Usando Estilos de Conferencia con LaTeX

Nauman

June 11, 2020

Abstract

Este es un texto abstracto. Esto se ha incluido solo para demostración. Es por eso que se mantiene breve.

1 Introducción

Texto de introducción aquí. Los teléfonos inteligentes se utilizan cada vez más para almacenar información personal, así como para acceder a datos confidenciales desde Internet y la nube. El establecimiento de la identidad de un usuario que solicita información de teléfonos inteligentes es un requisito previo para sistemas seguros en tales escenarios. En el pasado, la identificación de usuario basada en pulsaciones de teclas se ha implementado con éxito en dispositivos móviles de nivel de producción para mitigar los riesgos asociados con la autenticación ingenua basada en nombre de usuario/contraseña. Sin embargo, estos enfoques tienen dos limitaciones principales: no son aplicables a los servicios donde la autenticación se produce fuera del dominio del dispositivo móvil tal como servicios basados en la web; y a menudo agravan demasiado las capacidades computacionales limitadas de los dispositivos móviles. En este artículo, proponemos un protocolo para el análisis dinámico de la pulsación de teclas que permite que las aplicaciones basadas en la web utilicen la certificación remota y el análisis delegado de pulsaciones de teclas. El resultado final es un mecanismo eficiente de identificación de usuarios basado en la pulsación de teclas que fortalece los servicios tradicionales protegidos por contraseña mientras mitiga los riesgos de la creación de perfiles de usuario mediante la colaboración de servicios web maliciosas. Presentamos una implementación prototipo de nuestro protocolo usando el popular sistema operativo Android para teléfonos inteligentes.

2 Antecedentes

Texto de introducción aquí. Los teléfonos inteligentes se utilizan cada vez más para almacenar información personal, así como para acceder a datos confidenciales desde Internet y la nube. El establecimiento de la identidad de un usuario que solicita información de teléfonos inteligentes es un requisito previo para sistemas seguros en tales escenarios. En el pasado, la identificación de usuario

basada en pulsaciones de teclas se ha implementado con éxito en dispositivos móviles de nivel de producción para mitigar los riesgos asociados con la autenticación ingenua basada en nombre de usuario/contraseña. Sin embargo, estos enfoques tienen dos limitaciones principales: no son aplicables a los servicios donde la autenticación se produce fuera del dominio del dispositivo móvil tal como servicios basados en la web; y a menudo agravan demasiado las capacidades computacionales limitadas de los dispositivos móviles. En este artículo, proponemos un protocolo para el análisis dinámico de la pulsación de teclas que permite que las aplicaciones basadas en la web utilicen la certificación remota y el análisis delegado de pulsaciones de teclas. El resultado final es un mecanismo eficiente de identificación de usuarios basado en la pulsación de teclas que fortalece los servicios tradicionales protegidos por contraseña mientras mitiga los riesgos de la creación de perfiles de usuario mediante la colaboración de servicios web maliciosas. Presentamos una implementación prototipo de nuestro protocolo usando el popular sistema operativo Android para teléfonos inteligentes.

2.1 Algunos trabajos relacionados

El establecimiento de la identidad de un usuario que solicita información de teléfonos inteligentes es un requisito previo para sistemas seguros en tales escenarios. En el pasado, la identificación de usuario basada en pulsaciones de teclas se ha implementado con éxito en dispositivos móviles de nivel de producción para mitigar los riesgos asociados con la autenticación ingenua basada en nombre de usuario/contraseña. Sin embargo, estos enfoques tienen dos limitaciones principales: no son aplicables a los servicios donde la autenticación se produce fuera del dominio del dispositivo móvil tal como servicios basados en la web; y a menudo gravan demasiado las capacidades computacionales limitadas de los dispositivos móviles. En este artículo, proponemos un protocolo para el análisis dinámico de la pulsación de teclas que permite que las aplicaciones basadas en la web utilicen la certificación remota y el análisis delegado de pulsaciones de teclas.

3 Conclusiones

En el pasado, la identificación de usuario basada en pulsaciones de teclas se ha implementado con éxito en dispositivos móviles de nivel de producción para mitigar los riesgos asociados con la autenticación ingenua basada en nombre de usuario/contraseña. Sin embargo, estos enfoques tienen dos limitaciones principales: no son aplicables a los servicios donde la autenticación se produce fuera del dominio del dispositivo móvil como servicios basados en la web.