Data analytics for Cyber security

-Human Centered Data Analytics for Cyber security-

Vandana P. Janeja

Outline

Human Perspective to Cybersecurity: Phishing

Human Perspective to Cybersecurity: Insider Threat

User/Employee Viewpoint

Attacker Viewpoint: Anomaly Detection Methods

Key players in a Cyber Attack

In general there are two key parties at play in a cyber attack, a user who is a victim and the attacker

In a cyber attack against a business there are three key parties in play, Business, User or employee and Attacker

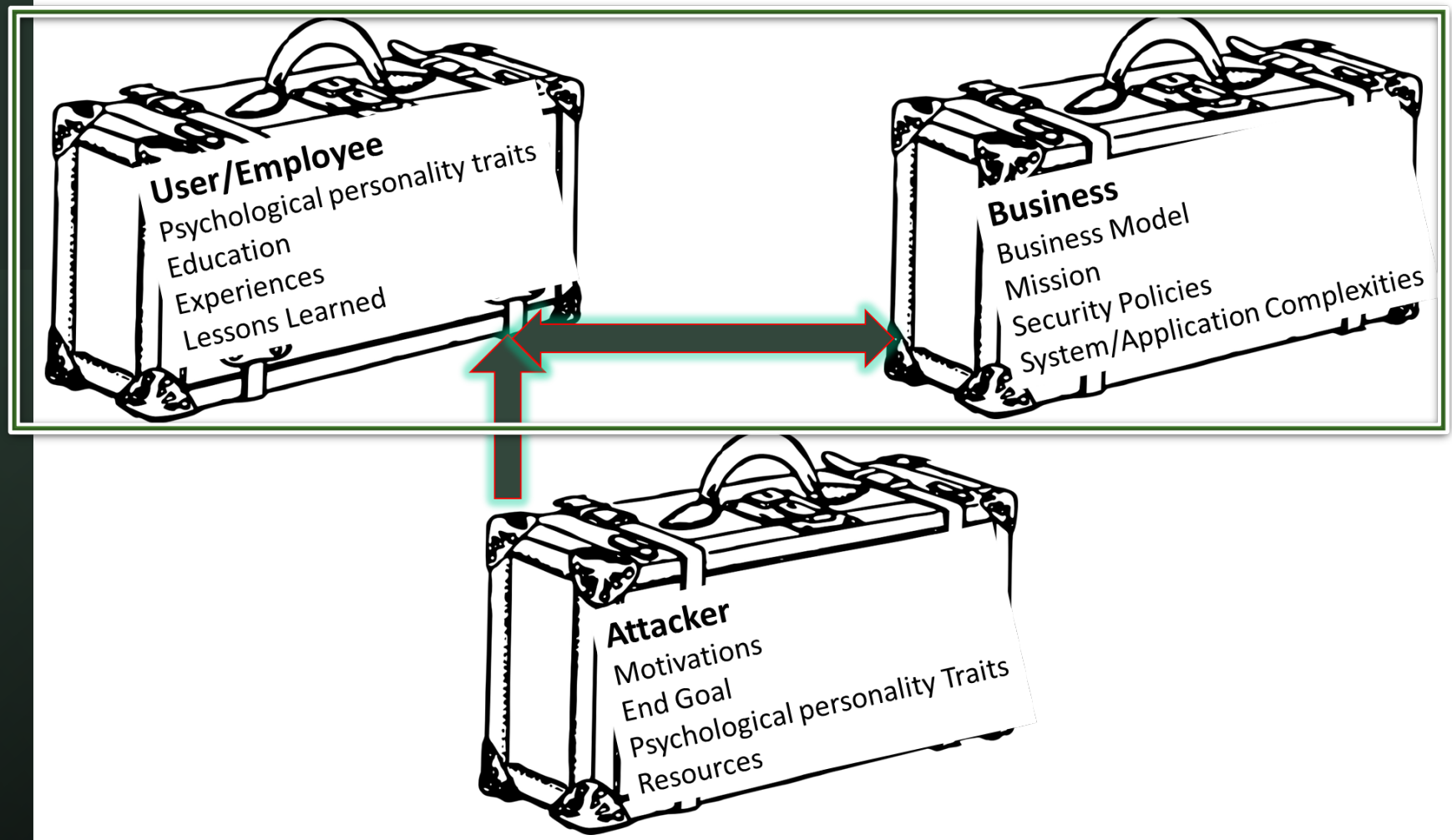
There may also be other types of employees involved such as network administrators or system administrators who are configuring the systems, programmers who are programming functionalities

- While this is a compartmentalized view of the real world fluid scenarios, it helps understand the dynamics of an attack and study ways to prevent it
- Each of these parties have a set of constraints and factors that help facilitate or restrict the perpetration of the attack.

Key players in a Cyber Attack

- A User or employee in a business comes with a certain educational background, experiences and any lessons learned in the past
- A user also has certain psychological traits which impact how they respond to certain types of requests, from clicking of links, downloading content or providing their credentials
- Businesses have to follow their business model which could be highly secure or more open
- They have a mission and a set of principles they abide by
- Business may or may not have a well-defined set of security policies
- The types of business applications being run in a business may have its own set of complexities and challenges
- In addition to technological know-how, an attacker has certain motivations and an end goal to achieve through perpetrating the attack
- An attacker may have certain psychological traits due to which these attacks may be instigated not unlike other types of crimes
- Additionally, depending on the amount of resources an attacker may have, the extent of the attack may vary from a single computer to a network or entire business being targeted
- An attacker targets a user of the business systems, be it a technology worker or an end user, utilizing the business systems

Key players in a Cyber Attack



Human Perspective to Cybersecurity: Phishing

- Spear phishing : an individual receives an email claiming to be from an organization known to the individual and is asking for the individual's username and password or interacting with the user through a malicious link in the email
- While users with knowledge of security threats, may be inclined to check the sender's email address and the validity of the link for authenticity, others may respond to the message, compromising security
- In general, cybersecurity can be aimed towards hardening our systems or taking offensive approaches: However, in this case, cybersecurity cannot simply be seen as an organization centric issue but an individual user level issue
- In social engineering type attacks, such as phishing, indeed it is an individual user who may lead to opening up an organization to bigger risks (for example by clicking on an unsafe link or providing the users credentials)
- A recent study by Trend Micro found that 91% of all targeted attacks are initiated with a spear-phishing email, potentially leading to Advanced Persistent Threats (APT)
- The human perspective is critical to evaluate and address questions such as:
  - what makes a user click on a potentially malicious link?
  - Why would a user open a malicious website or provide their credentials?
  - How do users determine whether an email appears to be fraudulent?

Evaluating User Perception: Phishing

- Evaluating behavioral factors affecting end users' ability to detect phishing, such as through survey-based methods to study users' psychological factors related to phishing detection
- Evaluating the effectiveness of a simply designed educational intervention and awareness program; The intervention can involve presentation of vignettes, carefully designed to support a diverse user group (those with or without technical background)
- Eye-tracking to determine areas of an interface where attention is focused when performing tasks where threats may be evident (e.g. when interacting online, the user may focus on the security icon on the toolbar)
- Data mining to evaluate patterns observed in the users eye gaze data and how those patterns affect phishing detection or interaction with threat prone areas on the user interface; This can include evaluating the focus of the user and associate different foci for different types of users (based on psychological profiles, background, demographics)

Human Perspective to Cybersecurity: Insider Threat

- Insider threats consist of an authorized user of a system that perpetrates an attack compromising the system's confidentiality, integrity and availability, which may include illegal copying of data, sending data to unauthorized users, providing access to unauthorized users
- Insider threat detection and masquerade detection can be categorized based on the approaches used namely: system call analysis, graph based analysis, network mapping/topology analysis, structural anomaly detection and rule based analysis
- Across the multiple areas of study there is no work which brings together multiple facets from data and behavioral perspectives for discovering insider threats.

Human Perspective to Cybersecurity: Insider Threat

- Studying how network traffic changes over time, which locations are the sources, where is it headed, how are people generating this traffic, and how do people respond physiologically (such as through stress indicators) when involved in these events, all these aspects become critical in distinguishing the normal from the abnormal in the domain of cybersecurity
- This requires shifting gears to view cybersecurity as a people problem rather than a purely technological problem
- Several features can be utilized from disparate domains such as computer usage including CPU, memory, and kernel modules, network traffic features including source, destination IP, port, protocol, derived geo-location and other location related features, such as geopolitical event information, physiological sensors providing knowledge of affective behaviors including features such as emotion and stress variations
- Each of these domains provide insights into the workings of a networked information system over a period of time. Each domain individually is not sufficient to indicate an insider threat
- When combined these disparate data streams can facilitate detection of potentially anomalous user traffic for deeper inspection
- These features can be evaluated individually and in conjunction to provide knowledge of potential insider threats

Human Perspective to Cybersecurity: Insider Threat

- Relating Multiple factors for insider threat evaluation:
- A user's systems usage changes over time, similarly network traffic evolves over time, and communication patterns change over time; These key changes which are deviant from the normal changes can be associated with anomalies in the network traffic and system usage
- Any type of attack has common underpinnings of how it is carried out, this has not changed from physical security breaches to computer security breaches; Thus, data representing the user's behavior from both the usage of the systems and affective behaviors (such as stress indicators) provide important knowledge; This knowledge can be leveraged to identify behavioral models of anomalies where patterns of misuse can be identified.
- Studying multiple types of datasets and monitoring users through the application of affective computing techniques can have ethical and privacy implications
- Effective adversarial monitoring techniques need to be developed such that they are ethical and respect user privacy.
- Utilizing data based and human behavioral aspects of learning, new knowledge from the vast array of processes can lead to new insights of understanding the challenges faced in this important domain of cybersecurity

User/Employee Viewpoint

- A cyber attack victim may be a technology savvy user or a user who is not as well versed with technology use
- While one may assume that non-technology users would be more prone to cyber attacks, technology savvy users are equally prone to attacks
- Studies have outlined personality factors and proposed a link between the personality traits and users who are likely to commit security infractions
- These could be unknowingly or through malicious intent
- For example, studies have shown that Conscientiousness and agreeableness are positively related to IT security compliant behavior
- Studies have established that individuals react differently to different scenarios and therefore the cybersecurity training approach should be adopted to differentiate between personality types
- There is also a fine grained evaluation within the personality types as well: For example, agreeable individuals with a low sense of sanction(fear of receiving a reprimand) are more likely to violate security policies
- As such there are very limited number of studies which establish the relationships between personality traits and IT security incidents where insider or an unknowing user was responsible for the perpetration of the attack.

Big Five personality factors

Human behavior and personality traits Manifesting in technological view points

- User Interaction: How a user interacts with a system is telling of their personalities and their preferences; One common example is setting passwords and saving passwords; Setting the same passwords for multiple is a big security threat and in some regards a single point of failure; Saving passwords on the system while convenient may be a security threat especially if the device is located in a somewhat non secure location

- Interface design: A very busy interface can leave average non-technical users confused; This is true for new users who may be starting to use an interface in a new job or for experienced users after a change in the systems they are used to; In some cases, it is also possible that highly technical systems with several parameters may leave users vulnerable to mistakes; Simple to use interfaces can be helpful in alleviating this.

- Where does the user look: Studies have been performed where user views are tracked to identify the level of interest a user while interacting with an interface such as a browser

- Education: A basic cyber education can be critical in averting the more common types of situations such as phishing attacks. Similarly educating users to keep their systems up to date is also very important to avert known attacks

- While these aspects are fairly simple, they need to be enumerated and carefully evaluated in an organization's context to avoid cyber-attacks which can be easily averted

Attacker Viewpoint: Anomaly Detection Methods

- A data oriented approach can be developed to understand how an attack is carried out or what the behavioral aspect of an attack is
- In cyber attacks, the intruder will first choose a target and then initiate attacks
- Before the attack is successful or failed, they will have to try multiple times and, they will continue trying different methods until they are successful or eventually give up
- This is the nature of the cyber attacks and almost universal in all attacks
- This does vary for attacks by insiders where they know the system well and do not need to scan the system and try multiple methods

Attacker Viewpoint: Anomaly Detection Methods

- Another behavioral factor in cyber attacks is that the attackers will target relatively few targets at each time, and most times, only attack one target at a time
- This provides a clue that when the attack happens, usually they will focus on one target in a short period of time
- The attackers assumed to be human will usually not spend a prolonged time on one target
- After they have tried extensively on one target in a short period of time, they will switch targets
- These behavioral factors provide hints in developing behavioral models of anomalies
- The intruders will essentially leave a trace of activities in network monitors such as in the Intrusion Detection System (IDS) logs
- IDS logs (for example SNORT alert log) can be utilized to generate behavioral models of anomalies

Models describing Attacker Behaviors

- Let us consider all the visitors N of a network, for each visitor of the network, V in N, a Source IP address, IP Source and a Target IP Address, IP Target , are displayed in the IDS log
- The alert information tells us what the actions from the source IP addresses are
- The IDS logs do not always categorize the attacks as such since they observe it in isolation
- The alerts in combination may be potentially related to identify the collective behavior of attackers
- Let us consider three user patterns and build them into three models to exhibit attacker behavior

	Model	
1	$Count\_Attempt(IP_{source}, IP_{target}, Interval(i)) \geq C$	Unique attempts between IP1 and IP2
2	$Count\_Source\_IP(IP_Target, Interval(i))$	Initiating an attack
3	$\frac{Total\_Traffic(IP_{Source}, IP_{Target}, Interval(i))}{U\_Source\_IP(i) + U\_Target\_IP(i)} \geq C$	total traffic between of Source IP in each feature in a given interval(i)

	Model	
1	$Count\_Attempt(IP_{source}, IP_{target}, Interval(i)) \geq C$	Unique attempts between IP1 and IP2

Models describing Attacker Behaviors: Model 1

- When a cyber attack happens, the attacker usually will not be successful the first time
- The attacker will attempt different methods in order to gain access to the target
- When an attack happens, it takes multiple steps: Probe, Scan, Intrusion and Goal
- Let us say each attacker is represented by a unique IP Source, and each attempt is differentiated by the alert messages
- If the time when the attack will happen is not known, then data can be divided into temporal neighborhoods as discussed in chapter 3
- This will reduce the amount of instances analyzed each time
- It also helps to show the attacks in a smaller dataset
- The count of number of unique attempts between *IP*1 and *IP*2 in a given Interval*(i)*, is greater than a threshold then this action can be considered anomalous and this Source IP address is a potential attacker
- Here C represents empirical criteria to differentiate attacks and non-attacks
- This is based on the context of a network
- If it is at a commercial network, C will be larger than in a private network
- Heuristically we can consider C as three times the average attempts of regular users
- If an *IPSource* is identified as an attacker IP address, its activities before or after the actions will be considered as part of the attack because its other incidents are likely to be in the probe or scanning stage and in preparation for the following attacks

Models describing Attacker Behaviors: Model 2

- When an attack happens, the target address usually is unique or relatively a few
- The attackers will target the unique targets persistently until success or failure
- If a target ID address is accessed by much higher number of unique IP addresses than usual within a short period of time, this target IP address is being attacked

	Model	
1	$Count\_Attempt(IP_{source}, IP_{target}, Interval(i)) \geq C$	Unique attempts between IP1 and IP2
2	$Count\_Source\_IP(IP_Target, Interval(i))$	Initiating an attack

	Model	
1	$Count\_Attempt(IP_{source}, IP_{target}, Interval(i)) \geq C$	Unique attempts between IP1 and IP2
2	$Count\_Source\_IP(IP_Target, Interval(i))$	Initiating an attack
3	$\frac{Total\_Traffic(IP_{Source}, IP_{Target}, Interval(i))}{U\_Source\_IP(i)+U\_Target\_IP(i)} \geq C$	total traffic between of Source IP in each feature in a given interval(i)

Models describing Attacker Behaviors: Model 3

- A common attack method is when there are massive attempts in a short time in order such as to obtain the password information
- Hence, if a IPTarget is experiencing much higher than normal traffic from a single or a few IPSources , this IPTarget is under attack
- This represents the percentage of total traffic between two IP addresses in a given interval (i)
- If this exceeds a threshold C, an alert can be raised
- C can be an empirical criteria to differentiate attacks and non-attacks, this can be based on experimental assessments and evaluating historic traffic patterns
- All these models are based on intuitions on how an attacker would think before attacking a network
- Other models can be developed based on psychological behavioral models such as those discussed in chapter 5 for social engineering threats

References

- Alseadoon, I., Chan, T., Foo, E., & Gonzales, N, J. (2012). Who is more susceptible to phishing emails? A Saudi Arabian study. In Proceedings of the 23rd Australasian Conference on Information Systems (pp. 1-11). ACIS.
- Anderson L. Catherine, Agarwal, Ritu. Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. September 2010. MIS Quarterly, vol. 34, No. 3, pp. 613-643.
- Ashish Garg, Shambhu Upadhyaya, and Kevin Kwiat. A user behavior monitoring and profiling scheme for masquerade detection. Handbook of Statistics: Machine Learning: Theory and Applications, 31:353, 2013.
- Chen, S., & Janeja, V. P. (2014). Human perspective to anomaly detection for cybersecurity. Journal of Intelligent Information Systems, 42(1), 133-153.
- Darwish, A.; Bataineh, E., "Eye tracking analysis of browser security indicators," Computer Systems and Industrial Informatics (ICCSII), 2012 International Conference on , vol., no., pp.1,6, 18-20 Dec. 2012
- doi: 10.1109/ICCSII.2012.6454330
- Fahmida Y. Rashid , DHS: Spear Phishing Campaign Targeted 11 Energy Sector Firms, on April 04, 2013, http://www.securityweek.com/dhs-spear-phishing-campaign-targeted-11-energy-sector-firms, Last Accessed Feb 23, 2014
- Fischer, P., Lea, S. E., & Evans, K. M. (2013). Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance. Journal of Applied Social Psychology, 43(10), 2060-2072.
- Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. (2011). Dimensions of cyber-attacks: Cultural, social, economic, and political. IEEE Technology and Society Magazine, 30(1), 28-38.
- Grazioli, S. (2004). Where did they go wrong? An analysis of the failure of knowledgeable internet consumers to detect deception over the internet. Group Decision and Negotiation, 13(2), 149-172.
- Greitzer L. Frank, Hohimer E. Ryan. Modeling Human Behavior to Anticipate Insider Attacks. Summer 2011. In Journal of Strategic Security: Strategic Security in Cyber Age. Volume 4, Number 2, Summer 2011.
- Halevi, T., Lewis, J., & Memon, N. (2013, May). A pilot study of cyber security and privacy related behavior and personality traits. In Proceedings of the 22nd international conference on World Wide Web companion (pp. 737-744). International World Wide Web Conferences Steering Committee.
- John, O. P., & Srivastava, S. (1999). The Big-Five trait taxonomy: History, measurement, and theoretical perspectives. In L. A. Pervin & O. P. John (Eds.), Handbook of personality: Theory and research (Vol. 2, pp. 102–138). New York: Guilford Press.
- Malek Ben Salem and Salvatore J Stolfo. Modeling user search behavior for masquerade detection. In International Workshop on Recent Advances in Intrusion Detection, pages 181–200. Springer, 2011.
-

References

- Malek Ben Salem, Shlomo Hershkop, and Salvatore J Stolfo. A survey of insider attack detection research. In Insider Attack and Cyber Security, pages 69–90. Springer, 2008.
- Markus Jakobsson, Alex Tsow,
- Min Wu, Robert C. Miller, and Simson L. Garfinkel. 2006. Do security toolbars actually prevent phishing attacks?. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '06), ACM, New York, NY, USA, 601-610.
- Oliver Brdiczka, Juan Liu, Bob Price, Jianqiang Shen, Akshay Patil, Richard Chow, Eugene Bart, and Nicolas Ducheneaut. Proactive insider threat detection through graph learning and psychological context. In Security and PrivacyWorkshops (SPW), 2012 IEEE Symposium on, pages 142–149. IEEE, 2012.
- Pfeiffer, T., Theuerling, H., & Kauer, M. (2013). Click Me If You Can! How do users decide whether to follow a call to action in an online message? In Human Aspects of Information Security, Privacy, and Trust (pp. 155-166). Springer Berlin Heidelberg.
- Picard, R. W. (2003). Affective computing: challenges. International Journal of Human-Computer Studies, 59(1), 55-64.
- Schlosser, A. E., White, T. B., & Lloyd, S. M. (2006). Converting web site visitors into buyers: how web site investment increases consumer trusting beliefs and online purchase intentions. Journal of Marketing, 70(2), 133-148.
- Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F., Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 373-382). ACM.
- Shropshire, J., Warkentin, M., Johnston, A., & Schmidt, M. (2006). Personality and IT security: An application of the five-factor model. AMCIS 2006 Proceedings, 415.
- Stefanie Hoffman , Cyber Attack Forces Internet Shut Down For DOE Lab, on July 8, 2011 http://www.crn.com/news/security/231001261/cyber-attack-forces-internet-shut-down-for-doe-lab.htm, Last Accessed Feb 23, 2014
- Top Federal Lab Hacked in Spear-Phishing Attack, (4/20/2011), Kim Zetter, http://www.wired.com/threatlevel/2011/04/oak-ridge-lab-hack/, Last Accessed Feb 23, 2014
- Trend Micro Incorporated, Research Paper, 2012, Spear-Phishing Email: Most Favored APT Attack Bait
- Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. Decision Support Systems, 51(3), 576-586.
- Wang, P. A. (2011). Online phishing in the eyes of online shoppers. IAENG International Journal of Computer Science, 38(4), 378-383.
- William Eberle, Jeffrey Graves, and Lawrence Holder. Insider threat detection using a graph-based approach. Journal of Applied Security Research, 6(1):32–81, 2010.
- Wright, R. T., & Marett, K. (2010). The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. Journal of Management Information Systems, 27(1), 27
- Wright, R., Chakraborty, S., Basoglu, A., & Marett, K. (2010). Where did they go right? Understanding the deception in phishing communications. Group Decision and Negotiation, 19(4), 391-416.
- Wybourne N. Martin, Austin F. Martha, Palmer C. Charles. National Cyber Security. Research and Development Challenges. Related to Economics, Physical Infrastructure and Human Behavior. 2009. I3P: Institute for Information Infrastructure Protection.
- Z. Liu, C. Wang, and S. Chen. Correlating multi-step attack and constructing attack scenarios based on attack pattern modeling. In Information Security and Assurance, 2008. ISA 2008. International Conference on, pages 214–219. IEEE, 2008.