

Hi,

Here's my write-up to go with my
presentation to at the RSA

conference:

-matt

=====cut here=====

- Cryptography Policy and the Information Economy
 - Matt Blaze
 - AT&T Labs -- Research
 - 600 Mountain Avenue
 - Murray Hill, NJ 07974
 - 908-582-5524
 - mab@research.att.com
- DRAFT -- 27 December 1996 -- DRAFT

1. Introduction

This paper is a high-level
technical overview of the impact
of

cryptography on the computing
and communications industries,
with

emphasis on the implications of
the Administration's recent

cryptography policy initiatives.
It represents the best judgement
of

its author, and does not
necessarily reflect the position of
AT&T or

any other organization.

We argue that unless a
fundamental change is made in
the direction of

our cryptography policy, the
United States' dominance in the
emerging

`information economy" will
ultimately be placed in jeopardy.

In

particular, current policy fails to
recognize several increasingly

important realities of
cryptographic technology:

* The wide availability of
cryptography will soon be vitally

important to the sustained
growth of a wide range of
American

enterprises. This importance
will arise not so much from the
direct

economic benefits of the sale of
cryptography services and
products by

cryptography vendors, but
rather from the enabling effect
that

cryptography will have on the
advanced services that will form
the

basis for the ``information
economy." Cryptography will
eventually

be embedded in most, perhaps
virtually all, advanced
communications

products and services; it will not
be merely a ``stand alone" or

`add-on" feature as it is today.

* The ongoing discussion
between industry and government
in search of a

``compromise" export key
length that satisfies both parties is

ill-considered from a technical
point of view and offers little

promise of resolving the debate.
In particular, the government's

offer to allow limited
exportability of systems with 56-
bit keys in

exchange for industry support
for ``key recovery" is much less

attractive than it might seem at
first. Aside from the potential
high

cost of committing to a key
recovery infrastructure, 56-bit
keys are

not strong enough for many
applications today and will soon
be

recognized as not being strong
enough for most commercially
important

applications in the very near
future.

* The ``key recovery" approach promoted by current policy is too

expensive and too poorly
understood to provide a viable
basis for

widely-deployed commercial
cryptography. Cryptography, as
used to

protect communications traffic
and stored data, is intrinsically

rather inexpensive in terms of
its direct cost and performance
impact.

``Key recovery" technology, on the other hand, is inherently

expensive and entails potentially
large risks. If key recovery

becomes a required or standard
component of future
cryptographic

systems, it is likely to greatly
slow and otherwise impair the

development of many future
businesses that that will depend
on the

availability of inexpensive,
widely-integrated cryptography.

2. Cryptography and the information economy

Cryptography is concerned with
the use of mathematical
functions,

called ``ciphers'', that separate the security of a message's content

from the security of the media
over which it is transmitted.

There

are several different types of
cipher functions. The most
familiar

are intended to make it difficult
to understand the content of
message

without knowledge of the secret
``key". A related type of cipher

function can be used to ensure
that information has not been
altered.

Still other functions can be used
to establish the origin of digital

information (`digital
signatures"). Applications of
cryptography

include securing wired and
wireless voice and data traffic
against

eavesdropping, protecting
computer files from unauthorized
access, and

enabling secure electronic
business transactions
(`electronic

commerce").

Cryptography is not widely used
today, especially relative to its

potential. This is true for several reasons. First, traditional

communications media have
historically offered a degree of
intrinsic

security. For example, it has
always been relatively difficult
and

risky to illegally ``tap" a
conventional telephone line (the

eavesdropper must locate the
correct wire pair, arrange for a

physical connection and
somehow record and recover the
traffic

without detection). Similarly,
data networks, to the extent that
they

existed at all, have until recently
been closed, private systems,
with

messages routed primarily within
the part of the network controlled
by

the end user's own equipment.

The technology and economics of modern communications and computing

systems, on the other hand,
strongly favors media that have
little or

no inherent security. For
example, wireless telephones
have great

advantages in convenience and
functionality compared with their

familiar wired counterparts and
are comprising an increasing

proportion of the telephone
network. This also makes
eavesdropping

much easier for curious
neighbors, burglars identifying
potential

targets, and industrial spies
seeking to misappropriate trade
secrets.

Similarly, decentralized computer
networks such as the Internet
have

lower barriers to entry, are much
less expensive, are more robust
and

can be used to accomplish a far
greater variety of tasks than the

proprietary networks of the past,
but, again, at the expense of

intrinsic security. The Internet makes it virtually impossible to

restrict, or even predict, the path
that a particular message will

traverse, and there is no way to
be certain where a message really

originated or whether its content
has been altered along the way.

It

is possible, even common, for
electronic mail messages to route

through the computers of
competitors. There is every
reason to

believe that these trends will
continue, and even accelerate, for
the

foreseeable future. The users of these networks, however, have

learned to depend on the intrinsic
security of the technology of the

past.

At the same time, electronic
communication is becoming
increasingly

critical to the smooth functioning
of our society and our economy
and

even to protect the safety of
human life. Communication
networks and

computer media are rapidly
displacing the less efficient,
traditional

modes of interaction whose
security properties are far better

understood. As teleconferences
replace face-to-face meetings,

electronic mail and fax replace
letters, electronic payment
systems

replace cash transactions, and on-line information services replace

written reference materials, we
enjoy undeniable gains in
efficiency,

but our assumptions about the
reliability of even the most
mundane

transactions are often
dangerously out-of-date.

Cryptography is

frequently the only viable
approach to assuring security as
these

trends continue.

Fortunately, cryptography is
usually a rather inexpensive
technology

to deploy. Although the cost of developing new cryptographic

algorithms and engineering
cryptography into specific
applications can

be significant, the marginal cost,
in terms of direct expense and

performance impact, of adding
cryptographic security can be
quite low,

especially compared with other
options. In the past,
cryptography

frequently required the use of
special-purpose hardware to
perform the

cipher algorithms. With modern
programmable personal
computers and

microprocessor-based consumer
devices (such as cellular
telephones),

however, it is often possible to
implement encryption functions

entirely in software, sometimes
with little or no performance
impact.

Similarly, the operational costs of using cryptography can be near

zero. Modern key management techniques, such as the use of public-key

`certificates," typically require
only minimal infrastructural

support from on-line secure key
management centers. Some

applications, including most
secure file storage systems,
require no

trusted infrastructure at all and
entail essentially no operational

costs.

The availability of cryptography
will soon be vitally important to
the

future of the telecommunications
and computing industries, if not
to

the future of the American
economy more generally. This
importance

will arise less from the direct sale
of cryptography services and

products than from the enabling
effect the existence of
cryptography

will have on the services that will
form the foundation of the future

information economy.

Cryptography will eventually be
embedded in

most, perhaps virtually all,
communications products and
services; it

will not be a ``stand alone" or
``add on" feature as it is today.

It is in the direct interest of any
industry that hopes to benefit

from electronic commerce to
encourage wide availability of
high-quality,

inexpensive cryptographic
products that enable secure
communications

and commerce.

3. Technical analysis of the administration's current policy

Although there are no restrictions
on the sale or use of
cryptography

within the United States, strict
regulations govern the export of

products that include encryption features. In general, with narrow

exceptions for products for use
by US-owned and certain
banking

industry customers, export
licenses are not granted for
products that

provide more than 40 ``bits" of
protection. Many domestic
vendors

supply only exportable-strength
cryptography in their domestic

products, to ensure inter-
operability and to avoid the need
to support

multiple product lines. The
regulations that govern
cryptography

exports therefore constitute, in
effect, de facto restrictions

on the encryption available
domestically.

The ``strength" of an encryption system depends on a number of

variables, including the
mathematical properties of the
underlying

encryption function, the quality
of the implementation, and the
number

of different "keys" from which
the user is able to choose. It is
very

important that a cryptosystem
and its implementation be of high

quality, since an error or bug in
either can expose the data it

protects to unexpected
vulnerabilities. Although the
mathematics of

cryptography is not completely
understood and cipher design is
an

exceptionally difficult discipline
(there is as yet no general

`theory" for designing cipher functions), there are a number of

common cipher systems that have
been extensively studied and that
are

widely trusted as building blocks
for secure systems. The

implementation of practical
systems out of these building
blocks, too,

is a subtle and difficult art, but
commercial experience in this
area

is beginning to lead to good
practices for adding high-quality

encryption to software and
hardware. Users and developers
of secure

systems can protect against
weaknesses in these areas by
choosing only

cipher functions that have been
carefully studied and by ensuring
that

their implementation follows
good engineering practices.

The most easily quantified
variable that contributes to the
strength

of an encryption system is the
number of possible keys.

Modern

ciphers depend on the secrecy of
the users' keys, and a secret-key

system is considered well-
designed only if the easiest
``attack''

involves trying every possible
key, one after the other, until the

correct one is found. An
encryption system can be
considered secure

only if the number of keys is
large enough to make such an
effort

infeasible. Keys are usually specified as a string of ``bits";

adding one bit to the key length
doubles the number of possible
keys.

An important question, then, is
the minimum key length
sufficient to

resist a key search attack in
practice. As technology
advances and it

becomes possible to try keys
more quickly and economically,
keys that

might have once been considered
sufficiently long become
increasingly

vulnerable.

It is almost universally
recognized that 40-bit keys
provide virtually

no protection against such threats
today, except against the most

casual ``attacker". Even 56-bit
keys, which are used in the

20-year-old Data Encryption
Standard, are too short to protect

commercial information given a
modestly well-funded attack
model.

Both the Business Software
Alliance's ``Minimum Key
Length" panel[1]

(in which the author participated)
and the National Research
Council

Cryptography Policy[2] study
group have noted the
vulnerability of

these short keys. The
cryptography marketplace, to the
extent it

exists today, is also beginning to
understand this, with many

customers demanding
cryptography that is at least
strong enough to

withstand a commercially-
motivated adversary. The BSA
panel's

``Minimum Key Lengths" white
paper (perhaps the most

widely-circulated current
reference to address the issue)
concludes

that secret keys today must be at
least 75 bits to withstand a