Publishable Executive Summary

WISDOM

(WIrespeed Security Domains using Optical Monitoring)

www.ist-wisdom.org

Type of instrument: STREP
Thematic Priority: IST call 5 FP6-2005-IST-5

Start date of project: 1st June 06
Duration: 36 months

Overview of the Project

WISDOM (Wirespeed Security Domains Using Optical Monitoring) is a 3 year, €1.9M funded project looking at developing novel optical processing modules which will be placed at the front end of a node firewall to provide the primary optical information filtering. Secondary processing would then be done electronically as is currently the case, but with the benefit of a reduction in the electronic processing capacity required.

These photonic firewalls will operate using novel algorithms and protocols, to extract and process wirespeed security information in high capacity multichannel (Tb/s) networks. The algorithms will combine the functionality of optical processing with secondary electronic security approaches to introduce new layers of security analysis.

The project brings together partners covering the complete value chain for such modules from research (UCC, FORTH), through component fabrication (CIP), OEM module supplier (Avanex – France) and end user (BT).

Technical Approach

There are two linked elements to the project:

- Development of Photonic Firewalls
  - develop new photonic sub-modules that expand the functionality available at wirespeed, based on high-speed (>40Gb/s) optical logic gates and optical processing circuits.
- Security protocol development
  - develop new algorithms suitable for security analysis based on the knowledge of both the limited wirespeed optical processing that is

currently available, and the additional functionality which will be developed in this project

Schematically, the objective can be represented as shown below where we show the elements to be developed within the optical module of the firewall and the interfaces to the Security Application Programming Interface.

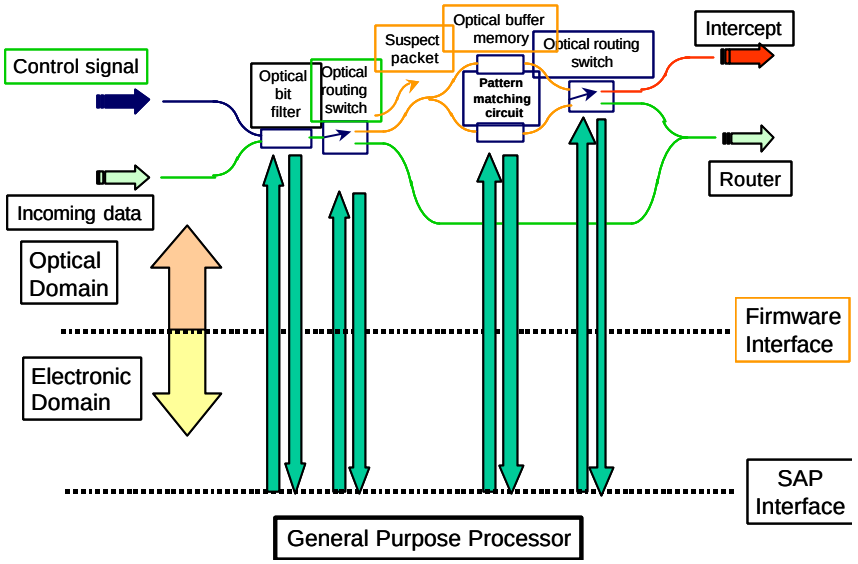

Figure 2. Optical Firewall Block Diagram

The main challenges for the WISDOM optical components are threefold:

1. Development of a scaleable platform for integration which will allow the integration of time delays, large amplifier arrays and faster non-linear SOAs into a manufactureable device
2. Addressing current optical processing limitations in the optical domain (such as optical buffering, level of integration, etc) through novel optical architecture designs
3. Development of the optical / electronic control plane and simple metrics for optical hybrid configuration and performance monitoring

The basic building blocks of logical elements and optical processing functions have been demonstrated in fibre based interferometric systems using semiconductor optical amplifiers as the non-linear element. These elements include functions such as parity checking, optical adding, regenerative memory with full read-write capability, pseudo-random bit sequence generator, AND, XOR, NAND, NOR gates. The main drawbacks are; the processing speed is limited to the length of the fibre loop, the devices are time consuming to set up, complex circuits take up a lot of space and fibre based versions are not capable of mass-production
However, higher levels of optical integration are now becoming available which uses an approach which is both manufactureable and scaleable. This is shown pictorially below. A wider variety of processing elements are now realiseable in an integrated form which is stable, compact and scaleable.

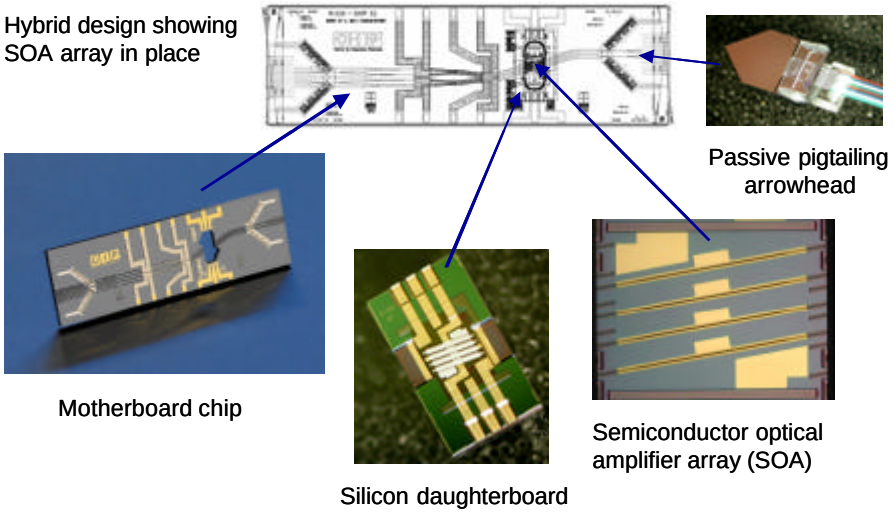

Figure 3. Elements of the hybrid integration platform

The challenges for the security algorithms relate to being able to identify critical security application components which can be ***efficiently*** implemented in the optical domain (e.g., optical bit filtering, simple optical bit pattern matching) given the restrictions imposed by technological limitations in the optical domain (buffering, level of integration, etc). This then imposes constraints to the algorithmic components and requires the development of novel analytical techniques for simplified pattern matching. The work will then focus on the partitioning of security applications (Firewalls, DoS attacks detection, IDS/IPS) into a high-level part (electronic) and low-level part (optical). From this, we will need to design a Security Application Programming Interface (SAPI) which will be the interface between high-level security applications and low-level optical implementation.

Previous work in this area (of efficient algorithm development and implementation) on other EU programs (NOAH, SCAMPI, LOBSTER) give confidence that the challenge is tractable. Figure 4 below gives an example of a Monitoring Application Programming Interface (MAPI). This is a portable monitoring platform, using high level programming language, which runs independently of the underlying hardware. It not only provides header filtering but also sampling, packet counting (anomaly detection), pattern matching in payload (signature-based). Whilst this may be more than is possible in the optical domain, it shows that device independent monitoring is feasible.

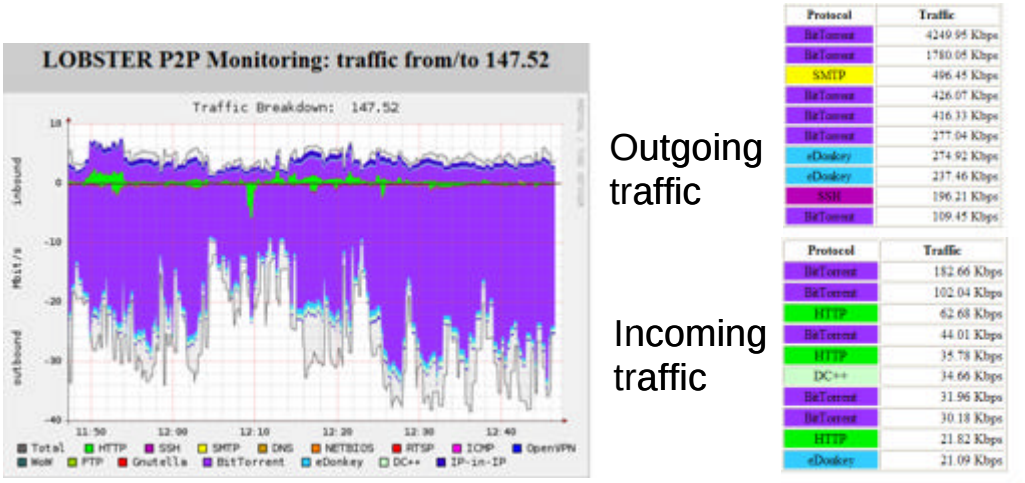

Figure 4. Example of data from MAPI

An additional example of a memory-efficient (since there is very limited memory capacity in the optical domain) signature-based intrusion detection system (IDS) is Piranha. In typical IDS, thousands of signatures are buffered for inspection, with no match most of the time. In this case, a fast and memory-efficient pattern matching routine for IDS has been developed which is based on an algorithm that rapidly identifies that something does not exist. If the rarest substring of a pattern does not appear on the input, then the whole pattern will definitely not match. This can reduce processing time by up to 28% and memory usage by up to 73%.

Generic Deliverables

There are a number of deliverables expected from the WISDOM project. Generic deliverables are detailed below, and cover the themes of; architectural design, photonic component design and fabrication, algorithm development and system validation.

Architecture:

- Definition of initial optical processing functionality, photonic firewall architecture and specifications for optical sub-system

Photonic component development:

- Realisation of hybrid integrated optical circuits required to implement the sub-system, Control firmware for the operation of the hybrid integrated circuits
- Validation of individual hybrid integrated subsystems at wirespeed (40Gbit/s)

Security algorithm development

- Creation of new algorithms for photonics security functions
- Algorithm testing using logical model of photonic firewall and linking of new algorithms to existing security techniques

System validation:

- Demonstration of security algorithm implementation using optical sub-systems
- Validation of optical packet security authentication on a network testbed

Partner Roles & Responsibilities

CIP

- Project lead
- Optical hardware design & fabrication

BT

- Application steer, security algorithm design, architectural design

UCC

- Optical system design, test & measurement

Avanex (France)

- Electronic firmware & control

FORTH

- security algorithm design & code generation

Workpackage List

The WISDOM project consists of seven workpackages as listed with the start and stop dates:

Workpackage	Title	Start date	Stop date
1	Project Management	M0	M36
2	Definition of Photonic Firewall Architecture	M0	M6
3	New Security Algorithm design	M6	M30
4	Optical Processing Sub-system Development	M6	M27
5	Wirespeed photonic firewall security validation	M27	M34
6	Manufactureability, Scalability and Functionality Study	M0	M36
7	Dissemination and Exploitation	M0	M36

The highlights from the workpackages that are currently running or have been completed in year 2 are summarised below.

Workpackage 1: Project Management

Objectives

- To provide administration and technical management of the project as a whole
- To liase with the EU project officer and the commission
- To disseminate commission information to the partners
- To prepare and deliver the monthly/quarterly management reports to the commission
- To ensure document & quality control
- To ensure project delivery

Key achievements:

- Project started and technical and managerial systems put in place.
- Resources distributed
- Project meetings held
- Deliverables achieved on time.

Workpackage 2: Definition of Photonic Firewall Architecture

The purpose of WP2 was to establish the landscape for both the optical hardware and the software algorithms possible.

There were two key deliverables from WP2:

- D2.1 Optical firewall architecture with target specifications for the optical sub-systems

With its main objectives being:

  - define the optical data format
  - define optical functions required within the firewall
  - define capacity requirements and access times for the optical buffer memory
  - define performance target specifications in terms of speed, crosstalk, extinction ratios

and,

- D2.2 Outline proposals for algorithm design
  - review and analys the many factors imposing boundary conditions to the design of security algorithms within the photonic firewall
  - outline applications which could operate with the firewall architecture defined in the concomitant WP2 Deliverable 2.1 and the implications for the physical hardware

The key outcomes in terms of the limitations imposed by the optics (primarily) were:

- Using Return to Zero (RZ) format at 40 Gbps data rate per channel.
- Operate in burst switching mode
- Synchronous operation using optoelectronic clock recovery. Asynchronous operations will be considered in WP6 for scalability
- Speed: bit rate will be 40Gbit/s, WP6 will consider 100Gbits/s & 160Gbits/s
- Bit-serial processing architecture
- Several optical processing functions will be implemented by combining sub-modules: XOR gate, Buffer memory, PRBS generator, Pattern generator, CRC function, optical space switch
- Due to absence of optical RAM (ie inability to carry out optical buffering dynamically) the hardware will be restricted to systems where the relationship between bits is fixed and deterministic. This means that the hardware restricts the analysis to consider packet headers only at this stage.

The key outcomes from the algorithm study were:

- Focus of attention will be on identifying security threats in packet headers
  - Less than 10% of signatures are header-based, but more than 90% security alerts are associate with header-based signatures
- The focus of the algorithm activity will be to look at header based signatures
- Security applications to implement within photonic firewall are those that target known attacks: firewall operations and DoS prevention
- Security applications will rely on 5 to 6 (growing to up to a dozen in the near future) optical gates performing XOR and AND logical operations and additional matching functions, possibly operating in parallel

Workpackage 3: New Security Algorithm design

Objectives

- Identify critical security application components which can be efficiently implemented in the optical domain.
- Characterise constraints to algorithmic components and develop novel analytical techniques for simplified pattern matching.
- Design a Security Application Programming Interface (SAPI) which will be the interface between high-level security applications and low-level optical implementation

Key achievements are:

- Development of symbolic simulation tool which can verify logical operation of complex circuits
- Identification of a number of security operations which can be implemented in the optical domain using simple pattern matching and anomaly detection

Workpackage 4: Optical Processing Sub-system Development

Objectives

- Bit serial Circuit Design and Modelling
- Hybrid Integrated Circuit Fabrication
- Required hybrid integrated optical circuits include :
  - Programmable optical bit filter
  - Optical bit pattern matching circuit
  - Optical buffer memory
  - Optical routing switch
- Control firmware for the operation of the hybrid integrated circuits
- Validation of individual hybrid integrated subsystems at wirespeed (40Gbit/s)

Key achievements are:

- Functional blocks (XOR and AND gates) established and demonstrated at >40Gbits/s
- Format conversion between NRZ and RZ demonstrated (other format conversions reviewed). This is being established and developed to ensure applicability of hardware in a network that does not use RZ format for transmission. Processing blocks will use RZ format, with ingress and egress ports undergoing format conversion.
- Pattern recognition circuit demonstrated at 40Gbits/s for target patterns of up to 256 bits using three logic gates.

Workpackage 6: Manufactureability, Scalability and Functionality Study

Objectives

- Assessment of manufacturability of the sub-systems used in the optical firewall
- Establishing the optimum balance between optical and electronic processing for the firewall function

- Platform scalability & functionality

Key achievements are:

- CIP hybrid platform provides manufactureable approach for the optical firewall. Key elements identified – specifically the silicon submounts - that require development to improve manufactureability
- Information gathered about electronics solution – 40Gbit/s systems currently being deployed, but cost > $100k/unit (for 40 Gbps). Optimum balance between optics and electronics still being considered
- Platform scaleability in terms of speed and gate array sizes looks promising – speed of operation >160Gbits/s feasible

Workpackage 7: Dissemination & Exploitation

Objectives

- Identification of potential groups of users of the developed technologies and devices: target users groups.
- Promote the WISDOM concept through the participation in the technical exhibition of major optical conferences and symposiums.
- Prepare and distribute technical brochures.
- Disseminate the scientific results by means of publications and presentations.
- Establish a Web site

Key achievements:

- Web site established www.ist-wisdom.org
- 19 publications
  - 16 conference (11 invited), 2 journal publications + 2 journal submissions
- 4 magazine articles (Photonics Spectra, PC Magazine, Greek Economist, Components in Electronics)
- 1 meeting with electronic firewall system manufacturer for project dissemination
- CIP exhibit at ECOC06, ECOC07 and OFC07, OFC08 & customer discussions
- Patent application on pattern matching filed