Contribution to the DOE National Collaboratories Program Investigator's Meeting, August 10-12 at ANL.

Cryptographic Foundation for Collaboration and Grid Technologies

Deborah Agarwal, Olivier Chevassut, and Frank Siebenlist

Abstract: Collaboration and Grid systems are networking technologies that enable complex interactions among computational and data resources. If these systems are to be successful and widely deployed in production computing environments, they need to be enhanced with proper cryptographic mechanisms. The present paper clearly identifies the necessary mechanisms in securing the collaboration systems, and the research and development steps to carry out to construct them.

Secure communication for collaboration and Grid systems needs to support many important features currently missing in the existing security technologies. Modifying these existing security technologies is risky and complicated since even minor modifications change the security model and the assumptions upon which the technologies were built. While the security goals (i.e. confidentiality, integrity, authentication, …) remain the same, new foundations need to be laid down in order to construct and develop cryptographic mechanisms that would support these goals for the collaboration and Grid systems. Fortunately, modern cryptography can help achieve this aim.

While modern cryptography has the potential to provide an evolutionary improvement to the security of collaboration and Grid systems, there are several steps to carry out before this vision can become a reality. The immediate need in securing these systems is the following:

- methods for authentication based on a Public-Key Infrastructure (PKI)
- methods for authentication based on One-Time Passwords (OTP)
- methods for exchange of a session key between two entities
- methods for exchange of a session key within the context of a group

The first step to constructing these methods is to clearly define the problem space. This means specifying in detail the requirements of authentication and key exchange for collaboration and Grid systems. For authentication we need to consider supporting various types of identity tokens (e.g. one time passwords and PKI certificates), and examine both end-to-end and intermediate node authentication. Password-based authentication is to enable clients with particular storage, computation, mobility, and bandwidth requirements (e.g., diskless base stations, cellular phones, pocket PCs) to identify themselves and exchange a session key with a server. One-time password (OTP) is a necessary future requirement to use DOE resources so it is essential that Grid Services can utilize OTP. The Globus Toolkit, for example, do not currently support

authentication based on OTP. For key exchange we need to look into establishing and refreshing session keys in two-party and group settings.

The second step in this process is to design and develop cryptographic methods that are not only efficient but also "*provably-secure*". Modern cryptography is the subtle art of designing and studying mathematical objects—called cryptographic methods—for entity authentication, confidentiality, and integrity. Its theoretical concepts go back to Diffie and Hellman in 1976, and the first public-key cryptosystem—the RSA cryptosystem—was proposed two years later by Rivest, Shamir, and Adelman. Since the publication of this algorithm, cryptographic methods have found a systematic and rigorous treatment in the framework of modern cryptography--often referred to as the science of "*provable-security*". This science provides a theoretical foundation on which to evaluate cryptographic methods that purport to solve them, and build cryptographic methods in which we can have confidence.

The final step is to make sure that once used by the security infrastructure supporting collaboration and Grid-enabled applications these methods retain their "*provable-secure*" features. A misconception about "*provable-security*" is that, even though it allows us to avoid many security flaws in designing a protocol, security can sometimes be compromised if the protocols are implemented and operated incorrectly. Cryptographers indeed see cryptographic methods as abstract mathematical objects while engineers must deal with them as concrete objects to be coded into a program. Because implementers are not cryptographers, they often overlook critical details. This fact combined with the incomprehensible nature of cryptographic codes, often result in flaws that are discovered and corrected only several years later. In practice, these implementation flaws are avoided by a thoroughly analyze of the cryptographic toolkit in order to give security arguments we can have confidence in. This is also achieved by providing detailed specifications of the implementation which can be used as evidence of the correctness of the toolkit, and by providing detailed implementation guidelines for the use of the cryptographic methods.

In conclusion, establishing a solid cryptographic foundation for collaboration and Grid systems involves analyzing the problem space, constructing cryptographic methods, and developing a "*provably-secure*" cryptographic toolkit.