Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 9 July 2021: 13552 – 13560

Research Article

A Review Article on Impact of Social Engineering Attacks against Security of IoT

Ambika V [1] Shashank N [2] Tanuja Kayarga [3] Pruthvi P R[4]
ambika.cs@vvce.ac.in shashank.n@vvce.ac.in tanuja.k@vvce.ac.in
pruthvi.pr@vvce.ac.in

[1] [2] [3][4] Assistant Professor, Vidyavardhaka College of Engineering, Mysuru, India

Abstract
Today, for many people Internet of Things (IoT) devices are accepted and trusted parts of everyday life. A security risk associated with IoT which is often overlooked is the increased vulnerability to social engineering attacks which are psychological attacks directly on humans using devices, rather than the devices themselves. The use of modern IoT devices has unfathomably expanded the span of an attacker, and the success of social engineering attacks. IoT devices often hold the trust of users as they belong to a family of devices which they have been able to safely use for years. The trust relationship between users and IoT devices makes them an effective avenue for social engineering attacks because users are more likely to accept information received from them without question. Social engineering in the IoT is a strong type of force-multiplier as people ultimately have control of all 'things' connected: hack the person and you have access to it all, which could be their home, their business, their car, and their personal information. Successful social engineering attacks through IoT frameworks could prompt an idea of being encircled by threatening gadgets, and extraordinarily impede advancement; making the results of consequences of social engineering attacks in the IoT convincing.

Keywords
Internet of things, Social Engineering , Security challenges of IoT , Social engineering attacks

1. Introduction

It’s not the time to know who has created the world, you have to see who are going to destroy it; Chomsky said [1]. The Internet has become the largest communication and information exchange medium. In our daily life, communication has become distributed over a variety of online communication channels. In this world of ubiquitous communication, people freely publish information in online communication and collaboration tools, such as cloud services and social networks, with very little thought of security and privacy. They share highly sensitive documents and information in cloud services with other virtual users around the globe.

Internet of Things (IoT) is rapidly developing and glamorous technology in which machines and devices are connected and interacted with each other via Internet anywhere anytime. Home machines, garments, traffic signals, vehicles and more things used by the individuals are prone to be correlated with the Internet of Things. Security is perhaps the best test of IoT. The everyday life of person is engaged with the IoT, consistently and whenever is conveyed or constrained by clients, along these lines an essential job will be capered in human cooperations by IoT. Affecting the social associations of people and their

regular day to day existences can represent the infiltration in the IoT and testing the security. More commonly organizations focus on technology-based cyber security risks while not focusing sufficiently on people and process, both of which are common failure points," said T.J. Laher, senior solutions marketing manager at Cloudera and host of the Cybersecurity On Call podcast. The IoT addresses a totally extraordinary and productive area for social engineering attacks from the contemporary Internet with assaults all the more normally found in the mechanical control world..

2. Social Engineering

While the threat of IoT security issues is apparent, people and the processes they create are often more problematic. Threat actors have long used social engineering to target traditional computer networks and computing platforms. But the technique is also perilous for enterprise IoT devices, nearly half of which have been breached in the past two years, according to a survey of 400 IT executives from Altman Vilandrie & Co. Social engineering attack is one in the top eight IoT security threat.

The "art" of affecting individuals to disclose delicate data is known as social engineering. Varied definitions of social engineering have been conferred but the intellectual form of social engineering is being considered since 1980s Exhaustive meaning of social engineering was introduced by authors in [2]. Social engineering is the art of misleading human and hacking their social practices so as to assemble delicate data [2]. Social engineering in itself in itself doesn't really require a gigantic measure of specialized information so as to be fruitful. Rather, social engineering goes after regular parts of human brain research, for example, interest, civility, artlessness, insatiability, neglectfulness, timidity and lack of care. Fig 1 illustrates the meaning of social engineering.

Fig 1: Meaning of social engineering

Social engineers are likely threat to the innovative present reality since security systems have made colossal advances ary component of information and specialized greatness , while social engineering does not require technical knowledge and has a superior return. Social Engineers as opposed to assaulting security frameworks, goes to the specialists of these frameworks and hacks their brains. Fig 2 shows the difference between hacking and social engineering.

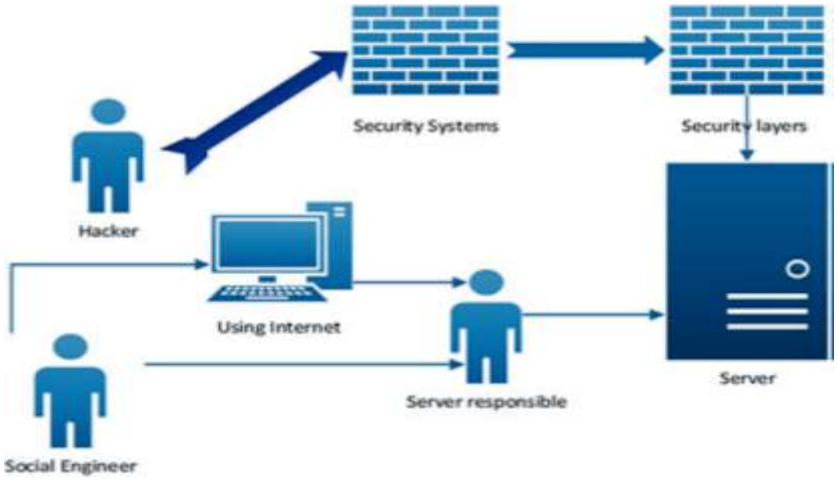


Fig 2: Difference between hacking and social engineering

Social engineering is cutting edge type of the certainty trick which frauds have consistently executed. Phishing emails, which deceitfully demand private information, are a typical variant of the attack, but social engineering comes in numerous structures intended to abuse mental shortcomings of the objective. Various exploratory investigations throughout the years have shown the sensitivity of people to social engineering attacks. The adequacy of social engineering has urged attackers utilize it more often, relying on social engineering as a component of larger attacks.

3. Characterization of Social Engineering Attacks

As shown in Fig 3, Social engineering attacks can be divided into the class of *generic* attacks, such as phishing, which are created for a broad audience, and the class of *targeted* attacks which are refined for a smaller target group, or even an individual .

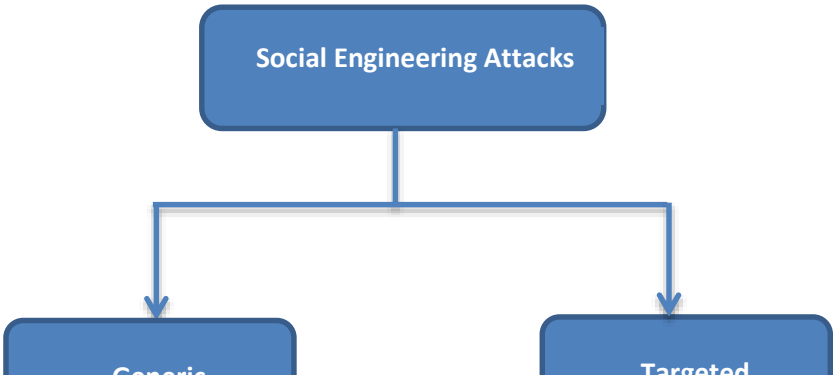


Fig 3: Characterization of Social Engineering Attacks

Basic phishing attacks are created in a generic way so that they can be automatically deployed to attack many people very easily. However, since they are generically constructed, they are not particularly effective against any individuals, so the success of a phishing attack is based on the number of people to whom it is deployed. Compared to a phishing attack, a targeted attack is created to focus on a smaller subset of people, and is often more effective than regular phishing attacks. *Spear phishing* is the term used to describe phishing attacks which are targeted in this way. An example of the type of targeting used in a spear phishing attack can be seen in the following excerpt from a real spear phishing email deployed against email users at the University of Buffalo.

"This mail is from the UBmail and it is to inform all our UBmail users ..."

The email continues to request various credentials including username and password. This spear phishing email contains a reference to "UBmail" which is the name of the email system at the University of Buffalo. By modifying the email to include local information, the attack is likely to be more effective because it tends to engender more trust in the target.

4. Social engineering attack framework.

The social engineering attack framework can be used to illustrate the planning and flow of the full attack[3]. Fig. 4 portray the social engineering attack framework. As illustrated in the fig 4, there are six core phases, namely attack formulation, information gathering, preparation, develop relationship, exploit relationship and debrief. The “attack formulation” phase is used to determine both the objective and the target of the precise attack. The “information gathering” phase is utilized to recognize both the goal and the target, just as to assemble data from the distinguished sources. In the “preparation” phase, all the accumulated data is combined and the social engineering attack vector is created.

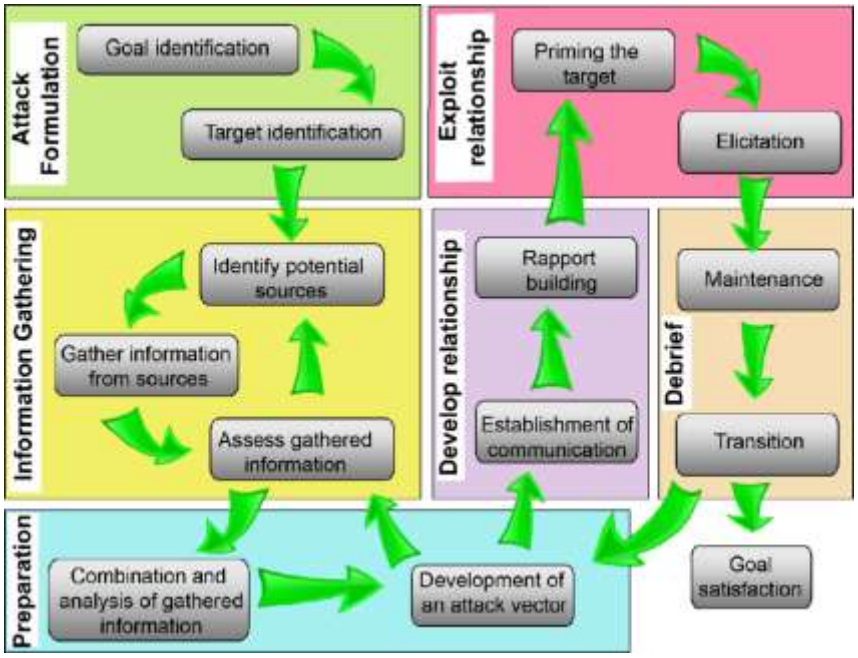


Fig 4: Social Engineering attack framework

It is during the “preparation” phase that all the components in the social engineering ontological model can be recognized. The “develop relationship” is the place where the attacker sets up correspondence with the objective and endeavors to fabricate a trust relationship with the objective. The “exploit relationship” phase is utilized to take action and to inspire the objective to play out the solicitation or activity. The last phase is the “debrief” phase, in which the target is brought out of a primed state during the “maintenance” step and the “transition” step tests whether the objective has been satisfied.

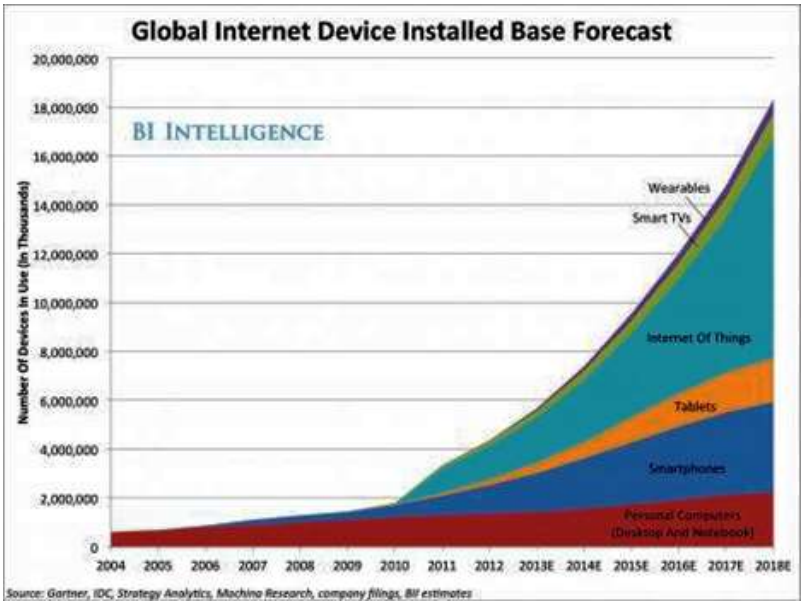
5. Security challenges for IoT

IoT brought users huge benefits; however, some challenges come along with it. Cyber security and privacy risks are the primary concerns of the researchers and security specialists cited [8]. t is assessed that with the ascent in number of things associated with IoT frameworks to amassing billions of gadgets by 2020, the potential weaknesses will likewise increment. Thus, the expansion in weaknesses due to non-normalization of IoT advances may offer ascent to security occurrences in IoT frameworks. During a security audit conducted by [9], numerous smart devices were checked for security breaches. According to discoveries of the security review, practically 90% of these gadgets assemble individual data about the clients in some structure or the other. This unapproved stockpiling of data is helpless against information security, protection and uprightness assaults. Researchers in [10] and [12] have also rendered security and privacy issues a threat to data confidentiality and user privacy. In addition, absence of dependable validation component in IoT gadgets is additionally a contributing element in frail IoT security [11]. Moreover, the absence of information encryption and system access control estimates empower an assailant to represent a genuine danger to client protection because of listening in and traffic investigation [13].

Prevalent high-profile cybersecurity attacks have demonstrated the vulnerabilities of IoT technologies. This vulnerability is simply because the interconnectivity of networks in the Internet of Things brings along accessibility from anonymous and untrusted Internet requiring novel security solutions [14]. adaptation, such as security and privacy. It is, however, unfortunate that the users do not often have the required acknowledgment of the security impacts until the time when a breach has occurred, causing massive damages such as loss of crucial data. With the ongoing security breaches which have compromised the privacy of users, the appetite of the consumers for poor security is now declining. In a recent review conducted regarding privacy and security, consumer-grade Internet of Things did not do well. There were a lot of vulnerabilities in modern automotive systems.

6. Social Engineering as a threat to IoT

It can be argued, convincingly, that the Internet of Things is already here. Web connected devices are everywhere and their prominence is increasing at a very high speed. Figure 4 below is taken from [4] and is indicative of the high rate of expected growth of connected devices in the next few years. This phenomenal growth is expected to have significant consequences for social engineering [5][6][7].
It is clear that if a cybercriminal can gain control of a multitude of such devices he/she can wreak havoc and cause significant damage.



An attack on IoT systems can trick a user by feeding him/her with misinformation to execute complex commands as to the cyber criminal's wish. A coordinated attack on many IoT systems simultaneously has the potential to create havoc. The social engineer can then utilize this havoc to manipulate victims in a variety of yet unknown creative ways. Attacks, for example, on a corporation will be harder to stop when a cybercriminal can study the Vice President's voice, habits and preferences without being detected. Successful social engineering attacks via IoT can give people the perception that they are surrounded by contentious devices. This could impede the development and public acceptance of IoT devices. Thus, the effects of social engineering on IoT may be very significant. As IoT devices become more prevalent and cyber-attacks on these systems become more damaging, new technologies for authentication and encryption of low-resource "Things" will be developed. These developments have already begun (e.g. multiparty authentication) but there is a long way to go!.
contentious
IoT is expected to revolutionize the way many services are currently offered, and it consequently has a promising business impact. The collection of very personalized data, as well as the ability of things to operate in the physical world, enables the development of high-level and specifically-tailored services for the users (e.g., medical-related services). However, such strong points are also the factors that most improve the capabilities of social engineers, and can make the IoT be perceived as a weak and dangerous technology. To allow this revolution, the academy and the industry must look for solutions which are cheaper than the current ones (to facilitate the deployment of devices) and that drastically reduce the freedom of movement of social engineers. Otherwise IoT will destroy instead of creating value. We now present the main aspects that it is necessary to focus on: development of well-defined security standards, and implementation of light but still effective security processes [15][16].

Now, there is not a widely-adopted security standard in the IoT world (such as the ISO 27000 for the traditional IT network). Without a coherent regulation, IoT networks become even more complex than what they already are. Thus, each network requires an individual and unique security investment/assessment [17]. The heterogeneity of IoT networks at all the layers (from the physical to the application one) make the malicious actions of a social engineer easier. Very heterogeneous systems should not lead users to properly know their devices and how they work. The social engineer can exploit this weakness, since he can more easily persuade the victim that a dangerous operation is a good one.
As far as security processes are concerned, being IoT devices resource-constrained, traditional authentication/encryption procedures are hardly applicable. The improvement of more appropriate security advancements will be a helpful cure additionally against social building assaults, since the simpler is to send and show warped messages by means of IoT gadgets, the simpler social designing will turn into [18].
The results of social designing assaults in the IoT could be more awful than similar in the “IT Internet” of today. The perception goes from one of “living with weak devices”, to being “surrounded by hostile devices”!. Gadgets that may whenever attempt to misdirect you into accomplishing something against your inclinations, similar to a vindictive robot from a sci-fi film. That would awful. It is one issue if your

Things are being hacked and compromised regardless of your great confidence, it is another issue if your Things are tricking you into hurting yourself, or others.

As an potential outcome:

- Social engineering attacks in the IoT will will delay adoption of technologies that otherwise might present major social and business benefits
- Social engineering attacks in the IoT will undermine confidence in the safety – not just the security – of the IoT. Social engineering in the IoT is a potent form of force-multiplier because people ultimately have control of all Things: hack the person and you have access to it all.
    - Social engineering attacks in the IoT might raise levels of regulation in a reflexive and ill-conceived manner, with outcomes as uncertain as leaving the IoT at its current, low state of security-maturity.

7. Addressing social engineering attacks on IoT

There is no single remedy to address social engineering attack on IoT. Layers of security and technology will need to be applied. Existing defenses against social engineering attacks are divided into two categories, *training-based* defenses which train the user to defend himself, and *automatic* defenses which attempt to analyze communication and detect attacks automatically. Preparing regimens have been proposed which teach users on the methods utilized in the past assaults, and the significance of different pieces of information. Preparing strategies rely upon the client's familiarity with his/her psychological state and manners of thinking, alluded to as *metacognition*. A user may be might be required to deliberately consider security inquiries in a discussion, while giving information to an outside specialist. Such training-based approaches are important but they cannot be relied upon in general because a user's response to an attack is highly dependent on his mental state at the time of the attack, and this is not predictable. A person who is upset due to an event in his personal life will be more susceptible to an attack than a person with a secure mental state. A person's reaction to an attack is also highly dependent on aspects of their personality which are not controllable. Some people may be more insecure and feel a need to please someone who they are communicating with by answering their questions. Mental state and personality issues are not strongly impacted by training.

A number of automatic approaches exist to detect phishing emails and phishing websites masquerading as trusted websites. Phishing website identification approaches inspect the features of the website and apply a set of rules which distinguish abnormal website properties. Recognizing highlights utilized incorporate the presence of deluding URLs, the presence of explicit pictures, customer side hunt history, and secret key solicitations. Recognition rules think about estimations of individual highlights and relationships between element esteems, for example, the incorporation of an organization logo at a site whose URL isn't identified with the organization. A few strategies have been urged to distinguish phishing messages by extricating highlights of the email header and body. Generally utilized highlights incorporate the utilization of IP-based URLs, URLs connected to new areas, HREF values which don't coordinate the showed connection, and HTML messages which permits URL names to be conceal.

Significance of solitude codes

Application developers and gadget makers mainly thinks about approaches for their items and, considering that, offer alternatives in items that clients with their settings can choose if their security assurances are exacting or not. . Security settings are not set as default by the producer carefully, and the

clients themselves must set them up just as he would prefer. For example, there is two-advance check in numerous acclaimed applications, yet low level of clients utilizes it.

Focus on the App authorizations and terms of utilization

The applications are turning into a major danger as there is no checking of their appropriation and security norms. Developers undoubtedly contact their enormous colossal crowd without separating them to survey their security. Applications that are utilized on gadgets n approach various pieces of the gadget. Crooks utilize this component and furnish applications with explicit gets to, and the client introduces it, and afterward the gadget is for all intents and purposes constrained by hoodlums. It is observed that the calculator application with access to the memory card and the user's camera, while it does not need any access to it. Users' regard for these accesses is significant.

8. Conclusion

IoT promises to synergize technology in new and innovative ways, and in doing so it presents major social, business, and economic benefits for modern society. Equally, for cybercriminals, the IoT promises significant rewards if they can execute a social engineering attack successfully, because hacking the user can provide access to all the "things" that they control. The more successful social engineering attacks against the IoT are, the more user confidence in its security is undermined, ultimately delaying adoption of the IoT and the realization of its potential benefits.

Social engineering attacks are not likely to disappear anytime soon as there is no patch for human stupidity.but IoT designers need to appreciate the significance of these attacks and start to build detection approaches into products. Training of users is useful for an employer to require for all employees, but automatic detection approaches directly integrated into IoT devices has a much greater potential for reliability in the long term. Automatic detection approaches need to scan user communication for suspicious activity while maintaining user privacy. This is a hard problem but it must be addressed if people are to be expected to continue accepting IoT technology to the degree that they have in the past.

This paper presents a review of social engineering attacks, possible threats on IoT caused by social engineering attacks and combating social engineering attacks. Future investigations can focus on procedures to forestall and moderate risks of social engineering attacks on IoT.

References

[1]. Chomsky N (2017) Noam Chomsky website, 17th March 2017. Retrieved from https:// chomsky.info

[2]. Ghasemi M, Saadaat M (2017) "Toward introduction of Social engineering as a threats against the security of personal and professional information". In 2nd conference on cyberspace security incidents and vulnerabilities (CSIV 2017), Fersousi University, Mashhad, Iran

[3]. Francois Mouton, Louise Leenen, H.S. Venter, "Social engineering attack examples, templates and scenarios", sciencedirect, 2016 Elsevier Ltd

[4]. E. Adler, "Here's Why "The Internet Of Things' Will Be Huge, And Drive Tremendous Value For People And Businesses" Business Insider 2013. [Online].

[5] C. Kerley, "From Smartphones to smart everything: Welcome to the 'smart' revolution (part 1 of 2)," 2014. [Online]. Available: http://allthingsck.com/wp-content/uploads/CK-From-smartphones-to-smart-everything.pdf . Accessed on: Dec. 16, 2015.

[6]. R. Miller, "Cheaper sensors will fuel the age of smart everything," TechCrunch, 2015. [Online]. Available: http://techcrunch.com/2015/03/10/cheaper-sensors-will-fuel-the-age-of-smart-everything/#.oeoofin:otGd . Accessed on: Dec. 16, 2015.
[7] "Smart everything," 2002. [Online]. Available: http://www.shapingtomorrow.com/home/alert/625628-Smart-Everything . Accessed on: Dec. 16, 2015.
[8] Lo'ai Tawalbeh, Fadi Muheidat, Mais Tawalbeh and Muhannad Quwaider, "IoT Privacy and Security: Challenges and Solutions"
[9] HPE Fortify and the Internet of Things, (2017) . [Online]. Available: http://go.saas.hpe.com/fod/internet-of-things
[10] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial Internet of Things," in Proc. 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), 2015, pp. 1–6.
[11] T. Borgohain, U. Kumar, and S. Sanyal, "Survey of security and privacy issues of Internet of Things," 2015.
[12] Gemalto. Securing the IoT-Building Trust in IoT Devices and Data. 2020. Available online: https: //www.gemalto.com/:https://www.gemalto.com/iot/iot-security. (accessed on 17 February 2020).
[13] H. Ning, H. Liu, and L. T. Yang, "Cyberentity security in the internet of things," Computer, vol. 46, no. 4, pp. 46–53, 2013.
[14] Tawalbeh, L.A.; Tawalbeh, H." Lightweight crypto and security. In Security and Privacy in Cyber-Physical
Systems: Foundations, Principles, and Applications"; Wiley: West Sussex, UK, 2017; pp. 243–261.
[15]https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf . Accessed on Dec 5, 2015
[16] T. Macaulay, "International Security Standards and the Internet of Things" [Online]. Available: https://blogs.mcafee.com/executive-perspectives/international-security-standards-internet-things/ . Accessed on Dec 5, 2015
[17] T. Macaulay, "Social Engineering in the Internet of Things (IoT)" [Online]. Available: https://blogs.mcafee.com/executive-perspectives/social-engineering-internet-things-iot/. Accessed on Dec 5, 2015
[18] T. Macaulay, "Multi-party authentication and cryptography in the IoT" [Online]. Available: https://blogs.mcafee.com/business/multi-party-authentication-cryptography-iot/ Accessed on Dec 5, 2015