

The Virtual Secretary Project: The Problem Definition

G. Hartvigsen¹

Department of Computer Science,
Institute of Mathematical and Physical Sciences,
University of Tromsø, N-9037 Tromsø, Norway

01.09.95

Virtual Secretary Working Report 95-01

Abstract

The Virtual Secretary project focuses on the construction of an environment for secure software agents. As a research vehicle, i.e., to enable full-scale experiments in realistic settings, some major secretarial tasks have been chosen. Our environment for secure software agents will include propagation mechanisms, mechanisms for authentication and control, and common user software. A key element in this environment will be the propagation of the Virtual Secretary's user model (i.e., non-executable control software). This report presents the problem definition for the Virtual Secretary project, specifies major problems and sketches a possible approach to the problem.

1 Background

In the last decade, mobile computers have introduced new problems and challenges to distributed systems and computer networks. Through wide area networks, computations can be distributed to and completed on computers in different geographical locations. Information stored in a global network can be fetched or updated in a few seconds. Mobile computers could connect to the network and services from nearly any geographical area in the world. In addition, the variation of computer usage will continue to increase – ubiquitous computing would affect the way of using computers for most user groups.

These opportunities demand tools and system paradigms that exploit their capabilities and reduce their problems. One such tool could be a software agent, i.e., worm-like programs, which effectively use the network and remote processing sites. A key issue in the utilization of a network of worm-like programs is the security. Most people are very sceptics toward the idea of letting worm-like programs enter their own secure environment. Especially horrifying is the idea of not being able to control what kind of operation

1. This work was partly supported by the Research Council of Norway, grant no. 100425/410.

the “intruder” is allowed to do. To construct more than a toy program for an open research network, security issues need to be seriously treated. Our approach will be to exclude as many security problems as possible.

This paper specifies the problem definition of the Virtual Secretary project and outlines the project’s approach.

2 Problem definition

The problem definition for the Virtual Secretary project is:

How can a secure environment for software agents for secretarial tasks in a global network be constructed?

The problem definition is based on the assumption that security can be improved through the transmission of only a model of the user (i.e., user model) which specifies the user’s current task and his/her most reasonable way of behave when a specified problem may occur. This approach implies that no executable code is transferred. The assumption requires that a general version of the Virtual Secretary already exist on the remote host. If not, given that security can be guaranteed, minimum code should be transferred. This means that the problem definition can be divided into the following subproblems:

1. How can a user model for propagation of processes (i.e., mobile agents) be constructed?
2. What are the security issues that have to be met in order to propagate user models in a secure way?
3. How can a control language for propagation of agents and tasks through user models be designed?
4. Based on the results from 1-3; How can a virtual secretary that handles (i) file retrieval from remote hosts in a global network, (ii) electronic mail, and (iii) propagation of the user’s environment, be constructed?

The tasks in point 4 do only involve the user’s Virtual Secretary (located on accessible hosts in the network), and not contact with other users’ Virtual Secretaries.

The file retrieval tool will be used when the user wants a file or several files from one of his workstations (file servers) given that he does not remember the file name and possibly also the name of the workstation(s).

The mail handling tool includes automatic forward of important mail, e.g., filters distribution lists and bogus mail. A scenario would be that the Virtual Secretary propagates a couple of hours ahead of the user and install his wanted features on the remote host.

Propagation of the user’s environment involves copying the user environment to the new host. This includes the graphical user interface with the same menus, access to (as many as possible of) the user’s applications, etc.

3 Approach

The ordinary way to deal with security problems is to adopt a *security policy* that defines appropriate levels of security for the system's activities, and enforced by a set of security mechanisms. This approach implies no additional precautions to meet new security challenges from software agents. The problem of this approach with respect to software agents is that we do not have any guarantees for what might happen when an active program is allowed to enter the system.

Another approach to the construction of software agents, to be taken by the Virtual Secretary project, is to exclude as many security risks as possible through the adoption of a different architectural approach to system design, especially the propagation scheme. In this approach an environment for secure software agents is created, including:

- propagation mechanisms,
- authentication and control mechanisms, and
- common user software.

To reduce the security problem we have chosen to propagate passive code in the form of user models. This approach is based on the assumption that a Virtual Secretary body process (i.e., a Virtual Secretary excluding a user model) exists on the target host, and that a description of this process is well known. A user model contains a description of the mission, the user (including the user's history, current tasks, preferences, etc.), administrative and control data, etc. The user model, or, if appropriate, part of the user model is initialized by the body process on the remote host to continue its mission. Authentication and control mechanisms ensure that traditional security issues such as authentication of principals, integrity of communication, confidentiality, etc., are obtained.

Common user software, i.e., that all users may get a complete description of the Virtual Secretary process and use the secretary himself/herself, de-mystifies the software. The description of the Virtual Secretary's tasks will be available for all users. When a user needs to send its Virtual Secretary on a mission in the network, the propagation will take place through the copying of the user model or part of the user model.

Another feature we expect to gain from the proposed architecture is reduced network costs involved in the process propagation. Given that the propagation is necessary, our approach is expected to reduce the amount of software necessary to be transmitted in order to propagate the process. One approach is to propagate part of the program, another to transfer the task description necessary to continue the process on a remote host. The latter may be conducted through the development of a user model (as the user model known from adaptive systems, e.g., adaptive user interfaces). In this way, a propagation of a process requires that a copy of the process exist on the remote host. Then the propagation will be analog to a "brain transplantation."

Even though the network bandwidth in wireless networks increases rapidly, still the question of power consumption (i.e., battery use) strongly indicates that the use of wireless network interface in mobile computers should be minimized. We expect that our approach also will reduce the network operations.