SECURITY CONSIDERATIONS FOR EDGE COMPUTING

John M. Acken[1] and Naresh K. Sehgal[2]

[1]ECE Department, Portland State University, Portland, OR
[2]Data Centre Group, Intel Corp, Santa Clara, CA

ABSTRACT

Present state of edge computing is an environment of different computing capabilities connecting via a wide variety of communication paths. This situation creates both great operational capability opportunities and unimaginable security problems. This paper emphasizes that the traditional approaches to security of identifying a security threat and developing the technology and policies to defend against that threat are no longer adequate. The wide variety of security levels, computational capabilities, and communication channels requires a learning, responsive, varied, and individualized approach to information security. We describe a classification of the nature of transactions with respect to security based upon relationships, history, trust status, requested actions and resulting response choices. Problem is that the trust evaluation has to be individualized between each pair of devices participating in edge computing. We propose that each element in the edge computing world utilizes a localized ability to establish an adaptive learning trust model with each entity that communicates with the element. Specifically, the model we propose increments or decrements the value of trust score based upon each interaction.

KEYWORDS

Edge Computing, Security, Adaptive learning, Trust model, Threats, Cloud Computing, Information Security

1. INTRODUCTION

Edge Computing represents a combination of distributed computing connected to centralized servers. Historically, centralized versus distributed models have alternated as computing and communication capabilities have grown, while the limiting factor has alternated between computational capability and communication capacity. The present environment of cloud and edge computing is a complex mixture of computing capability, communication capacity, and security considerations. In this paper, we will focus on the security aspects of edge computing. Any such investigation must include multiple subtopics, e.g., protecting information content from observation and alteration, protection of operational capability from unauthorized access, protection of normal operation in the presence of malicious overloaded requests etc. Solution components need to consider prevention from and response to any security threats [1]. Examples of prevention include encryption to protect content from observation and alteration, access checking protocols to prevent unauthorized accesses, tracking mechanisms to identify attempted attacks, and blocking messages except from trusted devices.

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 187-194, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90915

2. Background

Today's information technology environment contains a wide variety of computing resources and a multiplicity of communication channels between the various computing resources. Economics drove creation of large datacenters, and Cloud computing was born to utilize this enormous computing power. As capability of inexpensive computing continued ahead of the communications capabilities, computational power moved back to the end nodes of a system. The age of IoT (Internet of Things) arrived a decade ago as demonstrated by the fact that more things were connected to the internet than people in the world [2]. The "things" connected to Internet include sensors, controllers, and intelligent devices [3]. These devices have limited power to create security problems but they have even more limited ability to provide security solutions. To date the biggest security breaches in the IoT world have been instructions sent to the IoT devices, which then launched massive denial of service attacks on central servers. The top three examples are Mirai, Hajime and Persirai codes [4].

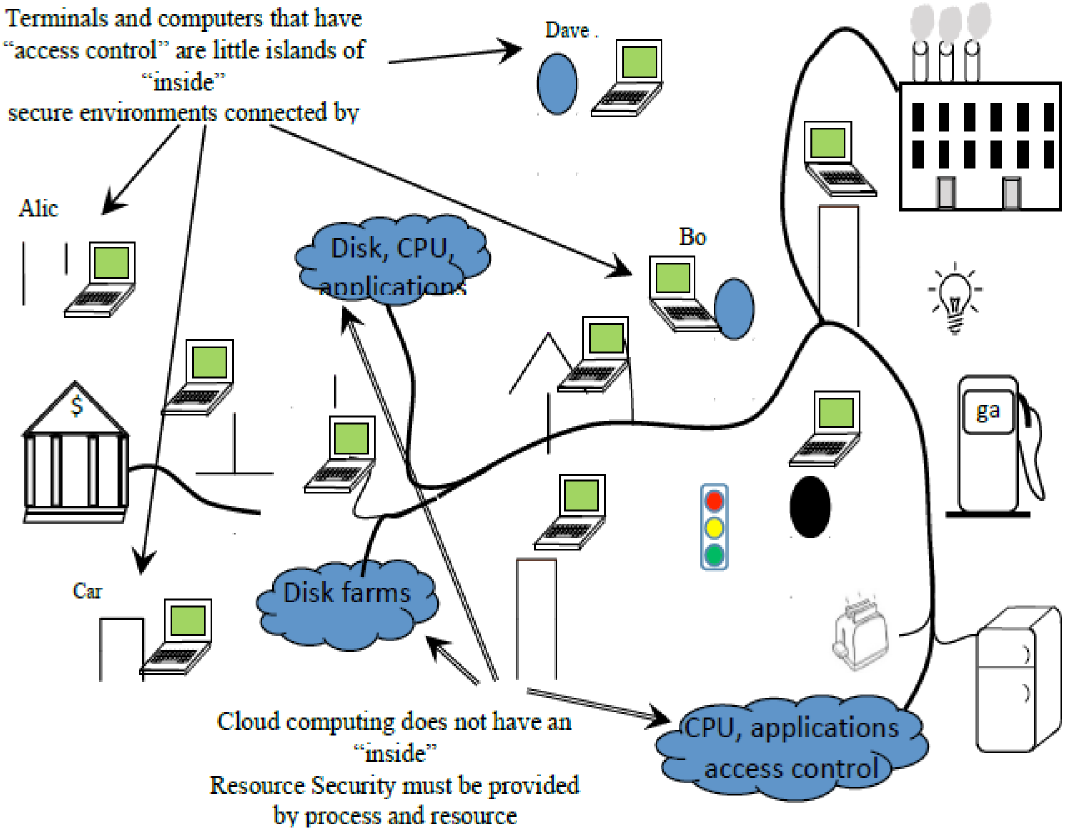

Terminals and computers that have "access control" are little islands of "inside" secure environments connected by
Dave .
Alic
Bo
Disk, CPU, applications
$
Car
Disk farms
ga
Cloud computing does not have an "inside" Resource Security must be provided by process and resource
CPU, applications access control

Figure 1. Variety of elements connected in the IoT world demonstrates security challenges, especially with a wide range of security requirements.

To visualize a wide variety of elements and security requirements in the IoT domain, consider Figure 1. The standard internet communication security approach (including virtual private networks, i.e., VPN) is to establish a link between Alice and Bob using access control to identify the authorized individuals and then to use encryption for information exchange between the "islands" of security containing Alice and Bob. Alternatively, Dave may want to do a transaction with his bank. Dave's transaction requires a higher level of security than Dave's normal activities. Carol may want to turn on her light bulbs at home since she will be arriving after dark. While this does not require a high level of security, Carol certainly does not want some random person turning her lights on and off. Other examples of low levels of security are the household appliances, such as a toaster or a refrigerator. The high levels of security examples include opening a home garage, accessing banks or operating factories.

3. EMERGENCE OF EDGE COMPUTING

In the era of edge computing another consideration is due to multiple connection paths for each device. Each element on the edge can connect using a choice of paths or even multiple paths between the same endpoints. Specifically, any computing element on the edge can connect via the internet, telephone lines, cell phone connections, wireless local area service networks (WiFi), or local wireless point-to-point connects such as Bluetooth or NFC (Near Field Communication) etc. See figure 2 for multiple paths from Alice to Bob, to a local server hub, to the internet, or to the house alarm system. Edge computing continues to mature and encompass more of our world. Standards are being created such as Waggle [5], which is an open sensor platform for edge computing, has been introduced to reduce some of the foreseen compatibility problems.Edge computing security issues encompass end-to-end devices and the networks in between.

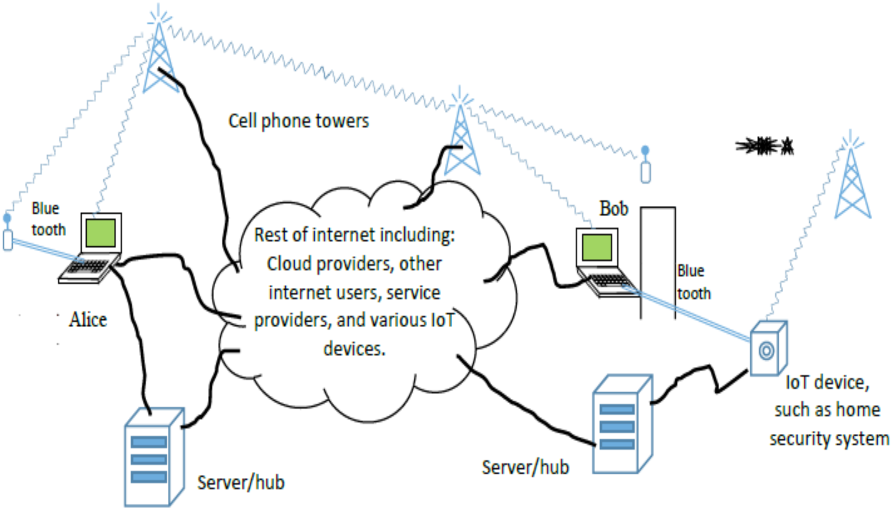

Cell phone towers
Blue tooth
Alice
Rest of internet including: Cloud providers, other internet users, service providers, and various IoT devices.
Bob
Blue tooth
IoT device, such as home security system
Server/hub
Server/hub

Figure 2. Communication connectivity from the edge

4. STATUS OF EDGE COMPUTING SECURITY AND RECENT BREACHES

The security issues for Edge computing often overlap with existing security problems. Access control using identity authentication is especially difficult in the IoT environment. Edge computing greatly increases the number of devices that need authentication. The pairwise authentication problem increases faster than exponentially (specifically the increase is N! where N is the number pairs) with increase in possible paths between the devices that need authentication. Added to the authentication problem, the problem of corrective action when unauthorized access is detected.

One of the largest attacks that Internet has ever experienced was recently launched using unsecure routers, digital video recorders (DVRs) and online surveillance cameras [6]. A collection of devices called botnet (an army of infected devices) was used to launch a Distributed Denial of Service (DDoS) attack on KrebsOnSecurity.com, the website of a Security journalist who had previously exposed cybercriminals. This attack generated > 660 Gbps of traffic, making it the largest attack on record in terms of data volume. In another case, a pair of researchers showed that they could remotely hijack a Jeep's digital systems over the Internet. It led to a recall of 1.4 million vehicles [7], which required a costly fix after it was shown that a moving Jeep's steering wheel could be turned, unintended acceleration caused and brakes disabled remotely. Many homes have Internet enabled devices including thermostats, garage door openers, smart TVs etc. Such devices may contain vulnerabilities, enabling hackers to compromise a home, including changing the heating or cooling settings, opening garage doors and use TVs to connect with PCs on the home networks for stealing personal data [8].

Threat tracking and tracing are difficult for the IoT environment, but there are only a few channels through which an attack may travel. With Edge computing, definition and enforcement of the virtual protection boundary is difficult. Therefore, monitoring and responding to threats is the key. Fortunately, the increased computational ability of the elements at the edge also offers the potential for increasing the sophistication of the security monitoring and corrective responses.

5. Security Modelling Targeting Edge Computing

Perimeter defence has long been insufficient for IoT security. Fixed protocols for boundaries of security with individual devices' security implementations will fail, because devices can have multiple channels of communications across boundaries.Each of these can be configured dynamically bypassing the fixed protocols. In addition, a fixed universal security policy is inadequate.However, components throughout the Edge computing environment must be adaptive in the sense that each device builds an individual trust model with the other devices to which it connects. This model must include monitoring to determine the level of trust applied to each individual connection between devices. The source device's trust (which sets the specific security policies and actions) increases based upon a history of successful connections and transactions with the responding devices. The source device's trust decreases based upon measured or detected failures for connections and transactions with the responding device. The decreased trust invokes increased security measures as will be described in a later section. Therefore, each device must learn who to trust and what level of trust to extend to other individuals and devices.

Each device may be part of the community of edge devices and cloud services. This community is similar to online communities of individuals and Hamilton et al describe the trust in an online community as a function of loyalty to the community [9]. Each edge device evaluates its trusted partners based upon preference, commitment, consistency vs surprise, and decisions or actions to be taken. The preference and commitment is established by the quantity and time spread of past communications. The measure of trust from one edge device to other entities is either increased by exchanges consistent with past exchanges or decreased by any surprisingly different exchanges. Thus, consistency increases trust and inconsistency decreases trust. The level of trust (based upon the past) and the immediate request drives a decision or action on the part of either the edge device or the cloud service component. A key to the success is the ability of each entity to learn and improve the measurement of trust.

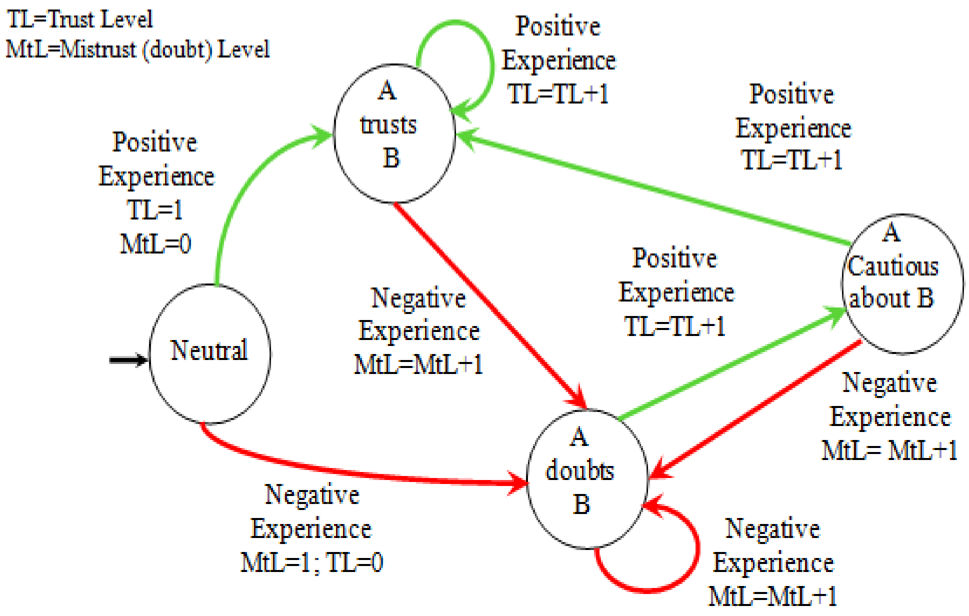

TL=Trust Level
MtL=Mistrust (doubt) Level
A trusts B
Positive Experience TL=TL+1
Positive Experience TL=TL+1
Positive Experience TL=1 MtL=0
A Cautious about B
Positive Experience TL=TL+1
Negative Experience MtL=MtL+1
Neutral
Negative Experience MtL= MtL+1
A doubts B
Negative Experience MtL=1; TL=0
Negative Experience MtL=MtL+1

Figure 3. Element A's State of Trust Level of element B.

Table 1. Categories of Security Considerations for connection from A to B

Length and frequency of relationship	Purpose of relationship	History	Action Request	Severity and Urgency	Status of Trust	Response
New, first contact _ _ _ _ _ _ _ Short term many contacts _ _ _ _ _ _ _ Short term, few contacts _ _ _ _ _ _ _ Medium term many contacts _ _ _ _ _ _ _ Medium term, few contacts _ _ _ _ _ _ _ Long term	Casual _ _ _ _ _ _ _ Medical _ _ _ _ _ _ _ Legal _ _ _ _ _ _ _ Financial _ _ _ _ _ _ _ Schedule or calendar _ _ _ _ _ _ _ Employment _ _ _ _ _ _ _ Political _ _ _ _ _ _ _ Religious _ _ _ _ _ _ _ Ownership/ Property _ _ _ _ _ _ _ None/just Information _ _ _ _ _ _ _ National Security	Neutral _ _ _ _ _ _ _ Successful _ _ _ _ _ _ _ Failure _ _ _ _ _ _ _ Mixed successes _ _ _ _ _ _ _ Past success, recent failure _ _ _ _ _ _ _ Past failure, recent success _ _ _ _ _ _ _ Relationship change	Data or message delivery _ _ _ _ _ _ _ Data or message request or exchange _ _ _ _ _ _ _ Monetary transfer _ _ _ _ _ _ _ _ Physical Action _ _ _ _ _ _ _ _ Verification _ _ _ _ _ _ _ _ Open connection_ _ _ _ _ _ _ _ Attestation	Emergenc y _ _ _ _ _ _ Critical _ _ _ _ _ _ Casual _ _ _ _ _ _ Serious _ _ _ _ _ _ Unclear _ _ _ _ _ _	Mutual trust _ _ _ _ _ _ A trusts B _ _ _ _ _ _ B trusts A _ _ _ _ _ _ Mutual doubt _ _ _ _ _ _ A doubts B _ _ _ _ _ _ B doubts A _ _ _ _ _ _ Neutral	Ignore _ _ _ _ _ Store _ _ _ _ _ Respond _ _ _ _ _ Forward request _ _ _ _ _ Alert _ _ _ _ _ Perform action
	Multiple Possible		Multiple Possible			Multiple possible

The previous discussion proposes that information security is far more complex in the current computing environment. Not only does each participant (device, element, or person) require different security considerations, but each relationship between each pair of participants requires different security considerations. Additionally these security considerations change over time based on the past actions and new information. Table 1 summarizes the categories of considerations. It shows that each element in edge computing world needs a localized ability to establish an adaptive learning trust model with each entity that communicates with the element. Our proposed model limits and prevents the spread of a device failure from contaminating the whole system. As a consequence, the trust score of the compromised device shall be lowered.

Let us consider some examples of applying Table 1 and Figure 3. First, consider the case of a patient and physician. For our example: the first column is long term, the second column is both Medical and financial, the third column is successful. The action requested is to renew a prescription which is "data or message request or exchange" in column four. The severity in column 5 is Serious, and the Status of Trust in column 6 is Mutual trust. Therefore, the Doctor's response in column 7 is "Forward Request" to Pharmacy. The level of Trust in the state diagram remains B trusts A and the positive experience raises the Trust Level (TL). Secondly, consider that the patient's friend contacts the physician requesting medical history. This is a new, first contact, and column 2 is medical, History is neutral, action request is data request, Severity is serious but the status is neutral. Now for medical requests the response is multiple in both responding to the requester that this is protected information and alerting the patient that the request was made. The level of trust in the state diagram moves to mistrust because this was an unexpected and not previously authorized request resulting in negative experience. This will be modified with the patient's response to the notification from the physician.

Finally, consider interactions between two devices, for example, a connected car and a cloud computing resource. Specifically, the car's computer contacts the automotive maintenance centre to schedule a regular maintenance. From Table 1, column 1 we see this is a medium term relationship with few contacts. From column 2 we see it is both scheduling and financial. From column 3 we have successful. Therefore, from state diagram 3 we have a positive trust level for between both the car and the maintenance shop. The Action Request column is for data message exchange of data, time, and financial commitment. From column 5, the severity is Casual as it is not urgent or serious. As mentioned before, in column 6 we have mutual trust based upon the history and the state diagram. The action is to respond. Now consider that the car maintenance shop attempts to contact the car and drive it. The first column is still a medium term relationship with few contacts. However, in column two the purpose of the relationship does not match the action request from column 5. Because column 3 and 6 point to some level of trust, but the severity of the action from column 5 leads to a response of "Alert" and "Forward request" but not perform action.

The previous discussions concentrates on trust levels between two entities. However, in reality there are multiple entities involved in some trust relationships. As an example, some security protocols include a third party security certification. In addition, there are some security situations where a third party monitors or records transactions. These considerations will be explored in future work.

The application of Deep Learning for speech recognition is advancing [10], and it could be applied for speaker recognition for authentication and other security evaluations. The concept is to push some of the security decisions to the edge computing devices. The additional compute power at the edge is already being applied for decision-making using machine learning [11][12]. The future of security with edge computing and the cloud is a mix of central protocols in the cloud [13], decision making at the edge based upon machine learning, monitoring and analysing communication activity[14]. A Machine Learning (ML) environment may allow the identification and defence against unexpected and unpredictable security challenges [15].However, ML is a double edged sword as hackers with access to training data can corrupt the learning process, or alter their attack code to specifically bypass a pre-determined security model [16]. There is a no silver bullet to ensure the security for all devices participating in Edge Computing, so a community based adaptive trust model may present an optimal solution.

6. SUMMARY

The present state of edge computing is an environment of vastly different computing capabilities connecting via a wide variety of communication paths. This situation creates both great operational capability opportunities and unimaginable security problems. This paper emphasizes that the traditional approaches to security of identifying a security threat and developing the technology and policies to defend against that threat are no longer adequate. The wide variety of security levels, computational capabilities, and communication channels require a learning, responsive, varied, and individualized approach to information security. We propose that each element in the edge computing world utilizes a localized ability to establish an adaptive learning trust model with each entity that communicates with that element.

REFERENCES

[1] N. K.. Sehgal, S. Sohoni, Y. Xiong, D. Fritz, W. Mulia, and J. M. Acken, “A cross section of the issues and research activities related to both information security and cloud computing,” IETE Technical Review, Volume 28, Issue 4 [p. 279-291], 2011.

[2] https://www.postscapes.com/internet-of-things-history/

[3] J. Ashton, "That 'Internet of Things' Thing", RFID Journal, Jun 22, 2009.

[4] http://blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/

[5] P. Beckman, R. Sankaran, C. Catlett, N. Ferrier, R. Jacob and M. Papka , "Waggle: An open sensor platform for edge computing," 2016 IEEE SENSORS, Orlando, FL, 2016, pp. 1-3. doi: 10.1109/ICSENS.2016.7808975

[6] https://motherboard.vice.com/en_us/article/15-million-connected-cameras-ddos-botnet-brian-krebs

[7] https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

[8] http://abc7chicago.com/technology/home-hackers-digital-invaders-a-threat-to-your-house/515520/

[9] W. L. Hamilton, et al., “Loyalty in Online Communities,” Proceedings of the Eleventh International AAAI Conference on Web and Social Media (ICWSM 2017). Pp 540-543.

[10] L. Deng et al., "Recent advances in deep learning for speech research at Microsoft," 2013 IEEE International Conference on Acoustics, Speech and Signal Processing, Vancouver, BC, 2013, pp. 8604-8608. doi: 10.1109/ICASSP.2013.6639345

[11] R. Nelson, “Smart factories leverage cloud, edge computing,” Evaluation Engineering, Vol. 56, No. 6, June 2017.b

[12] https://www.kdnuggets.com/2017/01/machine-learning-cyber-security.html

[13] Wei Li, "An adaptive security model for communication on cloud," Proceedings of 2011 International Conference on Computer Science and Network Technology, 24-26 Dec, 2011.

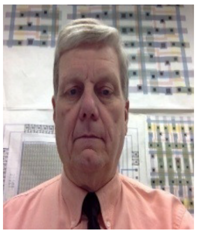
[14] R. Sommer, V. Paxson, "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection" 2010 IEEE Symposium on Security and Privacy, May, 2010.

[15] https://www.information-age.com/machine-learning-cyber-security-123475346/

[16] https://www.technologyreview.com/s/611860/ai-for-cybersecurity-is-a-hot-new-thing-and-a-dangerous-gamble/

AUTHORS

JOHN M. ACKEN is a faculty member in the Electrical and Computer Engineering Department, Portland State University, Portland, OR. John received his BS and MS in Electrical Engineering from Oklahoma State University and Ph. D. in Electrical Engineering from Stanford University. He projects include technology and devices for information security and identity authentication. John has worked as an Electrical Engineer and Manager at several companies, including the US Army, Sandia National Labs in Albuquerque, New Mexico and Intel in Santa Clara, CA. John's time in the US Army was in the Army Security Agency, a branch of NSA during the Vietnam War.



NARESH is the Data-center Security Director at Intel Corp. He has been with Intel for over 30 years in various roles, including EDA development, Silicon Design Automation, Intel-HP Alliance management, and for launching Virtualization technology on all Intel platforms. Naresh holds a Ph.D. in Computer Engineering from Syracuse Univ. and MBA from Santa Clara Univ. He holds 5 patents and has authored 30+ publications in the CAD domain. He has co-authored a book on Cloud Computing published by Springer in 2018.