Knowledge Transfer Office

香港城市大學
City University of Hong Kong

基于浏览器的恶意扩展防护安全框架

通信和信息

计算机/人工智能/数据处理和信息技术

其他

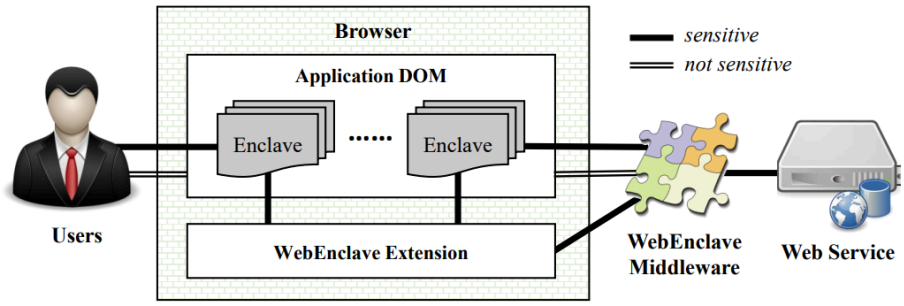

图1 WebEnclave整体架构

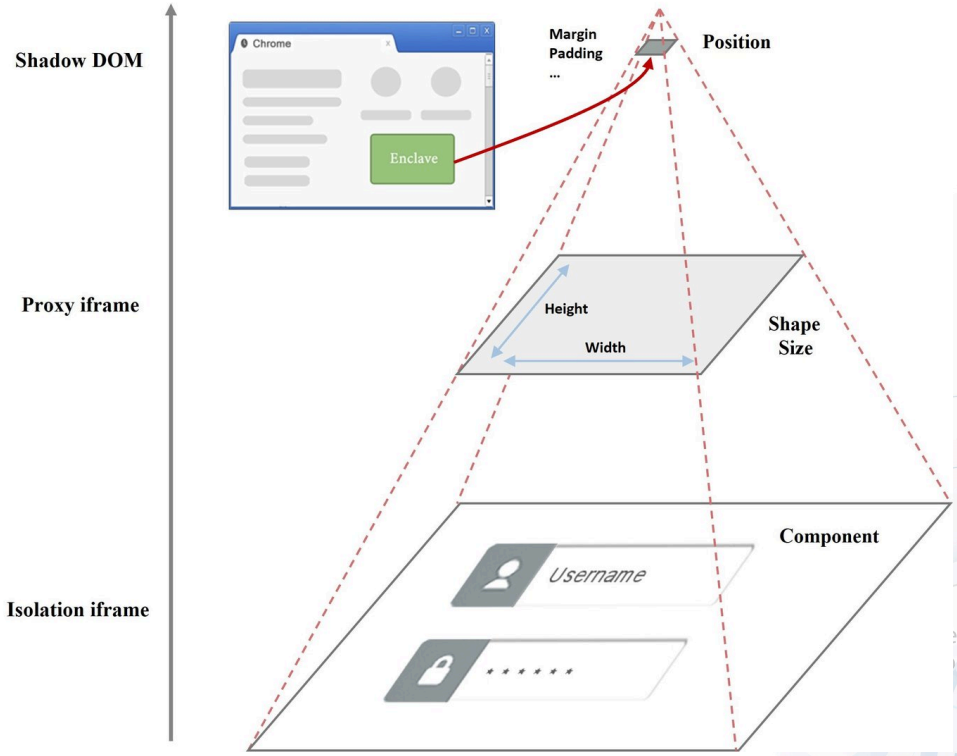

图 2 使用安全区隔离敏感组件以防御恶意扩展

IP状态
专利已授权

技术成熟度等级 (TRL) 5

发明人

王聪教授

杜越风

王新宇

詢問： kto@cityu.edu.hk

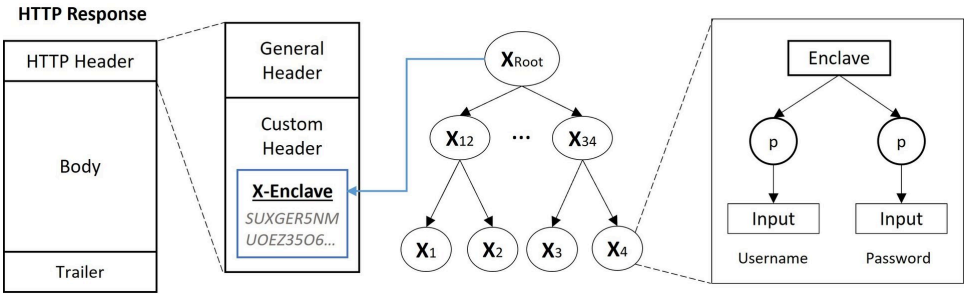

图 3 在整个生命周期内对隔离区域进行完整性检查，以防止未经授权的对抗性修改。

机会

越来越多的人通过安装搜索工具栏、广告拦截器和密码管理器来个性化他们的浏览体验。然而，这些扩展也带来了安全和隐私问题，因为它们对敏感用户数据具有特权访问，这些数据可能被用来发起复杂的网络攻击。因此，迫切需要保护庞大且不断增长的互联网用户免受浏览器扩展恶意行为的侵害。现有的安全机制无法覆盖可以在任何时候读取和写入Web应用程序的扩展，甚至最先进的检测方法也无法追踪恶意扩展迅速演变的行为。为了创造一个更安全的浏览环境，研究人员开发了一种新颖的安全框架，通过将敏感用户信息封闭在恶意扩展无法访问的“隔离区”中来保护Web应用程序上的敏感数据。

技术

WebEnclave是第一个基于浏览器的框架，在Web应用程序开发者的支持下保护用户免受具有完全特权的浏览器扩展的恶意行为。该发明由三个主要组成部分构成： 1. 一个JavaScript库，帮助开发者构建安全的Web应用程序；2. 一个中间件，使Web应用程序提供者能够方便地部署新颖的安全机制； 3. 一个浏览器扩展，使个人用户能够隔离并保护Web应用程序上的敏感数据。WebEnclave的重要特征是一个软件隔离区的安全区域，Web应用程序提供者可以在其中封闭敏感数据，防止恶意浏览器扩展窃取或篡改用户信息。实际上，WebEnclave提供用户友好且精细的应用程序接口，使开发者能够隔离Web应用程序中特定的敏感部分进行保护，同时保留其原始功能和外观。用户无需依赖特定硬件或安装修改过的浏览器即可享受该发明的安全保障。他们还可以根据需求在安全性与功能性之间找到平衡，例如在浏览需要完全功能的浏览器扩展的网站时禁用保护。

优势

- 据研究人员所知，WebEnclave是第一个基于浏览器的解决方案，保护Web应用程序的敏感部分免受具有完全特权的浏览器扩展的恶意行为。它没有直接竞争对手。
- 与其少数间接竞争对手（如Fidelius和Protection）不同，WebEnclave不需要特定的硬件配置。
- 与Fidelius等竞争对手不同，WebEnclave不会通过改变Web应用程序的用户界面或行为来影响用户的浏览体验。

应用

- 该设计和算法可以出售给浏览器厂商，以增强他们面对越来越复杂的网络攻击时防御恶意浏览器扩展的能力。
- 对于普通用户，WebEnclave扩展模板可以很容易地安装在现代浏览器上，使他们确信自己的秘密得到保护。
- 基于Web的银行服务可以使用WebEnclave来保护敏感的金融数据和操作，而不会损害用户体验。
- 在线广告商可以使用这一技术拒绝浏览器扩展对在线产品和服务广告的拦截，从而吸引更多潜在客户并增加利润。