Remote Laboratories Framework: Focus on Reusability and Security in m-Learning Situations

doi:10.3991/ijoe.v5i3.897

J. Fayolle, C. Gravier, M. Ates, J. Lardon
Laboratoire DIOM, TELECOM Saint-Etienne, école associée de l'Institut TELECOM
Université de Saint-Etienne, Université de Lyon, France

Abstract—Remote laboratories is a spreading concept which allows the remote use of devices through Internet connexion. The paper deals with the providing of a framework which is reusable for many devices, from different end-user media such as phone, computer or TV and acceptable in industry, therefore taking into account multi information systems securities.
The problem is addressed through the point of view of m-learning situations which involves the lack of rich user interactions and the fact that the user belongs to external information systems when he interacts with the remote device.
The modelisation of the remote device with ontologies, the use of a central application server, message oriented middleware and standard web services (database, authentication) are the keys allowing the independence of the framework to the device.
The adaptation of the GUI to the end-user device is made through a proxy which refactor the requests and responses according to the capabilities of the end-user device (size of screen, interactions tools).
The use of a user-centric model of identities federation allows us to provide an efficient way to reach the goal of transparency to security constraints.

Index Terms—Mobile Learning, Remote Control,Security Federation, SAML, Ontologies, Adaptative Hypermedia, Collaborative Remote Laboratories

I. M-LEARNING AND REMOTE LABS

One commonly used definition of the Mobile Learning (henceforth m-Learning) is:

Learning that happens across locations, or that takes advantage of learning opportunities offered by portable technologies. In other words, mobile learning decreases limitation of learning location with the mobility of general portable devices [2].

The challenges of m-Learning are numerous on the technological aspects but also in the social and educational parts. Among the main technical challenges, we can cite the multiple standards, multiple screen sizes, multiple operating systems, the adaptation of existing e-Learning materials for mobile platforms,etc. The pedagogical issues focuse on the support to learning activities across many different contexts, design of technologies for life-long learning, private information and content,etc.

These problems are already considered as compulsory for “traditional lessons”, which do not involve the relationship with material devices. In the field of professional training, such as being addressed in engineering schools, we have to consider the aims of the learning activities. In the engineering schools, education embraces technical learning on real devices such as hyperfrequency analyzers, optical fiber stretcher and characterizer for optic, etc. The introduction in the distance learning process of real devices is clearly a way to achieve the robustness of student skills.

However, the intersection of the difficulties coming from the remote control of real devices and the ones coming from the mobility leaves us an interesting research field.

To sum up, the three pillars of m-Learning are:

- the heterogeneity of client devices,
- geographical distributions of users and devices,
- the software development cost of m-Learning solutions adapted to each situation, each client device and each remote device.

If we want to promote the use of m-Learning in real situations (with students working on real instruments), we have to address the three above problems in a global approach. On the whole, these three questions can be reformulated in the following way (see Figure 1):

- the genericity of the framework according to the client device and according to the remote device,
- the security considerations: how to interact between peoples and devices which are very probably not authenticated in the same Information Systems
- the Human Computer Interface of the remote control and especially its adaptation to the mobile context.

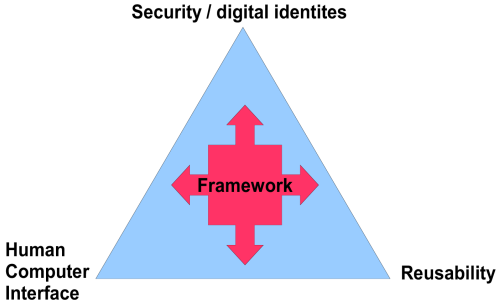

Figure 1. M-Learning tryptic :Human computer Interface, Reusability and Security

That is the reason why we argue that these three criterions need to be represented and balanced in a Remote Laboratory framework for a better efficiency.

In this paper we focus on the remote control of devices, the adaptation of interfaces to the context and the consequences of such open door on the security of the Information System. First, we address the problem of taking the control on a physical device through the Internet. Such an approach is known as Remote Laboratories, and tries to cope with the lack of remote hands-on approaches within distance learning or remote services in industrial fields.

The paper is organized as follows. First, we propose our framework for remote control, focusing on device independence (a solution of remote laboratory framework that is not supposed to be dedicated to the device it supports). Then, we show how this framework allows the adaptation of the distant user interface to the client device context and mobility. Next, we briefly explain how security federation can be the key for sharing devices between different firms and clients coming from different Information Systems) without breaking any security constraints. Finally, section 6 concludes.

II. RELATED WORKS

Since few years, we assist to a strong evolution of Mobile Learning and its use for long-life training in extended enterprise. Distance learning has brought to the Web a number of learning tools, making lectures possible in the case of teachers and learners are in different place and/or at different time. The mobility adds a new dimension: the fact that one client is not coming all the time from the same point (geographical mobility) and the use of new media (smartphone, personal assistant) to interact with the learning platform. For most of these solutions, the approach is web based ([24,21,18,11]), sometimes uses continue multimedia streaming ([3]) or integrated environments such as the set of Matlab toolkits ([9]). Almost all of the actual solutions, however, are not adapted to transfer professional skills on real devices (for example, the way the device is supposed to be manipulated). What we address here is either the initial training which can be done in institutions (universities, engineering schools, ...) and the life-long training in firms. In our opinion, this last field is almost important as the first one. A survey of remote laboratories paradigm coming from an important set of related works can be found in [15].

There is no denying that the use of a computer or a phone introduces a new media. But we have to assure that "felt-life" ([20,17]) has also to be translated within the platform, for the computer link to be as transparent as possible. It is known that the learning process is widely based on previous personal experiences: "this is principal means by which knowledge transitions from a declarative form (encoding of examples) to a procedural form (production rules)" ([4]). However, this aim is very hard to reintroduce in the context of remote control of device. This is why many e-learning schemes only address the theoretical point of view, leaving the hands-on sessions to activities with physical presence.

The objective of our work is to demonstrate that we can build a generic and collaborative framework on which we can plug any kind of real and distance devices and control them through the Internet.

The proposed framework has to be generic in the way that we do not want to redevelop the protocol of information exchange since, on the whole, the information are similar (commands, answers, parameters, ...). If we have to code this behavior independently for each device, this will be unsatisfactory, especially when the number of devices is large. The second point is to show how this approach can be generalized in order to adapt the distant GUI[1] according to the media (computer, phone, IPTV, ...) and to the user (expert or beginner for example). Indeed, we need more and more mobility and there is some need to control remote devices through new devices such as smartphones for example. This is the foundation of pervasive computing to allow the control of real world objects without thinking of how the system acts under the cover ([23]).

We identify two ways of addressing the issue of transforming a User Interface - or more specifically Internet content - to match an ability limited device. To separate the two approaches, we rely on the Model-Driven Engineering ([13]).These two ways are: by direct code to code transformation (or transcoding) or by re-engineering which passes through three steps: reverse-engineering, model to model transformation and forward-engineering. The main difference between these two approaches is that the former tries to address the transformation in a higher level of abstraction whereas the later tries to build a model over the content and then adapt the model. In this paper, we will show that we can use both type of transformations: code to code transformation in order to adapt the interface to the user (for example through the disappearance of commands which need a high level expertise) and re-engineering to adapt the interface to the media.

Lastly, we address the problem of security. By allowing the remote control of devices through the Internet, we may create security holes. Indeed, by thinking about the use of one device belonging to one firm, and which is proposed as a service to other ones, we have to allow the connection to people which are not known in the second Information System. To perform this, we have to build a solution which exchanges informations about identities and security associated to these identities. An obvious solution is to work on the feeling of trust you get about people coming from this firm. Identity federation aims at creating Circles of Trust (namely CoT) between Information Systems sharing pre-established administrative bounds. It means to make the retrieval of the clearance of access from the Information System possible the requested digital identity belongs to. Identity federation means safely transport identity information in respect of users' privacy in an undefined environment, by taking care of privacy legislation according the domain of application[2] . In Liberty Alliance architectures, for example, users are asked to give their approval when a service provider requires identity attributes. Furthermore, federation architectures rely on pseudonymity ([22]) to support privacy.

[1] Graphic User Interface

[2] Two main references are two European directives: The Framework Data Protection Directive 95/46/EC (Directive) et The Electronic Communications Data Protection Directive 02/58/EC (ECDP Directive)

III. REMOTE CONTROL FRAMEWORK

A. *On the reusability of remote labs*

We started Remote Laboratory researches in 2000 ([6]), based on a network analyzer[3] and an antenna workbench we wanted to put online. Of course, unlike the network analyzer, the antenna workbench conveys mechanical experiences (moving antenna and starting/stopping motors). The resulting GUI, however, is close to one another, because the GUI displays the same kind of widgets, whatever the device is (square, rectangle, round or knob buttons, led, curves, moving objects, menus, etc). Besides, we become aware that we were about to reinvent the wheel each time we want another device online. This tends to illustrate that dedicated integrations are short term answers that are not supposed to be reused for other experiments involving other devices. Moreover, as we exploited this solution in our teaching, we understood how authenticity of the device displayed is important. Because students mostly learn from hands-on approaches *how to use* appliances, not *how they work*. As such, it is very important to be as real as possible since it will enhance the learning experience. Consequently we can say we learn from past experiences that genericity is a major issue for bringing several devices online *and* authenticity is a major factor for the learning experience to succeed. Nowadays, laboratories based their experiments on a heterogeneous set of devices. In the context of Remote Laboratories design, aiming at devices' independence means supplying interoperability tools, in order to get Remote Laboratories platform able to support any kind of "remote-able" devices. Such an objective needs a formal representation of what a device is, qualifying the device with no more and no less details than necessary. To reach that goal, we need a representation of knowledge that allows to conceptualize a specific domain *and* to specialize (instantiate) that domain ([16]). This way, the representation of the knowledge is shared among all devices, and each device goes with a specialization of that domain of knowledge. This requirement of interoperability perfectly fits the definition of ontologies (and one standard specification known as OWL[4] , from the W3C).

Another possibility would have been to describe the interface and the behavior in a XML file. But, if we choose this approach, we cannot assure the interoperability between different Remote Laboratories, and with other platforms such as Learning Management Systems (LMS). What we need is a common language between different devices and the framework in order to exchange informations between devices in a global experiment, which involves more than one device (mesh up of instruments). The knowledge of this language can also be used for evaluation purpose (detection of good and false sequences). To build this common language, we need a vocabulary and somehow a grammar to use this vocabulary but also a commitment on the subsequent concepts and relationships between these concepts. Ontologies are an answer to this problem since it is a normalized approach for the description of nature and composition of something.

[3] A network analyzer allows the measurement of module and phase of reflected and transmitted signals of a device.

[4] Ontology Web Language

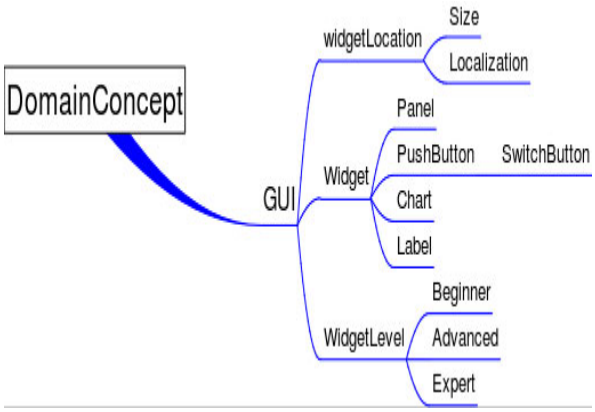

Figure 2. Part of the Laboratory devices' ontology used for specializing distance interfaces.

We established the ontology of devices that one could find in a laboratory. With such an ontology (see Figure 2), we are able to dress the complete GUI of a device without any link to the media which will be used to control it.

The vocabulary part of the ontology is common to all the devices. Upper the vocabulary, we have to described the functionalities of each device, which are obviously dependent of device type. The result is an OWL file per device grouping together the vocabulary and the "functionalities". With this approach, we have described in a semantic way very different devices such as a network analyzer and an antenna workbench and we are about to dress the OWL of an optic fiber stretcher.

B. *Implementation*

The OWL file associated to each device is put on a Web server. A rich standalone client downloads and parses it to build the distance interface of the real remote device. The aim of this parsing step is, on one hand, to build the graphical interface, and on the other, to associate to this interface the different functionalities of the device. The interface is as close as possible to the real one. The standalone client uses a MOM[5] above an application server (for authentication, authorization and transactions). We use publish/subscribe paradigm ([12]) to deliver message to all learners in the classroom.

Mainly, the message between the client, the application server and the device are splitted in three types using ASK, ACK and ANS performatives:

- *ASK*, stand for "asking". This kind of message is sent when the user interacts with a widget. Then, this message is unicasted to the instrument with arguments describing the command (identifier, associated parameters, ...)
- *ACK*, stands for "acknowledgment". We need immediate reaction from the server side because commands performed on a device can last long (if an antenna needs to be moved for example). This message is multicasted to all the users allowing them to see that someone has asked this functionality or measurement.
- *ANS*, stands for "answering". Obviously, when the device has performed the actions corresponding to the request, it sends the response to all the users (multicast message).

[5] Message Oriented Middleware

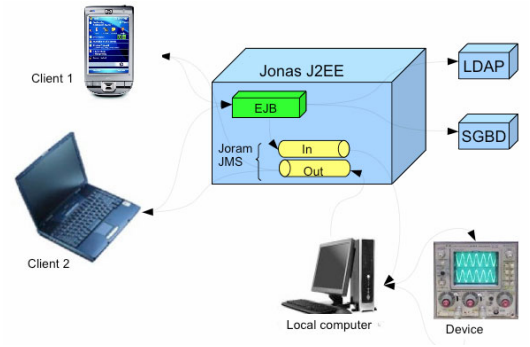

Figure 3. Online architecture we implemented.

Upper this very simple protocol of message exchange, we use some normalized services to assure different tasks:

- we use JAAS[6] for authentication and authorization purpose. The framework verifies for each action if the user has the permission to do it. Since we try to be fully compliant to traditional Information System, the information about users credentials are stored within a LDAP directory (openLDAP is chosen as implementation).
- logging of the actions are made in a PostgreSQL database for two purposes: the post session evaluation by the teacher and the analysis of users' behavior.
- messages transportation is built thanks to a Java Messaging Service implementation: JORAM[7] , an ObjectWeb[8] open source Message Oriented Middleware.
- All the system is controlled by JOnAS[9] , as we were looking for a J2EE certified application server.

IV. ADAPTATION OF THE REMOTE INTERFACE TO THE CONTEXT

One of the major aspects of a global approach for remote control is to allow a high flexibility of the proposed platform. We have seen earlier (see section 3.1) that the use of an ontology tool allows to represent in a same way very different kinds of devices and their distance control. However, we want to overcome another limitation which is the adaptation of the remote interface to the context: geographic localization, media used to interact with the device.

Mainly, we identify three components in the context :

- the localization of the user
- the user's context based on its skills or clearance of access. Does the devices used by an expert user or a beginner (for example in training session) or does the user paid to get all of the functionalities offered by the device ?
- the media used to control the device. We are more and more dependant to Information Systems and we need to interact with it at anytime and any places. Therefore, we have to provide the control of Information System and the underlying remote devices through different terminals such as smartphone, television and game consoles for instance.

[6] Java Authentication and Authorization Service
[7] Java Open and Reliable Asynchronous Messaging
[8] http://www.objectweb.org
[9] Java Open Application Server

Figure 4. Figure 4: Hiding of buttons on remote interface according to their level of use.

The use of modelization tools such as ontologies helps us in solving the first and second goals. For the localization, if we put apart the security considerations (addressed in the next section), the localization adaptation consists mainly to present an interface in the right language. To do that, we have to re-interpret the ontology with the right language set, by trying to minimize the encoding bias. The second goal is not very difficult: indeed, since we get a formalization of the interface, we can therefore associate a level of use to each widget. When the user plays with the remote interface, he only has to specify what is the level of use he wants to select. Then, we re-interpret the ontology according to this level, ignoring the widget which have a level greater than the selected one. For example, if a button is dedicated to level 3, and the user select level 2, he will not see it in its remote interface. The figure 4 illustrates this kind of degradation of remote interface.

The third goal is more difficult to reach as it is not obvious to control what are the features of the remote backend. The features of the media can be very different from one to the other. A smartphone has a very small screen, a bandwith which are not so high and very poor interaction tools (no or small keyboard, ...). On the other hand, a television connected to the Internet can have a very high resolution, but still poor interaction tools (no keyboard). At last, a game console such as Nintendo Wii can be usefull to get at the same time a high resolution and interaction tools and therefore reconstruct an environment very close to computer ones. On the whole, on the server side of the remote control framework, we cannot know what are the features of the client terminal.

The objective of our research is to propose a way to dynamically adapt the GUI to the possibilities of the client devices.

We propose here as an architecture a proxy-like approach like Top Gun Wingman ([10]), Digestor ([7]) and Power Browser ([8]). The reason of this choice is that we have no guarantee that all targetted devices will have enough processing power to handle the adaptation ([19]). The adaptation will therefore be on the fly. It functions as the following (see figure 5):

- the user asks for a distant interface on a proxy
- if the proxy already knows the client's display features, it dispatches the request to the server which send the correct interface and the proxy relays it to the client
- if the proxy does not know the client's display features, an exchange with the client is necessary to get these features (from direct answer of the client or through a request on the underlying operating system if it is possible). After this exchange, the proxy stores in a database the features corresponding to this client and we can process further.

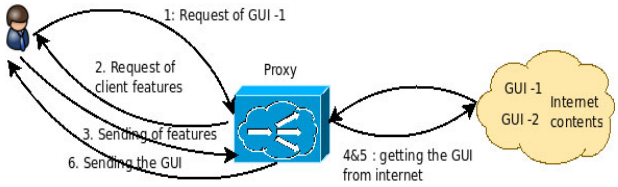

Figure 5. Getting a GUI adapted to the client context through a proxy

The core of the algorithm is therefore implemented as a plugin of a traditional proxy (squid for example). The plugin is based on a genetic algorithm which takes as input a GUI description, apply to it many transformations (each transformation is a chromosome), in order to get the optimal solutions according to the specifications of the used device.

V. DISTRIBUTED SECURITY

As we said in introduction, there is three axis of research to build a global solution for m-Learning on Remote Laboratories. We have already viewed the two first ones: reusability and adaptation of GUI. The last point is to deal with security. This is clearly a major problem in most of the frameworks proposed in the literature, especially those dealing with solutions such as VNC (virtual network computer). Indeed, with this kind of solutions, you have the control not only of the remote device but on *the remote computer*, which can be considered as an unacceptable situation, considered by most of us as an authorized intrusion in Information System.

Here, we have shown in the previous sections, that the framework is mainly on the server side. More precisely, the J2EE server asks an authentication server if the current client is allowed to use the remote device. Each command can be verified with this control, contributing to a very safe access to the device.

But, this kind of scheme is correct if you trust the authentication server. In fact, all the security tokens are given by this server (commonly a LDAP server). In an usual case, the client and the device are not from the same entity (for example, a firm proposes as a service the use of its devices, or in m-Learning context a student accesses to a device from any world point through its phone subscription). The probability that the client is already registered in the authentication server corresponding to the device is therefore very low. The worse solution is to create an anonymous account, or an account dedicated to the client, which is usually forgotten by the system administrator and remains in the identities repository. Moreover, anonymous identities do not allow a relevant accounting service.

As a matter of fact, we think that a better solution lies in the fields of the identity federation. Indeed, if one have to wonder how to give access to some people to one's devices, there should have strong confidence in the distance user. This approach can be generalized to the concept of Circle of Trust (CoT) between two Information Systems. In a CoT, one can use the security tokens from one authentication server in order to use the services proposed by the other system. The first thing to do is to determine if the remote parties feel confident enough to trust each other. If the answer is positive an organization can trust the other one to establish the identity of their users and provide signed information about them.

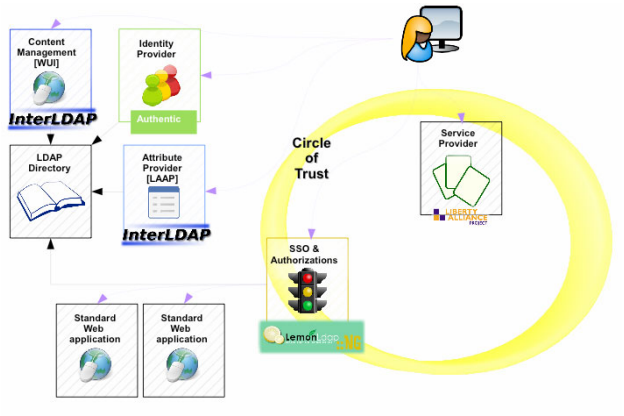

Figure 6. Principle of identity federation in the FEDERID Project: the different providers

For Mobile Learning, the construction of a CoT between Information Systems of firms and the different Information Systems of telecommunication operators can be build.

The basics of identity federation is the establishment of a trust architecture between partners and the implementation of protocols allowing to retrieve signed information. The main expected functionalities are identification of partners' members, establishment of user identity, and being able to retrieve information about them. The stake of identity federation between Information Systems is the interoperability through normalized protocols. The objective is not to build a metaserver which collects and synchronizes information from slave servers, but to build a decentralized architecture built on a consensus to safely exchange identity informations.

The federation can be based on different protocols, leading to different solutions. At this time, the main architectures, such as universities or e-government, are SAML-based ([1]) through Liberty Alliance ([22]). We have contributed to SAML implementation in order to propose a complete solution of identity federation named *FederID* [5]. This solution is based on different tools: a reverse proxy (lemonLDAP), an (or multiple) identity provider (Authentic) and an attribute provider (InterLDAP). The figure 6 summarizes the different security information exchanges through Web Services in Circles of Trust.

With this kind of structure, a client can use a device belonging to another Information System, provided that both information systems are in the same CoT.

However, it is clear that this kind of structures is very comple and the actual implementation is user centric in order to guarantee that no extra informations are given to someone which is not accredited for.

Therefore, the final implementation is summarized in figure 7: the user gets its private key and when he needs to interact with a extern service, the key is provided by the security server through an acknoledgment of the user.

Further work has to be done in order to do the same thing between two CoT.

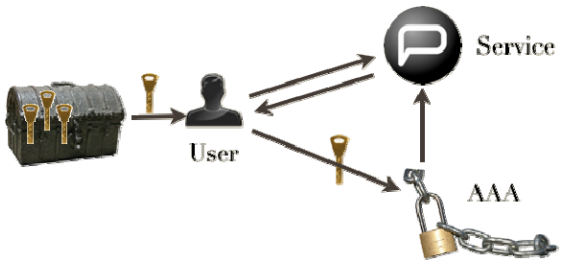

Figure 7. providing of security tokens in a user centric model of identities federation: the user, who needs a service, has to provide a token to the service from his repository. The security token has been itself provided from a identity provider.

VI. CONCLUSIONS

In this paper, we have tried to address all the parts which are involved in the remote control of devices for distance education trough mobile Learning as well as lifelong training, putting the focus mainly on

- the reusability of the framework in order to put more and more devices online without reinventing the wheel each time,
- the adaptation of the GUI to the used tool (phone, pc, iptv, ..) and the user mobility,
- the security the exchange of the required security tokens between the client of the device and the authentication server devoted to the device.

For each of these parts, we have shown how the problem can be solved and we have proposed and implemented a solution, giving us the opportunity to propose a global framework for remote control of devices [14] which is applied to mobile learning context.

Obviously, there is still a lot of work to be done in order to propose a complete set of remote devices in a m-learning framework. Among the principal tasks, we plan to address quickly:

- the evaluation of the framework according to its usability through a direct investigation of users,
- how to confirm the genericity of the proposed framework through the proposal of new devices on the m-learning framework,

VII. REFERENCES

[1] Security assertion markup language (saml) v2.0. Technical report, OASIS, http://www.oasis-open.org/specs/index.php, 2006.

[2] Mlearning, http://en.wikipedia.org/wiki/m-learning. Technical report, Wikipedia, Revised on 2008,October 8.

[3] H. Abdel-Wahab, K. Maly, A. Youssef, E. Stoica, M. Overstreet, K. Wild, and A. Gupta. The software architecture and interprocess communications of IRI: an Internet-based interactive distance learning system. In I. C. Society, editor, *Proceedings of the 5th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE'96)*, page 4, 1996.

[4] J. R. Anderson, J. Fincham, and S. Douglass:. The role of examples and rules in the acquisition of a cognitive skill. *Journal of Experimental Psychology: Learning, Memory, and Cognition*, 23:932–945, 1997.

[5] M. Ates, C. Gravier, J. Lardon, J. Fayolle, and B. Sauviac. Interoperability between heterogeneous federation architectures: illustration with saml and ws federation. In *SITIS-Septis'07 IEEE International Conference On Signal-Image Technology and Internet based systems, Workshop on security and privacy in telecommunication and information system*, December 2007.

[6] B. Bayard, B. Sauviac, J. Fayolle, B. Allard, and G. Noyel. Projet webanalyzer internet et l'instrumentation à distance. In *TICE 2002, Technologies de l'information et de la communication dans l'Enseignement Supérieur et l'Entreprise*, pages 415–416, Novembre 2002.

[7] T. Bickmore, A. Girgensohn, and J. Sullivan. Web page filtering and re-authoring for mobile users. *Computer Journal*, 42(6):534–546, 1999.

[8] O. Buyukkokten, H. Garcia-Molina, A. Paepcke, and T. Winograd. Power browser: efficient web browsing for pdas. pages 430–437, 2000.

[9] A. R. S. Castellanos, L. H. Santana, E. Rubio, I. S. Ching, and R. A. Santonja. Virtual and remote laboratory for robot manipulator control study. *The International Journal of Engineering Education*, 22(4):702–710, 2006.

[10] A. Fox, I. Goldberg, S. Gribble, and D. Lee. Experience with top gun wingman: A proxy-based graphical web browser for the 3com palmpilot. In *In Proceedings of Middleware '98*, 1998.

[11] M. A. Garcia-Ruiz, A. Edwards, S. A. El-Seoud, and R. Aquino-Santos. Collaborating and learning a second language in a wireless virtual reality environment. *International Journal of Mobile Learning and Organisation*, 2(4):369 – 377, 2008.

[12] K. Geihs. Middleware challenges ahead. *IEEE Computer*, 34:24–31, 2001.

[13] A. Gerber, M. Lawley, K. Raymond, J. Steel, and A. Wood. Transformation: The missing link of mda. In Springer-Verlag, editor, *ICGT '02: Proceedings of the First InternationalConference on Graph Transformation*, pages 90–105, 2002.

[14] C. Gravier and J. Fayolle. Web site of the einst project. Technical report, Istase, http://diom.istase.fr/satin/einst, 2007.

[15] C. Gravier, J. Fayolle, B. Bayard, M. Ates, and J. Lardon. State of the art about remote laboratories paradigms - foundations of the ongoing mutations. *iJOE: International Journal of Online Engineering*, 4(1):19–25, February 2008.

[16] T. Gruber. Toward principles for the design of ontologies used for knowledge sharing. *Elsevier Science Ltd.*, 43:907–928, 1993.

[17] S. Guss. Interface metaphors and web-based learning. *Lecture Notes in Computer Science*, 2783:168–179, 2003.

[18] K. Kathryn Mac Callum. Mobile technology in collaboration: evaluation of a web-based discussion board. *International Journal of Mobile Learning and Organisation*, 2(4):318–328, 2008.

[19] J. Lardon, M. Ates, C. Gravier, and J. Fayolle. Overview of web content adaptation. In *Proceedings of ICEIS 2008*, volume HCI, pages 384–387, June 2008.

[20] J. McCarhty and P. Wright. Putting felt-life at the centre of human-computer interaction. *Proceedings of In Reflective HCI Workshop*, 2004.

[21] R. Pastor, C. Martin, J. Sanchez, and S. Dormido. Development of an xml-based lab for remote control experiments on a servo motor. *International Journal of Electrical Engineering Education*, 42(2):173–184, 2005.

[22] B. Pfitzmann. Privacy in enterprise identity federation: Policies for liberty single sign on. *Lecture notes in computer science Privacy Enhancing Technologies*, pages 189–204, 2003.

[23] M. Weiser. The computer for the 21st century. *ACM SIGMOBILE Mobile Computing and Communications Review*, 3(3):3–11, 1999.

[24] Z. Yanga and Q. Liu. Research and development of web-based virtual online classroom. *Computers & Education*, 48(2):171–184, 2007.

ACKNOWLEDGMENTS

This work is granted thanks to the General Council of Loire Department, France and by the French National Agency of Research (FEDERID project).

AUTHORS

J. Fayolle, C. Gravier, M. Ates and J. Lardon are with the Laboratoire DIOM, TELECOM Saint-Etienne, école associée de l'Institut TELECOM Université de Saint-Etienne, Université de Lyon, France.

Submitted, April, 6, 2009. Published as resubmitted by the authors on July, 15, 2009.