Security and Privacy in the NII

P. Weinberger (chair)
C. Callan
W. Dally
A. Peterson
W. Press

February 1995

JSR-94-150

Approved for public release; distribution unlimited.

JASON
The MITRE Corporation
7525 Colshire Drive
McLean, Virginia 22102-3481
(703) 883-6997

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (*Leave blank*)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	February 23, 1995	

4. TITLE AND SUBTITLE

Security and Privacy in the NII

5. FUNDING NUMBERS

04-958533-01

6. AUTHOR(S)

P. Weinberger, C. Callan, W. Dally, A. Peterson, W. Press

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

The MITRE Corporation
JASON Program Office
7525 Colshire Drive
McLean Virginia 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

JSR-94-150

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

ARPA/DIRO
3701 North Fairfax Drive
Arlington, Va. 22203-1714

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

JSR-94-150

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

The National Information Infrastructure (NII) is a vast undertaking to provide a web of networks, computers and databases to communication and information throughout the country. One of the more difficult topics is privacy and security on the NII. These are areas that are crucial to making the NII fully useful for government and for commerce. The JASON study examined technical issues of security and privacy and came to the conclusion that the problems are policy and not technical in nature. That is, the technology exists to provide security and privacy services on the NII but that issues of what services and their implementation must be resolved. The report suggests some steps that ARPA can make to help resolve the policy issues.

14. SUBJECT TERMS

cryptography, internet, e-mail, NII, encryption lite

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	SAR

INTRODUCTION

JASON NII Study 1

The National Information Infrastructure (NII) is a vast undertaking to provide a seamless web of networks, computers, and databases to provide communication and information throughout the country. Both inside and outside of government many organizations are working on parts of the NII. There are innumerable committees and task forces looking into aspects of the NII, producing innumerable reports, and trying to build consensus on all kinds of topics.

One of the more difficult topics is privacy and security on the NII. These are areas that are crucial to making the NII fully useful for government and for commerce. Proper protection of intellectual property will be crucial to making the NII fully useful for education and for entertainment. Privacy rights of various sorts are deeply embedded in the laws of the United States, and in the regulations of government. Varying views of the privacy rights of individuals vis a vis corporations and the government are at the core of contentious national policy debates. Thus there are many groups contributing to discussions on privacy and security for the NII.

Summary

- **The major problems are not technical but policy**
  - **Many examples to follow**
- **There is a lot of technology available for implementing sensible policies**
- **It is not easy to make up sensible policies**
- **And, it is not known what users will insist on**
  - **For ease-of-use**
  - **For acceptable security**
- **It's not even known who all the players are!**
- **Are "good enough" solutions good enough, or must we try to find a workable path to new, globally-engineered solutions?**

JASON NII Study 2

Our overall conclusion is that the problems of security and privacy on the NII are policy problems, not technical problems. There is a lot of existing technology that would support most sensible policies, but it is hard to make up sensible policies. Worse yet for those looking for technological solutions to privacy issues, the process of setting policy is fundamentally a messy political discussion which many of the important participants haven't yet joined. Further, solutions to privacy and security problems, either technical or policy, can fail because people reject the inconvenience.

Just to be specific, let's look at...

- **Security and Privacy on the Internet**
  - Can the Internet grow up to be the NII?
- **Business-quality electronic mail**
  - Why it's important
  - What are the security and privacy issues

JASON NII Study 3

In this report we concentrate on two areas, the Internet and electronic mail for commerce and government. For the former, there is a largely unspoken belief among many associated with the Internet that it is both a model for the NII and that it will expand into being the NII. Thus this section of the report is an attempt to look at an old and evolving and widespread network with its protocols and many different sorts of applications. Electronic mail is practically at the other end of the data network spectrum. It can be carried on the Internet, but it can also be carried by modems on phone lines. It is an enabling technology for electronic commerce and government. Security and privacy issues can be brought out clearly in this context.

Definitions

- All seemingly desirable properties, but ...
- Confidentiality
  - Keep the material secret (but for law enforcement)
  - And whose data is it anyway?
- Authentication
  - Know who is talking and when (but for Caller ID?)
- Non-Repudiation
  - Prove authentication to a third party's satisfaction
- Integrity
  - Keep it unmodified (but for removing personal identification)
- Solutions not universal; lots of policy issues
  - And then the international situation varies by country
  - and the cryptography may involve export restrictions

JASON NII Study 4

We start with some definitions. It is easy to describe desirable security and privacy properties for electronic communications. It is sometimes hard to apply them.

The first is *confidentiality* which is keeping the contents of the communication secret from outsiders. Even this, as the Clipper controversy shows, is controversial. Who is an outsider? How must the technology adapt to be able to respond to court orders? How are insiders to be assured of confidentiality? People act in many roles other than private citizen, and these roles affect who is an insider and who is not. For instance, in many cases communications are not the property of the employee involved, but of the company or government agency.

A second property is *authentication*, which is knowing whose communication it is. This is clearly critical in some cases, such as getting money out of an ATM. But in many states, telephone caller ID is viewed as a right of the originator of the call but not of the receiver. Closely related is *non-repudiation*, the idea being that having authorized something, I can't later repudiate my action.

A third property is *integrity*, which is knowing that information wasn't changed. The complexity here is that technology exists to ensure that no bits were changed, but it is more difficult to control legitimate changes, such as deleting personal identifying information in gathering epidemiological data.

Cryptography

- Encoding depends on a key
- Recipient must know the key to read the message
- Strength of encryption depends (at least) on the key size
  - But even algorithms with large keys can be very weak
    - »Newspaper cryptograms have more than 100 bits of key
    - »Password guessing is relatively easy
- Various sufficiently strong algorithms known
  - DES (56 bit key)
  - Triple DES
  - Skipjack
- Various countries (including the US) have laws and restrictions

JASON NII Study 5

Here, and in the next three charts, we very briefly review the technical foundations that allow, in principle, implementation of all the desirable features on the previous chart.

Cryptographic Hash Functions

- A cryptographic hash function is a kind of check sum
- NIST has proposed a standard, but there are other proposals too
- 'Cryptographic' means that it is hard to arrange to get a particular result
  - Modifying a message whose checksum is known will be detected
- Using public keys and cryptographic hash functions I can send messages that have to have come from me, that I cannot repudiate, pre- or post-date, that cannot be altered undetectably, and that can only be read by the authorized recipient

JASON NII Study 7

So what issues could be left?

- **Where do the public keys come from?**
  - The issue is that public keys are used to authenticate
  - The IRS' public key can be trusted, but getting public keys for most of us would seem to require a central authority
  - A central authority (even in the U.S.) seems unlikely
- **How would each of us keep our secrets?**
  - There are a lot of bits in a public key
  - The decrypting calculations cannot be done in your head
  - What device would we all carry?
  - What happens if you lose it?
- **This implementation of privacy/security requires a substantial infrastructure**
  - There is no obviously good path to there from where we are now

JASON NII Study 8

One of the hardest issues, with both practical and political dimensions, is to understand how ordinary citizens will be able to keep their secret keys secret. Will secret keys be lifetime perfect identifiers? If so, a possible technology would be government-issued "smart cards" -- but this may well be politically unviable. On the other hand, secret keys might be minor items of personal paraphernalia, like (perhaps virtual) credit cards, with expiration dates. In that case, establishing a sufficient set of bona fides for any particular transaction will be (as it is today) an ad hoc and variable process.

Is it useable,
and does anyone really care?

- **Real world practice depends on conscious and unconscious risk calculations**
  - Faxed authorizations, credit card numbers orders by phone
  - (some times the calculation is bad: Charles and Diana)
- **Laws make a difference**
  - Technically easy malfeasance is deterred by threat of fine/prison
  - E.g., lost credit cards, forged signatures
- **The economy accepts some serious risks...**
  - Telephone + faxed purchase order + overnight delivery
- **... and might *or might not* be able to accept new ones**
  - Faxed signatures, telephone checks
  - Private information on open cellular and airplane phones
  - Unauthenticated email

JASON NII Study 9

It is easy to write down principles that seem like they ought to govern security, privacy, and other aspects of commerce. It is likely to be more useful to understand what people do in practice. Practice likely represents a subtle compromise among security and privacy, inconvenience, and risk. Here are some examples: Vendors accept credit card numbers over the phone. This practice violates authentication and non-repudiation, but is enshrined in commercial practice.

People communicate private information over cellular phones (Charles and Diana come right to mind). This is crazy, but common. Digital cellular service will have some privacy between the phone and the base, but the history of GSM in Europe is instructive: one country insisted on a weaker privacy algorithm. People also communicate private information over the phones in airplanes.

It appears that Clipper will not catch on despite the fact that it greatly increases the privacy of phone conversations. It's hard to decide which of the opposing forces really matter, but they include a group that mistrusts the government's key escrow scheme, the additional cost of special hardware for many applications, and the self-reinforcing market uncertainty.

For most purposes, people and companies rely on first class mail to deliver valuable papers, despite the lack of a delivery receipt.

Introduction to the Internet

The Internet (with a capital letter) is a huge collection of connected networks using a set of IP-based network protocols. (IP is the name of the network protocol.) Each machine on the Internet has a 32-bit address, part of which is in common with the other machines on its network. By the middle of 1994 there were about 30,000 networks and 2,000,000 computers world-wide on the Internet. Of the computers, about 30% were at educational sites (mostly in the US), about 30% at commercial sites (mostly in the US), and the remainder were government or in the rest of the world. These numbers are strongly affected by the way people and organizations connect to the network. Most of the organizations run internal IP-based networks that can be easily connected to the Internet through a router. A router is a computer that decides what to do with each IP packet. Most individuals get on the Internet by belonging to an organization that is on the Internet. There is a growing number of providers of Internet service to individuals, either at the level of some applications, or by routing IP packets across phone lines. (Computer networks operate on packets of data, which typically consist of header information, data, and maybe a check sum.)

The Internet is useful. A simple application like electronic mail connects people all over the country and all around the world. Much data is freely available on the Internet, although finding it is hard, and sites are frequently unavailable or overloaded. New applications, such as Mosaic (which is public domain software) make searching for and getting data much easier than it had been.

There are three sorts of security problems on the Internet: eavesdropping on local broadcasts, using familiar buggy applications, and inviting trouble. (The last corresponds to putting a floppy disk with a virus on a PC.) The third is a common computer problem and has nothing special to do with the Internet, or even with computer networks, except insofar as networks provide more attractive bait. For the second, most of the problems are associated with connections, so adding authentication would, in principle, fix the problem. It would fix the X problem. It would fix the NFS problem. It would not fix the Mosaic problem, which will be fixed anyway in the natural course of Mosaic evolution. (Mosaic started as a free program, but in the near future most new Mosaics will be commercial.) However, the fixes have to become widespread.

Most computers are on local area networks that are broadcast media. That means that a misbehaving host can read all the packets on the local net. IP packets tell eavesdroppers more than they deserve to know. The header of an IP packet gives the source and destination machine addresses (which can be translated easily into machine names) and frequently indicates which service the packet goes with. One of the presently popular Internet breakins involves getting on a much used machine, and collecting the beginnings of every conversation, which may well contain the beginning of a remote login, with user name and password.

This simple example indicates one of the fundamental issues with security on computer networks. Most decisions were made with no concern for security, and these decisions are firmly embedded in the infrastructure. It would not be hard to build a local area network in which most packets are not broadcast. Indeed, some kinds of twisted pair ethernets can be run that way. Further, the need for broadcast packets could be avoided altogether, at the cost of requiring a reliable machine with stable storage at a well-known address on each network. That's what we are used to in the telephone network, where the network provider assigns phone numbers and provides connectivity, even for private networks and PBXs.

Asynchronous Transfer Mode (not cash machines!) networks could ameliorate this problem, because ATM networks will likely include a switch that could provide the local directory services that are now obtained by broadcast. ATM inherently provides byte streams between two endpoints, roughly corresponding to TCP on the Internet. One difference is that ATM headers do not contain the address of the destination, but just a circuit identifier that the next switch uses to forward the packet.

The Internet has problems

- **The Internet change mechanism is very slow**
  - **32 bits isn't enough and never was**
  - **And nothing has changed for years**
  - **Not a security issue, but lack of progress on so simple a technical issue does not inspire confidence when we turn to complicated, politically charged, security/privacy issues**
- **IP packets tell eavesdroppers too much**
  - **Who it's from, who it's to, and frequently what service**
  - **ATM may be better, but can it be improved?**
- **The Internet's weaknesses are common knowledge**
  - **Widely available hacking tools**

JASON NII Study 12

One of the strengths of the Internet culture has been the value placed on openness and consensus-based decision making. However, change has been slow. One sign of this torpor is the 32 bit IP address itself. For many years it has been clear that 32 bits is not enough, especially when they are used as they are now, with some prefix of the 32 designating a network, and the remainder designating a host. (For comparison, Ethernet addresses are 48 bits long. Telephone numbers in the US phone system are about the same number of bits, but subnetworks are geographical (area codes and the next three digits), most phones don't have unique addresses (extensions and many in businesses), and a 15 digit scheme is coming in a few years.)There is no security implication in short IP addresses, but the fact that such a basic flaw is so hard to fix indicates that the change mechanisms in the Internet are slow, being on the same scale as regulated utilities. The NII won't wait.

One force that may encourage recalcitrant sites to take security more seriously would be tort law. Allowing one's machines to be used as way stations as intruders attempt to break into other machines may get some university into court. Uncontrolled machines may be damaging in other ways. One possibility is allowing the unauthorized redistribution of intellectual property. One or the other of these is likely to be a much more powerful catalyst for change than the normal Internet change process.

The security and privacy properties of any computer network depend on properties of the individual computers and properties of the network. A network that broadcasts its packets (as did the pioneering Hawaiian Aloha network) contributes nothing to privacy or security. Once an outsider gets a program to run on a computer with no internal protection mechanisms (such as DOS), files (where the

Internet's end user orientation engenders bad security

- **System administration is sloppy, especially at `.edu` sites**
  - Never type your password far from home (the attack of today)
- **Lots of unsafe old software**
  - NFS
- **New services open new holes**
  - X gets incoming connections that can capture all keystrokes
  - Mosaic
- **Most people just don't care**
  - Are we waiting for the big law suits?
  - MIT 'allows' [fails to prevent] illegal redistribution of software
  - Stanford 'allows' Dutch hacker to use its machines to break into commercial and government sites

JASON NII Study 13

data is stored) can be deleted, changed, or copied. (Computer viruses are a non-networked example of the problem.) The Internet (and most computer networks) suffers from much subtler versions of these generic problems. In addition, each common service that is added to the network or to hosts brings its own opportunity to lessen security and worsen privacy.

Because Internet knowledge is widespread (see your local bookstore) and the Internet is widely accessible, programs to take advantage of Internet security weaknesses are also widely known and widely available.

It is frequently said that the security problems of computer networks are just system administration problems. The idea is that a careful system administrator can configure the system so that it does not have weaknesses that can be exploited. Unfortunately this is not true in any useful sense. As a practical matter, a local area network is not much more secure than its weakest machine, and most sites have machines maintained with different levels of care. At a human level, security is frequently intrusive, so people don't always do the secure thing. Finally, programs are buggy, and some of the bugs are security bugs. Even when the security bugs become known it may not be possible to get the manufacturer to ship fixes. The choice is then living with the bug or doing without the program.

Many sites, especially commercial sites, ameliorate this problem by installing firewalls, which are computers that sit between the outside world and the internal network. For the Internet there are two kinds of firewalls. The first filters IP packets, possibly looking at the source address, the destination address, and as much of the service information as it can deduce. These gateways tend to allow more services, especially new services, through, but provide less security. The second kind of firewall allows no IP packets through, but relays services. This kind can be made

The Internet isn't all there is or will be

- 'Internet' is the collection of interconnected IP-based networks
- There are many alternative networks in use
  - Novell IPX, long-distance companies announcing public services
  - Services: America Online, Delphi, CompuServe, Prodigy, etc.
  - Lotus Notes
- Will the different networks virtualize each other?
- What will the big commercial players do?
  - Microsoft, Microsoft, Novell, and Microsoft
- Can the Internet commercialize fast enough to force out the alternatives?
- Voice and video

JASON NII Study 14

quite secure, for instance passing only mail, outgoing ftp, and the kind of secure incoming telnet described above. On the other hand, even some mail implementations are not safe, and many services are crippled in the name of security.

The Internet is unlikely to be the only computer network in the NII. The most popular PC networks are based on Novell software and use a protocol named IPX. Like IP, IPX uses datagrams. IPX addresses are longer than IP addresses, having 32 bits for network numbers, but include the host's physical address on its local network as part of the IPX address. Thus IPX addresses are more physical than IP addresses and so require better directory services. In any case, there are a lot of IPX networks, and several of the big common carriers have announced public IPX services. Networks with incompatible protocols require service-level gateways between them, for instance, to handle electronic mail.

In many ways the Internet protocol suite is more sophisticated than the IPX suite. However, IPX implementations have been designed with at least some security in mind.

There are other widespread network protocols that might make a difference to the NII. For instance, there is IBM's SNA. Also, there is the OSI protocol family, which (at least some parts of) the federal government are supposed to use.

\What will the commercial software industry do? This section should be titled What will Microsoft do? It makes a difference. If software or network providers agree on the Internet as a common basis, then the NII will have a very large Internet component.

Internet security

- **Regrettably few opportunities at physical and logical layers below the "socket level" used by applications**
  - Slow-as-molasses consensus process for change
  - Huge, heterogeneous installed user base
- **Lots of opportunity (some lost) at application level**
  - Plenty of cryptography is known; problems are not technical
  - Centralized key management and authentication are well understood
    - »PEM
  - Centralized services seem very unlikely in present climate
- **Standards are likely to be de facto and application-specific**
  - increasingly, in future, derivative of commercial offerings

JASON NII Study 15

(continued) However, if commercial forces see protocols and services as potentially leading to competitive advantage, they will compete by differentiating themselves. That is to say, their offerings will be different, and no more compatible than necessary. This is already true in electronic mail systems. Further, the commercial world need not divide up its services using the Internet model. For instance, Lotus Notes provides (at least abstractly) many network-like services within itself, including many security, privacy, and reliability functions. One could imagine, in principle at least, public access Notes installations that would provide access to large amounts of information.

Solutions must deal with many protected classes of information

- Personal information
  - Medical
  - Financial
  - Just plain personal
- Proprietary information
  - Within a firm
  - Between firms
  - Procurement selection and pre-procurement information
- Intellectual property
  - Copyright
  - Trade Secret
- And, no doubt, classes yet to be recognized

JASON NII Study 16

A major complexity of the real world is that there are potentially many different, incommensurable, kinds of protected information, each of which has different legal, personal, and political implications.

Email Is a (Sleeper) Killer App

- It is so much a part of our life that we (members of the techno-elite) forget how revolutionary it may be for taxpayers Joe and Jane Citizen, or their kids
- Universal access easier to achieve than for more state-of-the-art services
- Email is a base vehicle for other applications...
  - Ordinary electronic mail
  - Mailing lists
  - Software and document distribution
  - FrEdNet
    - »Email-based network of writing teachers and students
- ... And for interactions between citizen and gov't
  - Queries (e.g. Social Security)
  - Tax filing

JASON NII Study 17

Rather than thinking about a single overarching network, like the Internet, it is useful to think about the capabilities of a relatively simple and ubiquitous service like electronic mail. Electronic mail could provide an enabling infrastructure for the NII, other than for those services, like multi-media communications, that require real time response. In some sense, email is the minimal mechanism for implementing much of the NII, and while it will not displace either the Internet or simple bulletin boards, it presents a realistic thought experiment for security and privacy issues both for electronic government and for electronic commerce.

Electronic mail is a store and forward service. That is, a user or program creates an email message which then goes through a sequence of mail transfer agents on its way to the recipient or recipients. Like the Post Office, the mail transfer agents can store the mail for a while before trying to deliver it, and typically they will retry over a period of days if the recipient is unavailable.

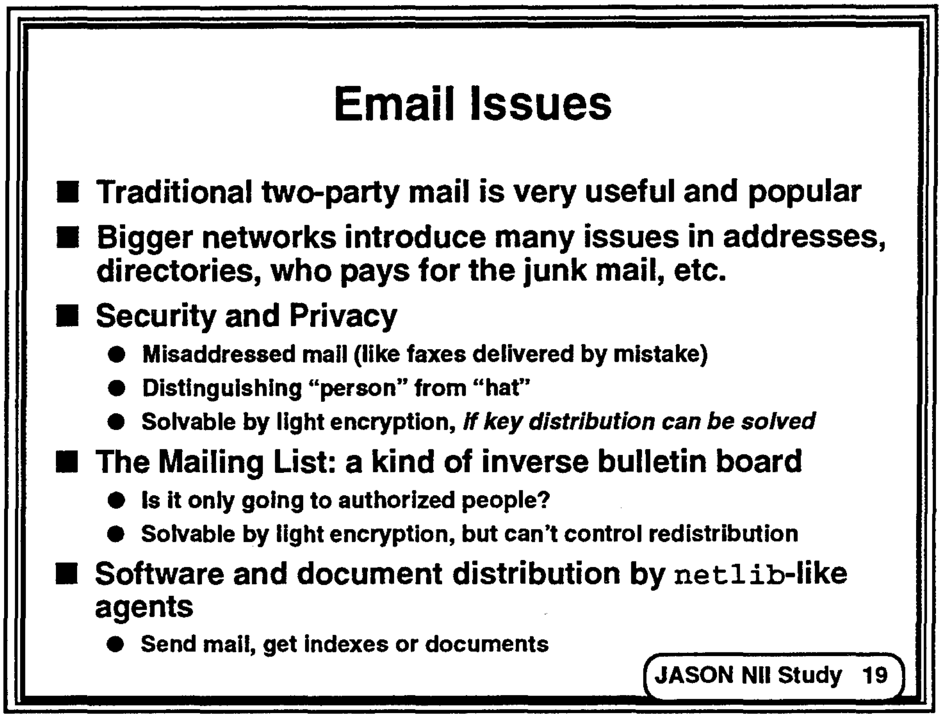
Two person electronic mail has traditionally been one of the most useful services on computer networks. Internetworks have uncovered a number of problems. Making separate email systems interoperable is not particularly easy. Roughly, there are three pieces to mail systems: the addresses, the descriptive headers, and the contents. Generally addresses can be embedded in other formats (like 123,451@CompuServ.com), and the other stuff gets reduced to lowest common denominator, which is typically ascii text.

Email to/from government is a good candidate for a demo-scale project

- An enabling technology for electronic government and wider public access
- Already 100s of government bulletin boards (dial in)
- Most agencies already have some form of internal email
- Potentially a leadership example for electronic commerce
  - Government example could be a catalyst to the private sector

JASON NII Study 18

Here is an example. For a return receipt, the IRS (say) could take the checksum off my electronically submitted tax return, add the time received, add an unforgeable signature (using its public key) and a cryptographic checksum for the whole thing. (They would undoubtedly want to check that the checksum I appended to my return was correctly computed.) Since I can check their signature using their public key, when I get the receipt I can be sure they got my tax return. The same technique would apply for any recipient. For this scenario to work, people would either have to agree on how public keys were to be used, or announce the algorithm along with their keys. Well-known organizations would have no trouble making their public keys public, and there would be little doubt that the IRS's public key really was the public key for the IRS.



Mailing lists are a kind of inverse bulletin board, in which the material is delivered to everyone on a list, instead of requiring people to take some action to find the material. Once again light encryption would make sure that the unauthorized don't get to scan the contents by mistake. The mailing list could either encrypt each message separately using the private key of the recipient, or there could be a mailing list key that people get when they join. In the latter case, the key could be redistributed periodically, or could just stay the same. Even the weakest version is clearly more secure than faxing to hotels.

The message "send index" to "netlib@research.att.com" returns a description of how to get lots of public domain software by electronic mail. The famous particle physics preprint service sends out preprints in a similar way, except that it also sends changes to its index automatically to everyone on a mailing list. It would be technically straightforward to add authentication and encryption to these services at various levels, to control distribution to authorized recipients. (Technical means will not control what the recipients then do. This is the same as the general problem of protecting intellectual property on computer networks.)

Addressing and privacy

- **Mistaken transmissions, address lists, aliases, forwarding to employees who move or leave**
  - **Sensitive information sent by typing mistake to wrong receiver**
  - **Sensitive information sent by indirection mistake**
  - **Directory correctness issues (watch out for caching)**
- **Up to date directories of people, positions, and roles**
  - **Obsolete entries could easily violate privacy**

JASON NII Study 20

Security and privacy issues show up just as a consequence of the scale of internets like the NII. It has become quite common to get misaddressed mail, sometimes surprisingly confidential. This can result from simple mistyping of the address, an obsolete entry in some mail alias file, the ambiguity in directories (which David.Johnson@att.com?), or many other causes. Avoiding the problem can be very straightforward some times, or very difficult. For instance, I can lightly encrypt, using their public keys, mail to people I correspond with a lot. At the other end, there are a lot of David Johnsons; the right one will be hard to find.

One of the more difficult issues in practice will be keeping directories up to date. Directories contain information on how to reach people and organizations, both their real names and in various roles. (The clerk of traffic court in Omaha also has a personal name, but it is the role that would collect the fines.) There is a substantial security/privacy issue in making sure that the directory is accurate and up to date. Otherwise private electronic mail may be misdirected, bids and filings misdirected, and the whole network viewed as insufficiently functional.

Issues for commerce

- Reliable delivery (acceptable performance)
- Non-repudiation of senders and recipients
  - Different problem for government side, as opposed to public
- Reliable date and time stamps
- News-like distribution of information rather than Mosaic-like pull
  - Do all interested parties get it at the same time?
    - »For instance, distribution of unemployment data
  - Not a security issue, but the kind of thing that may interact badly with the security mechanisms

JASON NII Study 21

In addition to the canonical security and privacy issues of integrity, confidentiality, and authentication of sender and receiver, commerce has additional needs. There will need to be analogies to certified mail, and to delivery receipts. The minimal certification in certified mail is that I sent something to a specific address at a specific time. Most theorists of security would see little value in such a weak assertion, but clearly it serves a real need in practice. Return receipts certify that something was actually delivered to a particular address at a particular time. Since it says nothing about the contents, the certification is fairly weak, but also useful.

Cryptographic techniques allow much more trustworthy certifications for email.

I can make sure that a message does not get changed by appending a cryptographic checksum, for which there are several well-known choices. In practice, since mail transfer agents change header information, it will have to be clear which part of the message corresponds to the checksum. Also, since there are several choices one would probably have to indicate which was being used.

I can protect the message's confidentiality by using (possibly weak) encryption with the recipient's public key. In practice this would require at least an unencrypted field in the header saying which encryption algorithm I chose.

Law and adjudication

- **It's a little harder for the government**
  - Extra requirements over private companies
- **Legal requirements**
  - Computer Security Act
  - Privacy Act
  - Freedom of Information Act
- **Evidence in judicial proceedings**
  - What is required for federal and state courts? (proof of non-tampering, chain of custody, or whatever)
- **It's a little easier for the government**
  - They (if they can get their act together) make the rules

JASON NII Study 22

Authentication of individuals is difficult. It is not more difficult in principle, since any central authority could assign authentications, at least for those people who would use them. In practice, it seems unlikely that there is a central authority who could be successful in the U.S. It is more likely that we will be authenticated in electronic commerce by techniques (including public keys) that depend on the situation. The rubric will be, ``Use something that is good enough." For instance, a bookstore might accept email orders with no more authentication than the return address looking right.

Email evolution (apart from the technology)

- Satisfy requirements of laws
- Satisfy requirements of commerce
  - Postmarks, delivery receipts, timeliness (?!), reliability of transport and postmarks and delivery receipts
- Laws, policies, and practices will evolve
- Buying a house electronically (a hard case)
  - All the authentication issues
  - What sort of 'paper' trail would there be
    - »Enforcing the agreement
    - »Maintaining title into the indefinite future
    - »And what about the bank and the mortgage?

JASON NII Study 23

Technically, it is not hard to provide security, privacy, authentication, etc, for commerce and government based on electronic mail. In practice it will not be easy. Unless widely useful free software becomes available, the future will be determined by commercial software providers, together with organizations having a real need (hypothetically the IRS). Many companies and parts of the government presently use EDI to transfer orders and payments, so it is not impossible, but at the moment electronic commerce works between parties that do a lot of business with each other and make special arrangements.

Email will have "arrived" as an accepted means of commerce when it becomes possible to buy or sell a house entirely over the net. Buying or selling a house is likely to require a lot more rigor than even filing a tax return. Both sides must be quite sure of the identity of the other party, and the transaction must leave a record that, with high probability, will stand up to legal challenges into the indefinite future.

Sensible laws and policies are hard: Three proposed (flawed) laws

- **'Illegal to use machines without explicit permission'**
  - Anonymous ftp, bulletin boards, catalog sales
- **'Terminals must beep when employees are being monitored'**
  - Many existing programs beep
- **'Illegal for a company to read employee's files'**
  - And how do they backup the data?

JASON NII Study 24

Sensible legislation is hard to design. If this isn't self-evident, here are three stories we heard from CERT about proposed laws, none of which passed:

To legislate on the problem of people breaking into computers, it was proposed that using a computer without explicit permission be made illegal. If that's what the law said, then anonymous ftp, bulletin boards, and catalog sales by computer would all involve illegal acts.

To protect the privacy of employees it was proposed that when employees were being monitored, their terminals would beep, and the terminal beeping would indicate that the employee was being monitored. Unfortunately it would be impossible to modify all of the other programs that cause beeps.

It was proposed that companies not be allowed to read employees' files. This is very close to a restriction in some software license agreements. Leaving out issues of who owns the files, it is hard to back up files without reading them.

Sensible proposals for any of these three cases would be hard. Indeed, even for the most informed policy maker, the worst pitfall would be foreclosing promising new ways of using computers. Clumsy policies could do great damage.

Findings (No surprises here!)

- **Security and privacy are difficult matters of policy**
  - **Technology exists to implement any sensible collection of policies**
  - **The government will be unable to impose solutions, except perhaps on itself**
- **The Internet's present technology and style of evolution will not enable it to satisfy universal privacy and security goals**
  - **This does not make partial solutions worthless, but their limited scope must be recognized**
- **Policy makers and staffs (Executive, Legislative, *and* Judiciary) badly need to be educated on the issues**

JASON NII Study 25

The surprise, perhaps, is that there is no surprise (though there may be controversy). While the Internet has millions of users, including a significant number of dogmatic, if not rabid, supporters, it is very, very hard to see how its present style of evolution will enable it to satisfy universal privacy goals that are necessary for the NII.

Summary Recommendations

- **Electronic government will need standards and algorithms for authentication, directories, postmarks and tracing, and receipts. Get going on real demos.**
  - Support the implementation and wide distribution of trial modules and systems
  - Require interoperability, robustness, and ease of use
- **Continue to support the fundamental research and systems engineering necessary for the foundations of a clean-slate, holistic, new approach.**
  - Demo if possible
  - Revolutionary might become possible by evolution!

JASON NII Study 26

Recommendations: We are of Three Minds

- **The Apathetic View**
  - Gov't work the highest level of policy only (e.g., deregulation)
  - Let commerce and the market take its course
- **The Incremental View**
  - ARPA should fund a small number of demo projects specifically targeted at the citizen-government interface
  - Involve other Federal (State? Local?) agencies, one per demo
  - While projects are *only demonstration* (finite breadth and lifetime) their implementation will be with scaleability (and de facto standardization) in mind
  - The technology should be good enough, not perfect. The goal is to get actual "operator" experience with real customers (citizens)
  - Examples follow
- **The Holistic View**
  - Develop a clean-slate approach to the NII (see example)

JASON NII Study 27

Something needs to be done, but what?

For ARPA, we see three possible paths. The choice among them is not clear cut.

APPENDIX

JASON NII Study 28

Demo Projects in NII Security/Privacy

- **Examine range of real-life complexity levels**
  - Working person's SSA inquiry about account contributions
  - File taxes electronically with IRS
    - » Existing IRS program *does* this
    - » But it lacks virtually any privacy or security features
  - Apply for SS or Medicare benefits
    - » Authentication for a walk-in target population
    - » Can we use existing infrastructure, e.g. Post Offices?
- **Consider range of target population**
  - Yuppies on CompuServe or inner-city residents?
- **Find right level of authentication and confidentiality**
  - What is the level considered appropriate in paper transactions, e.g.
- **Develop technically sound, scaleable, system solutions, as if proto-standards**

JASON NII Study 29

File your taxes electronically

- How do you keep it secret from the intermediate mail agents?
  - Encrypt it
- How do you persuade the IRS you really sent it on time?
  - Either they will need to have gotten it or you will need some sort of receipt from a trusted mail agent
- How might you know the IRS got it?
  - They would return a digitally signed receipt. (You can't forge these)
- How would everyone know you sent what you claimed?
  - You would add a cryptographic checksum, they would check it and include it in the receipt
- How would you sign it?
  - Alas, this is the part where reality intrudes. Probably have to hand out digital signatures by regular mail?

JASON NII Study 30

"Encryption Lite"

- Current authentication in citizen-government interactions is often no more than a signature and Social Security Number
  - If not "good enough", it is pretty close
  - Government's protection is (existing) criminal law
- Current confidentiality is often no more than an envelope in the mail
- Better authentication and confidentiality can easily be provided with "light encryption"
  - 40-bit security (say) user-typable as 4 groups of 5 letters
  - Not a replacement for secure communication, just an available service allowing increased privacy/security in citizen-government interaction on the net.
  - Finesse export problems, Clipper controversy

JASON NII Study 31

Clean Slate approach to the NII

- **Model the NII as a secure, distributed database**
  - Uniform naming, security, and access methods
  - Service and security guarantees (limit user liability)
  - Metering
  - Multiple, private service providers
- **Uses**
  - E-mail: append a record to an in-box, voice, video, or text
  - Bulletin board: append record to publicly readable file
  - Payment: debit-credit transaction
  - Distribution of information products:
    - »government information - personal and summary
    - »commercial - software, periodicals, books, audio, video
    - »service - multimedia 800 number
- **Advantages**
  - uniform access model - read, write, append records to tables
  - uniform security - key management, access lists, authentication, encryption
  - integral metering, billing, and transaction logging
  - solid foundation for electronic commerce

JASON NII Study 32

Evolution of the existing Internet is unlikely to result in an effective information infrastructure in a timely manner. On the other hand, the existing network provides sufficient utility that users are unlikely to abandon it for an unproven alternative. Only after alternatives have been demonstrated in pilot projects can they be considered for adoption.

Many of the problems of the current Internet stem from a few root causes

1. Most of the focus is on the "plumbing" of the network (e.g., IP) rather than on terminals, services, and modes of use. It is likely that commercial "connectivity" providers (e.g., ATT, MCI...) will provide adequate plumbing.

2. There is no uniform system for naming, security, and resource management. These are handled on an ad-hoc basis by each application.

The database community provides a large and well tested body of knowledge in this area. Thus, it is natural to consider a secure, distributed database as a model for the NII.

In such a model, the fabric of the network is "invisible" to the user. A user connects to a "service" using a location independent name. The location of the service is immaterial. It may be distributed and it may migrate. A users sees the network not as a set of nodes each with independent services but rather as a single, large database through which she can navigate using a number of access methods or views.

Once connected to a service, a user would authenticate herself using a level of security adequate for the task at hand. Once a user is authenticated to a given level, access control and protection within the system may make use of conventional systems technology (access control lists and/or capabilities) to provide a uniform and powerful method for selecting which "users" can access which "data" using which access methods. An appropriate entry in a table of permissions, for example, could grant all members of the group "medical researchers" access to "patient data" with for access modes of type "summary" while restricting access to individual records.

Because all accesses to the database take the form of applying an access method to an object, a single metering mechanism can be used to handle arbitrary transactions ranging from the purchase of an information product, to billing a user for sending e-mail.

All current uses of the network can be viewed as performing a transaction on a database. Sending e-mail or posting to a bulletin board, for example is just appending a record to a file. Complex business transactions can be made atomic by setting up conditions that commit the transaction only when all preconditons have been met.

The database would be provided by multiple, private service providers that each provide a secure repository for data. The model is similar to that of banks which provide secure repositories of a different sort.

Building the NII as a distributed database lets us solve problems of security, naming, metering, logging, etc... once rather than having ad-hoc solutions be proposed for each application. This is the same reason that has led database systems to become the pervasive substrate for most business software. A database can provide an equally strong foundation for building the NII.

DISTRIBUTION LIST

Director of Space and SDI Programs
SAF/AQSC
1060 Air Force Pentagon
Washington, DC 20330-1060

CMDR & Program Executive Officer
U S Army/CSSD-ZA
Strategic Defense Command
PO Box 15280
Arlington, VA 22215-0150

A R P A Library
3701 North Fairfax Drive
Arlington, VA 22209-2308

Dr Arthur E Bisson
Director
Technology Directorate
Office of Naval Research
Room 407
800 N. Quincy Street
Arlington, VA 20350-1000

Dr Albert Brandenstein
Chief Scientist
Office of Nat'l Drug Control Policy
Executive Office of the President
Washington, DC 20500

Mr. Edward Brown
Assistant Director
ARPA/SISTO
3701 North Fairfax Drive
Arlington, VA 22203

Dr H Lee Buchanan, I I I
Director
ARPA/DSO
3701 North Fairfax Drive
Arlington, VA 22203-1714

Dr Curtis G Callan Jr
50 Lafayette Road, West
Princeton, NJ 08540

Dr Ashton B Carter
Nuclear Security & Counter Proliferation
Office of the Secretary of Defense
The Pentagon, Room 4E821
Washington, DC 20301-2600

Dr Collier
Chief Scientist
U S Army Strategic Defense Command
PO Box 15280
Arlington, VA 22215-0280

Dr. John M Cornwall
Dept of Physics
Univ of California/Los Angeles
Los Angeles, CA 90024

DTIC [2]
Cameron Station
Alexandria, VA 22314

Dr William J Dally
Massachusetts Inst of Technology
Dept of Electrical Eng & Compt Science
Bldg NE43, Room 620A
545 Technology Square
Cambridge, MA 02193

Mr John Darrah
Senior Scientist and Technical Advisor
HQAF SPACOM/CN
Peterson AFB, CO 80914-5001

Dr Gary L Denman
Director
ARPA/DIRO
3701 North Fairfax Drive
Arlington, VA 22203-1714

DISTRIBUTION LIST

Dr John M Deutch
Under Secretary
DOD, OUSD (Acquisition)
The Pentagon, Room 3E933
Washington, DC 20301

Mr John N Entzminger
Chief, Advance Technology
ARPA/ASTO
3701 North Fairfax Drive
Arlington, VA 22203-1714

Dr Lawrence K. Gershwin
Central Intelligence Agency
NIC/NIO/S&T
7E47, OHB
Washington, DC 20505

Mr. Thomas H Handel
Office of Naval Intelligence
The Pentagon, Room 5D660
Washington, DC 20350-2000

Dr Robert G Henderson
Director
JASON Program Office
The MITRE Corporation
7525 Colshire Drive
Mailstop Z561
McLean, VA 22102

Dr Barry Horowitz
President and Chief Exec Officer
The MITRE Corporation
202 Burlington Road
Bedford, MA 01730-1420

Dr William E Howard I I I [2]
Director of Advanced Concepts &
Systems Design
The Pentagon Room 3E480
Washington, DC 20301-0103

Dr Gerald J Iafrate
U S Army Research Office
PO Box 12211
4330 South Miami Boulevard
Research Triangle NC 27709-2211

J A S O N Library [5]
The MITRE Corporation
Mail Stop W002
7525 Colshire Drive
McLean, VA 22102

Dr Anita Jones
Department of Defense
DOD, DDR&E
The Pentagon, Room 3E1014
Washington, DC 20301

Dr Bobby R Junker
Office of Naval Research
Code 111
800 North Quincy Street
Arlington, VA 22217

Lt Gen, Howard W. Leaf, (Retired)
Director, Test and Evaluation
HQ USAF/TE
1650 Air Force Pentagon
Washington, DC 20330-1650

Dr Alfred Lieberman
Chief Science Advisor, Acting
USACDA
320 21st Street NW
Washington, DC 20451

Dr. John Lyons
Director of Corporate Laboratory
US Army Laboratory Command
2800 Powder Mill Road
Adelphi, MD 20783-1145

DISTRIBUTION LIST

Col Ed Mahen
ARPA/DIRO
3701 North Fairfax Drive
Arlington, VA 22203-1714

Dr. Arthur Manfredi [5]
OSWR
Central Intelligence Agency
Washington, DC 20505

Mr Joe Martin
Director
OUSD(A)/TWP/NW&M
The Pentagon, Room 3D1048
Washington, DC 20301

Mr James J Mattice
Deputy Asst Secretary
(Research & Engineering)
SAF/AQ
Pentagon, Room 4D-977
Washington, DC 20330-1000

Dr Greg Moore [10]
JASON Program Coordinator
Central Intelligence Agency
DDS&T/P&RS
Washington, DC 20505

Dr Bill Murphy
Central Intelligence Agency
ORD
Washington, DC 20505

Mr Ronald Murphy
ARPA/ASTO
3701 North Fairfax Drive
Arlington, VA 22203-1714

Dr Julian C Nall
Institute for Defense Analyses
1801 North Beauregard Street
Alexandria, VA 22311

Dr Michael R. Nelson
Executive Office of the President
Office of Science & Technology Policy
The White House
Washington, DC 20500

Dr Ari Patrinos
Director
Environmental Sciences Division
ER74/GTN
US Department of Energy
Washington, DC 20585

Dr Bruce Pierce
USD(A)D S
The Pentagon, Room 3D136
Washington, DC 20301-3090

Dr William H Press
Harvard College Observatory
60 Garden Street
Cambridge, MA 02138

Mr John Rausch [2]
Division Head 06 Department
NAVOPINTCEN
4301 Suitland Road
Washington, DC 20390

Records Resource
The MITRE Corporation
Mailstop W115
7525 Colshire Drive
McLean, VA 22102

Dr Victor H Reis
US Department of Energy
DP-1, Room 4A019
1000 Independence Ave, SW
Washington, DC 20585

DISTRIBUTION LIST

Dr Fred E Saalfeld
Director
Office of Naval Research
800 North Quincy Street
Arlington, VA 22217-5000

Dr John Schuster
Technical Director of Submarine
and SSBN Security Program
Department of the Navy OP-02T
The Pentagon Room 4D534
Washington, DC 20350-2000

Dr Michael A Stroscio
US Army Research Office
P. O. Box 12211
Research Triangle NC 27709-2211

Superintendent
Code 1424
Attn Documents Librarian
Naval Postgraduate School
Monterey, CA 93943

Dr George W Ullrich [3]
Deputy Director
Defense Nuclear Agency
6801 Telegraph Road
Alexandria, VA 22310

Dr Walter N Warnick [25]
Acting Director for Program Analysis
U S Department of Energy
ER30 / OER
Washington, DC 20585

Peter J Weinberger
22 Clinton Avenue
Maplewood, NJ 07040

Dr Edward C Whitman
Dep Assistant Secretary of the Navy
C3I Electronic Warfare & Space
Department of the Navy
The Pentagon 4D745
Washington, DC 20350-5000

Capt H. A. Williams, U S N
Director Undersea Warfare Space
& Naval Warfare Sys Cmd
PD80
2451 Crystal Drive
Arlington, VA 22245-5200

Mr Charles A Zraket
Trustee
The MITRE Corporation
Mail Stop A130
202 Burlington Road
Bedford, MA 01730