IJDACR
ISSN: 2319-4863

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary research
Website: www.ijdacr.com (Volume 3, Issue 8, March 2015)

Advanced Network Security Implementations

Sujit Shome[1]
[1]*Assistant Professor,*
SGI,Rajasthan
sujitshome2014@gmail.com

Neeraj Arya[2]
[2]*Department of CSE,*
SGI,Rajasthan
neeruarya5259@gmail.com

Monika Chahar[3]
[3]*Department of CSE,*
SGI,Rajasthan
mona.33198@gmail.com

***Abstract*: Be it computing or mobile applications development, network security is a big concern to every organization or even personal users that demands advanced network security technology development. Initially the paper focuses on introducing a concept based on the rewiring of bank's authentication by advanced cryptographic implementations followed by ensuring better security mechanisms of our personal information based on 'Databox' and 'Remote Trojan Access' detection by introducing two different techniques which normal firewalls or antiviruses cannot detect easily. As we already know the vastness of network security, research work on this field will further develop newer ideas to detect the vulnerabilities associated and develop advanced technologies.**

***Keywords*—Antivirus, Databox, Firewalls, Remote Trojan Access, Vulnerabilities.**

I. INTRODUCTION

With the advancements in networked systems and terminals the improvement in security is the most challenging issue in today's date. Where researchers and experts are working on decentralization, improved security systems are also expected [4]. In this paper we introduced a concept based on improved cryptographic ideas for implementing better authentication in banks and currency exchange ensuring digital money security. Later we discussed a security mechanism of personal information security which works on the network field services that filters and shows the limited information of the customers based on 'Databox' technology. At the end the paper discusses the Advanced Persistent Threats and their detection techniques that which the normal firewalls or antiviruses could not identify that would help organizations to identify security vulnerabilities and mitigate those.

II. REWIRING BANK AUTHENTICATION FOR DIGITAL MONEY SECURITY

While the focus of the whole world is shifting towards digital money i.e. Bitcoin for transferring and storing money, it has become an essentiality to build such a system that reduces the risks of data leakage and theft that should be much safer, faster and technologically improved than the systems used till date.

A company known as Ripple Labs has already proposed and started implementing a system that works on some cryptographic tricks. The system uses these tricks to make the identification of the customer's better among the different financial companies. Additionally it too offers secure log in facilities to different online services. Along with secure communications and cost cuts, the emergence of low cost data brokers can be expected under this system. The banks can now start their operations even at the impecunious and deprived areas of the world where till date the verification process were considered to be expensive. Experts say that by using this system the verification and identification would be much appropriate and safer. While a number of companies previously has spent on faulty

IJDACR
ISSN: 2319-4863

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary research
Website: www.ijdacr.com (Volume 3, Issue 8, March 2015)

verification techniques like a few weeks ago PayPal, a payment processing company signed an agreement to pay an amount of $7.7 million to the U.S. Treasury for they failed to block about five hundred number of transactions that included people who were subjected to U.S restrictions. But for several financial companies switching to such systems would not be such easy since the compatibility factors will come into concern.

B. Implemented Technology

As discussed earlier, the system developed by Ripple Labs uses certain cryptographic tricks that help in rapid verification and identification of the customers those are associated with different financial organizations. When it comes to verifying and identifying the customer, it's a hectic deal for the financial organizations since organizations spends a huge amount on data brokers who thoroughly checks the customer ID and verifies his/her identification so that the cases of money laundering and fraud are restricted. In the Ripple system a unique cryptographic token is generated from the personal information that is provided to the financial organization. The token is later send to the data broker by the bank that has its own token that has been formed from one's personal information earlier. The data broker then analyses with the help of certain device that processes the information associated with the Ripple system confirming the correctness of the information, without even revealing the confidential data with the bank and the broker as shown if Fig 1. Similar technology is implemented by Apple's mobile payment technology where a cryptographic token is sent to the merchant that represents the credit card number that does not reveal any number between the third party vendors. Experts analyses that these kinds of ID verification systems can reduce the risk of accidental data leakages where money can be easily transferred without any security risks. The people working under this system are planning to start their talks with several financial organizations that already use Ripple so as to put the system into test.

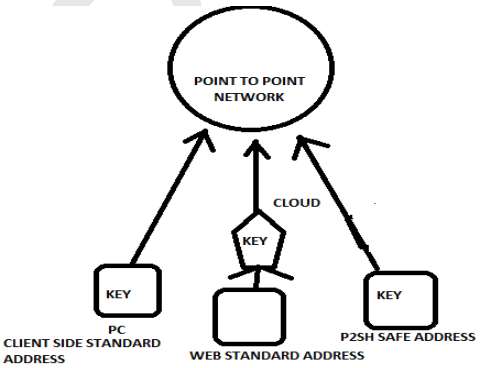

Fig 1. Secure Bitcoin money transfer

III. DATABOX: THE NEXT GENERATION SAFEGUARD FOR OUR PERSONAL INFORMATION

One of the most complex issues now is to manage personal data, since almost all type of web sites surfing discloses data that many use for their benefits by social networks and advertisement companies. This form of data availability is mostly controlled by online business where popular advertising is a source of earning. The collected personal information can be misused with several effects where only victim has to pay for the same in terms of security and information leakages. Different companies take advantage of those data for sending spams and unauthorized

IJDACR
ISSN: 2319-4863

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary research
Website: www.ijdacr.com (Volume 3, Issue 8, March 2015)

messages. Though people can use other facilities, they are made not to do so. To avoid these unfair means, the next option is using offline methods, but that is a viable.

A. Data box

Recently few experts from Queen Mary University and his friends from University of Cambridge provided a solution though an imaginary software which manages the personal data in such a way that only formal data is available to companies. They named it as the data box technology. Basically data box are networking field services that works on a mutual relationship on one's personal information collected from different devices and makes the access possible only to selected information that is authorized by the user as shown in Fig 2. It will come with a number of features. Predominantly, trust from the user's part will be a big concern since user's data will be gathered in terms browsing and financial information and related habits comprising of social media and bank details. To make these technologies feasible it is required that the data must be made to store at a single registry along with data security. Along with that a treaty of trust must be maintained not only with the customers but the third party auditors will be responsible for system operations. The Databox will come with the access feature facility, since the user here controls and can manipulate all the settings on the data access by the third party, additionally the third party too gets the chance to selectively ask for the user's access allowance[1]. Thus it can minimize the company expenses for example certain company don't have to worry about data storage and can be carried and run by some third parties to manage those.

B. Future expectations from the box

Though there are certain challenges incorporating this totally new data source and access to higher device, it is much predictable that government will play an important role in controlling landscape, where such facilities can be created. A project named Nymofe, is on the papers that will allow people to control digital lives which will work on a software infrastructure and is worth watching. It will be promising if certain technologies like Databox like services will be available everywhere for data access and add-on security features.

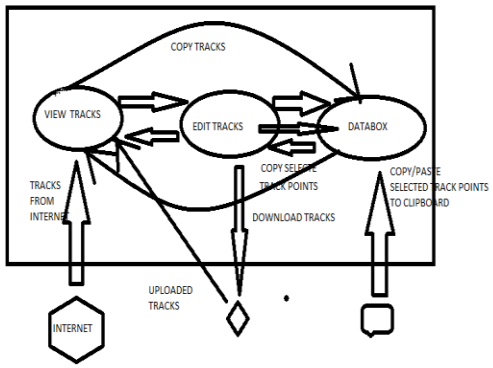

Fig 2. Databox implementation

IV. ADVANCED PERSISTANT THREAT (APT) AND ITS RELATED ADVERSITIES

With the development of large open network globally, security threats have increase and there is an immediate need to detect such threats as it is becoming a challenge. APT (Advanced persistent threat) are such kinds of malicious attempts that cannot be detected by

IJDACR
ISSN: 2319-4863

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary research
Website: www.ijdacr.com (Volume 3, Issue 8, March 2015)

normal anti viruses that are available in the market. RAT (Remote Trojan Access), the most common type of APT infiltrates the network through an email message or by some other means. The attacker can carry out hidden information through remotely controlled operation that is disguised in the flow of ordinary communication for a long period of time. So it becomes difficult to discover the problem at the exit point of internal network. Due to huge stream of traffic, its processing requires time to identify the communication associated with an attack. For the high speed detection of malware in real time, a technology has been developed that would work using general purpose servers. This technology protects against data breaches before they occur.

A. Detection of RAT

For analyzing high speed latent activity of RAT within an internal network Fujitsu Laboratories developed two new technologies that identify attack related communication traffic an infected PC sends to its target[3]. Choke point method is used by this technology at high speed which makes it practical to perform with network devices that uses limited computer resources for this operation as shown in Fig 3.

Specific Domain Detection Method: Detailed analysis must be performed to check whether the communication is associated with an attack or not. Now new ways are developed that reduces the processing load that is required for analyzing attack related communication. Under this method the relationship between data on specific domains for multiple communication sequence is used.

Screening Method: Screening process that detects multiple suspicious communications by screens at each stage of an attack. The processing procedure of an attack and communication information is compared in order to screen at each level of an attack. This technique reduces the processing time for extracting enormous data from multiple communications that comprises an attack.

By using these two techniques it was possible to monitor malicious traffic flowing over a network that helps in the detection of APT malware, that firewalls and antivirus can't detect. [2]In a recent research done on few thousand devices where work-related communication systems were flowing, the RAT activity and detection were verified the resultant of which showed the detection of RAT malware, that showed 0.0001% of overall packet communication volume that represented the total RAT detections.

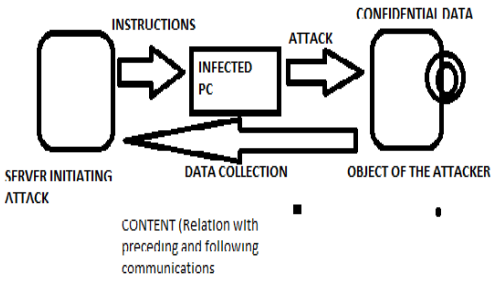

Fig 3. Monitoring method of choke point

V. CONCLUSION

Network security is a joint combination and culmination of cryptographic tools and techniques for development, analysis of network terminals. Thus with an

IJDACR
International Journal Of Digital Application & Contemporary Research

International Journal of Digital Application & Contemporary research
Website: www.ijdacr.com (Volume 3, Issue 8, March 2015)

intent to highlight these advancements we tried to discuss few technologies based on advanced networks. While deployment of 'Databox' technology will revolutionize the security systems and access methods between the organization and the third parties with a trust among them, while the Ripple system associated with rewiring the bank's authentication using cryptographic tricks that generates a unique token for digital money transfer security. At the end we explained few mechanisms that identifies 'Remote Trojan Access' in a network which cannot be done with antiviruses or firewalls in real time operations and further work on improved network practices and policies.

REFERENCES

[1] Haddadi, H, Howard, H, Chaudhry, A, Crowcroft, J, Madhavapeddy, A. and Mortier, R. 2015. Personal Data: Thinking Inside the Box.

[2] Fujitsu. 2014. Fujitsu develops technology to quickly detect latent malware activity in internal networks.

[3] Simonite, T. 2015. Ripple, a Cryptocurrency Company, Wants to Rewire Bank Authentication.

[4] Westin, A. F. 1998. E-commerce & Privacy: What Net UsersWant. Privacy & American Business.