Chapter 22
Security and Trust in a Global Research Infrastructure

Jens Jensen
Science and Technology Facilities Council, UK

David L. Groep
National Institute for Subatomic Physics, The Netherlands

ABSTRACT

Modern science increasingly depends on international collaborations. Large instruments are expensive and have to be funded by several countries, and they generate very large volumes of data that must be archived and analysed. Scientific research infrastructures, e-Infrastructures, or cyber infrastructures support these collaborations and many others. In this chapter we look at the issue of trust for such infrastructures, particularly when scaling up from a small one. This growth can be "natural," as more researchers are added, but can also be dramatic if whole new communities are added, possibly with different requirements. Our focus is on authentication, since for most realistic infrastructures, authentication is the foundation upon which further security is built. Our aim has been to focus on real-life experiences and examples, distilling them into practical advice.

INTRODUCTION

Science and research are increasingly becoming global: where researchers previously only communicated by email, they now collaborate closely across national boundaries using supporting e-infrastructures or cyber infrastructures. For a small group of researchers sharing few resources, it is fairly easy to establish a trusted relationship between the users and the resources: for example by getting everyone together in the same room and hand out passwords. It becomes much more difficult to establish and maintain these relationships when the group grows, when many other resources are added, or when the resources need higher levels of protection (e.g. if accessing sensitive data or controlling an instrument.)

This chapter looks at the challenges in scaling up from small infrastructures to large ones. Our emphasis is more on human processes than technology: ultimately trust is between humans, supported by processes and policies; the role of

DOI: 10.4018/978-1-61350-116-0.ch022

technology is to *mediate* the trust in a *distributed* infrastructure. Purely technological proposals for scaling to larger infrastructures have been studied elsewhere, e.g. identity based encryption (Shamir, 1984), or more recently, building PKI (Public Key Infrastructure) with secure "mediators" (Boneh, 2001; Vanrenen, Smith, & Marchesini, 2005) these and others will not be pursued here. When we need to cover aspects of commonly used technology, we do so to assess how much it can help scale the trust infrastructure.

In addition to being "sociological," our overall aim is highly practical: we focus on processes and technology which are known to work on a global scale.

A high level outline of this chapter is as follows:

1. Introduction
2. A discussion of the participants and their trust relationships.
3. Investigating scalability issues.
4. A discussion of issues and controversies.
5. Practical advice for people seeking to scale a trust infrastructure.
6. Future directions.

PARTICIPANTS AND SECURITY GOALS

Let us first look at the simplest case mentioned in the introduction: a group of users accessing a shared resource. They may use a password to authenticate to the resource, and the password can be reset using their email address if they forget it. e-Commerce (see Example 1 and Anderson (2008, sec. 10.5) for further discussion) is similar. In both cases, we have a group of users who interact only with the resource, not with each other.

Example 1. Doohickey Inc sells widgets on the Internet.

Alice signs up and gets a password mailed to her. She uses the password to log in and buy widgets using her credit card. Each time Alice logs in, she sees her account and can track her order. If she forgets her password, she clicks a reset button and a new (possibly temporary) password is sent to her email account.

The need for security is not high because the account is used mainly for presentation purposes (unless the server remembers her credit card details and no additional checks are performed!)

Security in this case appears to be symmetric, being based on a secret shared between the user and the resource, namely the password[1]. (The *trust relationship* need not be symmetric, though, as we shall see in sections *Resources* and *Scalability of the Infrastructure*.)

When we start adding other resources, the simple model is normally repeated: for each resource, users will have to register again with a password. Of course they may choose to use the same password with all resources, which will make it easier for them to remember, but if the password is then compromised, potentially all resources are at risk (or rather, the user's accounts with all the resources are at risk). It is worth noting that the resources have no way of knowing this: they can perform simple checks of the strengths of the password, and maybe weigh the risk of the complexity of the password with the likelihood of the user having written it down, but they have no way of knowing whether the user has used the password elsewhere.

The apparent symmetry is then broken: a resource can manage hundreds of thousands of users because a database can easily maintain the shared secret and other account data for all users, but a user cannot easily maintain a hundred thousand resource accounts except by reusing passwords or using a password manager of their own – which in turn poses a "all eggs in one basket" problem.

This situation is not necessarily a bad one for individual users: it may be unlikely that things go wrong, although it takes a lot of work to fix it