NEWSLETTER

October 2017

National Critical Information Infrastructure Protection Centre

VOLUME 1 ISSUE 4

@NCIIPC

NCIIPC Newsletter

October 2017

Inside This Issue

1	Message from NCIIPC Desk
2	News Snippets - National
4	News Snippets - International
7	Security App
7	Learning
11	Trends
17	NCIIPC Initiatives
20	Vulnerability Watch
22	Upcoming Events – International
23	Upcoming Events - National

Social media is a great way to connect. In this endeavour, NCIIPC has started its Twitter handle @nciipc to engage with the community and its stakeholders.

Message from the NCIIPC Desk

Dear Readers,

Welcome to the fourth issue of the NCIIPC Newsletter. In the issue we bring several positive developments in the national cyber security domain. India has been ranked 23rd in the Global Cyber Security Index released by International Telecommunication Union (ITU). India has been ranked ahead of its neighbours China and Pakistan who are positioned at 32nd and 67th respectively. According to the survey, India lacked in sectoral specific CERT, which the Government of India has already initiated by setting up separate CERTs for Finance, Power and Telecom sectors. India has signed a MoU for cooperation on Cyber Security with Bangladesh. India has held bilateral dialogues on cyber security with the European Union and Japan. The dialogues emphasised on applicability of International laws in the field of Cyber Security. Recently the State Government of Punjab has made the cyber security compliance mandatory for its websites. It is an exemplary effort which we hope will be followed by other state governments.

In international events, People's Republic of China made a major breakthrough by sending the first quantum encrypted communication through space. It is being said that it is an ambitious project by China to secure its military communications. In Ukraine police seized servers of an accounting software company, which is suspected of spreading the 'NotPetya' ransomware in June this year. It's a new strategy of spreading malware through applications used by employees in critical sectors. It gives us a new dimension to work upon for the security of Critical Information Infrastructure (CII).

Social media is a great way to connect. In this endeavour, NCIIPC has started its Twitter handle @nciipc to engage with the community and its stakeholders. Please follow us to receive the latest alerts, advisories and updates. We wish a very happy and safe *Deepawali* to all of our readers. We solicit your feedback and contributions to make our newsletter more lively and relevant.

News Snippets - National

Cyber Spying Campaign, against Indian and Pakistani Entities

Source: www.reuters.com

Symantec Corp. has identified a cyber spying campaign, against Indian and Pakistani entities involved in regional security issues. In a report, Symantec said the online espionage effort dated back to October 2016. The campaign appeared to be the work of several groups, but tactics and techniques used suggest that the groups were operating with "similar goals or under the same sponsor", probably a nation state. The malware utilizes the so-called 'Ehdoor' backdoor to access files on computers. To install the malware, the attackers used decoy documents related to the security issues in South Asia. The documents included reports from *Reuters*, *Zee News*, and *The Hindu*, and were related to military issues, Kashmir, and militancy.

The documents included reports from Reuters, Zee News, and The Hindu, and were related to military issues, Kashmir, and militancy.

Industry and Government need to have a Collaborative Outlook

Source: www.smetimes.in

Release of FICCI & Pinkerton report on 'India Risk Survey 2017'

The industry and the Government need to have a collaborative outlook to address the risk of information and cyber insecurity, said Alok Joshi, Chairman, NTRO during a FICCI seminar on 'New Age Risks 2017', held in New Delhi. He said, "It is becoming difficult for businesses as well as Governments to deal with non-state actors located outside, who are involved in cyber-attacks. Once any business becomes part of the Internet then it becomes a part of the global network and cannot operate in isolation. In this regard, Industry and Government need to have a collaborative outlook to address the emerging threat of information and cyber insecurity." He also mentioned that NCIIPC has successfully safeguarded 300 establishments across India from the recent worldwide cyberattack by the 'WannaCry' ransomware. On the occasion, Gopal Krishna Agarwal, National Spokesperson for Economic Issues, Bharatiya Janta Party and NTRO Chairman Alok Joshi along with other dignitaries released the FICCI & Pinkerton report on 'India Risk Survey 2017'. The report highlighted the severity of risks and their impact cross economic sectors and geographical regions of the country.

Once any business becomes part of the Internet then it becomes a part of the global network and cannot operate in isolation.

Note: Different frameworks and guidelines have been provided by NCIIPC in this aspect. The industry is also constantly upgrading technology to support such frameworks. Industry players such as Cloud service providers, ISP/TSP etc. play a vital role in implementing these guidelines and providing a secure environment for others. Close coordination in terms of sharing information with the agencies like NCIIPC during an incident is the need of the hour.

Areas of discussion included domestic cyber policy landscape, cyber threats and mitigation, Internet governance, mechanism on bilateral cooperation and possible cooperation at various international and regional fora.

The Fourth India - European Union Cyber Dialogue

Source: http://economictimes.indiatimes.com

India and European Union (EU) stressed on the need to deepen deliberations on the applicability of international law to cyberspace and set norms of responsible behaviour of states. During the fourth India-EU cyber dialogue, the two sides also reaffirmed their commitment to an open, free, secure, stable, peaceful and accessible cyberspace, enabling economic growth and innovation. Led by Sanjay Kumar Verma, Joint Secretary in the Ministry of External Affairs, the Indian delegation had representatives from the Ministry of Electronics and Information Technology, National Security Council Secretariat, CBI, Department of Telecommunication, NCIIPC and NIA. The EU delegation was led by Herczynski Pawel, Director for Security Policy, European External Action Service, who was accompanied by representatives from European External Action Service and officials from the EU Delegation in New Delhi. The two sides reaffirmed that the bilateral cyber dialogue provided a strong foundation for existing and future cooperation. Areas of discussion included domestic cyber policy landscape, cyber threats and mitigation, Internet governance, mechanism on bilateral cooperation and possible cooperation at various international and regional fora. Both sides agreed to hold the next India-EU Cyber dialogue in Brussels in 2018.

Government of Punjab has asked all its departments, boards, corporations, societies and public sector undertakings to undertake thorough cyber security audit and send a compliance report.

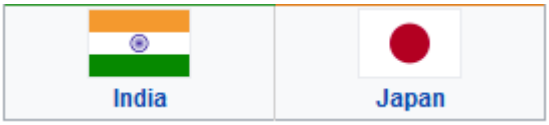
Government of Punjab to undertake thorough Cyber Security Audit

Source: http://timesofindia.indiatimes.com

The Government of Punjab has asked all its departments, Boards, Corporations, Societies and Public Sector Undertakings to undertake a thorough cyber security audit at their own cost and send a compliance report. These directions have been issued by the Punjab State e-Governance body following a proposal from NCIIPC. Many websites have been attacked by hackers in the past. Recently, on August 15, the website of Real Estate Regulatory Authority on the Punjab Urban Planning and Development Authority's website was hacked. Pro-Pakistan slogans were put on the webpage along with picture of Kashmiri militant. The government has tasked NCIIPC to coordinate, monitor, collect, analyse and forecast national level threat to CII for policy guidance. However, the basis responsibility for protecting the CII shall be with the agency running it. NCIIPC will also be developing and organising training and awareness programmes for protection of CII. It will also ensure development of audit and certification agencies for CII protection.

Second Japan-India Cyber Dialogue

Source: http://www.ptinews.com



India and Japan have resolved to strengthen their cooperation in the field of cyberspace, and reaffirmed their commitment to an open, secure and accessible cyberspace, enabling economic growth and innovation, the Ministry of External Affairs said. The 2nd Japan-India Cyber Dialogue, held on 17th August, saw discussions on domestic cyber policy landscape, cyber threats and mitigation, mechanism on bilateral cooperation and possible cooperation at various international and regional forums. Both sides attested that existing international law is generally applicable in cyberspace. At the same time no country should conduct or support ICT (Information Communication Technology)-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to its companies or commercial sectors, a statement by the ministry said. The Japanese delegation was led by Masato Otaka, the envoy in charge of Cyber Policy and Deputy Director General of Foreign Policy Bureau, Ministry of Foreign Affairs of Japan. The Indian delegation was led by Sanjay Kumar Verma, Joint Secretary in the MEA, and comprised representatives from the ministries of electronics and information technology and home affairs, NSCS, CBI, NIA, Dept. of Telecommunication, and NCIIPC. Both sides agreed to hold the next Japan-India Cyber dialogue in Tokyo in 2018.

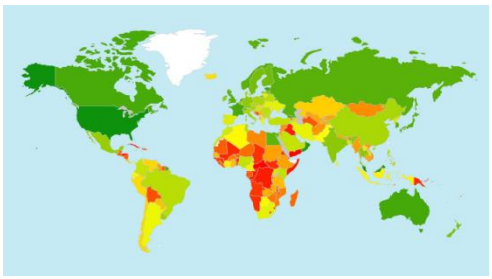
Both sides attested that existing international law is generally applicable in cyberspace. At the same time no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to its companies or commercial sectors.

News Snippets - International

India Stood 23rd in Global Cybersecurity Index

https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

This report has been produced by the International Telecommunication Union (ITU). First launched in 2014, the goal of the Global Cybersecurity Index (GCI) is to help foster a global culture of cybersecurity and its integration at the core of ICTs. The GCI revolves around the ITU Global Cybersecurity Agenda and its five pillars (legal, technical, organizational, capacity building and cooperation). The GCI results reported cover all 193 ITU Member States. The GCI is included under Resolution 130 (Rev. Busan, 2014) on strengthening the role of ITU in building confidence and security in the use of ICT. Singapore has got the first position with score of 0.925. United States stood second with score of 0.919. India has got 23rd place with score of 0.683. China stood 32nd with score of 0.624. Bangladesh and Pakistan has got 53rd and 67th positions respectively.



Heat Map of National Cybersecurity Commitments
Green (highest) to Red (lowest)

Member State	Score	Global Rank
Singapore	0.925	1
USA	0.919	2
Malaysia	0.893	3
Oman	0.871	4
Estonia	0.846	5
Mauritius	0.83	6
Australia	0.824	7
Georgia	0.819	8
France	0.819	8
Canada	0.818	9
Russian Federation	0.788	10

Mia Ash LinkedIn page

Geographical distribution of non-photography LinkedIn connections of Mia Ash. The darker is the blue shading, the higher the concentration of connections from that country. (Source: SecureWorks)

A well-established collection of fake social media profiles that appear intended to build trust and rapport with potential victims.

COBALT GYPSY has used spear phishing to target telecommunications, government, defence, oil, and financial services organizations.

Targeted Social Engineering Attacks on CII Employees

https://www.secureworks.com/research/the-curious-case-of-mia-ash

In early 2017, SecureWorks® Counter Threat Unit™ (CTU) researchers observed phishing campaigns targeting several entities in the Middle East and North Africa (MENA). The campaigns delivered PupyRAT, an open-source cross-platform remote access Trojan. CTU™ researchers observed likely unsuccessful phishing campaigns being followed by highly targeted spear phishing and social engineering attacks from a threat actor using the name Mia Ash. Further analysis revealed a well-established collection of fake social media profiles that appear intended to build trust and rapport with potential victims. The connections associated with these profiles indicate the threat actor began using the persona to target organisations in April 2016. CTU researchers assess that COBALT GYPSY (formerly known as TG-2889) group is likely responsible for these campaigns. COBALT GYPSY has used spear phishing to target telecom, govt., defence, oil, and financial services organisations based in or affiliated with the MENA region, identifying individual victims through social media. CTU researchers assess it highly likely that the Mia Ash persona is a fake identity used to perform reconnaissance on and establish relationships with employees of targeted organisations. CTU researchers categorised connections associated with the Mia Ash into photography versus non-photography profiles. The non-photography endorsers were located in Saudi Arabia, US, Iraq, Iran, Israel, India, and Bangladesh and worked for technology, oil/gas, healthcare, aerospace, and consulting organisations. They were mid-level employees in technical or management roles with job titles such as technical support engineer, software developer, and system support.

Note: A strict social media policy must be adhered to in organisations. Deployment of anti-spam and anti-phishing solutions is necessary to avoid targeted attacks. Organisations should apply regular patches and update systems. Organisations should conduct regular awareness programs among employees.

Ukraine's National Postal Service Hit by DDoS Attack

Source: www.bbc.com

Ukraine's national postal service was hit by a two day long cyber-attack targeting its online systems. Unknown hackers carried out a DDoS attack against *Ukrposhta*'s website. The attack began on a Monday morning, up to 21:00 local time and continued again on next day.

Укрпошта
@ukrposhta

This is not the first time that Ukraine's postal service has been targeted this year - in June, *Ukrposhta* was hit by the 'NotPetya' ransomware attacks, as part of wider attacks.

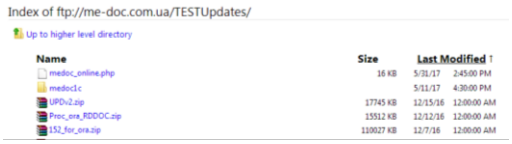
Note: Protection strategy such as deployment of dedicated DDoS mitigation appliance which needs to be constantly updated by the IT security team with the latest threats, Cloud mitigation providers, providing DDoS mitigation from the cloud, update rules for firewall to mitigate DDoS.

Ukrainian Police Seized the 'NotPetya' Outbreak Servers

Source: www.bleepingcomputer.com

Ukrainian Police seized the servers from where the 'NotPetya' ransomware outbreak first started to spread. The servers belonged to Intellect Service, a Ukrainian company that sells accounting software under the names of IS-pro and M.E.Doc. The group behind 'NotPetya' compromised the company's servers and pushed malicious updates for the company's M.E.Doc software, which in turn installed the 'NotPetya' ransomware. The 'NotPetya' group obviously miscalculated the ransomware's self-spreading component, and just like 'WannaCry' last month, 'NotPetya' spread uncontrollably to many countries around the globe. While Intellect Service denied any wrongdoing, Microsoft, Bitdefender, Kaspersky, Cisco, and ESET have gone on record saying the M.E.Doc update servers were responsible for the initial 'NotPetya' infections.

The servers from where the NotPetya ransomware outbreak first started to spread.

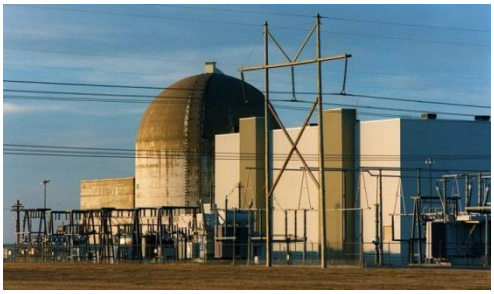


An ESET report includes visual evidence, an image of a PHP backdoor (medoc_online.php) found on the company's update server during past incidents.

Hackers Penetrating the Nuclear Power Stations

Source: www.nytimes.com

Since May this year, hackers have been penetrating computer networks of companies that operate nuclear power stations and other energy facilities, as well as manufacturing plants in the United States and other countries. In most cases, the attacks targeted engineers who have direct access to systems that, if damaged, could lead to an explosion, fire or a spill of dangerous material. The origins of the hackers are not known, but the report indicated that an "advanced persistent threat" actor was responsible. Hackers wrote highly targeted email messages containing fake résumés for control engineering jobs and sent them to the senior industrial control engineers who maintain broad access to critical industrial control systems, the government report said.



The Wolf Creek nuclear power plant in Kansas. The corporation that runs the plant was targeted by hackers.

Note: Critical networks such as ICS/SCADA require strict policy of segregation from corporate networks. Solutions such as Data Diode, simplex one way communication may be deployed for same. No personal communication through official emails should be allowed.

Security App

ShieldFS Makes Filesystem Immune to Ransomware Attacks

http://shieldfs.necst.it/continella-shieldfs-2016.pdf

SHIELDFS
A Self-healing, Ransomware-aware Filesystem

ShieldFS was able to detect the malicious activity at runtime and transparently recover all the original files.

Researchers from Politecnico di Milano, Milan, Italy have proposed a solution called ShieldFS that makes the Windows filesystem immune to ransomware attacks. For each running process, ShieldFS dynamically toggles a protection layer that acts as a copy-on-write mechanism, according to the outcome of its detection component. Internally, ShieldFS monitors the low-level filesystem activity to update a set of adaptive models that profile the system activity over time. Whenever one or more processes violate these models, their operations are deemed malicious and the side effects on the filesystem are transparently rolled back. ShieldFS was able to detect the malicious activity at runtime and recover all the original files.

Collection of 320 Million Passwords Exposed in Data Breaches

https://haveibeenpwned.com/Passwords

The entire collection of 320 million hashed passwords can be directly downloaded from the Pwned Passwords page.

Pwned Passwords are real world passwords exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online as well as being downloadable for use in other online system. The Pwned Passwords service was created after NIST released guidance specifically recommending that user-provided passwords be checked against existing data breaches. The entire collection of 320 million hashed passwords can be directly downloaded from the Pwned Passwords page. Each of the 320 million passwords is being provided as a SHA1 hash. Anyone using this data can take a plain text password from their end (for example during registration, password change or at login), hash it with SHA1 and see if it's previously been leaked.

Note: It is strongly recommended that readers don't enter a password they are currently using into any third-party service online!

Learning

Checklist for Secure Programming

http://meity.gov.in/writereaddata/files/checklist_development_0.pdf

NATIONAL INFORMATICS CENTRE
GOVERNMENT OF INDIA

National Informatics Centre has released a checklist to ensure the security of Government applications. Following is the top 10 guidelines. For full details the URL may be referred.

- Implement minimum 6 characters alphanumeric CAPTCHA on all entry-forms in public pages. Implement CAPTCHA or account-lockout feature on the login page.

- Implement proper white-listing validations for all input parameters on server side.
- Use parametrised queries or stored procedures to query databases.
- Implement proper audit/action trails in applications.
- Use different pre and post authentication session-values/authentication cookies.
- Implement proper access matrix to prevent unauthorised access to resources/pages/forms in website.
- Do not use reference components such as JavaScript, stylesheets etc. directly from third party sites. They can be downloaded and self-referenced in website.
- Use third-party components from trusted source only. Components with known vulnerabilities are not recommended.
- The private data such as PAN number, Mobile number, Aadhar number etc. must be stored in encrypted form. Hashing of sensitive information is preferred over encryption unless required to be decrypted.
- Prevent sensitive information like credit card number, account number, Aadhar number etc. from public access by any means. It should be restricted to authorised persons only. If such information is stored in static files such as excel, pdf, etc. sufficient measures should be taken so that it is not accessible to unauthorised persons or in public.

Implement CAPTCHA on all entry-forms.

Implement white-listing validations for all input parameters.

Use parametrized queries to databases.

Implement proper audit/action trails.

Use different pre and post authentication session-values.

Implement proper access matrix.

Do not reference components directly from third party sites.

Models for Risk Calculation

Sh. Navdeep Pal Singh, Sectoral Coordinator, Government

Risk Assessment is the identification, analyses, evaluation and quantification of the risks to the CIIs, as accurately as possible for ensuring the selection of appropriate controls. These controls emerging out of the risk assessment exercise ensure the appropriate mitigation of threat vectors to the organisation.

Generic Model for Risk Calculation

Organisations can quantify the risk for the CIIs with the help of Vulnerability, Threat, Impact/Consequences and Probability of occurrence of incidence. We need to have the following information for quantifying the risk:

- Hardware Details
- Software Details
- System interfaces (e.g., internal and external connectivity)

Organisations can quantify the risk for the CIIs with the help of Vulnerability, Threat, Impact/Consequence and Probability of occurrence of incidence.

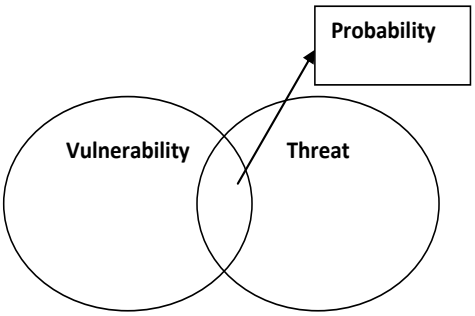


Figure 1

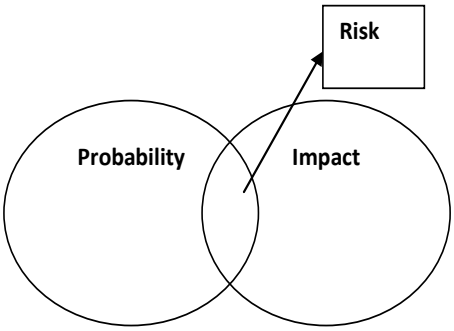


Figure 2

- Data and information
- Persons who support and use the IT system
- Business Processes
- System and data criticality
- Interdependencies (if any)

Exploitation Probability is the assurance for occurrence of any malicious incident, which is dependent on both vulnerability and threat. Probability can be ranging from 0 to 1, depending on the overlap (Figure 1). Probability 0 means no exploitation of vulnerability by listed threat whereas probability 1 indicates the possibility of all the vulnerabilities being exploited. Once probability is documented, the risk associated can also be evolved which is dependent on the probability and impact, coming out of the successful exploitation of the vulnerability by the listed threats as highlighted in Figure 2. Probability is vital in defining the impact i.e. loss to the CIIs. Probability 1 will lead to maximising the impact with complete overlap, whereas 0 probabilities will lead to ideally zero impact on the CIIs.

Mathematical Model for Risk Calculation

*A m*athematical model will quantify the process of Risk Identification. Risk Identification value can be derived from the mathematical mean function with dependencies on the Asset Value, Vulnerability value and Threat Value.

The Asset Value of the IT assets in the CIIs can be identified based upon different parameters like Confidentiality (C), Integrity (I), Availability (A), Authentication (Au), Authorisation (At), Non-Repudiation (NR), Operational Cost (OC), Legacy Systems (LS) and Interdependencies (ID) etc.

Asset Value = function (C, I, A, Au, At, NR, OC, LS, ID etc.)

This asset value can be normalised on a scale of 1 to 10.

Vulnerability Value can be calculated on the parameters depending on the critical business processes of the CIIs. Some of the indicative parameters are: Social Engineering, Mis-configuration, Missing Updates and Upgrades, Application Vulnerability Checks, Missing Secure Coding Practices, Missing RBAC (Role Based Access Control), Missing Multi-Factor Authentication, Missing Backup Procedures, Missing Data Protection (At Rest, Transit and Process), Missing Controls and Missing Skill-Up Gradation.

Vulnerability value will be the normalised value depending on all the identified parameters or vulnerabilities identified during the detailed risk assessment process. Value of the Vulnerability can also be defined on scale of 1 to 10 with all the identified parameters taken into account.

Probability 1 will lead to maximising the impact with complete overlap, whereas 0 probabilities will lead to ideally zero impact on the CIIs.

Vulnerability Value = function (all the identified vulnerabilities / parameters)

Threat Value can be influenced from lot of parameters ranging from motivation to SLAs (Service Level Agreements) as like Motivation (Espionage, Spoofing etc.), Deliberate Threats, Technological Threats, Accidental Threats, Asset Interface (Public or Intranet), Interdependencies, Environmental Threats, Current Control Set and Denial of Service.

Threat Value = function (all the identified Threat factors)

Assembling all the values of Measurement of Risk can be calculated as mean arising out of the above discussed values of Asset, Vulnerability and Threat as highlighted below.

Measurement of Risk = Mean (Asset Value, Vulnerability Value and Threat Value)

Risk of all the assets will be coming on 1 to 10 scales. This will help CIIs to prioritise the Risk and will help to evolve the suitable security control to be implemented to mitigate or contain the corresponding risk.

Note: Residual risk (if any) coming out of the Risk assessment exercise should be dully mentioned and approved by the Head of the organisation.

Sample V/T/R Assessment Chart

Proposed is the sample V/T/R assessment chart which every CII entity is encouraged to promulgate for getting the insight regarding the proper identification of risks, residual risks and mitigation plans.

Risk value	Classification	Remarks
1 to 2	Low	Can be addressed in long term plans.
3 to 4	Medium	Comprehensive plans can be set in short term duration for additional security controls.
5 to 6	High	Immediate additional Control Sets are required to mitigate the Risks
7 to 10	Critical	Immediate Mitigation Plan is required to contain the Risk

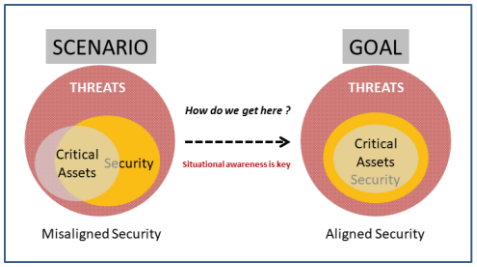
Indicative table for helping in prioritising the Risk addressing mechanism

Risk of all the assets will be coming on 1 to 10 scales. This will help CIIs to prioritise the Risk and will help to evolve the suitable security control to be implemented to mitigate or contain the corresponding risk.

Critical Business Process	*Justification*	*IT Infrastructure*	*Access Authorization*	*Existing Controls (NCIIPC)*	*Threats*	*Vulnerability*	*Risk Priority*
Database	Why this database is critical	All the IT Logistics required to make the identified Critical Business process functional	Name , Designation & Address	List of Existing controls implemented	Listing all the Identified threats to the process	All the vulnerabilities which can be exploited by Listed Threats	Highlight the present Risk status of the database
Application	Application Criticality	All the IT Logistics required to make application functional	Name , Designation & Address	List of Existing controls implemented	Listing all the Identified threats to the Application	All the vulnerabilities which can be exploited by Listed Threats	Highlight the present Risk status of the application

Trends

Challenges in Cyber Advanced Warning System



Sh. Shiv Charan Kataria, NCIIPC

The increased penetration and advancement in cyber technologies while have facilitated effective delivery system to the masses, also exposed the organizations as well as users to ever increasing cyber threats. The sophistication of attacks, scale, architecture and non-productive traffic has made the task of Intrusion Detection System (IDS) difficult as never. Cyber Advanced Warning System (CAWS) uses preliminary indicators to alert on such threats at their nascent stage. A typical CAWS focuses on a variety of threats categorized as follows:

Cyber Advanced Warning System (CAWS) uses preliminary indicators to alert on such threats at their nascent stage.

Social Engineering Attacks: Such as deceits to click on Malicious Content and Download Executables.

Web-Based Exploits: Visiting a webpage that hosts malicious codes. (Also known as "Drive-By-Downloads")

Non-HTTP Malware Delivery: Such as email, a cloaked executable (.jpeg, .exe, .zip), FTP, or an infected USB drive.

Doc-jacking: Delivered via network protocols through common document formats e.g. .doc, .xls, .pdf etc.

Offline Infections: Typically involves connecting an infected device to corporate network.

Considering the magnitude as well as the dynamic and rapid nature of evolution in the attack methods, their detection in-time poses multitude of challenges:

Minimising False Positives: IDS must detect and evade various threats, breaches and malicious contents while at the same time letting the legitimate traffic through.

Resistance to Evasion: Typically attackers are the best users of emerging and new technologies. They use sophisticated disguising and modifying techniques at the point of attack delivery in order to avoid detection by security products. High profile websites are increasingly being compromised to spread exploits and evade detection. This poses a challenge to Security Researchers in designing an effective product.

Network Performance: There is always a trade-off between effectiveness of security and performance of the network. Security Administrators have to jostle to achieve optimal security with minimal performance compromise. Applying a data reduction technique would be possible method to address scalability issues.

Resilience: Failure of the IDS causes exposure to non-detected traffic. Thus stability and reliability need to be ensured at maximum levels.

Configuration Management: There is an inherent complexity in security device deployment. Centralised management console options, log aggregation, and event correlation/management systems further complicate the purchasing decision. Policy management, Alert Handling and Reporting in time followed by Corrective Action are other areas of concern.

Total Cost of Ownership: Implementation of security solutions can be complex, with several factors affecting the overall cost of deployment, maintenance, and upkeep. It involves cost of acquisition, maintenance and management. Finding an optimised balance between costs involved and asset at stake is the key.

A solution that checks all the imminent challenges listed above given the dynamic nature of ever evolving threats in the Cyber space becomes a necessity. Learnings from recent incidents have shown criticality of the problem thereby attracts utmost attention from the management. Organisations must be proactive while implementing and updating Security Solutions to avoid possible catastrophic consequences.

References:

[1]https://link.springer.com/chapter/10.1007/978-3-319-39028-4_3

[2]https://www.researchgate.net/publication/301736666_Early_Warning_Systems_for_Cyber_Defence

[3]https://www.nsslabs.com/index.cfm/_api/render/file/?method=inline&fileID=6E72405E-F053-51B8-5AADC49129E9C43D

Cyber Espionage Campaigns Targeting Energy Sector

Sh. Mohammed Zaki Ahmed, Sectoral Coordinator, Power & Energy

Cyber Espionage activities are being performed by cyber criminals and rival companies to gain monetary benefits and sensitive business information. State level Cyber Espionage involves targeting critical sectors for gaining political and strategic advantages. Traditionally, target of state sponsored cyber espionage campaigns have been Defence and Government Sectors. However, recently the trends of targeting Critical Sectors such as Energy Sector and Health Sector have been noticed. Recent Symantec report on "Dragonfly 2.0" campaign provides insides of targeting Energy Sectors. The 'Dragonfly' campaign has been observed since 2010. However, this time the same campaign has been observed targeting the Energy Sector. Attack vectors for the 'Dragonfly' campaign are Phishing and Trojan toolkits and targets are Business Networks of Energy Sector companies. Once compromised, Operational Technology (OT) networks may also be attacked. So far the Dragonfly Campaign has been focused to North America and European countries.

Attack vectors for the 'Dragonfly' campaign are Phishing and Trojan toolkits and targets are Business Networks of Energy Sector companies. Once compromised, OT networks may also be attacked.

To protect CII against cyber espionage campaigns, organisations need to implement:

- Good behaviour based Anti-malware solutions
- Cyber Security Control for updating Operating System, Application and Anti-malware
- Implementation of Intrusion Detection System and Security Incidents & Events Management System
- 24x7x365 monitoring of events and Inbound/outbound connections for detection of compromised systems and Command & Control (CNC) systems
- Segregation of IT and OT; or
- Implementation of "Network Zoning"
- Usage of data diodes between IT/OT and/or network
- Generating awareness in employees against phishing attacks by regular training and workshops.

There are five main components that are essentially required to be in a smart city: modern information and communication technologies, buildings, utilities and infrastructure, transportation and traffic management and the city itself.

Cyber Security Threats and Challenges in Smart City

Sh. Neeraj Saini, Sectoral Coordinator, Telecom

A smart city is an urban development vision to make citizen's life easy and comfortable by integrating multiple Information and Communication Technology (ICT) solutions in a secure way to manage a city's assets which include local departments' information systems, schools, library, transport system, hospital, power plant, law reinforcement, and many more community services. The concept of Internet of Things (IoT) is mostly involved in it. There are five main components that are essentially required to be in a smart city: modern information and communication technologies, buildings, utilities and infrastructure, transportation and traffic management and the city itself.

Threats to CII: The five components constitute a CII for a city. Each new technology or system i.e. IoT in case of smart city, creates a new opportunity for cyber attackers. Some of threat to the key technologies and systems that together make up the smart city's complex attack surface are:

- Traffic Control Systems
- Smart Street Lighting
- City Management Systems
- Sensors
- Public Data
- Mobile Applications
- Cloud and SaaS(Software As A Service) Solutions
- Smart Grid

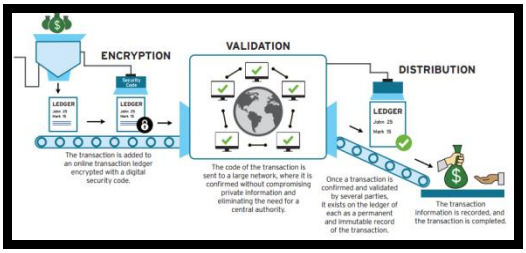
Challenges in securing CII: Every new technology and innovation brings new challenges and problems. There are some problems related to cyber security will affect smart cities in general around the world. Some of them are:

- Lack of Cyber Security Testing & Poor or Non-existent Security
- Encryption Issues & Large and Complex Attack Surfaces
- Lack of Computer Emergency Response Teams (CERT)
- Patch Deployment Issues & Insecure Legacy Systems
- Simple Bugs with Huge Impact
- Public Sector Issues
- Lack of Cyber Attack Emergency Plans
- Susceptibility to Denial of Service
- Technology Vendors who Impede Security Researches

Blockchain Technology and BFSI Sector

Sh. Tanay Bhattacharya, NCIIPC

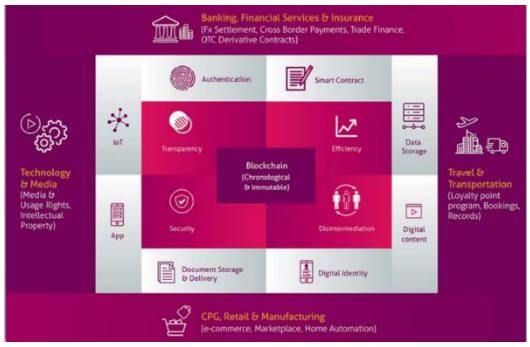
Blockchain Technology is used for almost real time transactions along with verifiable property using shared and distributed ledgers of transactions made among parties. This is fundamentally a tamper evident linked list where the transactions are cryptographically secure and hence are tamper proof. A typical flow of Blockchain transaction is depicted in side figure[1]. Without the presence of any central information storage, Blockchain contains transaction details among all parties in the network using shared, distributed ledgers[2]. It is the Technology behind well-known Crypto Currency 'Bitcoin'. However, Blockchain Technology can be used for more services than what well known Bitcoin offers. Although, the anonymity that is unique property to Bitcoin is not an integral part of Blockchain. Blockchain lets all parties in the network know about a transaction. It can be used for a multiple of other services beyond financial services. However, so far industry has majorly used this technology for financial activities only.



Typical Blockchain Transaction

Indian perspective: India in near future going to use Blockchain Technology extensively for various Fintech related Services. Already, Bank consortium consisting of major banks of India such as SBI, ICICI Bank, Kotak Bank, Bank of Baroda etc. have opted for Blockchain Technology support through Microsoft Cloud solution along with Primechain Technologies for various services such as KYC verification, Anti Money Laundering etc[3,4]. The project has been named as Primechain-KYC is basically a Permission based Blockchain and the platform for this consortium is called Bankchain[5]. So far, there are total 27 Banks in India that have become Bankchain member.

This is fundamentally a tamper evident linked list where the transactions are cryptographically secure and hence are tamper proof.



Emerging Blockchain landscape[6]

Designing, maintaining, troubleshooting, securing, updating and financing such complex setup is a big challenge.

With this, Blockchain as a Service (BaaS) is certainly going to make a big leap towards BFSI sector with faster transaction, transparency, auditability and security. Challenges however are there. What would be the utilisation of existing assets and other legacy items in case BFSI sector is completely migrated to Blockchain Technology? Are Fintech providers going to migrate to a new of Operating Modules and Business Process Management? It is understood that even if the Blockchain has potential to shift the entire business technique to a new dimension, but it is not going to be an easy migration. In fact designing, maintaining, troubleshooting, securing, updating and financing such complex setup is a big challenge. More time along with technological maturity among Fintech service providers are still required for a comprehensive implementation of Blockchain technology across BFSI sector.

References:

[1]https://www.cognizant.com/whitepapers/Blockchain-in-Banking-A-Measured-Approach-codex1809.pdf

[2]https://www.pwc.com/us/en/financial-services/research-institute/blockchain.html

[3]https://www.coindesk.com/indian-banks-select-microsoft-exclusive-cloud-blockchain-provider/

[4]https://news.microsoft.com/en-in/microsoft-azure-accelerate-blockchain-adoption-bfsi-sector-india-exclusive-cloud-partner-bankchain/

[5]http://www.bankchain.org.in/

[6]https://blogs.mindtree.com/blockchain-for-banks-an-implementation-guide

This experiment was a crucial test for a budding technology called quantum cryptography, which uses quantum particles like photons to send secure information.

China Developed Quantum Secured Communications

https://www.wired.com/story/chinese-satellite-relays-a-quantum-signal-between-cities/

On a clear night at the end of last year, a green dot appeared on the horizon near the Chinese-Myanmar border. "It was like a very bright green star," says physicist Chao-Yang Lu. Lu, a professor at the University of Science and Technology of China, saw it from an observing station on the outskirts of the Chinese city of Lijiang. The green star was actually a laser, beamed from a satellite orbiting over 300 miles overhead, like a lighthouse beacon advertising the spacecraft's location. This experiment was a crucial test for a budding technology called quantum cryptography, which uses quantum particles like photons to send secure information. China launched the $100 million satellite, known as Quantum Experiments at Space Scale, last August from the Jiuquan Satellite Launch Centre. Before the launch, researchers placed a complicated system of lasers, mirrors, and a special crystal on board.

When a specific laser shone on the crystal, it would create pairs of light particles known as entangled photons. The crystal makes 6 million pairs of photons at a time, but on the ground, the two ground stations could only detect about one pair per second. Researchers like Lu and his colleagues think quantum cryptography could be the encryption tool of the future. Properly executed, the protocol goes like this: You first measure characteristics of photons to generate a key of 1's and 0's that you send to your intended recipient. Then, you encrypt your message with the key and send it. If a hacker tried to steal the key in transit, quantum mechanics theory says they'd instantly change it to a different set of numbers. Jian-Wei Pan of the University of Science and Technology of China, the physicist who led the project, proposed the satellite experiment back in 2003. His team of some 100 people painstakingly designed, built, and tweaked the laser and satellite system over many years. But they moved fast compared to the rest of the field, says physicist Thomas Jennewein of the University of Waterloo in Canada, who recently sent a quantum key from the ground to an airborne airplane. The reason they could do it so quickly is that people at the highest level of the Chinese government prioritised the project, says Denis Simon of Duke Kunshan University, an expert on Chinese science policy. Because the high-ups wanted it, the group didn't have to go through the usual bureaucratic funding steps, he says. The govt. is particularly interested in this technology because it wants quantum-secured communications in the national interest. "The Chinese government wants to communicate with their naval ships, with their South China Sea activities," he says. "They want to do a lot of things with it." Meanwhile, researchers in other countries are attempting similar experiments—but with more red tape. By 2030, Pan has said that China plans to launch a fleet of these satellites to create a global network. "We are very lucky and benefit from a fast decision-making system," says Lu. There's nothing like when political and scientific interests align.

The protocol goes like this: You first measure characteristics of photons to generate a key of 1's and 0's that you send to your intended recipient. Then, you encrypt your message with the key and send it. If a hacker tried to steal the key in transit, quantum mechanics theory says they'd instantly change it to a different set of numbers.

Estonia is the First Government to Build a Data Embassy

Source: securityintelligence.com

Lots of companies have disaster recovery data centres located far from their headquarters, but Estonia is the first government to build an off-site data centre in another country. The small Baltic nation will make backup copies of its critical data infrastructure and store them in Luxembourg. The idea is that Estonia could continue operating outside its borders in the event of a war or natural disaster. Officials from Luxembourg will be barred from accessing the Estonian data, just like they would be restricted from entering another country's embassy.

NCIIPC Initiatives

Sh. Alok Joshi, Chairman, NTRO with participants

Dr. Ajeet Bajpai, DG, NCIIPC with participants

Five Days Workshop for CISOs of the BFSI Sector

Sh. Aniruddha Kumar, Sectoral Coordinator, BFSI

NCIIPC organised a five day workshop for CISOs of the BFSI sector entities in Mumbai from 24 to 28 August 2017. The sector was chosen in view of the alarming increase in Threat vectors affecting the BFSI sector in view of major steps towards cashless economy and demonetisation. Following points were discussed among the participants, trainers and NCIIPC team:

- Unified reporting framework for cyber security breaches in Finance Sector.
- Customisation of NIST Cyber Security Framework in line with Indian ecosystem.
- Change/patch management and Roll Out management issues.
- Regulations on Crypto Currency such as Bitcoins.
- Investment in the Responsible Vulnerability Disclosure Programme (RVDP) as it is vital in identifying the vulnerabilities in CIIs.
- Monitoring Dark Web to obtain vital source of information regarding their security posture and prevalent threats.
- Development of SOPs and scripts in order to reduce the response time for banking applications to migrate to upgraded browser.
- Inclusion of clause in SLAs with vendors allowing vulnerability assessment or penetration testing of cyber security solutions.
- Policy on qualification, length of service, posting for the CISOs of the BFSI sector.

Most Prevalent Malware Files

Sh. Navdeep Pal Singh, NCIIPC

Following are the most prevalent malware files detected by NCIIPC. The advisories specific to these malwares are periodically pushed to all the CISOs enrolled with NCIIPC.

SHA 256: 1abb85ea0baebf6af74054f0f84a21100b82867020f20e7c2b27ddcc3473a58e

MD5: CEAE16ED783DF0DF24831E93ADC3FE80

Typical Filename: svchost.exe

Detection Name: Trojan.Win32

Command and Control IP: 115.159.5.86

Virustotal Link:

https://www.virustotal.com/en/file/1abb85ea0baebf6af74054f0f84a21100b82867020f20e7c2b27ddcc3473a58e/analysis/

IP Address: 115.159.5.86

Location: China, Beijing

ISP: Tencent Cloud Computing (Beijing) Co. Ltd.

SHA 256: 2357e4158dfbc81d3525d693ad24b47677c390056ec164cf00055cdc924e260c

MD5: 196E0EC9EBB5670069CA366CFFC51D15

Typical Filename: google

Detection Name: Backdoor.Linux

Command and Control IP: 103.25.9.229

Virustotal Link:

https://www.virustotal.com/en/file/2357e4158dfbc81d3525d693ad24b47677c390056ec164cf00055cdc924e260c/analysis/

IP Address: 103.25.9.229

Location: Hong Kong (SAR)

ISP: Cloud Rely Limited

SHA 256: 7baee22c9834bef64f0c1b7f5988d9717855942d87c82f019606d07589bc51a9

MD5: 8C19D83FF359A1B77CB06939C2E5F0CB

Typical Filename: NetSyst96.dll

Detection Name: Trojan.Agent

Command and Control IP: 173.254.236.47

Virustotal Link:

https://www.virustotal.com/en/file/7baee22c9834bef64f0c1b7f5988d9717855942d87c82f019606d07589bc51a9/analysis/

IP Address: 173.254.236.47

Location: United States, California, Los Angeles

ISP: QuadraNet Inc

SHA 256: 441cd81d113dbc4214f7f7de97583441d1f46f4500d985fa38ccad34b12d8b02

MD5: BA4D52AF88BFBF72BE0FD50DE8598FFF

Typical Filename: 441cd81d113dbc4214f7f7de97583441d1f46f4500d985fa38ccad34b12d8b02

Detection Name: Backdoor.Linux

Command and Control IP: 118.193.217.144

Virustotal Link:

https://www.virustotal.com/en/file/441cd81d113dbc4214f7f7de97583441d1f46f4500d985fa38ccad34b12d8b02/analysis/

IP Address: 118.193.217.144

Location: China, Shanghai

ISP: Shanghai Anchnet Network Technology Stock Co. Ltd

SHA 256: 6c70f08143f6bedd39918b822ad9188c605d534838a73f61a640cc76ca6fca94

MD5: 929C0D8596A8DCF7F526947C161CE3FC

Typical Filename: linux

IP Address: 119.29.110.29

Location: China, Beijing

ISP: Tencent Cloud Computing (Beijing) Co. Ltd.

Detection Name: Trojan.Linux

Command and Control IP: 119.29.110.29

Virustotal Link:

https://www.virustotal.com/en/file/6c70f08143f6bedd39918b822ad9188c605d534838a73f61a640cc76ca6fca94/analysis/

Most Prevalent Malicious Domains

Sh. Navdeep Pal Singh, NCIIPC

The following are the most prevalent domains used by the malware droppers detected by NCIIPC. These domains are usually loaded with malicious binaries used by the malicious files to compromise the system.

- 888689.f3322.net
- blog752.serveblog.net
- myss.ter.tf
- www.linuxhoumen.com
- mhacker.cc

NCIIPC on Twitter

https://twitter.com/NCIIPC

Social media is a great means to connect and disseminate information with ease. In its endeavour to connect with its stakeholders/community, NCIIPC launched its Twitter handle on 17th August this year. The stakeholders may follow @NCIIPC to receive the latest alerts, advisories and updates related to cyber security of CII. The aim is to reach out to the target audiences in a faster and effective way. NCIIPC tweets are likely to issue:

- Advisories
- Security news and incidents
- Guidelines
- NCIIPC activities etc.

NCIIPC tweets or re-tweets only content/news/articles relevant to security of CII. However, NCIIPC will not tweet any incident/breaches that is specifically targeted towards a particular CII. NCIIPC will mostly follow other accounts who are involved in the domain on CII protection, Cyber and Information Security related topics etc. However NCIIPC "following" twitter accounts does not imply any endorsements whatsoever.

Vulnerability Watch

Critical Vulnerability in Juniper Junos OS

https://tools.cisco.com/security/center/viewAlert.x?alertId=54492

Vulnerability in Juniper Junos OS could allow an unauthenticated, remote attacker to gain access to sensitive information on a targeted system. The vulnerability is due to improper security restrictions imposed by the affected software. SRX Series devices contain hard-coded authentication credentials in the Integrated User Firewall (UserFW) feature of the affected software.

SRX Series devices contain hard-coded authentication credentials in the Integrated User Firewall (UserFW) feature of the affected software.

Critical Vulnerability in Search Component of Windows

https://tools.cisco.com/security/center/viewAlert.x?alertId=54386

Vulnerability in the Search component of Microsoft Windows could allow an unauthenticated, remote attacker to execute arbitrary code on a targeted system. The vulnerability is due to improper memory operations performed by the affected software when handling objects in memory. An attacker could exploit the vulnerability by transmitting messages, crafted to submit malicious input, to the affected software or via a Server Message Block (SMB) connection.

An attacker could exploit the vulnerability by transmitting messages, crafted to submit malicious input, to the affected software or via a SMB connection.

Critical Vulnerability in Hololens Component of Windows

https://tools.cisco.com/security/center/viewAlert.x?alertId=54382

Vulnerability in the Hololens component of Microsoft Windows could allow an unauthenticated, remote attacker to execute arbitrary code on a targeted system. The vulnerability is due to improper memory operations performed by the affected software when handling Wi-Fi requests. An attacker could exploit the vulnerability by transmitting crafted Wi-Fi requests designed to submit malicious input to the affected software.

An attacker could exploit the vulnerability by transmitting crafted Wi-Fi requests designed to submit malicious input to the affected software.

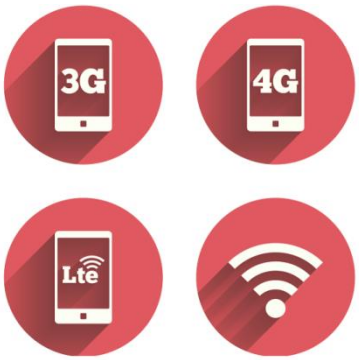
Critical Vulnerability in Apache Subversion Clients

https://tools.cisco.com/security/center/viewAlert.x?alertId=54853

Vulnerability in Apache Subversion clients could allow an authenticated, remote attacker to execute arbitrary shell commands. The vulnerability is due to improper handling of svn+ssh:// URLs by the affected software. An attacker could exploit this vulnerability by using a malicious server to generate a crafted svn+ssh:// URL or placing a crafted svn+ssh:// URL on a trusted server and persuading a targeted user of that server's repositories to follow the crafted URL.

The vulnerability affects Subversion clients that use file://, http://, and plain svn://.

An exploit could allow the attacker to run arbitrary shell commands with the privileges of the user of the Subversion client. If the user has elevated privileges, an exploit could result in a complete system compromise. To exploit this vulnerability, the attacker may provide a user with a link containing a crafted svn+ssh:// URL and use misleading language or instructions to persuade the user to follow the link. The vulnerability affects Subversion clients that use file://, http://, and plain svn://.



Cryptographic Flaw in 3G and 4G LTE Networks

http://www.zdnet.com/article/stingray-security-flaw-cell-networks-phone-tracking-surveillance/

That can allow an attacker to monitor consumption patterns, such as when calls are made and when text messages are sent, and track the physical location of a cell phone.

The findings, revealed at the Black Hat conference in Las Vegas, detail a cryptographic flaw in the protocol used in 3G and 4G LTE networks which enables mobile devices to connect with the cell operator. Ravishankar Borgaonkar and Lucca Hirschi, who co-authored the research, found a weakness in the authentication and key agreement, which lets a Phone, communicate securely with the subscriber's cell network. The agreement protocol relies on a counter that's stored on the phone operator's systems to authenticate the device and to prevent replay attacks, but the researchers found that the counter isn't well protected and partially leaks. That can allow an attacker to monitor consumption patterns, such as when calls are made and when text messages are sent, and track the physical location of a cell phone. But the flaw doesn't allow the interception of calls or text messages. This flaw could pave the way for a next-generation of stingray devices, otherwise known as cell site (or IMSI) simulators.

Upcoming Events - International

October 2017

- 24th International Computer Security Symposium and 9th SABSA World Congress, Kildare, Ireland — 1-5 Oct
- IEEE Symposium on Visualization for Cyber Security, Phoenix, Arizona, United States — 1-5 Oct
- Cyberclub, London — 2 Oct
- Cybercon 2017, Atlanta — 4 Oct
- IP Expo/Cyber Expo, London — 4-5 Oct
- Cyber Security for Critical Assets, London — 4-5 Oct
- Virus Bulletin International Conference, Madrid — 4-6 Oct
- (ISC)2 Secure Johannesburg 2017 — 5 Oct
- BruCON, Belgium — 5-6 Oct
- EC-Council Global CISO Forum 2017, Atlanta — 9-10 Oct
- ISSA International Conference, San Diego — 9-11 Oct
- Cloud and Cyber Security Expo, Singapore — 11-12 Oct
- ASIS Wharton Program for Security Executives, Philadelphia, USA — 15-20 Oct
- CISQ's Cyber Resilience Summit, Arlington, VA — 19 Oct
- ISACA Ireland Conference 2017 — 20 Oct
- The 13th Meridian Annual Conference, Norway — 24-25 Oct
- International Conference on Information System Modelling and ICT System Security, Kathmandu, Nepal — 27-28 Oct

OCTOBER 2017

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

NOVEMBER 2017

S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

November 2017

- Security and hacking conference, Seoul, Korea — 2-3 Nov
- 2nd AIEE Energy Symposium on Current and Future Challenges to Energy Security, Rome, Italy — 2-4 Nov
- International conference on cyber conflict, Washington DC, US — 7-8 Nov
- RSA Conference 2017, Abu Dhabi — 7-8 Nov
- International Cyber Security and Intelligence Conference, Toronto, Canada — 7-8 Nov
- DefCamp, Bucharest, Romania — 9-10 Nov
- SecTor, Underground cyber threats and corporate defences, Toronto, Canada — 13-15 Nov
- UK Security Expo, London Olympia — 29-30 Nov
- Cyber Security - Oil, Gas, Power 2017, London — 29-30 Nov

December 2017

- Black Hat Europe, London 4-7 Dec
- International Conference on Information and Network Security, Jakarta, Indonesia 5-7 Dec

January 2018

- 4th International Conference on Information Systems Security and Privacy, Funchal, Portugal 8-11 Jan
- International Conference on Cyber Security, New York 22-24 Jan

Upcoming Events - National

October 2017

- CyFy 2017, New Delhi 3-4 Oct
- HAKON 2017 Insane Cyber of Things, Indore 6-8 Oct
- InfoSec Intelligence Conclave 2017, Bangalore 12-13 Oct
- Global Cyber Challenge (GCCS 2017) 5-25 Oct
- BSides, New Delhi 27 Oct

November 2017

- USI National Security Seminar, New Delhi 2 Nov
- Security Architecture Conference, Bangalore 10-11 Nov
- Cyber Security Conclave, Hyderabad 22-23 Nov
- 5th Global Conference on Cyberspace, New Delhi 23-24 Nov

December 2017

- International Conference on Advances in Computing, Communication and Control, Mumbai 1-2 Dec
- SANS Bangalore 2017 11-16 Dec
- Cyber Security Conclave 3.0, Hyderabad 14-15 Dec

DECEMBER 2017

S	M	T	W	T	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

JANUARY 2018

S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

General Help	helpdesk1@nciipc.gov.in helpdesk2@nciipc.gov.in
Incident Reporting	ir@nciipc.gov.in
Vulnerability Disclosure	rvdp@nciipc.gov.in
Malware Upload	mal.repository@nciipc.gov.in

Feedback/Contribution

Suggestions, feedback and contributions are welcome at newsletter@nciipc.gov.in

Disclaimer

NCIIPC does not endorse any vendor, product or service. The content of the newsletter is for informational purpose only. Readers may validate the information on their own.