Consideration of Insider Based Collusion Attacks on Cyber Systems

James B. McNicholas III and Houssain Kettani

***Abstract*—Insider threats are a growing concern to both public and private entities. Like other threats within the cyber realm, these threats tend to be dynamic in nature. Organizational structures and varying motivating factors of threat actors can impact the effectiveness of mitigating technologies and strategies. This paper explores the gaps that result when organizations try to segment logical and physical assets, which in turn creates the opportunity for collusion or coordinated attacks. In this paper, various data sources have been examined to identify organizational patterns that can potentially contribute to the successful outcome of these types of attacks. A motivating example is then presented, in junction with the data, to hypothesis what percentage of organizations would be able to identify the actions of insiders working in tandem based on the current state of the industry.**

***Index Terms*—Collusion attack, coordinated attack, cyber threats, insider threat.**

I. Introduction

Insider threats continue to be a growing concern to both public and private entities [1]. Specifically, there were reported increases in the number of insider attacks between 2014-2018 [2-5]. The exact number and frequency of attacks is difficult if not impossible to determine as many insider attacks go unreported [6]. While it has been reported that many organizations have implemented some form of insider threat protection model [1], it has been suggested that many of these models do not adequately capture the interrelations between physical and logical cyber assets [7]. For example, controlling access and protecting logical assets can be accomplished by way of implementing algorithms designed to identify abnormal behavioral patterns. Some of the models currently employed in practice include intention models, individual behavioral models, and capability models, which tend to be either predictive or detective in nature [8].

Physical assets, such as cell phones and servers cannot necessarily be afforded the same protections. With these assets, once access is granted, the potential for physical damage is only limited by the physical safeguards in place. With physical security, it is assumed that the authorized party meets or exceeds trust requirements to that asset, thus negating the need for redundancy. These gaps create the opportunity for collusion or coordinated attacks [8].

While it has been shown that leveraging various types of Behavior Analytic (BA) models can be effective in identifying insider threats, many of these models tend to rely heavily on system interaction such as logging and usage patterns. Intention modeling is a derivative model used to assess potential threats by examining an insider's psychological profile. When anomalies are detected, the model examines the actor's psychological profile to establish if the action may lead to malicious activity. It must be noted that this specific type of modeling requires pre-analysis by other means in order to be effective [8].

In a collusion or coordinated attack scenario the actors may avoid triggers by leveraging the actions of others. To further complicate matters, insider threat detection is considered a temporal phenomenon. In other words, the possible variations in time and frequency add significant amounts of complexity. When dealing with more than one individual working in unison, the variables can increase significantly. To increase the chances of identifying a collusion or coordinated attack, aggerated views of resources are required. This aggregation can be accomplished by leveraging resource usage or other similar types of models [8]. Properly identifying organizational resources is an important step, which may be a challenge to small organizations. With many of these models we see a dependence on internal inputs into a system to generate data to cause a trigger event.

An overreliance on system interaction trigger events can result in outside triggers being overlooked. Outside triggers, which include things such as increases in spending and delinquent accounts, can serve to identify the potential rise of an insider threat [9]. Since not all insider threat actors may directly interact with an internal logical system, gaps begin to emerge that place both physical and logical assets at risk. Insider threat modeling does a poor job of capturing the possibility of collusion attacks [8]. For the process to be successful one must consider not only the threat actors, motivating factors and controls, but also the dynamic nature of human interaction and influence. In the following section, these factors are considered to identify the nature and direction of these trends between 2015-2018. In Section III, we consider a motivating example to begin to understand the relationships that make collusion or coordinated attacks possible. The scenario is then analyzed to identify possible areas of weakness within the insider threat modeling process for these types of attacks. Finally, in Section IV the findings are summarized along with a proposed approach to further investigate and build out a model to identify collusion and coordinated attacks.

II. Trends and Statistics

This section examines the trends and statistics regarding insider attacks. First, an examination of the frequency of such

Manuscript received February 27, 2019; revised May 1, 2019.

James B. McNicholas III and Houssain Kettani are with Dakota State University, United States (e-mail: James.McNicholas@trojans.dsu.edu, houssain.kettani@dsu.edu)

doi: 10.18178/ijssh.2019.9.2.986

attacks will be presented. The threat actor pool will then be examined. This will then be followed by an examination of motivating factors and targeted assets. Finally, we will look at noted barriers to the effectiveness of insider threat models.

A. Frequency of Attacks

Since 2014, the European Union Agency for Network and Information Security (ENISA) has consistently listed insider threats as one of the top fifteen cyber threats in its Threat Landscape (ETL) annual report [2-5]. Insider threat was ranked ninth since 2016, which is an increase from the eleventh position in 2014. Other studies specific to this topic are the annual Insider Threat Studies (ITS) which were based on a comprehensive online survey of hundreds of cybersecurity professionals, providing deep insights into the current state of insider threats and how organizations are responding to protect themselves [10-13]. Open and closed ended questions were used as to both identify and rank areas of interest. In 2018, the sample population consisted of 472 professionals within the cybersecurity community of varying seniority and from organizations ranging from less than a hundred to greater than ten thousand [10].

In 2017, as reported in [12], 51% of survey participants believed that insider attacks increased in 2017. This pattern shifted in 2018, with 27% of respondents reporting increases, 21% reporting decreases, and 46% reporting sustained levels [13]. There was 1% increase, up from 46% of the number of respondents that were not sure if their organization had experienced an insider attack. This rise could possibly be attributed to several factors. For example, it was found that 30% of organizations examined had insufficient data protection strategies or solutions. These trends continued through 2018, with 90% of respondents reporting feeling vulnerable to insider threats, which was a 16% increase over the previous year.

B. Threat Actors

In 2017 privileged users, such as managers and administrators, were found to pose the greatest insider threat. In 2018 this attitude shifted towards regular employees posing the greatest threat. Contractors, consultants, and clients were also mentioned, but ranked lower in both years [12, 13]. It should be noted that these threat actors may be a party to an event as an intentional or unintentional actor depending on the given circumstance. That last point is especially important to consider as motives are considered.

C. Motivating Factors

According to [11], some of the primary motivating factors that are promoting this trend are the monetization of sensitive data, fraud, and sabotage. Using a multiple choice and multiple answer question set 55% of respondents stated that monetization was considered the greatest motivating factor. Fraud and sabotage were reported were ranked second and third, respectively. To a lesser extent, IP theft, espionage and undetermined factors were also reported by respondents.

D. Targeted Assets

The ITS reports identified several organizational assets as being the targets of insider attacks and ranked them according to their levels of vulnerability as considered by the respondents. Table I represents these common IT assets and their vulnerability rankings per [10]-[13]. From a purely logical perspective customer data was considered to be the most vulnerable data type to insider attacks in both 2016 and 2018. It should be noted that this data was not reported in [12]. Table II represents these common data types and their vulnerability rankings per ITS since 2015.

TABLE I: VULNERABILITY RANKING OF COMMON IT ASSETS BASED ON % OF COMPANIES RANKING IT AS SUCH PER ITS

IT Assets	2018		2016		2015	
	%	Rank	%	Rank	%	Rank
Databases	50	1	57	1	57	1
File Servers	46	2	55	2	55	2
Cloud Applications	39	3	24	7	31	7
Cloud Infrastructure	36	4	19	8	-	-
Endpoints	33	5	44	4	42	4
Network	32	6	38	6	36	6
Active Directory	30	7	-	-	-	-
Business Applications	29	8	42	5	41	5
Mobile Devices	25	9	44	3	44	3

TABLE II: VULNERABILITY RANKING OF COMMON DATA TYPES BASED ON % OF COMPANIES RANKING IT AS SUCH PER ITS

Data type	2018		2016		2015	
	%	Rank	%	Rank	%	Rank
Confidential Business Information (Financials, Customer Data, Employee Data)	57	1	-	-	-	-
Privileged Account Information	52	2	-	-	-	-
Sensitive Personal Information (PII/PHI)	49	3	-	-	-	-
Intellectual Property (Trade Secrets, Research, Product Design)	32	4	54	3	54	2
Operational/ Infrastructure Data (Network Infrastructure Controls)	27	5	-	-	-	-
Employee Data (HR)	31	6	48	4	45	5
Not Sure or Other	1	7	6	8	-	-
Customer Data	-	-	63	1	57	1
Sensitive Financial Data	-	-	55	2	52	3
Company Data	-	-	48	4	46	4
Sales & Marketing Data	-	-	30	6	30	6
Healthcare Data	-	-	24	7	20	7

E. Barriers to Effectiveness

In order for any insider threat model to be effective, there needs to be buy-in and support, which can come from proper employee training and stable organizational structures as well as proper funding [9]. The current state of the industry reflects

a shifting attitude towards removing these barriers. In [13] many organizations noted decreases in vulnerability concerns, from the previous year's report, in all areas except improvements in supporting technology. It should be noted that this data was not reported in [12]. These barriers have been summarized in Table III, which shows vulnerability rankings as a result of mitigating factors per ITS since 2015.

TABLE III: VULNERABILITY RANKING AS A RESULT MITIGATING FACTORS BASED ON % OF COMPANIES RANKING IT AS SUCH PER ITS

Source	2018		2016		2015	
	%	Rank	%	Rank	%	Rank
Lack of Training & Expertise	52	1	60	1	63	1
Lack of Suitable Technology	43	2	28	6	29	5
Lack of Budget	34	3	50	2	48	2
Lack of Collaboration Between Separate Departments	34	3	48	3	40	4
Lack of Staff	22	5	35	5	23	6
Not a Priority	10	6	43	4	43	3
Not Sure \ Other	5	7	11	7	9	7

TABLE IV: MOTIVATING FACTORS AND ACCESS LEVELS OF THE POTENTIAL INSIDER THREAT ACTORS USED DURING THE ANALYSIS PHASE

Motivating Factors & Access Levels	Employee A	Employee B
Monetary Gain	-	X
Revenge	X	-
Logical	X	-
Physical	X	X
Position of Authority	X	-
Position of Trust (Company Level)	X	X

III. SCENARIO AND ANALYSIS

To illustrate the problem being proposed, the following narrative will be used to guide the analysis. This narrative is important in helping to understand the gaps identified during the review of the literature and can also serve as the foundation to begin to develop new and novel scenarios. The assets considered in this narrative include both physical and logical assets.

The company in question is a small organization that specializes in data analysis or analytics. Its offices are housed somewhere within the continental United States. All operations are conducted in one building, which houses all physical and logical assets for the organization. Physical assets include all hardware that are used to support the business such as servers, mobile devices and computers. Logical assets include all code sources, applications and databases.

Two employees are working together to target the company. The primary motivating factors are revenge and financial gain. Employee A is a manager that has privileged access to hardware and logical resources. Employee A was recently passed over for promotion. Employee B is a custodian that has access to sensitive areas including server rooms but does not have logical access to any system. For the purpose of this scenario, card-based access is considered as physical, so the logical role assignments or possible methods of exploitation will not be considered. Employee B is in heavy financial debt. Each of these factors are summarized in Table IV. Using this motivating example, the statistics presented can then be applied to attempt to determine the number of organizations that would catch a collusion or coordinated attack. To begin the analysis, we need to first look at the insider's motive.

A. Threat Actors

Motive in an investigative context is the reason or cause that leads to a malicious action [8]. Employee A was noted as being recently being passed over for promotion. Case studies demonstrate that this type of motivating factor was found to be a prominent theme in several reported insider threat attacks [14]. One notable case involved Army Specialist Ivan A. Lopez who was placed in a non-promotion status and subsequently shot and killed several fellow service members in Fort Hood, TX in 2014 [15]. Although other risk indicators were present in this case, the extreme nature of the actions of the actor serve to demonstrate possible outcomes.

Employee B's financial situation may not be a direct threat now; however, financial problems have the potential to evolve into a motivating factor [9]. There are many high-profile cases involving financial gain as a motivating factor within various sectors. One case, which demonstrates financial gain and the ability to be coerced, involved former Naval Criminal Investigative Service (NCIS) Special Agent John Beliveau who was found in 2013 to have accepted bribes in the form of cash, goods, and services for assisting suspects in avoiding criminal charges involving contract fraud [16].

B. Situational Context I

From this information it can be derived that the potential exists for Employee A to utilize their authority to influence Employee B to commit a malicious action. For example, Employee A may pay Employee B to "accidentally" damage the physical servers to which they have access. As previously mentioned, physical safeguards are a critical part to securing an originations cyber infrastructure [2]. Mitigations could include server isolation or physical (elemental damage) barriers. Clean room protocols could also be implemented to avoid the need for Employee B. Eliminating the need for Employee B does not necessarily negate the threat of collusion or coordination. Someone at some point will need physical access. To assist in the detection of a possible collusion or coordination event more advanced models, such as intention models, could be employed. This may require psychological profiling and would need to include anyone who has access to the secured area [8]. This may prove to be cost prohibitive. Another major concern with this methodology would be the possible exposure to legal liability as in [17].

C. Situational Context II

It was noted that Employee B does not have any access to logical systems within the organization. This does not mean that Employee B does not have the ability to gather and utilize user credentials. As such, a collusion or coordination scenario can be presented as follows. Employee A wants to expose company pay records to the entire organization. Employee B

agrees to participate in hopes that this information will lead to a possible pay raise. Employee A provides Employee B with information that Employee C leaves their access information on a piece of paper located within their office and that Employee C takes a lunch break at a specific time. Employee A provides Employee B with instructions on how to access the financial records and how to generate a group email. Employee B is able to locate the information and is then able to execute the plan.

Several important statistics including an increase in the number of organizations monitoring insider user behavior between 2017-2018 was noted in [18]. Only 6% of respondents reported not having some sort of monitoring mechanism in place. However, only 47% of respondents continuously monitor sensitive assets [13]. In this scenario, Employee B would be authorized as a byproduct of the scenario, so even continuous monitoring may not be enough. Compensating controls on the restriction of the distribution of this type of data would strengthen the overall security posture of this organization and should be considered. This could include data parsing and restrictions on the account in question. In a true collusion or coordinated scenario the actors may take additional actions to circumvent these types of controls bypassing the systems logical branches. When this is considered, many controls only serve as a delay.

D. Situational Context III

This scenario adds a branch to the existing motivational scenario. This is being done to demonstrate the dynamic nature of human behavior and direct threat to established models in relation to collusion or coordinated attacks. The branch modification is as follows. Employee A and Employee B are secretly seeing each other. Employee B has recently started their own business in the same sector but is leveraging the corporate veil. Employee B has been hired by Employee A in an administrative role within the new company. The motivating factor for both employees is to damage the credibility and profitability of their current company, which is now a competitor to the newly formed company.

As was demonstrated in the previous scenarios, Employee B's access is limited without either exploiting security lapses such as written passwords, by way of direct assistance, or by direct physical means such as damage. All three of these triggers can be captured by proper implementation of a set of models at both the physical and logical levels. Short circuiting a proper implementation would be difficult, but still possible. Physical workplace violence can not only be used as an indicator of a possible future attack but can also be leveraged in an exploit [9]. In the realm of cyber security, people must be considered as assets of the system [6]. An assault, whether physical or emotional, can disrupt the performance of the system. In order to cause disruption, both Employee A and Employee B have decided to target weaker members of the organization. Employee B starts by spreading derogatory information about other employees. Employee A begins to treat lesser subordinates in a way that is demoralizing. Before long productivity decreases. From an organizational perspective this may only be seen as a Human Resource (HR) problem, but this can be much more as suggested in [1].

As was previously noted, insider threat management programs are often compromised by various factors [11]. One concerning factor is the lack of collaboration between separate departments as noted in [11]. Another concern that would directly influence this scenario is a lack of training and expertise as noted in [11], [13]. Considering these statistics, the scenario could play out as follows. First, as morale goes down, complaints are likely to be generated. These reports would likely be forwarded to HR, who may or may not act. Considering the likelihood that the HR staff is not properly trained to identify a possible insider threat, appropriate actions may not be taken [11]. Even if action is taken, the behavior can continue in a different form and may still yield the negative results.

IV. Summary and Concluding Remarks

During this analysis it was shown that inside threats will continue to be a growing concern for many organizations [13]. This trend is expected to continue to increase as threats become more dynamic in nature [5, 13]. Collusion or coordinated attacks complicate the detection and mitigation process. Threat modeling can assist in the identification of potential threats; however, there is still room for error when considering collusion scenarios. As was demonstrated using the motivating example, the number of participants and the number of motivating factors may increase the likelihood of this type of attack. Even with compensation controls, the knowledge of such controls creates opportunity as noted in [19].

Based on the current statistics as noted in the previous section, insider collusion and coordinated attacks will continue to represent a major problem. While models are continuing to improve, the resources and expertise required to implement them represents a significant barrier to many organizations [8]. The abstraction of logical and physical security also poses a problem as views seem to be weighted one way or the other [1]. This analysis demonstrated that the abstraction itself is problematic in that one-sided applications tend to fail to capture branches within scenarios. It is evident from this analysis that a multifaceted approach would yield better results. Moving away from over abstracted or one-sided views of security will ensure that mitigation efforts take a holistic approach that may serve to capture many branches during collusion and coordination events.

As indicated in this paper, future research initiatives need to be dedicated towards the creation of a model that focuses on collusion and coordinated attacks. To accomplish this many of the models presented will be examined in depth. These models may be assessed not only for their application, but also their overall effectiveness using simulation and probability analysis. To test the effectiveness of any given model, the same motivating scenario framework can be applied. To strengthen the argument, previous case studied could also be leveraged with modifications that demonstrate collusion or coordinated attacks. The goal would be a model that leverages existing models in order to fully capture the events. As previously noted, the implementation of many models tends to be resource prohibitive for many

organizations [8]. As such, significant emphasis will also be placed on a model that is both easy to implement and cost effective. In addition, the model must also consider the legal and ethical implications of implementations

REFERENCES

[1] E. Cole. (2016, December 1). Insider threats and the need for fast and directed response. *SANS Threat/Vulnerabilities Analyst Papers*. [Online]. Available: https://www.sans.org/reading-room/whitepapers/threats/insider-threats-fast-directed-response-37447

[2] European Union Agency for Network and Information Security (ENISA). (2013). *ENISA Threat Landscape Report 2013: Overview of Current and Emerging Cyber-Threats*. Heraklion: ENISA. [Online]. Available: https://doi.org/10.2824/022950

[3] European Union Agency for Network and Information Security (ENISA). (2015). *ENISA Threat Landscape Report 2014: Overview of Current and Emerging Cyber-Thretas*. Heraklion: ENISA. [Online]. Available: https://doi.org/10.2824/061861

[4] European Union Agency for Network and Information Security (ENISA). (2017). *ENISA Threat Landscape Report 2016: 15 top Cyber-Threats and Trends*. Heraklion: ENISA. [Online]. Available: https//doi.org/10.2824/92184

[5] European Union Agency for Network and Information Security (ENISA). (2019). *ENISA Threat Landscape Report 2018: 15 Top Cyber-Threats and Trends*. Heraklion: ENISA. [Online]. Available: https://doi.org/10.2824/622757

[6] J. R. C. Nurse, O. Buckley, P. A. Legg, M. Goldsmith, S. Creese, G. R. T. Wright, and M. Whitty. (2014, May). Understanding insider threat: A framework for characterising attacks. *Proceedings of the 2014 IEEE Security and Privacy Workshops, San Jose, CA*, 214-228. Piscataway, NJ: Institute of Electrical and Electronic Engineers (IEEE). [Online]. Available: https://doi.org/10.1109/spw.2014.38

[7] C. Tsigkanos, L. Pasquale, C. Ghezzi, and B. Nuseibe. (2018). On the interplay between cyber and physical spaces for adaptive security. *IEEE Transactions on Dependable and Secure Computing*, [Online]. *15*(3), pp. 466–480. Available: http://doi.org/10.1109/TDSC.2016.2599880

[8] I. Gheyas and A. Abdallah. (2016). Detection and prediction of insider threats to cyber security: A systematic literature review and meta-analysis. *Big Data Analytics*. [Online]. *1*(6), pp. 1-29. Available: https://doi.org/10.1186/s41044-016-0006-0

[9] D. Ritchey. (2018, May 1). Insider threart: Why physical security still reigns. *Security*. [Online]. Available: https://www.securitymagazine.com/

[10] H. Schulze. (2015). Insider threat: Spotlight report. *Information Security Community on LinkedIn*. [Online]. Available: https://info.vectranetworks.com/insider-threat-survey-report-thankyou

[11] H. Schulze. (2016). Insider threat: Spotligh report. *Information Security Community on LinkedIn.* [Online]. Available: https://www.veriato.com/docs/default-source/whitepapers/insider-threat-report-2016.pdf

[12] H. Schulze. (2017). Threat monitoring, detection & response: 2017 report.. *Crowd Research Partners*. [Online]. Available: https://crowdresearchpartners.com/portfolio/threat-monitoring-detection-response-report/

[13] H. Schulze. (2018). Insider threat: 2018 report. *Crowd Research Partners*. [Online]. Available: https://www.veriato.com/docs/default-source/whitepapers/insider-threat-report-2018.pdf

[14] M. Keeney, E. Kowalski, D. Cappelli, A. Moore, T. Shimeall, S. Rogers. (2005). Insider threat study: Computer system sabotage in critical infrastructure sectors. *United States Secret Service and CERT Coordination Center and Carnegie Mellon Software Engineering Institute (SEI) Special Report.* Pittsburgh, PA: SEI.

[15] Center for Development of Security Excellence (CDSE). (2018, May). Awarness in Action: Case Study. *Insder Threat Job Aid*. Washington, DC:CDSE. [Online]. Available: https://www.cdse.edu/documents/cdse/case-study-ivan-lopez.pdf

[16] Center for Development of Security Excellence (CDSE). (2016, November). Awarness in action: Case study. *Insder Threat Job Aid*. Washington, DC:CDSE. [Online]. Available: https://www.cdse.edu/documents/toolkits-insider/case-study-john-beliveau.pdf

[17] L. R. Seegal and E. J. Caputo. (2006, February). When a test turns into a trial: Things to keep in mind about psycological testing. *Business Law Today*. [Online]. *15(3).* Available: http://apps.americanbar.org/buslaw/blt/2006-01-02/caputo.html

[18] E. Cole. (2017, July 31). Defending Against the Wrong Enemy: 2017 SANS Insider Threat Survey. North Bethesda, MD: SANS Technology Institute. [Online]. Available: https://www.sans.org/reading-room/whitepapers/awareness/paper/37890

[19] Consumer Financial Protection Bureau (CFPB). (2017, January 30). *Statement of Mark Bialek, Inspector General for the Board of Governors of the Federal Reserve System and the Consumer Financial Protection Bureau, on sentencing of former Federal Reserve Board employee*. Washington, DC: CFPB. [Online]. Available: https://oig.federalreserve.gov/releases/news-berthaume-sentencing-jan2017.htm

James B. Mcnicholas III received the associate's degrees in arts & humanities, arts & sciences, communication, speech communication and general studies from the College of Southern Maryland in 2006. He received his bachelor's degree in computer and information science and computer studies in 2007 from the University of Maryland University College, UMUC. He also earned the master's degrees in software engineering in 2009, business administration (2013), and digital forensics & cyber investigation (2016) also from UMUC. He is currently working on a doctorate degree in cyber operations at Dakota State University, Madison, SD. Since 2007 he has worked for the federal government as a civilian employee in information technology and is headquartered in Washington, D.C., USA. He worked as an adjunct professor at the College of Southern Maryland (CSM) in La Plata, MD, USA for two years (2015-2017) before accepting a role as an Assistant Professor and program coordinator of both the cybersecurity and computer science programs (2017-2018). During his time at CSM he redesigned the institution's cybersecurity degree program and created multiple new courses. This new degree and the associated courses were approved by the Maryland Higher Education Commission (MHEC) in 2018. In addition, he is also the CEO and founder of the cybersecurity consulting firm Kissaki Group LLC, which specializes in digital forensics investigations, incident response and training. His current research interests include digital forensics, malware analysis, reverse engineering, and threat analytics. Mr. McNicholas is a professional member of the Association for Computer Machinery and the International Association of Computer Investigative Specialist.

Houssain Kettani received the bachelor's degree in electrical and electronic engineering from Eastern Mediterranean University, Cyprus in 1998, and the master's and the doctorate degrees both in electrical engineering from the University of Wisconsin at Madison in 2000 and 2002, respectively. Dr. Kettani served as faculty member at the University of South Alabama (2002-2003), Jackson State University (2003-2007), Polytechnic University of Puerto Rico (2007-2012), Fort Hays State University (2012-2016), Florida Polytechnic University (2016-2018) and Dakota State University since 2018. Dr. Kettani has served as staff research assistant at Los Alamos National Laboratory in summer of 2000, Visiting Research Professor at Oak Ridge National Laboratory in summers of 2005 to 2011, Visiting Research Professor at the Arctic Region Supercomputing Center at the University of Alaska in summer of 2008 and Visiting Professor at the Joint Institute for Computational Sciences at the University of Tennessee at Knoxville in summer of 2010. Dr. Kettani's research interests include computational science and engineering, high performance computing algorithms, information retrieval, network traffic characterization, number theory, robust control and optimization, and Muslim population studies. He presented his research in over seventy refereed conference and journal publications and his work received over five hundred citations by researchers all over the world. He chaired over hundred international conferences throughout the world and successfully secured external funding in millions of dollars for research and education from US federal agencies such as NSF, DOE, DOD, and NRC.