CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày 31 tháng 8 năm 2021

BÁO CÁO KẾT QUẢ TỰ ĐÁNH GIÁ
NHIỆM VỤ KHOA HỌC VÀ CÔNG NGHỆ CẤP QUỐC GIA

I. Thông tin chung về nhiệm vụ:

1. Tên nhiệm vụ, mã số:

Nghiên cứu thiết kế, chế tạo thiết bị phát hiện, phòng chống xâm nhập mạng máy tính phục vụ phát triển Chính phủ điện tử.

Mã số: KC.01.28/16-20

Thuộc: Chương trình: Chương trình Khoa học và Công nghệ trọng điểm Quốc gia giai đoạn 2016 2020 về "Nghiên cứu công nghệ và phát triển sản phẩm công nghệ thông tin phục vụ Chính phủ điện tử", Mã số: KC.01/16-20.

2. Mục tiêu nhiệm vụ:

Trong đề tài này, chúng tôi hướng đến thực hiện hai mục tiêu đã xác lập trong đặt hàng của Bộ Khoa học và Công nghệ, cụ thể như sau:

1. Làm chủ giải pháp kỹ thuật, công nghệ thiết kế, chế tạo thiết bị phát hiện, phòng chống xâm nhập mạng nội bộ (NetIPS), phát hiện và phòng chống xâm nhập máy chủ (HostIPS), quản trị các NetIPS và HostIPS (IPS Manager).

2. Chế tạo, triển khai thử nghiệm thiết bị tại cơ quan quản lý nhà nước phục vụ hoạt động của Chính phủ điện tử.

3. Chủ nhiệm nhiệm vụ:

Họ và tên: Hà Quang Thuỵ Học hàm, học vị: PGS.TS.

Chức danh khoa học: Giảng viên cao cấp

Cơ quan: Trường Đại học Công nghệ - ĐHQGHN58

Địa chỉ: E3, 144 Xuân Thủy, Cầu Giấy, Hà Nội

Điện thoại: Tổ chức: 024.37547.813 Mobile: 09.13.58.59.69

E-mail: thuyhq@vnu.edu.vn

4. Tổ chức chủ trì nhiệm vụ:

Trường Đại học Công nghệ - Đại học Quốc gia Hà Nội

Địa chỉ: Nhà E3 – 144 Xuân Thuỷ - Cầu Giấy – Hà Nội

Điện thoại: (84-24) 37547.461 Fax: (84-24) 37547460

Website: http://uet.vnu.edu.vn

5. Tổng kinh phí thực hiện: **7.820triệu đồng.**

Trong đó, kinh phí từ ngân sách SNKH: 7.820 triệu đồng.

Kinh phí từ nguồn khác: 0 triệu đồng.

6. Thời gian thực hiện theo Hợp đồng: 18 tháng

Bắt đầu: 07/2019

Kết thúc: 12/2020

Thời gian thực hiện theo văn bản điều chỉnh của cơ quan có thẩm quyền *(nếu có)*: kéo dài thêm 08 tháng, kết thúc 08/2021

7. Danh sách thành viên chính thực hiện nhiệm vụ nêu trên gồm:

TT	Họ và tên	Chức danh khoa học, học vị	Tổ chức công tác
1	Hà Quang Thuỵ	PGS.TS	Trường Đại học Công nghệ - ĐHQG HN
2	Nguyễn Hải Châu,	PGS.TS	Trường Đại học Công nghệ - ĐHQG HN
3	Trần Quang Đức	PGS.TS	Viện CNTT - Trường ĐHBK HN
4	Nguyễn Linh Giang	PGS.TS	Viện CNTT - Trường ĐHBK HN
5	Ngô Lam Trung	TS	Viện CNTT - Trường ĐHBK HN
6	Trần Hải Anh	TS	Viện CNTT - Trường ĐHBK HN
7	Bùi Trọng Tùng	ThS	Viện CNTT - Trường ĐHBK HN
8	Nguyễn Trí Thành	PGS.TS	Trường Đại học Công nghệ - ĐHQG HN
9	Vũ Bá Duy, ThS	ThS	Trường Đại học Công nghệ - ĐHQG HN
10	Hoàng Xuân Tùng	TS	Trường Đại học Công nghệ - ĐHQG HN
11	Nguyễn Hoài Sơn	PGS.TS	Trường Đại học Công nghệ - ĐHQG HN
12	Dư Phương Hạnh	TS	Trường Đại học Công nghệ - ĐHQG HN
13	Phạm Hải Đăng	ThS	Trường Đại học Công nghệ - ĐHQG HN
14	Trần Mạnh Thắng	TS	Cục ATTT – Bộ TTTT
15	Phùng Văn Trọng	ThS	Trung tâm CNTT – Bộ GTVT
16	Hoàng Mạnh Cường	ThS	Trung tâm CNTT – Bộ GTVT
17	Trần Tiềm	ThS	Trung tâm CNTT – Bộ GTVT
18	Lê Thùy Dung	ThS	Trung tâm CNTT – Bộ GTVT
19	Nguyễn Đức Thuận	ThS	Trung tâm Tin học – Công báo TP HN
20	Đào Tuấn Hùng	TS	Viện 10 - Bộ Tư Lệnh 86
21	Lê Xuân Đức	TS	Viện 10 - Bộ Tư Lệnh 86
22	Phạm Thị Huyền	TS	Viện 10- Bộ Tư Lệnh 86
23	Nguyễn Trọng Hải	TS	Viện 10 - Bộ Tư Lệnh 86

II. Nội dung tự đánh giá về kết quả thực hiện nhiệm vụ:

1. Về sản phẩm khoa học:

1.1. Danh mục sản phẩm đã hoàn thành:

Số TT	Tên sản phẩm	Số lượng			Chất lượng		
		Xuất sắc	Đạt	Không đạt	Xuất sắc	Đạt	Không đạt
1.	Thiết bị phát hiện, phòng chống xâm nhập mạng nội bộ NetIPS		X			**<u>01 bộ với chỉ tiêu kỹ thuật:</u>** ***Cấu hình phần cứng*** • Kiểu dáng: 4U Rackmount; • CPU: 2 CPU Intel Xeon-Platinum 8160 (2.1GHz/24-core/150W) • Mạng: (i) 01 card mạng tăng tốc tiền xử lý và phân lớp gói tin SmartNIC Napatech NT40E3-4-PTP (10Gb 4-port SFP+, 4 GB DDR3 RAM buffer, API for high performance and advanced features libpcap, WinPcap and DPDK) (ii) 4 cổng vào/ra x 10Gb SFP • Lưu trữ: 4 x 960GB SATA 6G Mixed Use SFF SSD • GPU: 1 x NVIDIA Tesla T4 16GB Computational Accelerator • Bộ nhớ hệ thống: 384 GB DDR4-2666 ***Phần mềm hệ thống NetIPS*** • Thông lượng kiểm tra IPS: **32,63Gbps** (theo phương pháp đo của NSS Lab) • Thông lượng kiểm tra IPS với ứng dụng HTTP: **20,52Gbps** (theo phương pháp đo của NSS Lab) • Độ trễ: ~**12 µs**; (theo phương pháp đo của NSS Lab) • Số kết nối mới/giây: **1.240.000** (theo phương pháp đo của NSS Lab) • Số phiên đồng thời tối đa: **92.930.056** (theo phương pháp đo của NSS Lab) • Có khả năng kiểm tra, ngăn chặn các hướng Inbound, Outbound, Lateral thời gian thực; • Cho phép tích hợp với các thiết bị Sandbox Analysis để mở rộng phạm vi bảo vệ; kiểm tra lưu lượng dữ liệu bất đối xứng; • Cung cấp tính năng bản vá ảo; cập nhật các bộ lọc malware định kỳ; phát hiện, ngăn chặn mối đe dọa, malware nâng cao; cập nhật cơ sở dữ liệu danh tiếng Reputation theo tần suất tuỳ biến trong ngày • Cho phép người dùng cuối ngăn chặn hoạt động của mã độc; phát hiện các hành vi bất thường, các yêu cầu DNS từ các máy bị nhiễm mã độc; các tấn công khai thác Zero-day. • Có khả năng phát hiện xâm nhập dựa vào mô hình lai, kết hợp dựa theo cả dấu hiệu lẫn mô hình bất thường. • Có khả năng thi hành các bộ phát hiện xâm nhập cả trên nhiều luồng lõi CPU lẫn GPU.	

						• Có hệ điều hành chuyên biệt được tuỳ biến cho thiết bị NetIPS. • Có kênh truyền bảo mật kết nối với IPS Manager để cập nhật tập dấu hiệu, mô hình dị thường và gửi vết phân tích về IPS Manager. • Có tập luật phục vụ phát hiện xâm nhập (do IPS Manager đẩy về) trên **43.492** luật phân theo trên **59** lớp (Web, Malware, Exploit, DoS,…). • Có giao diện quản trị cả ở dạng console lẫn trên nền Web; cho phép huấn luyện cục bộ để cập nhật mô hình dị thường phát hiện xâm nhập. ***Mẫu tương tự:*** Vượt một số chỉ tiêu so với sản phẩm TPS2200T của hãng TrendMicro và Security Gateway 5600 của hãng Checkpoint Đã được kiểm tra, đánh giá cả hiệu năng và chức năng tại Trung tâm chứng nhận phù hợp QUACERT – Bộ KHCN.	
2.	Thiết bị phát hiện, phòng chống xâm nhập máy chủ HostIPS		X			**<u>01 bộ với chỉ tiêu kỹ thuật:</u>** ***Cấu hình phần cứng*** • Kiểu dáng: 1U Rackmount; • 2x 1200W High-efficiency Power Supply Platinum Level Certified • AOC-S3108L-H8iR-16DD & 2x CBL-SAST-0593, RAID 0, 1, 5,6, 10, 50, 60 • 2 x Xeon Gold 5218 4/2P 16C/32T 2.3G 22M 10.4GT 125W 3647 B1 • 2 x 32GB DDR4-2666 2Rx4 ECC REG DIMM • 2x SSD Samsung 970 EVO PLUS NVMe M.2 PCIe 500GB • 2x 1GbE LAN ports • AOC-SLG3-2M2 Supports up to 2 NVMe M.2 SSDs ***Phần mềm hệ thống HostIPS*** • Có khả năng bảo vệ các lỗ hổng bảo mật; bảo vệ ứng dụng Web; nhận biết, kiểm soát các phần mềm độc hại truy cập mạng; bảo vệ người dùng, ứng dụng; • Có khả năng ngăn chặn tấn công từ chối dịch vụ phân tán, phát hiện hành vi quét thăm dò; • Hỗ trợ nhiều loại hệ điều hành, gồm Windows, Linux. • Có tường lửa bảo vệ ứng dụng cung cấp dịch vụ công trực tuyến. • Có khả năng gia cố cấu hình hệ thống và các ứng dụng cung cấp dịch vụ mạng. • Có chức năng sinh báo cáo thống kê. • Có tập luật phát hiện xâm nhập gồm 37.680 luật hỗ trợ nhiều nền tảng khác nhau gồm Internet Information Services (IIS), Litespeed, Apache và Nginx; có tập mẫu mã độc trên **6.600.000** dấu hiệu (chữ ký); được cập nhật theo tần suất tùy biến được từ IPS Manager.	

						• Có tập các dấu hiệu phát hiện xâm nhập với tổng số trên **37.680** mẫu; tập các mẫu mã độc trên **6.600.000** dấu hiệu (chữ ký). • Có kênh truyền bảo mật kết nối với IPS Manager để gửi dữ liệu vết phân tích về và nhận lệnh điều khiển. o Có giao diện quản trị trên nền Web.	
3.	Thiết bị quản trị NetIPS và HostIPS (IPS Manager)		X			**<u>01 bộ với chỉ tiêu kỹ thuật:</u>** ***Cấu hình phần cứng*** • Kiểu dáng: 1U Rackmount. • 2x 1200W High-efficiency Power Supply Platinum Level Certified • AOC-S3108L-H8iR-16DD & 2x CBL-SAST-0593, RAID 0, 1, 5,6, 10, 50, 60 • 2 x Xeon Gold 5218 4/2P 16C/32T 2.3G 22M 10.4GT 125W 3647 B1 • 2 x 32GB DDR4-2666 2Rx4 ECC REG DIMM • 2x SSD Samsung 970 EVO PLUS NVMe M.2 PCIe 500GB • 2x 1GbE LAN ports • AOC-SLG3-2M2 Supports up to 2 NVMe M.2 SSDs ***Phần mềm IPS Manager*** • Quản lý người dùng theo vai trò và quyền; hỗ trợ phân quyền truy cập để thiết lập chức năng quản trị thiết bị, hệ thống; Cho phép cấu hình kiểm tra, giám sát theo luật an ninh; từ đó cập nhật vào tập luật NetIPS, HostIPS. • Đưa ra thông báo theo các dạng Logfile, Management Console trên giao diện Web, gửi E-mail và gửi tin nhắn Telegram đến người quản trị khi có cảnh báo rủi ro cao. • Cho phép quản trị, cấu hình chính sách, cập nhật NetIPS, HostIPS từ xa qua các kênh được mã hóa; • Cho phép tùy biến các mẫu báo cáo theo định dạng PDF, HTML, CSV, DOCX, XLS; Cụ thể hơn, các báo cáo về cảnh bảo hỗ trợ định dạng thông thường PDF, HTML; các báo cáo liên quan đến danh mục người dùng; hệ thống NetIPS, HostIPS theo các định dạng DOCX, XLS, CSV. • Cho phép cấu hình phát hiện, ngăn chặn theo địa chỉ IP, tên máy chủ, miền địa lý, quốc gia thông qua việc cập nhật các luật vào trong tập luật NetIPS, HostIPS. • 200 ngày (với giả định mỗi ngày hệ thống tiếp nhận 20GB dữ liệu cảnh báo). • Có khả năng quản lý giám sát xâm nhập trên toàn bộ các NetIPS và HostIPS. • Cung cấp chức năng để tiền xử lý, huấn luyện sinh/cập nhật mô hình bất thường phục vụ phát hiện xâm nhập trong NetIPS/HostIPS. • Có tập luật phục vụ phát hiện xâm nhập (do IPS Manager đẩy về) trên **43.492** luật phân theo trên **59** lớp (Web, Malware, Exploit, DoS,…). • Có tập các mẫu mã độc trên 6.600.000 chỉ dấu (chữ ký).	

4.	Tài liệu giải pháp tổng thể phát hiện và chống xâm nhập trong các hệ thống thông tin tại các cơ quan nhà nước		X			Tài liệu gồm sáu chương, được tổ chức như sau: - Chương 1, 2 giới thiệu tổng quan về an toàn thông tin và phòng chống xâm nhập mạng hiện nay trong các cơ quan cấp Bộ của Chính phủ điện tử. - Chương 3 đặc tả giải pháp tổng thể về phát hiện và phòng chống xâm nhập trong các hệ thống thông tin. - Chương 4 giới thiệu mô hình giải pháp tích hợp, phối ghép thiết bị để hình thành thiết bị phòng chống xâm nhập mạng NetIPS. - Chương 5 mô tả giải pháp xây dựng hệ thống phòng chống xâm nhập máy chủ HostIPS. Chương 6 giới thiệu khái quát mô hình giải pháp IPS Manager để quản lý các thiết bị NetIPS cũng như các hệ thống HostIPS.	
5.	Tài liệu thiết kế thiết bị NetIPS và quy trình chế tạo		X			Tài liệu gồm bốn chương tổng hợp kết quả thiết kế NetIPS và quy trình chế tạo vỏ với cấu trúc như sâu: - Chương 1 giới thiệu chung về giải pháp phòng chống xâm nhập mạng, từ đó thiết kế phần cứng, xây dựng phương án lựa chọn linh kiện cần thiết cho phần cứng thiết bị NetIPS. - Chương 2: đặc tả quy trình công nghệ tích hợp, chế tạo vỏ NetIPS. - Chương 3 tổng hợp kết quả tích hợp thiết bị mạng chuyên dụng SmartNIC và nền tảng tính toán và kết quả chế tạo vỏ thiết bị NetIPS. - Chương 4 tóm lược kết quả tích hợp, hình thành và thử nghiệm cục bộ NetIPS.	
6.	Tài liệu phân tích, thiết kế toàn bộ hệ thống HostIPS		X			Tài liệu gồm tám chương đã đặc tả được cả quá trình phân tích yêu cầu lẫn thiết kế hệ thống HostIPS: - Chương 1 tập trung phân tích, thiết kế kiến trúc tổng thể của hệ thống phát hiện và ngăn chặn xâm nhập HostIPS. - Chương 2 mô tả thiết kế và đặc tả chi tiết cho phân hệ bảo vệ hệ thống tệp tin: giám sát toàn vẹn, xây dựng các công cụ mã hóa, kiểm soát truy cập tới tệp tin và thư mục quan trọng. - Chương 3 tập trung vào việc thu thập thông tin về hệ thống các ứng dụng, đưa ra đánh giá, cảnh báo về lỗ hổng bảo mật của các ứng dụng đang được cài đặt trên hạ tầng máy chủ cung cấp dịch vụ công. - Chương 4 tập trung vào thiết kế, xây dựng các công cụ rà soát tệp tin mã độc trên hệ thống, tệp tin đính kèm qua email, quét rootkit, …. - Chương 5 trình bày việc xây dựng tường lửa mức hệ thống kiểm soát truy cập trên cả hai hệ điều hành Windows và Linux, xây dựng các tập luật, cơ sở dữ liệu tên miền và địa chỉ IP độc hại, xây dựng các cơ chế ngăn chặn tấn công đối với các ứng dụng cung cấp dịch vụ công trực tuyến mà chủ yếu là dựa trên nền tảng web.	

						- Chương 6 tập trung vào việc thiết kế và xây dựng các công cụ, cung cấp API cho phép đánh giá lỗ hổng và cập nhật bản vá cho hệ điều hành Windows/Linux, cho các máy chủ Web Server như Apache/IIS, cho hệ quản trị cơ sở dữ liệu MySQL theo bộ tiêu chuẩn CIS Benchmark., từ đó, đưa ra các khuyến cáo, cấu hình hệ thống đảm bảo an toàn trước các nguy cơ tấn công. - Chương 7 mô tả thiết kế và đặc tả chi tiết phân hệ xây dựng báo cáo thống kê, bao gồm thống kê trạng thái toàn vẹn của hệ thống tệp tin, thống kê lưu lượng mạng, thống kê kết quả của quá trình rà quét mã độc cho toàn bộ hệ thống, …. - Chương 8 trình bày tường minh cách thức xây dựng kết nối bảo mật, cho phép gửi và nhận dữ liệu log từ HostIPS tới IPS Manager, đồng thời, cập nhật các lệnh điều khiển, các cấu hình tập luật một cách an toàn.	
7.	Tài liệu phân tích, thiết kế toàn bộ hệ thống IPS Manager		X			Tài liệu đã tổng hợp kết quả phân tích thiết kế hệ thống IPSManager với tổ chức như sau: - Chương 1 trình bày về các giải pháp, phương pháp phát hiện xâm nhập và giới thiệu chung về IPSManager. - Chương 2 tập trung phân tích, thiết kế hệ thống IPSManager quản lý các NetIPS và HostIPS bao gồm các phân tích - đánh giá yêu cầu (yêu cầu chi tiết, yêu cầu về chức năng), kiến trúc hệ thống, thiết kế chi tiết (xác định tác nhân và ca sử dụng, biểu đồ ca sử dụng và biểu đồ tuần tự), phân hệ quản lý toàn bộ dữ liệu IPS Manager (quản lý dữ liệu chữ ký, dấu hiệu, quản lý dữ liệu bất thường, quản lý thông tin thiết bị NetIPS và HostIPS, quản lý dữ liệu sự kiện xâm nhập, quản lý dữ liệu người dùng, quản lý dữ liệu cảnh báo, quản lý báo cáo thống kê), phân hệ quản lý NetIPS (thiết lập kênh truyền bảo mật kết nối với NetIPS, mô đun chức năng tiếp nhận dữ liệu từ NetIPS, mô đun chức năng điều khiển NetIPS, mô đun chức năng cập nhật luật về NetIPS,mô đun chức năng cập nhật chính sách về NetIPS, mô đun chức năng cập nhật mô hình phát hiện về NetIPS), phân hệ quản lý HostIPS (thiết lập kênh truyền bảo mật kết nối với HostIPS, mô đun chức năng tiếp nhận dữ liệu từ HostIPS, mô đun chức năng điều khiển HostIPS, mô đun chức năng cập nhật luật về HostIPS, mô đun chức năng cập nhật chính sách về HostIPS, mô đun chức năng cập nhật mô hình phát hiện về HostIPS), phân hệ quản lý giám sát xâm nhập.	
8.	Tài liệu hướng dẫn quản lý, vận hành, khai thác và sử		X			Tài liệu đã mô tả hướng dẫn chi tiết để cài đặt, vận hành, quản lý, khai thác sử dụng cả ba sản phẩm chính của đề tài: NetIPS, HostIPS và IPSManager. Tổ chức tài liệu được phân thành 3 chương chính tương ứng với hướng dẫn cụ thể của từng sản phẩm.	

	dụng thiết bị NetIPS, HostIPS và IPS Manager						
9.	Báo cáo kết quả triển khai, đánh giá thử nghiệm các hệ thống		X			Đã tổng hợp lại toàn bộ quá trình thử nghiệm tại Trung tâm CNTT – Bộ GTVT và Trung tâm Tin học – Công báo trong 2 báo cáo riêng biệt cho từng đơn vị đã triển khai thử nghiệm. Mỗi báo cáo đã làm rõ được kết quả khảo sát, đánh giá hiện trạng; từ đó xây dựng kịch bản thử nghiệm; ghi nhận kết quả thử nghiệm đối với từng sản phẩm NetIPS, HostIPS và IPSManager. Các kết quả đánh giá, nhận xét từ đơn vị thử nghiệm cũng đã được tổng hợp trong báo cáo.	
10.	Báo cáo giải pháp hữu ích về hệ thống phát hiện và phòng chống xâm nhập mạng NetIPS		X			Đã xây dựng được 02 giải pháp nộp Bộ KHCN để xin cấp bằng sáng chế/giải pháp hữu ích: 1. " *Phương pháp và hệ thống phát hiện và ngăn chặn xâm nhập mạng sử dụng luật và mô hình học sâu* ". Mã số đơn 1-2021-05291 đã được Cục Sở hữu trí tuệ Bộ KH&CN tiếp nhận hồ sơ từ ngày 16/08/2021. 2. "*Phương pháp phát hiện đoạn mã độc trong mã nguồn ứng dụng Web sử dụng ngôn ngữ ASP*". Mã số đơn 1-2021-00205 đã được Cục Sở hữu trí tuệ, Bộ KH&CN chấp nhận đơn hợp lệ theo Quyết định số 6306w/QĐ-SHTT ngày 28/04/2021.	
11.	Báo cáo tổng kết và tóm tắt kết quả đề tài		X			Báo cáo tổng kết đã tổng hợp được toàn bộ những kết quả thu được từ các nội dung đã thực hiện trong nhiệm vụ này với cấu trúc 8 chương, ngoài phần Mở đầu và Kết luận. Báo cáo tóm tắt đã tóm lược những kết quả chính thu được trong đề tài.	
12.	Bài báo khoa học		X			*Đã công bố được 04+01 công trình, gồm:* 1. Dung Truong, Duc Tran, Lam Nguyen, Hieu Mac, Hai Anh Tran, and Tung Bui. 2019. *Detecting Web Attacks using Stacked Denoising Autoencoder and Ensemble Learning Methods*. In The Tenth International Symposium on Information and Communication Technology (SoICT 2019), December 4–6, 2019, Hanoi - Ha Long Bay, Vietnam, Viet Nam. ACM, New York, NY, USA, 6 pages. 2. Tran-Tuan CHU, Van TONG, Hai Anh TRAN, Sami SOUIHI, Duc Quang TRAN, and Abdelhamid MELLOUK. 2019. *NextLab: A new hybrid testbed and development platform for Software-defned Networking*. In The Tenth International Symposium on Information and Communication Technology (SoICT 2019), December 4–6, 2019, Hanoi - Ha Long Bay, Vietnam, Viet Nam. ACM, New York, NY, USA, 5 pages.	

						3. Vuong TH., Thi CV.N., Ha QT. (2021) *N-Tier Machine Learning-Based Architecture for DDoS Attack Detection*. In: Nguyen N.T., Chittayasothorn S., Niyato D., Trawiński B. (eds) Intelligent Information and Database Systems. ACIIDS 2021. Lecture Notes in Computer Science, vol 12672. Springer, Cham. 4. Can DC., Le HQ., Ha QT. (2021) *Detection of Distributed Denial of Service Attacks Using Automatic Feature Selection with Enhancement for Imbalance Dataset*. In: Nguyen N.T., Chittayasothorn S., Niyato D., Trawiński B. (eds) Intelligent Information and Database Systems. ACIIDS 2021. Lecture Notes in Computer Science, vol 12672. Springer, Cham. 5. Hoang V.V., Ha V.L., Tu N.N, Hoa N.N., Cybersecurity: Webshell Detection Using the Deep HTTP Traffic Analysis, submitted in *International Journal of Web and Grid Services*, 2021(Q1, SCI-E)	
13.	Đào tạo thạc sỹ		X			Đã đào tạo được 04 thạc sỹ 1. Vũ Mạnh Cường, *Nghiên cứu ứng dụng mô hình học sâu trong phát hiện xâm nhập mạng*, Thạc sỹ HTTT, 7/2021. Người hướng dẫn: PGS.TS. Nguyễn Ngọc Hoá. 2. Nguyễn Quốc Khánh, *Hệ thống và phương pháp phát hiện thiết bị nhiễm mã độc DGA dựa trên học tăng cường*, Thạc sỹ KHDL, 5/2021. Người hướng dẫn PGS.TS. Trần Quang Đức. 3. Vũ Việt Dũng, *Áp dụng công nghệ mới vào việc lưu trữ và xử lý dữ liệu cho hệ thống Billing*, Thạc sỹ HTTT, 1/2020. Người hướng dẫn: PGS. TS. Nguyễn Hải Châu. 4. Đàm Văn Hải, *Nghiên cứu triển khai và đánh giá hiệu năng của các giải pháp networking nâng cao cho hệ thống ảo hoá sử dụng OpenStack*, Thạc sỹ MTT, 12/2019. Người hướng dẫn: TS. Hoàng Xuân Tùng.	
14.	Tham gia đào tạo tiến sỹ		X			Đã hỗ trợ đào tạo 02 NCS: - NCS. Phạm Hải Đăng, "*Nghiên cứu một số phương pháp phát hiện chỉ dấu xâm nhập hệ thống dựa trên phân tích thông tin mối đe dọa*", bắt đầu từ 10/2020. - NCS. Võ Văn Hoàng, "*Nghiên cứu, phát triển một số phương pháp học máy để phát hiện xâm nhập mạng*", bắt đầu từ 10/2020.	

1.2. Danh mục sản phẩm khoa học dự kiến ứng dụng, chuyển giao (nếu có):

Số TT	Tên sản phẩm	Thời gian dự kiến ứng dụng	Cơ quan dự kiến ứng dụng	Ghi chú
1	Hệ thống phát hiện và phòng chống xâm nhập mạng NetIPS, máy chủ HostIPS và IPSManager	2021	Bộ Giao thông vận tại	
2	Hệ thống phát hiện và phòng chống xâm nhập mạng NetIPS, máy chủ HostIPS và IPSManager	2021	UBND TP Hà Nội	
3	Hệ thống phát hiện và phòng chống xâm nhập mạng NetIPS, máy chủ HostIPS và IPSManager	2021	Văn phòng Chính phủ	
4	Hệ thống phát hiện và phòng chống xâm nhập mạng NetIPS, máy chủ HostIPS và IPSManager	2021	Tổng cục kỹ thuật – Bộ Quốc phòng	

2. Về những đóng góp mới của nhiệm vụ:

- Nhóm thực hiện đề tài đã tiến hành nghiên cứu và phân tích công phu, có hệ thống và toàn diện các kết quả nghiên cứu và triển khai tiên tiến về phát hiện và ngăn chặn xâm nhập trên thế giới. Trên cơ sở đó, nhóm thực hiện đề tài hình thành nền tảng khoa học và công nghệ cho các sản phẩm NetIPS, HostIPS và IPSManager. Các sản phẩm này được hình thành dựa trên các tiếp cận tiên tiến trên thế giới (từ các nhà khoa học, các phòng thí nghiệm, các công ty nổi tiếng), vì vậy, không chỉ được xây dựng dựa trên các kỹ thuật tiên tiến nhất mà còn dựa trên việc sử dụng hiệu quả các tài nguyên mở đáng giá nhất.
- Tiếp cận tích hợp nhiều hệ thống NetIPS, HostIPS dựa trên một hệ thống quản lý nhất quán và cộng tác thông qua IPSManager là phù hợp với xu thế hiện đại trên thế giới về triển khai các hệ thống phát hiện và ngăn chặn xâm nhập trong các tổ chức có quy mô lớn. Hơn nữa, việc sử dụng phương pháp lai kết hợp phát hiện dựa trên chỉ dấu (với bộ tài nguyên chỉ dấu lớn) và phát hiện dựa trên bất thường (với các kỹ thuật học máy tiên tiến) giúp các sản phẩm của đề tài đáp ứng đầy đủ các yêu cầu đặt ra cho đề tài.
- Các mô hình phát hiện xâm nhập dựa trên bất thường của đề tài được xây dựng dựa trên các kỹ thuật học máy tiên tiến, đặc biệt là các kỹ thuật học sâu (có tiềm năng giải quyết các thách thức lớn đối với kỹ thuật học máy truyền thống). Đồng thời, các mô hình này được định kỳ cải tiến. Hơn nữa, một số vấn đề chuyên sâu như "mất cân bằng lớp" hoặc sử dụng hàm mất mát đa lề trong học sâu phát hiện xâm nhập cũng đã được phân tích giải quyết. Cách tiếp cận như vậy cho thấy tiềm năng đáp ứng yêu cầu "khu vực công dựa trên dữ liệu" của Chính phủ điện tử và Chính phủ số Việt Nam với hạ tầng kỹ thuật sử dụng các công

nghệ tiên tiến như Dữ liệu lớn, Trí tuệ nhân tạo, v.v. đã được xác định trong Khung CPĐT 2.0 đã được ban hành.

- Ý tưởng kết hợp sử dụng phần cứng hiệu năng cao (CPU kết hợp GPU) với chế tạo bo mạch ASIC riêng kèm những bộ xử lý mạng NIC để thiết lập hệ thống tích hợp phần cứng - phần mềm phát hiện và ngăn chặn xâm nhập mạng lưu lượng lớn đã tạo ra một sáng kiến có ý nghĩa. Sáng kiến này được kế thừa từ các kết quả nghiên cứu khoa học cập nhật nhất, các kết quả thiết kế thiết bị của một số hãng có uy tín (chẳng hạn, Firepower 9300 SM48 của Cisco, Tippingpoint 8200TX của Trend Micro) đã giúp sản phẩm NetIPS của đề tài đáp ứng vượt mức yêu cầu 80 triệu kết nối đồng thời mà ban đầu tưởng chừng không thể vượt qua. Toàn bộ các chỉ tiêu cả về hiệu năng lẫn các chức năng sử dụng của hệ thống NetIPS đã được kiểm tra, đánh giá và xác nhận bởi Trung tâm chứng nhận phù hợp QUACERT, Tổng cục tiêu chuẩn đo lường chất lượng, Bộ KHCN.
- Nhóm thực hiện đề tài đã tập hợp được nhiều nhóm thành viên có chuyên môn sâu, kinh nghiệm nhiều, tinh thần cộng tác tốt, để đạt nhiều sáng kiến trong xây dựng và đánh giá các sản phẩm của đề tài. Chính vì vậy, các sản phẩm của đề tài được xây dựng có chất lượng đáp ứng yêu cầu, được đánh giá thử nghiệm công phu và chuyên nghiệp tại Trung tâm CNTT (Bộ Giao thông Vận tải) và Trung tâm Tin học – Công báo (Ủy ban nhân dân Thành phố Hà Nội).
- Các kết quả khoa học, công nghệ đã được nhóm làm chủ có thể kể đến như: công nghệ xử lý, phân tích gói tin ở không gian người dùng sử dụng thư viện DPDK của Intel; công nghệ học sâu (CNN, DNN, LSTM, ...) ứng dụng trong phát hiện xâm nhập mạng, phòng chống tấn công DDoS, phát hiện mã độc; công nghệ tính toán hiệu năng cao, xử lý song song trong CPU với kỹ thuật phân tách và gán chuyên biệt từng lõi CPU để xử lý công việc theo chức năng (phân tích dữ liệu/ra quyết định/điều phối) và theo từng luồng dữ liệu mạng. Kết hợp xử lý dữ liệu trong GPU để nâng cao hiệu năng dự đoán xâm nhập mạng với mô hình học sâu; công nghệ quản lý dữ liệu lớn sử dụng Elastic Stack trên môi trường cụm máy tính, cho phép vận chuyển, phân tích, chuẩn hoá, truy vấn, trực quan hoá dữ liệu vết xâm nhập đạt mức 100GB mỗi ngày; và công nghệ chủ động dò quét, ngăn chặn mã độc trong suốt với người dùng dựa trên cơ chế Sandbox.
- Những đóng góp về mặt học thuật cũng đã được thể hiện thông qua 02 phương pháp xin cấp bằng Sáng chế của Bộ KHCN và đã được chấp nhận đơn hợp lệ; 04 bài đăng kỷ yếu hội thảo quốc tế Scopus/WoS; và đang gửi xét đăng 01 bài tạp chí quốc tế thuộc danh mục ISI, Q1-Scopus.

3. Về hiệu quả của nhiệm vụ:

3.1. Hiệu quả kinh tế

Ngoài việc phục vụ cho các cơ quan nhà nước, ba sản phẩm chính của nhiệm vụ là (i) Thiết bị phát hiện, phòng chống xâm nhập mạng nội bộ NetIPS, (ii) hệ thống phát hiện, phòng chống xâm nhập máy chủ HostIPS, (iii) hệ thống IPSManager quản lý NetIPS và HostIPS hoàn

toàn có thể mở rộng, đưa ra thị trường trong nước để phục vụ các tổ chức, doanh nghiệp ngoài công lập trong công tác đảm bảo ATTT nói chung. Các sản phẩm của đề tài hoàn toàn có thể được thương mại hoá và triển khai như là giải pháp phát hiện và phòng chống xâm nhập mạng nội bộ và máy chủ. Các sản phẩm này sẽ cho phép giảm được chi phí mà các tổ chức, doanh nghiệp phải đầu tư, xây dựng hệ thống sản phẩm thương mại có giá thành rất cao.

HostIPS được phát triển để bảo vệ máy chủ, nhưng hoàn toàn có thể tùy biến để phù hợp khi cài đặt tại các máy trạm. Với định hướng này, HostIPS sẽ có các tính năng tương đương với một số sản phẩm thương mại như Kaspersky Internet Security và có thể triển khai tại hầu hết cơ quan, tổ chức nhà nước và doanh nghiệp tư nhân.

Thiết bị NetIPS có tiềm năng phát triển, mở rộng để sản xuất đại trà phục vụ cho các doanh nghiệp trong lĩnh vực an ninh mạng. Hệ thống IPS Manager có thể triển khai theo mô hình điện toán đám mây. Trong mô hình này, IPS Manager thực hiện thu thập thông tin từ các NetIPS và HostIPS. Từ đó, cung cấp cái nhìn tổng quan hơn về tình hình an ninh mạng tại Việt Nam, các nguy cơ gây mất an toàn thông tin, thực hiện cập nhật kịp thời luật, bản vá và mẫu mã độc để bảo vệ hạ tầng mạng và CNTT tại các đơn vị triển khai.

3.2. Hiệu quả xã hội

Ngoài những tác động về kinh tế nêu trên, các kết quả, sản phẩm của đề tài cũng có những tác động tích cực đối với xã hội và môi trường nói chung. Một số những tác động chính từ các kết quả nghiên cứu trong đề tài này có thể liệt kê ra như dưới đây:

- Giảm thiểu chi phí ngoại tệ trong việc mua các sản phẩm tương tự của nước ngoài, đặc biệt đối với những hệ thống NetIPS, HostIPS với quy mô lớn;
- Đảm bảo được những vấn đề an toàn phần mềm khi triển khai những hệ thống đảm bảo ATTT nói chung trong cơ quan nhà nước. Đây cũng là một trong những lợi điểm nổi bật nhất khi các sản phẩm của đề tài được các nhóm nghiên cứu từ các trường Đại học, cơ sở nghiên cứu của Nhà nước xây dựng và phát triển; từ đó góp phần giảm thiểu cũng như tránh được những nguy cơ mất ATTT từ chính những sản phẩm ngoài nước, đặc biệt đối với thiết bị NetIPS khi đặt kiểm soát ở mạng nội bộ.
- Từng bước xây dựng được đội ngũ chuyên trách làm dịch vụ đảm bảo cập nhập và vận hành trơn tru thiết bị phát hiện và phòng chống xâm nhập NetIPS, phát hiện và phòng chống xâm nhập máy chủ HostIPS.

Ngoài ra, sản phẩm của đề tài hoàn toàn có thể được mở rộng, ứng dụng cho các doanh nghiệp, tổ chức khác. Khi đó, toàn bộ những tác động nêu trên còn có phổ lan toả rộng hơn nữa, từ đó minh chứng rõ nét hơn những tác động tích cực và hữu ích của các sản phẩm đề tài trong kinh tế - xã hội và môi trường.

Sau khi hoàn thiện, phát triển thêm các tính năng chuyên biệt, hai hệ thống phần mềm trong nhiệm vụ này có thể triển khai phục vụ công tác nghiệp vụ trong các đơn vị có nhiệm vụ đảm bảo an ninh xã hội, quốc phòng như Cục CNTT, Cục An ninh mạng - Bộ Công an, Bộ Tư lệnh 86 – Bộ Quốc phòng.

III. Tự đánh giá, xếp loại kết quả thực hiện nhiệm vụ

1. Về tiến độ thực hiện: *(đánh dấu √ vào ô tương ứng)*:

- *Nộp hồ sơ đúng hạn* ☒
- *Nộp chậm từ trên 30 ngày đến 06 tháng* ☐
- *Nộp hồ sơ chậm trên 06 tháng* ☐

2. Về kết quả thực hiện nhiệm vụ:

- *Xuất sắc* ☐
- *Đạt* ☒
- *Không đạt* ☐

Giải thích lý do:

Đề tài KC.01.28/16-20 đã hoàn thành mục tiêu nghiên cứu, đã hoàn thành đầy đủ các sản phẩm, đáp ứng được các yêu cầu về số lượng, chất lượng, khối lượng đã đặt ra trong thuyết minh và hợp đồng đã ký.

Cam đoan nội dung của Báo cáo là trung thực; Chủ nhiệm và các thành viên tham gia thực hiện nhiệm vụ không sử dụng kết quả nghiên cứu của người khác trái với quy định của pháp luật.

CHỦ NHIỆM NHIỆM VỤ	**THỦ TRƯỞNG** **TỔ CHỨC CHỦ TRÌ NHIỆM VỤ**
PGS.TS. Hà Quang Thuỵ	**GS.TS. Chử Đức Trình**

K/T HIỆU TRƯỞNG
PHÓ HIỆU TRƯỞNG

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ