Best practices
in
Digital Payments
to
Minimize Security Threats

Ratnaboli Ghorai Dinda

Sr. Technical Director

Objectives of driving digital payments

- Convenience and ease of transaction and is more secure compared to making transactions involving cash withdrawal.
- Drive the development and modernisation of the payment system, promote transparency and accountability, reduce transaction costs, and decrease the size of the grey or informal economy.
- Help business people grow their customer base and resource pool, far beyond the limitations of their immediate geographic area.
- Adds up to environment as no tree will be cut for printing paper money.
- Reduces Corruption
- Overall they boost the rural economy and enables better development of the rural masses.

Components & Stakeholders

- **Major components**
  - The application (eg website/ mobile app for ordering seed)
  - The payment mechanisms
  - The interface – the glue

- **Major stakeholders**
  - The application user
  - Payment brokerage (Banks, eWallet companies)
  - Service providers

Modes of Digital Payment

- **Banking Cards** (Credit, Debit, Stored value/prepaid)
  - Used in conjunction with PoS machines, ATMs, Online
- **Unified Payment Interface** (UPI)
  - authenticates the identity of the user like a debit card does using the phone as a tool instead of a separate card
  - Smart phone & bank account
- **e-Wallets**
  - a type of electronic card which is used for transactions made online through a computer or a smart-phone
  - Utility of e-wallet is same as a credit or debit card
  - Make paperless money transaction easier.
- **Unstructured Supplementary Service Data** (USSD)
  - Mobile banking for feature phones
  - Offered through a National Unified USSD Platform (NUUP) on a short code *99#.
- **AADHAR Enabled Payments**
  - Allows bank-to-bank transaction at PoS (MicroATM) with the help of Banking Correspondent

Cyber Security

General perspective

- National security, economic prosperity, innovation and social well-being are critically dependent upon the **availability, integrity and confidentiality** of a range of Information and Communications Technologies (ICT).
- Nearly every aspect of citizen's daily life has been considerably transformed by the information revolution and modern life depends upon the timely, adequate and confidential performance of cyberspace.
- The security issues in the physical world have been well understood and the mechanism and processes/procedures for protecting the physical space is in place.
- However, cyberspace has evolved in the last decade and is rapidly evolving.
- The problem gets compounded by the fact that cyberspace is border-less and there is no need for substantial resource/expertise for carrying out attacks.
- Therefore, protection of national cyberspace needs to be a continuous activity.
- The rapid change in technology, in terms of flexibility and ubiquitous use across the globe, necessitates that the country be **up-to-date in Technology, both for products & security along with trained & dedicated manpower (People), and Policies/Procedures/Guidelines.**

Indicative lists of threats

- Defacement of web sites / applications, content modification.
- Unauthorized access to system resources through network or system interfaces.
- Visiting malicious websites or Internet applications may lead to system compromise.
- Sensitive data may be lost during data transfer or during storage on the system.
- Malicious programs may get installed unknowingly.
- Sensitive data may be lost during disposal or replacement of storage media.
- In critical / sensitive ministry, there may be targeted attack on the systems.
- Attempt to send out sensitive data from the system.
- Malicious user may attempt to get unauthorized access to the system.

Most talked about ones

- Phishing
- Ransomware
- Smart cities / IoT (security and privacy issues)
- Cyber Espionage
- Distributed Denial of Service (DDoS)

Phishing

- **Phishing**
  - criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials.
- **Social engineering** schemes
  - use spoofed e-mails purporting to be from legitimate businesses and agencies, designed to lead consumers to counterfeit websites that trick recipients into divulging financial data such as user names and passwords.
- **Technical subterfuge** schemes
  - plant crimeware onto PCs to steal credentials directly, often using systems to intercept consumers online account user names and passwords – and to corrupt local navigational infrastructures to misdirect consumers to counterfeit websites (or authentic websites through phisher-controlled proxies used to monitor and intercept consumers' keystrokes).
- **Spear phishing**
  - appears to come from an individual or business that one knows. But it isn't. It's from the same criminal hackers who want your credit card and bank account numbers, passwords, and the financial information on your PC**.**

Ransomware

- Ransomware has become one of the most widespread and damaging threats that internet users face.
- Since the infamous CryptoLocker first appeared in 2013, there has been a new era of file-encrypting Ransomware variants delivered through spam messages and Exploit Kits, extorting money from home users and businesses alike.
- In many cases unbreakable encryption is used, meaning that extortion has evolved from simple social engineering, with little to no consequences for failure to comply, to permanent loss of data unless payment is made.

Smart cities / IoT

(security and privacy issues)

- The world (and our country also) is experiencing an evolution of **Smart Cities**. These emerge from innovations in information technology that, while they create new economic and social opportunities, pose challenges to security and expectations of privacy.
- Humans are already interconnected via smart phones and gadgets. Smart energy meters, security devices and smart appliances are being used in many cities.
- Homes, cars, public venues and other social systems are now on their path to the full connectivity known as the '**Internet of Things (IoT)**.
- Standards are evolving for all of these potentially connected systems. They will lead to unprecedented improvements in the quality of life.
- To benefit from them, city infrastructures and services are changing with new interconnected systems for monitoring, control and automation.
- Intelligent transportation, public and private, will access a web of interconnected data from GPS location to weather and traffic updates. Integrated systems will aid public safety, emergency responders and in disaster recovery.
- **Security includes illegal access to information and attacks causing physical disruptions in service availability.**
- As digital citizens are more and more instrumented with data available about their location and activities, privacy seems to disappear.
- Privacy protecting systems that gather data and trigger emergency response when needed are technological challenges that go hand-in-hand with the continuous security challenges. Their implementation is essential for a Smart City in which we would wish to live.
- The major element in the Smart City and their interactions are what we need to protect.
- As the number of IoT manufacturers and users proliferate, and as the devices become mainstream household appliances, it seems probable we'll see even more high-profile security issues.

Cyber Espionage

- State sponsored cyber hacking and espionage has come up in the news more often in the past couple of years. With ever increasing amount of classified information that is stored in databases and personal computers, the amount of state sponsored hackings and cyber espionage will increase dramatically.
- State sponsored cyber hacking and espionage uses funding and support provided by governments, sometimes anonymously and without acknowledgement.
- The goals are to gather intelligence, steal technology and designs, steal personal information, to sabotage, or to vandalize. Countries and people are affected negatively by cyber hacking and espionage.
- **Stolen trade secrets and designs make the company less competitive when competing manufacturers duplicate items and sells them. People also have personal and sensitive information taken from them, such as bank account numbers and records, and personal emails.**
- With the constant security threats facing the consumer, more money is spent to prevent and defend against such attacks.
- Organizations have to hire information security professionals to harden their networks and block them from malicious attacks and data breaches.

Advanced Persistent Threat (APT)

- The use of APT vectors are a major concern, wherein the cyber attack launched by a group of sophisticated, determined, and coordinated attackers who systematically compromise the network of a specific target machine or entity for a prolonged period.
  - Advanced: not an average sophistication may be government funded, may have zero-day vulnerabilities
  - Persistent: initial access leads to the creation of many access methods and long-term exploration -- including use of **Remote Access Trojans (RAT)**
  - Threat: defines the group of attackers with these capabilities, not an actual

Distributed Denial of Service (DDoS)

- A DDoS attack uses many computers (often bots) distributed across the Internet in an attempt to consume available resources on the target.
- DDoS assaults are intended to do just what the name implies – render a server or network resource unavailable to its intended users.
- Attackers can use network attacks, protocol attacks or application layer attacks.

CSPfNII

- **Cyber Security Policies, Guidelines and Procedures for NIC Information Infrastructure (CSPfNII)**
- CSPfNII aims at providing secure and acceptable use of ICT Resources and services of the NII. The policy governs the usage of ICT Resources and services of the NII.
- The policy is applicable to all employees of the GoI, employees of State / UT Governments and their third-party personnel.
- It takes into account the best practices in security and the previous / existing documents like Cyber Security Policies for Government of India by NIC and the NISPG issued by Ministry of Home Affairs. For easy cross reference mapping of policy statements of NISPG are also provided.
- Cover both network & application security issues.
  - Contains **Application security guidelines**
    - Enlists probable application level attacks & best practices to follow

Digital payment / Credit card / Mobile / online banking threats & best practices

- Recently Indian Computer Emergency Team (CERT-In), the national incident response centre for computer security incidents of the Indian cyber community, published a series of advisories regarding the best practices to be followed in relation to security of:
  - **Point of Sale (PoS) systems,**
  - **Micro ATMs,**
  - **eWallets,**
  - **online banking,**
  - **smart phone,**
  - **mobile banking,**
  - **online payment through UPI,**
  - **biometric devices,**
  - **web browsers,**
  - **mobile ransom-ware,**
  - **USSD based mobile banking** and
  - **preventing social engineering attacks.**

- These advisories are available at the CERT-In site:
  - (**www.cert-in.org.in** -> ADVISORIES)

Maintaining cyber hygiene

- As a responsible cyber citizen, practice basic preventative measures /precautions /cyber hygiene (as an end user, as an administrator, as a security specialist, or any other role…..)
  - Regularly update anti-virus / anti-malware software and applications.
  - Avoid the use of public Wi-Fi networks, which are target-rich for cyber thieves.
  - Turning off the devices when not in use.
  - Regularly change passwords, choose strong password and separate passwords for different site one frequent.
  - Try to recognize and avoid phishing scams and other malware intrusions.
  - Install dual-factor authentication/tokens, biometric solutions (e.g., fingerprint, facial recognition and iris scanning software) and other data encryption software onto electronic devices.
  - Get a security audit or risk assessment by a qualified professional who can point out areas of vulnerability & available attack surface.
  - Backing up files onto external drive (to safely restore, in case of eventuality).
  - Prepare a strategy in advance to respond to a security incident, put it into practice and conduct a root-cause analysis.
  - Only engage with verified social media pages and use official mobile apps linked from a official web site.

DOs & DON'Ts

- DOs
  - Password protect the mobile phone / device.
  - It is recommended to set the maximum number of incorrect password submissions no more than three.
  - Choose a strong password to keep the account and data safe.
  - Review the account statements frequently to check for any unauthorized transactions.
  - Change the PIN regularly.
  - Report a lost or stolen phone / device immediately to the service provider and law enforcement authorities.

- DON'Ts
  - Never give the PIN or confidential information over the phone or internet. Never share these details with anyone.
  - Don't click on links embedded in emails/social networking sites claiming to be from the bank or financial institutions.
  - Don't transfer funds without due validation of the recipient, as funds once transferred cannot be reversed.
  - Don't store sensitive information such as credit card details, mobile banking password and user ID in a separate folder on your phone.
  - Don't forget to inform the bank of changes in the mobile number to ensure that SMS notifications are not sent to someone else.
  - Never reveal or write down PINs or retain any email or paper communication from the bank with regard to the PIN or password.
  - Be cautious while accepting offers such as caller tunes or dialer tunes or open/download emails or attachments from known or unknown sources.
  - Be cautious while using Bluetooth in public places as someone may access the confidential data/information. Similarly with using public WiFi.

Prevention is better than cure...

- Prevent account data from being intercepted when entered into a mobile device.
- Prevent account data from compromise while processed or stored within the mobile device.
- Prevent account data from interception upon transmission out of the mobile device.
- Prevent unauthorized logical device access.
- Create server-side controls and report unauthorized access.
- Prevent escalation of privileges.
- Create the ability to remotely disable the payment application.
- Detect theft or loss.
- Harden supporting systems.
- Conform to secure coding, engineering, and testing.
- Protect against known vulnerabilities.
- Protect the mobile device from unauthorized applications.
- Protect the mobile device from malware.
- Protect the mobile device from unauthorized attachments.
- Create instructional materials for implementation and use – user awareness
- Support secure merchant receipts.
- Provide an indication of secure state(https)

Lastly – think simple steps...

- **Be Vigilant**
  - If an email looks too good to be true, it probably is.
  - Be cautious when opening attachments and clicking links.
  - While connecting to web sites make sure it is a secure connection (https://www.site.in)

- **Backup Data**
  - Plan and maintain regular backup routines.
  - Ensure that backups are secure, and not constantly connected or mapped to the live network.
  - Test the backups regularly to verify their integrity and usability in case of emergency.

- **Disable Macros**
  - Document macros have been a common infection vector for ransomware in 2016.
  - Macros from email and documents should be disabled by default to avoid infection.

- **Patch and Purge**
  - Maintain regular software updates for all devices, including operating systems and apps.
  - Update any software you use often and delete applications you rarely access.

Thank You.....