UNIVERSIDAD DE LAS PALMAS DE GRAN CANARIA
Instituto Universitario de Microelectrónica Aplicada

Máster de Tecnologías de Telecomunicación

Trabajo Fin de Máster

Análisis y diseño de aceleradores hardware sobre SoC basados en FPGA orientados a aplicaciones de seguridad en Internet de las Cosas

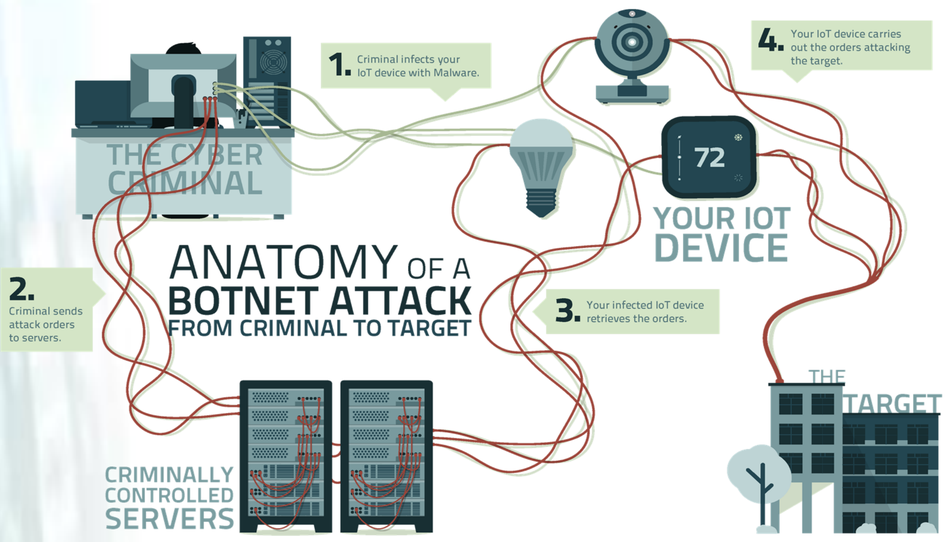
Yubal Barrios Alfaro

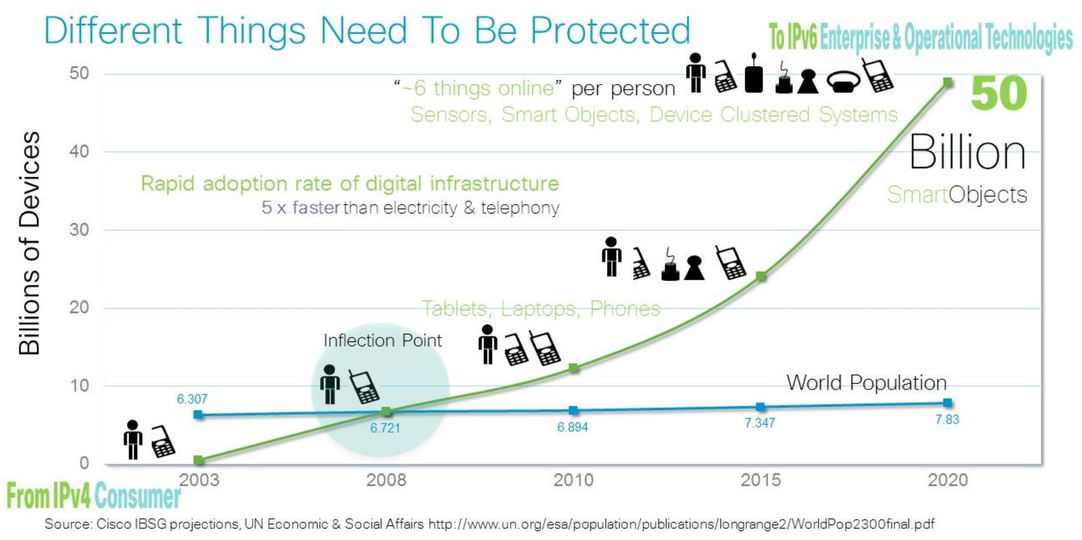
Pedro Pérez Carballo, Antonio Núñez Ordóñez

Julio de 2017

Resumen:

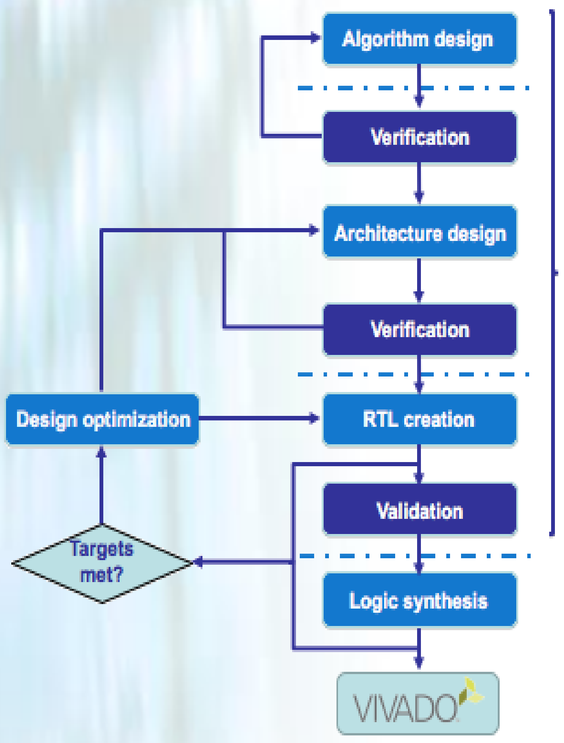
- El auge en el empleo de dispositivos IoT en la actualidad y la falta de regulación existente respecto a requisitos de seguridad que deben satisfacer, están conduciendo a la existencia de vulnerabilidades que comprometen la privacidad de la información de los usuarios.
- En el presente TFM se ha realizado el diseño de un sistema encargado de asegurar las comunicaciones recibidas por un nodo Fog.
- Se ha modelado en alto nivel una etapa de filtrado doble tanto a nivel de la capa de red como de la capa de transporte del modelo OSI, orientada a los protocolos de estos niveles empleados en una arquitectura de IoT (IPv6 y UDP, respectivamente).
- Con el fin de asegurar las comunicaciones, se ha diseñado un bloque de cifrado que implementa el algoritmo Simon, con una configuración de 64 bits de tamaño de palabra y una clave única de 42 palabras de 32 bits.





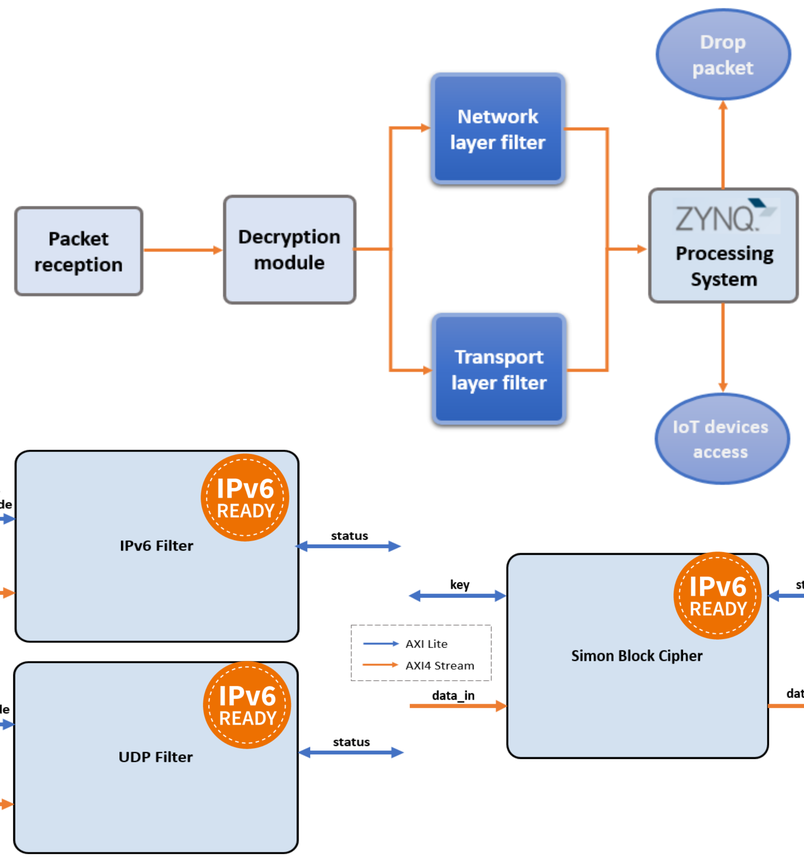
Flujo de diseño:

- El modelado de la funcionalidad de los bloques IP se ha realizado en alto nivel empleando Vivado HLS, obteniendo tras la etapa de síntesis la descripción RTL equivalente.
- Verificados los módulos creados, se realiza su integración con el resto de bloques que conforman el sistema final en Vivado, siguiendo una metodología de diseño basada en plataformas.



Arquitectura del sistema:

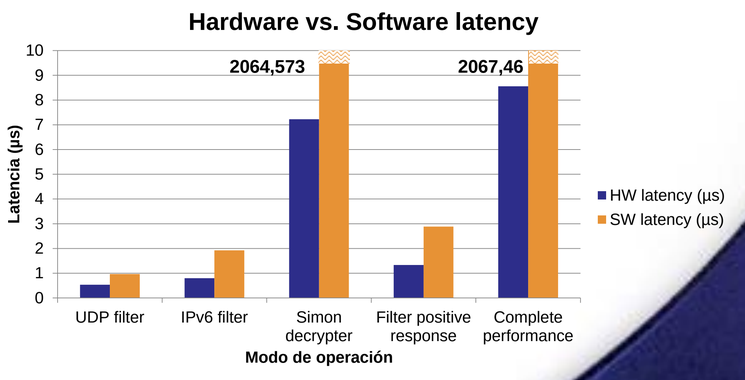
- El sistema consta de dos etapas bien diferenciadas: filtrado de paquetes Ethernet en función de parámetros de su cabecera y descifrado del *payload*.
- La implementación del sistema completo se ha realizado sobre un dispositivo Zynq Z-7020 de Xilinx, compuesto tanto por núcleos ARM como por una FPGA de la familia 7.



Resultados finales:

- En términos de latencia y consumo de recursos lógicos, se considera que los resultados medidos para las distintas etapas son satisfactorios, obteniendo una latencia total de **8,558 µs** y un consumo del **19,82%** del total de *slices* disponibles.
- En referencia al *throughput*, se alcanzan valores de casi **200 Mbps**, estando este parámetro limitado a la acción del bloque de descifrado.
- Adicionalmente, se ha realizado un estudio del consumo de potencia del sistema, aplicando optimizaciones orientadas a *low-power*.

	Slices	Frequency	Throughput
UDP filter	1,27%	277 MHz	3 Gbps
IPv6 filter	3,11%	229 MHz	2 Gbps
Simon decypter	2,58%	159 MHz	221,5 Mbps
Total System	**19,82%**	**150 MHz**	**187 Mbps**



Conclusiones:

- La solución alcanzada proporciona resultados satisfactorios en términos de PPA *(Power, Performance and Area)*.
- Se consigue un *speedup* de **x241** respecto a la versión puramente *software* del sistema, y un consumo de potencia de hasta dos órdenes de magnitud menor que un *host* destinado para la misma aplicación.
- El sistema final implementado presenta la suficiente robustez para evitar ataques comunes en entornos IoT, como DDoS o *Man-in-the-Middle*.

IUMA
Universidad de Las Palmas de Gran Canaria
Campus Universitario de Tafira
Las Palmas de Gran Canaria, SPAIN
tel.: +34 928451086
+34928451250
Fax: +34 928451083
URL: www.iuma.ulpgc.es