

Internet2 PKI Research and Development Laboratory

Principal Investigator

Dr Roy Campbell, University of Illinois, CS Department

Co-Principal Investigators

Randy Butler, National Center for Supercomputing Applications

*Edward Krol, University of Illinois Communications and Computing Services
Organization*

1. Introduction

The rapid growth of high-speed networks, advances in global interconnectivity, increased frequency of computer-based collaborations, and development and deployment of advance applications require new approaches to information security. These advanced services, networks and protocols must be built on a secure foundation. Modern networks are dynamic; they change frequently as components are added and deleted. The security foundation for tomorrow's Internet should tolerate the dynamic nature of these networks by incorporating a dynamic view of security. The increasing level of services provided by high-speed networks enables computational grids and computer-based collaborations. New associations between academic institutions and between academia and industry require security solutions that protect each party's interests, interoperate with site-specific implementations and are scalable to the national and international level. Using asymmetric cryptography technology in advance global networks on a massive scale while offering dynamism to fulfill advanced application and collaboration needs requires a more autonomous, scalable, interoperable and agile PKI.

The University of Illinois Urbana Campus (UIUC) has a long tradition of computer science research that dates back even before the ILLIAC project in 1949. With this proposal, we propose collaboration among three campus organizations to enhance PKI research and deployment efforts both within and external to the University. Our team includes Dr Roy Campbell from Computer Science (CS), Randy Butler from the National Center for Supercomputing Applications (NCSA), and Ed Krol from the Computing and Communications Services Organization (CCSO). This collaboration represents a unique opportunity for the I2 community to leverage the rich environment of security research, national scale technology transition, and eventual deployment into the UIUC campus infrastructure.

2. Partnership

We propose to leverage the key strengths and experiences of these three University of Illinois partners whose history of cooperation forms a basis for this proposal to adapt new security concepts to the production environment and provide necessary feedback to the developers.

The UIUC Computer Science Department is ranked in the top 5 CS departments nation wide, and its security lab is one of 14 NSA approved Center for Excellence in Education in Information Assurance [Nsa]. Campbell's team researches aspects of security that span the range from authentication systems to intrusion detection and adaptive response. The Internet2 PKI laboratory will be housed in the Computer Science Department and managed by Campbell. This linkage gives CS Department researchers, under-graduates and graduate students access to the laboratory for research and prototyping. We believe that much ongoing UIUC research can be extended and deployed to support a more interoperable, agile and scalable PKI that meets the demands of grids, advance applications and high-speed networks.

NCSA is a National Science Foundation funded super-computing center that has international recognition for the support of high performance computing applications researchers and grid based computing. The major focus of the National Computational Science Alliance (Alliance) program [All] led by NCSA is the development and deployment of advance grid infrastructures. As part of this effort the Alliance has developed and deployed a PKI authentication system [But99] that provides authentication to compute resources and services within the Alliance Virtual Machine Room (VMR) [Vmr]. The Alliance PKI solution layers on top of site-specific authentication systems including Kerberos. NCSA will work closely with Computer Science and CCSO on prototype development, testing, and packaging. NCSA will deploy promising

prototypes into the Alliance Virtual Machine Room (VMR), which today includes resources at NCSA, Boston University, University of Wisconsin, Albuquerque High Performance Computing Center, University of Kentucky Computing Center and the Maui High Performance Computing Center. This national scale grid offers a tremendous technology transfer opportunity that exposes 6 highly diverse sites around country and their academic researchers, students, and support personnel. Key to our efforts will be Alliance grid applications whose requirements will serve as a driver for all of our efforts.

NCSA and its Alliance partners have extensive experience in dealing with computer systems and human factors. We will work with Tom DeFanti at EVL, and Polly Baker at NCSA to aid us both in 1) understanding human factor issues and 2) in crafting effective strategies.

CCSO is the academic computing and networking infrastructure provider to the Urbana campus of the University. It provides a Kerberos infrastructure for production authentication and authorization services for the campus community and maintains the only combined database of all University affiliated people. This database is used for authorization by many academic and administrative applications on campus. CCSO is the distribution point on campus for commercial grade X.509 certificates.

CCSO advocates PKI as a major technology for the provision of future campus authentication and authorization services. It has been tracking PKI initiatives and planning its integration with legacy systems on campus. Part of this has been working within the University administration to integrate the University's PKI efforts with that of the state and working with a Digital Library Initiative PKI test project. CCSO is therefore a natural way within the community to provide production experience to the Department of Computer Science and NCSA.

Project management will be shared among the three principals with Campbell fulfilling the role of Principal Investigator and Butler and Krol in Co-PI roles. The team will establish bi-weekly meetings to coordinate efforts. Whenever possible, team members will work across organizations. Developers will work with deployment teams, and deployment personnel will aid in prototype development and testing.

We anticipate positive interactions with the Internet2 program management team and their corporate, government, and academic partners. Regular presentations on research efforts, prototyping, and deployment successes and failures will be reported at I2 meetings.

3. Existing Research Programs

There are a number of security related research programs underway now, what follows is a sampling of those that are most directly related to the Internet2 PKI research agenda.

Dynamic Interoperability between Infrastructures. This effort is developing techniques for dynamic interoperability between different *Object Request Brokers* (ORBs) in CORBA [Omg96]. We utilize a *role-based access control* (RBAC) model that has proven flexible, policy-neutral and an effective alternative to traditional access control techniques. To allow different domains to interoperate securely, we propose and have implemented the IRBAC 2000 (*Interoperable RBAC*) model [Kap00]. This model was integrated with JacORB a Java-based ORB [Bro97] that we are using as a test bed for interoperability and mutual recognition research. To facilitate management of IRBAC and maintaining the interoperability constraints among autonomous components, we proposed the A-IRBAC 2000 (*Administrative IRBAC*) [Muh00a].

SESAME: A Combination of Kerberos and Public Key Technologies. SESAME (*A Secure European System for Applications in a Multi-vendor Environment*) [Ses], [Mcm95] and [Kai94] extends Kerberos with additional services. SESAME supports asymmetric cryptography and uses PKI while preserving compatibility with Kerberos. Additionally, SESAME has controlled delegation of privileges (stored in special data structures called PACs or *Privileged Attribute Certificates*) so that targets can proxy their client's privileges to call other services on their behalf. Our research in the Nephilim project developed UIUC SESAME, a portable version of SESAME implemented fully in Java [Nep] and [Cha99]. UIUC SESAME services are accessed through the GSS-API and the extended GSS-API that accommodates security attributes [Muh99]. A CORBA security level 2 and SecIOP are implemented with UIUC SESAME.

Tiny UIUC SESAME [Muh00b] is a lightweight subset of SESAME customized for use on handheld and consumer devices. It is capable of dynamically loading different security components and protocols on the fly, allowing it to adapt to environments with scarce resources with the potential to evolve once more resources become available.

Active Network Security. The Seraphim research project [Ser] is constructing a security architecture that recursively installs and supports the secure deployment of new security mechanisms. Security policies may be installed dynamically on routers belonging to different domains. For securing Active Networks, we utilize *active* capabilities, which are capsules that incorporate security code like a security policy or access control [Cam00]. Further, we are investigating the construction of an Active Caching framework for Active Capabilities. Smart caching of reusable Active Capabilities has proven to improve performance significantly.

Security Protocols. Furthermore, we have implemented SecIOP and CORBA level 2 security services completely in Java and integrated it with JacORB [Bro97] as part of the Malakim research project [Mal]. Additionally, since many of the ongoing research projects require a PKI, we have developed our own experimental PKI in Java [Con00].

Center for Excellence in Information Assurance. The Computer Science Department is an NSA approved center for excellence in information assurance education [Nsa] and [Srr]. Through various security research projects, they have contact with DARPA, NSA, CISCO, NAI, SRI, ARGUS, Motorola and several schools.

4. Leverage

Leverage from numerous other grants and efforts will be applied if our proposal is successful. The Computer Science Department Laboratory has numerous students that will fully utilize such a facility. NCSA and the Alliance will devote a minimum 50% of a senior developer to work specifically on PKI and authorization services. NCSA will also leverage its and its Alliance partner experience in dealing of human factors. CCSO will leverage campus PKI efforts as well. In addition we plan to aggressively pursue funding for new research, prototype development and deployment. NCSA's Industrial Partners have expressed a keen interest in PKI related technologies and in providing additional funding should the University of Illinois win this award.

In summary there is great potential to leverage this activity with current efforts and we anticipate additional funding opportunities from sources.

5. Investigators

Roy Campbell received his Honors B.S. Degree in Mathematics, with a Minor in Physics from the University of Sussex in 1969 and his M.S. and Ph.D. Degrees in Computer Science from the University of Newcastle upon Tyne in 1972 and 1976, respectively. In 1976 he joined the faculty of the University of Illinois, where he is currently a Full Professor of Computer Science. During the past twenty-four years he has supervised the completion of twenty-nine Ph.D. dissertations and over ninety-eight M.S. theses. He is the author of over one hundred and sixty research papers on security, programming languages, software engineering, operating systems, distributed systems, and networking. His past research accomplishments include path expressions, various deadline and error recovery mechanisms for asynchronous processes, the Choices object-oriented operating system, the VDP protocols for streaming audio and video used by Vosaic LLC, dynamic TAO a reconfigurable version of the TAO ORB, 2K a distributed object operating system, UIUC Sesame a Java implementation of Sesame security protocols, and the Seraphim active security policies. His current research projects include smart spaces, security interoperability, security policies and active security in active networks. He is an active participant in the department's distance learning program. Professor Campbell is director of the NSA designated University of Illinois Center of Academic Excellence in Information Assurance Education.

Randy Butler has worked for the National Center for Supercomputing Applications (NCSA) since 1987. He has worked in and managed teams with responsibilities for the support and advancement of wide area and local area networking, security of center wide computer systems, and grid infrastructure design and deployment. Butler is Division Director for the Alliance Computational Environment and Security division, a team that is funded by the NSF, NASA, and DOE with a focus on development and deployment of grid infrastructures. Key experiences related to this proposal include active participation as a member of the vBNS Network Technical Committee and management of the NCSA and Alliance Secure Authentication Projects

Currently Butler is co-lead for the National Computational Science Alliance (Alliance) efforts to build and deploy the VMR, and leads the Security Working Group [Vpki], and their efforts to deploy PKI authentication. Butler and his team work closely with the Globus [Glo] project on the development of grid infrastructure. In addition Butler is Co-Chair of the Grid Forum Security Working Group [GF].

Edward Krol is the area director within CCSO responsible for the department's involvement in security research, development, and deployment. Ed has a BS in Computer Science from the University of Illinois and has been involved with the Internet since 1985, when he was the project manager for the original 56kb NSFnet. He has authored three books, three RFC's, numerous articles about Internet usage and given a variety of lectures and interviews about the Internet. Recently, he taught a variety of short courses on the user end of PKI (e.g. use of digital signatures, digital contracts, key management issues, PKI safety).

6. Conclusion

We have proposed directions for crafting a more scalable, interoperable and agile PKI to manage the massive-scale use of asymmetric cryptography in tomorrow's advance networks and applications. Our combined experience provides an expert team to develop practical security solutions for distributed systems, active networks, active spaces, and ubiquitous computing devices. NCSA and CCSO give our effort a natural mechanism, complete with critical feedback and application users, to test, evaluate and deploy successful PKI prototypes both at the campus and national scale. Thus, we have the expertise and sufficient intellectual resources to be designated as one of two Internet2 PKI laboratories.

Of course this is a preliminary discussion. If we are selected as a source, we will prepare a formal proposal with deliverables and cost information at that time

7. References

- [All] <http://www.ncsa.uiuc.edu/>
- [Bro97] G. Brose, "*JacORB – a Java Object Request Broker*", technical report, April 1997.
- [Cam00] R. Campbell, Z. Liu, D. Mickunas, P. Naldurg, and S. Yi. *Seraphim: Dynamic interoperable security architecture for active networks*, IEEE OPENARCH 2000, Tel-Aviv, March 2000.
- [Cha99] M. Chandak, "*U-SESAME: Achieving a Portable Authentication, Access Control, and Delegation Protocol*", Masters Thesis at Department of Computer Science, University of Illinois at Urbana-Champaign, 1999.
- [Con00] R. Connolly, "*Key Management Software Development*", technical report, 2000.
- [Gf] <http://www.gridforum.org/>
- [Glo] <http://www.globus.org>
- [Kai94] P. Kaijser, T. Parker, and D. Pinkas, "*SESAME: The Solution to Security for Open Distributed Systems*", Computer Communications, 17(7):501-518, July '94
- [Kap00] Apu Kapadia, Jalal Al-Muhtadi, R. Campbell, D. Mickunas, *IRBAC 2000: Secure Interoperability Using Dynamic Role Translation*, The 1st International Conference on Internet Computing, June 26th - 29th, 2000, Monte Carlo Resort, Las Vegas, Nevada, USA.
- [Mal] Malakim Research Project page: <http://choices.cs.uiuc.edu/Security/malakim>
- [Mcm95] P. McMahon, "*SESAME V2 Public Key and Authorisation Extensions to Kerberos*", in proceedings of the symposium on Network and Distributed System Security, pages 114-131, February 1995.
- [Muh00a] J. Al-Muhtadi, A. Kapadia, R. Campbell, D. Mickunas, "*The A-IRBAC 2000 Model: Administrative Interoperable Role-Based Access Control*", submitted to the 7th ACM Conference on Computer and Communication Security, Athens, Greece, 2000.
- [Muh00b] J. Al-Muhtadi, M. Anand, R. Campbell, D. Mickunas, "*Secure Smart Homes Using Jini and UIUC SESAME*", submitted to the Annual Computer Security Application Conference, New Orleans, Louisiana, USA, 2000.
- [Muh99] J. Al-Muhtadi, "*SGSS-API Documentation and Developer's Guide*", Technical report, 1999.
- [Nep] Nephilim Research Project page: <http://choices.cs.uiuc.edu/Security/nephilim>
- [Nsa] <http://www.nsa.gov:8080/isso/programs/coeiae/index.htm>
- [Omg96] Object Management Group, *CORBA 2.3.1/IIOP Specifications*, technical report, 1996.
- [Ser] Seraphim Research Project page: <http://choices.cs.uiuc.edu/Security/seraphim>
- [Ses] SESAME. The SESAME homepage <https://www.cosic.esat.kuleuven.ac.be/sesame/>
- [Srr] University of Illinois at Urbana-Champaign Security Research Resource Link: <http://ciae.cs.uiuc.edu/>
- [But99] Design and Deployment of a National-Scale Authentication Infrastructure. R. Butler, D. Engert, I. Foster, C. Kesselman, S. Tuecke, J. Volmer, V. Welch. (Submitting).
- [Vpki] <http://www.ncsa.uiuc.edu/SCD/Alliance/VMR/Security.html>
- [Vmr] <http://www.ncsa.uiuc.edu/SCD/Alliance/VMR>