RESEARCH STATEMENT

DR. IBRAHIM BAGGILI

My research, in general, focuses on Cyber Security. In specific, it focuses on the domain of Digital Forensics and Computer Investigations, from both the technical and non-technical perspectives. As cyber crimes become prominent in today's societies, we need to understand how they happen, why they happen, and just as important, we need to understand how to deal with cyber-criminal related incidents when they occur.

I consider myself a scholar that does not limit his research to just the technical side of cyber security and digital forensics, but one that is interested in the social and psychological aspects of these disciplines; therefore, I do consider myself a true, multidisciplinary scholar.

I would also like to point out that most of my research questions are formulated through my ties with the cyber security and digital forensics industry and practice. Through my various industry consulting efforts, and my ties with private sector and public sector organizations, I have always been able to extrapolate research questions. To this end, my research efforts have a direct impact on applied cyber security and digital forensics. After all, need is mother of invention.

I outline below my major research initiatives. I would like to point out that my interest is in applied research. I always try to put my research findings to good use. A good example of that is forensics2020, which is a company that was created based on my research in understanding digital forensic triage.

As seen from my curriculum vitae, the following topics resonate in my publications:

- Defining error rates for testing digital forensic tools
- Research Trends in Digital Forensics
- Social networking & digital evidence
- iPhone forensics, BlackBerry Forensics
- Computer activity timeline detection
- SMS authorship attribution
- Defining a standard for reporting digital evidence items
- Self-Reported Cyber Crime: Analysis of anonymity on self-reported pre-employment integrity
- Challenges for digital forensics investigations
- Survey on cloud forensics and critical criteria for cloud forensic capability: A preliminary analysis

I outline below the broader topics of research that I am interested that also encompass my prior publications in this area. Please be advised that my publications are all listed in my CV, and some may also be downloaded from my personal website: http://baggili.weebly.com.

TECHNICAL RESEARCH

Digital Forensics Process Improvement

- Digital Forensics Triage: Implementing a technical process and digital forensic tools that aid in speeding up the lawful and scientific extraction of digital evidence from computer devices. Embarking on this research initiative has led to the creation of a company (forensics2020.com), in which I have headed the development of a bleeding edge digital forensics triage tool that can aid in the timely discovery of digital evidence on a computer system. The technical ingenuity behind the product is based on a bootable USB stick that runs a patent-pending technology that is semi-automated, multi-phased, and multi-threaded.
- Digital Forensics Standardization and Best Practices: Throughout various publications, and in specific one that aimed at creating a standard XML format for digital evidence items extracted during an investigation (this research won the best paper award at the 2nd International Conference on Digital Forensics and Cyber Crime), I'm continuously trying to exert efforts towards finding ways of standardizing the process of an investigation, or formulating best practices to perform an investigation in a scientific, yet, legally sound manner, without the alteration of the digital evidence on hand.

Small Scale Digital Device Forensics

- The scientific and lawful extraction of digital evidence from small scale digital devices such as mobile phones (iPhone, Blackberry, Nokia) and, handheld gaming devices, has become critical due to the ubiquity of such devices. I have been able to work with my research team towards formalizing the process of extracting digital evidence from iPhones by parsing out iPhone backup files. Through this initiative, I was involved with the team that was first to discover that the iPhone stored GPS data on the device.

Digital Forensics: Challenges

- There are many challenges that face digital investigators such as encryption, anti-forensics and cloud computing. Part of my research agenda aims at understanding these various challenges through survey research, as well as formulating solutions to these challenges. My latest publication in this domain dealt with a survey research effort to help the community in understanding the critical criteria needed for cloud forensics with a research team at the University College Dublin (UCD). Additionally, I have two ongoing research initiatives that deal with fingerprinting anti-forensic tools and detecting them during a digital forensic investigation, as well as some more survey-based research that can help the scientific community understand the challenges that are being faced by digital forensic investigators.

NON-TECHNICAL RESEARCH

Despite my technical background, during my PhD I took a stance that people will always be the major issue in cyber security. After all, a human at the end of the day is designing cyber attacks and viruses. A human is also the one responding to the cyber-incident when it takes place. A computer does not exist in a vacuum; someone has to create it and use it. Therefore, I embarked on a journey of engaging in truly multidisciplinary research in which I was awarded the Bilsland Scholarship for my Dissertation entitled "Effects of anonymity, pre-employment integrity and anti-social behavior on self-reported cyber crime: an exploratory study".

In this research, through an experimental design, participants were randomly assigned to three groups with varying degrees of anonymity. After each treatment, participants were asked to self-report their cyber crime engagement, antisocial behavior and pre-employment integrity. The results indicated that the anonymity manipulation had a main effect on self-reported cyber crime engagement. The results also showed that there is a statistically significant positive relationship between self-reported antisocial behaviors and cyber crime engagement, and a statistically significant negative relationship between self-reported cyber crime engagement and pre-employment integrity.

I continue to pursue research in the psychological domain as I am currently working on another publication that illustrates the relationship between bypassing the internet proxy in the United Arab Emirates and cyber criminal engagement.

FORMULA FOR RESEARCH

During my experience, I have been successful at attracting several private and public sector grants, sponsorships, and gifts for the establishment of two digital forensic research laboratories. I believe the following items of critical importance for pursuing a strong research agenda:

1. Passion and motivation

   Passion and motivation for research are critical. Without the intrinsic motivation towards driving research, top-notch research won't get accomplished.

2. Collaboration with other researchers

   It is imperative to collaborate with other research groups. Not everyone is an expert on every topic, so collaboration is critical. As you can see from my publication record, I rigorously collaborate with research groups in different countries.

3. Continuous Interaction with public and private sector organizations

   It is critical in today's world, as an academic in the field of cyber security, to continuously interact with both private and public sector organizations. From the interaction with them, one gains insight into upcoming research problems that need solving. Additionally, once their trust is gained, they can be extremely helpful in providing sponsorships, gifts, and funding opportunities for research projects and conferences. In the past three years, I was able to gain the trust of organizations such as Ernst & Young, Guidance Software, AccessData and Crytpic Software just to name a few.

4. A good research team of top quality faculty and students

   Without a strong and dedicated research team, great research cannot be accomplished. It is important to establish a multidisciplinary team of students with various backgrounds to work on research problems from various angles, especially in the cyber security domain. The diversity in the backgrounds of the researchers helps paint a more complete picture of the problem as well as the solutions to the problem.

5. Involvement in conferences

   It goes without saying that research teams should be involved in various journals and conferences, not just by submitting papers to them, but by playing an active role and setting the standard for the discipline under study.

6. Dissemination of research results and media involvement

   Many academics disseminate their results in academic journals and conferences. However, not many get involved with the media. Fortunately, I have been quite extensively involved with the media with respect to digital forensics. When a paper is published in an academic journal, it is a great way of disseminating the research results to other academics, but many people and practitioners do not read these academic journals. Therefore, I believe it is imperative that scholars should be involved with the media in order to show the world what their research team is doing and how their research is driving innovation. This, in return, will gain the research program popularity, credibility, partnerships, and funding opportunities.