Security Aspects of Remote E-Laboratories

http://dx.doi.org/10.3991/ijoe.v9i3.2586

M. Krbeček[1], F.Schauer[1,2] and R. Jašek[1]
[1] Tomas Bata University in Zlín, Zlín, Czech Republic
[2] University of Trnava, Trnava, Slovak Republic

***Abstract*—The paper is focussed on remote, sometimes denoted by e-laboratories and their security. In the introduction the basic features, working principles and state of the art of this new ICT teaching tool are described. The main topic of the paper is a new and emerging issue of the safety and security of e-laboratories, whose safety measures are often inadequate. For easy-to-follow purposes e-laboratories are divided into three working groups according to their complexity. The analysis of potential risks that may occur in both hardware and software side are presented and possible precautions to eliminate these risks are given. As an example the measures, taken in our e-laboratories (in Prague http://www.ises.info, Zlin and Trnava http://kf.truni.sk/remotelab) are mentioned.**

***Index Terms*—Remote experiments, remote laboratories, security of remote experiments.**

I. REMOTE LABORATORIES – STATE OF THE ART

The contemporary society is characterized by growing virtualization and sharing of resources and assets through the Internet. This approach saves the cost of expensive shared devices, available through the network. This trend can be found in a wide range of sectors of human activities in general and in teaching process in particular. Teaching of natural sciences is no exception. A great deal of attention worldwide has been devoted to e-laboratories offering access to various real world remote experiments (REs) [1-4]. The ultimate goals in forming teaching support for a teacher are grids of remote laboratories and their integration into a cloud-system with an easy data processing and storing.

Only recently has emerged a serious problem stemming from security aspects of e-laboratories. As the chain is always as strong as its weakest link, it is necessary to start from the security of basic constituent of the system and we will describe the security precautions of the remote experiment (RE) itself. The RE is actually a real experiment running in a real laboratory by using real instruments and equipment. It can be controlled by a teacher, student or any other user from his/her computer through the Internet on the general controlling scheme of server-client. Controlling of the experiments is enabled via Web interface, by means of which the user can perform the appropriate settings, options, and starting or stopping the experiment. The measured data from the experiment are transferred across the Internet and presented through the web interface to the client. Web page may include the option to export data directly into one of the spreadsheets editor (most often Microsoft Excel) for easy processing. Most of the experiments include the Web camera that allows monitoring the ongoing experiment in real time and/or communication with the instructor. Schematic arrangement of the remote experiment is shown in Figure 1.

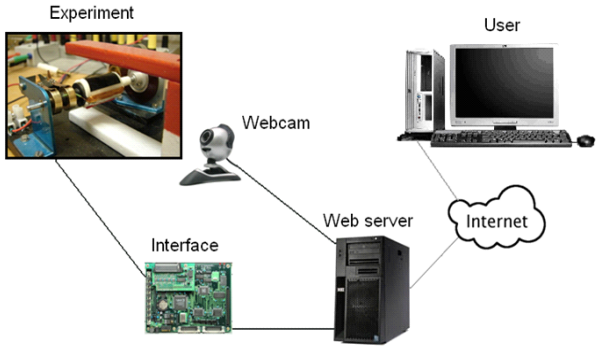

Figure 1. Schematical arrangement of the remote experiment

Such experiments are mainly designed under the auspices of the universities for the purpose of teaching. For this reason usage of some of them is only for students of the university in question and access is secured by the user name and password (especially at American universities). In Europe and Australia several projects exist supporting building of open remote laboratories - with free access, either with or without registration. Some labs offer to insert client´s initials (name, country, e-mail) for voluntary statistical purposes. With necessary exceptions (maintenance, modification, technical issues...) experiments are accessible 24 hours a day, seven days a week [5-6].

REs can be divided according to many criteria. One of them is their sophistication and complexity of physical hardware they use. From this viewpoint, experiments can be divided into three categories as the security hazards:

a) *Basic REs*, which do not use complex devices and are used for logging the data from detecting probe and/or for retrieving stored data from the experiment. The clients cannot interact with the experiment (in some cases, he/she can only start or stop the data logging) or affect it in any way. In this case one-way data transfer takes place from physical hardware to the client. Classical representatives of this category are weather stations giving the client the access to the logged data (the temperature, pressure, sunlight intensity or radioactive background). (See Czech laboratory www.ises.info and their environment monitoring at http://kdt-16.karlov.mff.cuni.cz/en/mereni.html or Slovak laboratory http://remotelab1.truni.sk).

b) *Complex REs:* These REs require two-way communication between a client and the server. The user sends control commands to the server and receives the confirming of the request and measured data. As an example we can give the Electrochemical cell characterization experiment, where the user can control the electrolyte volume

and concentration in the electrochemical cell (see: http://remotelab2.truni.sk).

c) The last category of REs are *scientific experiments*, very often based on a commercial apparatus controlled by the authoring SW, delivered by the producer, and used for the remote controlling. Additional services provided by sophisticated experiments are their cooperative features; instruments sharing and their use reserving. Especially these REs are susceptible to many hazards and damages. Instrumentation is usually based on expensive equipment susceptible to damage and strict rules of exploitation for the control of experiment have to be observed and REs have to be secured against all possible breaching of these rules of instrument exploitation. Controlling of astronomical telescope may be an example of this category (see: http://my.telescope.org/index.php).

It is worth mentioning that unreliable or malfunctioning RE may cause the ill "psychological" effect, especially on newcomers in the field, about the usefulness of this new and prospective teaching and scientific tool [4].

In the light of the maturity of e-laboratories and their importance, it is surprising how a little attention has been devoted to the security risks of REs and e-laboratories. We want to contribute to this acute field by this paper and describe the risks of security to remote laboratories in general and our first experience with security in our remote laboratories.

II. THE GENERAL SECURITY RISKS OF REMOTE EXPERIMENTS

Let us discuss first the general aspects of security that applies to all REs. These aspects can be divided according to the different constituent parts of a RE depicted in Figure 2. RE always consists of the physical hardware, informatics hardware and informatics software. Let's now look at the security risks of these individual parts of the RE. To these risks we add aspect of the environment that can affect the experiment and cannot be easily eliminated.

Physical and Informatics hardware security aspect: As the name suggests, this category includes deliberate damage of the physical hardware of the experiment. This aspect is in the most cases given by situating the experiment in a building and a locked room. Adequate and regular inspection and maintenance of the RE equipment is a stringent and often underestimated condition for the running of the e-laboratory. The REs hardware can also be damaged through the fault or mishandling by the client controlling the RE. All these circumstances should have been attended to in the controlling RE program.

Informatics (RE) software security aspect: This is an attack to the experiment via informatics software mostly across the Internet. This aspect will be described later.

Security aspect due to environment: This category includes failure of the power supply (power outages, voltage spikes and surges). The security level of this aspect is of course dependent on the cost of the experiment. Surge protection and circuit breakers are usually adequate security for simple experiments. But the experiments using expensive measuring devices require a comprehensive security via UPS sources.

A. Software risks of remote laboratories

The main problem of the REs is the remote access from anywhere via the Internet. To make this thing feasible the

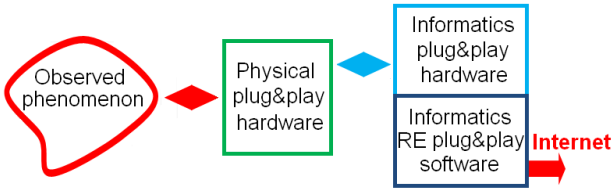

Figure 2. Schematical representation of the remote experiment [8]

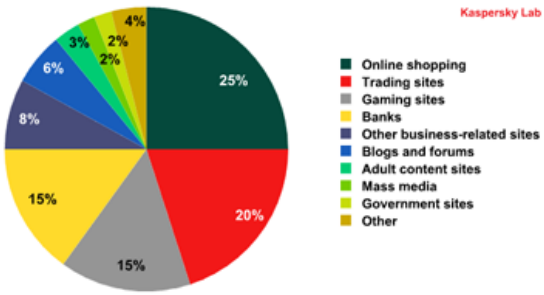

Figure 3. Breakdown of attacked sites by areas of activity – the second half of 2011[9]

server, on which the experiment runs, must have a public IP address. With this requirement comes a whole range of security risks. Public IP address allows finding and attempting to connect to the server to potential unauthorized attackers. The attacks on the servers are not an infrequent phenomenon on the Internet. There are many different types of attacks which threaten the functionality of web servers. Recently we have encountered the so-called DDoS type of the most powerful attack in the media. Report of Kaspersky Lab brings the statistics of the targets of DDoS attacks in the second half of 2011[9] (Fig. 3). We can see the most attacks were directed at commercial sites such as online stores (25%) and trading sites (20%). Actually the attacks on the RE were in 2011 not an acute problem , but it may easily aggravate when remote laboratories become a wide spread tool of experimentation at schools and universities. Figure 4 shows the most used types of DDoS attacks.

Next, we will describe typical representatives and functionality of DDoS attacks and few other basic types of attacks one might encounter. To the most often encountered and obvious security risk belong:

Attempt to connect using RDP, WMI, and FTP. Access to the server allows direct possibility to control of the experiment lading to the damage of the experiment.

Denial-of-service attack - (DoS attack) is an attempt to make a computer or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person, or multiple people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. [10]

Distributed Denial of Service - refers to a variant of DoS attacks where attacks not come only from one computer, but from a large number of parallel channels. It means that there are tens, hundreds and even thousands of stations which are involved into attack. Owners of these computers do not know about involving theirs computer into attack. It is possible because of malicious software (called zombies), which are installed on their systems.

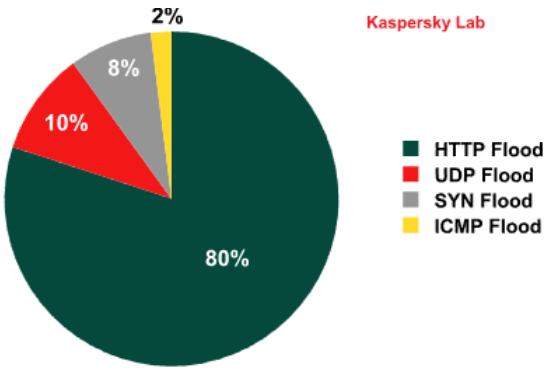

Figure 4. Types of DDoS attacks – the second half of 2011[14]

ICMP flood - Ping of death - (abbreviated "POD") is a type of attack on a computer that involves sending a malformed or otherwise malicious ping to a computer. A ping is normally 32 bytes in size (or 84 bytes when the Internet Protocol (IP) header is considered); historically, many computer systems could not handle a ping packet larger than the maximum IPv4 packet size, which is 65,535 bytes. Sending a ping of this size could crash the target computer.[11]

ICMP flood - Smurf attack - is one particular variant of a flooding DoS attack on the public Internet. It relies on misconfigured network devices that allow packets to be sent to all computer hosts on a particular network via the broadcast address of the network, rather than a specific machine. The network then serves as a smurf amplifier. In such an attack, the perpetrators will send large numbers of IP packets with the source address faked to appear to be the address of the victim. The network's bandwidth is quickly used up, preventing legitimate packets from getting through to their destination. To combat Denial of Service attacks on the Internet, services like the Smurf Amplifier Registry have given network service providers the ability to identify misconfigured networks and to take appropriate action such as filtering.[12]

SYN flood - is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic. This attack is based on how TCP / IP connection is established. It normally works like this: An application that initiates the session sends SYN packet synchronization recipients. The recipient sends back a confirmation packet to the TCP SYN-ACK, the initiator responds by confirmation packet ACK. When a SYN attack hacker floods the target system by series of TCP SYN packets. Each packet causes the target system to sends SYN ACK response. While the target system waits for an ACK, inserts all outstanding SYN-ACK response to the queue. When the queue is full, the system will ignore all incoming SYN requests. [13]

UDP flood - UDP Flood Attack is one of the attacks causing host based Denial of Service. UDP is a connectionless protocol and it does not require any connection setup procedure to transfer data. A UDP Flood Attack is possible when an attacker sends a UDP packet to a random port on the victim system. When the victim system receives a UDP packet, it will determine what application is waiting on the destination port. When it realizes that there is no application that is waiting on the port, it will generate an ICMP packet of destination unreachable to the forged source address. If enough UDP packets are delivered to ports on victim, the system will go down. [14]

HTTP flood - HTTP Flood remains the most popular type of attack (80%). It involves simultaneously sending a large number of HTTP requests to the site being attacked. Cybercriminals use several different technologies to conduct this type of attack. In 55% of all HTTP Flood attacks bots try to access a single page of the site. The second most common type (22%) is attacks on various authorization forms. The third most common type (12%) is attacks that involve numerous attempts to download a file from the site. More sophisticated attacks, in which cybercriminals attempt to mask the bots by imitating the behavior of real users, are conducted in only 10% of all cases. [9]

Fake identity - For more complex experiments the fake identity may lead to direct access to the control of experiment. It can lead to damage of the experiment.

B. *Consequences of software attacks on remote laboratories*

From the division of REs it is obvious that the security requirements of the three groups of REs differ with respect to their functionality. All attacks on REs can lead to a controlled shutdown of RE (in a better case) or to an undefined state of RE (in the worse case) and therefore they call for some security precautions. Security measures depend on the type of experiment.

Basic REs: Attack on basic REs may lead to shutdown of the server thus preventing their proper use (Fig. 5). Because it is simple experiments that run without user intervention and do not allow any control, attack on them will not cause any further damage. Basic securities and outsourcing using remote access is the remedy in this case.

Complex REs: As in the previous case the attack may lead to the server shutdown and therefore unavailability of the experiment. Due to the sophisticated physical HW involved with the rather sophisticated control program (informatics SW), there is another risk. The hacker can cause damage of controlling software and in extreme cases even hardware component parts of the experiment by attacking the server. When the hacker takes over the control of the server, he/she can send malicious commands which may lead to damage of the experiment (Fig. 6). As an example we can mention "water level control experiment" (http://195.178.94.32/) when the overwriting of controlling limits can lead to overflow the tank. If the experiment is not secured against this possibility, it could cause flooding, short-circuiting of electronics and even a fire.

Scientific REs: Attack on these experiments involves the risks mentioned for the previous two groups. The risk with scientific REs is enhanced by the cost of the used sophisticated measuring instruments whose price may soar

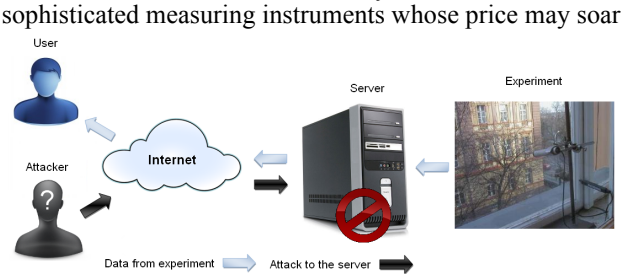

Figure 5. Scheme of attack to the basic experiments

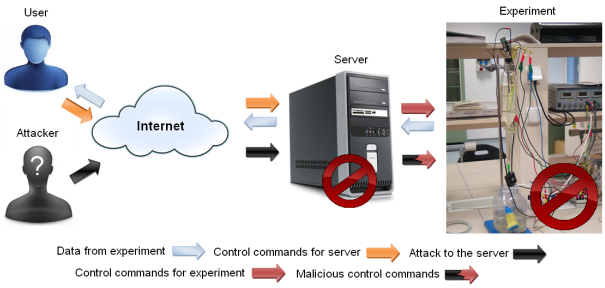

Figure 6. Scheme of attack to the complex experiments

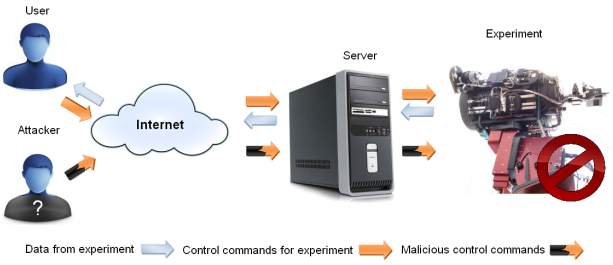

Figure 7. Scheme of attack to the scientific experiment

to millions. Damaging of such devices, either only software part or even hardware can cause extensive damages. Because of this, these experiments require the best care and security for all possible disturbances due to external interference. Some of these experiments can be controlled directly. It means that the user sends controlling commands directly to the experiment. It creates another security risk, because hacker can fake the identity of the authorized user. In this case, he can send malicious commands which may damage experiment (Fig. 7).

III. DESIGN OF SPECIFIC SECURITY SOLUTIONS

The following sections will be concerned with security protection of REs against software attacks from outside. Again, as mentioned above, the level of security will vary depending on the type of experiments sophistication given above.

A. Security of basic remote experiments

These experiments do not require special security. We just have to stick to basic safety rules such as regular update of antivirus, system firewall that allows locking ports and securing proper system services running. Special security of server or secured access to the experiment would be costly due to the nature of the experiment. The least precaution should be the warning that the experiment is out of function and under repair. Generally the controlling SW of even simple experiments should have the self healing property, i.e. to either restart to the initial starting conditions and/or other defined state enabling the continuation of data logging after simple shutdowns resulting from blackouts or other interfering influences.

B. Security of complex remote experiments

With this group of REs it is important to follow basic rules of security as in the previous case. Because this type of REs cannot be damaged directly by the control commands it is not necessary to secure the connection against eavesdropping or confusion. But we should cover all the possible problems arising from the running of the experiment both software and hardware (working with fluid in the experiment http://195.178.94.32/ - the experiment is placed into the tank where the water cannot drain to the electrical devices). If we want to make the experiment accessible only for some groups of users it is appropriate to arrange the access by the user´s name and password, which directly leads to a better security. The biggest potential risk is the access procedure to the server of the experiment. Fortunately the attacks to the server can not in majority of cases lead to the damage of physical hardware, but only to an unavailability of the experiment. As mentioned in Introduction, the main ill effect is then the general feeling of unreliability of REs as education tool.

C. Security of scientific remote experiments

Experiments in this category are characterized by their high costs. For this reason, the security of them is of utmost importance and it is necessary to devote much effort and resources to ensure it. The attack on these experiments can be provided in two ways:

1) Attack to the server (informatics HW)

Attacks to the server can prevent access to the experiment, which can lead to material losses. Most common types of attacks to the server are DoS and DDoS attacks with straightforward solutions to this problem:

-Firewall, switches, and routers - The right choice and setting of these devices can prevent basic types of attacks. By using mechanisms such as access control list, rate limiting, traffic shaping, delayed binding (TCP splicing), deep packet inspection and Bogon filtering, DoS attacks can be detected and remedied. All these measures work only as long as the measures taken aredesigned for DoS attacks in question. For example SYN flood can be prevented using delayed binding or TCP splicing. Similarly content based DoS can be prevented using deep packet inspection. Attacks originating from dark addresses or going to dark addresses can be prevented using Bogon filtering. However if the attacks are based on a different principle, these security systems are ineffective [15].

-Application front end hardware - Application front end hardware is intelligent hardware placed on the network before traffic reaches the servers. It can be used on networks in conjunction with routers and switches. Application front end hardware analyzes data packets as they enter the system, and then identifies them as priority, regular, or dangerous. There are more than 25 bandwidth management vendors [16].

-IPS based prevention - Intrusion-prevention systems (IPS) are effective if the attacks have associated signs. However, the trend among the attacks is to have legitimate content but bad intent. IPS which works on content recognition cannot block behavior-based DoS attacks. An ASIC based IPS can detect and block denial of service attacks because they have the processing power and the granularity to analyze the attacks and act like a circuit breaker in an automated way [16].

-DDS based defense - More focused on the problem than IPS, a DoS Defense System (DDS) is able to block connection-based DoS attacks and those with legitimate content but bad intent. A DDS can also address both protocol attacks (such as Teardrop and Ping of death) and rate-based attacks (such as ICMP floods and SYN floods). Like IPS, a purpose-built system, such as the well-known Top Layer IPS products, can detect and block denial of

service attacks at much nearer line speed than a software based system. [17]

-Clean pipes – Is the service where all traffic is passed through a "cleaning center" via a proxy, which separates "bad" traffic (DDoS and also other common internet attacks) and only sends good traffic beyond to the server. The provider needs central connectivity to the Internet to manage this kind of service. Prolexic, Tata Communications and VeriSign are examples of providers of this service. [17]

Access to the server can also help an attacker to damage experiment by sending of malicious control commands directly to the device. This problem is already included in the most security solutions mentioned above.

2) Attack to the physical HW

Another security risk is appearing due to the fact that experiments allow direct control by control commands. They allow an attacker to attack directly the experiment without being influenced by the security measures of the server. By sending malicious control commands sophisticated equipment can be damaged and major financial losses can be caused. It is obvious that with expensive physical HW it is necessary to provide access to the experiment only to authorized users.

The solution of this problem may be secure access to the experiment by using the user ´s name and password. However, this may turn out as absolutely insufficient for this type of REs. An attacker may use social engineering and phishing to gain the access to the data. He/she also may change his/her internet identity, i.e. redirect the flow of the data to a false computer, to look like an authorized user and thus gaining access to the experiment. A good remedy is then securing the connection between the server and client by using encryption and authentication of the identity on both sides. For this purpose you can use different types of symmetric and asymmetric encryption. However the application layer of network protocols offers a comprehensive solution of this problem. It is HTTPS protocol (Hypertext Transfer Protocol Secure). [18]

HTTPS is an extension of the HTTP network protocol, which enables secure connection between web browsers and web server from eavesdroppers and data-faking. It also verifies the identity of the counterparty. HTTPS protocol uses asymmetric encryption. Both parties have to generate a key pair (private and public) before communication. At the start of communication, both sides exchange public keys, which should be checked by a different communication channel.

The encryption protects communications from eavesdroppers, but without authentication of public keys, there are communication risks from a "Man in the middle". This issue involves an attacker who intercepts the communication when establishing a connection. By capturing and replacing of the public keys of both counterparties he obtains unlimited access to communication and allows changing or disrupting communication. Because of that it is necessary to solve the problem of handing the keys. There are some solutions:

-The most trusted verification, is handing the keys personally. This option is applicable for a limited number of experiment´s users and the possibility of their meeting.

-Verification can be done by checking the extract of keys (hash) for example by using telephone call.

-You can also use the principle of "transfer of trust"; public key is digitally signed in this case. This signature is verified by a certification authority that we trust (e.g. VeriSign).

IV. CONCLUSIONS

REs in e-laboratories are becoming modern and prospective trend in teaching at school and university level. Unfortunately, along with this come the threats of possible attacks. Attacks may vary depending on the type of experiment and the purpose for which they are performed so, similarly, the defence also varies.

Attacks may be directed to the control servers of experiments usually leading to the shutdown of the experiment and the impossibility of access. DoS interference is used predominantly for these attacks. These attacks can be applied to any server in the Internet. This issue is adequately described in theliterature and different types of defence can be used. The safest protection measures are based on a hardware basis itself. All these solutions are rather expensive; therefore their use is seldom to be found with simple experiments. [10]

The security of remote laboratories is much more susceptible to the attack aimed at the experiment hardware. These attacks lead to the damaging of expensive equipments resulting in a substantial financial loss. Attacks can be executed by the access to the servers or directly by sending of malicious control commands to the REs. Possible solution of this situation is to secure experiment by user´s name and password. However this approach is susceptible to eavesdropping or the user's identity confusion. Therefore, it is appropriate to use an encrypted connection between the user and experiment, based on HTTPS protocol in this case. [18] This protocol ensures a sufficient connection security and verification the user's identity if used correctly. This solution brings some security risks as well. There is a possibility interception of public keys eliminated by using certificates validated by a certification authority.

We are currently involved in the administration of three remote laboratory located in Zlín (Tomas Bata University), Prague (Charle´s University; http://www.ises.info) and Trnava (Trnava University in Trnava; http://kf.truni.sk/remotelab). Their security is universally solved at the level of complex REs. In addition to the conventional security, such as antivirus and firewall, we implemented several other measures that may help in the protection of experiment framework building. Our experiments create automatically so-called "log-file" where addresses of connected users and their activities in the experiment in question are automatically stored. This does not guarantee safety itself, but allows the detection and analysis of failures or malfunctions of experiments. This file ensures faster recovery of the service in case of outage. Our experiments provide security through user´s registration and reservation system as well, so the simultaneous control of the experiment by two users is excluded, allowing for the observation of the experiment run only. Also we have exerted considerable efforts on the side of RE programming to treat all undefined conditions of experiments that could arise from ill controlling or hardware failure. Our experiments are generally backed up by UPS power supplies, ensuring the restart and accessibility after a power blackout.

REFERENCES

[1] Humos, A. A., Alhalabi, B., Hamzal, M., Shufro, E., & Awada, W.(2005). Remote labs environments (RLE): A constructivist online experimentation in science, engineering, and information technology. In Proceedings of IECON 2005. 32nd Annual Conference of IEEE, Industrial Electronics Society (pp. 2156-2161). Raleigh, NC: IEEE

[2] C. Gravier, J. Fayolle, B. Bayard, M. Ates, and J. Lardon, State of the art about remote laboratories paradigms - foundations of ongoing mutations, International Journal of Online Engineering 4, 1 (2008) 19-25, http://www.online-journals.org/index.php/ijoe/article/view/480/391,

[3] Auer M.E. and Gravier C. (2009 October-Decmber),The Many Facets of Remote Laboratories in Online Engineering Education IEEE Trans. Learn. Techn. Vol. 2, No. 4, p.260

[4] [František Schauer, František Lustig, Miroslava Ožvoldová: Internet Natural Science Remote e-Laboratory (INRe-L) for Remote Experiments /.In: Innovations 2011: World Innovations in Engineering Education and Research (USA), iNEER / ed. W. Aung, et al. - (2011), s.51-68.,]

[5] Cooper M 2005 Remote laboratories in teaching and learning – issues impinging on widespread adoption in science and engineering education, iJOE Intern., J. Onl. Egin. 1 1.

[6] Remote Farm. Remote Farm [online]. 2012 [Read: 2012-03-19]. http://remote.physik.tu-berlin.de/farm/

[7] Krbecek, Michal. Creation of multimedia interactive teaching tool with utilisation of remote experiments. Zlín, 2011. 108 s. Diploma thesis. UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ.

[8] Lustig, František, František Schauer a Miroslava Ožvoldová. Plug and play system for hands on and remote laboratories. In: Proceeding book of the joint international conference MPTL '16 - HSCI 2011. Slovenia: Organizers, 2012, s. 50-56. ISBN 978-961-269-637-5. See: http://194.249.18.139/mptl_hsci/images/stories/booklet_mptl_hsci_web.pdf

[9] Garnaeva, Maria a Yury Namestnikov. DDoS attacks in H2 2011. In: Securelist [online]. 22 Feb 2012 [Read: 2012-02-27]. http://www.securelist.com/en/analysis/204792221/DDoS_attacks_in_H2_2011

[10] Yuval, Fledel. Uri, Kanonov. Yuval, Elovici. Shlomi, Dolev. Chanan,. "Google Android: A Comprehensive Security Assessment". IEEE Security & Privacy Vol 8 Issue 2 March-April 2010 pp35 – 44

[11] Ping of death. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 10 October 2011 [Read: 2012-02-06]. http://en.wikipedia.org/wiki/Ping_of_death

[12] Denial-of-service attack: ICMP flood. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 1 February 2012 Read: 2012-02-06]. http://en.wikipedia.org/wiki/Denial-of-service_attack

[13] SYN flood. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 22 January 2012 [Read: 2012-02-06]. http://en.wikipedia.org/wiki/SYN_flood

[14] UDP Flood Attack. In: Javvin [online]. 2011 [cit. 2012-02-27]. http://www.javvin.com/networksecurity/UDPFloodAttack.html

[15] GOPI, Midhun. Distributed Denial of Service Attack (DDoS). In: Security Research [online]. November 21, 2011 [Read: 2012-02-27]. http://securityresearch.in/index.php/tutorials/how-to/distributed-denial-of-service-attack-ddos/

[16] Denial-of-Service Attacks. In: Webhosting Depot [online]. © 2001 - 2012 [Read: 2012-02-27]. http://www.webhosting-depot.com/articles/ddos-attacks.php

[17] DoS Attack: Prevention And Response. In: Serving History [online]. 2012 [Read: 2012-02-27]. http://www.webhosting-depot.com/articles/ddos-attacks.php

[18] The World Wide Web Security FAQ: Securing against Denial of Service attacks. W3C: Security [online]. 1.7. W3C, 2003, 2003/02/23 [Read: 2012-02-06]. http://www.w3.org/Security/Faq/wwwsf6.html

AUTHORS

M. Krbeček, F. Schauer and **R. Jašek** are with the Tomas Bata University in Zlín, Faculty of Applied Informatics, Nad Stráněmi 4511, Zlín, CZ- 760 05, Czech Republic (krbecek@fai.utb.cz, fschauer@fai.utb.cz, jasek@fai.utb.cz).

Received 18 March 2913. Published as resubmitted by the authors 12 June 2013.