Independent Research and Development Proposal

Small Microprocessor-Based Verified Network Security Control Unit

John Nagle

FACC / Palo Alto

Summary

It is proposed to explore a new technique of developing small, highly reliable/secure microcomputer applications. The Scientific Research Laboratory at Ford Engineering and Research in Dearborn has developed a new computer language called Pascal-F. This language is designed for small real-time applications, particulary vehicle engine control. Over the past two years, a computer program verification system for this Pascal-F language has been developed at WDL under contract to Ford Motor. This system is intended for use in discovering possible errors in the engine control computer programs used in Ford cars. The language and the verification system are not restricted to this application, however, and we propose to try it out on a problem relevant to WDL and DoD needs.

The candidate application should be a small (~1500 lines of code) stand-alone microcomputer program. We propose to select a suitable application by consulting with the WDL business operations and finding a problem amenable to this treatment. A possible application would be a network protection unit capable of protecting a packet-switched network from certain kinds of unauthorized access. We call this application the Security Control Unit. The remainder of this proposal is written on the assumption that this will be the application selected for implementation.

Building secure software systems is known to be very difficult. There exist no software systems validated to the highest level of approval defined by the DoD Computer Security Center at NSA. This one could be the first. By using tools developed on another contract, and undertaking to do a useful but very limited task, we can build a small, special-purpose secure system at moderate cost. This technology may be directly usable on future contracts related to the DDN-I network (the common packet network under construction for DoD, replacing Autodin II).

Functions of the Security Control Unit

The Security Control Unit sits between a local network and a more public network, and only permits passage of data between the networks in accordance with a built-in policy. For this project, the policy will be quite simple. The intent of the policy is to forbid any traffic from the public network to the local network other than mail sent from the public network unless the connection was initiated from the local network side.

Once the unit has been tested, it will be tried out in practice by connecting it between our local network and the ARPANET. This will have the useful benefit of preventing any user of the ARPANET from trying to log into our computers. (At present our protection in this area is weak; certain small systems, particular in Dearborn, are unprotected.)

Description of the Control Unit

The Security Control Unit is to have two 9600 baud asynchronous ports. It is to be a standalone unit mounted in a small box. There will be no user interface. Two options exist for the hardware; the Digital Equipment Corporation LSI-11 and the Intel 8061. Pascal-F compilers exist for both machines. We propose to defer selection of the specific hardware pending a decision on acquiring a development system for the 8061 at WDL. Suitable development facilities already exist for the LSI-11.

The basic functions of the Control Unit are to

1. Decode and check IP datagrams
2. Decode and check TCP headers
3. Generate ICMP "unreachable" messages when messages are rejected
4. Note TCP connection establishment and teardown
5. Keep track of the TCP connections currently passing through the Control Unit
6. Reject any packet from the public network which does not belong to a current TCP connection and which is not an attempt to establish a mail connection.

The Control Unit will not have a full IP/TCP implementation. It will be able only to decode IP datagrams and find TCP headers in them, and recognize which headers represent connection setup and teardown. No knowledge of TCP sequence numbers will be present in the Control Unit. Fragments of IP datagrams will be passed only if a matching first fragment was passed in the last few seconds; however, no reassembly of fragments will take place in the Control Unit.

Cost and Schedule

Hardware	$12,000
Labor	4 man-months
Total (est.)	$52,000