FIDO 安全参考 V1.0

FIDO 联盟推荐标准 2014-12-08

当前版本:

https://fidoalliance.org/specs/fido-uaf-v1.0-ps-20141208/fido-security-ref-v1.0-ps-20141208.html

之前版本:

https://fidoalliance.org/specs/fido-security-ref-v1.0-rd-20141008.pdf

编写者:

罗尔夫•林德曼博士（Dr. Rolf Lindemann）， Nok Nok Labs, Inc.

达维特•巴格达萨利安（Davit Baghdasaryan）, Nok Nok Labs, Inc.

布拉德•希尔（Brad Hill），贝宝（PayPal, Inc.）

摘要

本文档对 FIDO 的安全性进行了分析，该分析是基于当前出版日期的 FIDO UAF 规范和 FIDO U2F 规范的。

文档状态

本章节描述了文档发布时的状态。本文档有可能会被其它文档所取代。当前 FIDO 联盟出版物的列表以及此技术报告的最新修订可在 FIDO 联盟规范索引上找到。网址：https://www.fidoalliance.org/specifications/.

本文档由 FIDO 联盟作为推荐标准发布。如果您希望就此文档发表评论，请联系我们。欢迎所有评论。

本规范中某些元素的实现可能需要获得第三方知识产权的许可，包括（但不限于）专利权。FIDO 联盟及其成员，以及此规范的其他贡献者们不能，也不应该为任何识别或未能识别所有这些第三方知识产权的行为负责。

本 FIDO 联盟规范是“按原样”提供，没有任何类型的担保，包括但不限于，任何明确的或暗示的不侵权、适销性或者适合某一特定用途的担保。

本文档已经由 FIDO 联盟成员评审并签署成为推荐标准。这是一篇稳定的文档，可能会作为参考材料被其它文档引用。FIDO 联盟的作用是引起对规范的注意并促进其广泛的分发。

目录

1. 注释

类型名称、属性名称和元素名称用代码形式书写。

字符串文本包含在双引号“”内，比如“UAF-TLV”。

公式中用 “|” 来表示按字节串联操作。

本文档中用到的 UAF 专用术语在 FIDO 术语表[FIDOGlossary]中均有定义。

1.1 关键字

本文档中的关键字：“必须”，“不得”，“要求”，“将”，“将不”，“应该”，“不应该”，“建议”，“可能”，“可选”都会按照[RFC2119]的描述来解释。

2. 简介

本文档分析了 FIDO UAF 和 U2F 协议簇的安全特性。图 1 是简单的 FIDO 结构概要。具体术语可参见 FIDO 术语表[FIDOGlossary]，架构的技术细节可参见 FIDO 联盟规范目录。

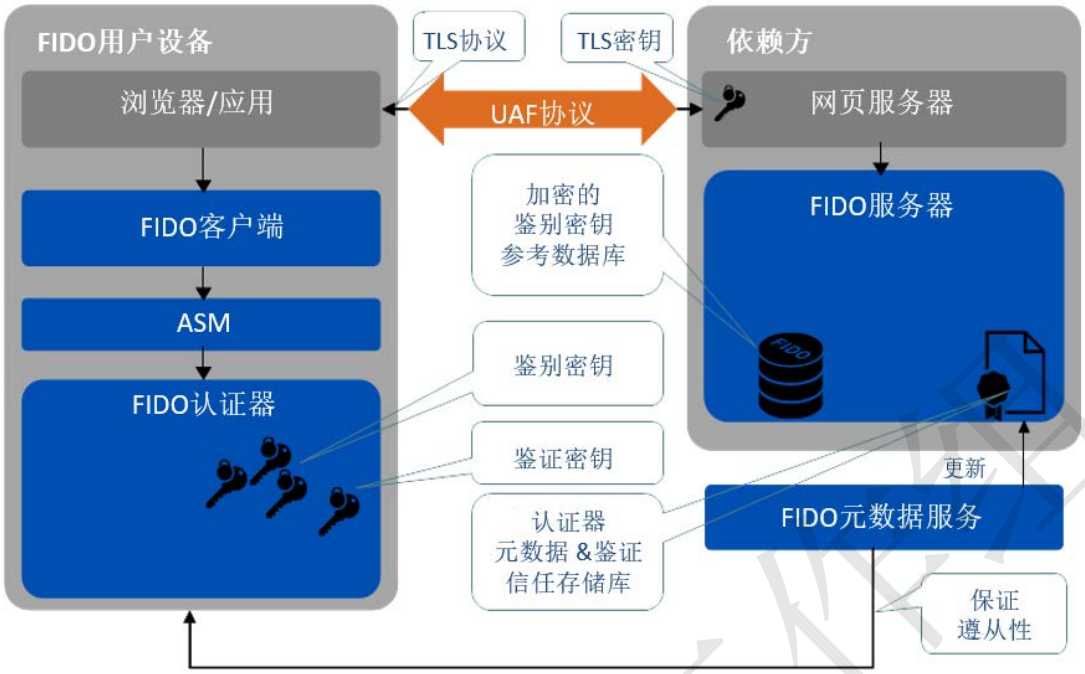

图 1 FIDO 参考架构

概念上讲，FIDO 包含依赖方控制的计算环境和用户控制的需要鉴别的计算环境之间的会话。依赖方的环境包含至少一个网页服务器、网页应用的服务器端以及一个 FIDO 服务器。FIDO 服务器有一个包含了用于鉴证 FIDO 认证器的（公开的）可信锚的可信存储区域。用户环境包括 FIDO 用户设备、至少一个 FIDO 认证器以及 FIDO 客户端和用户代理软件。FIDO 客户端是 UAF 和 U2F 会话的终端。用户代理软件可能是依赖方提供的托管在浏览器的网页应用，也可能是独立的应用。无论是何种情况，FIDO 客户端作为一个概念上明确的实体，实际上可以在用户代理的边界内全部或部分实现。

2.1 目标受众

本文档面向能精通计算系统和网络协议安全分析，以及对 FIDO 架构和协议簇特征熟悉的技术人员。文档讨论了安全目标、安全措施、安全假定和一系列 FIDO 系统所面临的威胁，包括用户的计算环境、依赖方的计算环境和包括 FIDO 组件供应商在内的供应链等的安全。

3. 攻击分类

我们想要区分以下威胁类型（所有威胁都导致用户仿冒）：

1. 对依赖方的自动化攻击，该攻击影响用户使用且用户不能防御。
2. 只执行一次的自动化攻击，可以在不涉及用户或用户设备的情况下持续仿冒用户攻击。
3. 每次成功仿冒用户都涉及用户和设备参与的自动化攻击。
4. 自动化攻击经过用户鉴别的会话。
5. 针对用户或者用户设备的非自动化攻击，该攻击运行一次即可在不直接涉及用户或用户设备的情况下持续地仿冒用户。
6. 每次成功仿冒用户都涉及用户和设备参与的非自动化攻击。

图 2 攻击分类

前 4 种攻击类型被认为是可扩展的，因为它们是自动化的（或者说至少可以自动化），第 5 和第 6 种是非自动化的，它们包含攻击者与用户或用户设备的人工/物理交互。我们把文中分析的威胁归为六类：AC1—AC6。

注释

1. FIDO UAF 使用非对称加密来保护用户防止这类攻击，将控制权返还给用户，例如，当使用强随机数时，用户的认证器可以使攻破密钥像因子分解（例如 RSA）或者离散对数（例如 DSA 或 ECDSA）一样难。
2. 一旦针对某种攻击的对策就位，攻击者就可能会转向其他类型的攻击。
3. 攻击分类的序号并不代表相关攻击的排名，例如攻击类型（4）不一定比攻击类型（3）更难。
4. 攻击类型（1）的可行性根本不受用户影响。这使得这种攻击类型特别糟糕。
5. 与攻击类型（5）（6）相关的物理安全概念（例如保护你的认证器不被窃取）比攻击类型（2）（3）（4）相关的逻辑安全的概念更容易被用户接受。
6. 为了防止鉴别会话被滥用（例如 MITB 浏览器中间人攻击），FIDO 认证器必须支持交易确认的概念，而且依赖方必须使用。
7. 任意一种攻击都足以令攻击者得手。

4. UAF 安全目标

本节介绍 UAF 的具体的安全目标。FIDO UAF 协议[UAFProtocol]支持不同类型的 FIDO 认证器，即使认证器的安全性不同，UAF 协议和 FIDO 服务器也该提供较高的安全等级，至少在概念层上应该如此。现实中，为了完全利用 UAF 的安全优势，需要 FIDO 认证器具有高安全级别。

注释

在一些环境下，显式身份鉴别（由 FIDO 提供）的整体安全变得不那么重要，因为可以由高级别的隐式身份鉴别所补充，或者应用不需要高强度的身份鉴别。

FIDO U2F 协议[U2F Overview]对支持的认证器性能做出了更多限制，除了[SG-14]交易非抵赖性外，它与 UAF 共享相同的安全目标。UAF 协议的安全目标如下：

[SG-1]

强用户鉴别：高强度地鉴别到依赖方的用户和设备。

[SG-2]

抗凭证猜测：提供强大的抗窃听保护，例如*抗物理观察，抗针对性的仿冒，抗有限制和无限制猜测*。

[SG-3]

抗凭证泄露：抗*钓鱼攻击*和实时钓鱼攻击，包括抗可主动操控网络流量的攻击者发动的在线攻击。

[SG-4]

不可链接性：保护协议会话，确保任意两个依赖方不能将会话关联到某一个用户（例如*不可链接*）。

[SG-5]

抗验证者泄露：抗*其他依赖方泄露*，例如，验证者泄露的任何信息都不能帮助攻击者在另一依赖方仿冒用户。

[SG-6]

抗认证器泄露：抗其他 FIDO 认证器泄露，例如，某个特定认证器泄露的任何信息都不能帮助攻击者在另一依赖方仿冒用户。

[SG-7]

用户许可：在与新的依赖方建立关系前通知用户（*需要明确的许可*）。

[SG-8]

受限的个人识别信息：将暴露给依赖方的个人识别信息限制在绝对最小值。

[SG-9]

鉴证属性：依赖方必须能够验证 FIDO 认证器的型号/类型（为了计算相关的风险）。

[SG-10]

抗拒绝服务：抗*拒绝服务攻击*，例如防止攻击者在合法用户下一次登录时插入无效的注册信息，之后合法用户就再也不能成功登录了。

[SG-11]

抗伪造：抗*伪造攻击（仿冒攻击）*，例如防止攻击者尝试修改截获的通讯

来假装合法用户登入系统。

[SG-12]

抗并行会话：抗*并行会话攻击*。在不知道用户鉴别凭证的情况下，攻击者可以通过监听用户和服务器之间的交互生成一个合法的鉴别消息伪装成合法用户。

[SG-13]

抗转发：抗*转发和重放攻击*。通过截获以前的通信，攻击者可以冒充合法用户来鉴别登陆到系统。攻击者能够重放或者转发截获的消息。

[SG-14]

交易的不可抵赖性：对安全交易提供强加密不可抵赖性。

[SG-15]

遵守操作环境安全边界：根据 FIDO 用户设备上的操作环境的权限边界，确保作为共享系统资源的注册和密钥材料处于合理保护状态。

> 注释
>
> 部分斜体打印的专业术语可参见[QuestToReplacePasswords] 和 [PasswordAuthSchemesKeyIssues]。

4.1 要保护的资产

不依赖于任何特定的实现，UAF 协议认为一些资产需要描述并且进行保护。

1. 加密鉴别密钥。通常情况下，FIDO 中的密钥对于每一个三元组（依赖方，用户账户，认证器）是唯一的。
2. 加密鉴别密钥参考。这是存储在依赖方的加密材料，用于唯一地校验加密鉴别密钥，通常是非对称密钥对的公钥。
3. 认证器鉴证密钥（存储在认证器）。该密钥只能用于鉴证加密鉴别密钥、认证器的类型和生产批次。为了防止认证器成为跨依赖方的可链接标识符，鉴证密钥和证书被某个供应商大量生产的某一类设备中的认证器所共享。认证器鉴证证书可以是自签名的，也可以是供应商控制的授权密钥签名的。
4. 认证器鉴证授权密钥。认证器供应商可以用每个供应商的证书授权密

钥来对认证器鉴证证书签名。

5. 认证器鉴证授权证书。作为 FIDO 服务器的一部分保存在默认的可信存储中或者保存在每个依赖方的活跃可信存储中。
6. 活跃可信存储。包含某个给定的 FIDO 服务器的所有可信的鉴证主证书。
7. 适用于跨依赖方的可唯一识别认证器的所有数据，攻击这些数据可以破坏不可链接性的安全目标。
8. 依赖方 TLS 服务器证书的私钥。
9. 用户浏览器或应用的 TLS 根证书可信存储。

5. FIDO 安全措施

> 注释
>
> FIDO 客户端、认证器、服务器和参与的应用在具体实现中可能不会实现所有的安全措施（例如安全显示和[SM-10]交易确认），也可能会（并且应该）实现额外的安全措施。

> 注释
>
> U2F 协议缺少对 [SM-5] 安全显示和[SM-10]交易确认的支持，只有服务器提供的[SM-8]协议随机数，并且由于只有一个单独的设备类别，[SM-3]认证器类别鉴证是隐含的。

[SM-1] (U2F + UAF)

密钥保护：保护鉴别密钥以防滥用。用户可以解锁存储在 FIDO 认证器（静默认证器除外）的加密鉴别密钥。

[SM-2] (U2F + UAF)

唯一鉴别密钥：加密鉴别密钥对于一个三元组（FIDO 认证器，用户，依赖方）是唯一的。

[SM-3] (U2F + UAF)

认证器类别鉴证：基于硬件的 FIDO 认证器通过共享鉴证证书来支持认证器鉴证。每个依赖方通过鉴证服务接收可信存储的定期更新。

[SM-4] (UAF)

认证器状态检测：认证器或认证器鉴别密钥遭到入侵后必须通知依赖方。FIDO 服务器必须考虑这些信息。认证器遭到入侵后认证器制造商必须通知 FIDO 联盟。

[SM-5] (UAF)

用户许可：FIDO 客户端实现用户界面，为了得到用户对某些动作（使用静默认证器的鉴别除外）的许可和显示依赖方的名称（来源于服务器 URL）。

[SM-6] (U2F + UAF)

加密的安全验证者数据库：依赖方只存储非对称密钥对的公共部分或者加密的密钥句柄，作为加密鉴别密钥参考。

[SM-7] (U2F + UAF)

服务器鉴别的安全信道：服务器鉴别的 TLS 协议或等效传输用于 UAF 的传输层协议。浏览器或依赖方应用强制使用 https。

[SM-8] (UAF)

协议随机数：UAF 注册和鉴别过程中都使用服务器和客户端提供随机数。U2F 需要服务器提供随机数。

[SM-9] (U2F + UAF)

认证器认证：只有满足 FIDO 联盟定义的认证需求和准确描述相关特征的认证器，其相关鉴别密钥会保存在默认的可信存储中。

[SM-10] (UAF)

交易确认（所见即所签）：FIDO 客户端用 FIDO 认证器实施的安全显示（所见即所签）（可选项）来显示用户要确认的依赖方名称和交易数据。

[SM-11] (U2F + UAF)

往返完整性：FIDO 服务器验证来自 FIDO 客户端的 UAF 消息中交易数据及相关的服务器挑战值，与 UAF 请求信息中的交易数据和服务器挑战值相同。

[SM-12] (U2F + UAF)

通道绑定：依赖方服务器要验证与客户端应用之间安全通道的连续性。

[SM-13] (UAF)

密钥句柄访问令牌：不在非可信系统间漫游的认证器可以根据用户设备的操作环境定义的特权边界来约束用户注册密钥的使用（每用户、 或每个应用程序、或每用户及每个应用程序，视情况而定）

[SM-14] (U2F + UAF)

信任类型列表：依赖方能够声明可以访问注册密钥的应用程序标识，前提是用户设备的操作环境支持这种概念。

[SM-15] (U2F + UAF)

签名计数器：认证器发送单调递增的签名计数器，依赖方使用计数器有可能检测出克隆认证器。

5.1 安全措施和安全目标的关系

安全目标	支持的安全措施
[SG-1]强用户鉴别	[SM-1]密钥保护 [SM-12]通道绑定 [SM-14]可信类型列表 [SM-15]签名计数器
[SG-2]抗凭证猜测	[SM-1]密钥保护 [SM-6]加密的安全验证者数据库
[SG-3]抗凭证泄露	[SM-1]密钥保护 [SM-9]认证器认证 [SM-15]签名计数器
[SG-4]不可链接性	[SM-2]唯一鉴别密钥 [SM-3]认证器类别鉴证
[SG-5]抗验证者泄露	[SM-2]唯一鉴别密钥 [SM-6]加密的安全验证者数据库
[SG-6]抗认证器泄露	[SM-9]认证器认证 [SM-15]签名计数器
[SG-7]用户许可	[SM-1]密钥保护

	[SM-5]用户许可 [SM-7]服务器鉴别的安全信道 [SM-10]交易确认 (所见即所签)
[SG-8]受限的个人识别信息	[SM-2]唯一鉴别密钥
[SG-9]鉴证属性	[SM-3]认证器类别鉴证 [SM-4]认证器状态检查 [SM-9]认证器认证
[SG-10]抗拒绝服务	[SM-8]协议随机数
[SG-11]抗伪造	[SM-7]服务器鉴别的安全信道 [SM-8]协议随机数 [SM-11]往返完整性 [SM-12]通道绑定
[SG-12]抗并行会话	[SM-7]服务器鉴别的安全信道 [SM-8]协议随机数 [SM-11]往返完整性 [SM-12]通道绑定
[SG-13]抗转发	[SM-7]服务器鉴别的安全信道 [SM-8]协议随机数 [SM-11]往返完整性 [SM-12]通道绑定
[SG-14]交易的不可抵赖性	[SM-1]密钥保护 [SM-2]唯一鉴别密钥 [SM-8]协议随机数 [SM-9]认证器认证 [SM-10]交易确认 (所见即所签) [SM-11]往返完整性 [SM-12]通道绑定
[SG-15]遵守操作环境安全边界	[SM-13]密钥句柄访问令牌 [SM-14]信任类型列表

6. UAF 安全假定

现在的计算机系统和加密算法都无法被证明是安全的。本节，我们列出一些安全性假定，例如，其他组件提供的安全性假定。违反任意的假定都会阻碍安全目标的实现。

[SA-1]

目前使用的加密算法和参数（密钥大小，模式，输出长度等）不受未知的弱点的控制，这些未知的弱点使得它们不符合加密、数字签名和鉴别消息的用途。

[SA-2]

参与在用户设备上执行 FIDO 操作的软件模块依赖于操作系统特权分离机制。例如，用户和内核模式之间的边界，用户账户之间的边界，应用之间的边界都安全地实施，安全主体能够相互安全识别。

[SA-3]

用户设备上的应用可以通过建立安全通道来保障可信的服务器鉴别以及消息的保密性和完整性。（例如通过 TLS）

[SA-4]

安全显示的实现是受保护的以免遭受欺诈和篡改。

[SA-5]

FIDO 用户设备的计算环境和参与 FIDO 操作的应用一起扮演了可信用户代理的角色。

[SA-6]

加密密钥的内在价值体现在它被赋予的信任，随着时间推移信任会减弱，与任何损害事件无关。因此认证器的有效保证级别会随时间推移而降低。

[SA-7]

参与处理 FIDO 操作的依赖方计算资源扮演了可信依赖方代理的角色。

6.1 讨论

对于[SA-5]和在 FIDO 用户设备上的恶意计算，在假定的范围内只能做有限的

保证。恶意代码在可信计算基础层的特权总是违反[SA-2]和[SA-3]。恶意代码在传统多用户环境中的用户账户层的特权也可以违反[SA-3]。

当用户选择故意违反[SA-5]时 FIDO 只能提供有限的防护。例如漫游 USB 认证器在一个不可信系统（如公共服务终端）使用或在移动环境为恶意程序授权访问所有鉴别密钥。交易确认可以作为防护泄露的 FIDO 用户设备的方法。

由认证器和软硬件混合的模块组成了类似于 FIDO 客户端、服务器等组件。端到端的安全目标依赖于其他参与组件（包括网页浏览器和依赖方应用程序）正确的实施和遵守 FIDO 安全指导。一些配置和使用可能与安全目标相违背。例如，认证器不具备安全显示功能，认证器仅有未认证的软件组件，认证器故意设计为在不可信操作环境中漫游，并且一些操作环境可能没有提供所有必要的安全基元。（例如：安全 IPC、应用程序隔离、现代 TLS 实现等）

7. 威胁分析

7.1 客户端威胁分析

7.1.1 利用用户模式匹配的弱点

T-1.1.1	**同形异义的误注册**	**违反**
AC3	用户在欺诈网站而不是真实的依赖方注册 FIDO 鉴别密钥。 **结果：**欺诈网站可能会让用户泄露一系列非 FIDO 凭证的信息，这些信息足以让攻击者在真实的依赖方注册 FIDO 认证器并由他自己控制，这违反了[SG-1]强用户认证。 **解决方法：**非 FIDO 凭证的泄露是在 FIDO 安全措施范围之外的,但是依赖方应该意识到鉴别密钥的初始强度不比注册过程中进行身份核实更好。	SG-1

7.1.2 用户设备、FIDO 客户端和依赖方客户端应用的威胁

T-1.2.1	FIDO 客户端攻击	违反
AC3	攻击者得到了在 FIDO 客户端的安全环境中执行代码的权限。 **结果：**违反了[SA-5]. **解决方案：**如果 FIDO 用户设备的操作环境允许，FIDO 客户端应该在[SA-2]的权限和隔离环境下操作，以保护自身免受可信计算基以外的恶意修改。	SA-5

T-1.2.2	逻辑/物理用户设备攻击	违反
AC3/AC5	攻击者得到了 FIDO 用户设备而不是 FIDO 认证器的访问权限。 **结果：**可能会安装恶意应用或篡改 FIDO 用户设备，违反了[SA-5]. **解决方案：**当 FIDO 用户设备被临时入侵时，[SM-1]密钥保护防止认证密钥和其他信息的泄露。 针对 FIDO 用户设备的持久入侵可导致违反[SA-5]，除非对 FIDO 用户设备实施 FIDO 范围外的保护措施。（例如全盘加密和启动链完整性）	SA-5

T-1.2.3	用户设备账户访问	违反
AC3/AC4	攻击者得到了 FIDO 用户设备的用户登录凭证的访问权。 **结果：**认证器可能被远程滥用，弱验证认证器可能在本地被滥用，违反了[SG-1]强用户认证和[SG-13]交易非抵赖性。 可能因为安装恶意应用导致违反[SA-5]. **解决方案：**依赖方可以用[SM-9]认证器认证和[SM-3] 认证器类别鉴证来决定认证器的性质，对于高价值操作不依靠弱的或弱验证的认证器。	SG-1，SG-13，SA-5

T-1.2.4	应用服务器验证错误	违反
AC3	客户端应用没有成功地验证远程服务器的身份，接受了伪造的或者窃取的远程服务器证书，或者允许弱的或丢失的安全信道的加密保护。 **结果：**活跃的网络攻击者可以修改依赖方的鉴别策略并且对客户选择的认证器降级从而使攻击变得更容易。 活跃的网络攻击者可以截获或窥探用于依赖方的 FIDO 消息。这样将违反[SG-12]抗并行会话、[SG-11]抗伪造或者[SG-13]抗转发。 **解决方案：**服务器可以验证[SM-8]协议随机数来检测重放消息并且可以对抗在安全信道上可读取但是不能修改通信流量的攻击者。 服务器可以授权一个强加密保护的信道来避免消息伪造，并且可以校验[SM-12]通道绑定来检测转发消息。	SG-11 ，SG-12 ，SG-13

T-1.2.5	依赖方网页应用破坏	违反
AC3	攻击者可以在依赖方应用的安全环境中执行恶意代码（例如通过跨站脚本），或者在用户成功鉴别之后滥用安全通道或会话标识符。 **结果：**攻击者可以控制用户的会话，违反了[SG-14]交易的不可抵赖性。 **解决方案：**针对高价值操作，服务器可以使用[SM-10]交易确认来获取额外确认。	SG-14

T-1.2.6	辨别认证器	违反
AC3	远程攻击者可以通过 FIDO 认证器上可发现的配置的特征来唯一标识一台 FIDO 用户设备 **结果：**暴露的信息违反了[SG-8] 受限的个人识别信息，攻击者在不了解用户的情况下强认证用户违反[SG-7]用	SG-4，SG-7，SG-8

	户许可，共享特征违反了[SG-4]不可链接性。 **解决方案：**[SM-3]认证器类别鉴证确保每个认证器的特征不唯一。 对于威胁最突出的网页浏览情况来说，用户代理可以在 FIDO 认证器的可发现性之外提供额外的用户控制。	

T-1.2.7	**应用到 FIDO 客户端的中间人攻击**	**违反**
AC3	FIDO 用户设备上的恶意软件可以读取、篡改、欺骗 FIDO 客户端和浏览器或依赖方程序的进程间通信信道的端点。 **结果：**攻击者可以破坏[SA-2]。 **解决方案：**[SA-2]不强壮的平台上，系统的安全可能依赖于阻止恶意程序到达 FIDO 用户设备上。这样的保护，例如应用商店策略，是在 FIDO 范围之外的。 当使用[SM-10]交易确认时，用户可以看到相关的 AppID 和交易内容以决定是否接受某项操作。	SA-2

T-1.2.8	**认证器到应用的只读中间人攻击**	**违反**
AC3	攻击者可以获取认证器的签名协议响应报文。 **结果：**攻击者尝试使用重放消息仿冒用户鉴别，违反了[SG-1]强用户认证，[SG-13] 抗转发[SG-12] 抗并行会话。 **解决方案：**服务器可以通过[SM-8]协议随机数来检测报文重放，通过验证[SM-11]往返完整性来发现被修改的消息。	SG-1， SG-12， SG-13

T-1.2.9	**恶意应用**	**违反**
AC3	用户安装一个代表自己与依赖方应用相关联的应用，但是事实上初始化了一个与不同的依赖方的协议会话，而且试	SG-7

	图滥用之前在依赖方注册的鉴别密钥。 **结果：**攻击者可以通过歪曲鉴别目标违反[SG-7]用户许可。其他结果与[T-1.2.5]相同。 **解决方案：**如果[SM-5]交易确认是存在的，用户可以确认操作的真实目标。 如果恶意应用尝试直接与采用[SM-13]密钥句柄访问令牌的认证器通信，其应该不能访问其他 FIDO 客户端注册的密钥。 如果 FIDO 用户设备上的操作环境支持，FIDO 客户端可以确定应用程序标识并且验证它是否被使用[SM-14]信任类型列表的依赖方授权。	

T-1.2.10	**网络钓鱼攻击**	**违反**
	钓鱼者诱骗用户在一个应用或者网页输入自己的用户验证 PIN 码，这些信息将发送给钓鱼者。在传统的用户名/密码场景下，这种攻击可以成功的仿冒用户。 **结果：**钓鱼者不需要额外的东西就可以通过用户验证[SM-1]访问认证器。在 FIDO 中，依赖方不知道用户验证 PIN 码（如果用户通过 PIN 码验证），因此用户模拟是不充分的。这也适用于用户使用其他的用户验证方法。 **解决方案：**在 FIDO 中，用户鉴别私钥用于对依赖方提供的挑战签名。不能访问密钥就不能仿冒用户。	

7.1.3 创建虚假客户端

T-1.3.1	**恶意 FIDO 客户端**	**违反**
AC3	攻击者诱骗用户安装和使用恶意的 FIDO 客户端。 **结果：**违反了[SA-5]。	SA-5

	解决方案：解决恶意软件的安装超出了 FIDO 的范围。 如果认证器支持[SM-1]密钥保护，用户可以通过从设备删除恶意软件来恢复对注册鉴别密钥的完全控制。 当应用[SM-10]交易确认时，用户可以看到真实的 AppID 和交易信息以决定接受或拒绝这个操作。	

7.1.4 对 FIDO 认证器的威胁

T-1.4.1	**恶意认证器**	**违反**
AC2	攻击者诱骗用户使用恶意安装的认证器。 **结果：**假的认证器没有执行适当的安全措施，会违反 FIDO 的所有安全目标。 **解决方案：**用户可能不能辨别出恶意认证器，但是依赖方可以用[SM-3]认证器类别鉴证来识别和允许那些通过了[SM-9]认证器认证的可信认证器的注册。 依赖方可以依靠[SM-4]认证器状态检查来核对恶意认证器提交的鉴证是否被标记为被盗用的。	SG-1

T-1.4.2	**用户私钥的破解**	**违反**
AC2	攻击者成功地抽取用户的加密鉴别密钥用于不同的环境中。 **结果：**攻击者可以用克隆的认证器仿冒用户，克隆的认证器不能进行可信的用户验证，违反了[SG-1]。 **解决方案：**[SM-1]密钥保护措施用来防止这类攻击。 依赖方可以检查[SM-9]认证器认证属性来决定给定的认证器类使用的密钥保护的类型。 如果认证器在做前置操作有过失败时，依赖方可以通过验证[SM-15]签名计数器来检测认证器是否被克隆。	SG-1

T-1.4.3	**旁路用户验证**	**违反**

AC3	在通知或不通知合法用户情况下，攻击者可以用加密鉴别密钥（在认证器中）。 **结果：**攻击者可以仿冒用户，违反了[SG-1]。 **解决方案：**用户只能注册并且依赖方也只允许特定的认证器，这类认证器通过提供适当安全的用户验证过程来实现[SM-1]密钥保护。 不适用于静默认证器。	SG-1

T-1.4.4	**物理认证器攻击**	**违反**
AC5/6	攻击者可以获得 FIDO 认证器的物理访问（例如窃取）。 **结果：**为了使用鉴别密钥，攻击者可以发起离线攻击。如果离线攻击成功，攻击者可以成功仿冒用户，违反了[SG-1]强用户认证。 攻击者可以引入低熵值的情景来复原 ECDSA 签名密钥（或者提取用户私钥），如果目标是鉴证密钥，就违反了[SG-9]鉴证属性，如果用户密钥是目标，就违反了[SG-1]强用户认证。 **解决方案：**[SM-1]密钥保护包括对密钥材料实施强保护的需要，包括抗离线攻击和低熵场景。 依赖方应该使用[SM-3] 认证器类别鉴证来只接受实施强用户鉴别方法的认证器。	SG-1

T-1.4.6	**伪认证器**	**违反**
	攻击者可以从认证器处提取认证器鉴证密钥，例如通过在实验室环境下使实质性对抗手段无效。 **结果：**攻击者可以通过创建一个合法的代表自己的恶意硬件或者软件设备，这违背了[SG-9]鉴证属性。 **解决方案：**依赖方可以用[SM-4]认证器状态检查来找出	SG-9

	已知泄露的密钥。找出这样的密钥超出了 FIDO 协议的严格范围。	

T-1.4.7	**交易确认显示覆盖攻击**	**违反**
	攻击者可以破坏[SM-5]安全显示功能（所见即所签），可能用错误的信息覆盖。 **结果：**这违背了[SG-14]。 **解决方案：**在安全显示的实施中，必须保护[SA-4]，例如在用户设备的操作环境下，通过实现明显的硬件显示或者使用合理权限来防止欺诈和篡改。 [SM-9]认证器认证提供给依赖方关于交易确认显示信息的元数据，交易确认显示信息可以用来评定依赖方针对特定交易的保障水平和风险承受能力是否匹配。	SG-14

T-1.4.8	**签名算法攻击**	**违反**
AC2	密码攻击是为了对付由 FIDO 认证器用于数据签名的公钥加密系统。 **结果：**攻击者可以用客户端产生的消息违反[SG-2]抗凭证猜测。 **解决方案：**[SM-8]协议随机数，包括客户端产生的熵，限制了攻击者对于认证器内部结构的控制量。 非静默认证器的[SM-1]密钥保护需要用户使用鉴别密钥交互授权才能进行任何操作，严格限制攻击者可以执行自适应加密攻击的比率。	SG-2

T-1.4.9	**功能滥用**	**违反**
	攻击者有可能通过向认证器发送不正确的参数或不正确的命令来滥用认证器功能。 **结果：**可能会导致例如用户旁路确认或者潜在的密钥提	SG-1

	取。 **解决方案：**适当的（例如归功于测试）认证器固件鲁棒性。	

T-1.4.10	**随机数预测**	**违反**
	攻击者有可能获取能够预测随机数发生器数据的信息。 **结果：**当使用 ECDSA 时（k 值重复使用或可以预测时），可能会导致密钥泄露的情形（T-1.4.2）。 **解决方案：**适当的认证器随机数发生器的鲁棒性和相关操作环境参数的验证。	SG-1

T-1.4.11	**固件回滚**	**违反**
	攻击者有可能安装之前版本的或者有潜在问题版本的固件。 **结果：**可能会导致成功攻击，例如 T-1.4.9。 **解决方案：**适当的固件鲁棒性验证方法。	SG-1

T-1.4.12	**用户验证数据注入**	**违反**
AC3/6	攻击者有可能向认证器注入之前抓取的用户确认数据。例如，如果口令是用于用户验证的方法，攻击者可以捕获用户输入的口令，之后发送正确的口令给认证器（绕过预期的键盘/PIN 键盘）。口令要在攻击前捕获，例如通过让用户输入口令到恶意应用（钓鱼攻击）或者直接或间接获取口令数据。 在另外一个例子中，一些恶意软件可以播放麦克风录制的音频流，该音频流可以在基于声音识别的认证器使用。 **结果：**如果攻击者可以访问有效的用户确认数据，可能会导致成功的用户仿冒。	SG-1

	解决方案：使用物理安全的用户验证输入方法，例如指纹传感器或有可信用户界面用于输入 PIN，这些都是不能被恶意软件绕过的。	

T-1.4.13	**验证参考数据修改**	**违反**
AC3/6	攻击者获取了对认证器的物理访问权限并且修改存储在认证器处的验证参考数据（例如 PIN 哈希值）或增加攻击者知道（复写）的参考数据。 **结果：**攻击者会被认为是合法用户，可以仿冒用户。 **解决方案：**对认证器处的验证参考数据进行适当保护。	SG-1

7.2 对依赖方的威胁

7.2.1 对 FIDO 服务器数据的威胁

T-2.1.1	**FIDO 服务器数据库读攻击**	**违反**
AC2	攻击者可以获取 FIDO 服务器注册数据库的读权限。 **结果：**攻击者可以访问所有的加密密钥句柄和与用户名相关的认证器特征。如果认证器或认证器组合是唯一的，这可能会违反[SG-4]不可链接性。 攻击者尝试执行对有权限访问的大数据集的公钥的因式分解，这违反了[SG-5] 抗验证者泄露和[SG-2] 抗凭证猜测。 **解决方案：**即使攻击成功，[SM-2]唯一鉴别密钥帮助防止公开的密钥材料在其他依赖方使用。 使用[SM-6]加密的安全验证者数据库帮助确保攻击任何泄露的验证者密钥是不可行的。 [SM-9] 认证器认证可以防止低熵的认证器进入市场，减少大量密钥材料集在安装攻击中被利用的可能性。	SG-2，SG-5

T-2.1.2	FIDO 服务器数据库修改攻击	违反
	攻击者可以获取 FIDO 服务器注册数据库的写权限。 **结果：**违反[SA-7]。 攻击者可以在其控制下注入注册密钥，违反[SG-1]强用户鉴别。 **解决方案：**缓解这些攻击超出了 FIDO 规范的范围。作为[SA-7]的一部分，依赖方必须维护用户识别信息的完整性。	SA-7

T-2.2.1	恶意网页应用	违反
	攻击者可以在依赖方网页应用或 FIDO 服务器的安全环境下执行代码。 **结果：**攻击者会违反[SG-1]，[SG-10]，[SG-9]和其他的依赖方控制。 **解决方案：**这种事件通过[SM-1]、[SM-2]、[SM-5]，其结果对用户和特定依赖方之前的关系影响有限。 即使在依赖方与用户的关系中，如果用户的计算环境未泄露，可以通过[SM-10]交易确认来保护用户。	SG-1，SG-9，SG-10

7.3 对客户端和依赖方间的安全信道的威胁

7.3.1 利用 FIDO 信息安全传输的弱点

FIDO 把[SA-3]用户设备上的应用能够建立安全信道作为基准假定，安全信道提供可信的服务器鉴别、消息的保密性和完整性，例如通过 TLS。[T-1.2.4]讨论了因为在浏览器或客户端应用上实施错误从而违反这个假定的后果，但是其他威胁存在于不同层。

T-3.1.1	TLS 代理	违反
	FIDO 用户设备配置为通过代理连接，该配置终止了 TLS 连接。虽然用户信任该设备，但是用户与 FIDO 服务器之	SG-11 ，SG-12 ，

	间已经不再是端到端的安全连接了。 **结果：**这样的代理引入新的一方到协议里。如果这方是不可信的，结果可能像[T-1.2.4]描述的一样。 **解决方案：**[T-1.2.4]的解决方案可以应用过来，除了客户端认为代理是可信的，[SM-12]通道绑定中的一些方法可以在没有攻击的情况下标明泄露的通道。服务器应该使用多种方法并适当地调整其风险评分。可信客户端上报未知的并且未链接到公共根的服务器证书可以表明该客户端在这样的代理之后。客户端上报未知的服务器证书，但是可以根据常用的公众信任的根验证服务器身份，更可能表明为[T-3.1.2]的问题。	SG-13

T-3.1.2	**欺骗的 TLS 服务器证书**	**违反**
	攻击者可能通过泄露的认证机构或防护措施简单的依赖方获取到依赖方证书的控制权。 **结果：**与[T-1.2.4]相同。 **解决方案：**与[T-1.2.4]相同。	

T-3.1.3	**协议级实时中间人攻击**	**违反**
	攻击者可以拦截和操作依赖方发送给客户端的网络包。攻击者用这种能力来（a）结束低层的客户端的 TLS 会话（b）同时在攻击者与依赖方之间建立 TLS 会话。在传统的用户名/口令环境中，这允许攻击者拦截用户名和口令，然后成功地在依赖方仿冒用户。 **结果：**如果使用[SM-12]FIDO 通道绑定和[SM-10]交易确认，就不会有什么影响。 **解决方案：**如果使用[SM-12]通道绑定，FIDO 服务器会在 TLS 通道中比较客户端提供的通道绑定信息和从服务器提取的通道绑定信息来检测中间人攻击。	

	如果使用[SM-10]交易确认，用户确认并同意一项交易。攻击者能在同意前修改交易，这会导致用户的拒绝。攻击者可以在用户批准后修改交易，但这会破坏交易确认响应的签名。FIDO 服务器不会接受它。	

7.4 对基础设施的威胁

7.4.1 对 FIDO 认证器制造商的威胁

T-4.1.1	**制造商级鉴证密钥泄露**	**违反**
	攻击者可以得到鉴证密钥或者鉴证密钥的分发密钥的控制权。 **结果：**与[T-1.4.6]相同，攻击者通过创建恶意的硬件或者软件设备来代表自己的合法身份，这违反了[SG-9]鉴证属性。 **解决方案：**与[T-1.4.6]相同，依赖方可以用[SM-4]认证器状态检查来找出已知的泄露密钥。找出泄露的密钥超出了 FIDO 协议的严格范围。	SG-9

T-4.1.2	**制造商级的鉴别密钥泄露**	**违反**
	FIDO 认证器制造商依靠产生弱加密鉴别密钥材料或包含后门的硬件或软件组件。 **结果：**违反了[SA-1]。 **解决方案：**[SM-9] 认证器认证的过程可能会揭示这种威胁的子集，但这是不可行的，因为所有集合都可以通过黑盒测试和白盒检查来揭示，但在经济上不可行。关心这类威胁的用户和依赖方必须提高供应商和供应链的可信度和确信度。	SA-1

7.4.2 对 FIDO 服务器供应商的威胁

T-4.2.1	供应商级的可信锚注入攻击	违反
	攻击者向 FIDO 服务器供应商提供的可信列表中加入恶意可信锚。 **结果：**攻击者可以使用依赖方不能检测到的、不执行安全措施的、能够违反所有的 FIDO 安全目标的假认证器。 **解决方案：**这种供应链类型的威胁超出了 FIDO 协议的严格范围，并违反了[SA-7]。依赖方可以检查可信列表来和 FIDO 联盟发布的定义数据进行比较。	SA-7

7.4.3 对 FIDO 元数据服务运营商的威胁

T-4.3.1	元数据服务签名密钥攻击	违反
	攻击者可以访问私有元数据签名密钥。 **结果：**攻击者可以对无效的元数据签名。攻击者可以让可信的认证器看起来不那么可信（例如，通过提高误报率）；让弱认证器看起来很强（把密钥保护方法改得更安全）；注入恶意鉴证可信锚，例如对原始鉴证可信锚进行交叉签名的根证书。恶意可信锚可以用来对虚假认证器的鉴证证书签名，例如认证器用可信认证器的 AAID 而不是保护元数据中描述的密钥。 **解决方案：**元数据服务运营商应该合理保护元数据签名密钥，例如用硬件保护的密钥存储。 依赖方可以用带外方法与独立的供应商交叉检查元数据描述，与元数据服务的提供者交叉检查元数据签名密钥的吊销状态。	SG-9

T-4.3.2	元数据服务数据注入	违反
	攻击者注入恶意认证器数据到元数据源。 **结果：**攻击者可以让元数据服务操作员对无效的元数据签名。攻击者可以让可信的认证器看起来不那么可信	SG-9

	（例如通过提高误报率）； 让弱认证器看起来很强（把密钥保护方法改得更安全）； 注入恶意确认可信锚，例如对原始确认可信锚进行交叉签名的根证书。恶意可信锚可以用来对虚假认证器的确认证书签名，例如认证器用可信认证器的 AAID 而不是保护元数据中描述的密钥。 **解决方案：**元数据服务运营商可以仔细检查新旧元数据的增量。认证器供应商可以验证与认证器相关的已公布的元数据。	

7.5 对特定 U2F 的威胁

T-5.1.1	**错误状态边信道**	**违反**
	依赖方向认证器发出鉴别挑战，如果认证器已经被注册则可以推断出错误状态。 **结果：**不需要用户交互的 U2F 认证器可在没有用户许可的情况下追踪用户，通过分配一个预认证挑战给 U2F 令牌，暴露出另外的匿名用户的身份。依赖方在没有他们信息的情况下就可以识别用户，违反了[SG-7]。 **解决方案：**U2F 规范建议浏览器提示用户是否允许使用与定位等隐私敏感操作类似的操作机制。	SG-7

T-5.1.2	**恶意依赖方**	**违反**
	恶意依赖方在它存储的密钥句柄上实施加密攻击。 **结果：**U2F 没有协议级的[SG-14] 交易的不可抵赖性的说明。但是如果依赖方可以恢复密钥句柄的内容，它可能会通过伪造协议交换的日志来把用户与他没有执行的操作相联系。 如果依赖方能恢复加密密钥句柄的密钥，那这个密钥可	

	能是共享的，可以用来解密其他依赖方存储的密钥句柄，违反了[SG-1]强用户认证。 **解决方案：**无。U2F 依赖于[SA-1]来进行密钥包裹操作。	

T-5.1.3	**物理 U2F 认证器攻击**	**违反**
	攻击者可以得到 U2F 认证器的物理访问权限，例如偷到它。 **结果：**与 T-1.4.4 相同。 U2F 认证器的本地用户核实能力很低。如果攻击者可以猜测用户名和口令/PIN 码，他们就可以仿冒用户，违反了[SG-1]强用户鉴别。 **解决方案：**依赖方可以使用额外的强因子。 依赖方应该给用户提供一种注销丢失设备密钥的方法。	SG-1

8. 致谢

感谢 iSECpartners 对本文档的检查和贡献。

A. 参考文献

A.1 参考资料

[FIDOGlossary]

R. Lindemann, D. Baghdasaryan, B. Hill, J. Hodges, FIDO Technical Glossary. FIDO Alliance Proposed Standard. URLs:

HTML: fido-glossary-v1.0-ps-20141208.html

PDF: fido-glossary-v1.0-ps-20141208.pdf

[PasswordAuthSchemesKeyIssues]

Chwei-Shyong Tsai, Cheng-Chi Lee, and Min-Shiang Hwang, Password Authentication Schemes: Current Status and Key Issues, International Journal of Network Security, Vol.3, No.2, PP.101–115, Sept. 2006, URL: http://ijns.femto.com.tw/contents/ijns-v3-n2/ijns-2006-v3-n2-p101-115.pdf

[QuestToReplacePasswords]

Joseph Bonneau, Cormac Herley, Paul C. van Oorschot and Frank Stajano, The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes, Microsoft Research, Carleton University and University of Cambridge, March 2012, URL:http://research.microsoft.com/pubs/161585/QuestToReplacePasswords.pdf

[RFC2119]

S. Bradner. Key words for use in RFCs to Indicate Requirement Levels. March 1997. Best Current Practice. URL: https://tools.ietf.org/html/rfc2119

[U2FOverview]

S. Srinivas, D. Balfanz, E. Tiffany, FIDO U2F Overview v1.0. FIDO Alliance Review Draft (Work in progress.) URL: http://fidoalliance.org/specs/fido-u2f-overview-v1.0-rd-20140209.pdf

[UAFProtocol]

R. Lindemann, D. Baghdasaryan, E. Tiffany, D. Balfanz, B. Hill, J. Hodges, FIDO UAF Protocol Specification v1.0. FIDO Alliance Proposed Standard. URLs:

HTML: fido-uaf-protocol-v1.0-ps-20141208.html

PDF: fido-uaf-protocol-v1.0-ps-20141208.pdf