Paper submitted for 1997 National Information Systems Security Conference

Title:

Connecting Classified Nets to the Outside World: Costs and Benefits

Abstract:

In November, 1996 L-3 Corporation's Communication Systems East Division in Camden, New Jersey, became the first contractor site accredited according to NISPOM standards to provide unclassified E-mail service between a Dedicated Classified network and the Unclassified world using a Mail Guard. This marks a significant and substantial change in Government policy: a door that has been firmly closed has opened a crack, and as technology matures, that door cannot but continue to open wider. Other sites, prodded, in part, by the MISSI program, will soon follow L-3's lead. This paper will try to remove some of the uncertainty by enumerating the major costs, benefits and risks, and outline the major equipment requirements, necessary tasks and operational changes.

Author:
Christopher P. Kocher

Organizational Affiliation:
L-3 Corp
Government Communications Systems Division
1 Federal St.
Camden, NJ 08102

Phone Number:
Voice: (609) 338-2018
FAX: (609) 338-3150

E-Mail Address:
Christopher.Kocher@lmco.com
ckocher@netaxs.com

CONNECTING CLASSIFIED NETS TO THE OUTSIDE WORLD: COSTS AND BENEFITS

Christopher P. Kocher
L-3 Corp.
Government Communications Systems East
1 Federal St.
Camden, NJ 08102

Introduction

In November, 1996, L-3 Corporation's Communication Systems East Division in Camden, New Jersey (at that time a part of Lockheed-Martin) became the first contractor site accredited according to National Industrial Security Program Operating Manual (NISPOM) standards to provide unclassified E-mail service between a Dedicated Classified network and the Unclassified world using an SNS Mail Guard, manufactured by Secure Computing Corp. This marks a significant and substantial change in Government policy: a door that had been firmly closed has opened a crack, and as technology matures, that door cannot but continue to open wider.

Other sites, prodded, in part, by the MISSI program, will soon follow L-3's lead. Still others will be tempted but hesitate, uncertain as to the costs and benefits involved. Hardware, software and certification activities must surely cost money, but if your site has never done it before, you have no basis for estimating how much. This paper will try to remove some of the uncertainty by enumerating the major task, benefits and risks. If you know what tasks are involved and what benefits you may reap, you will be better able to decide if such a connection is appropriate for your site.

We cannot, of course, give dollar values to either the costs or the benefits, since the actual costs of many activities will vary markedly from site to site. Instead we shall outline the major equipment requirements, necessary tasks and operational changes. We shall also distinguish between one time costs and benefits and recurring costs and benefits, since that seems to be the most useful distinction for evaluating both dollars and manpower.

Costs

One Time or Short-Term Costs

Planning: The first cost that you will encounter is the cost of planning. But the better you plan, the lower will be your final cost. Time and money spent in effective planning are likely to reduce other costs.

Keep in mind that you will really be planning two related activities:

- Installing and configuring the Mail Guard
- Getting the Guard certified for operation.

These two activities may require different people and different skills. The Installation and configuration task is probably no harder than installing and configuring a firewall, but getting the installation certified will require that you *prove* to your Certification Authority that you have written an appropriate policy, that you have installed and configured your guard in accordance with that policy, that your Guard provides the functionality claimed for it, and that you have means to detect and document any significant configuration changes that would affect adherence to the policy.

As early as possible you will want to have one or more technical interchange meetings with your Certification Authority. You may also want to include your principal customers or subcontractors if the purpose of the Guard is to enhance your ability to communicate with them. The CA will help you understand what is needed for certification and can give you a realistic idea of what services the Guard will and will not be able to provide. They may also be able to give you a list of products that have already been approved for use in your intended application—this will save you considerable evaluation and testing effort. Understanding the capabilities and requirements of your primary communication partners will avoid embarrassing or expensive basic configuration choices. You would avoid a configuration that required Fortezza signatures, for example, if your communication partner was not capable of furnishing them.

You will also want to meet with your internal network service group or external Internet Services Provider (ISP) to determine what changes you will need to make to your current unclassified network, and you will need to meet with the administrators of your classified network to assess what changes will have to be made to it.

L-3's accrediting authority told us that either of two architectures would be approvable:

- A Guard with a dedicated firewall installed directly against it on the low side.
- A Guard protected on the low side by our remotely-located corporate firewall, but requiring Fortezza-based authentication of all mail coming in from the Low side.

The first option was primarily intended to be an interim solution in anticipation of more wide-spread Fortezza deployment.

We chose the second option to avoid the cost of an additional firewall, because our primary customers are Fortezza aware and because we had more Fortezza expertise than firewall expertise at our site. This first important choice did much to determine the character, if not the total, of subsequent installation and configuration costs, and ultimately dictated many of the hardware and software products that we subsequently obtained.

Hardware, Software and Facility Upgrade Costs

Our most significant hardware cost was the cost of the Mail Guard itself, plus the cost of training two engineers to install, configure, and operate it.

Other hardware costs included cabling, several additional ethernet hubs, a computer to act as an additional DNS server for our dedicated unclassified subnet, some ancillary computers and test equipment, and the Fortezza cards themselves (along with some add-on PCMCIA slots for computers that did not already have them). If you choose an

installation that requires a dedicated firewall instead of Fortezza, you can trade the Fortezza costs for the purchase cost of a turn-key firewall system or firewall software to install on a host that you already own.

The only additional operational software that we required was an add-on that provided a Fortezza signature and encryption capabilities to our existing mail user agents. We selected ArmorMail from LJL, Inc. which could be installed as an add-on to our existing Microsoft CC-Mail installation. (Since the user interface was practically the same as the underlying CC-Mail product, this product offered the additional benefit of requiring very little retraining of users.) We also purchased some test software to aid in configuring and evaluating the Guard. The one piece of test software that we found really invaluable was an Ethernet sniffer that ran on a surplus Macintosh that we had lying around.

Note that all the operational software must be installed by someone, and that installation may require adjustments to the configuration of the platforms or tweaking of related software that is already installed and running.

Some facility upgrade costs that you may encounter include:

- Additional power lines, air conditioning or floor space for your Classified computer room,
- An additional unclassified network drop to your Classified computer room.

Installation and Configuration

Installing and configuring the Guard is not a simple, one-step activity. The Guard offers many configuration options; while this provides flexibility, it also provides copious opportunities to make mistakes. You cannot get your guard installation certified for use until you have proven to your Certification Authority that it is installed and configured correctly, and you cannot verify that it is installed and configured correctly until you have actually tried it. What do you do?

We solved the problem by creating a small "toy" network out of surplus PCs and workstations that we had lying around. After obtaining approval from our CA, we first connected the high side of the guard to the Classified network and the low side to the toy network that we configured to look like our unclassified network. We installed Mail User Agents with the Fortezza enhancements on the low side and verified the ability of the guard to deal with signed and encrypted mail. Since the toy network was wholly contained within our classified computer room, any mistakes we made in our initial configuration attempts would not result in any actual threat to the classified environment.

Once we had satisfied ourselves that the guard was properly configured to talk to the High side network, we scrubbed the toy network and the Guard's hard drive to remove any possible Classified data. [This was not so straight-forward a task as it might seem. The Guard itself provided no facility to wipe its own hard disk and overwrite the erased data to NISPOM standards. After some experimentation, we disconnected the driver from the Guard's SCSI bus, reconnected it to a classified PC, and used the PC's approved *wipedisk* utility to reformat and over-write the disk.]

We then reconfigured the toy network to look like the High side network, connected it to the High side of the Guard, and connected the Low side of the Guard to the actual unclassified network. This, in turn, required the necessary Low side network configuration changes to be in place. In our case, we established a dedicated subnet with its own DNS server for the Guard. Only after we were able to successfully send mail back and forth between the simulated High side and external unclassified hosts were we reasonably confident that we were ready for formal certification test.

Each of these preliminary test configurations helped us to uncover and solve configuration problems and gave us experience and confidence in our ability to use the Mail Guard correctly. In the long run, they undoubtedly saved us money. But each setup took time, cost money and uncovered unforeseen problems.

The connection to the actual low side network was particularly thorny. We found that somewhere, beyond the immediate boundaries of our plant, our corporate network insisted on applying an additional layer of uuencoding to the base-64 encoding required by the MSP format of the signed mail messages. The Mail Guard could not deal with this second level of encoding. It took us a long time to locate the source of the problem, find the responsible parties, and establish a work around.

Moreover, it is not sufficient to just make sure that the Guard can talk properly to the Formerly Isolated Network (FIN) on the High side and the Unclassified network on the Low side. The FIN must be upgraded in anticipation of its incipient connection to the outside world. The administrator must examine the operating system and mail server software to verify the version number and to determine whether or not there are any outstanding security patches that must be installed. It may also be necessary to install software such as a Domain Name Server which was not needed when the network was isolated, but which will be useful when it is connected to the outside world. Although not strictly necessary, it may even be prudent to renumber the IP addresses of the FIN if they overlap someone else's address space.

Certification Activities

It is, of course, not enough to just plan and install a system that you think is secure; before you can connect a classified network to an unclassified one, you must convince your Certification Authority that your proposed installation is secure. To meet certification requirements, you will have to write and have approved by your Certification Authority some or all of the documents listed in Table 1. If you require a dedicated firewall in front of your Mail Guard, it will also represent a part of the security posture of the Guard, and you will therefore have to address its configuration, operation and maintenance in these documents.

If you are uncertain about any of the aspects of configuration or certification, you may wish to hire a consultant to help you. Hiring a consultant may actually decrease your cost by eliminating misdirected effort, false starts and unproductive labor.

Table -1. *Documents that may be required for certification*

- **Security Policy:** Describes in detail your security goals and rules.
- **Concept of Operations(CONOPS):** Describes what the Guard does, how it does it, and how it will be used
- **Security Procedures**
    - *For the Mail Guard:* Describes the Guard's configuration and procedures to be followed by Guard users and administrators
    - *For the Classified Network:* Describes the Classified network's configuration and procedures to be followed by Classified Network users and administrators (This document must be modified when you connect the network to the outside world)
- **Certification Test Plan:** Describes the tests you will perform to demonstrate that you Guard is installed in a way that meets your security objectives
- **Certification Test Procedure:** Step-by-step description of each test described in the Certification Test Plan, with spaces for expected results and witness's signature.

Certification Testing

Once your Certification Authority has approved your documentation, your installation will be subject to a formal Certification Test, following the steps outlined in your Certification Test Plan. Representatives of your Certification Authority will watch as you conduct the tests described in the Test Plan. If the results are satisfactory, they may issue authorization to use the installation as configured; if the results are not completely satisfactory, they may offer authorization contingent on required changes to the configuration or procedures, or they may require a retest.

Training

By the time the Guard is Certified for use, the Guard administrators who installed it are not likely to require further training. But you may need to train others to take over specific portions of the Guard administrator's duties, either for back-up or because your security policy requires separation of certain duties.

You may also have to give the Administrator of your Classified network additional training. Paradoxically, the administrators of your secure networks may know least about security threats from external connections, since they have never had to deal with such connections. They may therefore need additional training to teach them not only about networking issues but also about how to recognize some of the threats that plague networks with external connectivity.

Finally, you will have to train your users. This training should be more than just the mechanics necessary for sending and receiving mail through the Guard. You should plan to give your users a thorough refresher (or primer!) on network security, threats, recognizing hostile applications and social engineering, and the legalities of foreign dissemination of controlled information. If people who send mail through the Guard from the low side must follow certain procedures and policies, you may also want to train your user on how to explain those procedures and policies to their correspondents. [You should also prepare an explanatory mail message that you can send to new low-side users.]

Other Short term costs and activities

If this is your first major application requiring Fortezza cards, you will have to establish an infrastructure for procuring, maintaining, and administering Fortezza applications. You will have to arrange to order cards and certificates and to get the cards programmed. You will need to find or designate an Organizational Registration Authority (ORA) to serve as an intermediary between the card users and the organization programming the cards, and you will need to establish some means to distribute periodic Compromised Key List updates to all users whose application software requires it.

If you require a new dedicated firewall in front of your Mail Guard, you will have to purchase the necessary hardware and software, and will probably have to train someone to configure and run it. Since this firewall represents part of the security posture of the Guard, you will have to include its configuration, operation, and maintenance in many of the security documents listed in Table A-1., and it will have to be examined and tested as part of your certification testing.

Short term post certification costs: During the initial use period, the administrators will have to spend additional time monitoring, correcting, and re-educating users, as well as trouble-shooting new software and fine-tuning configurations and procedures.

Continuing

One continuing cost is the “Real estate” cost of the space in which you house the Guard. If there is sufficient empty space in your Classified computer room for the Guard and associated administrator terminals, this cost will be minor: if there is not sufficient space, you will have to either expand or rearrange the facility.

A primary continuing cost will be the cost of increased vigilance. The SysAdmin and the Security Officer of the formerly-isolated network will have the additional task of maintaining and operating the Mail Guard, and maintaining whatever records required by your Certification Authority. Additional tasks can include:

- Manually reviewing some (configurable) random fraction of the journaled message traffic
- Fixing problems; reviewing audit information...
- Continuing education of users
- Maintaining and upgrading additional software (e.g., Fortezza-aware mailers)

- Creating and maintaining lists of approved sites, dirty word lists, etc.
- Administering Fortezza cards and infrastructure, if used
- Administering and maintaining the dedicated firewall, if used
- Maintaining and examining audit logs and records for the CA.
- Preparing documentation configuration changes that require Certification Authority approval.

Less obviously, but just as importantly, the SysAdmin will suddenly have to start spending additional time tending to security holes and patches. Before it was connected to the outside world, the classified network's administrator may have paid little attention to such things as Computer Emergency Response Team (CERT) advisories, Computer Incident Advisory Capability (CIAC) Bulletins and vendor-supplied security patches: all the users with access to the network were cleared employees, and the SysAdmin therefore had some powerful sticks to wave at the occasional "explorer." Since there was no real external threat, security patches were low-priority items. Suddenly the network is, potentially, accessible to those who would exploit the security holes he has been ignoring. (If you need a Guard, you have classified assets to protect; you therefore represent a more attractive target to a whole class of attackers.) The change in attitude needed to make the administrator properly paranoid may require both time and retraining.

Benefits: Costs decreased with Guard

One of the often-quoted benefits of a Mail Guard is the elimination of a duplicate set of classified and unclassified terminals and networks for classified users. To the extent that this is true, you will receive some of the benefits enumerated below. But keep in mind that the Guard may not be certifiable to duplicate the entire functionality of your separate unclassified network. If your Guard only passes E-mail, for example, you may still need to maintain some hosts on a separate unclassified network to allow users to perform activities such as FTP or web-surfing, and such traffic is likely to constitute an increasing fraction of your total network traffic as time goes by.

To get a clear picture of benefits, you must also consider:

- Does the through-put limitation of the guard impose an upper limit to the size of the network that can be replaced? Will the throughput of the guard support the anticipated traffic volume?
- What percentage of the traffic out of the area served by the guard is actually e-mail? Is that percentage likely to increase or decrease with time? Will the total volume increase or decrease with time?
- Will the security policy or certification authority permit unrestricted access to unclassified e-mail, or will the volume be less than anticipated because only specific I&A'ed correspondents are permitted?
- Security may dictate that you disallow communications with certain sites: foreign sites or even educational sites. Will this significantly affect your anticipated use?

One Time Savings

Certainly there is the salvage value of duplicate equipment removed: extra hosts, terminals and network hardware. Unnecessary duplicate equipment currently used to provide external E-mail capability to your Classified users may be used elsewhere or even sold off.

Continuing

When the duplicate equipment is removed, you will also remove the per-unit maintenance costs on removed equipment. There will be less hardware to maintain. You will require fewer licenses and have fewer seats to maintain for some duplicated software products. You may even end up with one fewer network to maintain and administer.

Removing hardware will also reduce real estate "costs" such as desktop space. [While this may be insignificant in a typical office environment, savings could be substantial in a mobile environment: in a shelter, on board a ship, on a plane or spacecraft... In such mobile environments, every piece of hardware removed could yield substantial cost benefits due to reduced weight, volume, etc...]

The most significant benefit is likely to be in operational costs. If you transfer a lot of data between your Classified network and the outside world, a Guard can either reduce or eliminate the time that a human reviewer would spend moving data in either direction. If you provide on-line customer problem reporting and/or support, the customer may be able to mail issues directly to an issue log or support data base, and customer support engineers may be able to send problem resolutions without having to jockey back and forth between the Classified design data base and an unclassified E-mail tool.

Possible Exogenous Considerations

Even if an external connection is not completely justifiable in dollars and cents terms, you may wish to ask: Does your competitor have one? Does your customer consider it a benefit?

Risks and uncertainties

Some expected benefits may not materialize immediately. You will probably *not* do away with every duplicate unclassified terminal; you will need to maintain a few or even many for such services as web access and casual communication that are currently not supported by the Guard and not accredited. Such traffic may actually become a higher percentage of net use as time goes on.

Maintenance on the Mail Guard and associated software is another risk. Things break. The more things you have, the greater your potential for breakage.

Certification may take longer than you expected; indeed, there is no iron-clad guarantee that you will be certified.

Adding external connectivity is not without risk. To some small degree, it will increase your exposure to data leaking out or harmful data leaking in. This risk may, in fact, be a

small increment in comparison with your current risk, but no matter how safe, some connection is not as safe as no connection. You can minimize that risk by working closely with your certification authority and by properly educating and indoctrinating your user community, but you cannot completely eliminate it. If you do appreciable "sneaker-netting" between your Classified and Unclassified networks, however, and rely on human reviewers, the Guard may ultimately *reduce* risk: the checks that it imposes cannot be bypassed, and it never does a less-than-thorough job when rushed.

Conclusions

While I have tried to indicate important costs and benefits of connecting a hitherto isolated classified network to the outside world, keep in mind that your mileage may vary. I have not given dollar figures for the tasks and benefits that I have enumerated here because I do not think that that would be particularly useful: tasks that are difficult, time consuming and costly at my location might be trivial and inexpensive at your location, and vice versa.

Moreover, the cost-benefit ratio tomorrow will almost certainly be more favorable than it is today. As such connections become more common, the costs are likely to go down dramatically, and the benefits are likely to gradually increase. Scenarios that are currently innovative and unusual, and therefore require a major effort to prove themselves worthy of certification, will become commonplace, and certification will become correspondingly easier. The certification authorities will quickly develop guidelines for what is and is not permitted, and designing a site will become a matter of picking and choosing from a menu of blessed alternatives. The technology and infrastructure supporting cryptographic services cards will improve and become cheaper. Users at many different sites will develop applications that expand the usefulness of the channel while maintaining the required high level of security. The door that is just slightly ajar today will continue to open.