April 20, 2005 -- Lecture 35

22C:169
Computer Security

Douglas W. Jones

Department of Computer Science

Some More Laws

Electronic Communications Bill

British: January 2000

Register crypto support service providers
defined broadly.

Makes electronic signatures legal
defined as a valid means of establishing the authenticity of the communication or data, the integrity of the communication or data, or both.

Prohibits this act from being used to require
key escrow.

Export controls on Cryptography

Unavoidable facts about Cryptography:

it is important to national defense.
many weapon systems must use it.
it is important to national diplomacy.

Therefore, national laws have

limited export of cryptographic tech.
limited use of cryptography.

One model has all crypto results

"born classified"

History of US Crypto Regulations

Early 1970's

Assume all crypto born classified

1976: Hellman and Diffie openly publish

New directions in cryptography

NSA alarmed, pushes for legislation!

Voluntary review system

Please ask NSA before publishing

Crypto tools subject to arms export controls

Just like cannons and bombs

State department permit
required to export strong crypto.

History of US Crypto Regulations II

CLIPPER crypto chip announced 1993

allowed for required key escrow system
CALEA, 1995 is what we got instead.

June 1995: RSA in Perl

```
#!/usr/local/bin/perl -s-- -export-a-crypto-system-sig -RSA-in-3-lines-PERL
($k,$n)=@ARGV;$m=unpack(H.$w,$m."\0"x$w),$_=`echo "16do$w 2+4Oi0$d*-^1[d2%
Sa2/d0<X+d*La1=z\U$n%0]SX$k"[$m*]\EszlXx++p|dc`,s/^.|\W//g,print pack('H*'
,$_)while read(STDIN,$m,($w=2*$d-1+length($n||die"$0 [-d] k n\n")&~1)/2)
```

British sold T-shirts with this to US.
Suggested tattoo to prevent deportation.
Two US newspapers printed snips of it.

Does first amendment apply to code?

History of US Crypto Regulations III

Jan 2000: Crypto export restrictions relax

Blanket license to export for civilian use, except embargoed countries.

But no guarantee it will stay this way!

Export for government use still licensed

Embargo list in constant flux:

Jan 2000 list was:

Cuba, Iran, Iraq, Libya, North Korea, Serbia, Sudan, Syria, and Taleban controlled areas of Afghanistan

Trusted Computing Initiative

Stated goal:

> *harden the platform from software-based attacks based on the expected behavior (trust) of the platform and transactions.* INTEL

Pro:

> *We desparately need it for secure systems.*

Con:

> *Push comes from RIAA, Hollywood.*
> *Goal seems to be to build systems that guarantee no copyright infringement.*
> *Goal could be to ban systems that do not incorporate the trusted platform.*