SENSOR-BASED MOBILE WEB FINGERPTINTING AND CROSS-SITE INPUT INFERENCE ATTACKS

Brandon David Meza Vargas - 3CV11

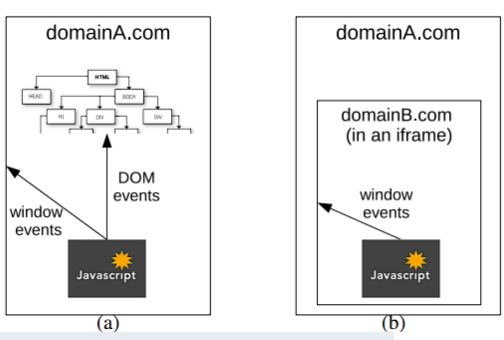
Los telefonos inteligentes han sido objetivo principal de cibercriminales.
Principalmente por los nuevos sensores que tienen hoy en día que abren las puertas a nuevos ataques ya que estos son accesibles por páginas web

Los 4 tipos de ataques

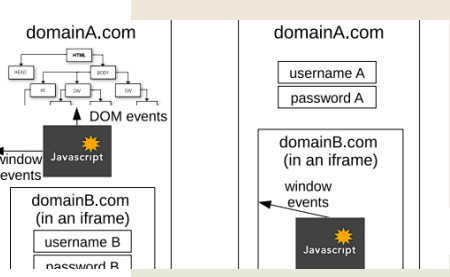
Se pueden identificar 4 tipos de ataques en los smartphones debido a la nula resticción para acceder a los sensores por medio de código javascript

- First-party user fingerprinting
- Third-party user fingerprinting
- Parent-to-child cross-site input inference
- child-to-parent cross-site input inference

User Fingerprinting Attacks



Estos ataques se presentan en los navegadores que usan los usuarios ya sea para un sitio first-party o third-party. Básicamente código Javascript registra eventos del dispositivo obteniendo la orientación del celular y datos de movimiento, de esta manera pueden obtener datos biométricos aunque las cookies esten deshabilitadas



Cross-site input inference attacks

AEstos ataques funcionan inyectando código Javascript que obtienen la orientación del dispositivo y movimiento que corresponde a escritura en teclado, de esta manera se crean modelos para inferir los datos sensibles que el usuario escribe

Efectividad de los ataques

Un problema en estos ataques es el identificar la fingerprint o las teclas que son tipadas por el usuario en un soft-keyboard. Una manera de solucionarlo es usando algoritmos de machine learning para el trabajo de identificación

Mecanismos de defensa

Un extremo es bloquear completamente el acceso a nuestros sensores de movimiento, aunque esto hará que perdamos funcionalidad. Otro extremo es siempre preguntar a nuestros usuarios si permiten o no el accesos a sus sensores.
Una solución potencial es agregar una nueva etiqueta HTML que restringa el acceso a los sensores en distintos elementos, por ejemplo un formulario.
Otra solución podría ser tener una configuración en el navegador para permitir decidir a los usuarios que paginas pueden acceder a sus sensores

Una última solución sería el que el navegador detecte los ataques específicos que pueden ocurrir analizando la relaciones de los frames y el registro de eventos y luego perturbar los datos para que la tarea de identificación de eventos sea más complicada.