FIDO UAF 协议的形式化分析

论文：A Formal Analysis of the FIDO UAF Protocol

会议：NDSS Symposium 2021

作者：冯皓楠, 李晖, 潘雪松（北京邮电大学）

赵子铭（CactiLab, University at Buffalo）

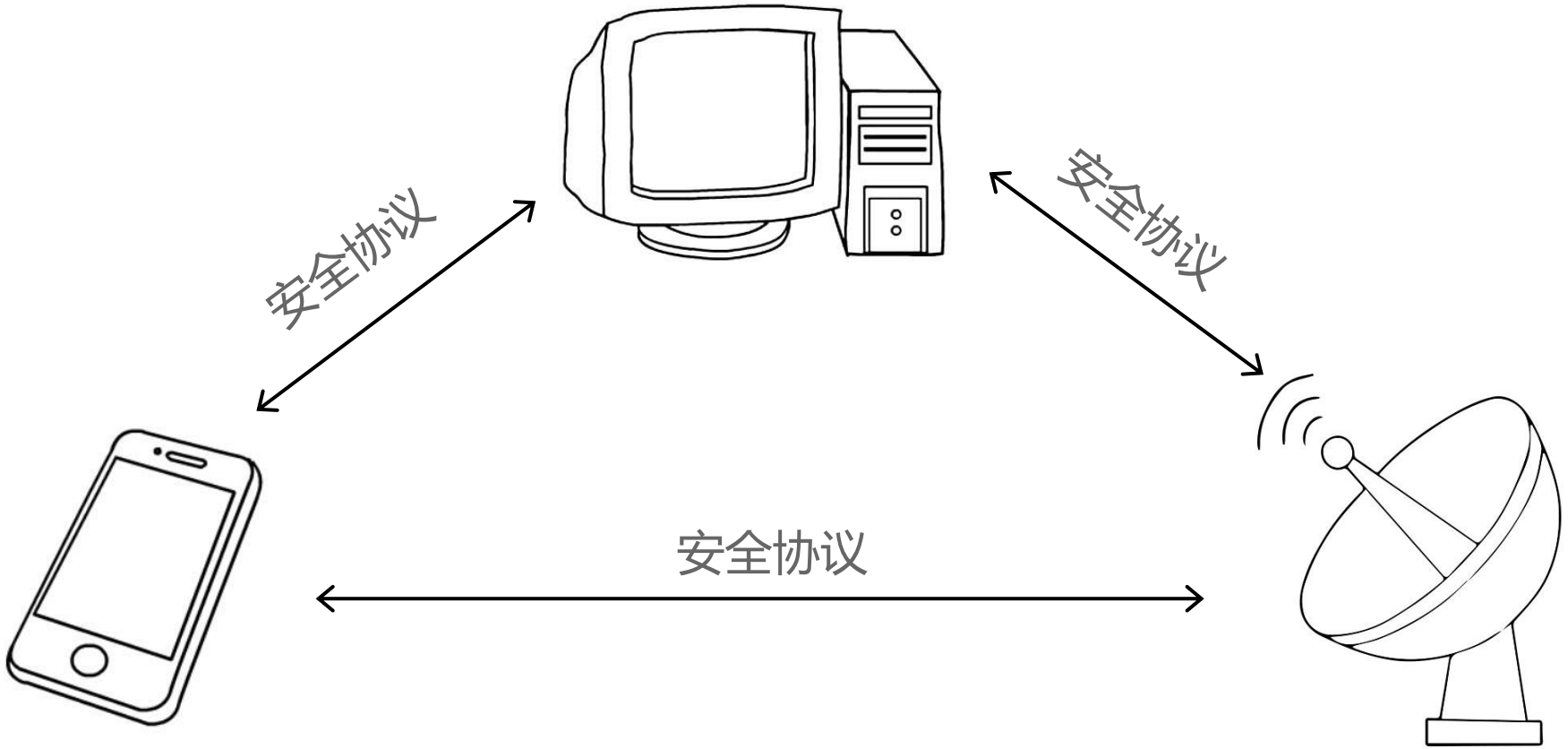
主讲：冯皓楠

关键词：安全协议，形式化分析，FIDO UAF协议

北京郵電大學 Beijing University of Posts and Telecommunications

University at Buffalo

安全协议在通信系统中的重要作用



以上图片均来源于互联网

安全协议不一定安全

WPA2安全加密协议被破解 一夜之间全世界WiFi都不安全了?

2017-10-17 18:39

外媒报道，比利时研究人员今日表示：WPA2安全加

Vanh

Wind

示已在

蓝牙协议爆严重安全漏洞影响53亿设备

2017.09.14 11:15:21 来源: cnBeta.com 作者:cnBeta.com

零日漏洞，这些漏

备到使用短距离无

ttack vect

立一个"中

【漏洞公告】CVE-2016-0800：DROWN 中间人劫持漏洞

更新时间： 2018-01-15

漏洞描述

国外安全专家发现了一种

若您的服务器支持以 SSL

穷举的方式破解出被加密

TLS 1.2 协议现漏洞， POODLE攻击卷土重来

2019-02-14 17:40

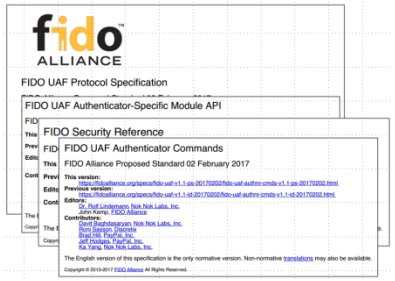
谷歌安全团队曾在2014年10月发现一个高危SSL漏洞POODLE（贵宾犬漏洞）影响SSL V3.0版本。后来，该漏洞卷土重来，甚至影响到SSL升级版——TLS协议。

一位研究人员在新的TLS中发现了两个新的相关漏洞1.2加密协议。该协议暴露了所谓的POODLE攻击的安全会话，并没有真正消亡。

安全协议分析领域的局限

安全协议专家
例如标准化组织

V1.2



协议标准
例如TLS 1.2标准

【漏洞公告】CVE-2016-0800：DROWN 中间人劫持漏洞

更新时间：2018-01-15

TLS 1.2 协议现漏洞， POODLE攻击卷土重来

2019-02-14 17:40

如何能发现所有的漏洞？

未知的新漏洞

北京郵電大學 Beijing University of Posts and Telecommunications

University at Buffalo

以上图片均来源于互联网

形式化分析技术

数学（可证）+计算机（便捷、高效、自动化）

技术原理

- 逻辑推理技术（BAN逻辑、GNY逻辑）
- 模型检测技术（状态空间遍历）
- 定理证明技术（归纳法、串空间模型、阶函数）

SATMC

Maude-NPA

Athena

AVISPA

FDR

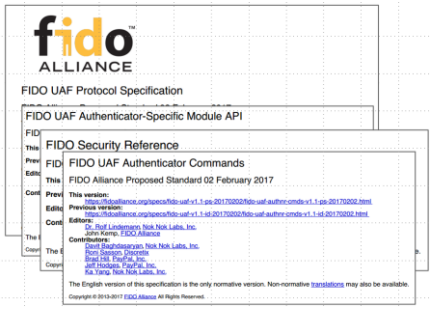
ProVerif

Isabelle

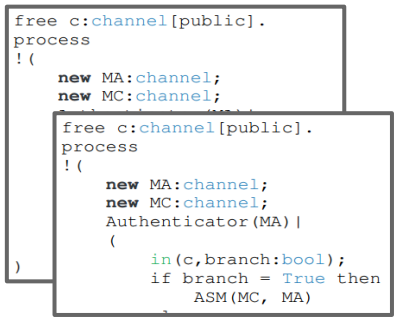
TA4SP

Scyther

Tamarin



协议标准文档



形式化模型

形式化分析工具

北京郵電大學 Beijing University of Posts and Telecommunications

University at Buffalo

形式化分析技术的应用

Formal analysis of privacy in Direct Anonymous Attestation schemes ☆

Ben Smyth [a,*], Mark

[a] Mathematical and Algorithmic Sc
[b] School of Computer Science, Univ
[c] HP Laboratories, Bristol, UK

CrossMark

A Formal Analysis of 5G Authentication

David Basin
Department of Computer Science
ETH Zurich

Formal Analysis of an E-Health Protocol

go Jonker [b], and Jun Pang [c,

nal University of Singapore, Singapore
ience, Open University, The Netherlands
ology and Communication
ecurity, Reliability and Trust,
bourg, Luxembourg

Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate

{ka

A Formal Analysis of the Norwegian E-voting Protocol*

Véronique

LOR

Component-Based Formal Analysis of 5G-AKA: Channel Assumptions and Session Confusion

Cas Cremers
CISPA Helmholtz Center for Information Security, Germany
cremers@cispa.saarland

Martin Dehnel-Wild
Department of Computer Science, University of Oxford
martin@dehnelwild.co.uk

北京郵電大學 Beijing University of Posts and Telecommunications

University at Buffalo

FIDO联盟：文本密码已经过时

北京郵電大學 Beijing University of Posts and Telecommunications

University at Buffalo

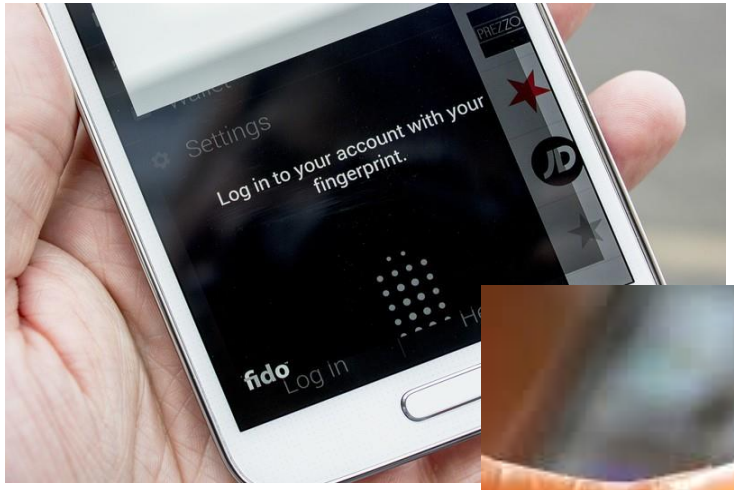
Fast Identity Online (FIDO)

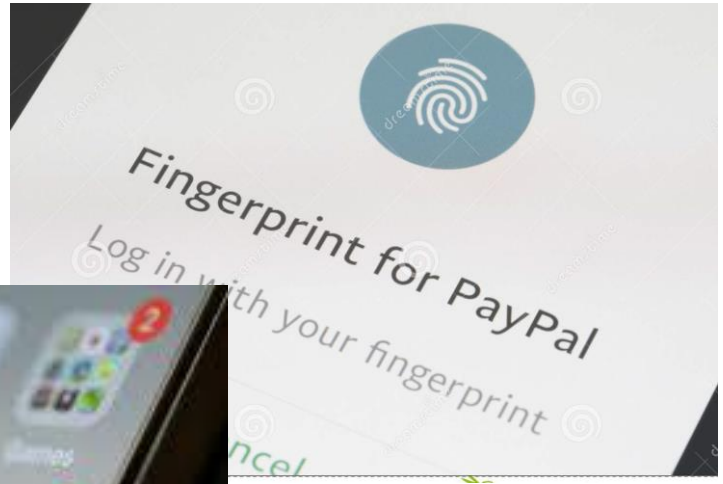
北京郵電大學 Beijing University of Posts and Telecommunications

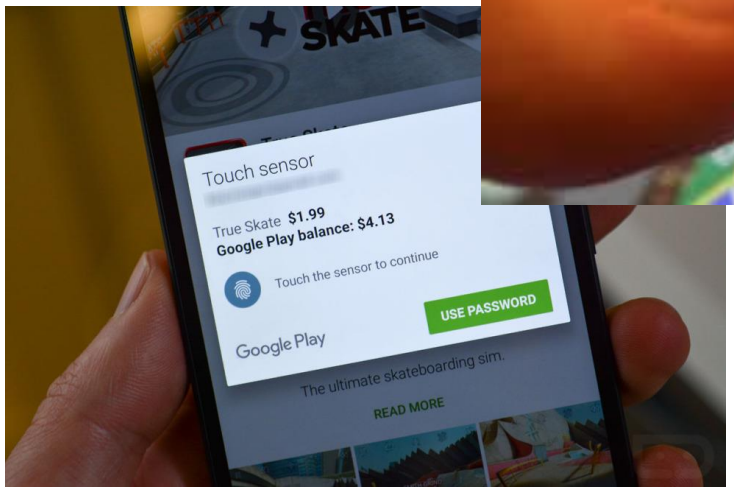
University at Buffalo

以上图片来源于fidoalliance.org

Universal Authentication Framework (UAF)



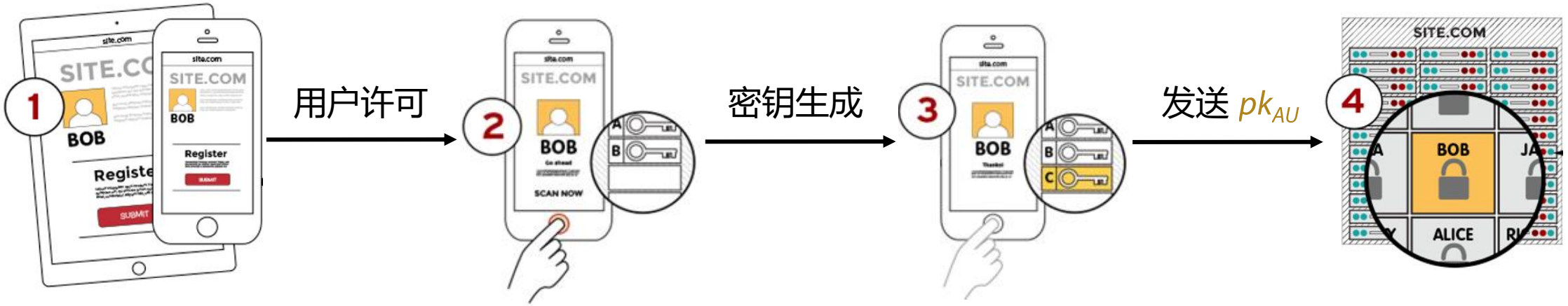




以上图片均来源于互联网

Universal Authentication Framework (UAF)

认证器注册阶段



注册开始

认证器本地记录指纹

生成用户认证签名密钥对

(sk_{AU}, pk_{AU})

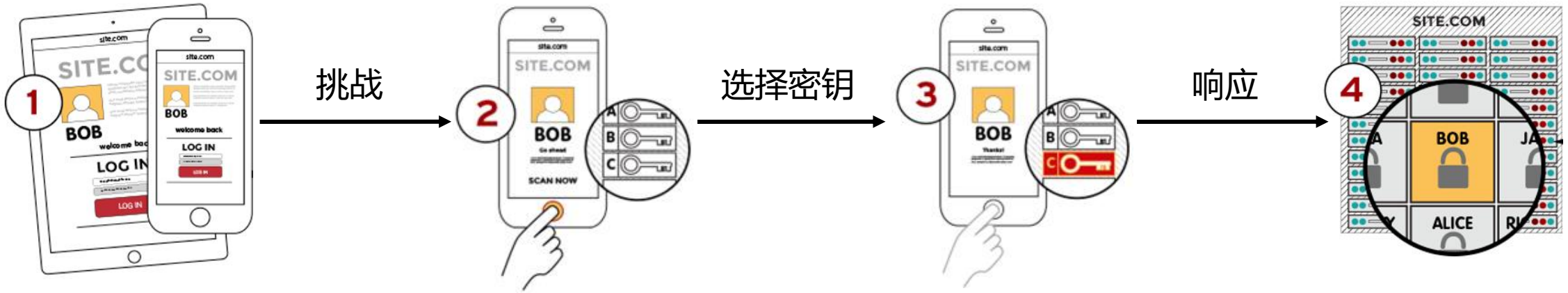
注册成功

例如：银行网站

以上图片来源于fidoalliance.org

Universal Authentication Framework (UAF)

登录/认证/交易确认过程



尝试登录

用户本地验证指纹

解锁认证私钥 sk_{AU}

使用 sk_{AU} 签名挑战值

计算响应

验证签名，成功登录

北京郵電大學 Beijing University of Posts and Telecommunications

University at Buffalo

以上图片来源于fidoalliance.org

UAF协议并不安全

A Security Evaluation of FIDO's UAF Protocol in Mobile and Embedded Devices

Christoforos Panos[1], Stefanos Malliaros[2], Christoforos
and Christos Xenakis[2]

[1] Department of Informatics & Telecommunications, U
cpanos@di.uoa.gr
[2] Department of Digital Systems, University
{stefmal, dadoyan, apanou, xena

3.1 UAF protocol vulnerabilities and limitations

Table 1. threats related to the UAF protocol and their

Asset	Threat	
Attestation private key	Attacker gains access to the attestation keys	Create
Authentication private key	Attacker gains access to the authentication keys	Attem ing pa
UAF authenticator	User installs a malicious authenticator	Impers ter the
TrustZone, UAF authenticator	Attacker compromises the trusted computing platform	Create user, c
UAF client, UAF authenticator, TrustZone	Attacker gains physical access to a user's device	Create user, c install
UAF authenticator	Attacker employs a cloned authenticator	Impers ter the

Security Analysis of an Attractive Online Authentication Standard: FIDO UAF Protocol

HU Kexin[1,2], ZHANG Zhenfeng[2]
[1]University of Science and Technology of China, Hefei, China.
[2]Laboratory of Trusted Computing and Information Assurance, Institute of Software, Chinese Academy of Sciences, Beijing, China.

V. ATTACKS

This section proposes the following three potential attacks. We name them as the "Mis-Binding" Attack, the "Parallel Session" Attack and the "Multi-User" Attack.

5.1 Attacks with the user device corruption

We first assume an attacker has the ability to control the ASM and the FIDO Client (denoted by "FA") by infecting the user device and this assumption is reasonable for a user device such as a mobile phone, or a laptop.

Mis-Binding Attack: The essence of this attack is that when an attacker C can corrupt FA at the UAF registration, C replaces the user's response with C's , which makes RP binds C's key materials to the user account after the verification. To avoid the awareness of the user, C can send the original message to the user's authenticator, but drop his response and send an

$$4.\ FA \rightarrow RP: \quad \begin{array}{l} Sig(sk_u, (ID_A, fc_1, n, KeyID_u, cntr')) \\ fcp_1, ID_A, fc_1, n, KeyID_u, cntr', \\ Sig(sk_u, (ID_A, fc_1, n, KeyID_u, cntr')) \end{array}$$

Fig.5 *Parallel Session Attack*

At the end of the attack, the RP successfully verifies the signature signed by the user, whereas in fact it is sent by C . The second session can be dropped after the receipt of message 3'.

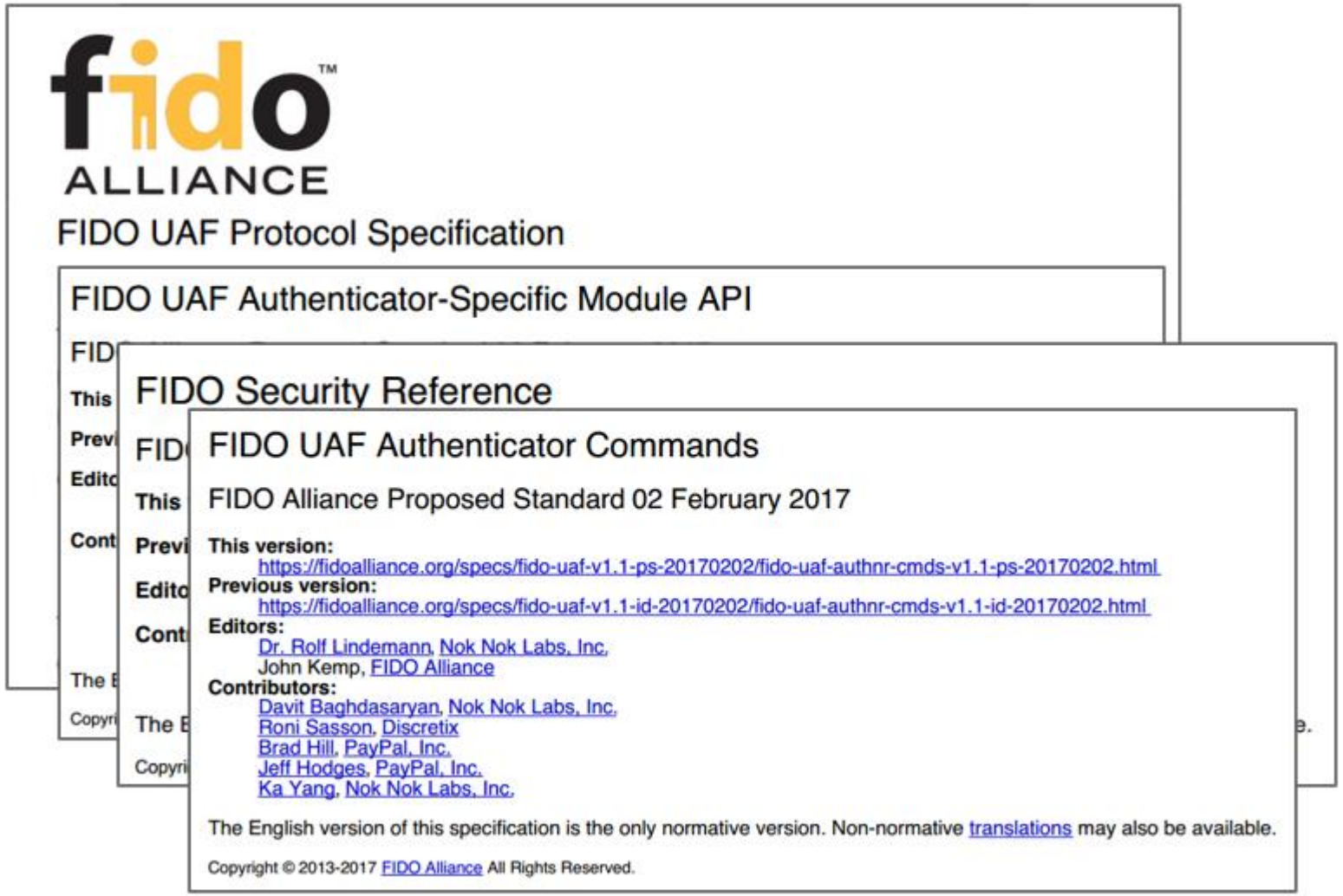
5.2 Multi-User Attack

From the authentication protocol's cryptographic abstraction presented in section 3, we can see that if a user passes the verification of the authenticator, the authenticator will fully trust him. If the authentication is not "a step-up authentication", which has explained in section 3.2, when the process gets into the authentication sub-protocol, the user can cheat the authenticator by choosing a username that not belongs to him to let the authenticator create other user's credential. And this user can impersonate the other one to pass the authentication.

北京郵電大學 Beijing University of Posts and Telecommunications
University at Buffalo

形式化分析UAF的困难

500+页的标准文档



北京郵電大學 Beijing University of Posts and Telecommunications

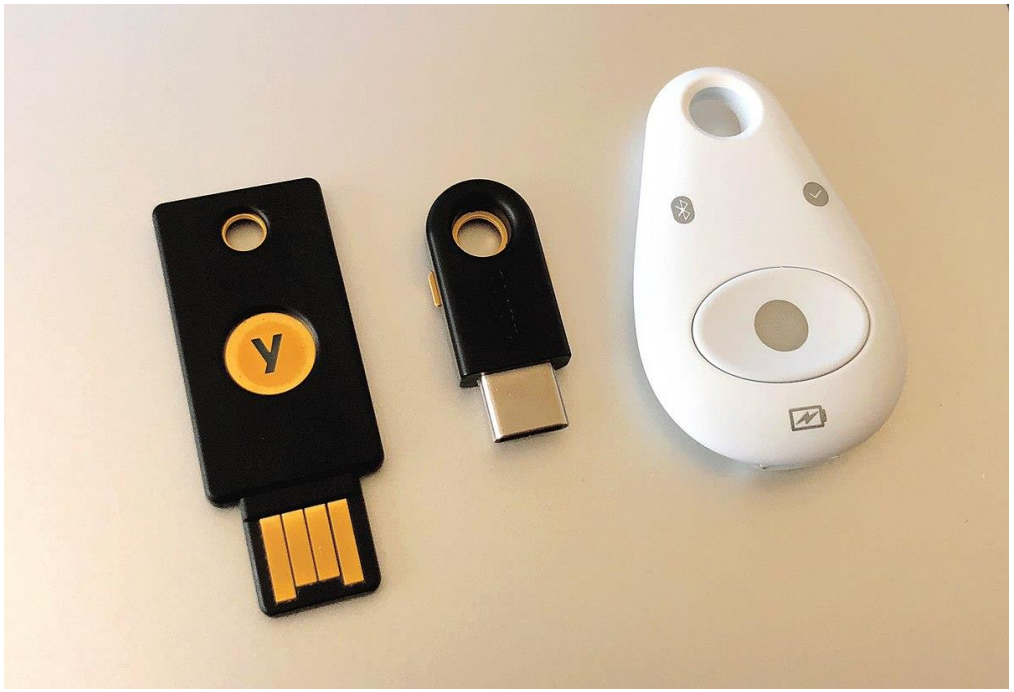
University at Buffalo

形式化分析UAF的困难

存在不同类型的认证器

绑定认证器

(只能在单一设备上使用UAF认证)



漫游认证器

(可以在任何地点使用UAF认证)

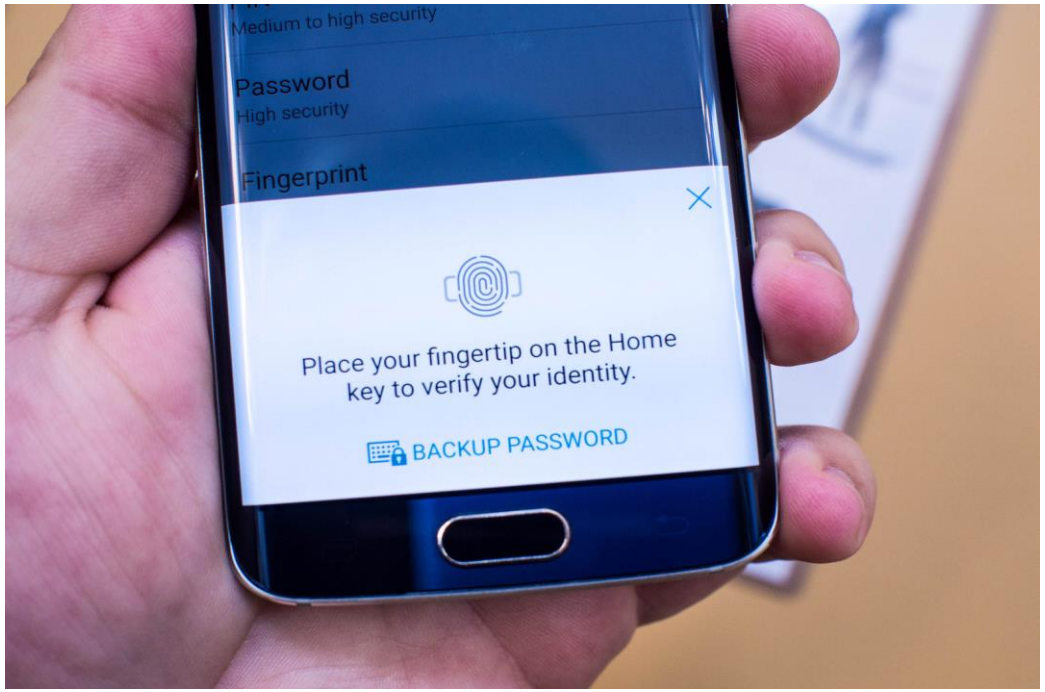
北京郵電大學 Beijing University of Posts and Telecommunications

University at Buffalo

以上图片均来源于互联网

形式化分析UAF的困难

不同的应用场景（首次登录/交易确认）



登录系统

（不存在用户会话，首次认证身份）

递进式鉴别

（已经存在用户会话，并需要再次认证）

例如：交易确认

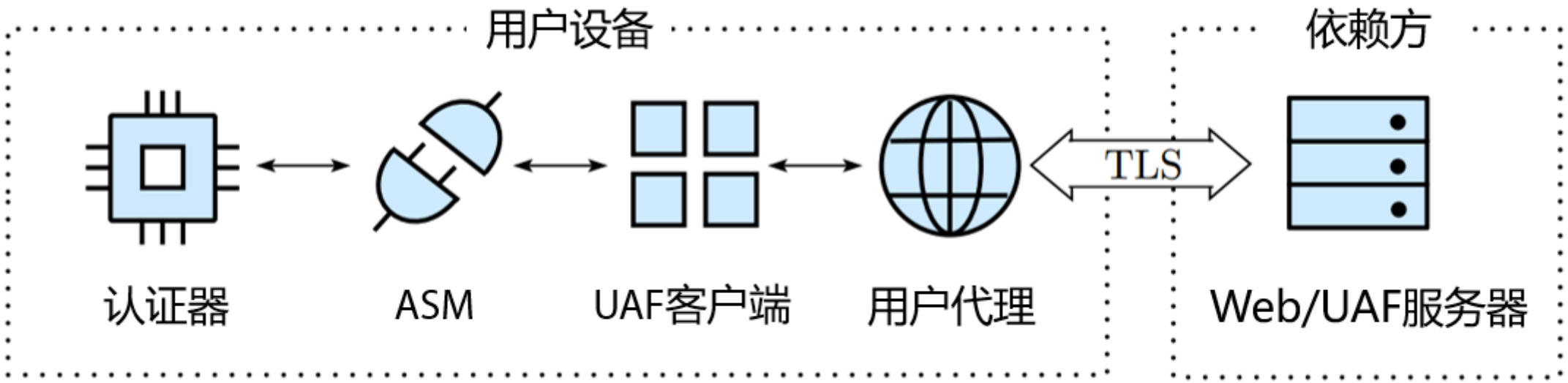
北京郵電大學 Beijing University of Posts and Telecommunications

University at Buffalo

以上图片均来源于互联网

形式化分析UAF的困难

多实体交互

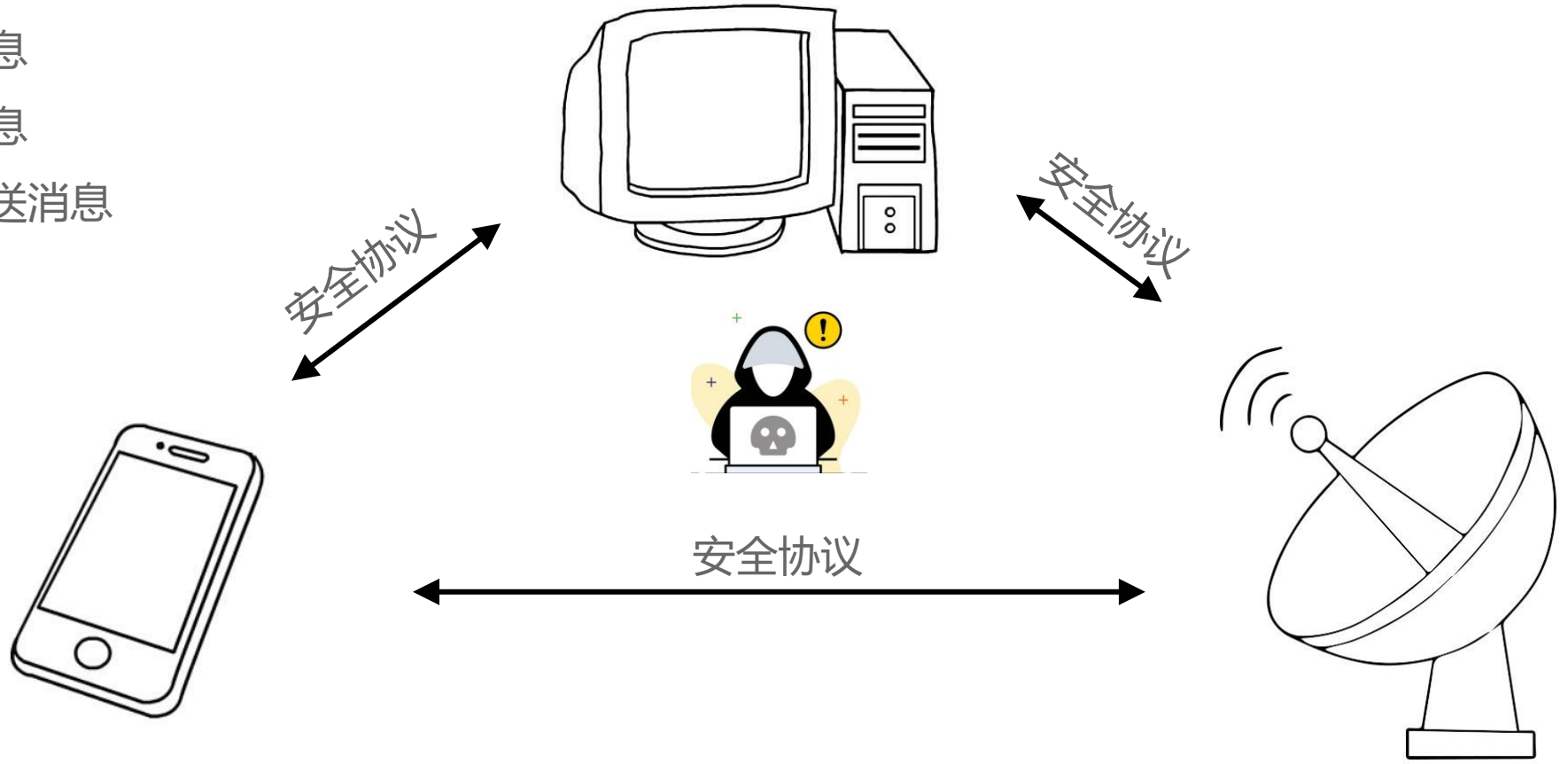


形式化分析UAF的困难

协议运行环境 ≠ Dolev-Yao模型

Dolev-Yao攻击者模型：

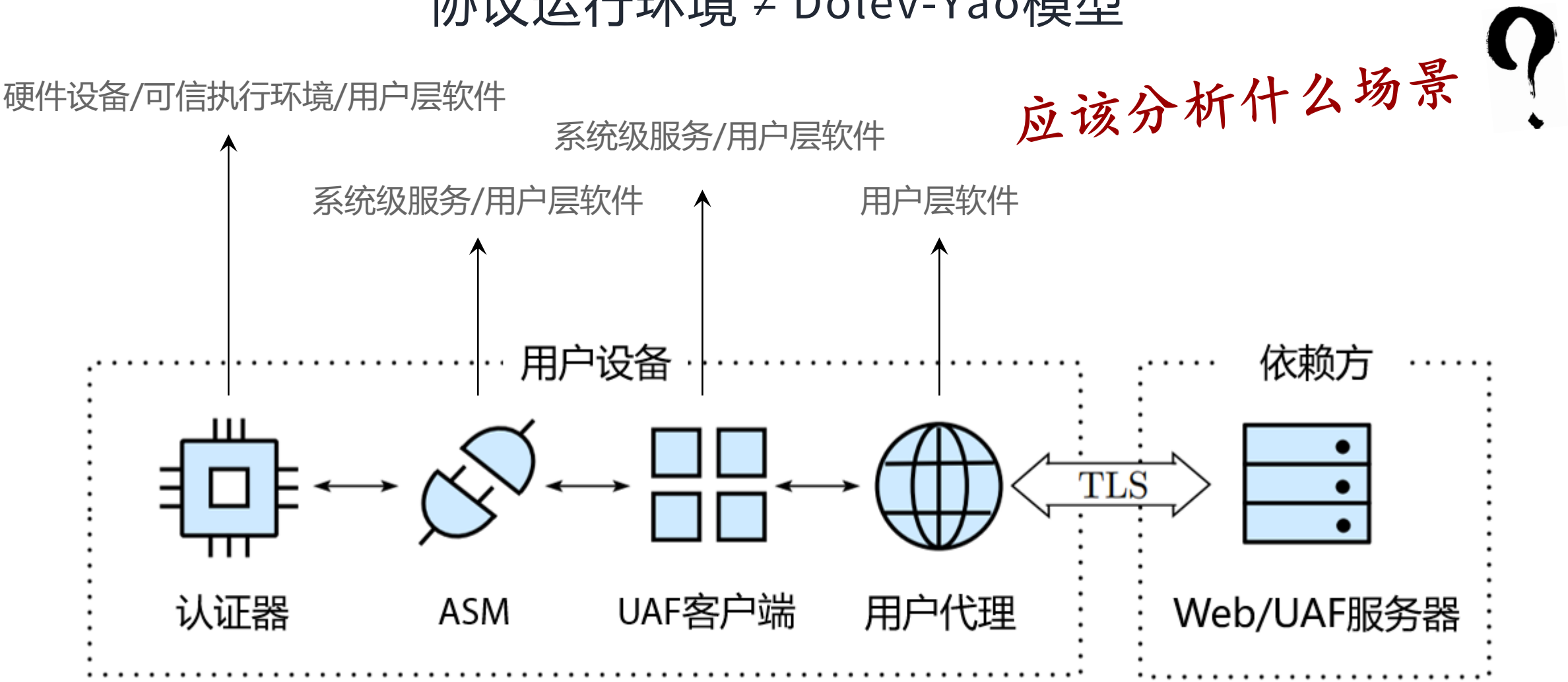
- 窃听、拦截消息
- 存储、转发消息
- 主动构造并发送消息
- 假冒合法主体



以上图片均来源于互联网

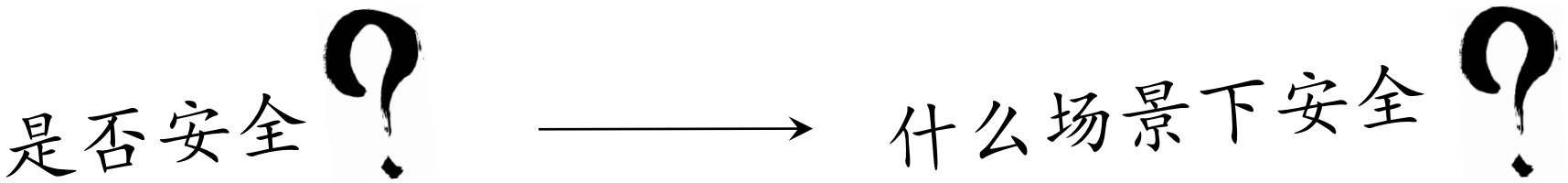
形式化分析UAF的困难

协议运行环境 ≠ Dolev-Yao模型



最小化安全假设算法

寻找使协议满足安全目标的最小条件



最小化安全假设算法

寻找使协议满足安全目标的最小条件

可能发生变化的安全假设：

① 假设认证签名私钥 sk_{AU} 没有泄露

② 假设用户名 *Uname* 没有泄露

③ 假设设备中不存在恶意的认证器

④ 假设设备中不存在恶意的ASM

⑤ 假设设备中不存在恶意的UAF客户端

⑥ 假设设备中不存在恶意的依赖方

⑦ …. **（n个安全假设）**

全组合 →

应用场景：

①

②

① ②

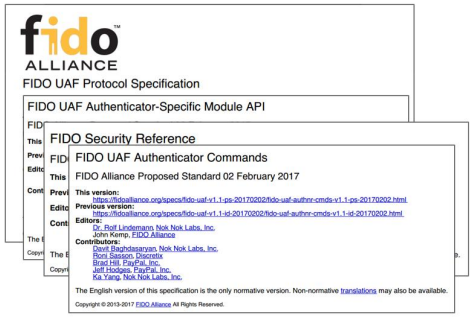
① ② ③

② ③ ⑤ ⑥

① ② ③ ④ ⑤ ⑥

… **（n!个场景）**

形式化分析过程



UAF标准

19个文档，500+页

形式化翻译

- 协议流程
- 安全目标
- 安全假设

精确/形式化的描述

形式化建模

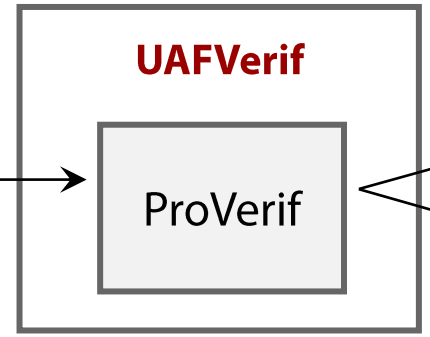
```
free c:channel[public].
process
!(
    new MA:channel;
    new MC:channel;
    Authenticator(MA)|
    (
        in(c,branch:bool);
        if branch = True then
            ASM(MC, MA)
        else
            ASM(MC, c)
    )
)
```

ProVerif形式化模型

扩展的应用π-演算描述

ProVerif形式化模型

400,000+应用场景



最小化安全假设

修改模型

北京郵電大學 Beijing University of Posts and Telecommunications

University at Buffalo

形式化描述：安全目标与安全假设

安全目标：

- 机密性目标（confidentiality）：私钥skAU的机密性、交易文本Tr的机密性、计数器的机密性
- 认证性目标（Authentication）：参考**Lowe提出的认证性分类标准**，如单射协议、非单射协议等
- 隐私性目标（Privacy）：不可链接性（相互勾结的依赖方无法将会话关联到同一用户）

密码算法的安全假设：假设密码算法是**安全**的黑盒

数据保护能力的安全假设

- 攻击者已知协议中的身份标识（如 *Uname*, *AppID*, *AAID*）和公钥（如 pk_{AU}）
- 攻击者**可能**已知私钥或其他机密字段（如 sk_{AU}, *CNTR*）
- 攻击者已知不同的机密字段构成可变的安全假设，用于分析最小化安全假设

信道与实体的安全假设 ≠ Dolev-Yao模型

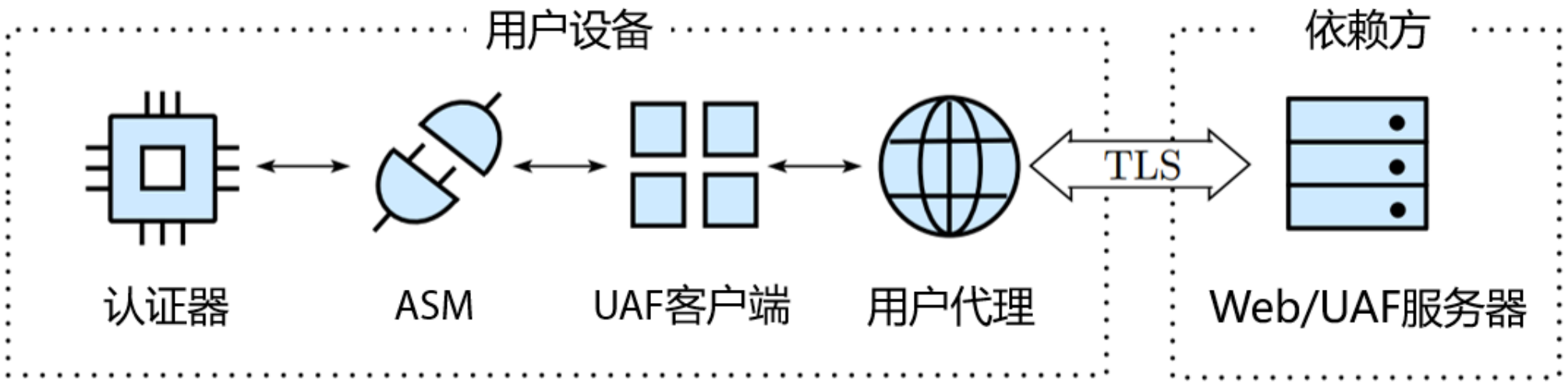
- 设备内部的信道不同于公开的网络信道

形式化描述：安全假设

设备内部的通信信道模型

- 假设设备环境能够保证**诚实实体**之间的通信信道是安全的，攻击者无法拦截或发送信息
- 攻击者**可能**可以作为合法实体参与协议并与诚实实体通信

以恶意UAF客户端为例，有**4种**可能的情况：

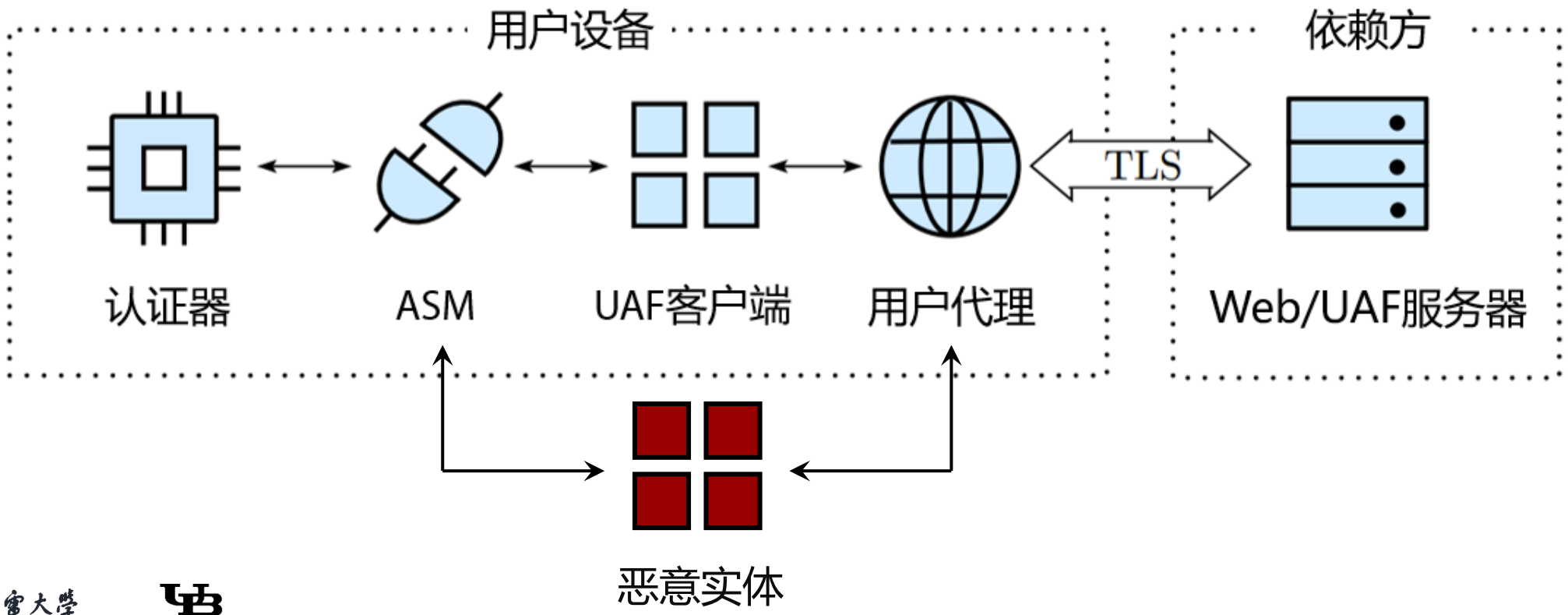


形式化描述：安全假设

设备内部的通信信道模型

- 假设设备环境能够保证**诚实实体**之间的通信信道是安全的，攻击者无法拦截或发送信息
- 攻击者**可能**可以作为合法实体参与协议并与诚实实体通信

1. 恶意实体可以伪造UAF客户端同时和诚实的用户代理以及诚实的ASM通信

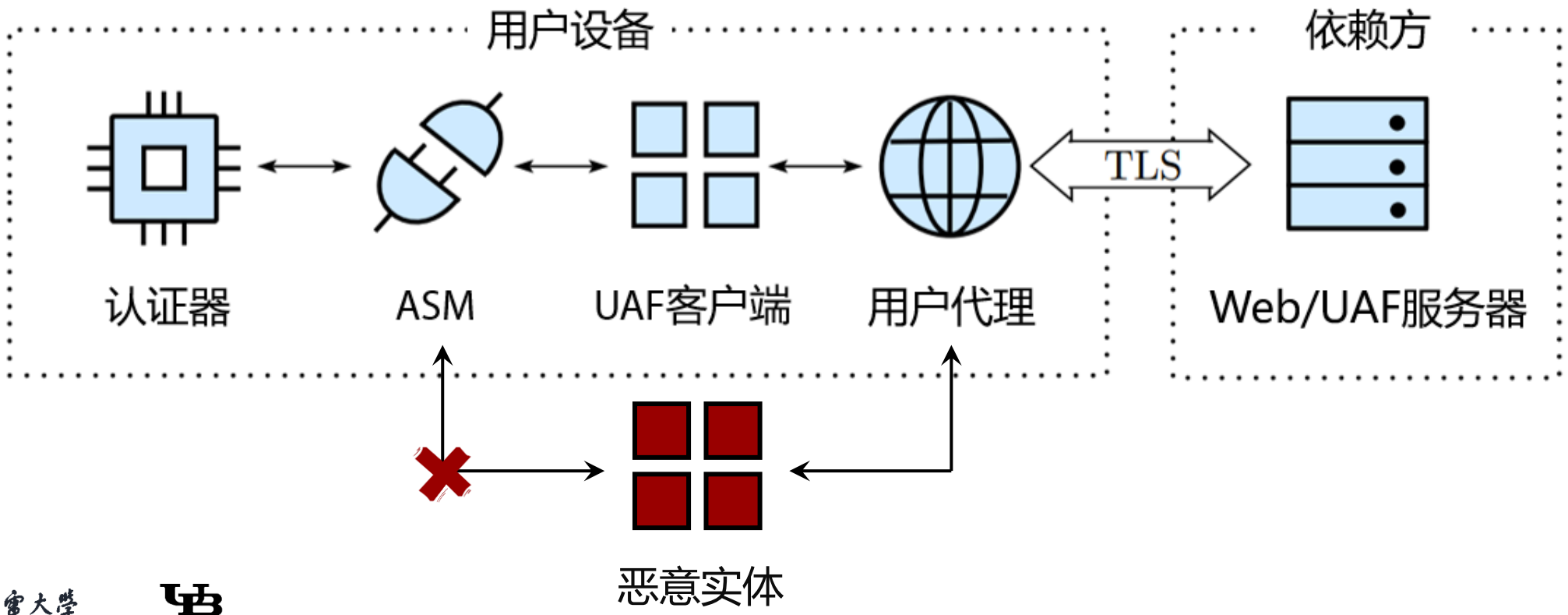


形式化描述：安全假设

设备内部的通信信道模型

- 假设设备环境能够保证**诚实实体**之间的通信信道是安全的，攻击者无法拦截或发送信息
- 攻击者**可能**可以作为合法实体参与协议并与诚实实体通信

2. 恶意实体可以伪造UAF客户端和诚实用户代理通信，但无法和诚实的ASM进行通信

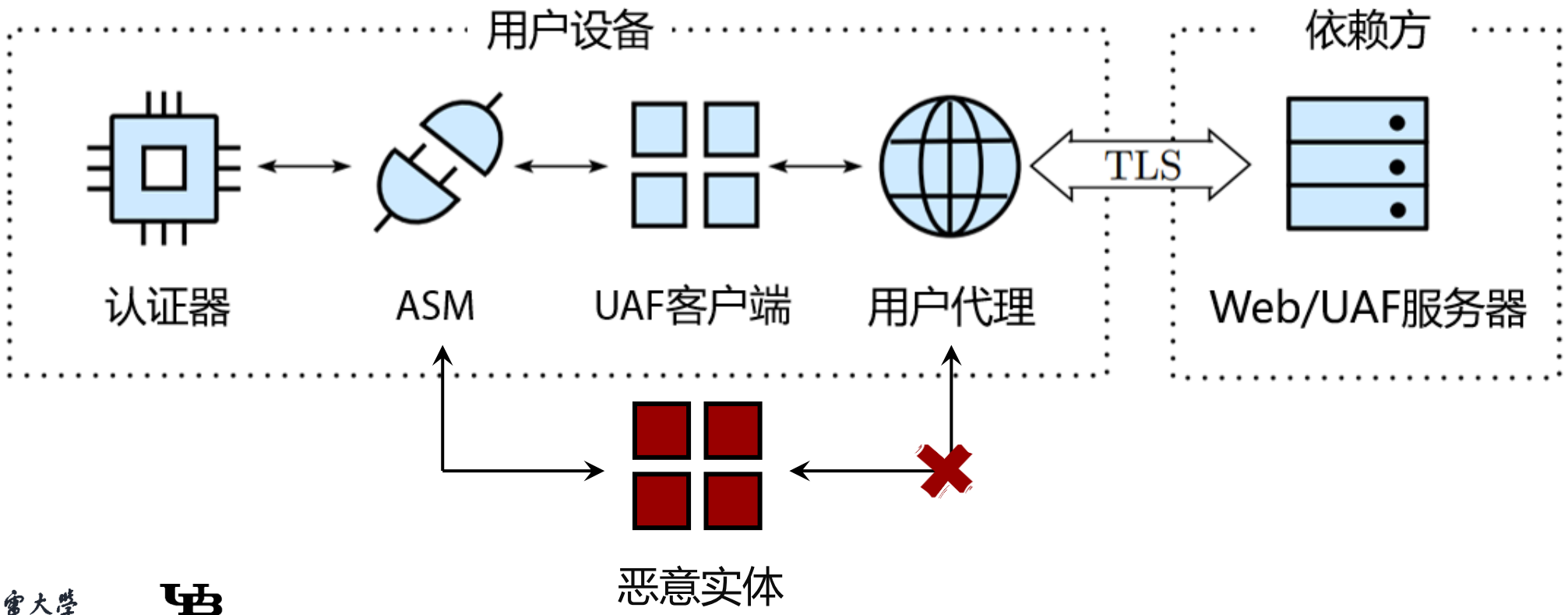


形式化描述：安全假设

设备内部的通信信道模型

- 假设设备环境能够保证**诚实实体**之间的通信信道是安全的，攻击者无法拦截或发送信息
- 攻击者**可能**可以作为合法实体参与协议并与诚实实体通信

3. 恶意实体可以伪造UAF客户端和诚实的ASM通信，但无法和诚实的用户代理进行通信

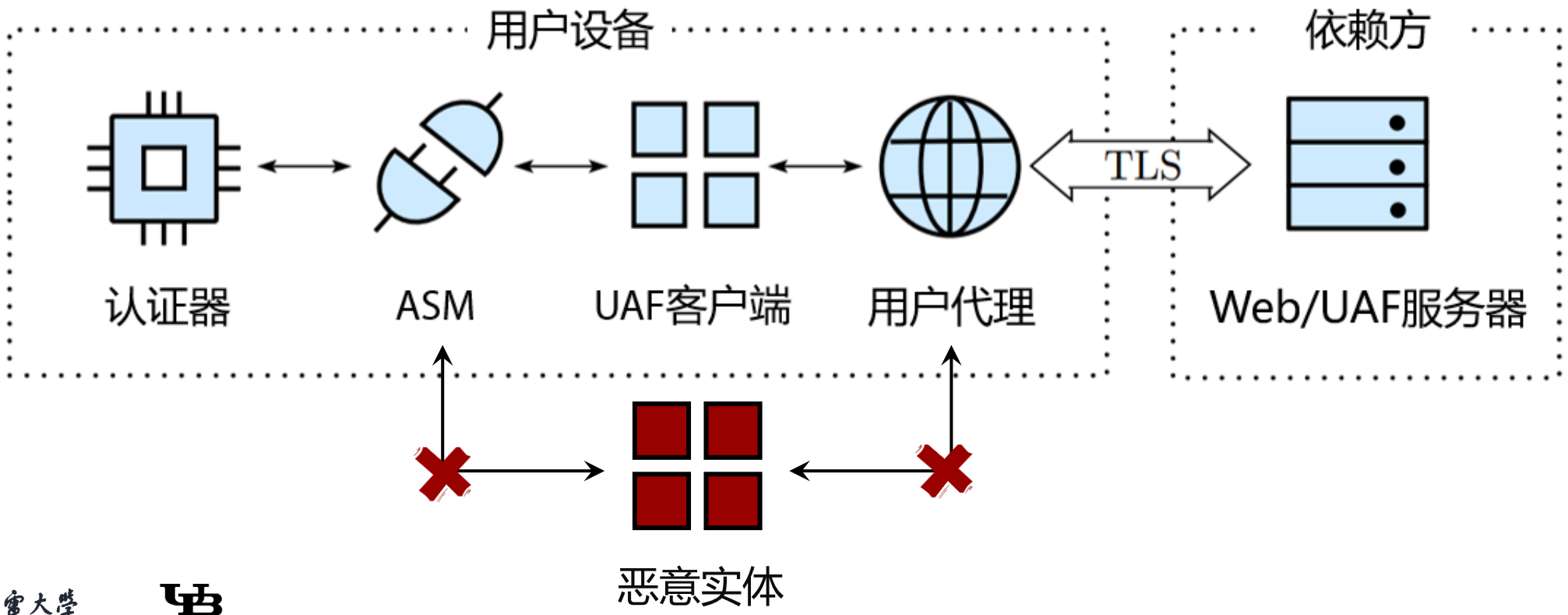


形式化描述：安全假设

设备内部的通信信道模型

- 假设设备环境能够保证**诚实实体**之间的通信信道是安全的，攻击者无法拦截或发送信息
- 攻击者**可能**可以作为合法实体参与协议并与诚实实体通信

4. 恶意实体既无法伪造UAF客户端与诚实的ASM通信，也无法和诚实的用户代理通信



形式化模型

协议流程 ~900LoC

- 支持**无限**数量并行运行的实体 + **无限**数量的协议会话
- 支持不同的应用场景

安全假设和安全目标

- 对**设备内部进程通信**存在恶意实体的场景建模（获得ProVerif开发者Bruno Blanchet教授认可）
- 发现ProVerif 2.00及以下版本的**漏洞**，并提出了一种**解决方案**（通知开发者并促进了ProVerif 2.01版本的更新）
- 使用**观测等价性**（observational equivalence）建模**不可链接性**（unlinkability）

UAFVerif ~1000LoC

- 自动生成并分析**400,000+**个不同安全假设下的应用场景
- 自动验证满足安全目标的**最小化安全假设**
- 分析需**80+**小时

最小化假设结论示例

UAF协议在注册阶段实现机密性和认证性目标的最小化假设

注册	类型	1st bound	2nd bound	1st roaming	2nd roaming
机密性	K_w	√			
	sk_{AT}	√			
	sk_{AU}	$\neg k_w \cup \neg M[A]$		√	$\neg k_w$
	ak	$\neg tok \cap \neg A[M]$		×	
	$CNTR$	$\neg C[M] \cap \neg M[A]$			
认证性		$\neg C[U] \cap \neg M[C] \cap \neg A[M]$			

UAF协议在注册阶段实现机密性和认证性目标的最小化假设

发现

KHAccesstoken 机制是无效的 ☹

- 攻击者可以很容易地计算出token的值并伪造ASM与认证器进行通信
- 攻击者可以通过拦截明文发送的token并伪造ASM与认证器进行通信

注册阶段比认证阶段更容易受到攻击 ☹

- 超过100,000个认证器可以共享相同的鉴证密钥和认证器ID
- 依赖方信任任何合法的认证器，即便是攻击者的认证器

UAF协议满足不可链接性 ☺

- 任何相互勾结的恶意依赖方无法将会话与用户关联

UAF协议能够抵御钓鱼攻击 ☺

- 认证过程中，恶意的依赖方（如钓鱼网站）无法通过诚实依赖方的检测
- 认证过程中，恶意的用户代理（如恶意的浏览器）无法通过诚实依赖方的检测

攻击

发现4种类型的攻击（涵盖了先前发现的攻击，并包含新的攻击）：

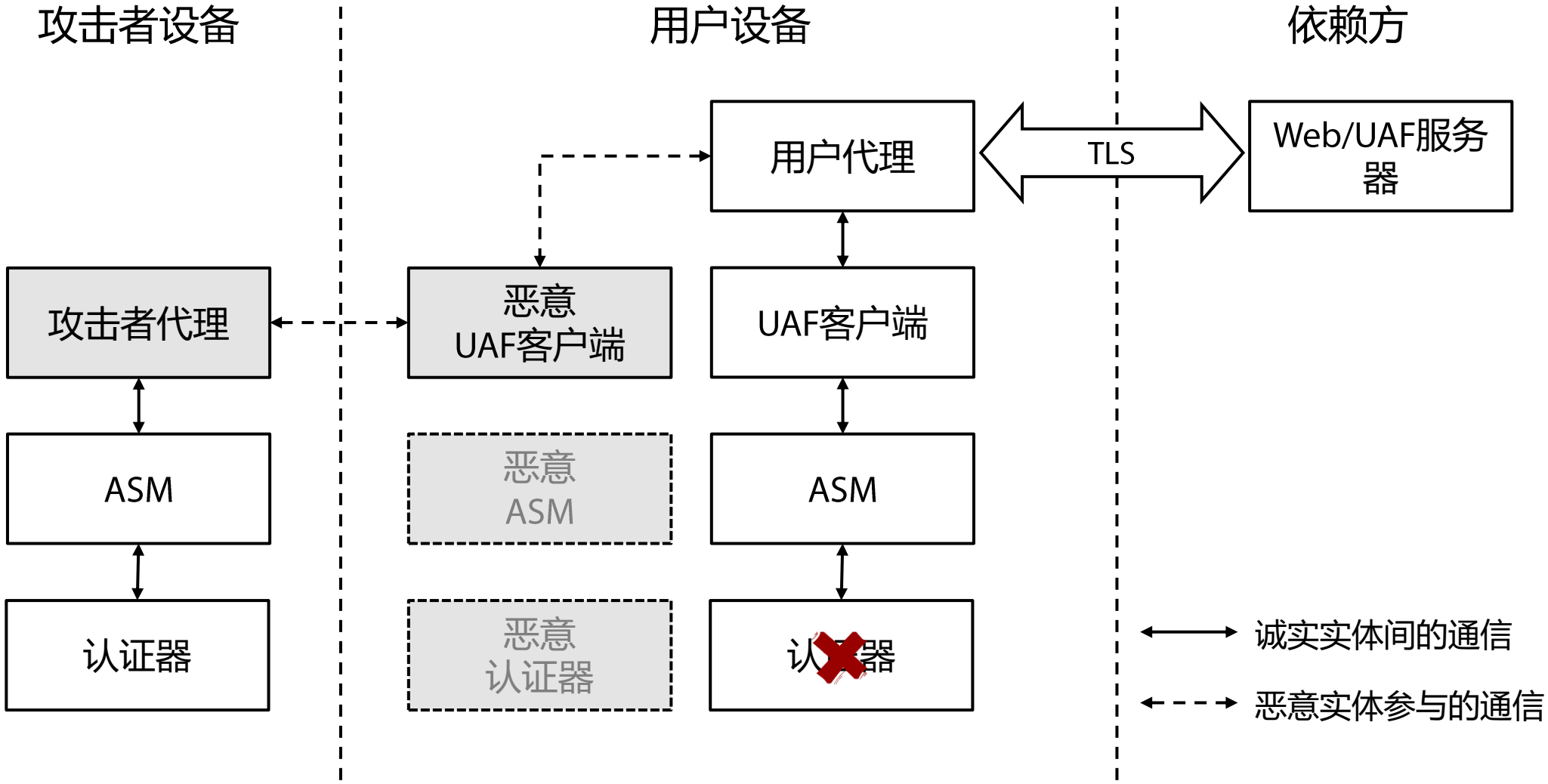
- **认证器重绑定攻击**：在注册阶段将用户的账户绑定在攻击者的认证器上，并仿冒用户
- **平行会话攻击**：在认证阶段使用用户的认证器为攻击者的认证挑战进行签名，并仿冒用户
- **隐私揭露攻击**：通过破坏 *CNTR* 和 *Tr* 字段跟踪用户认证次数、交易等隐私行为
- **拒绝服务攻击**：使 *CNTR* 失序并阻止用户登录

在两个流行的APP上实施认证器重绑定攻击：

- 从**1856**个支付相关的APP中找到**42**个使用UAF协议的APP
- 其中**8**个APP使用硬件认证器部署方案（如：移动和包）
- 其中**34**个APP使用软件认证器部署方案（如：京东金融）
- 成功在移动和包和京东金融上部署攻击（获得1个**CNNVD中危漏洞** CNNVD-202005-1219）

攻击

认证器重绑定攻击原理



攻击

认证器重绑定攻击原理

恶意的UAF客户端

改进建议

明确安全需求

- 阐明“**强认证**（Strong Authentication）”的含义
- 不要以“协议能够抵抗xxx攻击”的方式给出安全目标，而应该以正向的，**形式化的方式**给出
- **注册阶段**只给出了“用户许可”一条安全目标，实际上还有很多**暗含的目标**应当说明

修改KHAccessToken机制

- 增加认证器对ASM的验证机制

在UAF实体之间增加额外的验证机制

- ASM需要验证UAF客户端
- UA需要验证UAF客户端

增加计数器恢复机制

总结

主要贡献

- **首次**对FIDO UAF协议的形式化分析
- 开发并开源**UAFVerif**工具，自动寻找满足安全目标的**最小化安全假设**
- 发现**4种攻击**方式，涵盖了目前对UAF协议人工分析发现的攻击，并包含新的攻击
- 在京东金融和移动和包两个安卓APP上成功**实施认证器重绑定攻击**（获得**CNNVD**漏洞）
- 对UAF协议提出**改进意见**
- 提出了“**设备内部进程通信场景**”的ProVerif建模方法，获得开发者认可
- 发现ProVerif的**漏洞**，并促进了工具的更新

UAF协议分析结论

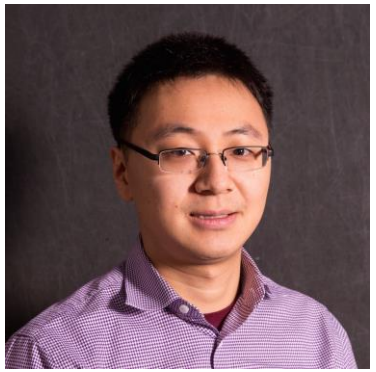
- 缺乏**明确的安全目标**描述 ☹
- **KHAccessToken机制**无法实现安全保障 ☹
- UAF协议额外的实体之间**缺乏认证机制** ☹
- 满足**不可链接性**、可以**抵御钓鱼攻击** ☺

UAFVerif: https://github.com/CactiLab/UAFVerif

冯皓楠
fenghaonan@bupt.edu.cn

李晖
lihuill@bupt.edu.cn

潘雪松
panxuesong@bupt.edu.cn



赵子铭
zimingzh@buffalo.edu