Distributed registration and key distribution for online universities

Rolf Oppliger, Martin Bracher
University of Berne, Institute for Computer Science
Neubrückstrasse 10, CH-3012 Berne, Switzerland
Phone +41 31 631 89 57, Fax +41 31 631 39 65,
{oppliger,bracher}@iam.unibe.ch

Andres Albanese
International Computer Science Institute (ICSI)
1947 Center Street, Berkeley, CA 94704-1105, USA
Phone (510) 643-9365, Fax (510) 643-7684, aa@icsi.berkeley.edu

Abstract

In this paper we focus on the role of universities in distance education and teleteaching. We argue that universities have to cooperate with commercial service providers to disseminate lectures to a wide audience, and that this cooperation requires new techniques with regard to the registration, validation, and certification of the parties involved, such as professors, service providers, and students. We also propose a technique that can be used in distance education and teleteaching to set up and run online universities. The technique has been named DiRK, an acronym derived from Distributed Registration and Key distribution. It can be used in a conferencing system, such as the Internet Multicast Backbone (MBone), to handle the registration of participants and the distribution of session keys in a decentralized and fully distributed way. DiRK is being prototyped in a session registration tool (`srt`) for the MBone. The `srt` will serve as a starting-point to evaluate and further enhance DiRK, as well as to develop similar tools that can be used in distance education and teleteaching to set up and run online universities.

Keywords

Distance education, teleteaching, online universities, Internet Multicast Backbone (MBone), participants registration, validation, key distribution

1 INTRODUCTION

Universities not only suffer from increasingly high operating costs, but their budgets are often reduced for the sake of the financial standing of the funding states. In this difficult situation, universities have either to downsize, or to effectively enlarge their audience and have more students participate and share the operating costs. Both possibilities are not satisfactory, mainly because it is, in general, not feasible for a university to downsize without simultaneously loosing educational quality, and because the enlargement of a university's audience is also limited by architectural and logistical restrictions. In this difficult situation, the idea of distance education and teleteaching has fallen on fruitful ground. The idea is to have networks interconnect the computers located at the professors' and students' sites, and to use the networks' multicast options to have registered students remotely participate in university lectures. In this paper, the terms distance education and teleteaching are used synonymously to refer to this general idea.

The Multicast Backbone (MBone) is an experimental network that is overlaid on the existing Internet to carry IP multicast datagrams (Deering and Cheriton, 1985; Deering, 1989; Deering and Cheriton, 1990; Deering, 1991). Application tools, such as `vat` (visual audio tool), `nevot` (network voice terminal), `nv` (network video), `ivs` (inria videoconferencing system), `vic` (video conferencing), and `wb` (white board) can be used to hold multimedia conference sessions within the existing MBone. In addition to that, session directory tools, such as `sd` and `sdr`, can be used to announce MBone conference sessions in public, and to indicate other MBone application tools how to start (Eriksson, 1994; Macedonia and Brutzman, 1994; Kumar, 1996).

The ability to route IP multicast (class D) datagrams through the MBone allows online universities to be set up and run today. More precisely, the MBone can be used to multicast university lectures to interested parties, such as registered students and employees of companies that participate in corresponding educational programs. However, it is important to note that the MBone (and the Internet) is just a prototype of a network that can be used for distance education and teleteaching, and that other networks that support multicast could be used as well. For example, if the asynchronous transfer mode (ATM) supported multicast similar to IP, ATM networks could be used for distance education and teleteaching, too.

In this paper we focus on the role of universities in distance education and teleteaching. We argue that universities have to cooperate with commercial service providers to disseminate lectures to a wide audience, and that this cooperation requires new techniques with regard to the registration, validation, and certification of the parties involved, such as professors, service providers, and students. We also propose a technique that can be used in distance education and teleteaching to set up and run online universities. The technique has been named DiRK, an acronym derived from Distributed Registration and Key distribution. It can be used in a conferencing system, such as the MBone, to handle the registration of participants and the distribution of session keys in a decentralized and fully distributed way. We have originally proposed the technique in (Oppliger and Albanese, 1996). At the University of Berne, it is being prototyped in a session registration tool (`srt`) for the MBone. The `srt` will serve as a starting-point to evaluate and further enhance DiRK, as well as to develop similar tools that can be used in distance education and teleteaching to set up and run online universities.

The paper is organized as follows. The idea of online universities is further elaborated in section 2. The terminology that is used to subsequently describe the cryptographic protocols that DiRK is based on is introduced in section 3, and the actual use of DiRK is addressed in section 4. Conclusions are finally drawn in section 5.

2 ONLINE UNIVERSITIES

University lectures are typically held by professors and attended by students. In this cast, the role of the university is twofold:

- on the one hand, the university has to provide an infrastructure that allows professors and students to physically meet in classrooms, and to hold lectures accordingly, and
- on the other hand, the university has to issue official and legally binding documents that certify the educational record of students that attend the lectures and pass final examinations.

It has already been mentioned previously that the idea of distance education and teleteaching is to have networks interconnect the computers located at the professors' and students' sites, and to use the networks' multicast options to have registered students remotely participate in university lectures. In this respect, the cast of the parties involved is not expected to change fundamentally: lectures are still held by professors and attended by students, and universities are still to certify the educational record of students. However, one of the distinguishing features of distance education and teleteaching is the fact that students don't have to physically attend lectures, but can use network links instead. In principle, this offers the possibility to disseminate university lectures to a very wide audience. Note that online universities are limited neither by architectural nor logistical restrictions, and that the size of a lecture's audience is limited only by what makes sense in terms of possible interactions between professors and students.

The idea of distance education and teleteaching is interesting primarily from an economical point of view. From a more practical point of view, however, one problem arises from the fact that universities have neither the network infrastructure nor the clientele to disseminate university lectures to a very wide audience. In this situation, a cooperation with commercial service providers, such as telephone, cable television, and satellite companies, as well as Internet service providers, offers a viable solution that is advantageous to all parties involved:

- online universities can use the service providers' network infrastructures and clientele to disseminate university lectures to a wide audience;
- service providers can enlarge their offerings;
- professors can reach more students;
- students can choose from more lectures to attend.

But in spite of its many advantages, a cooperation with commercial service providers also raises new questions with regard to the way in which the parties involved are to cooperate and interact. In general, there are several possibilities to address these questions, and one possibility that one might think of first is to have an online university cooperate with a constant set of service providers. Following this rather static approach requires the online university to enter into a legal agreement with every single service provider that it cooperates with. On the one hand, the service provider is made responsible for the dissemination of the university lectures, as well as the registration, validation, and certification of the students that attend these lectures, and on the other hand, the university has to accept the registration certificates that are issued by this particular service provider. This approach is yet simple and straightforward, but also lacks the flexibility and dynamics that is useful if not mandatory in distance education and teleteaching. Note that it would be very convenient for a professor to hold a lecture that is accepted by several universities, and to have as many service providers as possible disseminate the lecture. The point is that the more service providers participate in lecture dissemination, the more students are actually able to attend. Ideally, a professor would not have to deal with every single service provider, but would allow service providers to deal with other service providers on his behalf. One point that must be considered with care in this case, however, is the traceability of the corresponding registration, validation, and certification processes.

This paper follows this line of argumentation: It proposes the use of DiRK in distance education and teleteaching to set up and run online universities. DiRK makes it possible to register, validate, and certify professors, students, and service providers in a decentralized and fully distributed way without loosing the traceability of the corresponding processes.

3 TERMINOLOGY

The following terminology is used in this paper:

- P_i is used to refer to professor i ($i \geq 1$).
- L_{ij} is used to refer to lecture j held by professor i ($i, j \geq 1$). More precisely, L_{ij} is used to refer to both a lecture and a multicast channel that is associated with the lecture. Note that the multicast channel may consist of several subchannels, each of them dedicated to a specific purpose, such as voice or video transmission. In this case, it is assumed that DiRK overlays an additional subchannel to handle the registration, validation, and certification of the parties involved.
- s_i is used to refer to student i ($i \geq 1$).
- S_i is used to refer to service provider i ($i \geq 1$).
- U_i is used to refer to online university i ($i \geq 1$).

A protocol specifies the format and relative timing of messages exchanged between communicating parties. A cryptographic protocol is a protocol that uses cryptography, meaning that all or parts of the messages are encrypted on the sender' side and decrypted on the receiver' side.

In the cryptographic protocols that follow, K is used to denote a secret key, whereas (k, k^{-1}) is used to denote a public key pair, which is a pair consisting of a public and a private key. In either case, key subscripts may be used to refer to professors, lectures, students, service providers, and online universities. The term $\{m\}K$ is used to denote a message m that is encrypted with the secret key K. The same key K is used for decryption, so $\{\{m\}K\}K$ equals m. Similarly, the term $\{m\}k$ is used to refer to a message m that is encrypted with the public key k. The message can be decrypted only with the corresponding private key k^{-1}. In a digital signature scheme, the user's private key is used to digitally sign messages, whereas the corresponding public key is used to verify the signatures. In this case, the term $\{m\}k^{-1}$ is used to refer to a digital signature giving message recovery, and the term $\langle m\rangle k^{-1}$ is used to refer to a digital signature with appendix

(ISO/IEC, 1989). Note that in the second case, $\langle m \rangle k^{-1}$ in fact abbreviates a pair that consists of m and $\{h(m)\}k^{-1}$, with h being a collision-resistant one-way hash function.

In accordance with international standardization, the term $X \ll Y \gg$ is used to refer to a certificate that has been issued by X for Y's long-term public key k_Y. This certificate may conform to any standard in use today, such as ITU-T X.509 (ITU-T, 1987) or Pretty Good Privacy (Zimmermann, 1995). In this paper, X typically represents an online university U_i $(i \geq 1)$, whereas Y represents a professor, lecture, student, or service provider.

In addition to the certificates mentioned above, the term $S_m < X, L_{ij} >$ is used to denote a registration certificate that has been issued by service provider S_m for X and lecture L_{ij}. Depending on whether X is a service provider (active participant) S_n or student (passive participant) s_n, $S_m < X, L_{ij} >$ expands to $\langle S_m, S_n, L_{ij}, k_{nij} \rangle k_{mij}^{-1}$ or $\langle S_m, s_n, L_{ij} \rangle k_{mij}^{-1}$. Note that the two types of registration certificates differ only with regard to the public key that is included in the service provider's certificate.

At last but not least, the term $U_m \ll s_n, L_{ij} \gg$ is used to denote a lecture attendence certificate (LAC) for student s_n and lecture L_{ij}. The LAC is to certify that student s_n has attended lecture L_{ij}. It thus expands to $\langle U_m, s_n, L_{ij} \rangle k_{U_m}^{-1}$.

4 DIRK

This section addresses the use of DiRK in distance education and teleteaching to set up and run online universities. The basic idea is to have service providers register as active participants, and students register as passive participants of university lectures. The distinguishing feature of an active participant is the ability to register other (active or passive) participants. Consequently, a service provider can register either other service providers as active participants, or students as passive participants. In either case, a newly registered participant receives a registration certificate that he periodically sends to the multicast channel that is associated with the lecture. The aim of this multicast is to allow other participants to validate the registration of the sending participant. If lecture attendance is a prerequisite for exam qualification, then the registration certificate can be used to request a LAC from an online university that sponsors the lecture. In this case, the student pays a registration fee that is subsequently divided up among the certificate-issuing online university and the service providers that have actually been involved in the registration of the requesting participant.

It is assumed that every online university U_i holds a public key pair $(k_{U_i}, k_{U_i}^{-1})$, of which the public key k_{U_i} is publicly available, and the private key $k_{U_i}^{-1}$ is kept secret. Similarly, it is assumed that every professor P_i and every service provider S_i holds a public key pair $(k_{P_i}, k_{P_i}^{-1})$ and $(k_{S_i}, k_{S_i}^{-1})$ respectively, of which the public keys k_{P_i} and k_{S_i} are publicly available but not trusted by everybody, and the corresponding private keys $k_{P_i}^{-1}$ and $k_{S_i}^{-1}$ are kept secret. If P_i (S_i) wants k_{P_i} (k_{S_i}) to be used, he has to provide a corresponding certificate $U_i \ll X_j \gg$. This certificate is issued by the online university U_i for X_j's public key k_{X_j}, with X_j being either a professor P_j or a service provider S_j.

DiRK provides session initialization, participants registration, registration validation, and session rekeying protocols (Oppliger and Albanese, 1996). With regard to distance education and teleteaching, a conference session refers to a university lecture. The first three protocols thus immediately lead to corresponding lecture initialization, participants registration, and registration validation protocols. The session rekeying protocols are discarded in this paper, and a participants cerification protocol is introduced instead.

4.1 Lecture Initialization Protocol

If a professor P_i wants to hold a lecture L_{ij}, he randomly selects a public key pair $(k_{L_{ij}}, k_{L_{ij}}^{-1})$ and looks for online universities that are willing to sponsor L_{ij}. In this context, the term sponsor is not primarily related to financial donations, but rather to mutual recognition and trust. The fact that university U_k sponsors lecture L_{ij} actually means that U_k recognizes P_i as a professor for L_{ij} on the one hand, and that P_i accepts U_k as a certification authority for L_{ij} on the other hand. Note that a registration for a particular lecture may be coupled with a final examination, and that in this case, P_i and U_k bothagree to cooperate in this matter, too.

As a result of a sponsoring agreement between a sponsoring university U_k and a sponsored professor P_i, U_k provides P_i with both a certificate $U_k \ll P_i \gg$ for P_i's public key k_{P_i}, as well as a certificate $U_k \ll L_{ij} \gg$ for L_{ij}'s public key $k_{L_{ij}}$. Both certificates are commonly referred to as sponsor certificates. Note that there are no general restrictions that address the number of sponsor certificates that a professor may hold for his lectures. As a matter of fact, it is possible and even very likely that a professor has several sponsors for his lectures, and that these sponsors are different for each of his lectures.

If P_i is provided with what he considers a sufficiently large set of sponsor certificates for L_{ij}, he announces the lecture in public. The corresponding lecture announcement consists of P_i's and L_{ij}'s identifiers, the corresponding sets of sponsor certificates, and an appended digital signature that P_i generates with his private key $k_{P_i}^{-1}$. Thus, together with an informal description of L_{ij}, P_i makes publicly available the following lecture announcement message:

$$\langle P_i, L_{ij}, \{U_k \ll P_i \gg\}, \{U_k \ll L_{ij} \gg\}\rangle k_{P_i}^{-1}$$

The lecture announcement message can e.g. be sent to a dedicated multicast channel, or be published on the Word Wide Web (WWW). Anybody who is able to grab the message can then use one of the sponsor certificates in $\{U_k \ll P_i \gg\}$ to extract P_i's public key k_{P_i}, and use k_{P_i} to verify the digital signature that is appended to the lecture announcement accordingly. If the signature is valid, the announcement is considered authentic. In this case, $k_{L_{ij}}$ can be extracted from the corresponding certificate in $\{U_k \ll L_{ij} \gg\}$. Note however that in order to extract k_{P_i} and $k_{L_{ij}}$, at least one university in the corresponding sponsor certificate sets $\{U_k \ll P_i \gg\}$ and $\{U_k \ll L_{ij} \gg\}$ must be trusted. Thus, in order to make the probability to find a trusted university in these sets sufficiently large, P_i has made publicly available all sponsor certificates that he currently holds for L_{ij}.

4.2 Participants Registration Protocol

Having initialized and announced lecture L_{ij} as described above, P_i is notably the first active participant of L_{ij}. It is now up to the service providers to register as active participants, and to the students to register as passive participants. The corresponding participants registration protocols are different in either case:

- If a service provider S_n wants to register as an active participant, he randomly selects a public key pair (k_{nij}, k_{nij}^{-1}) for L_{ij}, and sends a corresponding registration request (REG_REQ) message to the multicast channel that is associated with the lecture. This protocol step can be summarized as follows:

$$S_n \quad \longrightarrow \quad L_{ij} : \text{REG\_REQ}(\langle k_{nij}, U_k \ll S_n \gg \rangle k_{S_n}^{-1})$$

  The REG_REQ message includes the public key k_{nij} and a certificate $U_k \ll S_n \gg$ issued by U_k for S_n's public key k_{S_n}. In order to provide message origin authentication, the message is digitally signed with the corresponding private key $k_{S_n}^{-1}$.
- If a student s_n wants to register as a passive participant, he also sends a REG_REQ message to the multicast channel that is associated with the lecture. In this case, however, the message does neither include a public key nor a certificate. Authentication has to be dealt with locally, and the message therefore is not necessarily signed by s_n.

In either case, the REG_REQ message can be grabbed and confirmed by any active participant S_m that has already registered for L_{ij}. In principle, S_m confirms X (which is either S_n or s_n) by sending a registration confirmation (REG_CONF) message to the multicast channel that is associated with the lecture. This protocol step can be summarized as follows:

$$S_m \quad \longrightarrow \quad L_{ij} : \text{REG\_CONF}(X, S_m < X, L_{ij} >)$$

Obviously, this message includes X's identifier and a registration certificate for X and lecture L_{ij}. It is now up to X to grab the message, and to store it locally.

4.3 Participants Validation Protocol

The basic mechanism that DiRK assigns for participants validation is to have both active and passive participants periodically send a registration validation (REG_VAL) message to the multicast channel that is associated with the session. In the context of distance education and teleteaching, this feature can be used to validate the registration of participating service providers and students.

- If the sending participant is a service provider (active participant) S_n, the REG_VAL message consists of S_n, S_n's registration certificate $S_m < S_n, L_{ij} >$, and a timestamp T that is digitally signed with k_{nij}^{-1}. This protocol step can be summarized as follows:

$$S_n \quad \longrightarrow \quad L_{ij} : \text{REG\_VAL}(S_n, S_m < S_n, L_{ij} >, \{T\} k_{nij}^{-1})$$

  Note that the private key k_{nij}^{-1} is the one that S_n has originally selected for his registration.
- If the sending participant is a student (passive participant), the REG_VAL message consists of s_n and s_n's registration certificate $S_m < s_n, L_{ij} >$. This protocol step can be summarized as follows:

$$s_n \longrightarrow L_{ij} : \text{REG\_VAL}(s_n, S_m < s_n, L_{ij} >)$$

In order to validate the registration of a particular participant, one has to wait until this participant sends a REG_VAL message to the multicast channel that is associated with the lecture. This message includes a registration certificate that is digitally signed with the private key of the active participant that has registered the participant. If the validating participant is equipped with the corresponding public key, he can verify the digital signature and validate the registration certificate accordingly. However, if the validating participant is not equipped with the public key, he must extract it from the REG_VAL message that the corresponding active participant sends to the multicast channel. This registration validation trace back continues until one reaches a registration certificate that is digitally signed with $k_{L_{ij}}^{-1}$, which is the master key of L_{ij}. Note that the corresponding public key $k_{L_{ij}}$ has been announced in public, and is thus assumed to be authentic. Also note that the participants validation mechanism that DiRK deploys requires clocks to be globally synchronized.

4.4 Participants Certification Protocol

In general, students register for a university lecture to get admission for a final examination. It is assumed that a similar approach must be adapted for distance education and teleteaching, too. More precisely, it is assumed that a student must be able to receive a lecture attendance certificate (LAC) from an online university that sponsors the lecture, and that a LAC is a prerequisite to get admission for a final examination. It is important to note that a registered participant already has a certificate, namely the registration certificate, but that this certificate is valid only for the lifetime of a lecture. Because the registration certificate becomes obsolete after the lecture's termination, a procedure is required that allows a student to turn his registration certificate into a long-term LAC.

If a student s_n wants to turn his registration certificate $S_m < s_n, L_{ij} >$ into a LAC for L_{ij}, he contacts one of the lecture sponsoring online universities U_k by sending a LAC request (LAC_REQ) message that includes his registration certificate. U_k has stored and maintained the participants registration tree (PRT) for L_{ij} during the lifetime of the lecture, and can thus use this tree to validate the registration certificate of s_n. If the certificate is valid, U_k returns a LAC confirmation (LAC_CONF) message that includes the requested LAC. Thus, the participants certification protocol can be summarized as follows:

$$\begin{array}{lcl} 1: s_n & \longrightarrow & U_k : \text{LAC\_REQ}(S_m < s_n, L_{ij} >) \\ 2: U_k & \longrightarrow & s_n \ : \text{LAC\_CONF}(U_k \ll s_n, L_{ij} \gg) \end{array}$$

Note that in this protocol, the messages are not sent to the multicast channel that is associated with a lecture, but directly to U_k and s_n instead. The point is that the requests may be sent after the lecture has terminated. As a matter of fact, the multicast channel may have ceased to exist or be overlaid by another conference session. Also note that s_n pays a registration fee to get a LAC, and that this fee may be divided up among the certificate-issuing university U_k and the service providers that have actually participated in the registration of the requesting participant. Again, U_k can use the PRT for L_{ij} to determine these service providers.

5 CONCLUSIONS

In conclusion, we have focused on the role of universities in distance education and teleteaching. We have argued that universities have to cooperate with commercial service providers to disseminate lectures to a wide audience, and that this cooperation requires new techniques with regard to the registration, validation, and certification of the parties involved, such as professors, service providers, and students. We have also proposed a technique that can be used in distance education and teleteaching to set up and run online universities. The technique has been named DiRK, an acronym derived from Distributed Registration and Key distribution. It can be used in a conferencing system, such as the Internet Multicast Backbone (MBone), to handle the registration of participants and the distribution of session keys in a decentralized and fully distributed way. It is assumed that this approach better fits the requirements of MBone conferencing in general, and the use of MBone conferencing for distance education and teleteaching in particular. However, there are some modifications and extensions necessary to adapt DiRK to distance education and teleteaching. The most important extension is obviously related to the online universities that in fact act as trusted third parties. It is up to the online universities that sponsor a lecture to build the participants registration tree (PRT) for that particular lecture, and to validate each participant who requests a lecture attendence certificate (LAC).

At the University of Berne, DiRK is being prototyped in a session registration tool (`srt`) for the MBone. The `srt` will be released for public scrunity later this year. It will serve as a staring-point to evaluate and further enhance DiRK, as well as to develop similar tools that can be used in distance education and teleteaching to set up and run online universities. Further information on DiRK, the `srt`, and applications thereof can be found on the World Wide Web (WWW) by following the Uniform Resource Locator (URL) `http://iamwww.unibe.ch/~oppliger/Research/dirk.html`.

ACKNOWLEDGMENTS

The authors would like to thank Patrick Frey, Boris Bremer, Gary S. Williams, and two anonymous referees for their review activities, as well as Prof. Dr. Dieter Hogrefe for his encouragement and support.

REFERENCES

Deering, S. and Cheriton, D. (1985) Host Groups: A Multicast Extension to the Internet Protocol. RFC 966.

Deering, S. (1989) Host Extensions for IP Multicast. RFC 1112.

Deering, S. and Cheriton, D. (1990) Multicast Routing in Datagram Internetworks and Extended LANs. *ACM Transactions on Computer Systems*, 8(2), 85-110.

Deering, S. (1991) Multicast Routing in a Datagram Internetwork. Ph.D. thesis, Stanford University.

Eriksson, H. (1994) MBONE: The Multicast Backbone. *Communications of the ACM*, 37(8), 54-60.

Macedonia, M. and Brutzman, D. (1994) MBone Provides Audio and Video Across the Internet. *IEEE Computer*, 27, 30-36.

Kumar, V. (1996) *MBone: Interactive Multimedia on the Internet.* New Riders Publishing, Indianapolis, IN.

Oppliger, R. and Albanese, A. (1996) Distributed registration and key distribution (DiRK), in *12th International Conference on Information Security (IFIP SEC '96).*

ISO/IEC 7498-2 (1989) Information Processing Systems — Open Systems Interconnection Reference Model — Part 2: Security Architecture.

ITU-T X.509 (1987) The Directory — Authentication Framework.

Zimmermann, P. (1995) *The Official PGP User's Guide.* The MIT Press, Cambridge, MA.

Zimmermann, P. (1995) *PGP Source Code and Internals.* The MIT Press, Cambridge, MA.

BIOGRAPHY

Rolf Oppliger studied computer science, mathematics, and economics at the University of Berne, Switzerland, where he received his M.Sc. and Ph.D. degrees both in computer science in 1991, and 1993 respecively. The focus of his current research activities is on network security in general, and Internet security in particular. He's with the Swiss Federal Office of Information Technology and Systems (BFI) and the University of Berne. He's a member of the Swiss Informaticians Society (SI) and its working group on security, the ACM, and the IEEE Computer Society. He also serves as current vice-chair of IFIP TC 11/WG 4 on network security.

Martin Bracher has studied computer science, mathematics, and physics at the University of Berne, Switzerland. With regard to his Master thesis, he currently focuses on DiRK and its application in distance education and teleteaching to set up and run online universities.

Andres Albanese holds a Ph.D. degree in electrical engineering from Stanford University, a M.Sc. in the same field from the University of Texas at Austin, and an "Ingeniero Electricista" degree from Universidad Central de Venezuela. He has been working in the areas of fiber optics, broadband communications, and high-speed computer networks for several years. His present research interest are in group multimedia applications for global networks. He has published widely and holds 13 patents. He's currently vice president at the International Computer Science Institute (ICSI) in Berkeley, California.