ETM

ENGINEERING & TECHNOLOGY MANAGEMENT

Title: Transferring Intrusion Detection System (IDS) – "Net Taster" technology from John Hopkins University-Applied Physics Laboratory

Course Title: Technology Transfer
Course Number: ETM 533/633
Instructor: Dr. Tugrul Daim
Term: Summer
Year: 2011
Author(s): Akhilesh Dwivedi, Aron E. Yucha, Chintan Jain, and Fredy Gomez

ETM OFFICE USE ONLY

Report No.:
Type: Student Project
Note:

Abstract

The Johns Hopkins University – Applied Physical Laboratory (JHU-APL), located in Laurel, Maryland, is a research and technology division of The Johns Hopkins University. JHU-APL conducts and maintains specialized research and test facilities, employs approximately 4,500 employees, and receives annual funds exceeding $988 million dollars.[1]

JHU-APL strengths lie primarily in sensor technology, biomedical applications, electronics, space technology and communications. JHU-APL has a rich portfolio with more than 700 active inventions. These inventions include software, tangible products and intangible products (copyrighted material and active/pending patents). JHU-APL has a rich portfolio of applications ready and available for commercial transfer, yet only received $32.8 million in licensing income from 1999 through 2010.[2]

After reviewing JHU-APL's available technologies, our team has selected "NetTaster" as a recommended technology to transfer. The team finds this technology to have a strong market need, key core functions/assets, many notable comparative advantages and complimentary assets promoting commercial success. In the past decade technological advances have increased the usage of internet by integrating many different environments/eco-systems (personal, business, government etc) into one platform. Technological advances and their internet integration have both enhanced life and created new and additional risks. Primary risks associated with the internet are "hackers". The said primary risk, hacker, grew from script kiddies (who hack for fun) to extremely sophisticated hackers or organizations of hackers who infiltrate cyber-systems for personal, commercial, and political agenda. Cyber attacks are ubiquitous and lead to loss of personal, professional as well as governmental secret information.[3]

Current day, organizations use Intrusion Detection Systems (IDS) or anti-malware/antivirus/anti-spyware to protect against these cyber attacks. However, these current technological solutions fail to protect against new (zero day) attacks. There is a tremendous market need for advanced technology that can detect zero day attacks. Our team discovered, reviewed, and selected JHU-APL's "NetTaster" technology for transfer due to its capability to detect instantaneous, zero day attacks as they occur.

This report will expand on topics discussed in the above Executive Summary. Topics to be discussed are: JHU-APL background & description, JHU-APL Office of Technology Transfer,[5] targeted technology - NetTaster, Technology Transfer Plan, and Recommendations & Conclusions.

Contents

List of Figures

Executive Summary

The Johns Hopkins University – Applied Physical Laboratory (JHU-APL), located in Laurel, Maryland, is a research and technology division of The Johns Hopkins University. JHU-APL conducts and maintains specialized research and test facilities, employs approximately 4,500 employees, and receives annual funds exceeding $988 million dollars. [1]

JHU-APL strengths lie primarily in sensor technology, biomedical applications, electronics, space technology and communications. JHU-APL has a rich portfolio with more than 700 active inventions. These inventions include software, tangible products and intangible products (copyrighted material and active/pending patents). JHU-APL has a rich portfolio of applications ready and available for commercial transfer, yet only received $32.8 million in licensing income from 1999 through 2010. [2]

After reviewing JHU-APL's available technologies, our team has selected "NetTaster" as a recommended technology to transfer. The team finds this technology to have a strong market need, key core functions/assets, many notable comparative advantages and complimentary assets promoting commercial success. In the past decade technological advances have increased the usage of internet by integrating many different environments/eco-systems (personal, business, government etc) into one platform. Technological advances and their internet integration have both enhanced life and created new and additional risks. Primary risks associated with the internet are "hackers". The said primary risk, hacker, grew from script kiddies (who hack for fun) to extremely sophisticated hackers or organizations of hackers who infiltrate cyber-systems for personal, commercial, and political agenda. Cyber attacks are ubiquitous and lead to loss of personal, professional as well as governmental secret information. [3]

Current day, organizations use Intrusion Detection Systems (IDS) or anti-malware/anti-virus/anti-spyware to protect against these cyber attacks. However, these current technological solutions fail to protect against new (zero day) attacks. There is a tremendous market need for advanced technology that can detect zero day attacks. Our team discovered, reviewed, and selected JHU-APL's "NetTaster" technology for transfer due to its capability to detect instantaneous, zero day attacks as they occur.

This report will expand on topics discussed in the above Executive Summary. Topics to be discussed are: JHU-APL background & description, JHU-APL Office of Technology Transfer, targeted technology - NetTaster, Technology Transfer Plan, and Recommendations & Conclusions.

Johns Hopkins University (JHU) - Applied Physics Laboratory (JHU-APL) Description

History[4]

The Johns Hopkins University - Applied Physics Laboratory (JHU-APL), is a not-for-profit research center. JHU-APL is primarily a defense contractor. It serves as a technical resource for the Department of Defense (DoD), NASA, and other government agencies. The Lab is a research and development organization rather than an academic division of Johns Hopkins University. JHU's Whiting School of Engineering offers part-time graduate programs through its engineering for professionals program.

Created during World War II (WWII) in 1942, JHU-APL was funded under the Office of Scientific Research and Development as part of the Government's effort to mobilize the nation's science and engineering expertise within its universities. The JHU-APL succeeded in developing the variable-time proximity fuse that played a significant role in the WWII allied victory. Expected to dissolve, JHU-APL instead was funded to help develop guided missile technology for the Navy all while maintaining the laboratory to also provide public service.

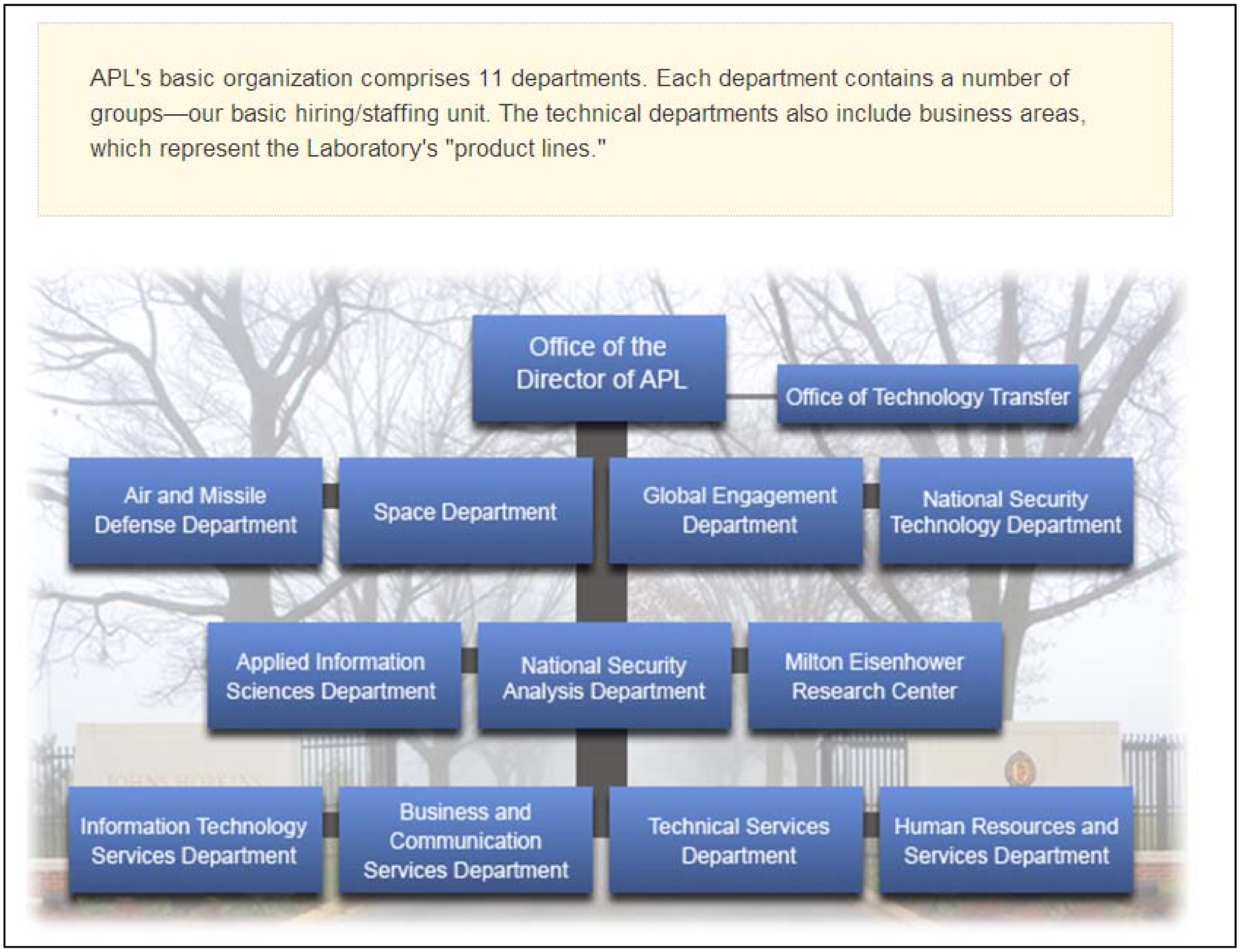
The JHU-APL's major strengths are system engineering and technology application. About half of the technical staff is engineers, and 25% have computer science and math degrees. JHU-APL conducts programs in fundamental and applied research, exploratory and advanced development, test and evaluation, and systems engineering/integration. From 1965 to 1990 JHU-APL served our nation by providing technical support and testing to improve survivability of the "Pershing" missile systems.

The U.S. Navy continues to be APL's primary long-term sponsor. The Laboratory performs work for the Missile Defense Agency, the Department of Homeland Security, intelligence agencies, the Defense Advanced Research Projects Agency (DARPA), and others. The Laboratory supports NASA through space science, spacecraft design and fabrication, and mission operations. To see JHU-APL markets served and programs offered, see Appendix A, Figures A.1 & A.2.

Office of Technology Transfer at JHU-APL

JHU-APL has a Office of Technology Transfer (OTT) that acts as a link between the viable APL research and technologies and commercial companies who can transition them to the local, national and international marketplace. Figure 1 depicts where OTT falls in the overall JHU-APL Organization. This section discusses the mission and goals of OTT, and also discusses JHU-APL technologies available for transfer.

Figure 1 depicts where OTT is in JHU-APL[5]



APL's basic organization comprises 11 departments. Each department contains a number of groups—our basic hiring/staffing unit. The technical departments also include business areas, which represent the Laboratory's "product lines."

Office of the Director of APL

Office of Technology Transfer

Air and Missile Defense Department

Space Department

Global Engagement Department

National Security Technology Department

Applied Information Sciences Department

National Security Analysis Department

Milton Eisenhower Research Center

Information Technology Services Department

Business and Communication Services Department

Technical Services Department

Human Resources and Services Department

OTT's Mission, Vision and Goals[6]

The mission of the Office of Technology Transfer (OTT) is to broaden the impact of APL's scientific and technical contributions by transferring APL-developed technology to industry to benefit the local economy, the Laboratory and their sponsors.

To maintain their activities with their vision JHUAPL's office of technology transfers has established the following goals. These goals aim at serving markets via bipolar strategy. They invent technology and try to push it to the market to create market need. At the same time, they identify the existing pain areas in the market and try to serve the existing needs by developing technologies to address those issues. OTT has established following goals:

- **Technology Push.** Identify market and license commercially viable technologies to business and industry. In this scenario JHUAPL aims at pushing the new invention to create a market need and push it to the commercial world to make it available to public mass.

- **Market Pull.** Apart from the push methodology, JHUAPL also looks forward to serving any existing pain areas in any specific market segment that technology innovations can eliminate. In the market pull methodology JHUAPL identifies current and future industry needs and matches APL capabilities to those needs through research partnerships.

To accomplish its goals, OTT employs a flexible set of technology transfer tools including:

- License agreements,
- Cooperative research agreements,
- Industrial funding agreements,
- Partnerships with regional high-tech companies, and
- New business spin-offs.

JHUAPL Technologies available to Transfer[7]

JHU-APL has rich portfolio of 700 active inventions and patents in various technologies and in various sectors, namely: Biomedical/Biochemical technology, Communications and distributed systems, electronics technology, information processing and management, materials and structures, sensors, sensor systems, space and environmental physics, systems analysis, test and evaluation, and vehicle technology. . JHU-APL has a rich portfolio with more than 700 active inventions. These inventions include software, tangible products and intangible products (copyrighted material and active/pending patents). The following technologies taken from the laboratory's hundreds of technologies available-for-license provide a glimpse of JHU-APL's rich portfolio.

Technology	Description
Anti-Backfeed Circuit Breaker	Based on a simple, double pole, double throw design, the anti-feedback circuit breaker offers failsafe isolation of generator power from the commercial main power.
Automated Integrated Distress Device (AIDD)	The Automated Integrated Distress Device (AIDD), is a new safety device that boaters can carry aboard their vessels.
Frontier Radio	A low-power, low-mass, radio with advanced communication and navigation features.
Digital Video Authenticator (DVA)	Digital Video Authenticator (DVA) A system that uses frame-by-frame digital signatures, along with chain-of-custody records and a public key infrastructure, to robustly authenticate digital video for use as evidence in a court of law.
Drowsy Driver Detection System	A non-invasive system to detect the onset of fatigue and measure its effect on the driver's activity level and eyelid behavior using low-power Doppler radar and signal processing.
NetTaster	NetTaster is a scalable IntrusiSon Detection System (IDS) that joins real-time network traffic content and node activity to sense both known and zero-day attacks on a network.

Table 1: Sample of featured technologies available to transfer

Past JHU-APL's successful transfers[8]

JHU-APL has been successful in past in transferring some technologies to the commercial market. Some of these are described below.

- Start-up Company Created: Applied Imagery, LLC of Silver Spring, Md. advances APL's QT Viewer™ into The Quick Terrain Modeler and the Quick Terrain Reader.

- Rapid Terrain Visualization, Navigation Planning and Flight Management Software (APL-NAV) is licensed to Optech Incorporated of Toronto, Ontario, Canada.

- Method and Apparatus to Identify and Treat Neovascular Membranes in the Eye and Methods and Apparatus for Improved Visualization of Choroidal Blood Flow and Aberrant Vascular Structures in the Eye Using Fluorescent Dye Angiography, international rights are licensed to Novadaq Technologies, Inc. of Toronto, Ontario, Canada

- Color Landform Atlas of the United States is licensed to North Star of Baltimore, Md

- Polyscore for Windows is licensed to Lafayette Instrument Company, Inc. of Lafayette, Ind.

- Ultrastable Quartz Oscillator Technology (6 inventions and related technical documents) is licensed to Syntonics, LLC of Columbia, Md.
- Automated Risk Management Software is licensed to FutureHealth Corporation® of Timonium, Md.
- CGAI Software and related inventions are nonexclusively licensed to Dot21 Real-Time Systems, Inc. of Columbia, Md.
- HLA Foundation Class (HFC) Software is nonexclusively licensed to Lockheed Martin Federal Systems of Oswego, N.Y.

Target Technology

Now that the team has chosen a technology lab and the team knows which technologies are available to transfer, the team needs to choose a technology that can be successfully transferred to the marketplace. In this section, the team will start with describing current market trends that will help us choose a technology to transfer from JHU-APL's rich portfolio. Then the team will proceed to choose a technology that will help fill this void in the marketplace. the team will then describe the features and architecture of the chosen technology and make a case for which target applications can the technology be successfully applied to. Once the team knows the target technology and its applications, the teamwill make a case for the impact that technology can make.

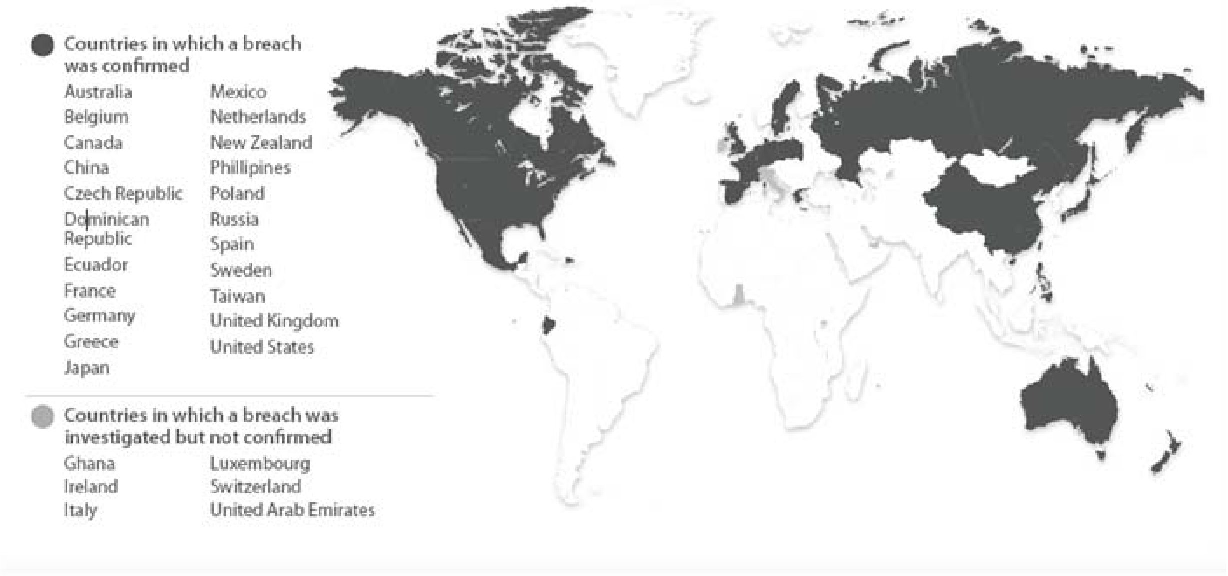
Market Trends

Today the computer systems are used to control and operate the world's electrical grids, oil and gas production, gas distribution facilities, nuclear power plants, water purification systems and financial systems. Accompanying an increase in reliance on internet transmission will also be an increase risk of hacker invasion on these computer systems. Systems, such as electrical utility systems/infrastructure, are at risk due to (computer system – business information system) integration being deployed on a common operating system. This integration allows for better data/information extraction and transmission. Along with benefits for these systems being integrated are also negatives such as a series of vulnerabilities that are opening the door to more viruses, worms and potential cyber-attackers. [9]

The increased number of cyber attacks prompted on political figure, US Representative Langvin, to state in 2010 during a CBS 60 minutes interview that **"***If the power grid was taken off line in the middle of winter, and it caused people to suffer and die, that would galvanize the nation. I hope we don't get there. But it's possible that we will."*[10] One top U.S. intelligence official is on record saying that "the Chinese have already aggressively infiltrated the computer networks of some U.S. banks and are operating inside U.S. electrical grids, mapping out our networks and presumably leaving behind malicious software that could be used to sabotage the systems" Verizon RISK team publishes a Data Breach Investigations Report which is very well regarded in the security industry. 2010 Verizon Data Breach report which Verizon prepared in collaboration with US Secret service showed disturbing trends towards rise of information security incidents. [11]

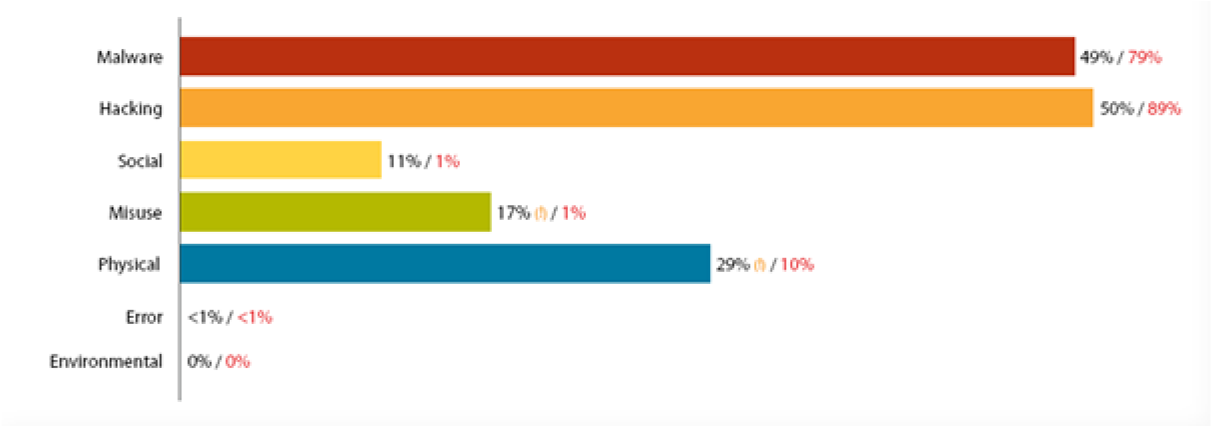
As seen in **Figure 2,** countries represented in 2010 caseload shows the widespread reach of countries in which a security breach was confirmed. As you can see from the graphic, security breaches have over the years increased their spread and now global and are impacting most parts of developed as well as advanced developing world.

Figure 2 Countries represented in 2010 Caseload where a security breach was either reported or confirmed by Verizon Investigations team[12]



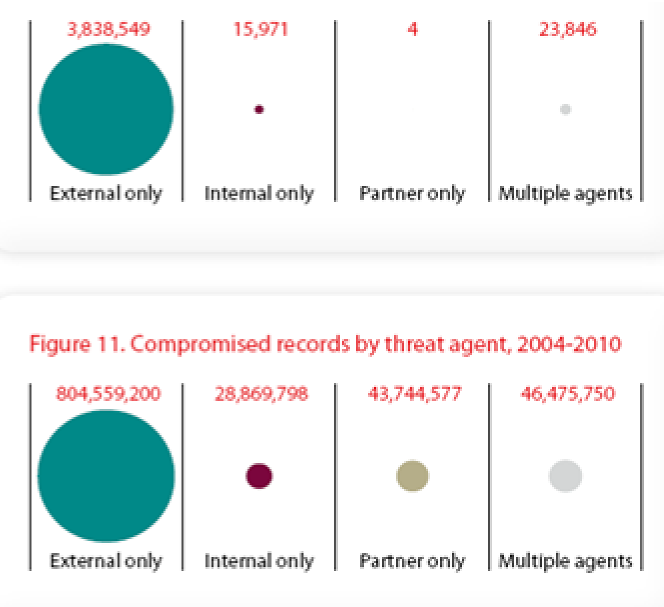
As seen in **Figure 3,** threat action categories by percent of breaches and percent of records classifies these security breaches into various types. For example, of all security breaches reported, 49% were caused by a Malware and impacted 79% of the records compromised. Similarly, hacking accounted for 50% of breaches and impacted 89% of the records compromised. Social Media; Twitter, Facebook, and “the like” misuse resulted in 11% and 17% of security breaches respectively and impacted less than 1 per cent of the records compromised.

Figure 3 Threat Action Categories by percent of breaches and percent of records[13]



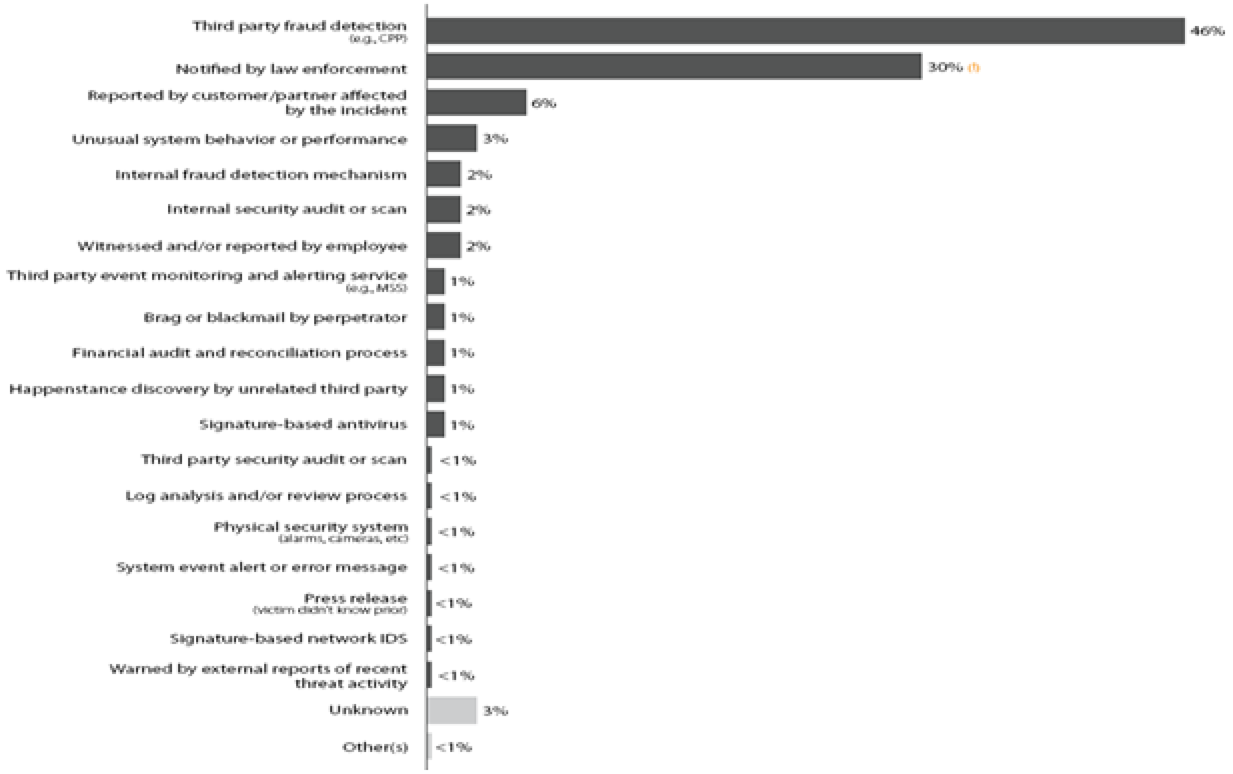
As seen in **Figure 4,** it's conveyed that most records are compromised due to external agents. Verizon RISK team also analyzed and reported overwhelming evidence that most all compromised information is due to external agents.

Figure 4 Threat Action Categories by percent of breaches and percent of records[14]



As seen in **Figure 5**, most attacks that occur are not detected by the user. Most attacks are actually detected by a third party; 46% of fraud detection being reported by fraud detection agencies, 30% of fraud detection being reported by law enforcement, and 6% of fraud being reported by customer/partners. Most users already use intrusion detection devices (IDS), if these devices performed as promised a majority, if NOT all, attacks should be detected. A strong market need for a successful IDS architecture that can detect these security attacks can clearly be established by data in **Figure 5**.

Figure 5 Breach discovery methods by percent of breaches[15]



"On January 14, 2010 McAfee Labs identified a zero-day vulnerability in Microsoft Internet Explorer that was used as an entry point for Operation Aurora to exploit Google and at least 20 other companies" (Operation Aurora, 2010)."[16]

Recently, sophisticated, targeted ZERO Day attacks such as Aurora, APT, Stuxnet and Night Dragon have been making headlines with goals of monetary gain and intellectual property theft. SANS(a company renowned for network security) recently said "we need to start thinking how we are going to defend our networks in the coming years and decades."

Currently the market is served by two types of intrusion detection system:

- **Signature Based IDS.** This type of intrusion detection system relies on attack signatures to detect attacks against nodes on the network. Signature based IDS are incapable of detecting "zero-day" attacks because the attacks signature is not defined.

- **Behavior Based IDS.** This type of intrusion detection looks for a pre-defined behavior. If the behavior of the traffic does not match the normal traffic behavior, this intrusion software will report an attack. Unfortunately, sophisticated hackers are able to fool Behavior Based IDS by presenting malicious payload in a normal manner. This results in this traffic going undetected.

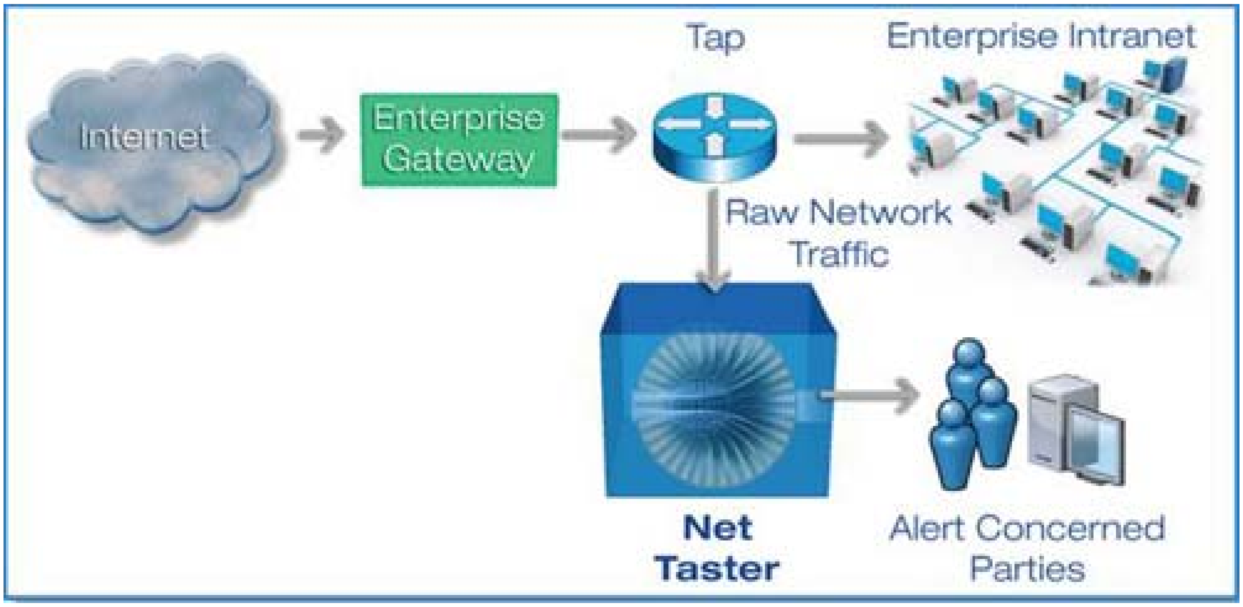
In addition to stated facts, both IDS systems suffer from false positive and negative detections. After all, our individual, societal, and national well being is highly dependent on the well being of these information systems that store and process all our data.

Looking at all above trends and current technologies serving the market, the team zeroed in on NetTaster, a JHU-APL developed technology that can help solve this very problem. NetTaster architecture detects zero day attacks.

Description of NetTaster[17]

NetTaster is a scalable Intrusion Detection System (IDS) that joins real-time network traffic content and node activity to sense both known and zero-day attacks on a network. NetTaster uses cutting-edge dynamic analysis technology to determine the behavior of network nodes in response to incoming traffic. Combining modular architecture with results from multiple analyses allows easy installation of new tools. Furthermore, NetTaster does not require customers to change their existing architecture. In fact, NetTaster can be installed at a border router allowing current infrastructure to remain static and eliminating install time that would traditionally be required if installing software to each computer system. The architecture of NetTaster is shown in **Figure 6** NetTaster Architecture.

Figure 6 NetTaster Architecture[18]



Features of NetTaster[19]

- Scalable: large enterprise networks or resident server
- Provides high detailed report of attack
- Provides specific detail of infection
- Provides specific detail of compromise and notes if data has be extracted
- Combines results of both network traffic analysis and traditional static analysis
- Supplies necessary information to stop future attacks
- Detects ZERO-DAY attacks
- Real-time analysis of downloaded network content
- No changes to in-situ/static network infrastructure
- Combines real-time network traffic content with node activity to detect attacks

Target Application and Application Impact

Many current IDS and anti-malware applications do a great job detecting attacks they were programmed to detect, but none are programmed to detect ZERO-DAY attacks. This deficiency sets the stage or creates a need for NetTaster with its main function to detect zero-day attacks. NetTaster would be a great complimentary asset to any IDS/Anti-malware software; fusing the software would create seemingly superior detection software. With the new found strength in detecting zero day attacks, hackers may find it very difficult to penetrate IDS and Anti-malware protected networks. This fusion might prove critical in winning the cyber war against the unknown insurgents or even unknown political enemies.

Targeted Customer

Many vendors already provide intrusion detection systems and anti-malware to millions of customers. With many of the said vendors having established complimentary assets, market base, and large revenue streams it might be advantageous for JHU-APL to partner with these vendors rather than compete. To all current IDS/Anti-Malware software lacking zero-day attack detection, combining this software with NetTaster would prove to be superior to competitors through comparative/competitive advantage. Hence, the team recommends JHU-APL target the following applications and vendors:

- **IDS Vendors**: Barracuda, Networks, Check Point, Cisco, eEye, Juniper Networks, Radware, Sourcefire, Third Brigade, IBM and Watchguard.
- **Antimalware Vendors**: Symantec, MacAfee (now acquired by Intel), Kaspersky, Norton, Microsoft.

The team recommends JHU-APL to adopt the following technology transfer plan by choosing Symantec as a preferred vendor to commercialize the technology. Following are tables showing some target companies and vendors.

Companies[20,21]	**Business Area**	**Revenues / Customers**
Barracuda, Networks, Check Point, Cisco, eEye, Juniper Networks	• Anti-Malware	Varies (in millions)
Kaspersky Lab	• Success in retail business • Company's current business areas – consumer products and services, corporate solutions and technology licensing to other vendors	Globally revenues grew by 38% year-on-year and exceeded US$500 million
McAfee	• Follow-up service, support, and ongoing subscriptions • The company sells directly and through resellers to corporations and consumers mainly in the US	2010 Revenue: US$ 2,065 million
Symantec	• More focused in enterprise segment	Annual Revenue in 2010: US$ 5,985 million

Table 2: Potential "NetTaster" Vendors

Technology Transfer Model for NetTaster - From JHU-APL to Symantec

The following section presents a series of potential academic technology transfer models along with associated advantages and disadvantages for each. The team will also outline a recommended technology transfer model for JHU-APL to adopt for future technology transfer. The simplest Technology Transfer Plan to implement is the Ramanathan's model (2000)[22]. In his model, technology transfer takes place when the owner of the technology (the transferor) transfers the technology to the business partner (the transferee) to sell and service. This representation implies that the final product (Technology) is simply being sold and serviced by the transferee. (Bommer et al, 1991)

Academic Technology Transfer Models

In the 70's, new models were developed to facilitate the effective planning and implementation of technology transfer projects. The Bar-Zakay Model (Bar-Zakay, 1971) developed a model based on a project management approach. He divided the Technology Transfer process into Search, Adaptation, Implementation, and Maintenance stages. The activities to be carried out were specified in detail in this model.[23] In 2007, Jagoda pointed out that this model focused on buyers who typically are passive recipients who depend greatly on aid programs in the purchase of technology.[24]

The Behrman and Wallender Model (Behrman and Wallender, 1976) propose a seven stage process for technology transfer that may be more relevant to multinational corporations. The seven stages are respectively the manufacturing proposal (Manufacturing and planning processes), Product Design, Infrastructure, Plant construction and production start-up, Local Implementation and Post-Service.[25]

The Dahlman and Westphal Model (Dahlman and Westphal, 1981) carried out considerable work in the Republic of Korea and proposed a nine stage process model as follows: Pre-investment feasibility (Gather information and techno-economic analysis), Technologies Identification, Engineering Studies, (Preparation of manufacturing process), Detailed Engineering Studies, Suppliers, Training Plan, Construct the plant, Commence operation, and Trouble-shooting Skills.[26]

The Schlie, Radnor, and Wad Model (Schlie et al. 1987) proposed a simple, generic model that delineates seven elements that can influence the planning, implementation, and eventual success of any Technology Transfer project. These seven elements are the transferor: entity selling the technology to the recipient, the transferee: entity buying the technology, the technology transferred technology, The transfer mechanism technology transfer mode/medium, the transferor environment (economic status, business orientation, stability, attitude and commitment), the transferee environment (physical and organizational infrastructure, skills available, attitude and commitment to the transfer project, technological status, business orientation, economic status, and stability) and the greater environment global environment surrounding both transferor and transferee.[27]

The Chantramonklasri Model (Chantramonklasri, 1990) proposes a five phase model, pre-investment and feasibility study, developing engineering specifications and design based on the feasibility study, commence capital goods production based on the engineering specifications and designs that have been developed, commissioning and start-up including comprehensive of the workforce and commence commercial production.[28]

Finally, The Ramanathan's - Life Cycle Approach for Planning and Implementing a Technology Transfer Projects takes a holistic view of a Technology Transfer project from its conception to its conclusion and is based on the recognition of the fact that a life cycle of a Technology Transfer project can be looked at from a process perspective as consisting of six major stages.[29] These stages have a respective gate that would allow the transition to the next stage. Both Stage and Gates and the description of the activities are explained in Appendix B. Table 3 below describes the stages and gates in brief.

Number	Stage	Gate
1	Identifying enhancing technologies	Confirming identified technologies
2	Focused technology search	Technology and supplier selection
3	Negotiation	Finalizing and approving the agreement
4	Preparing a project implementation plan	Approving the implementation plan
5	Implementing technology transfer	Implementation audit
6	Technology transfer impact assessment	Developing guidelines for a new project

Table 3: Ramanathan’s - Life Cycle Stages

Plan to transfer NetTaster technology to market based on Ramanathan's model

Based on Ramanathan's Life Cycle stages, NetTaster is at stage 3 - Negotiation stage. At this stage, a vendor needs to be chosen and license agreement needs to be negotiated with the vendor. Once the license agreement is finalized and approved, the technology transfer stage will move on to preparing a stage 4 - project implementation plan. The following section describes each of the subsequent stages proposed in Ramanthan's life cycle stages.

Ramanathan's Stage 3 – Negotiation

First of all, a vendor needs to be chosen who would be most successful in commercializing the NetTaster technology. The team believes that JHU-APL will not be successful as a standalone company competing against the current IDS and Antimalware vendors. The team recommends that JHU-APL needs to partner with one of the already successful players in the market. The list of vendors serving the current market was described in Table 2. Following steps can be taken to market the technology and attract potential vendors.

Showcase Technology through web sites and prototypes

1. Constructing websites in-house
2. Create Prototype to detect Zero-Day-Attack
3. Gather data to prove results

All the above described steps are aimed at creating a prototype and establishing that the technology invented is capable of handling zero-day attacks and gathering the data so as to be prepared for and avoid future attacks.

Build publicity campaign

1. Create a plan for advertising
2. Show case in seminars, conferences, trade fairs
3. Generate lead with existing vendors, organizations

Various channels can be used to bring the technology to market. This being a technology oriented product and most applicable in web based applications all the online channels should be utilized to the fullest. Social media channels like digital marketing, facebook, twitter can be used.

Choosing a vendor

Once the technology is showcased, and there is interest from vendors, among all vendors listed in Table 2, the team recommends JHU-APL partner with Symantec as first adopter/partner. Symantec is very mature and stable company, has a high revenue stream, great market position and the team believes is best suited to successfully launch NetTaster.

Licensing

After Symantec agrees to partner with JHU-APL, the team believes that the terms of the agreement should be non-exclusive license to copy, modify and distribute NetTaster Technology for Symantec. These license terms will enable JHU-APL to transfer the technology to different vendors in future. Some other sample agreement terms currently employed by JHU-APL are given in Appendix 3. In this phase legal may work on getting the agreements ready and finalized which may go through some iteration/negotiation process. Once the agreements are agreed upon and signed-off by both parties, JHUAPL will move on to the next step that is Project Implementation Plan.

Ramanathan's Stage 4 and 5- Preparing and Implementing Technology Transfer Plan

This phase consists of actually creating and implementing a project plan for successful technology transfer. The team proposes following phases for the successful implementation on project

Requirements

The activities in this phase of the project include:

1. Gather requirements for security attacks on existing apps

This is typically needed for IT related projects and is used to understand detailed requirements from individual customer needs point of view.

Architecture and Design

The activities in this phase of the project include:

a. Architecture identification
b. High Level Design
c. Low level design

Architecture design will enable the lab and the organization to identify the boundaries between several of technologies already deployed at the organization and also to identify and special security requirements that need attention. Following the architecture decision, high level design will be created that will lead to low level/detailed design that meets the requirements gathered in the step above.

Development

The activities in this phase of the project include:

a. Coding (if any)
b. Customization and Configuration

In this step, any code modification will be performed for specific needs of the vendor and mostly customization in terms of look and feel, any specific filters and configuration steps will be performed.

Testing

The activities in this phase of the project include:

a. Unit Testing
b. Integration Testing
c. User Acceptance Testing

Testing will be executed at each level, namely – developer, quality assurance group, a group representing the actual users out in the field to ensure the quality of the software delivered to the users at mass out in the market.

The following steps are executed to deploy the software in actual production environment where the organization will actually start using the IDS software in the real life usage environment. Post the deployment

Deployment

This phase consisting of actually applying the software to production.

Ramanathan's Stage 6 Technology Transfer Impact Assessment

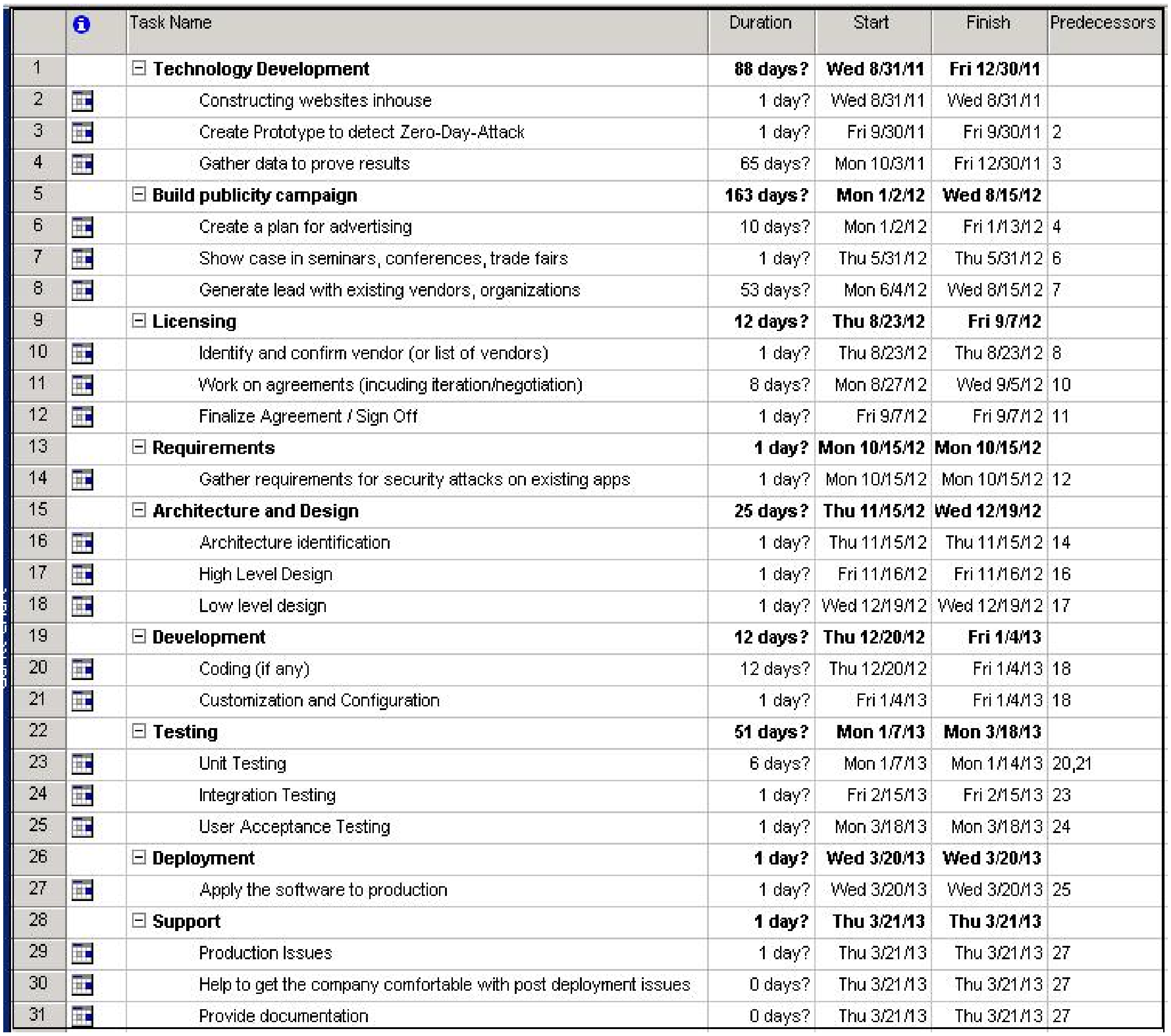
Support

The activities in this phase of the project include:

1. Resolve Production Issues
2. Study the assessment of technology
3. Make Enhancements based on end customer's feedback

A tentative project plan is attached below in Figure 11, depicting the approximate duration for this process to commence – as seen below, this technology can be transferred in as little as one year.

Figure 7 Example Breakdown of Technology Transfer Project



	ℹ	Task Name	Duration	Start	Finish	Predecessors
1		⊟ **Technology Development**	**88 days?**	**Wed 8/31/11**	**Fri 12/30/11**	
2		Constructing websites inhouse	1 day?	Wed 8/31/11	Wed 8/31/11	
3		Create Prototype to detect Zero-Day-Attack	1 day?	Fri 9/30/11	Fri 9/30/11	2
4		Gather data to prove results	65 days?	Mon 10/3/11	Fri 12/30/11	3
5		⊟ **Build publicity campaign**	**163 days?**	**Mon 1/2/12**	**Wed 8/15/12**	
6		Create a plan for advertising	10 days?	Mon 1/2/12	Fri 1/13/12	4
7		Show case in seminars, conferences, trade fairs	1 day?	Thu 5/31/12	Thu 5/31/12	6
8		Generate lead with existing vendors, organizations	53 days?	Mon 6/4/12	Wed 8/15/12	7
9		⊟ **Licensing**	**12 days?**	**Thu 8/23/12**	**Fri 9/7/12**	
10		Identify and confirm vendor (or list of vendors)	1 day?	Thu 8/23/12	Thu 8/23/12	8
11		Work on agreements (incuding iteration/negotiation)	8 days?	Mon 8/27/12	Wed 9/5/12	10
12		Finalize Agreement / Sign Off	1 day?	Fri 9/7/12	Fri 9/7/12	11
13		⊟ **Requirements**	**1 day?**	**Mon 10/15/12**	**Mon 10/15/12**	
14		Gather requirements for security attacks on existing apps	1 day?	Mon 10/15/12	Mon 10/15/12	12
15		⊟ **Architecture and Design**	**25 days?**	**Thu 11/15/12**	**Wed 12/19/12**	
16		Architecture identification	1 day?	Thu 11/15/12	Thu 11/15/12	14
17		High Level Design	1 day?	Fri 11/16/12	Fri 11/16/12	16
18		Low level design	1 day?	Wed 12/19/12	Wed 12/19/12	17
19		⊟ **Development**	**12 days?**	**Thu 12/20/12**	**Fri 1/4/13**	
20		Coding (if any)	12 days?	Thu 12/20/12	Fri 1/4/13	18
21		Customization and Configuration	1 day?	Fri 1/4/13	Fri 1/4/13	18
22		⊟ **Testing**	**51 days?**	**Mon 1/7/13**	**Mon 3/18/13**	
23		Unit Testing	6 days?	Mon 1/7/13	Mon 1/14/13	20,21
24		Integration Testing	1 day?	Fri 2/15/13	Fri 2/15/13	23
25		User Acceptance Testing	1 day?	Mon 3/18/13	Mon 3/18/13	24
26		⊟ **Deployment**	**1 day?**	**Wed 3/20/13**	**Wed 3/20/13**	
27		Apply the software to production	1 day?	Wed 3/20/13	Wed 3/20/13	25
28		⊟ **Support**	**1 day?**	**Thu 3/21/13**	**Thu 3/21/13**	
29		Production Issues	1 day?	Thu 3/21/13	Thu 3/21/13	27
30		Help to get the company comfortable with post deployment issues	0 days?	Thu 3/21/13	Thu 3/21/13	27
31		Provide documentation	0 days?	Thu 3/21/13	Thu 3/21/13	27

Recommendations and Conclusion

As one of our nations pronounced institutions, Johns Hopkins University continues to better our world through superior education and innovation. Johns Hopkins University – Applied Physics Laboratory developed a technology called NetTaster that the team recognizes as an important technology to transfer to our marketplace. In the next decade our systems; electrical, nuclear, water, internet, military and others, will continue to become more integrated, more complex. As our systems increase in complexity so will the need for a superior Intrusion Detection System such as NetTaster. This system has the ability to mate with other IDS/Anti-Malware systems allowing a multi-function detection sytem that will enhance our ability to detect intruders. Now is no better time to start integrating NetTaster into the market place. This proactive approach will enable us to mature this software and continue to realize new and unforeseen security issues.

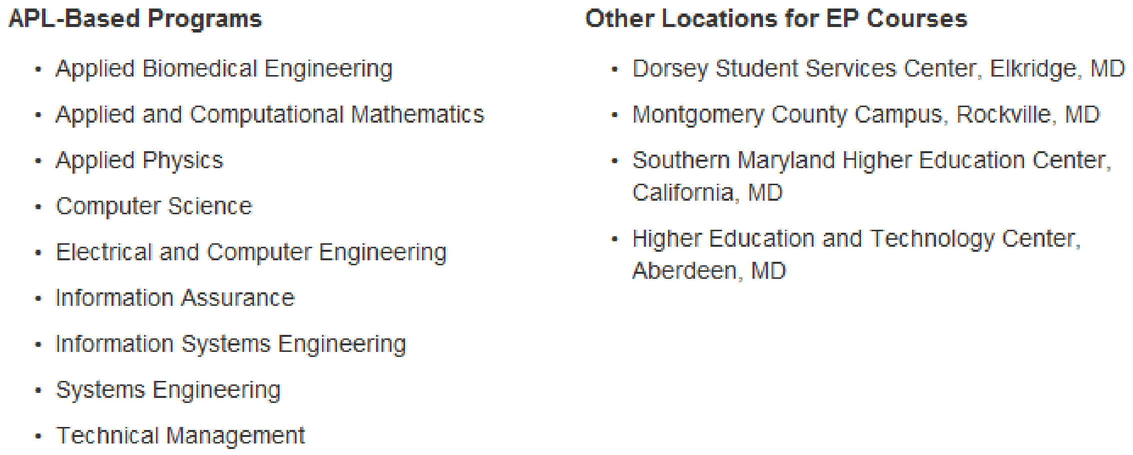
The team recommends JHU-APL:

- Develop, implement, than execute a concrete technology transfer plan using Ramanathan's model and create a project plan based on this model.
- Transfer NetTaster to IDS/Anti-malware vendors, starting with Symantec. Given these vendors are well established having mature: business/organization structure, culture, brand, market share, relationships… in all (Banking, Insurance, Financial institutions, Medical, Educational, Engineering and Government) sectors will help ensure, if not accelerate, widespread adoption.
- Creatively market NetTaster by way of: trade shows, seminars, gorilla marketing, face-to-face presentation, e-marketing and social networking.
- License NetTaster to companies on a non-exclusive basis. JHU-APL may need to provide Orgaware, Humanware, Infoware and Technoware support for successful transfer and may need to modify technology for commercial use.

This type of technology transfer works best to merge research labs and commercial entities. This will not only result in financial benefits for both parties but also result in increased protection for both commercial and national infrastructure.

APPENDIX

Appendix A JHU-APL programs offered and markets served[30]



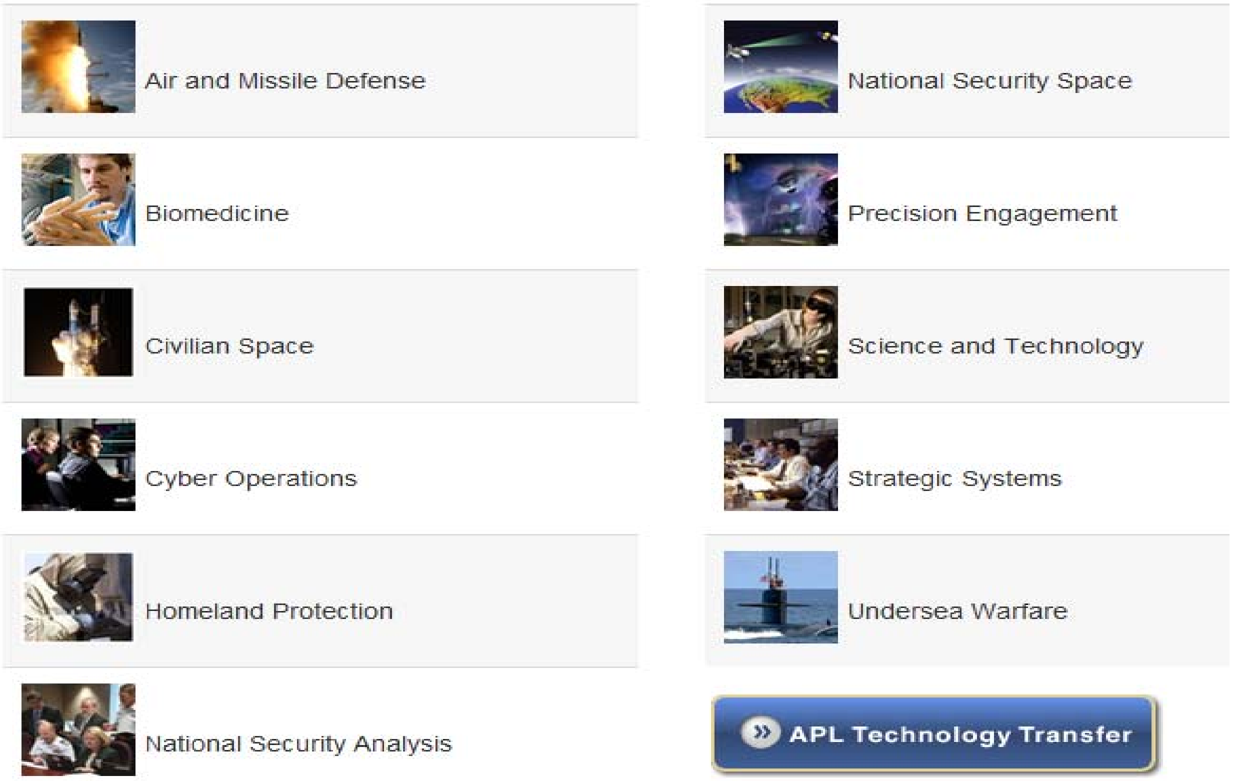
APL-Based Programs

- Applied Biomedical Engineering
- Applied and Computational Mathematics
- Applied Physics
- Computer Science
- Electrical and Computer Engineering
- Information Assurance
- Information Systems Engineering
- Systems Engineering
- Technical Management

Other Locations for EP Courses

- Dorsey Student Services Center, Elkridge, MD
- Montgomery County Campus, Rockville, MD
- Southern Maryland Higher Education Center, California, MD
- Higher Education and Technology Center, Aberdeen, MD

Figure A.1 JHU-APL programs offered



Air and Missile Defense

Biomedicine

Civilian Space

Cyber Operations

Homeland Protection

National Security Analysis

National Security Space

Precision Engagement

Science and Technology

Strategic Systems

Undersea Warfare

Figure A.2 JHU-APL markets served

Appendix B Ramanathan's - Life Cycle Stages[31]

Stages	Activities	Gates	Activities
Identifying enhancing technologies	An informal technology transfer steering committee is set up A list of technologies needed is developed and technology roadmaps are constructed A quick market assessment that examines market size, market potential, and likely market acceptance of the proposed initiatives is carried out A technical assessment is also carried out to estimate, approximately, the resources and capabilities needed to adopt the new technologies	Confirming identified technologies	Criteria Evaluation: Strategic alignment, Project feasibility in terms of technical and resource considerations, Magnitude of opportunity, Market attractiveness, Sales force and customer reaction to the proposed technology, Regulatory, Legal, Policy factors, Financial returns
Focused technology search	How the technology sought is expected to enhance customer value What components of technology are needed The extent to which the abilities to use the technology are available in-house and what gaps have to be bridged The resource commitments needed and the expected benefits Prioritized short list of suppliers for the technology based on their business strategy, technological capabilities, experience in handling TT projects, past performance, and cross cultural expertise. Competitive analysis to assess the impact of the technology sought on competitiveness Based on a consideration of these aspects, a business case is developed that includes clear technology specifications, discounted cash flow (DCF) analysis, project justification, and business plan.	Technology and supplier selection	All suggestions with regard to technology choice, components of technology needed, capability gaps to bridge, resource commitments needed, expected benefits, and supplier profile ratings are critically examined. The technology will be assessed very rigorously using techno-economic, socio, and politico-legal factors. The preferred supplier ranking will be reassessed rigorously based on strategic fit and process support capability and may be modified from the ranking proposed in Stage 2. The financial analysis is rechecked very rigorously here. The team may have to revise the analysis in the light of the critical evaluations (as indicated in the figure) and submit the new analysis for further evaluation. If the decision is a Go-decision then the team is converted to a full technology transfer project team that is empowered,

			multifunctional, and headed by a leader with authority.
Negotiation	Agreeing upon a basis for the valuation of the technology and reaching agreement on issues related to payments and intellectual property protection Delineation of each party's contribution and responsibilities towards the TT project Discussion of issues and methods related to the transfer of coded and not coded aspects of technology including training Creation of effective channels of communication between both parties including visits to each other's facilities Consultation with government authorities to ensure concurrence with government policies and identification of possible barriers, likely policy changes and government support available. Finalizing the most appropriate mechanism(s) for transferring the technology components sought. Preparation of a detailed transfer agreement with emphasis on ensuring intellectual property protection Reaching agreement upon payment amounts, procedures, and time frames	Finalizing and approving the agreement	The comprehensiveness of the detailed transfer agreement The adequacy of intellectual property protection arrangements The appropriateness of the proposed mechanism(s) for transferring the technology The suitability and affordability of the payment amounts, procedures, and time frames
Preparing a project implementation plan	Identification of changes to be made to the organizational structure and work design based on an understanding of the transfer components Identification of changes to be made in the knowledge management system and policy regimes to accommodate the new technology Development of pragmatic training and	Approving the implementation plan	Whether agreement has been reached with the transferor with respect to the schedule Adequacy of the training arrangements Adequacy of the modification of the infrastructure

	education schedules for the workforce that matches with the components to be transferred Formulation of measures to build good relationships between the transfer personnel Formulation of a realistic TT project implementation plan that can form the basis of a working relationship between the transferor and transferee Milestones are specified to help strengthen project management and control.		Intellectual property protection measures Durations of critical activities Quality assurance procedures Payment schedules If these are satisfactory then a go-ahead signal will be given. Otherwise revisions will be needed. At this gate an initial payment to the transferor, if specified in the agreement, will also be approved.
Implementing technology transfer	Identification of changes to be made to the product or process to suit local conditions and making the necessary adaptations. Recruitment and selection of personnel not already available within the organization and conducting training programs for existing staff. Development of improved remuneration plan to facilitate change management. Formulation of arrangements with ancillary suppliers of materials, parts and services based on a make vs. buy analysis Maintaining links with government authorities to keep track of policy changes Commissioning the transferred technology on or before schedule	Implementation audit	Commitment displayed Conflicts experienced Time frames Cost incurred Quality achieved Extent of learning and skill upgrading New knowledge generated Communication effectiveness
Technology transfer impact assessment	Development of a "Balanced Scorecard (BSC)" approach to assess impacts. Identification of the variances (if applicable) between actual and expected outcomes and the formulation of organizational corrective measures.	Developing guidelines for a new project	A new technology transfer project Internal development A mix of both in partnership with the transferor.

	Examining the feasibility of improving the transferred technology. Identification of new or complementary technologies that could be transferred to consolidate the gains made.		

Appendix 3 Sample Licensing Agreement Terms[32]

1. Non-exclusive license to copy, modify and distribute THIRD PARTY SOFTWARE solely as part of LICENSED PRODUCT(S) and LICENSED SERVICES
2. The Company may sublicense others under this Agreement
3. Reimburse JHU for the reasonable costs of preparing, filing, maintaining and prosecuting JHU/APL PATENT RIGHTS (30 days)
4. A nonrefundable initial licensing fee of USD 20,000(30 days)
5. Pay to JHU/APL USD 5,000 annual maintenance fee due within thirty (30) days of each anniversary of the Agreement
6. For the term of this Agreement (until expiration of the patent), the Company shall pay to JHU/APL 10% of Net sales

Bibliography

[1] The John Hopkins University Applied Physics Laboratory, JHUAPL, http://jhuapl.edu/, Accessed on July 20, 2011

[2] Ibid

[3] Arcsight Inc, Research 021-111609-03, Cyber war: Sabotaging the System Managing Network-Centric Risks and Regulations

[4] The John Hopkins University Applied Physics Laboratory, JHUAPL, http://jhuapl.edu/, Accessed on July 20, 2011

[5] The John Hopkins University Applied Physics Laboratory, JHUAPL, http://www.jhuapl.edu/aboutapl/organization/default.asp, Accessed on July 20, 2011

[6] John Hopkins Applied Physics Laboratory Technology Transfer Lab, http://www.jhuapl.edu/ott/default.asp, Accessed on July 20, 2011

[7] John Hopkins Applied Physics Laboratory Technology Transfer Lab, http://www.jhuapl.edu/ott/technologies/technology/all.asp, Accessed on July 20, 2011

[8] Technologies: Success Stories, JHU-APL, http://www.jhuapl.edu/ott/Technologies/successStories/default.asp, Accessed on July 20, 2011

[9] Arcsight Inc, Research 021-111609-03, Cyber war: Sabotaging the System Managing Network-Centric Risks and Regulations

[10] Arcsight Inc, Research 021-111609-03, Cyber war: Sabotaging the System Managing Network-Centric Risks and Regulations

[11] Arcsight Inc, Research 021-111609-03, Cyber war: Sabotaging the System Managing Network-Centric Risks and Regulations

[12] 2011 Data Breach Report: Verizon, http://www.verizonbusiness.com/resources/reports/rp_data-breach-

investigations-report-2011_en_xg.pdf

[13] 2011 Data Breach Report: Verizon, http://www.verizonbusiness.com/resources/reports/rp_data-breach-

investigations-report-2011_en_xg.pdf

[14] Ibid

[15] Ibid

[16] Arcsight Inc, Research 021-111609-03, Cyber war: Sabotaging the System Managing Network-Centric Risks and Regulations

[17] Featured Technology-NetTaster, JHU-APL, http://www.jhuapl.edu/ott/Technologies/successStories/default.asp, Accessed on July 20, 2011

[18] Featured Technology-NetTaster, JHU-APL, http://www.jhuapl.edu/ott/Technologies/successStories/default.asp, Accessed on July 20, 2011

[19] Featured Technology-NetTaster, JHU-APL, http://www.jhuapl.edu/ott/Technologies/successStories/default.asp, Accessed on July 20, 2011

[20] Network security and malware companies, SANS Information, http://www.sans,.org, Accessed on July 10, 2011

[21] Individual company sites for revenue and background information

[22] Ramanathan, K., Taxonomy of International Technology Transfer Modes, Proceedings of the Third International Conference on Operations and Quantitative Management, Sydney, 17-20 December.

[23] Bar-Zakay, S.N., A technology transfer model. Technological Forecasting & Social Change, 2, pp.321-337.

[24] Jagoda, K. I., A Stage-gate Model for Planning and Implementing International Technology Transfer. Doctoral Thesis. University of Western Sydney, Australia.

[25] Behrman J.N. and Wallender, H.W., Transfers of Manufacturing Technology within Multinational Enterprises. Ballinger Publishing Company, Cambridge, MA.

[26] Dahlman, C.J. and Westphal. L.E., The managing of technological mastery in relation to transfer of technology. Annals of the American Academy of Political and Social Science, 458 (November), pp.12-26.

[27] Schlie, T.M., Radnor A. and Wad, A., Indicators of International Technology Transfer. Centre for the Interdisciplinary Study of Science and Technology, North Western University, Evanston.

[28] Chantramonklasri, N., The development of technological and managerial capability in the developing countries. In: M. Chatterji, ed. Technology Transfer in the Developing Countries, the Macmillan Press, London.

[29] Ramanathan, K., Taxonomy of International Technology Transfer Modes, Proceedings of the Third International Conference on Operations and Quantitative Management, Sydney, 17-20 December.

[30] The John Hopkins University Applied Physics Laboratory, JHUAPL, http://jhuapl.edu/, Accessed on July 20, 2011

[31] Ramanathan, K., Taxonomy of International Technology Transfer Modes, Proceedings of the Third International Conference on Operations and Quantitative Management, Sydney, 17-20 December.

[32] John Hopkins Applied Physics Laboratory Technology Transfer Lab, http://www.jhuapl.edu/ott/technologies/technology/all.asp, Accessed on July 20, 2011