒，Fatal和Warning
- Record : 包括对消息的分段、压缩、消息认证和完整性保护、加密等

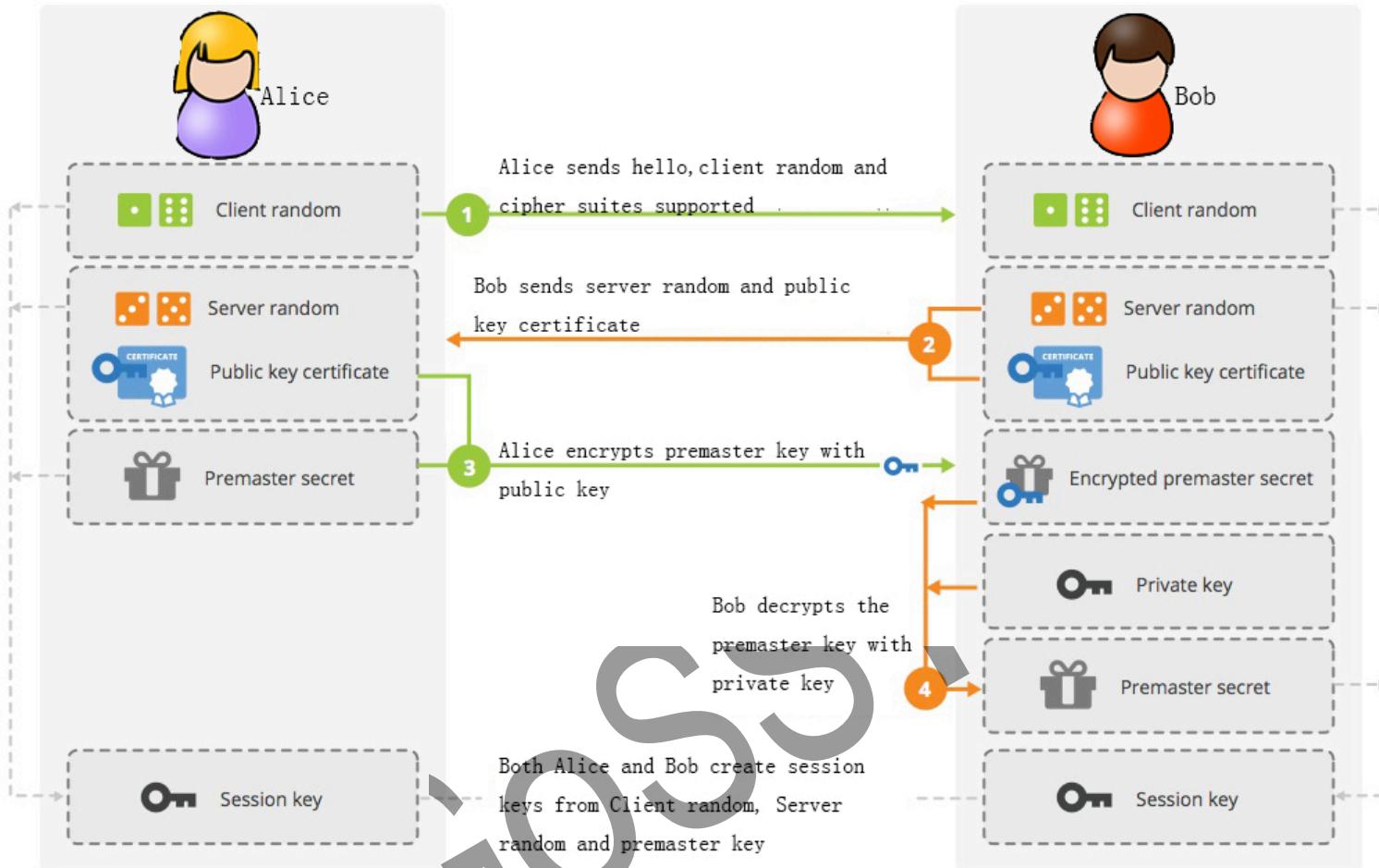
SSL协议简介



SSL协议简介



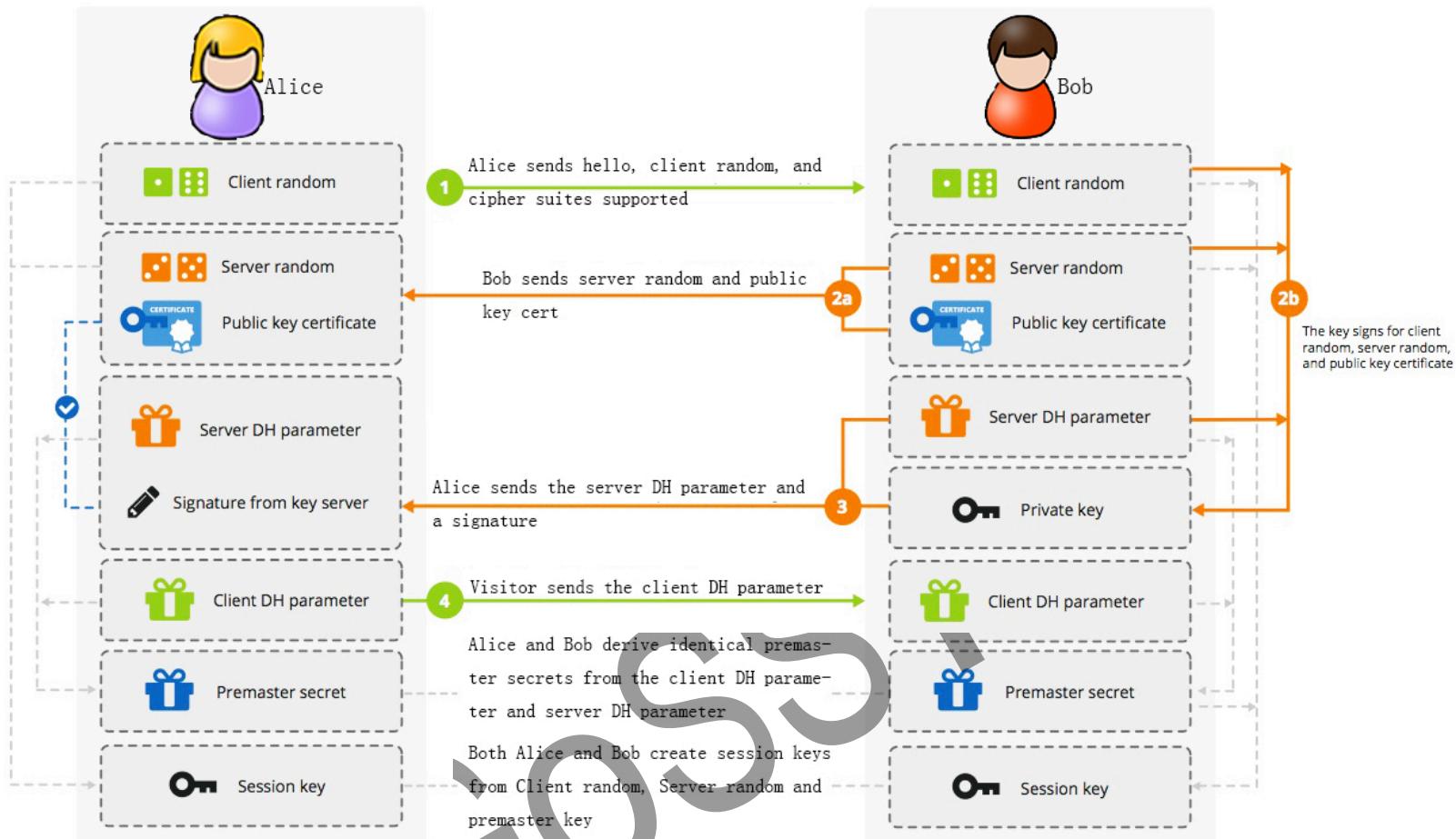
基于RSA的密钥交换



SSL协议简介

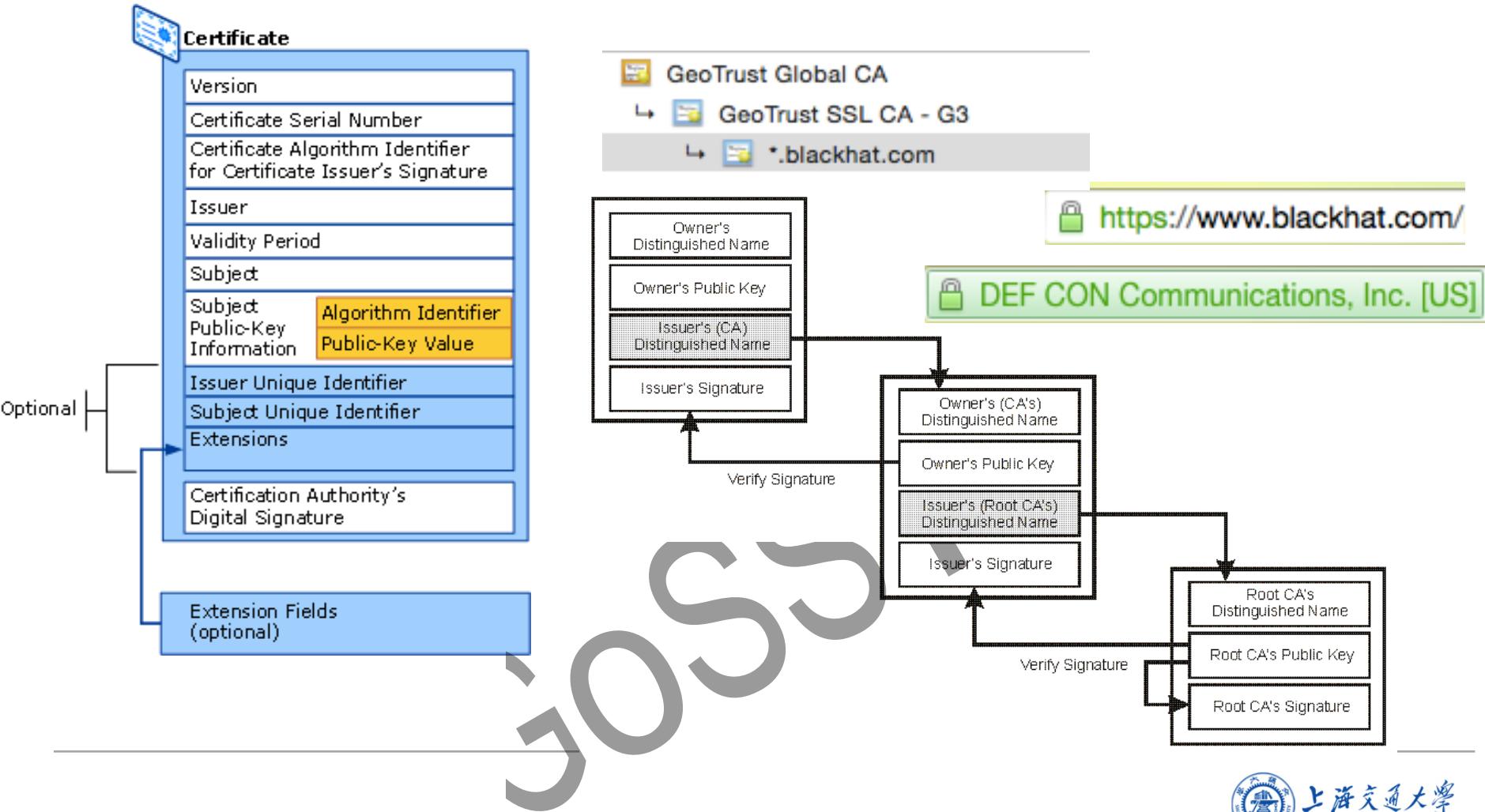


基于Diffie-Hellman的密钥交换



SSL协议简介

X509 PKI体制



SSL安全问题

参见2015暑期学校《SSL安全之路》



SSL协议CBC加密模式的安全问题

Padding Oracle, Beast, Crime, Lucky Thirteen, Poodle Attack

SSL协议降级攻击

Freak, Logjam

弱PRNG带来的安全问题

Linux, OpenWRT, Debian

SSL协议CA/B模型下的安全问题

Certificate Validation, Security Indication

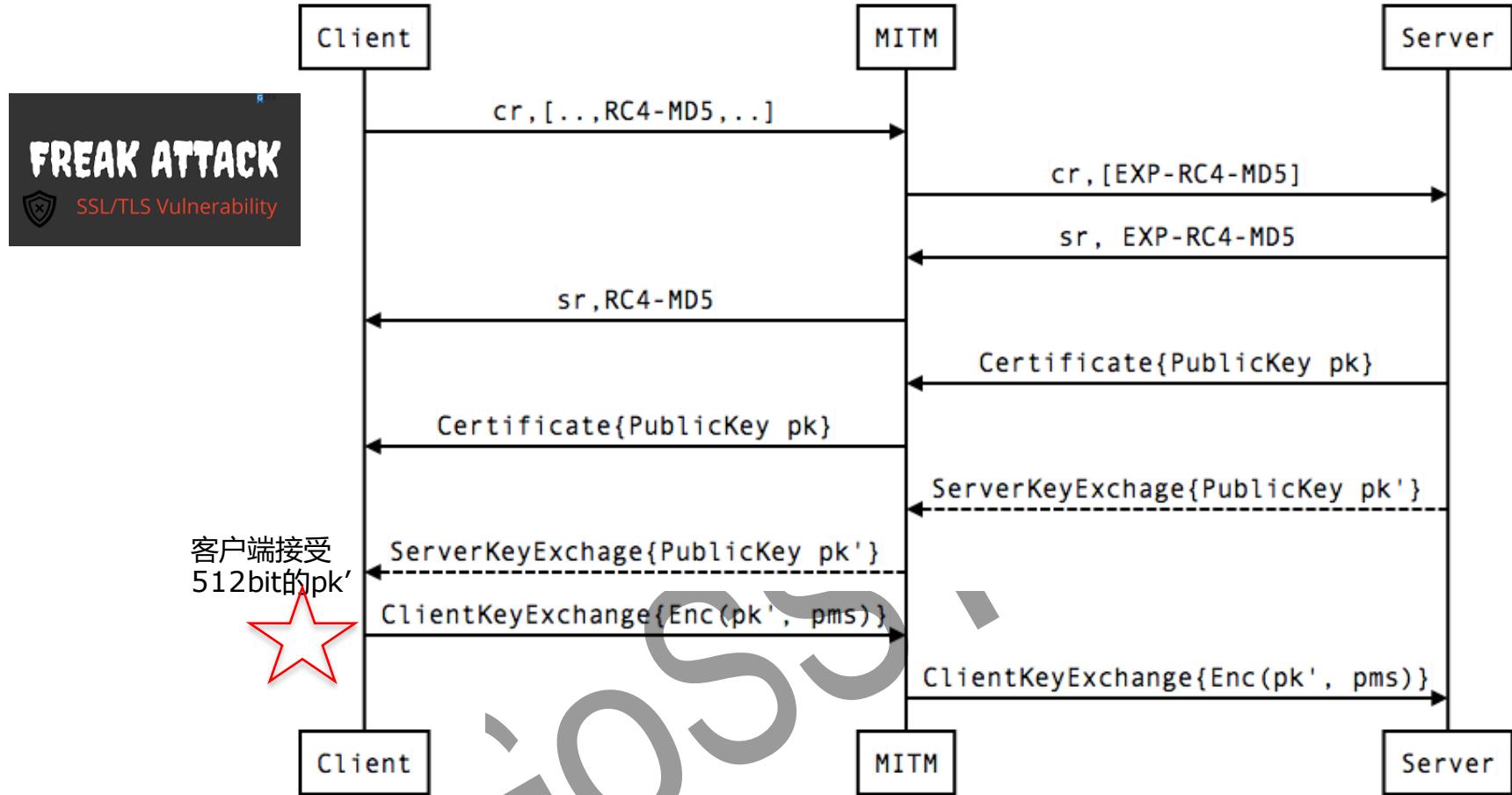
移动平台中SSL的安全问题

Android Truststore, Apple Goto Fail

SSL

SSL安全

中间人攻击



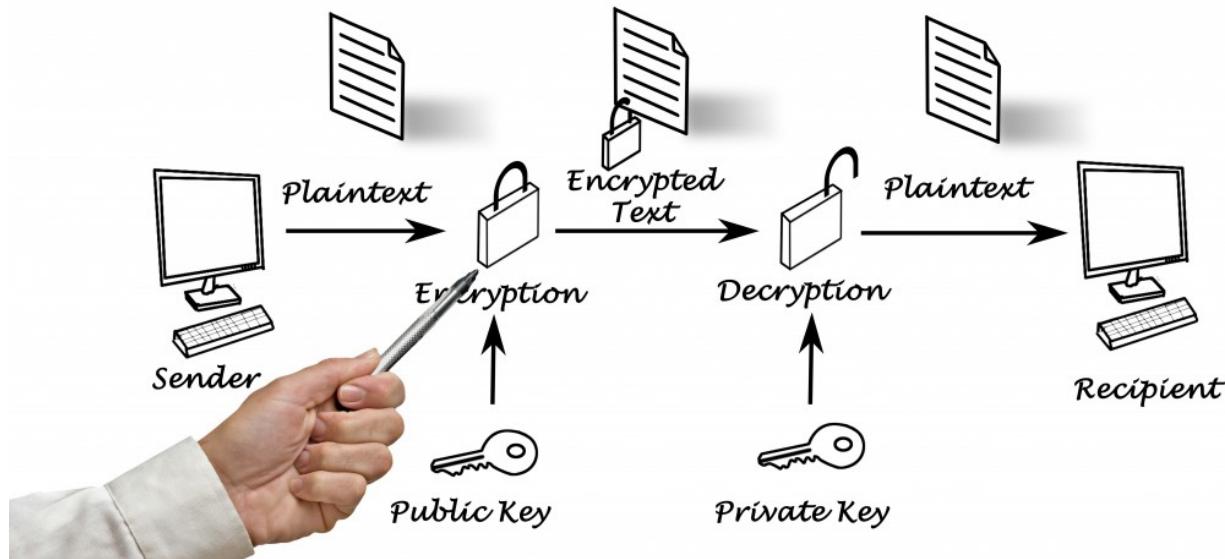
SSL安全

中间人攻击



- 替换证书
 - 不正确的证书检查
 - 不再安全的根CA
 - 吊销证书查询机制受阻
- 解决方案
 - 把信任的基础存放到本地
 - Certificate Pinning
 - 将服务器的证书签名硬编码在客户端代码中，帮助进行证书验证
 - app实现
 - 浏览器实现

JOSS



密钥管理

goss

密钥管理



包括对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档与销毁等环节进行管理和策略制定的全过程

□ 密钥及密钥材料的生成

□ 低熵环境下，随机数生成器的随机性

□ 密钥的存储、分发

□ 硬编码在程序中

□ 不安全存储在介质中

Diffie-Hellman + Pinning

30SS



测评方法

密码系统的提取



确定分析目标

口界定相关的实体，实体间的交互

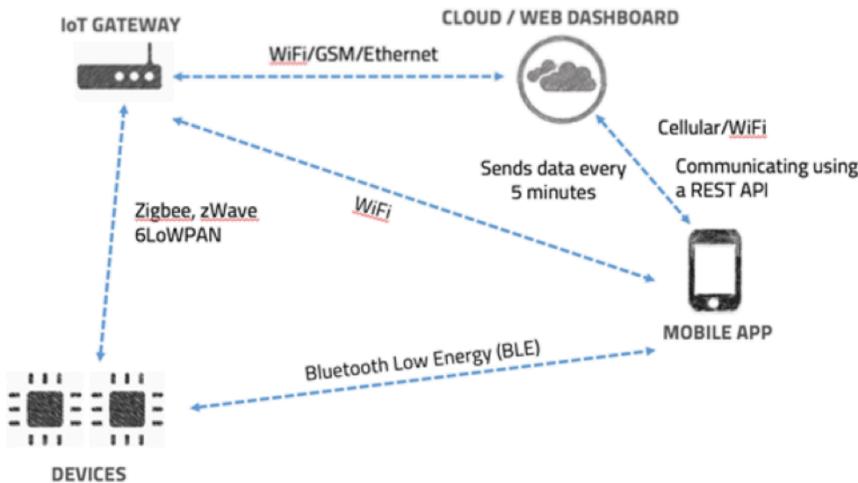
口分析实体间交互协议

口设备固件安全分析

口无线通信协议安全分析

口私有协议安全分析

口APP安全分析



JOSS

Android主流私有协议安全性分析

分析方法



- 流量分析
 - 基于差分模糊测试的动态流量分析
 - 基于特征指纹的协议规范提取
- 移动应用分析
 - 方法：污点分析、符号执行
- 协议漏洞检测方法
 - 基于模型匹配的漏洞检测
 - 基于模板攻击的漏洞检测
 - 协议规范提取后的人工检测



测评结果

密码应用测评关键结果



- ✓ 身份鉴别 ✓ 数据传输抗重放
- ✓ 数据传输机密性 ✓ 数据存储机密性
- ✓ 数据传输完整性 ✓ 数据存储完整性
- ✓ 数据传输真实性 ✓ 密钥管理
- ✓ 数据传输抗抵赖 ✓ 生成、存储、使用、更新、归档、销毁、备份和恢复

GOSS

测评结果



Case Study

- ✓ 应用名称：xxx安卓版
- ✓ 分析结果：
 - ✓ 用户在客户端进行登录时使用了以下机制的一种或两种机制的组合：静态口令、短信验证码
 - ✓ 口令经一些密码变换后发送，通信通道为HTTP
 - ✓ 对口令的具体处理为：
 - ✓ 使用XXTEA对称加密算法加密口令（密钥为本地生成的随机数，但由于实现问题，该随机数是一个固定的值），之后拼接上述随机数加密后的结果，加密同样使用XXTEA算法，密钥硬编码，密钥材料是“[B@1f80ce47”。最后拼接手机号、系统信息等内容，作为待发送消息。
 - ✓ 通信通道HTTP的负载均经加密处理，加密算法为3DES/CBC，密钥（“richeninfo.3322.org@nqz#211”作为密钥材料）与IV（“01234567”）均硬编码在程序中

iossey

谢谢！



hui.liu803@gmail.com

5055