# Project Report:

# Network-Embedded Security using In-Network Packet Marking

**Project Objectives**

The primary objective of this project was to research and evaluate a cutting-edge and radically-new network security solution in Pakistan. Our objective was to develop a security solution that could be deployed inline in a network without impacting the production networks traffic. We wanted to evaluate two types of solutions: 1) Patching solutions, which could be patched on to the current network architecture, and 2) Clean-slate solutions which were not constrained by the shortcomings of the current networking gear.

This solution was developed and its research was published in the top security conferences and journals of the world. A US patent was also filed to protect the intellectual property created during this project.

The security software was tested on academic (online) and industrial (offline) networks in Pakistan. In particular, the developed security algorithms were tested in NUST production network. We also used offline datasets from Nayatel and PTCL to test our algorithms.

After development and testing, the proposed security solution was made publicly available under an open-source license.

This project gave graduate and undergraduate students the opportunity to work on a state-of-the-art problem being faced by the internet arena today. Working on this cutting-edge problem has opened up remarkable opportunities for the students, while also establishing Pakistan as a credible parent in the network security research community.

**Team Structure**

The project team comprised the PI and the Co-PI in supervisory roles. The main research work was carried out by three graduate researchers who were being assisted by three undergraduate researchers.

In addition to the international publications and its open-source release, this project has resulted in two MS theses.

**Significant Achievements of the Project**

- Development of some of the most efficient and advanced in-network security processing detection algorithms.
- Collection of a comprehensive attack dataset that is being used by researchers across the world.
- Open-Source software release which is being used by developers and industry professionals around the world.
- Implementation of the security algorithms on an OpenFlow testbed, resulting in one of the first-ever research publications to propose an OpenFlow-based security architecture.
- Deployment of the solution in NUST and testing on offline datasets from PTCL and Nayatel.
- A patent filed with the US Patents and Trademarks Office (USPTO).
- Publication of four conference papers and one journal paper in the following venues:
    - One journal paper published in the prestigious ACM Sigcomm Computer Communications Review (CCR). (ACM Sigcomm CCR is ranked as the *top journal in the "Networks & Communications" area by Microsoft Academic Search* [http://academic.research.microsoft.com/RankList?entitytype=4&topdomainid=2&subdomainid=14&last=0].)
    - Three papers published in the prestigious International Symposium on Recent Advances in Intrusion Detection (RAID) in 2009, 2010 and 2011.
    - One paper published in IEEE ICC, the flagship IEEE in communications research.
- Two MS theses and three undergraduate Final Year Projects were conducted under this project.
- Graduate researcher, Mobin Javed, won fully-funded PhD positions in both MIT and UC Berkeley.
- Graduate researcher, Junaid Khalid, was selected for a fully-funded summer internship at the UC Berkeley International Computer Science Institute (ICSI).

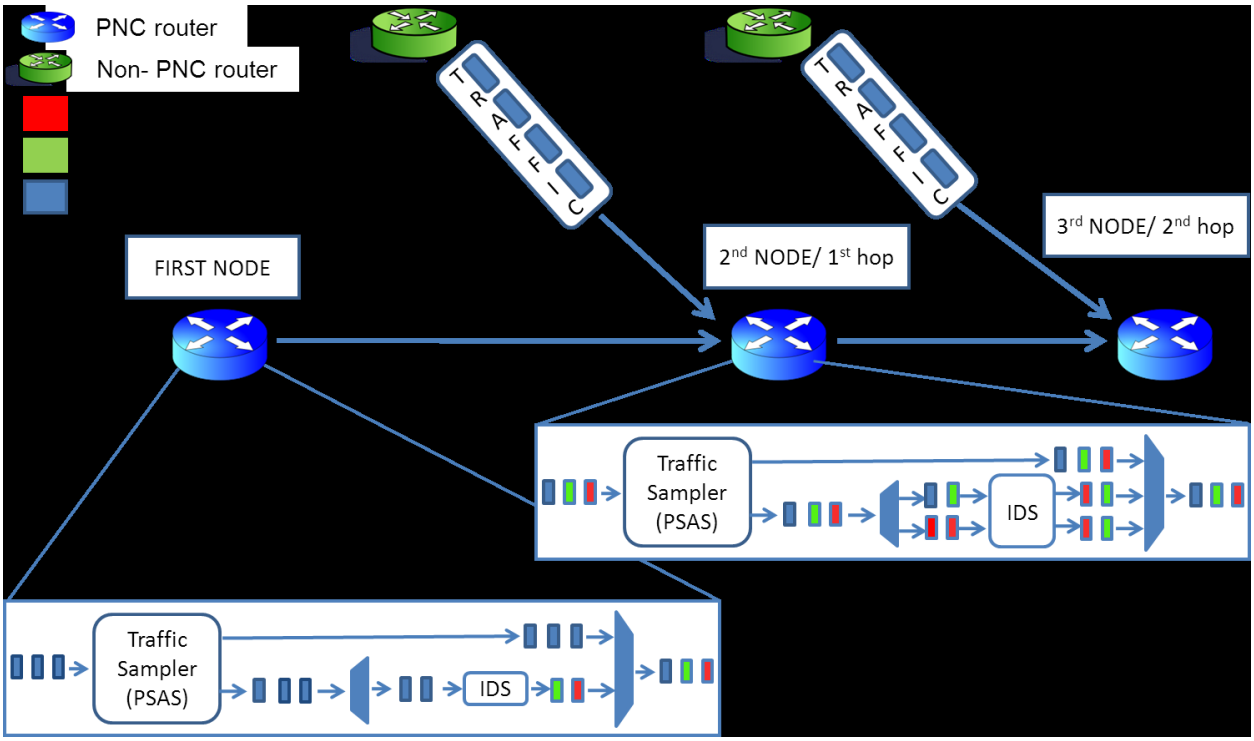
- Graduate researcher, Sajjad Rizvi, was awarded the Erasmus Mundus Scholarship to undertake MS studies in Europe.
- Undergraduate researchers, Syed Amier Haider and Asad Usman, working on this project won the Rector's Gold Medal for Best FYP for the year 2010. (This is one of the highest academic honors for an undergraduate NUST student.)
- The PI was invited to serve on the Program Committee of the prestigious International Symposium on Recent Advances in Intrusion Detection (RAID).

**Research Approach**

In our proposed Progressive Node Collaboration (PNC) architectures, Anomaly Detection Systems (ADSs) are deployed progressively on nodes on a packet's path. These ADSs communicate with each other by encoding their binary opinion (malicious or benign) of a packet inside the packet header before forwarding it to the next hop node. The ADS operating at the next hop uses this score as side information for anomaly detection. This binary side information can be effortlessly encoded inside IP packets, thus allowing different nodes to collaborate without any additional communication overhead. For the experiments in this paper, we use the IP reserved flag to communicate the binary score.

For real-world implementation of the security architecture, we developed PNC-based sampling algorithms [4] and Progressive anomaly detection algorithms [5]. First, these methods were implemented offline on packet captures. In the second phase of the project, these techniques were implemented inline in a production network using the recently introduced OpenFlow technology. Our security architecture introduced significant and consistent improvements in anomaly detection accuracy.

Our basic architecture is shown in the figure below. Details are provided in our research papers.



**Objectives and achievements**

**Objective 1:** The primary objective of this project is to indigenously design and develop a state-of-the-art enterprise network security solution in Pakistan.

**Objective 2:** The security software should tested on academic (online) and industrial (offline) networks in Pakistan.

**Objective 3:** Human resources should be trained in this cutting-edge field.

**■ Objectives Achieved**

**Objective 1:** The system developed in this project was developed and its research was published in the top security conferences and journals of the world. A US patent was also filed to protect the intellectual property created during this project.

**Objective 2:** The proposed security architecture was tested in the NUST production network using Open Flow. We also used offline datasets from Nayatel and PTCL to test our algorithms.

After development and testing, the proposed security solution was made publicly available under an open-source license.

**Objective 3:** In addition to software developers working on a cutting-edge problem, two MS theses and three undergraduate Final Year Projects were conducted under this effort. Moreover, an active research collaboration was initiated with Professor Scott Shenker from UC Berkeley—Prof. Shenker is the world's leading authority in networking and communications research.

**Technology Transfer/Commercialization Approach:**

This is the biggest challenge for our team right now. We have released our code base and data sets in open-source and it is being used extensively by the research community. However, we have not been very successful in targeting industrial partners for commercialization of the project research.

Nevertheless, some success in commercialization has been achieved which are enumerated below:

1. Since OpenFlow is one of the biggest revolutions in the networking industry, we have repositioned our research as a use case for security algorithms' implementation using OpenFlow. In our RAID 2011 paper, we advocated that our security architecture is pushed downstream in home networks for pervasive deployments. Now that the architecture has been well-received by the community, we are contacting some home networking product companies and some DSL/Cable telecom operators to deploy our technology in their products.

2. We have filed a patent in the US Patents and Trademarks Office (USPTO) to protect the innovations undertaken in this project.

3. We have contacted many security companies to license some of this technology in their existing product lines. We have not been very successful with this business model because companies lack the trust to incorporate security technologies developed in Pakistan in their running production lines.

Now that the project is complete and is in demonstrable form, we will continue approaching different security companies to commercialize the outcomes of this project.

**Benefits of the Project:**

**■ Outputs of the project and potential beneficiaries:**

**Outcome 1:** Design and prototype development of a novel network-embedded security architecture that solves fundamental problems of existing security solutions. The research community is already benefitting from this project as our datasets and system code is being used extensively by researchers around the world. We also believe that commercial companies can benefit from the technology developed in this project, but so far we have not had much success in convincing commercial to deploy our algorithms in their systems.

**Outcome 2:** The research conducted in this project has been recognized by the worldwide security community. We have published papers in the most competitive conferences and journals where no paper from Pakistan has ever been accepted before. Pakistani students, developers and researchers have benefitted a lot from working on this cutting-edge technology. Most of the students working on this project were offered fully-funded PhDs by high-ranking USA universities. Other students got highly paid jobs in the industry. Undergraduate students also won institution-level awards for their research.

**■ Organizational Outcomes:**

**Organizational Outcome 1:** NUST and Pakistan's credibility has increased considerably in the security research community.

**Organizational Outcome 2:** NUST has won sponsored research projects from Silicon Valley companies by showcasing the results of this research.

**National Impacts:**

**Impact 1:** Due in part to this project and other security project funded by ICTRDF, Pakistan has emerged as a strong contributor in the worldwide security research community.

**Impact 2:** A number of resources have been trained in this cutting-edge field. Some of these resources are now working in public sector organizations to implement strong security systems to protect critical Pakistani networks. Other resources are working in the industry and are producing high-quality security products.

**Assessment of Project Structure :**

**■ Project Team**

The core project team was hired after extensive interviewing and scrutiny. This was a highly professional and motivated team which worked on the project for the first two years. After that, and as a result of the high-quality research undertaken in this project, two of our researchers were offered funded PhD studies in the USA and Europe. Fortunately, we were able to identify and hire replacement researchers.

**■ Collaborations**

During the course of this project, we developed an active collaboration with Prof. Scott Shenker's research group at UC Berkeley. According to Microsoft Academic search [http://academic.research.microsoft.com/], Prof. Shenker is currently the most cited CS author in the entire world. A collaboration with his group was an extremely prestigious achievement. Based on our novel research, Prof. Shenker signed up on the project team members for a PhD position, while another MS student was awarded a funded internship position at UC Berkeley.

We also collaborated with the CyberDNA Research Center at UNCC.

Moreover, we initiated contact with Nayatel and PTCL to test our system in their networks. While we did not get access to their live network, both ISPs provided us comprehensive network traces for evaluation and benchmarking.

**Research Approach**

The main project hypothesis that security algorithms' accuracy can be improved through network-embedded security marking was sound and was validated in this project. Three factors deviated from the approach proposed in the project proposal:

**Packet Marking:** We observed that even a one-bit packet marker is sufficient to communicate rich contextual information about the last hop security analysis. Therefore, instead of an increasing/decreasing maliciousness level, we encoded a binary score (malicious/benign) in the packet's IP header (reserved bits).

**Benign Traffic's Impact on Anomaly Detection:** We grossly underestimated the negative impact of contemporary benign traffic on the accuracy of our security architecture. In particular, large amounts of peer-to-peer (p2p) traffic introduced significant degradations in the accuracy of our architecture. Consequently, it was imperative that we first devise a behavioral classifier for p2p traffic and integrate it as a pre-processor on each network-embedded security device.

**Clean Slate and Patching Implementations:** We originally intended to implement our security architecture in a software router. Fortunately, during the last three years a very promising new technology called OpenFlow was introduced and drafted. This technology allows a network to have logically disparate control and data plane, so that experimental algorithms can be introduced in the control plane without affecting production traffic in the data plane. Exploiting this technology, we implemented all of our security algorithms using OpenFlow, and deployed and tested our security architecture inline in NUST's production network. Due to its bleeding-edge nature, our work gained seminal importance in the networking research community and we have been invited to demonstrate the technology at three premier applied research conferences: NSF GENI Conference (March 2011), Stanford SDN Summit (October 2011) and SuperComputing (November 2011).