Ministry of Higher Education of Afghanistan

Technische Universität Berlin

ZiiK-Report No. 44

Conference "Information Technology for Higher Education in Afghanistan"
Part XII

18. - 20.12.2016
Kabul, Afghanistan
Ministry of Higher Education

ISSN 1619-3660

Organized by

IT department of the Ministry of Higher Education (MoHE) and

Center for international and intercultural
Communication (ZiiK)
at Technische Universität Berlin (TU Berlin)

Funding

Imprint

Edited by Dr. Nazir Peroz
Compiled by Daniel Tippmann, Ahmad Masood Latif Rai and Ghezal Ahmad Zia
Photographs: MoHE, ITCC

Technische Universität Berlin
Center for international and intercultural Communication (ZiiK)
Faculty of Electrical Engineering and Computer Science
Fraunhoferstr. 33-36, 10587 Berlin
www.tu-berlin.de/ziik

Berlin, January 2016

ISSN 1619-3660

Introduction

This conference is the twelfth in a series of conferences on Information Technology (IT) that has been taking place in Kabul, Afghanistan, on an annual basis since 2005. It is hosted by the Ministry of Higher Education (MoHE) with technical assistance from the IT Competence Center (ITCC) Afghanistan and the Center for international and intercultural Communication (ZiiK) at Technische Universität Berlin (TU Berlin), with funding from the German Federal Foreign Office and with support from the German Academic Exchange Service (DAAD).

This year's IT conference topic was "Cyber Security". The digitalization and interconnection of many areas of daily life and work is proceeding apace. At the same time, technical innovations and developments are demonstrating that the potential of information technology is far from being fully exploited yet. This technology can only be successfully implemented, if, besides functional and economical aspects, also IT security will be considered respectively. Digitalization without IT security will cause unpredictable risks and costs.

The goal of this three-day conference was to discuss aspects of IT security with representatives of the Afghan Government, authorities, universities, the Information Security Group of Afghanistan as well as international guests. On the second day, three workshops took place about the topics of **IT Education and Awareness**, **IT Security Infrastructure** and **Management of IT Security**. The results of these workshops were presented on the third day of the conference. A large part of the presentations of this year's conference was held by computer science Master's graduates who performed research about Cyber Security and who graduated from TU Berlin in October this year.

Highlight of the conference was the opening by the First Lady of the Islamic Republic of Afghanistan, H.E. Mrs. Rula Ghani. Further guests were representatives from the Afghan Ministries of Communication, Interior Affairs, Foreign Affairs, and Defense, the Ambassador of the Federal Republic of Germany in Kabul, Mr. Walter Haßmann, and numerous representatives from public and private Afghan universities, their presidents, deans of computer science faculties, heads of IT departments, and graduates of the computer science Master's program at TU Berlin. The opening of the conference was broadcast by several Afghan TV stations.

Right after the IT conference there was a presentation of IT projects from students of Afghan universities on December 21st and 22nd, 2016 on the premises of the ITCC Afghanistan. The best five of these IT projects were selected by a jury of representatives from science, politics and the industry to receive a prize.

Invited guests of the IT conference had the opportunity to visit these IT projects during the first conference day.

First day: Sunday, December 18th, 2016

Reception and Opening

Dr. Safiullah Jalalzai, spokesman of the Ministry of Higher Education welcomed all contributors and guests to the 12th conference on Information Technology for Higher Education in Afghanistan. He stated that the conference will be opened with the recitation of a few verses of the Holy Quran, followed by the national anthem of Afghanistan. In the following, Mr. Jalalzai gave the word to H.E. the Minister of Higher Education Prof. Dr. Farida Momand.

H.E. Prof. Dr. Farida Momand, Minister of Higher Education Afghanistan,

welcomed all honorable guests to the 12th IT Conference. She said to be very happy to celebrate the 12th in a series of annual IT Conferences at the Ministry of Higher Education. She expected that this conference will grow the knowledge of the academic and administration staff and define the importance of IT in all organizations. H.E. Prof. Momand confirmed that the MoHE is committed to increasing the usage of IT such as accessing information worldwide, education and training, communication, and more. IT, as she went on, can have useful impacts on good governance like reducing overload, increasing transparency, easy accessibility, storage, and generation of reports.

Reflecting on the conference topic, she stated that IT services across the country, like nation-wide email systems, the Higher Education Management Information System (HEMIS) which store sensitive data and many other services need protection against cyber-attacks and other threats.

She continued to talk about the 2nd IT strategy plan of the MoHE which is to establish and extend the IT Infrastructures like fiber optic cables and its related services with priority. In this strategy, as she pointed out, there are the following main objectives: Improvement of the IT infrastructures and maintenance, establishing of IT centers at the Afghan universities, localizing IT traffic, improving and extending AfgREN, establishing connections between the MoHE and the universities, as well as between the Ministry of Education and other related organizations.

H.E. Prof. Momand went on to explain that for the usage of IT in good governance, the following programs are to be implemented: Extension and implementation of HEMIS at the MoHE and at least eight universities, providing services via websites, increasing the bandwidth of Internet connections, creating IT policies for users, increasing employees' capacities, and increasing privacy awareness.

As further applications of IT in the academic field, H.E. Prof. Momand named the creation of secure connections for universities to international digital libraries, establishing digital libraries for Afghanistan, effective usage of AfgREN services, improvement of the education by the usage of IT, providing e-campus and e-learning services, as well as creating an IT culture.

Further activities include the establishing of IT centers at Ghazni, Khost and Kabul Education University, which are to be completed by the end of this year. Further IT centers are planned to be established by HEDP until end of 2020.

She expressed her hope to have secure infrastructures and good services at the MoHE and the Universities through the implementation of the mentioned programs, and she thanked the organizers of this year's conference about Cyber Security. Through these conferences, as she was sure, users will be aware of attacks and will be able to protect their systems.

She went on to especially thank TU Berlin, DAAD, HEDP, USWDP, MCIT, ATRA, and other related organizations for supporting the MoHE. She expressed her particular personal gratitude to Dr. Peroz for his long-standing commitment to Afghanistan and for his activities throughout the entire country by establishing IT centers, educating academic staff in MSc and PhD levels and the series of IT conferences since 2002.

H.E. Prof. Momand finished her speech by stating that she hoped the results of this conference will help to protect data and systems in Afghanistan.

H.E. Mrs. Rula Ghani, First Lady of the Islamic Republic of Afghanistan

H.E. Mrs. Ghani delivered her opening speech via video message.

H.E. Mrs. Ghani expressed her happiness to speak today to the educated young generation of Afghanistan and she thanked the students and the young generation who just came back to their homeland after completion of their studies in Germany in order to help and build up their country. Even though these students, as she continued, know about the problems of the country, they still wanted to serve and struggle for Afghanistan and be a role-model for other young people. She expressed her confidence that the new generation is able to apply their good ideas and experiences to build up this country.

H.E. Mrs. Ghani went on to thank Dr. Peroz for his efforts to educate these graduates and for his concept for the future of Afghanistan. She praised him for his great job in the area of IT.

She emphasized that Information Technology and Cyber Security are one of the major global tasks of our time. Therefore, it makes her proud that there are numerous Afghan students active in this area today. She stated that today we are living in a world of technology, which has advantages and disadvantages. Therefore, information and education in this area, as she added, is one of the major requirements of society today.

She pointed out that recently there were reports of hackers who manipulated the voting system during the presidential election in the USA and that there are increasing numbers of incidents of unauthorized access to bank accounts or personal emails, which also results in privacy infringements of the victims. She stressed that now there are information security experts in Afghanistan who are aware of such attacks and who are able to counter them and protect sensitive data. She was confident that the young educated generation in Afghanistan now is equipped with the knowledge to use the new technologies to bring Afghanistan into the 21st century.

H.E. Mrs. Ghani finished her speech by wishing all the best and much success to the brave young generation of Afghanistan and for their future careers.

Mr. Walter Haßmann, Ambassador of the Federal Republic of Germany

Mr. Haßmann began his speech by stating that in terms of information technology, he can still remember the old days of researching solely in books in libraries in order to find information. Today, however, he said he is, like everybody else, a regular user of the Internet and of information technology facilities.

Furthermore, as he continued, no organization of today could function without the new technologies, and everything is getting faster and smaller. He confirmed the subject of this conference, "Cyber Security", to be chosen very wisely, as there would also be a "dark side" to this development, too.

He stressed that IT security affects us in two ways: On the one hand, regarding the protection of our personality, thoughts and identity, and the digital secrets we have, and on the other hand, regarding the safety and security of governments, countries and nations, and their secrets. Mr. Haßmann gave the example of the accusations of data manipulations and cheatings between the USA and Russia which made the news recently. To him, this draws a frightening image.

Therefore, he suggested to stay critical on a personal level and to not digest everything which is offered digitally. Similarly, nations and governments have to protect themselves against digital crimes and data theft. However, as he added, freedom and liberty in the electronic world should not be sacrificed.

Electronic media, as he went on, offers tremendous opportunities for learning, for management, the administration, and for increasing individual knowledge and skills. He emphasized that experts in the IT field would have an enormous responsibility of walking the very fine line between chances and risks of information technologies.

Mr. Haßmann finished his speech by encouraging the audience to continue the good work in this field, given the fact that individuals, governments and whole nations are depending on IT experts. He thanked all participants for their past contributions in this area and hoped for a fruitful conference and for the development of new ideas, new ways and new technologies to protect our IT infrastructures.

Mr. Ajmal Marjan, Deputy Minister of Information Technology at the Ministry of Communications and IT, Afghanistan

Mr. Marjan began his speech by congratulating the Ministry of Higher Education for continuing the tradition of the annual national IT Conference for the past 12 years. He especially thanked Dr. Nazir Peroz for his commitment and dedication for all his efforts in the field of computer science in Afghanistan.

Mr. Marjan stated that IT is present in Afghanistan for quite some time already, as it was introduced to the country already in 1975 and 1976, when the first IT Center was established by Mr. Malikzai. Mr. Marjan used the opportunity to thank Mr. Malikzai who was present in the audience.

He continued to explain that the nation had taken a break during the civil wars which prevented it from walking step by step with other nations. Fortunately, as he went on, the nation grew together in the past 15 years and it learnt how to employ the new technology along with other nations. However, as he added, like all other things, technology has positive and negative aspects. When traditional processes are being transformed from manual to computerized systems, certain issues need to be taken care of, as it's impossible to achieve 100 % control over data in electronic form. Therefore, Mr. Marjan expressed his gratitude towards Dr. Peroz for selecting the important issue of Cyber Security as the topic of this conference.

When new technology arrives, it brings some new terminologies with it. “Cyber” is also one of those words: If we translate this word to our language, then it will lose its originality. Cyber is the space in which any object communicates with any other object in electronic form. It covers our telephonic conversations, all satellite communications, banking transactions, radar communications, electronic libraries, data of all organizations, ministries, courts, etc. Now if cyber is expanded to such a huge extent, then what do you think about its importance? How complex will it be? How important will its security be? It is very easy to secure this conference hall, as it has limited doors and windows. If you appoint guards on each entrance, then the security of this hall can be ensured. But if we consider cyber, its complex structure, its huge size, etc. then it is very difficult. The first problem is that the components along with its users are all heterogeneous. Someone is working in a bank, someone is surfing the internet, someone is posting on Facebook, someone is writing emails, someone is doing research, someone is running the government, etc. In this scenario it is very difficult to ensure security. To ensure security, all our organizations, our universities, our police, our courts, our IT companies, our telecommunication companies, our IT specialists, our students, our teachers, our security experts, etc., everyone is responsible to take part in this process of securing the cyber space. If we include all these entities in this process, only then we can develop a security concept for the cyber space and develop an organized and national agenda for cyber security.

From the political point of view, the Ministry of Communication and Information Technology is the responsible organization for ensuring cyber security. All issues are directed to this organization. But if we realize the huge size of cyber space and consider its complexity, then this issue is out of scope of one organization only. Mr. Marjan once again thanked the Ministry of Higher Education for organizing the discussion of this issue in today's conference.

Dr. Nazir Peroz, Director of the ZiiK at TU Berlin

Dr. Peroz welcomed all participants of the IT conference and expressed his thanks to the MoHE for the good cooperation, to the German Federal Foreign Office and the DAAD for the financial support, and to the German Embassy in Kabul, for the support. He remembered how, in 2013, the team of the ZiiK selected 25 young lecturers from nine Afghan universities to Berlin for participating in a computer science Master's program. Now, as he said, he is returning them with their Master's degree back to H.E. the Minister of Higher Education in order to support their universities and the society.

Dr. Peroz emphasized that since 2002, Afghanistan is on its path into the information age and has already travelled a long way. The nation, the industry and the whole society is making extensive use of modern IT. Today, IT belongs to the national infrastructure, besides roads, water and power supply, and public and professional life would hardly be possible without.

Despite this development, as he went on, the Afghan society and government is under threat of a new form of risks and dangers. Considering the global connectivity, IT security incidents can lead to dropouts and failures, even if their causes are outside Afghanistan. Attacks from hackers and criminals on IT systems are increasing, no matter if they belong to private persons or to large corporations. There are three challenges for the implementation of IT security: Hardware, software and awareness. Digital devices are increasingly used throughout society, and possibilities of remote access bear the risk of a malicious takeover of these devices. Dr. Peroz gave the example of a steering wheel of a car which could potentially be taken over by a hacker who would then be able to steer the car.

On the other hand, Dr. Peroz stated that there is no piece of software which is 100 % secure. Thus, there will always be criminal hackers who aim at finding security holes in software systems. Lastly, a certain security awareness is crucial for all users of IT. Today, as he explained, about 80 % of all IT users worldwide have too little knowledge about the consequences and impacts of security issues within the devices they use.

As this topic is relatively new to Afghanistan, it should be expected that the country is especially vulnerable to such attacks. The interior security of a nation today is inseparable from secure IT structures. Their protection is of outstanding

significance to the national security policy. Thus, a “national IT security plan” is to be developed in order to protect IT systems in Afghanistan against global attacks.

This national IT security plan has three strategic goals:

- **Prevention:** Adequate protection of IT structures
- **Intervention**: Act effectively in case of IT security incidents
- **Sustainability**: Strengthening IT security competences in Afghanistan and meeting international standards

At the end of his speech, Dr. Peroz stressed that this year’s IT conference with the topic of Cyber Security is targeting all societal, political and academic actors. Focus of this conference are topics like **IT Education and Awareness**, **IT Security Infrastructure** and **Management of IT Security**, which are going to be worked on during three workshops on the following day. The results are going to be discussed on the third conference day.

Keynotes

On the first day of the conference, in addition to the opening speeches, two keynote presentations were given on the subject of Cyber Security:

Cyber Security - introduction and overview

Mr. Christopher Nguyen, Lecturer at the Institute of Telecommunication Systems and member of the research group “IT Security” at TU Berlin

Mr. Nguyen gave an introduction to Cyber Security. The presentation highlighted that IT security is a consequence of choices that are made. This was illustrated by the example of bicycle locks: They exist in various forms, different types of locks and different advantages and disadvantages. These include various degrees of resistance against theft, but also the question of how to grant other users access to the bicycle, and no less importantly how to revoke it again.

Following that, Mr. Nguyen started a discussion on how to prevent unauthorized access to computer systems and data. A good security strategy includes measures that are effective in case of software vulnerabilities, loss or theft of equipment, social engineering and insider attacks.

In his concluding remarks, Mr. Nguyen emphasized that informed and trained staff, timely installation of security updates, and using encryption when storing data on portable equipment are simple but effective measures that can increase the IT security in an organization.

Cyber security and its challenges for Afghanistan

Mr. Ahmad Masood Latif Rai, Lecturer at the Computer Engineering and Informatics Faculty at Kabul Polytechnic University

The presentation was about the importance of Cyber Security in the current era of digitalization of information. In the first part of the presentation, Mr. Masood provided some statistics regarding the costs of Cyber Crime in the world which consisted of costs of values being hacked, recovery costs, as well as technical and human resource costs. He then presented a forecasting report of Cyber Security Ventures world-wide and provided an anticipated overview of the global population, the amount of digital content and the expected number of connected devices in 2022.

In the second part of the presentation, Mr. Masood explained the types of threats in Cyber Security and discussed different types of malicious software (malware) which are composed of adware, spyware, bots, botnets, trojan horses, viruses, logic bombs (time bombs), rootkits, worms, hoaxes and ransomware. He presented some hacking cases in 2016 which were conducted using ransomware which involved the usage of Bitcoin, stressed the importance of mobile security and compared the security threats of iOS, Android, Blackberry OS and Windows Phone.

At the third part of the presentation, Mr. Masood pointed out some current technology trends like Industry 4.0, Cloud Computing, Internet of Things, Internet of Services, Mobile Banking, E-Government, Miniaturization, etc. At the end he proposed the establishment of a National Agency of Information Security Standards which should provide standards for different concepts regarding Information Technology in Afghanistan.

Visit of the exhibition of IT projects from computer science faculties of Afghan universities at the IT Competence Center (ITCC)

After the keynote presentations, the participants of the conference were invited to visit the ITCC for the exhibition of IT projects.

The IT exhibition was opened by the Minister H.E. Prof. Momand. The exhibition consisted of current and finished IT projects by students of computer science faculties who had the chance to present them to the public during the IT Conference.

The topics of these projects ranged from the development of software for the Afghan administration, of security technologies for different applications and biometric scanning of voters during elections etc.

On December 21st, a jury of representatives from science, politics and the industry, selected the five best out of the 20 projects presented. These winners received a prize which were handed over by H.E. the First Lady Mrs. Rula Ghani on December 22nd.

The event received general acclaim and national TV stations were reporting in the evening news from both the conference and the IT exhibition. Further information about the IT exhibition can be found in attachment 2.

End of the first day

Second day: Monday, December 19th, 2016

Organization and introduction to the workshop topics

Mr. Zubair Sediqi, Acting Head of the IT-Department at the MoHE

The three workshops of the second day were introduced to the participants of the conference by Mr. Zubair Sediqi. The workshop topics were "**IT Education and Awareness"**, "**IT Security Infrastructure"** and "**Management of IT Security"**. Mr. Sediqi asked all participants to decide in which workshop they would like to participate.

Workshop: IT Education and Awareness

Moderated by: Mr. Hassan Adelyar, Dean of the Computer Science Faculty at Kabul University

Opening by: Mrs. Zohra Zekeria, Lecturer at the Computer Engineering and Informatics Faculty at Kabul Polytechnic University

---

Introduction

Mr. Hassan Adelyar, Dean of Computer Science Faculty at Kabul University, presented the schedule of the workshop to the participants. He stated there were four keynotes in the morning.

The Workshop has been opened by a presentation of Mrs. Zohra Zekeria, lecturer of the Computer Engineering and Informatics Faculty at Kabul Polytechnic University, about the topic "Current situation of IT security education and awareness in Afghanistan".

This was followed Mr. Adelyar introduced Mr. Sohail Mukhtar, lecturer of the Computer Engineering and Informatics Faculty at Kabul Polytechnic University, as the next speaker. His presentation was about "Measurements to increase IT security awareness in Afghanistan". As third presenter, Mr. Adelyar introduced Mr. Abdul Rahman Sherzad, lecturer at Computer Science Faculty of Herat University, and Ph.D. student at Technical University of Berlin. Mr Sherzad spoke about "Web application security and awareness". Last speaker of this workshop was Mr. Shakirullah Waseeb, Lecturer of the Computer Science Faculty at Nangarhar University, who spoke about the "Role of MoHE and the Afghan universities in IT security awareness and education in Afghanistan".

In the afternoon, concrete measures about the workshop topics and their implementation have been discussed. Altogether, 30 persons participated in this workshop.

Keynotes

Current situation of IT security education and awareness in Afghanistan

Mrs. Zohra Zekeria, Lecturer at the Computer Engineering and Informatics Faculty at Kabul Polytechnic University

Mrs. Zekeria began her presentation by stating that advances in information and communication technologies have revolutionized government, educational and commercial infra-structures. Recently, the Afghanistan Payment System (AFPay), which promotes financial inclusion and building a robust and modern payment system in Afghanistan, has successfully been launched. The operational stability and security of critical information infrastructure are vital for the economic security of the country. Intellectual property of individuals such as reputation, personal data, bank account details and health information can be hard to replace and are potentially dangerous if a malicious person gets access to it. To alleviate risks resulting from data leakage, it is of paramount importance to have a secure IT system. A data breach can put the reputation at risk and is a very expensive problem to solve. Weaknesses or vulnerabilities allow an attacker to perform acts of cyber crime. The vulnerabilities in IT systems are classified as technical (ex: SQL injection) and organizational (human behavior, social engineering).

The only effective way to mitigate the technical and social engineering threats is through the combination of security policies, security technology, and security awareness. Besides the security policies and technologies, it is very important to raise the awareness of the staff about IT security. Awareness programs train individuals to recognize IT security concerns and respond accordingly.

Afghanistan as a developing nation has partially implemented IT services. Both technical and non-technical staff do not have enough knowledge about security yet. However, some organizations have security professionals but the rest of the staff is not aware of security. They believe that the security of the IT system is just the responsibility of the security specialists. They are not aware that their common mistakes create big problems. For example, it is very usual in Afghanistan to use jail-breaked mobile operating systems and unauthorized applications. In offices, the computer systems are often used for personal use and relatives and friends are allowed to have access to the systems. In short, we have a cultural problem when using IT systems.

Afghanistan needs an awareness program to educate staff that security is everyone's responsibility and not just for geeks. A continued security education and awareness is required to be made part of the common culture.

Measurements to increase IT security awareness in Afghanistan

Mr. Sohail Mukhtar, Lecturer at the Computer Engineering and Informatics Faculty at Kabul Polytechnic University

In his presentation, Mr. Mukhtar described "measurements to increase IT security awareness (ITSA) in Afghanistan". He discussed objectives, importance and challenges of implementing ITSA. The behavior of employees affects information systems, which can be positive or negative. An IT security awareness program is needed to reduce unpredictable costs. Information technologies are slightly new in Afghanistan and most of the employees are uneducated about IT security issues so far.

In the following, Mr. Mukhtar offered an IT security awareness training program to extend the knowledge level of users about IT security. He also proposed a structure for an ITSA training program starting with the design, training, implementation and post-implementation of ITSA.

Web application security and awareness

Mr. Abdul Rahman Sherzad, Lecturer at the Computer Science Faculty of Herat University, and Ph.D. student at TU Berlin

Mr. Sherzad began his presentation about web application security challenges by mentioning that major security problems were only caused by a collection of smaller issues and ignorance, and only a reverse similar behavior is needed to resolve the given condition.

Secure web programming plus end users' awareness are the last line of defense against attacks targeted at the corporate systems, particularly web applications, in the era of the world-wide web. Mr. Sherzad's presentation was an introduction to web application security threats, in which he demonstrated the security problems that exist in corporate systems with a strong emphasis on secure development. Major security vulnerabilities, secure design and coding best practices when designing and developing web-based applications were covered.

The main objective of the presentation was raising awareness about the problems that might occur in web-application systems, as well as secure coding practices and principles. The presentation's aims were to build security awareness for web applications, to discuss the threat landscape and the controls users should use during the software development lifecycle, to introduce attack methods, to discuss approaches for discovering security vulnerabilities, and finally to discuss the basics of secure web development techniques and principles.

Most web application attacks occur through Cross Site Scripting (XSS), and SQL Injection. On the other hand, most web application vulnerabilities arise from weak coding with failure to properly validate users' input, and failure to properly sanitize output while displaying the data to the visitors. Literature also confirms the following web application weaknesses in 2010: 26 % improper output handling, 22 % improper input handling, and 15 % insufficient authentication, and others.
Then Mr. Sherzad talked about the vulnerabilities of client-side user's input validation, the concept and risk of phishing, Cross-Site Scripting (a.k.a. XSS) and SQL injection attacks. He clearly and practically demonstrated the risks and dangers of those attacks with real life examples. After explaining the mentioned security threats and vulnerabilities he presented the proper and standard approaches as solution to keep our web applications secure and/or mitigate the risks from those attacks and threats.
As a conclusion, Mr. Sherzad recommended the following factors as the core security principles: use least privilege, do not trust user input, apply defense in depth, turn off un-needed services, keep systems patched, watch for logic holes, hide sensitive information using encryption and access controls methods, and finally increase end users' awareness.

Role of the MoHE and the Afghan universities in IT security awareness and education in Afghanistan

Mr. Shakirullah Waseeb, Lecturer at the Computer Science Faculty at Nangarhar University

In the beginning of his presentation, Mr. Shakirullah emphasized that the Ministry of Higher Education (MoHE) and the Afghan universities play a significant role in the IT security awareness and education, because the MoHE facilitates higher education opportunities throughout Afghanistan as well as abroad. Similarly, Afghan universities present a platform for delivering higher education and, subsequently, for providing professionals to society and the marketplace. Therefore, the MoHE and the Afghan universities can play a vital role in IT security awareness and education.
Most Afghan universities have computer science faculties and therefore employ academic members who are responsible for establishing and including IT

security subjects in computer science syllabuses. These subjects should cover theoretical, practical, as well as management aspects of IT security. Therefore, Mr. Shakirullah proposed some subjects, which can be quite effective. These subjects include “IT security fundamentals”; in this subject most of the security terms and concepts can be touched, “Information Security Management”; here frameworks and standards will be studied in order to manage security risks, policies, team, contingency planning etc., “Software Security Engineering”; considering security in development and maintenance of software, “Security Lab”; a practical approach to security evaluation and mitigation. Similarly, as he went on, there are IT centers at some universities e.g. IT Center Kabul (ITCK), IT Center Nangarhar (ITCN), IT Center Herat (ITCH), IT Center Balkh (ITCB), and IT Center Qandahar (ITCQ). These centers are responsible for organizing security awareness programs for students from different faculties of the university. Likewise, there are IT teams at the universities who are responsible for designating an Information Security Officer; who will handle security related incidents and will continuously arrange security awareness training for administrative personnel.

Mr. Shakirullah suggested that the MoHE should establish a security team which is also responsible for security awareness and education. The security team members have to be provided with trainings abroad in order to bring them to an international level of IT security. Similarly, the security team is responsible for arranging seminars, workshops, and trainings to both MoHE and universities’ employees. This team should be given enough authority and support. Currently, most of the organizations are required to spend money in order to secure their infrastructures. Therefore, MoHE is accountable to allocate a budget for IT security.
Eventually, Mr. Shakirullah summarized that the MoHE and the Afghan universities are very important in raising the security awareness level throughout Afghanistan by education and training.

Discussion: Challenges, proposals and implementation

In the afternoon, all participants of this workshop discussed the issues which have been presented in the keynotes and the topic of “IT Education and Awareness”. The results of this discussion were to be presented and discussed on the third conference day.

Workshop: IT Security Infrastructure

Moderated by: Mr. Mirza Mohammad Mirza, Dean of the Computer Engineering and Informatics Faculty at Kabul Polytechnic University

Opening by: Mr. Said Jawad Saidi, Lecturer at the Computer Education and Information Technology Faculty at the Education University of Shaheed Ustad Rabani in Kabul

---

Introduction

Mr. Mirza Mohammad Mirza, Dean of the Computer Engineering and Informatics Faculty at Kabul Polytechnic University, presented the schedule of this workshop to the participants. He explained there were four keynotes in the morning.

The first presentation of the day was from Mr. Said Jawad Saidi, Lecturer of the Computer Education and Information Technology Faculty at Education University of Shaheed Ustad Rabani, about the “Current situation of IT security infrastructure in Afghanistan”. The second presentation came from Mr. Ramin Ahadi, Lecturer of the Computer Education and Information Technology Faculty at Education University of Shaheed Ustad Rabani, and was about a “Mechanism for securing IT infrastructure and services in government organizations in Afghanistan”. The following speech was from Bismillah Hossainy, Lecturer at the Computer Engineering and Informatics Faculty at Kabul Polytechnic University, about “Development of a Public Key Infrastructure for secure communication at Afghan authorities”. The last presentation was from Mr. Mohammad Mustafa Naier, Lecturer at the Computer Science Faculty at Balkh University, about “Security concepts for IT infrastructure”

In the afternoon, measures and their implementation have been discussed. Altogether, more than 30 persons participated in the workshop.

Keynotes

Current situation of IT security infrastructure in Afghanistan

Mr. Said Jawad Saidi, Lecturer at the Computer Education and Information Technology Faculty at Education University of Shaheed Ustad Rabani

Mr. Jawad enumerated some of the recent cyber attacks on Internet infrastructures to emphasize the importance of Cyber Security. According to him, the number of data breach incidents has been growing for the past 5 years. Afghanistan would be increasingly modernizing government operations and processes by implementing various projects such as E-Tazkera and E-Government. Increasing the number of online services and information, as he pointed out, widens the potential attack surface. Assessing the current status of IT infrastructure security would be a critical step towards establishing a more secure infrastructure.

He argued that measuring the security is a challenging task, because of different goals pursued by each organization as well as increasing diversity and complexity of equipment, devices, and applications. Therefore, he outlined a systematic approach to uncover the security status of the IT Infrastructure. The approach starts by categorizing the IT infrastructure. Adequate metrics are important for any measurement system, and finding appropriate metrics for each element of IT infrastructure is not a trivial task. Therefore, he suggested a threat-safeguard approach for determining the security status. This approach, as he explained, collects as many threats as possible to an item in the categorization and checks whether appropriate safeguards are applied. He finished his speech by stating that the status of the safeguards generates enough information for preparing future steps for securing IT infrastructures.

Mechanisms for securing IT infrastructure and services in government organizations in Afghanistan

Mr. Ahmad Ramin Ahadi, Lecturer at the Computer Education and Information Technology Faculty at Education University of Shaheed Ustad Rabani Kabul

In the beginning of his presentation, Mr. Ahadi pointed out that IT infrastructure comprises of physical/technical circumstances (buildings, IT centers, server rooms, cabling, protective cabinets, racks etc), IT systems (computers, servers, network devices, fax machines, mobile telephones and many more), and services (applications running inside the IT systems providing services throughout the network infrastructure) for the clients and users.

According to him, securing this infrastructure requires a high amount of facilities and mechanisms to establish sustainable business processes within the organizations. He went on to discuss issues and mechanisms related to IT security of governmental sectors in Afghanistan. Typical mechanisms which are being recommended by security standards are the following:

- Cryptography
- Authentication
- Access control lists
- Implementation of rules & policies, and
- Availability

Mr. Ahadi explained that securing IT infrastructures is a continuous process organizations should follow based on their Information Security Management System (ISMS). However, as he pointed out, whether organizations in Afghanistan maintain an ISMS or not, is a question which still needs to be investigated. In the end of his speech, he suggested that each organization asks itself the following key questions relating to IT security:

- How secure is the information technology of the organization?
- How carefully is business-relevant information handled?
- Does the organization maintain an ISMS?

Development of a Public Key Infrastructure for secure communication at Afghan authorities

Mr. Bismillah Hossainy, Lecturer at the Computer Engineering and Informatics Faculty at Kabul Polytechnic University

Mr. Hossainy began his presentation by stating that Information security has become crucial due to the evolution and widespread use of Information and Communication Technology. With a new beginning in 2002, as he went on, the IT sector in Afghanistan has also experienced a satisfactory growth. Information interchanges via electronic communications are common amongst government agencies. Similarly, the growth of IT has empowered the Afghan govern-ment to move its services online to serve the Afghan citizens better. Although the use of IT is widening in the country day by day, its security aspects have often been forgotten. For government organizations, especially security-related agencies, it is an undeniable requirement to ensure the security of their information assets. For data security, Public Key Infrastructure (PKI) is a promising technology and has become an ideal solution for securing information systems. However, PKI is not just a technical solution; it rather comprises technology, people, policies, as well as procedures.

Mr. Hossainy proposed a national Government PKI (GPKI) for establishing a secure and reliable communication environment for electronic data transmissions and an eGovernment platform in Afghanistan. This solution includes the architecture, success factors for implementation, as well as the implementation steps. The proposed solution has a hierarchical and scalable architecture to mimic the organizational structures in Afghanistan and support future growth.

Security concepts for IT infrastructure

Mr. Mohammad Mustafa Naier, Lecturer at the Computer Science Faculty at Balkh University

Mr. Naier presented a security concept for IT infrastructures in Afghanistan. He mentioned that a security concept for IT infrastructure should be comprehensive and include all aspects of the infra-structure. In order to preserve a secured infrastructure, it is to be understood as the intersection of people/organizations, technologies, processes and policies.

First, it would be important to con-vince the top management about the importance of security which enables more investment in this area. Additionally, it should be based on the organization securi-ty objective. The security domains for IT infrastructure should be defined.

He listed the following security domains as relevant for the infrastructure:

1. laws, investigation and ethics
2. physical security
3. access control (i.e. responsibilities of employees)
4. security management (i.e. policy development, policy enforcement, standards, risk analyses)
5. security architectures
6. education, trainings and awareness
7. business continuation and disaster recovery plans

The aforementioned security domains, as he finished his presentation, would enable organizations to maintain the intersection that is mentioned for a secure infrastructure.

Discussion: challenges, proposals and implementation

In the afternoon, all participants of this workshop discussed the issues which have been presented in the keynotes and the topic of “IT Security Infrastructure”. The results of this discussion were to be presented and discussed on the third conference day.

Workshop: Management of IT Security

Moderated by: Mrs. Foawziah Nasery, Dean of the Computer Science Faculty at Herat University

Opening by: Mr. Mohammad Zia Sana, Lecturer at the Computer Engineering and Informatics Faculty at Kabul Polytechnic University

---

Introduction

Mrs. Foawziah Nasery, Dean of the Computer Science Faculty at Herat University, presented the schedule of this workshop to the participants. She stated there would be four keynotes in the morning.

The first presentation was from Mr. Mohammad Zia Sana, Lecturer at the Computer Engineering and Informatics Faculty at Kabul Polytechnic University, about the "Current situation of IT security management in Afghanistan". As next speaker, Mrs. Nasery introduced Mr. Pazir Ahmad Ahmad, Lecturer at the Computer Engineering and Informatics Faculty at Kabul Polytechnic University, who spoke about "Development of IT security policies and guidelines". The next speaker of the day was Mr. Abdul Ghafar Tavakkoli, Lecturer at the Computer Science Faculty at Herat University, about "IT security and responsibility". As last presenter, Mrs. Nasery introduced Mr. Abdullah Hamidi, Lecturer at the Computer Science Faculty at Herat University, who spoke about "Securing E-government services in Afghanistan".

In the afternoon, measures and their implementation were discussed. Altogether, more than 70 persons participated in the workshop.

Keynotes

Current situation of IT security management in Afghanistan

Mr. Mohammad Zia Sana, Lecturer at the Computer Engineering and Informatics Faculty at Kabul Polytechnic University

In today's world, as Mr. Sana began his speech, where most organizations, businesses and governments are online and provide online services and on the other hand, online communication becomes a necessity, the likelihood of cyber-attacks increases. Hence, as he concluded, protecting information is necessary, and respectively, information security has become a very important field which is considered as an integral asset for most organizations. In spite of online attacks, there are attacks against computers in both business and home environments.

Cyber Security attacks, as he explained, have grown world-wide during the past several years. Accordingly, Afghanistan is also suffering from cyber crimes. Mr. Sana referenced a research which demonstrates that the aggregate misfortune resulting from cyber-crimes between 2011 and 2015 amounts to $ 28 million. The majority of these attacks, 70 %, were reported by staff members at financial organizations.

Mr. Sana complained that information security is considered a marginal topic in Afghanistan and generally broken down into a few technical safeguards like installing firewalls, antivirus software, applying strong passwords, validation of application forms, employment of guards or locking of server rooms. Even though this might secure the outer border of the organization, there still are threats from insiders because many organizations lack appropriate processes, policies and standards for protecting data throughout its lifecycle and most failed to properly train and certify employees.

Therefore, as Mr. Sana concluded, an Information Security Management System (ISMS) is a necessity and increasingly important within organizations to properly protect their information. According to him, ISMS is a systematic, structured and ongoing approach to enclose people, processes and information technology systems that protect information and systems from internal and external threats. In order to protect the information and granted the organization's information security, ISMS should be established, implemented and monitored. Eventually, he considered the top management responsible for running the ISMS as a continuous process.

Development of IT security policies and guidelines

Mr. Pazir Ahmad Ahmad, Lecturer at the Computer Engineering and Informatics Faculty at Kabul Polytechnic University

Mr. Ahmad began his presentation by stating that organizations should have four types of documents to ensure information security: information security policy, standards, procedures and guidelines. The information security policy is needed to ensure that the organization complies with the rules and regulations, and fulfill the security needs of the organization.

He explained that the information security policy is a formal document containing rules and regulations which are released by the top management in order to protect the information assets. It can be supplemented by policy guidelines which specify how to follow the policy; these guidelines are not mandatory but recommended.

Mr. Ahmad further elaborated that the policy development is a continuous process where developers, human resources, audits and other end users in the organization are involved. During the development process, as he explained at the end of his speech, the policy developers should consider the laws and regulations set by the government, as well as business objectives and all possible threat types expected at the organization. A good security policy should be brief, clear and easy to understand.

IT security and responsibility

Mr. Abdul Ghafar Tavakkoli, Lecturer at the Computer Science Faculty at Herat University

First, Mr. Tavakkoli stated that Information Technologies are developing quickly, both the number of users and use cases of the new technologies are growing, and they are becoming an indispensable part of the life of many people around the world. While IT has many benefits, using these technologies bears different risks and dangers, which also increase day by day. Cyber crimes such as trojan horses, phishing, spyware, adware, and other computer attacks are rapidly growing and evolving everyday with advancement of the new IT services.

Mr. Tavakkoli explained that almost all countries are reacting to such threats by increasing and expanding Cyber Security. This is the responsibility of the government, the private sector and individuals all together. While a collective responsibility, only governments are in the position to lead, create and supervise national Cyber Security efforts. In addition to that, the government has to increase the awareness and understanding of the importance of Cyber Security and clarify the stakeholder's roles and responsibilities.

Also, as Mr. Tavakkoli went on, the contribution of the private sector to the national Cyber Security is essential as private companies own most of the IT infrastructure in many countries. Many of the cyber attacks make use of internal computers which have been compromised because of lack of awareness of the staff. Thus, national Cyber Security must address vulnerabilities of individuals, too. An effective Cyber Security can be achieved when governments determine objectives, explain how to achieve and specify the roles and responsibilities of different parties.

Mr. Tavakkoli closed his speech by stating that cyber crimes can originate from one country and effect another country, which makes Cyber Security borderless and thus there is a need of cooperation on different levels, local, regional and international.

Securing E-government services in Afghanistan

Mr. Abdullah Hamidi, Lecturer at the Computer Science Faculty at Herat University

Mr. Hamidi began his speech by explaining that the use of information and communications technology (IT) is increasing every day. One of the recent trends of using IT in developed and developing countries is eGovernment, which refers to the use of IT by the governments to deliver online governmental services to citizens as well as the industry. Through e-government, as he further elaborated, government services are available to citizens 24/7, they are more transparent, accessible with lower costs, of higher quality, and more time-efficient. In addition, people would be able to have greater influence on governmental decision-making processes by online voting, by providing their opinions in forums or by contacting governmental organizations directly e.g. via email or contact forms.

Mr. Hamidi emphasized that one of the key challenges in providing eGovernment services is the security of information and the respective services. He stated there are many attackers in the world aiming at information stored in government database systems. Most of the online services provided by the governments are based on web applications. Therefore, attackers try to find vulnerabilities of such web applications and use various ways to access the systems. He stressed that this can result in damages like loss of information, breaches of confidentiality, and problems with availability or integrity which in turn affects the overall eGovernment's performance. As an example, Mr. Hamidi listed several threats for eGovernment services like packet sniffers, DoS attacks, SQL injection, cross-site scripting etc. which have to be known by the software developers as well as the governmental organizations. Besides, related actions have to be taken to overcome those threats and secure eGovernment services.

Therefore, as Mr. Hamidi concluded his presentation, governmental organizations have to have defined security rules and policies, defined roles and responsibilities, and have to use different security tools and applications such as cryptography, firewalls, analyzing and monitoring tools. The aim must be to find vulnerabilities and to resolve them in order to prevent attackers from accessing valuable information stored in governmental online systems.

Discussion: challenges, proposals and implementation

In the afternoon, all participants of this workshop discussed the issues which have been presented in the keynotes and the topic of “Management of IT Security”. The results of this discussion were to be presented and discussed on the third conference day.

End of the Second day

Third day: Tuesday, December 20th, 2016

Moderation: Prof. Osman Babury, Deputy Minister of Higher Education,
Dr. Nazir Peroz, Head of ZiiK at TU Berlin

First, Prof. Babury welcomed all participants to the third conference day and wished all a successful day. Dr. Peroz briefly presented the schedule of this day and stated that the aim of the last conference day was to discuss the results of the three workshops.

The results of the workshop **"IT Education and Awareness"** were presented by Mr. Mohibullah Amin Wardak, Kabul University, of the workshop "**IT Security Infrastructure**" by Mr. Rafiullah Momand, Kabul University, and of the workshop "**IT Security Management**" by Mrs. Mursal Dawodi, Kabul University.

Results of the Workshop: IT Education and Awareness

Mr. Wardak summarized the results of the workshop "IT Educa-tion and Awareness". After the key-note presentations, the workshop participants discussed the following topics and proposed possible solutions:

Means to deliver the necessary IT security skills and awareness

As a result of the discussion, the following means for delivering IT security awareness were proposed:

- Training programs and courses
- Seminars and conferences
- Journals (It will help the staff who is unable to attend courses and conferences)
- Bulletin boards
- Posters
- Media coverage
- Daily news websites

Approach for deploying an IT security awareness program at the MoHE

Proposed approach:

- Define domain and scope
  - Who is the target group?
- Define goals
  - What is expected from the staff regarding IT security awareness?
- Selecting awareness topics
  - Web usage, social engineering, mobile device security issues, allowed software on organization systems, access control issues, and many more

Methods for evaluating an IT security awareness program at the MoHE

Proposed methods:

- Written test
- Interview
- Questionnaire
- Survey
- White Hacking (send a test link, and wait for user to click it)
- Online platform for self evaluation

Including IT security subjects in the Bachelor's program of computer science faculties

Proposed subjects:

- Computer Code of Ethics
- Information Security Management
- Security Lab (vulnerabilities exploitation)
- Network Security (network specialization)
- Software Security (software engineering specialization)

Results of the Workshop: IT Security Infrastructure

The summary of the workshop "IT Security Infrastructure" was presented by Mr. Momand. The summary included the conclusion of the workshop's presentations and the results of the discussions.

All workshop participants agreed that in order to improve the current situation of the IT security infrastructure of Afghanistan, first an analysis of the current situation needs to be performed to identify problems and vulnerabilities. On the basis of the results of this analysis, a security team can develop security policies with the help of international standards and recommendations. The discussion also focused on the risks, different threats and problems of IT security.

After the discussion, the following possible solutions were proposed:

- Securing IT buildings
- Obtaining secure hardware and network equipment
- Secure configuration of routers, switches and firewalls
- Enforcing security standards for applied software
- Defining responsibilities
- Establishing a national IT security response team

Further questions from the audience were:

- Does the use of IT make our daily activities easier or more difficult? Especially considering the security?
- Do we need a security team or IT specialist for the security of IT systems?
- How to convince the top management to provide a budget and to support the implementation of security policies and mechanisms?

During the following, these questions were discussed.

It was concluded, that IT makes daily activities easy, there are e.g. barcode cards for students' attendance, and students can be found and managed easily throughout the university.

It was argued that if there is an IT specialist in an organization, it might be sufficient, and no security team would be required in the organization. This was responded by the argument that a security team or department is required, and it should take responsibility for such issues. Furthermore it was added that if an ISMS exists, it just needs to be adopted. However, the problem remains that there is no security officer in the organizations. Therefore, internal IT problems should be first solved and then an ISMS department should be created which takes responsibility of the security of the network and the policy.

There are various methods and techniques to convince the top management. It can be invited to security awareness programs or be given a security related presentation to convince it of the importance of IT security within organizations. In particular, the audience made the following suggestions:

- The government of Afghanistan has to have a dedicated budget for IT security
- Conducting conferences and presentations can convince the government to strongly consider IT security
- The lecturers of computer science and IT centers have to start IT security programs at each university
- All IT centers and IT resources have to be updated frequently for security purposes
- Top-level management has to help security teams
- The government of Afghanistan has to recruit eligible and expert people for the IT security
- The government of Afghanistan has to establish an IT security institution
- The government of Afghanistan has to establish IT security team in each governmental organization
- The government of Afghanistan has to create security policies for both logical and physical security
- The government of Afghanistan has to develop its own national IT security strategy plan.
- IT security subject has to be included in curricula
- In every office and administration the security requirements are different. First, there should be an analysis to identify vulnerabilities, and after that the respective security measures have to be suggested.

Results of the Workshop: IT Security Management

The summary of the work-shop "IT Security Manage-ment" was presented by Mrs. Dawodi, Lecturer at the Computer Engineering and Informatics Faculty of Kabul Polytechnic University. It included the conclusions of the workshop keynote presentations and the results of the discussions.

Before the discussions, the workshop participants were asked the questions via a questionnaire. They had 10 minutes to answer them and were divided into groups. After 10 minutes the questionnaires were collected. The questionnaire consisted of the following five questions:

- Why do we need a security policy?
- How to motivate end users to know and follow policy rules?
- Assume a governmental organization that has implemented and developed firewalls, anti-virus software and other safeguards. How can it still be vulnerable to some attacks? How to fix this issue to prevent attacks?
- An employee leaves the organization, but some sensitive data is still on his personal laptop. Who is responsible?
- Why is an information security concept a continuous process?

The groups were working to find answers to these questions, and came to the following conclusion: An IT security policy is required for a sustainable operation of IT infrastructure and for the protection of sensitive and personal data. Respective measures to increase IT security awareness are required in order to make end users understand the requirements and to act accordingly.

In order to provide a comprehensive protection against attacks, a number of measures are required. IT security needs to be understood as a process which needs to be permanently enforced, audited and updated. Furthermore, all involved staff members need to be qualified respectively. An emergency response plan needs to be developed to organize counter-measures in case of an actual attack.

For the lifecycle management of IT equipment, well-defined procedures need to be in place. Before an employee leaves the organization, his private equipment has to be wiped from sensitive data respectively.

IT structures change permanently, and so do IT security requirements. Therefore, a centralized organization needs to coordinate and supervise the implementation of the IT security strategy plan.

Discussion of the results

After the presentation of the workshop results, all participants agreed that information technology and the Internet today are important tools for all organizations and have to be protected respectively. Therefore, IT security should be made part of the curricula of all faculties of computer science. Some of the university's and authority's members reported about their poor IT security situation.

At most organizations, responsibilities are not clearly defined and there are no binding regulations:

- IT experts are missing for issues of IT security and for specific tasks (e.g. planning, acquisition, employment, support) for a sustainable implementation of IT systems
- Qualified personnel for PC workspaces and basic support is often missing
- Work processes are poorly coordinated.
- Analyses about the day-to-day operation are not being performed
- There are often contradictory interests within the organizations which are not compatible with each other.
- There is no central certification authority for the security of the infrastructure, IT systems, the network and for applications.

All participants agreed that the availability and security of IT systems is to be guarateed and coordinated, which is the task of the government. It was added that it is not only about employing IT within the organizations, but to make IT reliable, available and secure throughout the country. Afghanistan has to develop a national IT strategy plan which defines the framework for the development, employment and management of IT structures. Also, the scope and direction of further activities is to be determined in order to reach long-term goals. Therefore, the following measures are to be implemented:

- Evaluation of the current state of development of the organizations and their resources and skills of the staff
- Determination of gaps between the current IT situation and the defined goals
- Development of a common understanding of
    - how and for which purpose new technologies can provide important contributions for the improvement of processes within the organizations
    - which strategic and operative security measures are currently present and which should be implemented
- Definition of pragmatic and realistic goals which can be reached in a given time-frame and with the available resources
- Definition of clear responsibilities and rules at the organizations
- Development of IT laws and regulations

Furthermore, education and trainings is to be provided for all IT end users in order to increase skills and awareness of IT security related matters. Private universities are to be included in this concept.

In the end Dr. Peroz thanked H.E. Mrs. Rula Ghani, the First Lady of the Islamic Republic of Afghanistan for her opening of the conference. Furthermore he thanked H.E. Prof. Farida Momand, Minister of Higher Education, as well as the presidents of the participating universities for their support. He also thanked the German Federal Foreign Office, the German Embassy in Kabul and the DAAD for their support and funding of the conference. He expressed his gratitude towards to the computer science Master's graduates from TU Berlin, the members of the IT Department of the MoHE and of the IT Competence Center and the team of the ZiiK of TU Berlin for the organization of the conference. At last, the president of Kunar University, Prof. Mir Ahmad Hamed, closed the conference with a prayer.

End of the third day and of the 12. IT Conference

Attachment 1

Conference Pictures: First day

Conference Pictures: Second day








Conference Pictures: Third day







در تحصیلات عالی

Attachment 2

IT Competence Center of Afghanistan
1st IT Projects Exhibition
Experience the digital future today in Afghanistan

The ITCC Afghanistan, in cooperation with the Ministry of Higher Education, various Afghan universities and the Center for international and intercultural Communication (ZiiK) of Technische Universität Berlin (TU Berlin), with funding from the German Federal Foreign Office and with support from the German Academic Exchange Service (DAAD), was organizing an IT projects exhibition on December 21st and 22nd 2016.

This exhibition took place within the scope of the 12th IT Conference in Kabul from December 18th until 20th where students of computer science faculties of various Afghan universities presented innovative IT projects they had developed during their studies.

Altogether, 30 IT projects had been nominated by the universities, 20 of which were selected for the IT exhibition by a professional technical team. After a brief presentation of these projects on December 21st, the best five were selected by the jury of representatives from politics, science and the industry. These five winners received a prize on December 22nd.

Sponsors of these prizes were the German Embassy in Kabul, the experts group „Computer Science and social development“ of the German Computer Science Society, and the ZiiK of TU Berlin.

The topics of the IT projects were divided in three categories:

- Software Application
- Network & Security
- Hardware Application

Members of the jury were:

Prof. Seddiqi, Deputy Minister of Higher Education, Dr. Fayez, Former Minister of Higher Education, Dr. Peroz, Head of the ZiiK at TU Berlin, Mr. Zia, CEO of Pashtany Bank, Mrs. Karokhi, Member of the Afghan Parliament, Mr. Rasuli, Head of Kankor at the MoHE, Prof. Mirza, Dean of the Computer Engineering and Informatics Faculty at Kabul Polytechnic University, Prof. Adelyar, Dean of the Computer Science Faculty of Kabul University, Mrs. Naseri, Dean of the Computer Science Faculty of Herat University, and Mr. Momand, Dean of the Computer Science Faculty of Nangarhar University.

The following projects had been presented:

1. Solar Water Pump, Kabul Polytechnic University
2. Car Tracking System, Nangarhar University
3. Security Awareness, Herat University
4. Network MIS (LibreNMS), Kabul Polytechnic University
5. Snort IDS, Kabul Polytechnic University
6. IPCop, Kabul Polytechnic University
7. GUI for Linux Administrators, Herat University
8. Academic MIS, Kabul University

9. Private University MIS, Kabul University
10. Kankorian, Kabul Polytechnic University
11. Archive MIS, Kabul University
12. Kankor MIS, Kabul Polytechnic University
13. Student MIS, Kabul University
14. Driving License Digitalizing, Qandahar University
15. Transcript & Diploma MIS, Nangarhar University
16. Human Resource MIS Kabul University
17. Learning Management Systems, Kabul University
18. Hospital MIS, Kabul Polytechnic University
19. Plagiarism Detection, Qandahar University
20. E-Election, Kabul Polytechnic University

Award Ceremony

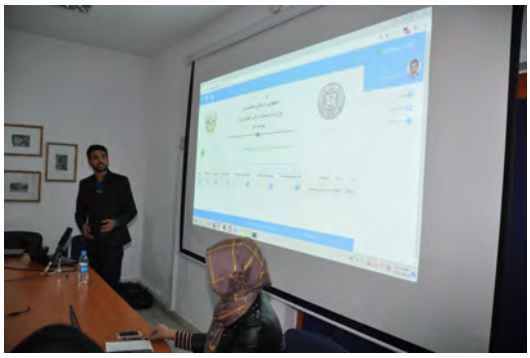
On December 22nd, the prizes were awarded to the five winner students within the scope of a ceremony. This event was moderated by Mr. Abdul Azim Noorbakhsh, spokesman of the ITCC. After the welcoming of all guests by Dr. Peroz, the ceremony was opened by H.E. the First Lady, Mrs. Rula Ghani, and H.E. Prof. Farida Momand, Minister of Higher Education.

H.E. Mrs. Rula Ghani, H.E. Prof. Momand, and Dr. Peroz awarded the prizes to the five winners. The other 15 participants of the exhibition received a certificate.

At the end of the event, H.E. Mrs. Ghani visited the IT projects of the students and thanked the teams of the ITCC and the MoHE for the organization of this exhibition. She expressed her gratitude for the commitment of the students and wished them all the best for their future careers in Afghanistan.

The pictures of the following three pages document the IT exhibition:

IT Projects Exhibition: December 21st 2016



IT Projects Exhibition: December 22nd 2016

IT Projects Exhibition: December 22nd 2016