Cyber Security Research Developments

Global and Indian Context

Authors:

Atul Kumar, Sr. Analyst
Chiranshu Ahuja, Sr. Analyst

DSCI
PROMOTING DATA PROTECTION

A NASSCOM® Initiative

1. Problem Definition

Today, given the increasing dependence on information and communication technologies (ICT), especially the Internet, for delivery of services and operations, one of the biggest challenges the world faces is that of cyber security. Cyber security is a complex issue, affecting many application domains and straddling many disciplines and fields. Securing the critical infrastructures requires protecting not only the physical systems but, just as important, the cyber portions of the systems on which they rely. The most significant cyber threats are fundamentally different from those posed by the "script kiddies" or virus writers who traditionally have plagued users of the Internet.

Given the kind of activities being carried out in the cyberspace, cyberspace merges seamlessly with the physical world. But so do cybercrimes. Backbone of cyber criminals the underground black market supported by exploit kits, packaged malware and hacks is expected to continue and evolve citing tried-and-true crime ware like Black Hole, ransomware, APTs which have been improved and refined in ways that shows the extent of professionalism and methodology for developing malwares. Cyber attackers can disrupt critical infrastructures such as financial and air traffic control systems, producing effects that are similar to terrorist attacks in the physical space. They can also carry out identity theft and financial fraud; steal corporate information such as intellectual property; conduct espionage to steal state and military secrets; and recruit criminals and others to carry out physical terrorist activities. What makes cyberspace even more attractive to criminals including non-state actors is that attribution in cyberspace is difficult, especially given that cyberspace is borderless and cuts across jurisdictions. It allows criminals to launch attacks remotely from anywhere in the world. With this growing threat landscape, cyber-readiness of the security systems has been constantly put to test.

2. Cyber Security Research

Cyber Security Research is one context where the solution to deal with cyber criminals is germinating. Investment of time and resources requires fostering strategies for research and developing transformative solution to meet critical cyber security challenges involving a certain technology (e.g. cloud computing), or a particular application domain (e.g. finance), or a combination of two.

To begin with the focus of cyber security research is nowadays to deal with new emerging threats and detecting the threats before they effect or cause good amount of damages. With growing number of phishing, APTs and botnet attacks, there is lot to be worked in terms of technological advancements and detection technology to meet the cyber threats of the future.

3. Cyber Security Research – Global Perspective

Following are the cyber security related areas where the nations, companies and academia are focusing their research efforts. All the efforts were made to cover the areas of research still the paper should not be considered as a viable source to encrust full ambit of all the ongoing cyber security research globally.

3.1 Research in Industry

3.1.1 Next Generation Detection Technology

Deploying perimeter security in networks helps to detect and prevent the attacks as early as possible, but the sheer volume of information in the age of Big Data often makes it difficult to detect anomalies that might indicate security issues.

Technological research challenges include binary hardening, network monitoring, IDS and IPS systems, and attack analysis. For instance, to detect and prevent attacks, we need techniques and tools to spot and remove vulnerabilities from software, and monitoring systems to raise an alarm when a system behaves in an anomalous manner.

In order to effectively detect such advanced malware – regardless of the attack methods being used, technology solutions are being developed which use a combination of sophisticated techniques to evaluate advance threats including checking real-time emerging campaigns and known new malicious websites that are being detected across organizations and static code analysis looking for suspicious behavior, obfuscated scripts, malicious code snippets, and redirects to other malicious sites. Further to add, solutions based on dynamic analysis by sandboxing the destination URL or attachments, to simulate a real user on a machine with a goal of observing any changes made to the system, are being worked on.

3.1.2 Command-and-Control Protection

Any enterprise connected to the Internet can become a target of bot driven attack. Unlike widespread attacks, targeted botnet attacks are very stealthy in nature and are difficult to detect using traditional security solutions. However, despite their quiet nature, they can cause very expensive, sometimes irreparable damage to an organization.

Research and product development hints at unique “fingerprint” detection of cloaked C&C traffic which can identify attackers’ use of legitimate applications and websites as well as other advanced techniques, such as the use of internal C&C servers. Deep discovery custom sandbox analysis can also discover new C&C destinations of zero-day malware attacks and update the intelligent network and all customer security protection points.

3.1.3 Malware and Malicious Infrastructure

The threat of malware will remain critical for the foreseeable future. There is already a noticeable trend of increasing malware on social networks, in cloud computing and on mobile devices.

In terms of research, it poses an interdisciplinary challenge. We need advances in technology, for instance in reverse engineering, de-obfuscation, botnet tracking, analysis of criminal infrastructures, and classification and clustering of malware. Likewise, we need reliable methods to estimate the number of infected machines and the effectiveness of counter-measures.

Latest funded development of the Inline Botnet Extraction and Response System, a botnet detection and mitigation tool which also integrates the inline botnet extraction capability, analysis engine, and the signature distributor is the technology direction being witnessed.

3.1.4 Moving Target Defense (MTD)

Cyber attacks are getting more sophisticated and numerous by the day. To combat this threat, future is in deploying automated systems that can react and adapt to reduce the attack surface of IT systems. Developing game changing solutions that increase the cost and risk to the adversary is one key to winning the cyber battle.

Current solutions that harden and defend the Network and System components alone do not properly support the mission due to application layer interdependencies. Application processes often rely on processes running on other servers across a distributed network and are particularly vulnerable to disruptions at the Network and Systems layer.

Research is moving towards delivering MTD technology to address application layer resiliency issues caused by disruptions to the application layer itself and to any of the preceding layers in the IT stack. MTD deployed at the application layer can mask and evade threats to OS/Network and HW/System layer components that can comprise a mission.

3.1.5 Self-Defense Service

IT systems today are static and allow the adversary time to plan and launch attacks. As proposed by in latest research, layered and changing self-defense service prevents attackers from exploiting a target system by removing the static network & system attributes that simplify reconnaissance. Continuously refreshing the target system to a new virtual instance with a known trusted state and random service attributes, this limited-time-use virtual instance is comprised of a single application and OS combination and reduces system complexity.

Further development would proceed on a DNSSEC-aware application that will build on a successful the self-defense service prototype will focus on protecting web services, including web content delivery. Application will allow multi-layer protections by deploying public

interface obfuscation and live service migration technique. It conceals the public interface from adversaries and enables web services to self-defend and self-recover. It is a game-changing cyber defense system, by concealing and by cleaning in contrast to traditional solutions.

3.2 Government Spending on Cyber Security Research

Cyber security research is found to be one of the focus areas in the cyber security strategies of different countries. This focus tends to indicate the willingness of the governments to work with academia and industry and make investments to develop cyber security solutions. The below sample compilation gives an idea of the investments being made by different governments for R&D in cyber security.

- **US:** The Cyber Security Enhancement Act in the US (which has been passed by the US House of Representatives) provisions allocation of **$396 million** for cyber security research and $94 million for providing scholarships to students pursuing cyber security studies, over a period of four years. The Act also focuses on increasing public awareness through various campaigns[1].

  Also, the **National Science Foundation** invests **$20 million** in large projects to keep the nation's cyberspace secure and trustworthy. With researchers from more than a dozen universities, three large "Frontier" collaborative projects highlight efforts to tackle fundamental challenges in cyber security. The three Frontier projects are part of more than 110 new cyber security research projects being funded in 33 states[2].

- **United Kingdom:** GCHQ, The Department for Business, Innovation and Skills, Cabinet Office, the Centre for the Protection of National Infrastructure and the Engineering and Physical Sciences Research Council are working together with academia to increase the UK's academic capability in all fields of cyber security as part of the UK Cyber Security Strategy. Eleven universities have been recognized as conducting world class research in the field of cyber security. As a part of a cross-government commitment towards increasing the nation's academic capability in the field Cyber Security and Research funds amounting to **£3.8 million** have been granted[3].

- **Germany:** Having a foresight to identify societal developments and challenges and develop and apply sustainable strategies on research and develop the solutions of tomorrow to deal effectively with future threats from cyberspace. The **Federal Ministry of Education and Research,** Germany (BMBF) has provided funding of around **€66 million** for projects in IT security and supports innovative procedures and technologies to protect IT systems where data protection plays an important role from attack and unauthorized access[4].

1 http://beta.congress.gov/bill/113th/house-bill/756

2 http://www.nsf.gov/news/news_summ.jsp?cntn_id=128679

3 www.cesg.gov.uk/publications/Documents/academia_datasheet.pdf

4 http://www.bmbf.de/en/73.php

Current developments will provide a stimulus to enhance the depth and breadth of cyber security research and also help make nations more resilient in cyberspace by extending knowledge and enhancing skills in cyber security.

3.3 Focus Cyber Security Research Areas for Governments

The governments around the world are eyeing continuous research in the field of cyber security to safeguard against the emerging and future threats. Some of the cyber security research areas that are in focus by various countries like Australia, Japan, Canada and USA are briefly mentioned below.

- The **Cyber Security Research Roadmap** released by the **Department of Homeland Security** (DHS) in the US, identifies the following eleven hard problems that require R&D efforts:

    a. Scalable trustworthy systems (including system architectures and requisite
    b. development methodology)
    c. Enterprise-level metrics (including measures of overall system trustworthiness)
    d. System evaluation life cycle (including approaches for sufficient assurance)
    e. Combating insider threats
    f. Combating malware and botnets
    g. Global-scale identity management
    h. Survivability of time-critical systems
    i. Situational understanding and attack attribution
    j. Provenance (relating to information, systems, and hardware)
    k. Privacy-aware security
    l. Usable security

- The **Science & Technology (S&T) Directorate** of the **DHS** runs a **Cyber Security Division Program** through which the DHS leads the government's charge in funding cyber security R&D that results in deployable security solutions and implementation of an aggressive cyber security research agenda encompassing the full lifecycle of technology—research, development, test, evaluation, and transition to practice—to produce unclassified solutions that can be implemented in both the public and private sectors. To accomplish its mission and serve its customers, CSD has organized its work into five major program areas[5]:

    Trustworthy Cyber Infrastructure (TCI) — focuses on ensuring that the nation's critical infrastructure – such as the oil and gas pipelines, information infrastructure, and the Internet – become more secure and less vulnerable to malicious and natural events.
    - Internet Measurement and Attack Modeling
    - Process Control Systems (PCS) Security
    - Secure Protocols

5 http://www.dhs.gov/csd-program-areas

- Cyber Infrastructure & Emerging Threats (DECIDE)

Foundational Elements of Cyber Systems (FECS) — focuses R&D activities on the characteristics that are essential to the desired end-states of trustworthy cyber systems and accelerates the transition of new cyber security technologies into commercial products and services.

- Cyber Economic Incentives
- Enterprise Level Security Metrics and Usability
- Homeland Open Security Technology (HOST)
- Leap Ahead Technologies
- Moving Target Defense
- Software Quality Assurance
- Tailored Trustworthy Spaces

Cyber Security User Protection & Education (CUPE) — focuses R&D activities on developing ways to help all types of users – from improving the security and protection of user online activity, to attracting the next generation of cyber security warriors, to providing the tools needed for investigating cyber criminal and terrorist activity.

- Cyber Security Competitions
- Cyber Security Forensics
- Identity Management & Data Privacy Technologies
- Insider Threat

Research Infrastructure to Support Cyber Security (RISC) — provides a national and international-level research infrastructure to enable the cyber security research community to discover, test, and analyze state of-the-art tools, technologies, and software in a scientifically rigorous and ethical manner.

- Experimental Research Testbed (DETER)
- Research Data Repository (PREDICT)
- Software Assurance Marketplace (SWAMP)

Cyber Technology Evaluation and Transition (CTET) — provides a coordinated process of assessments, evaluations, and operational experiments and pilots to transition the fruits of research into practice.

- Cyber Security Assessment and Evaluation
- Cyber Security Experiments and Pilots
- Transition to Practice

- The **National Strategy for Trusted Identities in Cyberspace** (NSTIC) in the US intends to create an 'Identity Ecosystem' wherein individuals and organizations will be able to trust each other as they follow agreed upon standards to obtain, authenticate and maintain their digital identities, and also of devices. The aim is to pull together software, services and hardware components, to address the entire identity lifecycle of establishment, management and usage. This research is driven by the fact that trusted identities

provide a variety of benefits including enhanced security and improved privacy, which in turn boost the trust in the online businesses. Individual users will be able to choose from a mixed bag of secure, privacy-enhancing and interoperable identity solutions in a manner that promotes confidence, privacy, choice, and innovation[6].

- The **U.S. Army Research Laboratory** (ARL) established a Collaborative Research Alliance led by **Pennsylvania State University** for research program to develop and advance the state of the art of Cyber Security. The areas focuses on development theories and models that relate properties and capabilities of cyber threat detection and recognition processes/mechanisms to properties of a malicious activity and support planning and control of cyber maneuver that would describe how control and end-state of the maneuver are influenced by fundamental properties of threats, such as might be rapidly inferred from limited observations of a new, recently observed threat[7].
- A focused research theme by **Australian Government's Cooperative Research Centre for Cyber Security** emphasizes cyber security solutions and research including ultra-high speed defense, Wireless cloud, BYOD, IPV6 and Internet of Things[8].
- **Network Security Research Institute of National Institute of Information and Communications Technology, Japan** is concentrating on three major research and development topics: cyber-security technology, which establishes a technical basis for leading-edge cyber-attack monitoring, tracking, analysis, response, and prevention to help solve social problems; security architecture technology, which provides secure networks by establishing techniques for optimized configuration, design, and evaluation of secure networks, including mobile, cloud, and new-generation NW; and security fundamentals technology, which establishes practical next-generation cryptographic technologies ranging from modern cryptography to quantum security[9].
- Cyber security research and experimental development program of **Communications Security Establishment, Canada** focuses its research on technical measures for blocking cyber-attacks, promising scientific approaches which comprehensively and rigorously underpin required security policy and engage research labs to investigate cyber security related research gaps and to de-risk scientific approaches and emerging technological solutions[10].

6 http://www.nist.gov/nstic/

7 http://www.arl.army.mil/www/default.cfm?page=1417

8 https://www.cybercrc.com/programs/next-generation-cyber-security-technologies/

9 http://xn--vuq85rhnhcvjeva615d9zdhy8c.jp/en/nsri/index.html

10 http://www.cse-cst.gc.ca/documents/publications/jro-bcr/csredp-prdecs-eng.pdf

4. Cyber Security Research – Indian Perspective

Over the past few years, India has witnessed massive adoption of cyber technologies in all the facets of life. This adoption on one hand is enabling nation to attain high economic growth, welfare, empowerment and active participation of people in policy matters, but on the other it is raising concerns and challenges from cyber security and privacy view point. These challenges become more severe when affecting the national security and economic prospects of the country. Moreover, India being a preferred outsourcing destination for IT and BPM services requires a focused and continued attention on security and privacy. This attention is essential to maintain confidence of the global clients, as security and privacy considerations are key parameters in the outsourcing decisions. Therefore, a demand for adequate efforts and investment in cyber security capability building and R&D activities has also been emerged in the cyber ecosystem.

Cyber security capability building is a rising phenomena globally and India is no exception in this and in the recent past country has witnessed significant improvement in this domain. R&D activities in cyber domain are gaining traction in private sector and academia in India, with the support of and encouragement by the government. In recent past country has witnessed numerous successful research outcomes and many of them have been translated into businesses, through the emergence of indigenous cyber security companies. Academia is playing a crucial role in India to build a healthy ecosystem for the cyber security research, which is evident from rising of indigenous cyber security companies emerging out from the incubation centers of these academic institutions. The global acceptance for the wide range of indigenous products & services offered by these companies has also been seen in recent past, validating indigenous competence. Traditional IT services providers are also giving due prominence to cyber security domain and some of the players have expanded their research activities in cyber security. In this paper, some of the ongoing research activities in the country have been discussed and this paper should not be considered as a credible source for all the ongoing research activities in the country. Some of the research areas are highlighted below.

Quantum Cryptography & Secure Multiparty Computation

R&D activities in India are focused both on the contemporary requirements and high-tech and futuristic need of security in cyberspace. Research in futuristic area such as Quantum Cryptography which allows conducting various cryptographic tasks that are proven to be impossible with classical processing is being undertaken by the researchers. This results in a highly secured communications (such as sharing of keys or sharing of information which is accessible to the receiver only at a specific location) among the parties, and allows detection and elimination of eavesdropping during the transit.

Secure Multiparty Computation and Privacy Preserving Data Mining are few research areas which enable data-mining algorithms to be executed on congenital data without revealing the same, and allow parties to jointly compute a function over their inputs, and keep these inputs private. In view of enormous opportunities that exist in the data-mining and analysis field and

inherent concerns around privacy and security in such analysis (as in case of medical records processing), this research area is gaining significant traction and already being undertaken by researchers in the country.

Threat Intelligence

Cyber threat landscape is expanding enormously in the cyberspace. Research related to mitigating cyber threats is already being undertaken by the researchers as a priority item. Response mechanism to cyber threats has changed from being reactive to proactive. This change in the response mechanism requires robust threat intelligence system to defend any of the evolving threats. R&D activities are already underway at various research organizations in India in areas such as threat research & response, specifically for Malware research analysis, Worm Propagation and Detection, Targeted remote malware clean-up, Advanced Persistent Threat Countermeasure, anomaly detection for zero-day attack, Intrusion Detection Systems, SPAM Detection & Filtering, exploitation and Reverse engineering, among others. Research is also being carried out on advancement of automated tool to simulate human hackers, one of the ways to create the threat intelligence. Moreover, some of the organizations are also working in the domain of antivirus and anti-malware research & development. As research outcomes, well accepted solutions catering to enterprises and end users, are already available in the Indian as well as global market.

Next Generation Firewall

Research organizations are also working in future-ready security solutions and Multi identity-based technology such as Next Generation Firewall, that offer security intelligence to enterprises and enable them to apply required and best suited security controls at the network perimeter. Integration of aforesaid technology with other security solutions such as threat intelligence and management systems, Web Application Firewall, Web filtering, Anti-Virus, Anti-Spam, etc, will help in creating more efficient and secure ecosystem.

Secured Protocol and Algorithms

Research in protocols and algorithms is an important aspect for strengthening the cyber security posture at a technical level. Protocols and algorithms define the rules for information sharing and processing over cyberspace. In India, research has also been undertaken at protocol & algorithm level such as Secure Routing Protocols, Efficient Authentication Protocols, reliability Enhanced Routing Protocol for Wireless Networks, Secure Transmission Control Protocol and Attack Simulation Algorithm, etc. These research activities are of great interest to the defense, critical sectors and other sensitive communications in the nation.

Authentication Techniques

It is important to establish trust and credibility in critical business processes that can be achieved through advance authentication techniques. In the country, research is moving towards authentication techniques such as Key Management, Two Factor Authentication,

Automated key management which provides the ability to encrypt and decrypt without a centralized key management system, File protection both on rest as well as in transit, access controls solutions on cloud, among others. Content protection especially in case of multimedia content distribution on web is a challenge for organizations which experience revenue loss because of unauthorized distribution and access. Some solutions have already been developed indigenously to address this problem. Moreover, research is underway for more advance products and solutions in this area.

BYOD, Cloud and Mobile Security

Increased adoption of varied types of mobile devices has raised the demand for initiating research that addresses the security and privacy related challenges. Application, Network and Mobile security testing technologies, BYOD risk mitigation, Cloud security assessment and protection are some of the areas where advancement of technologies is taking place through R&D activities.

Cyber Forensics

With the proliferation of the Internet, cyber-crime incidents have also increased, and elevated the demand of advance forensic technologies to expedite investigation and attribution process. In India, the research is being carried out to build indigenous capabilities for cyber forensics. Some of the specific areas in which research is taking place in the country are: Disk Forensics, Network Forensics, Mobile Device Forensics, Memory Forensics, Multimedia Forensics and Internet Forensics.

Other areas in which researches are being undertaken are Internet Monitoring Systems, Extensive web security, Wireless Network Security Enhancement, VOIP security, encryption & cryptography, and encryption as a service among others. These indigenous research activities are moving towards enhancing the capabilities of existing technologies and also evolving advanced solutions with new and innovative ideas.

5. The Way Forward for India

For strengthening the cyber ecosystem, a focused attention and adequate investment of efforts & resources would be required for cyber security. Investment in the R&D activities in cyber security domain could result in high returns such as opportunities for entrepreneurs leading to expansion of businesses which in turn could result in more jobs in the market, increased trust & credibility and self-reliance of the nation. Though R&D activities pertaining to cyber security being undertaken in India have risen lately, a lot more needs to be done, specially to match the level of technological advancements happening globally. By virtue of its dynamic nature, cyber security requires continuous tracking of evolving technologies globally and its alignment with a country's R&D objectives and agenda. Increasing role of cyberspace puts in place a high demand of extensive R&D activities to be carried out in the nation, with a set agenda. This

demand is re-enforced in the light of huge opportunities that exists in the global and domestic market.

Contribution would be required from all the stakeholders - government, Industry and academia - requiring that they come together and define a cyber security R&D roadmap for the country. Public Private Partnership (PPP) is the way forward, as it would help in combining best of both worlds and complement capabilities to develop a securer cyber ecosystem. Arrangements also need to be put in place for retaining the talent in the country and providing appropriate protection to the IPRs developed by the indigenous cyber security research organizations. The government should fund research in academia and also in the industry, and provide incentives to the businesses for investing in R&D activities. The research should be market driven, and deliver solutions for the real world.

The emergence of cyberspace as fifth domain requires attention, and enhancement of R&D capabilities stands as an important component. There is growing focus on developing R&D capabilities in India. Enormous opportunities exist and sustained efforts need to be undertaken to take forward the momentum built in our country.

DATA SECURITY COUNCIL OF INDIA

A NASSCOM® Initiative

L: Niryat Bhawan, 3rd Floor, Rao Tula Ram Marg, New Delhi - 110057, India
P: +91-11-26155071 | F: +91-11-26155070 | E: info@dsci.in | W: www.dsci.in