Three Pillars of Information Security

Anshuman Pund¹, Second Author², Third Author³

¹Head Information Security, IDBI Intech Ltd, Belapur, Navi-Mumbai
²Second Author Affiliation & Address
³Third Author Affiliation & Address

Abstract— This document help us understanding Three main pillar of Information Security considering latest threats landscape. Document will explain about problem statement for each of the pillar with traditional security control implemented (illustration purpose). Next generation technology available and can be implemented considering advance threats with the evolution of new technologies and rapid adaption which is in line to three main pillar of Information Security.

Keywords— AI – Artificial Intelligence, IoT – Internet of things, CnC – Command and control, MITM- Man in middle attack, EOL/S- end of life support, APT- Advance persistent Threat, IOC- Indicator of Compromised, BMS-Building Management System, SCD- Secure configuration document, NAC- network access control, DAM- Database activity monitoring, gen – generation and E.g.- Example.

I. INTRODUCTION

Information is knowledge derived from a particular source. For example email, websites, documents etc. and protecting or safeguarding information are called information security.

Cybersecurity refers to preventative mechanism using technologies used to protect digital information of systems, networks or data at rest or in transit, all over the World Wide Web/ internet/ cyber, from being stolen, compromised or attacked from unauthorized access, due to vulnerabilities and is a critical issue for all businesses.

Three pillars ensures to avoid prevention of data loss, financial loss, reputation loss, opportunity loss, unfavorable media exposure, outage-disruption of services, compromised sensitive – classified information, fraud- Abuse and Lawsuit.

Also, ensures to fight cyber threat and cybercrime. Cyber Threat -The possibility of a malicious attempt to damage or disrupt a computer network or system. Cyber Crime- Criminal activities carried out by means of computers or the Internet.

Following are the known threats and crimes.

- Virus, Malware, Spyware, Trojan, Spam, Phishing/Vishing, shoulder surfing, dumpster driving, brute force, hacking, insider threats, social engineering, DOS, Zero day, Botnet, defacing websites and lack of knowledge and awareness.

Credit card/ATM fraud, Spamming, Spoofing, hacking, software piracy, pornography and so on.

II. PROBLEM STATEMENT FOR EACH PILLAR

Protecting Information such as customer data, trade secrets, intellectual property, historical data, business plans & budgets, financial & management data, employee/personal information etc. which resides at and transit through information systems like Cloud, Data-Centers, Application servers, Databases, storages, Desktops, Laptops, Network Devices, Smart Phone, PoS, websites, ATMs, etc.

While doing so.

- Problem Statement for the First Pillar is – Unauthorized access to information
- Problem Statement for the Second Pillar is – Unauthorized changes to information
- Problem Statement for the Third Pillar is – Information is not available when required

III. TRADITIONAL OR APPLIED SOLUTION FOR EACH PILLAR

Few example to illustrate for the first pillar where traditional solution have been applied.

Encryption is the solution used to prevent from unauthorized access where plain text convert to cipher text i.e. Cryptography - Cryptography is used to protect confidential data such as email messages, chat session, web transactions, personal data, corporate data, e-commerce apps or data at rest or in transit.

Encryption is used in hardware devices and in software. A System or product that provides encryption & decryption is referred to as a cryptosystem. There are methods of Encryption or Cryptography i.e. Symmetric, Asymmetric, Hybrid and PKI. Cryptosystem uses an encryption algorithms, keys.

Old weak hash / encryption algorithms and lower value keys are being still allowed like MD5, RC4, DES, Blowfish, SHA1, SSLv2/3, TLS1/1/1.1/1.2, with key size 32, 48, 128 etc.
Enterprise Anti-Virus solution is used to prevent threats like keyloggers or Trojan which is trying to steal or capture information to further compromise your system.

IPsec VPN system used with special type of header to the packet are AH.

Windows file servers with SMB v1/v2 protocol

Wi-Fi uses WEP, WPA1/2 protocols is being used for wi-fi wireless communication

Physical security where information resides is being protected from natural threats like Floods or any physical intrusion by provisioning security guard with access control mechanism.

Similarly, Few example to illustrate for the second pillar where traditional solution have been applied.

Windows file permission

Anti-malware feature in Enterprise Anti-virus solution which prevent any change to execution of malicious software on to the system

Role base access to database, application or OS administrators as database is goldmine for any organization and data changes to it may be disaster. The integrity of a database is enforced through a User Access Control system that defines permissions for who can access which data.

Application security testing tool for the web sites to prevent from SQL injection, DOS, Buffer overflow, Cross site injections, privilege escalation attack etc.

Vulnerability assessment tool and Penetration testing tool for the OS and system to identify vulnerability and mitigation to it for OS or system to prevent it from exploitation.

Old Hashing algorithm used for authentication, SSL Certificates i.e. SHA1 (160 bit Hash) others Hashing algorithm are used for Message exchange, Digital Certificates uses message digest MD2/4/5. To maintain backwards compatibility with SSL, there is a protocol downgrade option during the TLS protocol handshake where the server and client negotiate which protocol version to use. This functionality means that even if a client and server both support TLS, an attacker may still be able to target weaknesses in the SSL protocol.

Also, Few example to illustrate for the third pillar where traditional solution have been applied.

Critical Devices, applications are getting use as standalone

Data Center with passive Disaster Recovery location

Establishment of NOC, SOC 24x7 support for ensuring network availability and identifying any attack vector to raise alert on real time for immediate mitigation to avoid any loss, damage or disasters

Backup and storage solutions to critical data.

No Access control and scanning mechanism implemented, security guards are illiterate, no background check done for security guards, lack of security awareness and no Fire drill conducted

### IV. NEXT GEN SOLUTION

Next generation thinking is required. Because of evolving technologies and new and advanced threat landscape

- **evolving Internet usages** – Online Banking, Online shopping, Virtual ClassRooms, Cloud Computing, Big Data
- **New way of doing Banking and social networking** - TAB Banking, Contactless Cards, Mobile Banking, NiKi AI Chat BOT, Twitter, Facebook, Instagram, LinkedIn.

Hence new threats and crimes are rising at the same time. Like Advance persistence threats, Ransomware, DDoS, MiTM, drive-by downloads, CnC, Malvertising, Rouge security software and so on

Crimes like Identity theft, hacking, e-Money laundering and so on

Some of the recent threats are

- Mark Zuckerber Hacked for the third time last year
- Hackers steals 17 million Zomato user’s data, put on the dark web
- You can now buy credit cards of Sonic customers for $25 on the dark web
- Bangladesh Bank $81 million SWIFT transition breach
- Cybercrime Gang tied to 20 million stolen cards
- Qatar National Bank suffers massive breach
- LOCKY, Petya, WannaCry Ransomware attack globally and so on….

Next generation thinking is required toward each pillars to encounter next generation threats leveraging new evolving technologies

### V. NEXT GEN SOLUTION FOR FIRST PILLAR

Latest Encryption algorithms/keys to be used which cannot be break by hackers. i.e. TLS 1.3/4, RSA 2014 with higher value keys 256 bit and above.

Organization to plan upgrade IT infra as per published EOL/S for respective OS, Applications. E.g. Support for Windows XP ended April 8, 2014.
Microsoft will no longer provide security updates or technical support for the Windows XP operating system. Microsoft has ended support for the Windows Server 2003 operating system on July 14, 2015. After this date, this product will no longer receives Security patches. On January 14, 2020, Microsoft will be officially ending its support for Windows Server 2008 R2 and Start using Windows Server 2016 R2, AIX 7.2.

While Developing Web applications, following inputs provision is being done by developers based on business requirement. Such data can be intercepted by hackers so to avoid developers should write or use secure coding which will encrypt such sensitive data while in transit.

Prevent interception at websites by provisioning encryption to specific input field like SPI, PII, TSI

- **SPI** – Sensitive Personal Information. Eg.- User ID, Username, password, PAN Number, CustID, A/c No etc.
- **PII** – Personal Identifiable Information. Eg.- Name, Guardian Name, Telephone Number, Occupation, Marital status etc.
- **TSI** –Technical Sensitive Information. Eg – IP address, email ID, DOB, Device ID, Android IMEI etc.

While developing application program say using Java, “java.util.Random” is considered a weak random number generator. “java.security.SecureRandom” should be used instead of "java.util.Random".

Adopting the OWASP (Open Web Application Security Project) Top 10 is perhaps the most effective first step towards changing the software development culture within your organization into one that produces secure code.

Anti-APT solution to be deployed which prevents an unauthorized access to a network and stays there undetected for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network or organization. APT attacks on target organizations with high-value information, such as national defense, manufacturing and the financial industry. Deployment should be tightly integrated with endpoint Anti-Virus solution, mail gateway and web gateway so that threats can be blocked based on suspected files, IOCs and signature can be pushed to endpoints.

IPsec VPN system used with special type of header to the packet called ESP. In the Tunnel mode of operation, complete encapsulation of the IP packet takes place in the data field of the IPsec packet. Additional security as it conceals the sources and destination field.

Special type of headers associates with the IPsec protocol make it different from the Internet Protocol. Two important modes of headers are recognized.1. AH – Authentication Header 2. ESP—Encapsulating Security Payload.

Wi-Fi Protected Access - WPA and WPA2 are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found in the previous system, Wired Equivalent Privacy- WEP. In January 2018, Wi-Fi Alliance announced the release WPA3 with several security improvements over WPA2.

Physical security is the protection of personnel, hardware, software, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise. This includes protection from fire, theft, vandalism, natural disasters, and terrorism. Monitoring and notification systems to be in place like CCTV, proper Fire EXIT indications, warning sign and assembly points to be draw, mechanical and electronic access control and BMS system to be installed. Fire marshal to be available on 24x7 basis.

VI. NEXT GEN SOLUTION FOR SECOND PILLAR

Secure configuration document (SCD) hardening document to be strictly deployed and maintain during inception of system. It is for any OS, Web applications and databases. Exception can be approved by CISO.

Enterprise Antivirus solution with new features like virtual patching, File Integrity, registry modification monitoring to be deployed for end systems.

Network control access- NAC to be deployed for checking host integrity and rouge device to be join in enterprise can be restricted. Auto-remediates noncompliance system before joining network.

Database activity monitoring and prevention that goes beyond monitoring and alerting it also block unauthorized activities. Data is extremely valuable and may get compromised by malicious users, viruses, compromised users or unintentional user mistakes. There is need for improved data centric security capabilities which not only meets the existing compliance requirements but also becomes a critical protection layer at the data access level especially for databases. This is required to gain deeper visibility in terms of who is touching sensitive data, what are they doing with it and what was taken.
According to Gartner, future investments need to focus instead on more effective and efficient Database activity monitoring (DAM) solutions that combine extensive data security and audit functionality with the ability to eliminate disparate management silos and inconsistencies by coordinating policies across numerous types of data stores.

Code analysis to be conducted periodically for the application hosted on premise or on cloud to identify loophole’s in business logic in the application and can be exploited for the known/unknown vulnerability.

TLS introduced over SSL and has multiple security improvements, including support for newer and more secure algorithms. SSL client browser connections to be refuse or drop or block on the gateway i.e. on the application load balancer till the time SSL get disable on globally.

VII. NEXT GEN SOLUTION FOR THIRD PILLAR

Devices, applications should be in High Availability, failover. Inline devices like IPSs are in fail open or bypass mode in case of device failure.

Active Data Center –Disaster Recovery setup for any organization, also with Near DR for core data replication.

Physical security where information resides is being protected from natural threats like Earthquakes, Cyclone-storm or by any physical intrusion. Periodic security awareness training to be given to employees and agency staff which includes security guard. Fire drill to be conducted regularly. Access control and scanning mechanism to be implemented at highest priority.

ISO 27000 series certification to be done from third party.

Above mentioned problem statements, technologies, processes discussed to illustrate the understanding of information security fundamentals based on Three Pillars.

Three Pillars are none other than Confidentiality, Integrity and Availability respectively.

Figure 1. Three Pillar of Information Security

REFERENCES
[1] ITPro Today –Randy Franklin Smith | May 2005