Approach by:

Washington Umpierres de Almeida Junior

The world society has watched the forms of communication evolve throughout its history. There have been times when the telegram was known as the fastest way to send a message to a person or company, and even in this scenario, there were people able to intercept this kind of information when it was in transit. However, in those times, these people should have physical access to the information since the data was traveling written on paper.
But the forms of communication continued to evolve until the emergence of the Internet, where communication methods went through a process of evolution that revolutionized the way people and companies communicated with each other. Nowadays, the methods used to do things have been changing dramatically. Today people use electronic transfers instead of exchanging checkbook sheets, send e-mails instead of writing letters, share information in social network instead of meeting acquaintances and friends somewhere and so on. From an industry point of view, the evolution goes the same way. Companies have been implementing complex automated methods to increase their production and more recently, financial institutions are working to implement the blockchain-based technology, which indicates a movement to replace the traditional bank business model.
The world and the way people and companies do things has been changing very quickly. This evolution has brought both benefits and challenges to modern society, which today has huge dependence on Internet resources. Along with these changes also arise the threats involved on each technological element around us. So what can we expect from incoming threats in 2017?

Incoming Threats

The incoming threats for the next years will be focused in SSL/TLS1 protocols, blockchain-based technology and smartphones. Why? Let us have a look at each one in more detail.

Attacks on SSL/TLS protocols

In a simplified way, the protocol running over SSL/TLS implementation adds an "S" in the end. Thus, for example, to a web application (http) implemented in a secure manner (SSL/TLS) it has the format "https", which is some times referenced as "http secure".
After the development of the Secure Socket Layer by Netscape2, it seemed the technology information industry would have found a way to provide a secure manner to navigate in the Internet. For many years, the security provided by SSL/TLS protocols seemed to be the best way to guarantee privacy and security over on-line transactions. Although still widely used over the Internet, SSL/TLS protocols present serious vulnerabilities that allow hackers to exploit numerous variations of these flaws to compromise systems and as a consequence it can be used to capture sensitive data such as personal information, credit card details, user ids, passwords and so on.

After the discoveries of attacks against SSL/TLS protocols, such as renegotiation, downgrade, mitm, drown, beast, crime, heartbleed, poodle, freak, rc4, among others, hackers and experts in digital security are sure that SSL/TLS based protocols will be the targets of cyber attacks for a long time and it will be up to the security experts to deal with the issues in order to minimize the risks.
Others protocols from the Application layer are being replaced by secure ones. As an example, it is common to verify the FTP3 protocol being replaced by SSH4 since this last one provides encryption. Even so, the SSH protocol is becoming a target of constant attacks through which hackers look for exploits so that they can gain access on remote systems and escalate privileges.
Increasingly, hackers are taking advantage of vulnerabilities on SSL/TLS to hide their malicious code and thus allowing the encryption of their communications, circumventing not only firewalls but sophisticated intrusion detection systems as well.
SSL/TLS implementations will still bring big challenges to the CSOs and cyber security professionals for the next years.

Attacks on blockchain-based technology

Blockchain and Bitcoin technologies had their origins in the deep web, also known as the hidden Internet that has been created by the US government's military strategy motivations, which was looking for a way to communicate with the intelligence fronts hosted in other countries without their communications being detected. In this environment of technological evolution with a new dark market promising anonymity, a new currency was born and it was called Bitcoin. The creation of Bitcoin is attributed to Satoshi Nakamoto5 whose identity has never been revealed. The account ledger system behind the bitcoin currency was a new technology called blockchain that basically consists of two types of elements: transactions and blocks. Transactions are all the actions created by the nodes that participate in the blockchain system and the blocks are responsible for recording the transaction’s information in the database, ensuring they are in the correct sequence and have not been tampered with. When adding a transaction to the chain, a large part of the nodes in the blockchain network have to validate it. After years operating on the hidden deepweb’s networks, blockchain technology has emerged to the surface6. Today there are two types of the blockchain-based systems: public and private. In the public blockchain system, the concept is that anyone can read and write data. The bitcoin is a currency that employs this public blockchain concept. In the private blockchain, all the participants are known and trusted in the system. This is the concept used by financial institutions like banks and capital fund companies where all participants of the system must be known. Ethereum is another currency that employs the private blockchain concept.
Blockchain release 2.0 has enabled the implementation of smart contracts, representing the next step in Blockchains' projection in the global legal landscape, by keeping track of financial transaction entries to automatically implement multi-party agreement terms.
Thus blockchain acts as a shared database providing a secure and true source, and smart contracts can automate approvals, calculations, and other transaction activities that are prone to errors.
The problem: Where there is money involved and automated systems controlling it, there will be someone trying to take advantage of it.
June 2016: DAO, a venture capital fund based its operations on decentralized blockchain was hacked for $60 million7.
August 2016: Bitfinex, one of the world’s largest digital currency exchanges had its customers’ bitcoins hacked nearly $68 million8.
Although it is known that cryptocurency is a success due to its baked-in decentralization, it is also a valuable target for attackers. These recent events have demonstrated that the blockchain is still vulnerable and in the coming years financial institutions around the globe will have major challenges to implement electronic transaction on blockchain-based systems.

Attacks on smartphone devices

In the smartphone market, numbers are easier to perceive. The world population is almost 7.5 billion people. In 2015, studies of the Cisco Visual Networking Index (VNI) accounted for 4.8 billion users connected to the Internet9, equivalent to a penetration of 64% of the world population. There are still no figures for 2016 but the company's forecast for 2020 is about 5.5 billion of the global mobile users. Most of these connections are made by mobile devices, which already surpass personal computers.
It is easy to see that smartphones are an increasingly attractive target for on-line criminals. People are using smartphones for the convenience and mobility they offer. In a single device, it is possible to carry out banking transactions, on-line purchases, access to social networks, instant messaging systems, manage cryptocurrency account transactions, store and share documents, among others resources. We can realize that users' sensitive data goes through their smartphones very often.
As a result, hackers are investing in more sophisticated types of attacks that are effective at stealing valuable personal data or extorting money from their victims, and the increase of malicious programs created with the objective to steal data from a mobile devices must be the main focus of cyber criminals next year and is at the top of the concerns of security experts.

Conclusion

The reason why hackers have success in their attacks is given by virtue of existing vulnerabilities in the most varied systems, database and elements of encryption. When people read that the traffic is encrypted, it can give a false sense of security. Sometimes by means of encrypted systems, hackers inject their codes to penetrate sophisticated defense systems such as firewalls and intrusion detection systems.
The security flaws that make these hacks possible is where the industry is working hard to make the cybercriminals' life more difficult.
Providing technological solutions that allow security to users in the Internet is just one of the obstacles. As soon as law enforcement boosts its forensic capabilities, hackers quickly adapt their systems to evade detection. Malware designed to penetrate networks, steal information, then cover up its tracks will emerge in 2017. So-called ghostware will make it extremely difficult for forensic companies to track exactly how much data has been compromised, and hinder the ability of law enforcement to prosecute cybercriminals.
Professionals from Law and Information Technology will need to join forces to fight new models of crimes in which they will not be easily in sight of justice. Now the challenges in digital security involve multidisciplinary areas to deal with digital threats.
Of course we know there are other threats in this digital theater that CSOs10 have to deal with everyday but given the capacity of penetration and the comprehensiveness presented in the attacks against SSL/TLS protocols, blockchains and smartphones deserve special attention from digital security specialists.

References:

//web.archive.org/web/19970614020952/http://home.netscape.com/newsref/std/SSL.html
THE SSL PROTOCOL. Access in 16 of November, 2016.

FORRESTER, Daniel & SOLOMON, Mark. BITCOIN EXPOSED. Today's Complete Guide to Tomorrow's Currency. Paperback. 2013. p.20.

http://fortune.com/2016/06/18/blockchain-vc-fund-hacked
Access in 17 of November, 2016.

http://www.marketwatch.com/story/bitfinex-hack-shows-how-bitcoins-blockchain-can-be-a liability-2016-08-03
Access in 17 of November, 2016.

https://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/vni-inforgraphic.html
Access in 19 of November, 2016.

Author: Washington Umpierres de Almeida Junior

Washington Almeida is an Electronic Engineer specialized in Cyber Security with more than 25 years of experience in the Information Technology and Engineering areas, working for large companies in the sectors as Engineering, Information Technology, Consulting, Chemical and Mining. Microsoft Enginner and Cisco Certified acts as Digital Forensic with in-depth knowledge of computer hardware, network technologies, telephony, programming, data communication protocols and a vast amount of information security knowledge with a set of skills known by ethical hackers, where this knowledge base is fundamental to assist the Justice.