CSE 467 - Information Security & Ethics was a 3 credit-hour course aimed to equip Bachelor’s of Computer Science final year students with a comprehensive understanding of information security and its real-world applications. The course was divided into a total of 28 sessions, conducted over the span of five months, twice a week. For assessing students’ learning, a combination of quizzes, report assignments, presentations of researched materials, midterm and final exams (with both scenario-based questions and objective questions components), and finally a term project and symposium, were used.

Each session was designed to convey a principal concept or topic, and consisted of activities or learning material based on it. In addition, sessions were almost always followed by appropriate tasks, assignments and projects to further enhance the understanding of the concepts delivered in the session and assess the candidates’ learning. The course was designed to teach key concepts related to information security principles and practices which includes all topics related to information security planning, management, policy-making, implementation and compliance. The course also aimed to provide hands-on experience with latest and most commonly used security technologies and tools including pen-testing tools and systems like Kali Linux, DevSecOps software like Snyk and Docker Scout, intrusion detection prevention systems, encryption techniques etc.

Students began this course by learning about the history of computing, the origin of information security, and its evolution. Understanding the impact of decrypting cipher systems like Enigma dating back to World War 2, and the evolution of security threats and information security that went hand in hand with technological advancements like Colossus, ENIAC, APRANET, MULTICS etc, was crucial in showing how we currently live in the age of cyberwarfare – highlighting the importance of this field in computer science and the relevance of this course.

What goes hand in hand with security is ethics, a domain that is often overlooked and formed the other half of what this course was about. Students were introduced to major ethical theories – utilitarianism, deontology, virtue ethics – and motivated to explore the advantages and disadvantages of sticking to each of those theories, as well as come up with examples of where each of them applied to the modern-day technical world. A prime example that was explored here was recommendation algorithms and the ethical concerns surrounding the data used to power them by social media and entertainment sites like YouTube and Instagram, and this particularly brew passionate and diverse opinions from students. The focus of this activity was to critique the impact of different ethical points of views in governing acceptable usage and security policies and other aspects of tech industries today.

As comprehensive and vast of a domain information security is, it boils down to a small set of fundamentals. Students were introduced to the idea of CIA – confidentiality, integrity, and availability – which forms the core of information security. Under these three aspects, they learned more about concepts like authentication versus authorization, different types and levels of access controls, data classification and the use of encryption for maintaining confidentiality of information; hashing and auditing for maintaining information integrity; and finally the importance of failover systems, disaster recovery, SLAs and security trade-offs to make sure information is available adequately.

Perhaps the most stringent form of access controls is most characteristics of financial organizations and places where unauthorized or fraudulent access comes with incredibly high stakes (and fines, for the organization). For this reason, we invited Mr. Farhan, Head of Cybersecurity at Habib Bank. Through an engaging activity where students divided themselves into groups that represented different departments in a bank, he demonstrated the multiple different layers of security at play when doing something as simple as depositing a cheque, and the particular significance of access controls, makers and checkers, and security checklists in each of these. One new concept we were also introduced to was the importance of 6 I’s compliance in banking security legal cases as well. In addition, the session also touched upon the challenges of ensuring adherence to security in a work-from-home employees environment that came about due to the recent global pandemic.

All measures of security are futile unless we can understand the nature of the attacks it will be facing. In the next few sessions, students learned about the difference between threats, vulnerabilities, and security controls. Crucial to this was the different forms each of these can take. Threats can be controllable and addressable like human errors, but also uncontrollable and unexpected like natural disasters. Similarly, vulnerabilities can be brought on by software or network vulnerabilities like open ports, or mistakes that simply anyone is prone to making such as clicking on a phishing email if it is not filtered away automatically. In addition, students also learned of the many types of attacks and security breaches, their impacts, as well as the motivations behind them, ransomware being the most harmful attack of these all.

To understand the nature of attacks and how they have evolved over the decades, students were assigned a group project to research notorious security breaches that made headlines in the recent decades and present them as a complete report of those attacks. This activity was graced with the presence of Mr. Azmatullah who not only offered his expert critique on the presentations given by the students, but offered leading questions and encouraged them to dig deeper into their chosen accounts of attacks to develop a better appreciation for the information security field.

Keeping all these in mind, it makes sense that to counter all these harms, a diverse set of security controls must also be needed which range from technical controls like security software and systems, to physical controls like biometric doors and CCTV surveillance, to administrative controls the most of which is a full-fledged security policy. Students learned the major categories of security controls – preventive, detective and corrective – and how each of these are used in different situations. A class activity aimed at brainstorming different kinds of security controls placed in the university’s own systems was a good way for students to understand these different types of controls and uses.

All the concepts taught to the student up until this point were important to set the context of arguably the most crucial stage in information security: risk assessment. Students were made to realize the important of risk assessment in understanding the threats and vulnerabilities in any organization that expose it to attacks. In another interactive classroom brainstorming session, students were encouraged to ideate threats faced by their university systems, the specific vulnerabilities that allow for it, and the controls that can be kept in place to mitigate them. At the same time, by reverse-evaluating how a certain types of attack like DDoS, espionage, XSS, SQL injections etc can take place at an organization, students also learned the specific shortcomings in effective security systems that can be overcome to prevent them.

Building upon this concept, students were introduced to the practice of penetration testing. The difference between offensive and defensive hackers was used to illustrate how the hacking mindset can be utilized for the use of good, just as much as it can be used to exploit people with malicious intent. Pen-testing is a standard industry practice for effective risk assessment and vulnerability identification. Students were tasked with an at-home assignment to break into their newly developed student portal and identify the vulnerabilities in its system that could compromise its CIA.

After doing so, students were then introduced to the professional means of performing penetration testing. BlackArch Linux and Kali Linux were introduced as industry-level software offering several tools used specifically for pen-testing. Industry experts and ethical hackers \_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_, and \_\_\_\_\_\_\_\_\_\_\_\_, from \_\_\_\_\_\_\_\_\_\_\_\_\_\_ were invited to give a live-demonstration on how BlackArch and Kali Linux can be used to hack into the university’s internal student WiFi network, create a virus infected email that causes our laptops to shutdown, and tap into our phones to capture our audio and video. In this session, students learned introductory Linux commands, open-port analysis, SQL injections, code folding, honeypots, RCEs and virtual box scraping along the way. As a fun challenge, students were tasked with the goal to create a PDF file with a device shutdown script embedded into it.

Hand in hand with this activity, students were assigned a group project for looking beyond just Kali Linux and experimenting with other up and coming pen-testing tools being used in the industry today. While experimenting with these tools, they were challenged to penetrate and analyse the complexity of finding an opening into the notorious Damn-Vulnerable-Web-Application (DVWA). Some of these pen-testing tools included Metasploit, Hydra, Wireshark and many more.

At this point in the course, it was now time to look at information security from a broader lens. Before any organization can put an information security plan in place, it must set an information security vision for itself. This session was about organizational visioning and its importance in enabling information security solutions. Students analysed vision statements from notorious global organizations and learned the key differences between goals, objectives, and a vision. In trying to understand how a vision makes or breaks an organization, students engaged in an activity to evaluate the positive and negative aspects of SpaceX’s vision by Elon Musk, and the ethical and information security challenges associated with it. Later, students were also tasked with a small activity to develop an information security vision for NADRA, one of our own highly significant national organizations.

To tie the knot on the first half of this course, students were introduced to a relatively new practice that sought to mitigate vulnerabilities and incorporate security at grass-root levels in addition to the higher level. In a guest speaker session with Folio3’s renowned Senior Lead Cloud Engineer, Sir Obaid ur Rehman helped students learn of the fundamentals of DevSecOps. In this session, students learned of the different phases of the DevSecOps cycle, CI/CD pipelines, and different testing environment. Inside these, students learned exactly how security and security-centric practices were integrated into the basic software development cycle through processes like SAST, SBOM, security tools like Docker Scout, Sneak and PyGoat, and specialized DevSecOps software development frameworks like Jenkins-Ansible-Docker and many more. The purpose of the session was to cultivate an appreciation for how significantly prioritizing security from the beginning at each level of development helps prevent vulnerabilities and errors that could lead to disastrous results if targeted only later in the process.

The latter sections of the course focused on the new and emerging aspects of information security in the modern day world and how to implement a full-fledged information security management system on a real enterprise-level organization.

To engage students in understanding the significance of an information security program in every type of organization, students played an interactive cybersecurity game called \_\_\_\_\_\_\_\_\_\_\_. In this game, students put on the hat of the head of cybersecurity for a hospital, and used their current understanding of information security and information security practices to choose from a list of options and security measures for evolving cases in the organization, enforcing a complete information security program across the entire hospital to evade all future cyberattacks compromising its operations. If all correct security measures and decisions were made throughout the game, the hospital would successfully safeguard itself against a ransomware attack on its systems, whereas if they weren’t, the hospital’s systems would be severely compromised. Students were asked to reflect on their choices for each decision, both the options they chose and which they did not and the implications of each in the larger lens of the entire organization and final outcome. In addition, another thing that was achieved was to understand that the lack of a strong and reliable information security management system in place can sometimes really mean life or death, as in the cases of this hospital. In the same session, the importance of the key element of any effective information security program was discussed: a comprehensive security policy.

In the next session, students began by learning about asymmetric and symmetric encryption or private and public keys, as well as their uses and benefits. Building upon this, students engaged in another class activity. Divided into groups, they were tasked with the goal of creating their own cipher for a given text, making it as difficult to crack as possible. After this, the groups were asked to try to decipher other groups’ ciphered text back to its original form. At the end of their activity, each of the groups presented the steps of ciphering their own texts. This activity was a fun way to introduce students to cryptography. Students analysed their own ciphers to learn which type of encryption they fell under, learning about different types of cipher techniques like substitution, transposition, Vernam and other ciphers. In addition, they also learned of some famous, well-established ciphers like Caesar and XOR ciphers and more. Students also discussed the strength, and utility of different encryption schemes including key size, time etc. Following this discussion, students were also introduced to common encryption schemes and encryption standards used in the industry e.g. AES, HTTPS, SSL, email encryption standards like SMIME, PEM, IMAPS, and web transition and wireless connection encryption standards like SET and WEP. The session went on to explore the differences between encryption and hashing, and discuss the properties of ‘good’ hashes and their uses in maintaining integrity of systems for example in the form of digital signatures and digital certificates.

In the following session, students took a deep-dive into security policy writing. They began by learning the difference between taking an operational approach versus an analytical approach to security policy writing. By discussing the three metrics for data governance – data access, data changes and data authenticity – students learned of the ‘homework’ that needs to be done before a policy can be written. Data classification based on criticality and access control, and publicity or privacy of different forms of data interacted with throughout the organization should be known by the policy maker and clearly defined in the policy. Students learned that no policy is any good until it can be executed and enforced, and so one of the most important steps in devising a security policy is to meet with stakeholders, sponsors and enforcers to create a policy that is centred around business needs and objectives and is implementable within the organization. Students were taught that a comprehensive, active security policy is the first layer of defence against attack and goes hand in hand with standards and practices to fully protect an organization. The different types of security policies including Enterprise Information Security Policy (EISP), Issue-Specific Security Policy (ISSP) and Systems-Specific Security Policy (SysSP), along with their characteristics and use cases were also explained.

After the policy, an organization’s next layer of defence falls on its networks, systems and applications. Therefore, students were now introduced to the workings of Intrusion Detection and Prevention Systems (IDPS). An intrusion or attack into a system can be met with three types of behaviour: prevention, detection, and correction. Students were explained how different types of IDPS exist for different areas of the organization e.g. physical IDPS, network IDPS, wireless IDPS etc. Students learned that at the crudest level, IDPS function through a cycle of some sort of monitoring of an instance (e.g. by scanning, or by verifying some incoming input or data etc), detecting some anomaly, inconsistency or invalidity, alerting the IDPS of this potential threat, and then either blocking or removing the threat from the system or relaying it to an isolated decoy system for further analysis so that future similar threats can also be averted. Students were also explained how the different deployment configurations of IDPS – centralized, partially/fully distributed – also play a role in the effectiveness of its function, similarly how the location and placement of an IDPS (e.g. behind or in front of a firewall) is also very particular to allow it to perform its function appropriately.

While IDPS provide a strong layer of security for an organization, they also have their weaknesses. Through a video explanation, students took an immersive view into the journey of a network packet in an organization and the many security checks it passes, and can bypass through different techniques (for example fragmentation, traffic obfuscation and polymorphic attacks etc). This detailed demonstration helped students understand evasion techniques against network IDPS, and other IDPS.

To further solidify the concept of IDPS capability and significance in preventing attacks, students took part in an activity to analyse different types of links in a system – reporting, monitoring, response, and main network links – and how they can be coupled with network, host-based and application monitoring systems to assemble IDPS. Using these concepts, they were given a semantics diagram of an organization and asked to place all these components and appropriate IDPS in it to best secure the system.

Finally, students were tasked with a group project to develop their own full-fledged IDPS. In this project, students analysed the security needs and threats faced by any website, defined the architecture of their IDPS-secure system and orchestrated detection and response components. Students programmed their IDPS from scratch and were also required to test and present the effective of their designed technology later in the course to cybersecurity experts in the industry for evaluation, feedback and improvement.

At this point, the course took an interesting tangent to explore the emerging technology of digital twins. Complimented by a live session by PhD scholar, \_\_\_\_\_\_\_\_\_\_\_\_, from George Mason University, students learned of the inception of digital twin systems from the evolution of technology from industrial to information and now to intelligent technology, most prominently from the advent of AlphaGo. Students learned of the significant shift in the idea of ‘big laws, small data’ to ‘big data, small laws’ that came with the creation of computationally powerful systems and how this induced the idea of ‘parallel players’ which eventually became the reason why digital twins came into being. Digital twins, unlike simulations, are computational models that are used to simulate instances of physical systems to be used for analysis, predictions, and variable control. Students learned that digital twins exist as two components: a digital shadow which replicates a real environment and a digital master which computes the behaviour of real environments on the digital shadow. In doing so, digital twins can be used to represent highly complex and critical systems – like natural environments, spacecraft, stock markets etc – and these models be used in real-time monitoring and proactive maintenance that improves operations, enhanced decision-making and performance optimization for faster design and development processes, offering predictive insights allowing for better planning and risk management. The same applies to the use of digital twins in security systems. The session ended with a demonstration of model-based system engineering feats at George Mason University by the guest speaker.

A course on information security is perhaps incomplete until we discuss a realm that is the forefront of attention of security experts across the world: the dark web. Information scientist, lawyer and notable alumnus of the University of Bedfordshire Mr. Qaiser Ahmed Raja led this intriguing session on the most hidden but largest unsupervised network operating in the present world. In this session, students first learned of the different layers of the Internet; surface web, deep web and dark web. They learned of the concept of onion-routing, and the origins of the dark web as a defence project, later evolving into much more through historical turning points like Ross Ulbricht’s Silk Road and more. In an engaging discussion, Mr. Raja encouraged the students to question the larger idea of anonymity, privacy and the benefits and harms that a platform like Tor and the dark web present to the world. In more technical aspects, students learned the differences between VPNs and proxy servers, their uses in maintaining security, and how they are often mistaken for derivatives of the dark web. In addition, students also learned of the concept of Virtual Machines and gained a hands-on workshop by Software Engineer at VentureDive, Saim Saudagar, on different means of accessing (and benefiting from) the dark web through dedicated Linux distributions used worldwide by security professionals and websites like Whonix and Tor that are available for use for amateurs as well. The session concluded with a reiteration of how information can be leaked and exploited on the dark web, the harms of accessing the dark web and the precaution that must be exercised when doing so which should only be done on a need-only basis, but also how, if done accurately, the dark web can provide us with a means of the most detailed Cyber Threat Intelligence (CTI) today.

Towards the end of the course, students were now fully immersed into the domain of security enforcement. As their term project, students were required to write a complete and comprehensive security policy and develop an effective security program for the industrial sector for an organization of their choice. In proceeding sessions, students were shown how to write detailed guidelines on the topics that form part of any good security policy, which included key areas such as data protection, access controls, incident response, risk management, and employee awareness. They were also educated on the significance of compliance, security standards, best practices and security accreditation and certification from organizations such as ISO, GDPR, PCI DSS, and other notable organization their selected company may be subjected to, and how to incorporate their standards and guidelines so that their policies comply with them. Next, students learned more about incident response and disaster recovery and how security policies must detail these for any organization, as well as ensure plans beforehand that allow them to ensure business continuity in the face of security incidents of all kinds. Finally, students needed to develop an implementation plan for their proposed security measures, tailoring their security policy to their chosen organization’s unique structure and needs, in order to enforce the information security management system they had come up with. Through this project, students finally connected all the theoretical knowledge they had learned in the classroom with practical experience. They learned, first-hand, the complexities of enforcing a security plan in a real world setting and accounting for all the variables that affect its effectiveness and operation. Students conducted thorough risk assessment for a full-fledged organization. They also learned the importance of collaborating with company stakeholders to ensure a successful implementation of any security plan, and the variations of ethical standards companies must navigate through today to maintain them.

At the end of the course, an institution-level information security symposium was organized for the students where they displayed their term project security policies and implementation plans, along with their penetration testing and IDPS program projects in front of leading security experts invited as guest judges to the event. These experts evaluated the students’ projects in detail, commending the semester-long efforts of the impressive work their teams had put into their projects, the information security knowledge they had accumulated over the course, and offered them insights into how they could take the work they had come up with forward to benefit them in their professional careers in the industry. Students, instructors and guests alike praised the organization of such a platform for bridging academia and industry under the umbrella of the ever-evolving field of information security, marking the end of an incredible semester of teaching, learning and discovery at IBA.

DATES/SCHEDULE TABLE

|  |  |  |  |
| --- | --- | --- | --- |
| Session # | Date | Topic | Learning Outcomes |
| 1 | 16 Jan | History of computing and need for Security | Alan Turing, WW2, Father of computing, MULTICS, |
| 2 | 18 Jan | History of ethics | Utilitarianism, deontology, ethical theories, pros, cons, applications, virtue ethics, Facebook |
| 3 | 23 Jan | Assignment 1 | CIA, Layers of security, Farhan Saeed Khan HBL session |
| 4 | 25 Jan |  | D/f b/t threats, vulnerabilities, pen-testing, Offensive and defensive hacking |
| 5 | 1 Feb | Quiz # 1 | Intro to Linux, Kali Linux, Black Purple etc |
| 6 | 3 Feb |  | Hacking session with those guests, ASSIGNMENT: Create pdf file for virus shutdown embedded script |
| 7 | 6 Feb |  | DevSecOps session Sir Obaid |
| 8 | 8 Feb |  | Organizational Visioning, comparison with Elon Musk vision, come up with vision for NADRA, |
| 9 | 13 Feb | Quiz # 2 | Policy-making intro |
| 10 | 15 Feb | Syed Azmat ullah  Assignment 2: Security News |  |
| 11 | 20 Feb |  |  |
| 12 | 22 Feb |  |  |
| 13 | 27 Feb | Quiz # 3? |  |
| 14 | 29 Feb |  |  |
| 15 | 5 Mar |  |  |
| 16 | 19 Mar | Assignment 3: Cybersecurity Game |  |
| 17 | 21 Mar | Assignment 4: | ------ |
| 18 | 26 Mar | Assignment 5: Encryption | Critiquing, deciphering, challenging output hashes |
| 19 | 28 Mar |  | Security Policy Writing |
| 20 | 2 Apr |  |  |
| 21 | 4 Apr | Online class | Bull’s Eye model for security |
| 22 | 9 Apr |  | IDPS |
| 23 | 11 Apr | Assignment 6: Pen-testing | Video on Network IDPS |
| 24 | 16 Apr | Assignment 7: IDPS |  |
| 25 | 18 Apr | Quiz: Network IDPS |  |
| 26 | 23 Apr |  |  |
| 27 | 25 Apr |  |  |
| 28 | 30 Apr |  |  |
| 29 | 2 May | George Mason university session |  |
| 30 | 7 May | Dark web,  Qaiser Ahmed Raja |  |
| 31 | 9 May | Digital Twins,  Assignment 8: Term Project – Security Policy |  |
| 32 | 29 May | Symposium |  |