## CROSS-WALK OF THREE SECURITY EXPERTS' RECOMMENDATIONS FOR SPENDING $1B/YEAR FOR NII SECURITY PROGRAM

Prepared as a Public Service by
Robert D. Steele, President
OPEN SOURCE SOLUTIONS, Inc.

23 August 1994

| FOUO Person | Winn Schwartau | William Caelli |
|---|---|---|
| CONTENT PROTECTION (No funding; permit market to provide software cryptography) | SECURE/OVERSEE GOVT SYSTEMS ($350 million/year) | |
| CONNECTION PROTECTION ($300 million/year) | TESTING & CERTIFICATION ($150 million/year) | PROTECTION TECHNOLOGIES |
| CHEAP ONE-TIME AUTHENTICATION ($200 million/year) | PRIVACY MODELS & GUIDELINES $250 million/year | |
| EDUCATION ($100-300 million/year) | EDUCATION ($150 million/year) | VULNERABILITY ANALYSIS |
| BASIC RESEARCH ($100 million/year for secondary dissemination audit and pay-back tools) | GENERAL (Create Federal Reserve Board equivalent to oversee C4I health) | NEXT GENERATION PROTECTION TECHNOLOGIES |
| OTHER ($100 million/year to develop National Trusted System standards) | STANDARDS ($100 million/year) | STANDARDS & PROTOCOLS |

The unabridged comments of each expert are attached for reference. Mr. Marty Ferris has been provided with the name and contact information for the person listed as FOUO.

NOTE: The author is an internationally-respected electronic security authority who retains full clearances at NSA, CIA, and other sensitive customer sites. He is in my view one of the most qualified to comment on the inadequacies of both the total government program within government, and also the vulnerabilities of the civilian infrastructure and individual corporate networks. His userid and signature have been deleted for privacy purposes. His identity has been provided to the NII Security Committee and they are at liberty to communicate with him directly.

Message 1:
From (FOUO)@DOCKMASTER.NCSC.MIL Fri Aug 12 23:23:12 1994
Subject: Late submission
To: Pres@OSS.NET

8/13/94

Here are the things I think the NII and or its ultimate expression need.

1. CONTENT PROTECTION. Needs no government funding.

This allows me to send you messages that no one can read even if they are camped on the connection. For this portion of the problem, we are actually in pretty good shape,since the availability of PGP and Secret Agent 3.0. Here it is a matter of users and providers having available a couple of reasonably good and reasonably fast software crypto functions. This needs no support except what the market provides.

2. CONNECTION PROTECTION. 30% of total government funding.

This is not available today at affordable prices. The old ATT 3600 that precipitated the Clipper crises is a good model of what is needed. It provided Single-DES secure end-to-end protection from a user to another user (phone), or a computer . The issue here is cost. The present ATT 3600 With Clipper etc. is priced at around $1300 each. Unfortunately it is too much for the average person. The price needs to be lowered to around $100-$300 /copy so a company with 30,000 employees could consider having one for each employee if needed.

Otherwise, it becomes VERY complicated to provide protection. For large organizations, one could imagine crypto-gateways that provide the function of the 3600-like device by multiplexing a high speed computer. That however, is not developed and may need some work. I don't think it needs much support. IF I had the call, I would put about 30% of whatever budget exists in lowering the cost of the connection crypto to a cost that ANYONE could afford, and make it as easy to use as falling off a log. As you are aware, I don't think the Key Escrow idea is fitting for an ostensible democracy. A triple DES with 3 keys pipelined would be the approach I would look for initially, but that needs some looking at as well. Repeating, 30% of dollars would go here.

3. CHEAP ONE-TIME AUTHENTICATION. 20% of government funding.

We need to get away from reusable passwords. There are already devices on the market in the 30-100 dollar range. Again, the problem is make them cheap and ubiquitous. Here again, the issue is volume and cost. There needs to be enough sales and competition to drive the prices down. Here a standard would be very nice to have, and a commitment to buy (say) a device for every Government employee (as a start). 20% of budget here.

4. EDUCATION. 10-30% of government funding, no bail-out policy.

Of system operators mostly to use the protection tools already provided in operating systems and avoid the horrible practices the UNIX people revel in. Either spend 30% here, or take a firm stand that there will be NO bail-outs for people who do not follow good security practices. I guess the latter would consume much of a 30% cut too. 10% applied to user education. The users, if provided the cheap devices noted above won't need too much education to use them, particularly if the services they try to access require (or make available) the other half of the equation.

5. BASIC RESEARCH. 10% of government funding.

Here, in my opinion, the unsolved problem is that of secondary distribution. I BUY something from you. I like it, then make copies and send it to my friends. I don't know off hand of any technological approaches that will provide a break through, but, it needs some funding. 10%.

NOTE by Steele: This really refers to the problem of having a global audit trail and the assurance that something retransmitted to others will result in an electronic funds transfer (of suitably modest proportions). Working with access providers to levy tolls on "marked" documents might be one solution, but "indelible" marking of copyrighted material needs to be developed.

6. OTHER. 10% of government funding.

If you want to shave 5% or so from the bigger slices, you might make up a 10% kitty to work on a National Trusted system standard for servers. No individuality allowed; it is an unwavering Government defined standard of what a trusted system needs to be. Anyone could bid on providing some or all of whatever needs are identified, but it would be by definition fully compatible down to the bit level. I know this is going against the path that we have been on for the last 20 years or so, but that path has led nowhere, and I still think we need to address this problem.

Hope this helps,

Cheers,

(FOUO)

# THIRD INTERNATIONAL SYMPOSIUM: NATIONAL SECURITY & NATIONAL COMPETITIVENESS: OPEN SOURCE SOLUTIONS Proceedings, 1994 Volume I - Link Page


| | |
|---|---|
| Previous | Correspondence to Mr. Marty Harris on the National Information Infrastructure Security Committee |
| Next | Letter from Winn Schwartau, Executive Director, Inter.Pact |

**Return to Electronic Index Page**