Password Managers: Attacks and Defenses

王凯

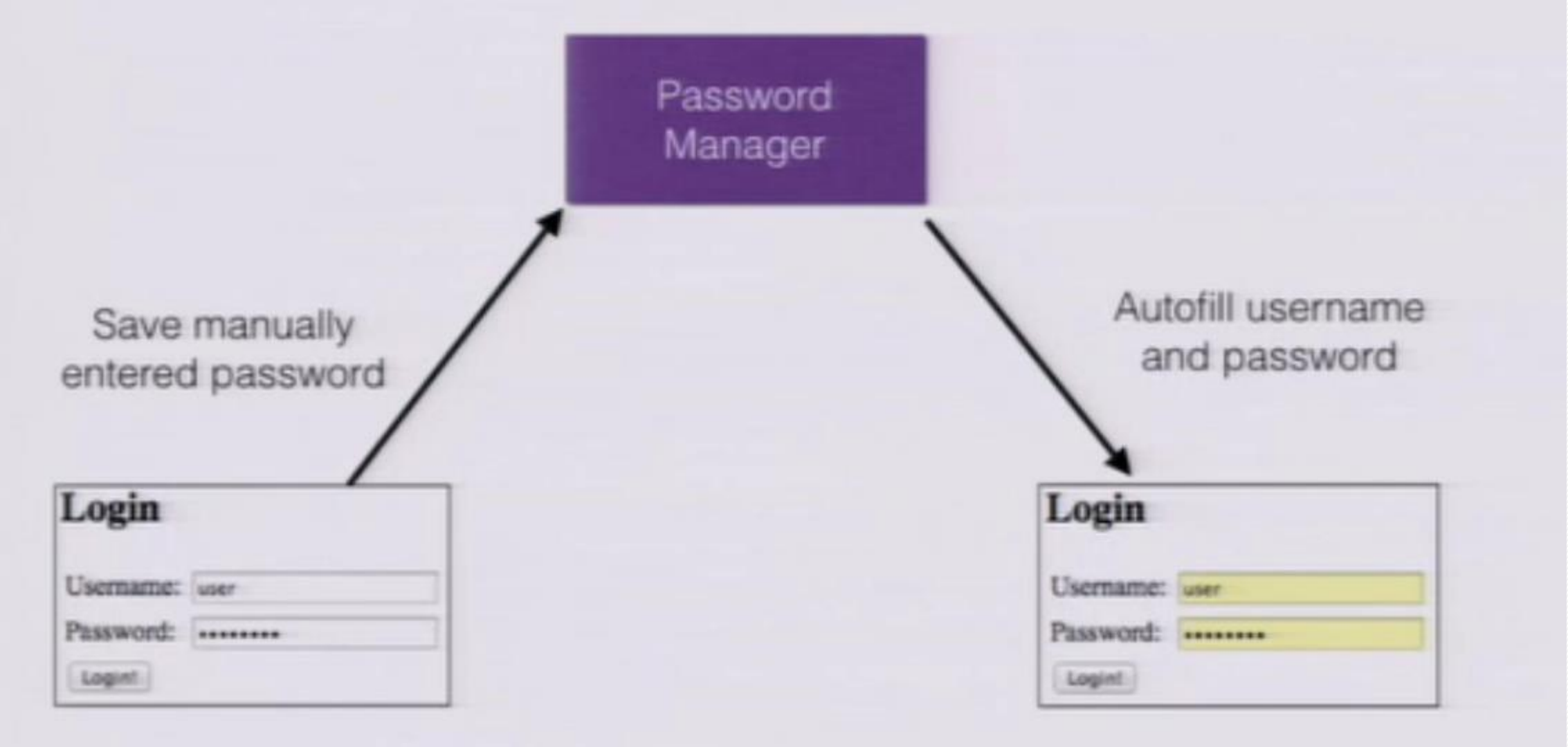
2016.10.12

A tool for…

Convenience?

Security?

Password Manager Workflow

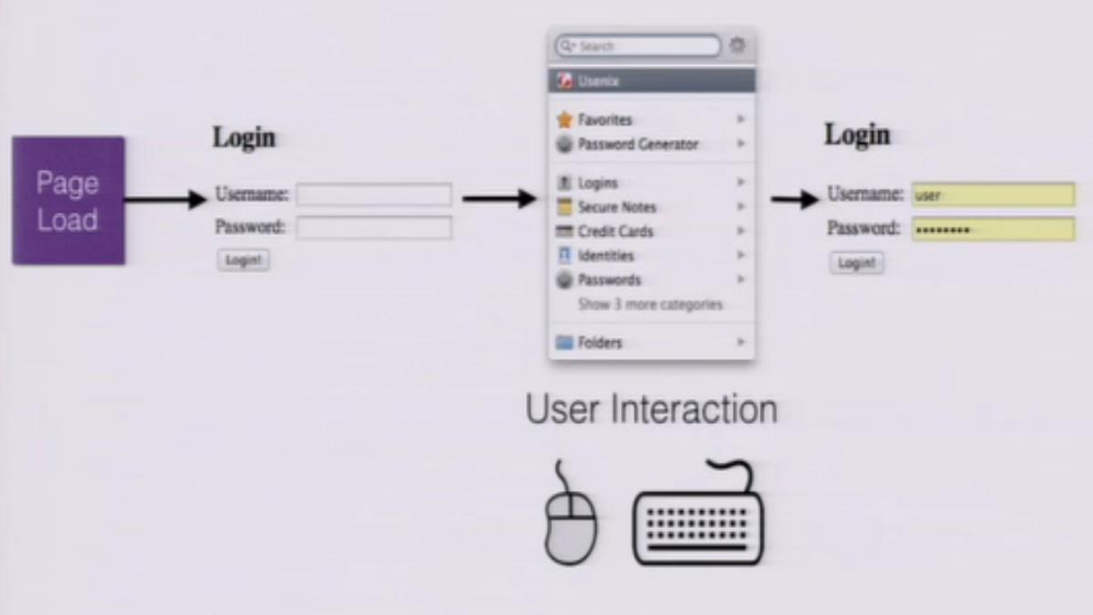


1.Automatic autofill

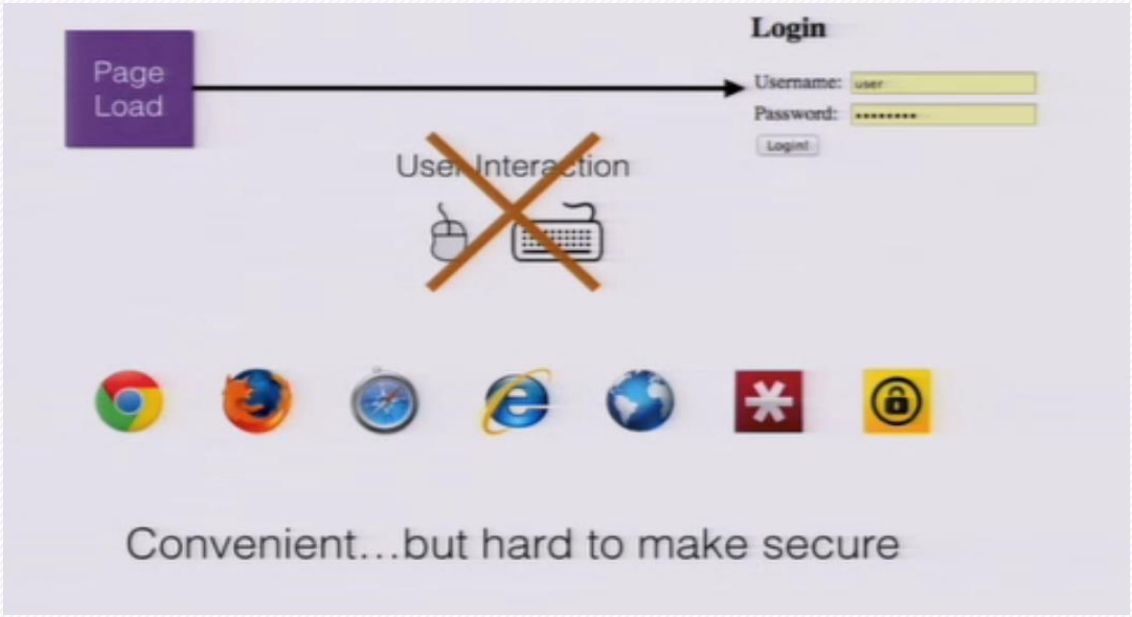
2.Manual autofill

3.A hybrid approach

Manual Autofill



Automatic Autofill



口令管理软件

1.基于桌面浏览器的口令管理软件（chrome，IE，Firefox）

2.第三方口令管理软件（1Password，LastPass）

3.IOS 口令管理（云同步）

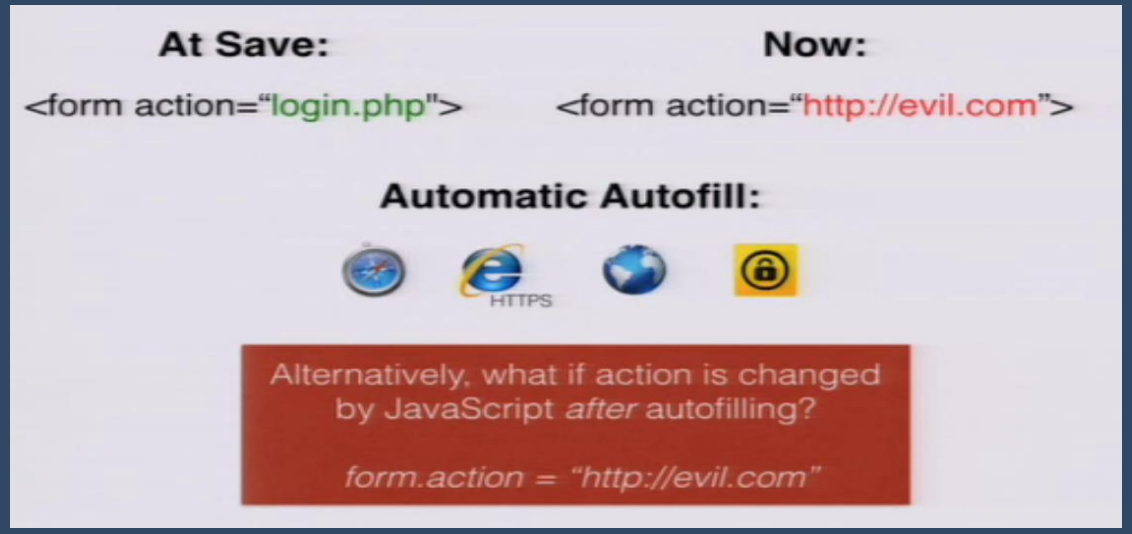
4.Android 口令管理（默认浏览器）

口令填写策略存在的风险

1.只要主域名相同，即可自动填表。（ https://www.example.com/aaa. php https://www.example.com/bbb. php ）

2.HTTP与HTTPS：如果当前提交表单的协议与口令第一次保存时的协议不一致，时则存在风险。（chrome,safari,firefox,IE 拒绝自动填表）

3.Action属性：表单的action决定了表单内容将提交至何处，所以攻击者可以注入javascript代码，修改action属性。软件会降级为手动填写，但不会给用户提示Action属性是否改变。



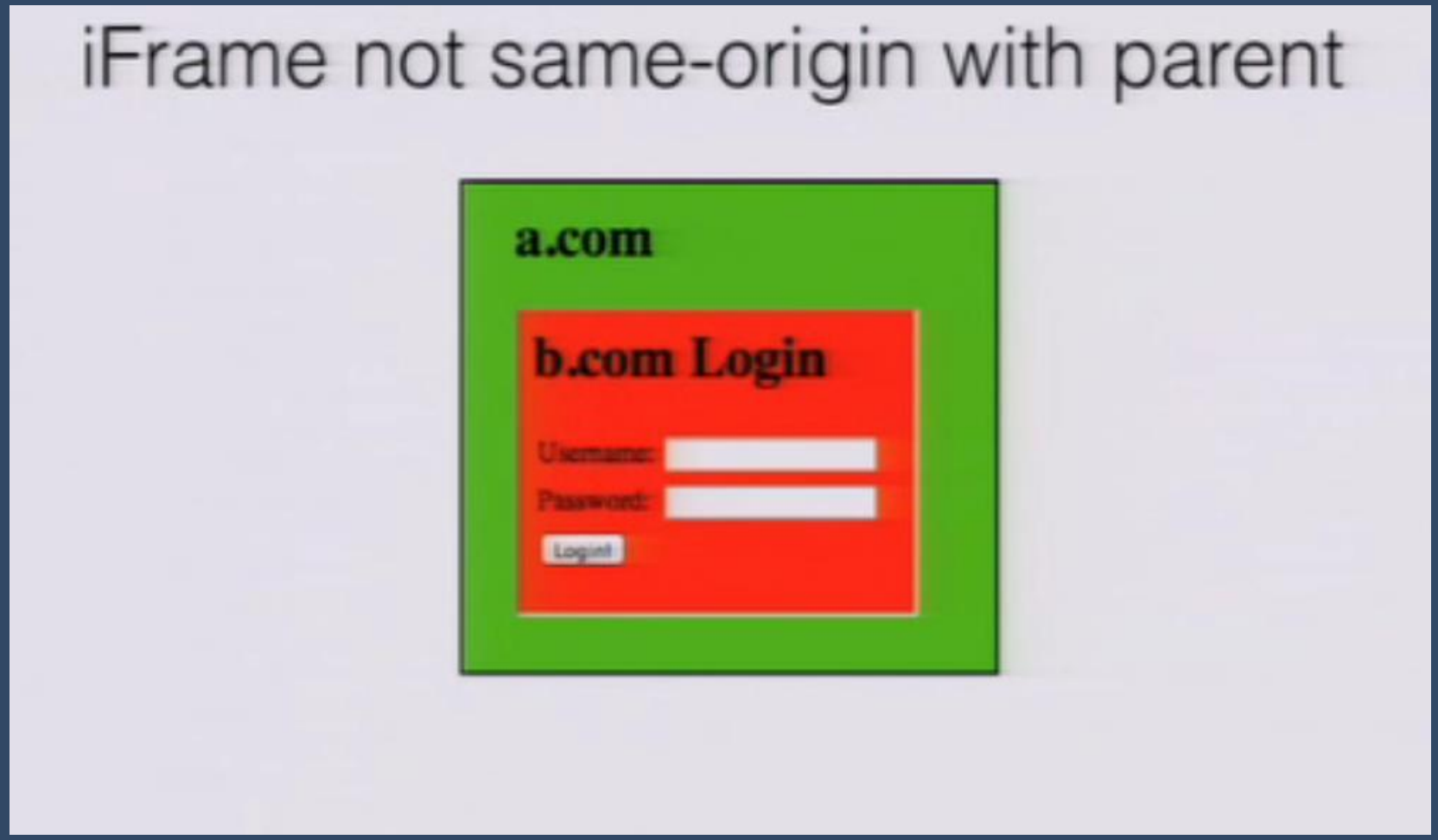
口令填写策略存在的风险

4.Autocomplete属性：当 Autocomplete 属性赋值off时，主流软件既不会自动填写口令，也不会保存当前口令。

5.HTTP的session被破坏时，会出现证书警告。Chrome拒绝填写口令，IE将自动填表降级为手动填表。其他软件忽略警告。

口令填写策略存在的风险

6.iFrame autofill



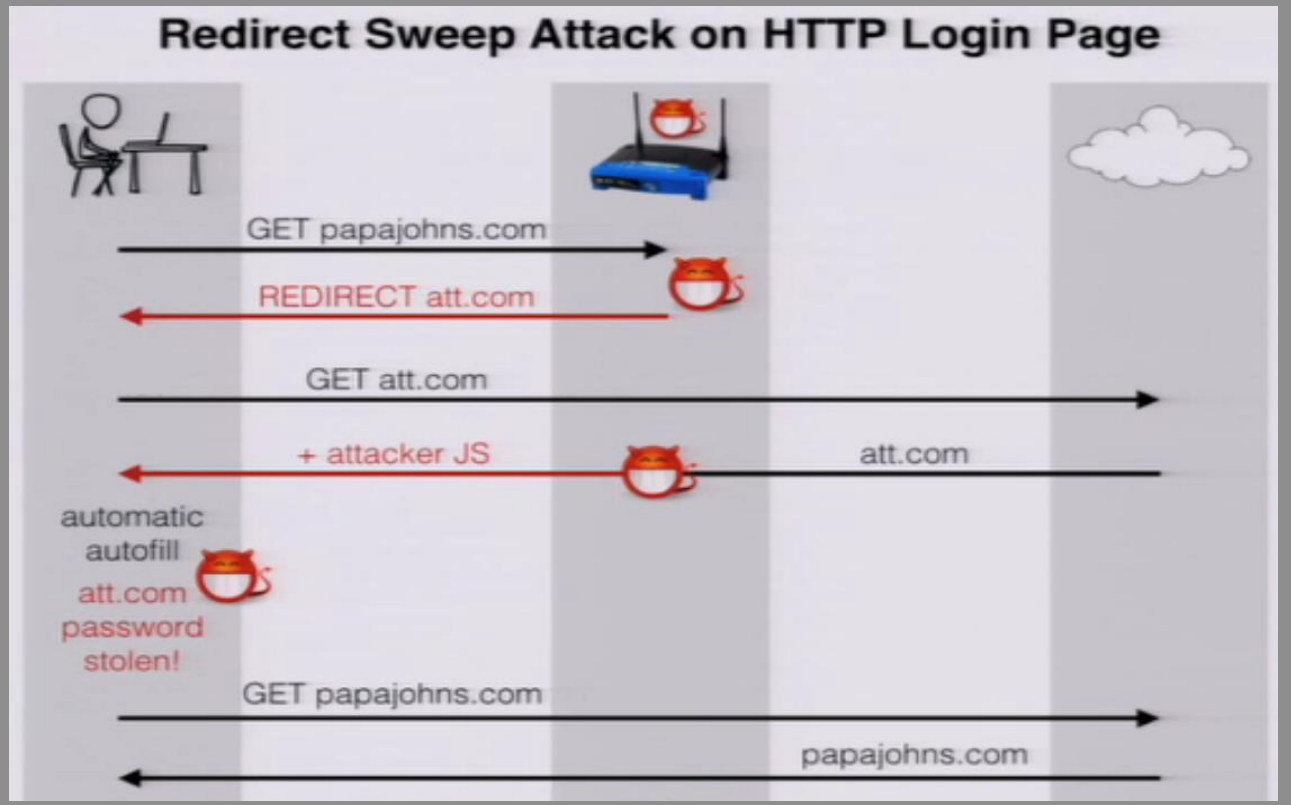
Attacks

1.Sweep attacks : iFrame , Windows, Redirect

2.Injection Techniques : HTTP login page

3.Attacks that need user interaction

攻击方法---Redirect扫描攻击



防御方法

1.用户的交互，可以有效阻止扫描攻击。在HTTP协议已被破坏的网站，软件应该总是拒绝自动填写口令。

2.安全填充策略：

1.第一次存储口令时，也存储action属性。

2.当口令管理软件自动填写口令时，将输入框的内容变为不可读。

3.正在填充口令时，如果输入框被修改，停止自动填写并清除已填写内容。

4.提交前检验当前action和存储的action是否一致，若不一致，则清除口令，停止提交。

结论：

自动填写口令策略有很多特殊情况。

扫描攻击：在没有用户交互的情况下进行口令窃取。

防御：

1.填充口令前需要用户交互

2.安全填充

思考和感想

口令管理软件在提供便捷的同时仍存在安全隐患，平衡好两者是一个重要的问题。

口令管理存在的有些问题不是技术问题而是策略上的问题。（Secure filling就是在策略上使口令更安全）

THANKS!