



Detecção de Vazamentos de Dados em Aplicativos JavaScript em Dispositivos Móveis

Gustavo Ferreira da Silva

Sistema Operacional Tizen

- Código Aberto
- Desenvolvido pela Linux Foundation em parceria com um consórcio de empresas, entre elas: Samsung, Panasonic, Intel.

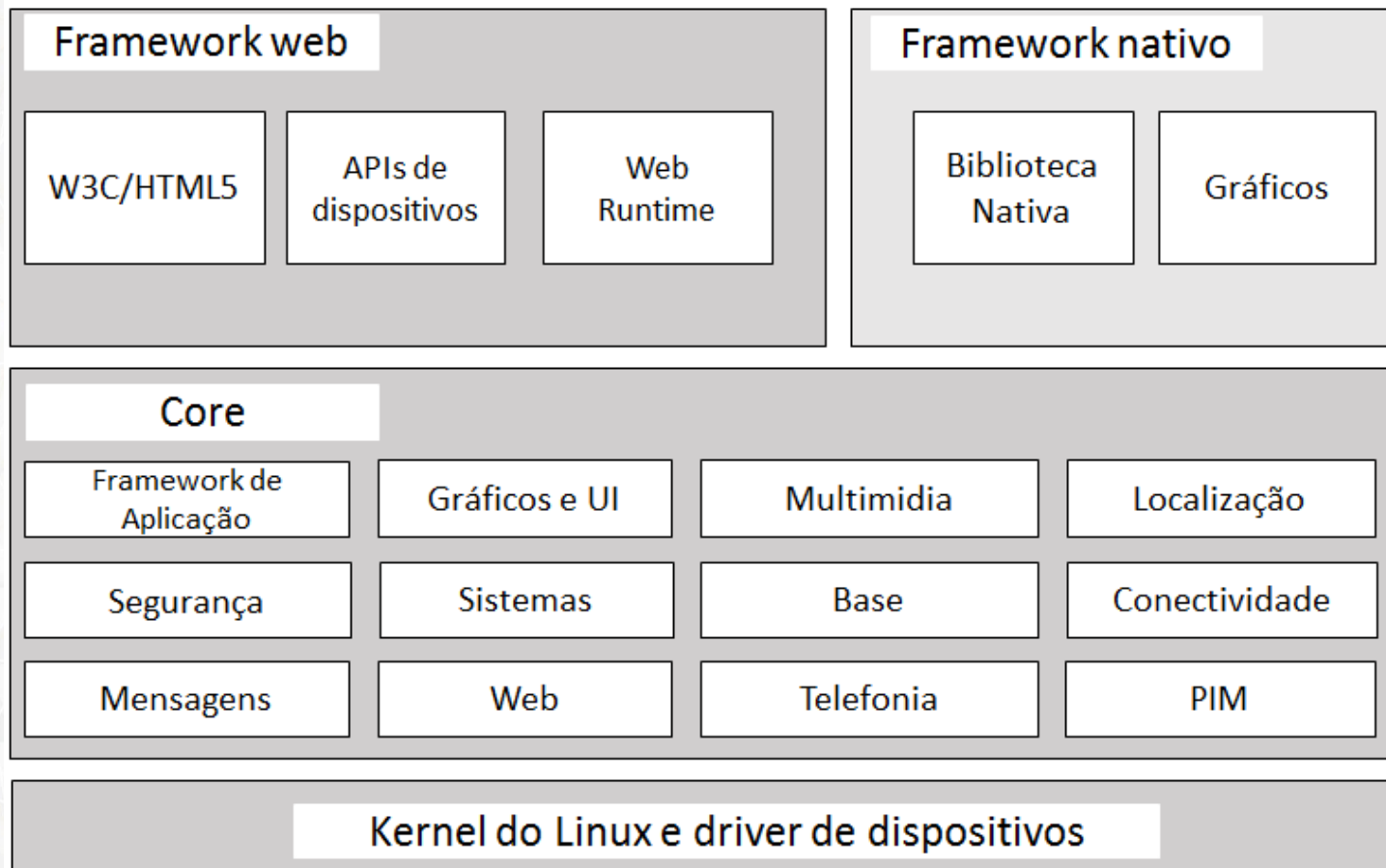
Aplicações do Tizen

The OS of Everything

Tizen is the open-source operating system for all device areas.



Arquitetura do Tizen



Tipos de Análise de Dados Sensíveis (Taint)

- Jasmine
- Estática
- Dinâmica

Conceitos de Análise Dinâmica

- Marcação (Taint)
- Fonte (Taint Source)
- Propagação (Taint Tracking)
- Saída (Taint Sink)

Tipos de Direção de Fluxo de Dados

- Implícito: Variável é afetada através de estruturas condicionais
- Explícito: Variável é passada diretamente entre valores.

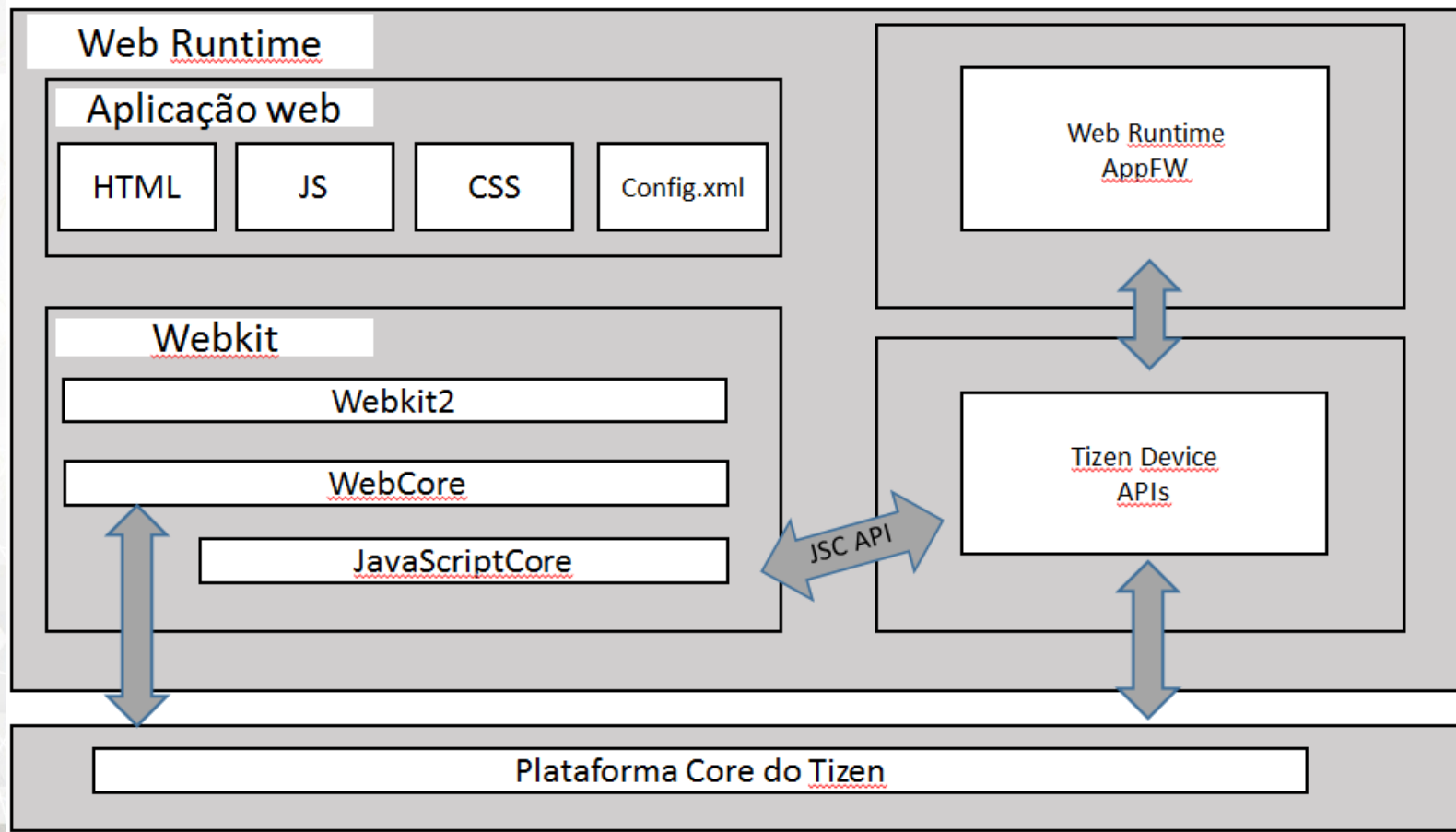
Exemplo de Análise Dinâmica

- Algoritmo 1
- 1: `c = source();`
- 2: `a = b+c;`
- 3: `send(a);`
- 4: ...

TTIZEN (Taint Tizen)

- Taint Source (Fonte)
- Taint Marking (Marcação)
- Taint Analysis
- Taint Sink

Web Runtime do Tizen



Identificação de Fontes

- API systeminfo
- Chamada da Função
- `getPropertyValue()`;
- `tizen.systeminfo.getPropertyValue`
(`<Informação>`, `<Função de Sucesso>`,
`<Função de Falha>`)

Propagação

- Bytecode gerado pelo JavaScriptCore
- /framework/web/webkit-efl/Source/JavaScriptCore/llint

Operações de Atribuição

- Operação mov
- mov <Reg>, <Valor>
- Reg – Registrador
- Valor – Valor a ser atribuído
-

Exemplo Operação mov

- function def() {
- var a = 5;
-
- }
- mov r1, @k1

Operação put_global_var

- put_global_var <Reg>, <Valor>
- var a = 5;
- function def() {
-
- }

Operação put_by_id

- Implementada em C
- Mapeamento explícito realizado pela JavaScriptCore

Operações de Retorno

- `var a = 5;`
- `var b = 6;`
- `var c = a + b;`

Operações de Retorno

- propagacao (Objeto $v_1, v_2, \dots, v_n$)
- Inicio
- resultado = operacao ($v_1, v_2, \dots, v_n$);
- Se estaMarcado($v_1, v_2, \dots, v_n$) então
- resultado.adicionaMarca()
- Fim se
- retorna resultado;
- Fim

Identificação de Saídas

- Classe Web Socket
- Verifica quando há uma saída HTTP
- Método send(): verifica marcação e gera o log.

My Observer

