Crypto Politics and Export Controls

In God we trust. All others we monitor

— NSA motto

Crypto Politics

It's almost impossible to avoid this

Some larger companies have special legal divisions set up just for this

Any real policy information is obtained through (US) freedom of information act (FOIA) lawsuits rather than official press releases

- Claimed policy and actual policy are often complete opposites

Data Storage vs Session Encryption Key Recovery

Legitimate need for stored data recovery in case of accident/lost keys/termination of employment

- Use secret sharing scheme for emergency access

No legitimate need (or commercial incentive) for communications session recovery

- If there's a problem, re-transmit the data

Strong push by governments to convince companies that data storage recovery = communications recovery

- Key recovery has been given so many names (key escrow, law enforcement access, key recovery, data recovery, trusted third parties, etc etc) that it's now known by the general term GAK (Government Access to Keys)

Early History

1977 NSA tried to block NSF funding of crypto research
Attempt to intimidate IEEE over security conference

1978 NSA uses Invention Secrecy Act to classify crypto patents

1979 Bobby Ray Inman's "The sky is falling" speech: NSA should control crypto research

1982 NSA blocked NBS request for public-key equivalent of DES

1984 NSDD-145 moves control of computer security from NBS to NSA (NSA memo calls NSDD-145 "NSA-engineered")

1986 NSDD-145 extended to allow NSA jurisdiction over private databases (Dialog, Compuserve)
NSA tries to decertify DES
CCEP (Commercial COMSEC Endorsement Program) using NSA-designed tamperproof hardware (eg Blacker)

Early History (ctd)

1987 Computer Security Act moved control of crypto back to NBS

1988 NSA tries to block publication of Khufu block cipher

1989 NSA/NIST memorandum of understanding moves control of crypto back to the NSA

1990 NSA designs signature-only PKC for NIST, begins work on Clipper

1991 NIST announces DSS and NSA-designed SHS
Industry reaction was almost universally negative

Digital Telephony

Law Enforcement Requirements for the Surveillance of Electronic Communications, 1992

- Real-time, full-time monitoring capability
- Intercepts undetectable to all parties (including service providers)
- Multiple simultaneous intercepts possible
- Decoding or decryption of all communications
- Supplementary information provided is:
  - Directory number, associated directory number, line equipment number, call type/bearer capability, service profile identifier, PBX directory number, PBX station identifier, electronic serial number (ESN), mobile identification number (MIN), termainl equipment identifier, and service site information (for cellphone tracking)

Digital Telephony

FBI spent two years promoting it (Operation Root Canal)

Digital Telephony & Privacy Improvement Act passed as Communications Assistance for Law Enforcement Act (CALEA), October 1994.

- FBI cost estimate (1992-1994): ~~$150M~~ ~~$300M~~ $500M
- Industry cost estimate (1994): $3B
- More recent study (1998): $8B per year
  - $12M per court-approved wiretap

CALEA still isn't reality

- Cost
- Technical difficulty

Clipper

1992 AT&T announces the AT&T 3600 Telephone Security Device (TSD), a commercial DES-encrypted phone add-on

The NSA goes ballistic

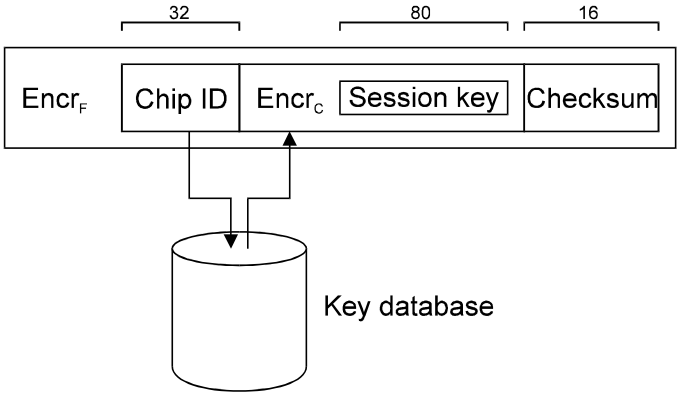
- NSA convinces AT&T to use Clipper in the TSD in exchange for guaranteed government purchases
- US government buys entire DES-based TSD production run of 9000, pays AT&T to retrofit them with Clipper

15 April 1993, White House announces Clipper

- CCEP laundered for public acceptability
- Third-party access guaranteed through Law Enforcement Access Field (LEAF)
  - Originally LEEF, then LEAF, now DRF

Clipper (ctd)

128-bit LEAF contains session key encrypted with Clipper family key and per-chip key



Clipper (ctd)

Clipper in operation

- Other party and third party decrypt LEAF with family key
- Both use checksum to detect bogus LEAF
- Third party looks up chip key in database, decrypts session key
- To increase public acceptability the key database is stored by two different agencies
- Communicate secure in the knowledge that only the worlds largest spy agency is listening

Clipper Weaknesses

80-bit key is too weak

Skipjack algorithm used in Clipper had no public scrutiny

16-bit checksum can be defeated

Cipher operation mode (OFB) allows message forgery

Chip ID served to neatly tag and identify every communication

Reaction to Clipper

80% of Americans opposed it

Of over 300 submissions, only 2 were supportive

Clipper adopted as Escrowed Encryption Standard (EES), FIPS 185, in February 1994

- The legal machinations required to get this adopted fill a 200-page law journal article

Noone bought Clipper

- AT&T shut down its product line
- FOIA'd documents obtained later showed that the government had a secret key escrow policy which was the exact opposite of the publicly claimed Clipper policy

Fortezza

Based on Capstone (Clipper + DH + DSA + SHA)

- Key exchange uses KEA, modified DH/DSA
- Data encryption uses Skipjack, NSA-designed block cipher

Specifics were a moving target

1991 = Pre Message Security Protocol (PMSP), device = smart card

1993 = MOSAIC, device = Tessera card

1994 = Multi-Level Information Systems Security Initiative (MISSI)

Later = Fortezza

Fortezza (ctd)

Used to implement MSP in the Defence Message System (DMS), the DoD's Internet

- DMS provided financial encouragement for Fortezza (Netscape, Oracle received $5M encouragement each)
- Fortezza cards are expensive
  - $70 each for the government
  - ~$250 each for everyone else
- Cards require PCMCIA readers and software
  - Have to shut down workstation to insert/remove card
  - Fortezza drivers conflict with other PCMCIA drivers
- Attempts were made to sell Fortezza to foreign governments

Later Fortezza versions removed GAK and added more useful (but classified) ciphers (eg Baton)

Skipjack

Skipjack and KEA were declassified in early 1998

- Expensive and scarce hardware necessitated software implementations, which would have been reverse-engineered
- Release was a denial-of-service attack on the worlds cryptographers
- 32-round, fairly conventional block cipher
  - Breakable if limited to 31 rounds
- Implementations were available worldwide within hours
- KEA specification contains errors, can't be implemented as per the specification

Post-Clipper Crypto Restrictions

Commercial key escrow, June 1995

- Anti-Electronic Racketeering Act
  - Outlaw distribution of encryption software

Clipper II, November 1995

- Software key escrow
- Up to 64-bit exportable with backdoors

Lotus Notes, January 1996

- 64-bit key with 24 bits held by the NSA
- Swedish government didn't discover this until 1998

Post-Clipper Crypto Restrictions (ctd)

Policy laundering, 1996

- Persuade the OECD to adopt US-style restrictions
- Special OECD ambassador appointed to lobby OECD nations
- OECD rejected US position

Clipper 3, May 1996

- More escrow based on X.509

NRC report, May 1996

- Don't restrict crypto
- Allow DES export
- Crypto debate can be carried out in public

Post-Clipper Crypto Restrictions (ctd)

Clipper 3.1, July 1996

- Even more software escrow
- Allow export now if you build in backdoors later
  - Even if backdoors were available now, there'd be no way to manage them

After 1996, an endless series of trivial revisions to Clipper 3.x

- "Dance of the seven (hundred) veils"

Boiling the Frog

Intent is to buy off the loudest opponents until only the ones who can be safely ignored remain

- Banks and financial institutions pacified with SGC
- Fortune 500 pacified with special export dispensations
- Subsidiaries of US companies pacified with case-by-case export of strong crypto
- Hospitals, some governments pacified with occasional special-case exports when they complain loudly enough

Only software companies losing foreign sales and civil liberties groups now remain

US to Relax Export Controls

This exact same announcement has been made (on average) every three months since April 1994

- The pace has accelerated in the last year or two

The same DES export announcement has been recycled more than half a dozen times

- “encryption products using keys of up to 56 bits will be allowed for export”
- “a relaxation of controls for non-recovery encryption products up to 56-bit key length DES”
- “allowed export of encryption whose keys are as long as 56 bits”

(one is from 1996, one from 1997, one from 1998)

US to Relax Export Controls (ctd)

In 1994 you couldn't buy general-purpose strong crypto from the US

... dozens of export control press releases later...

In 1999 you still can't buy general-purpose strong crypto from the US

Export Controls

The four rules of US export controls

1. They don't make any sense
2. They change constantly
3. If you get it wrong, you go to jail
4. The enforcers have no sense of humour

Corollary

- If there's a rule you don't like, wait. It'll change
- If there's a rule you like, wait. It'll change

US Export Controls

Based on International Traffic in Arms Regulations (ITAR), 1943 law designed to stop Nazi Germany and Imperial Japan from obtaining US technology

Redone as EAR (Export Administration Regulations) in 1996

- ITAR was handled by the State Department who allowed almost nothing out
- Intent of EAR was to transfer controls to the more business-friendly Commerce Department
  - Unfortunately the State Department baggage came with them
  - Government showed software companies a piece of prime real estate, then moved the boundary markers into a swamp once they'd signed the cheque

US Export Controls (ctd)

Export controls don't exist as a conventional law

- In the third week of August of each year, the US president declares a national emergency under the International Emergency Economic Powers Act, 1933 (based on the Trading with the Enemy Act, 1917), with the duration of the emergency being one year
  - The emergency being used is the Great Depression
- Using the powers given to him by the act, he issues a presidential decree which extends the export controls for another year
- The following year at the same time, the charade is repeated
- The constitutionality of this has been called into question

Effects of Export Controls

Export controls are completely ineffective in stopping anyone from acquiring any type of encryption

- Anyone who wants it can get strong encryption anywhere within minutes
- Average public key sizes used when users have a choice
  - 1024 bits in 1996
  - 2048 bits in 1998
- (corresponding to the default "strong" encryption key size in PGP 2.x and 5.x)

but...

Effects of Export Controls (ctd)

Export controls are highly effective in ensuring that the masses have no real security

- The majority of all crypto in use worldwide is crippled or broken
  - 77% of Thawte users are using weak encryption
  - 60% of them are in the US
  - For most of its existence, Verisign issued weak (512-bit) keys to users outside *and inside* the US

Effects of Export Controls (ctd)

In practice, US companies have strong encryption, everyone else has weak encryption

Practical example of export control effects is demonstrated by CIA hacking into European parliament computers in 1996 (Sunday Times):

> "includes details of the private medical and financial records of many MEPs and officials, and discussion documents on confidential issues, including trade, tariff and quota agreements. The breach came to light when officials believed that American negotiators had been given advance warning of confidential European Union positions in last year's trade negotiations"
>
> "They were able to exploit the fact that parts of the system were manufactured by two American firms"

Economic Effects of Controls

The worldwide crypto market is in the low billions, but sales which require crypto are in the hundreds of billions

- 500 non-US firms sell 700 crypto products
- A web search for encryption produced over 50,000 hits
- RSADSI claims 300 million RSA products are used worldwide

Controls lead to lost sales and slowed growth in encryption-dependent industries

Cost savings due to intranets and extranets can't be realised

Economic Strategy Iustitute report estimates the US crypto policy will cost US industry $50B in 2003, $65B in 2004

- Imposing GAK would cost $140B as everyone switched to foreign products

Legal Challenges to US Controls

Three main challenges, intent is to get a Supreme Court ruling on export controls

Karn Case, 1995

- "Applied Cryptography" can be exported as a book but not as a floppy disk

Bernstein Case, 1995

- ITAR/EAR is unconstitutional since it violates the First Amendment

Junger Case, 1996

- Export controls prevent the teaching of crypto to foreign students (still being decided)

French and Russian Crypto Controls

French controls are based on the "decret de 18 avril 1939"

- On a scale of 1 to 8, encryption is rated 2
  - Netscape is the second most dangerous weapon type recognised by the French government
- Modified constantly over the years, "decret 86-250 du 18 fev 1986" explicitly mentions encryption software, "loi 90-1170 du 29 decembre 1990" requires approval for encryption use from the Prime Minister
  - "If you don't tell us you're using PGP, noone will bother you. If you ask us for permission to use it, we will refuse" — J. Vincent-Carrefour, head of the SCSSI

French and Russian Crypto Controls (ctd)

- Companies big enough to afford it would go to some lengths to sidestep the controls
  - Daily couriers carried information from Paris to London
  - Information was encrypted and sent to corporate HQ
  - Replies were decrypted and carried back to Paris
- 40-bit encryption was allowed in 1996 after a French researcher demonstrated how easy it was to break

French controls were removed in 1999 after publication of a European Parliament report detailing massive US communications interception and surveillance initiatives in Europe (Echelon)

- Sole effect of controls was to make US industrial espionage easier

French and Russian Crypto Controls (ctd)

Russian controls created by presidential decree (ukaz), April 1995

- Places encryption under the control of Federal Agency for Governmental Communications and Information (FAPSI), a department of the (former) KGB
- Requires that all commercial banks dealing with the Central Bank of Russia, and by extension all businesses dealing with that, use only FAPSI-approved encryption
- Provides a nice guaranteed money-earner for the (ex-)KGB.

"The severity of Russian law is compensated for by it's non-mandatoryness". Individuals and companies openly use and sell encryption with no repercussions

Non-US controls

Based on Cold War COCOM controls

- Predated PC's, fax machines, the Internet, etc. Regarded as archaic and unrealistic
- Run from the US embassy in Paris, seen as merely an extension of the US State Department
  - COCOM-era "New Zealands Export Controls" are actually US documents with US wording and spelling
- Growing resentment in Europe where controls were seen as US-imposed trade barriers

Wassenaar and Software Export

COCOM was disbanded in March 1994, reformed as the Wassenaar Arrangement in November 1996

- Wassenaar = COCOM with the section numbers changed (and localised spelling)

Wassenaar has four main purposes, of which one is to "not impede bona fide civil transactions"

In recognition of COCOM's unrealistic nature, Wassenaar created blanket exceptions for public domain and mass-market software

- Software exceptions are implemented via the General Software Note (GSN)

Wassenaar and Software Export (ctd)

```
General Software Note (GSN)

(This note overrides any control within section D of
  Categories 0 to 9)

Categories 0 to 9 of this list do not control
  'software' which is either:

  a. Generally available to the public by being:
    1. Sold from stock at retail selling points,
       without restriction, by means of:
      a. Over-the-counter transactions;
      b. Mail order transactions; or
      c. Telephone order transactions; and
    2. Designed for installation by the user without
       further substantial support by the supplier; or
  b. 'In the public domain'
```

Wassenaar and Software Export (ctd)

'In the public domain' is defined as:

```
'Technology' or 'software' which has been made
  available without restrictions upon its further
  dissemination (copyright restrictions do no remove
  'technology' or 'software' from being 'in the public
  domain')
```

('technology' and 'software' are further defined)

This allows almost unrestricted crypto software export

Doctoring Wassenaar

After Wassenaar was finalised, Australia and New Zealand altered it as follows:

```
With the exception of Category 5, Part 2 (Information
  Security), Categories 0 to 9 of this list do not
  control 'software' which is either:
```

The altered form of the Wassenaar text reverses the original intent and directly contravenes the requirement that the controls not impede bona fide exports

- Noone has ever been able to explain why this alteration was made, or by whom

Enforcing the Controls

"My life as an international arms courier", 1995

- Attempt to export US-exportable crypto device
- Noone knew how to handle this "routine" export
  - "Anyone trying to follow the regulations is forced to jump through pointless hoops so obscure that even the people charged with enforcing them don't know what to make of them"

"My life as a Kiwi arms courier", 1998

- Noone in NZ knows what to do either

Enforcing the Controls (ctd)

Typical effects of controls on US companies

- "Order placed by *large foreign company*"
- "Advised that approval would be unlikely"
- "Contract went to foreign competitor"

There are hundreds of these cases, totalling hundreds of millions of dollars

Menwith Hill

World's largest regional sigint interception centre (RSOC)

Located in UK, staffed by 1,200 US personnel

Intercepts communications from all over Europe for transmission back to the US

- 28 radomes
- Outgoing comms capacity for 100,000 simultaneous phonecalls
- Taps into UK microwave trunk at Hunters Stones, this carried almost all UK long-distance calls in the 1970's and 1980's
- NSA director Studeman statement on state of interception in 1992
  - 2 million intercepted messages/hour
  - 17.5 billion intercepted messages/year

Menwith Hill (ctd)

SILKWORTH

- 56 satellites which intercept long-distance microwave links
- Mercury, Mentor, Trumpet, satellites controlled via the RUNWAY radomes

MOONPENNY

- Unauthorised interception of standard satellite communications

Echelon

US interception stations similar to Menwith Hill are scattered worldwide

Intelsat

- Morwenstow, UK (Atlantic satellites)
- Rossman, North Carolina (Atlantic satellites)
- Sugar Grove, West Virginia (Atlantic satellites)
- Yakima, Washington (Pacific satellites)
- Geraldton, West Australia (Indian ocean satellites)
- Waihopai, NZ (Pacific satellites)

Echelon (ctd)

Other satellites

- Bad Aibling, Germany
- Bude, Cornwall
- Kojarena, Australia
- Leitrim, outside Ottawa
- Menwith Hill again
- Misawa, Japan
- Sabana Seca, Puerto Rico (US)
- Shoal Bay, outside Darwin

Echelon (ctd)

Radio

- Many sites in the US and UK
- Bamaga, Australia
- Diego Garcia, Indian Ocean
- Tangimoana, New Zealand

Currently around 120 satellite collection systems are in operation

- 40 targeting western commercial communications satellites
- 30 controlling space-based interception satellites
- 50 targeting Soviet communications satellites (some have since been reassigned to commercial western satellites)

Echelon (ctd)

US satellites monitor terrestrial radio, microwave, and cellphone communications

- Operated by CIA and NSA, launched by NRO
  - Ferret in 1960's
  - Canyon, Rhyolite, Aquacade in 1970's
  - Chalet, Vortex, Magnum, Orion, Jumpseat in 1980's
  - Mercury, Mentor, Trumpet in 1990's
    - Cost ~$1B each
- Orion, Vortex intercept telecoms, Trumpet intercepts cellphones
- Britain (Project Zircon) and France (Project Zenon) have attempted similar schemes

Echelon (ctd)

- Ground stations located in
  - Buckley ANGB, Denver, Colorado
  - Menwith Hill, UK
  - Bad Aibling, Germany
  - Pine Gap (Merino), Australia

Information is collected and processed at Regional Sigint Operations Centres (RSOC)

- European RSOC, Bad Aibling, Germany
- Central RSOC, Fort Gordon, Georgia
- Pacific RSOC, Kunia, Hawaii
- Atlantic RSOC, Menwith Hill, UK
- Southern RSOC, Lackland AFB, Texas

Echelon (ctd)

Stations intercept private phonecalls, faxes, telexes, emails, and other communications and forward them to the NSA

All communications are automatically scanned for keywords (PATHFINDER at Menwith Hill) and/or voice patterns (VOICECAST at Menwith Hill)

- Economic information is forwarded to US companies by the Office of Intelligence Liason
- Preferential beneficiaries are the defence contractors (Lockheed, Boeing, Loral, TRW, Raytheon) who built Echelon

Echelon is covered in the European Parliament reports "Assessing the Technologies of Political Control" and "Interception Capabilities 2000"

Blind Signal Demodulation

Signal demodulation without the cooperation of the sender/receiver

Avoids the need for adapative equalisation or other initialisation and training

- Automatically adapts to modulation techniques such as QAM
- Can adapt to unknown baud rates (V.34 can employ any of six symbol rates)
- A decade ago this was regarded as impossible to do

Implemented in standard DSP hardware (modems) or ASICs (digital video, digitalmicrowave)

Modem signals can be demodulated in software using a Pentium MMX/MicroSparc

Blind Signal Demodulation (ctd)

Typical commercial blind demodulation equipment

- Voice Channel Demodulator
  - Input = E1 or E3
  - Output = all leased-line and dialup modem, fax, voice, and digital data signals with all data and protocols (eg V.42bis compression, PPP, and Internet protocols like POP for a modem link) decoded

Blind Signal Demodulation (ctd)

- Signals Analysis Workstation
  - Input = Any type of link signal (FDM basebands, IF signals, PCM bitstreams, DS1 bitstreams, Ethernet)
  - Output = modem, fax, pager, cellphone, voice data decoded and ready for use
  - "VGC content identification, signalling recognition, train-on-data capability. Easy to use GUI with extensive online help"
- Ex-NSA satellite interception gear is occasionally sold as surplus

Data Analysis

Custom hardware used to speed analysis

- Paracel Fast Data Finder (FDF) contains 6,000 to 12,000 custom processors
- "The fastest, most accurate adaptive information filtering system in the world"
- Typical application compares 1GB of data against 50,000 match profiles every day
- Standard US test benchmark involves locating information about "Airbus subsidies"

NSA-developed N-gram analysis, a general method to retrieve data according to topic

- "Find every document covering the same topic as this one"
- System works on very large data sets and in presence of errors

Undersea Cable Tapping

Operation IVY BELLS tapped Soviet cables in the Sea of Okhotsk

- Tapping occurred from 1972 to 1982, when an NSA employee sold the details to the Soviet Union
- From 1979 to 1992 a cable in the Barents Sea was similarly tapped
- Submarine crews who placed the taps earned presidential citations
- Every year from 1994 to 1997, crews have received similar commendations (noone knows what for)

Echelon in Action

German company Enercon GmbH develops a new type of wind energy generator

Shortly afterwards, US company Kennetech filed a patent for exactly identical technology in the US

- Obtained a court order preventing Enercon from operating in the US

Loss to Enercon: 100 million DM, 300 jobs

- Enercon now uses secure communications methods

Enercon data was probably intercepted via the NSA RSOC in Bad Aibling, Germany

- GCHQ ordered UK patent office to use 256-bit public-key encryption to communicate with European patent office in Munich, Enercon may have been using similar “security”

Other Typical Echelon Uses

- Aiding transfer of $200M Indonesian deal from NEC to AT&T (Der Spiegel)
- Forwarding details of Thomson-CSF deal in Brazil to Raytheon (Baltimore Sun)
- Obtaining Japanese research on advanced automobiles for Ford, GM, and Chrysler (Mainichi)
- Providing information to US negotiators facing Japanese car companies in trade dispute (New York Times)
- Providing information on APEC deals to Democratic Party campaign contributors (Insight Magazine)
- Intercepting Mexican trade representatives during NAFTA negotiations (Financial Post (Canada))
- Intercepting Canadian negotiations for sale of 3 reactors to South Korea (Financial Post (Canada))
- Monitoring activities of Robert Maxwell (Financial Mail (UK))

Other Typical Echelon Uses (ctd)

NSA also targets private individuals

- NSA maintained 1,056 pages of files on Princess Diana (Washington Post)
- NSA produced 39 internal publications on Diana
- Information was collected over a period of years
- "NSA systematically intercepts international communications, both voice and cable"

  — NSA Director Lt.General Lew Allen testifying before Congress

Other Typical Echelon Uses (ctd)

"Within Europe, all email, telephone, and fax communications are routinely intercepted by the United States National Security Agency"

— European Parliament report "Assessing the Technologies of Political Control"

- This report prompted the French government to remove its crypto restrictions

"The end of the Cold War has not brought to an end the Echelon eavesdropping system. This system has become a weapon of economic warfare"

— Rossiyskaya Gazeta (Russian state-funded daily paper)

Echelon is "this incredible communications vaccuum cleaner"

— Il Mondo

Other Typical Echelon Uses (ctd)

"Former intelligence officials say tips based on spying […] regularly flow from the Commerce Department to US companies to help them win contracts overseas"

— The Baltimore Sun

Interception Capabilities 2000

European parliament report on Echelon

- Annual communications interception budget = $15-20 billion
- "Comprehensive systems exist to access, intercept and process every important modern form of communications, with few exceptions"
- Intent of US diplomatic initiatives over crypto controls was motivated by intelligence collection requirements, "a long-term program which undermines the communications privacy of European governments, companies, and citizens"
- "Documents obtained under the Freedom of Information Act indicate that [crypto] policymaking was led exclusively by NSA officials, sometimes to the complete exclusion of police or judicial officials"

Echelon and Export Controls

With the end of the cold war, intelligence agency concerns switched from INFOSEC and COMSEC to JOBSEC

Increasingly, economic and industrial data rather than military data was targeted

- Some countries had been doing this for decades
- Intelligence agencies feed information obtained from foreign companies back to favoured local companies
  - – Whole books have been written about these things
- If crypto were freely available, this goldmine of economic, industrial, and trade information would dry up
  - – Despite the rhetoric about terrorists and pornographers and other bogeymen, it's really about money

Echelon and Export Controls (ctd)

Export controls are utterly ineffective on an individual basis, but extremely effective for blanket surveillance and espionage

- Export controls help criminals and terrorists by leaving information systems vulnerable to attack

If crypto becomes widespread, the spooks will lose a $*x*00-million-dollar investment in surveillance technology

- The export controls will never go away if the spooks can help it

"The real aim of current policy is to ensure the continued effectiveness of US information warfare assets against individuals, businesses and governments in Europe and elsewhere" — Ross Anderson

Cloud Cover

Confidentiality Key Infrastructure (CKI)

Designed by CESG, the trading name of GCHQ

Design goals

- PKI provides trust infrastructure for keys
- CKI provides backdoor access infrstructure for keys

Cloud Cover (ctd)

CA's are replaced by certificate management authorities (CMA's)

- CMA's provide shared key generation capability
- Can recover the confidentiality keys used by both parties
- Can recover signature keys distributed via confidentiality keys
- Can revoke the ability of parties to communicate in private

CMA's were referred to as "trusted third parties", yet another new synonym for GAK

Problems with Cloud Cover

Provides no benefit over PKI, and many liabilities

Very complex protocol

- Generation of a simple shared key is a laborious, multi-step process
- Nothing works without the CMA's cooperation

Assumes the only threat is from outsiders

- UK security incident statistics show ~95% of attacks are by insiders
- Cloud Cover facilitates these attacks immensely

Problems with Cloud Cover (ctd)

Attempt made to sell Cloud Cover to the National Health Service (NHS)

- Rejected by the British Medical Association and NHS

Flaws found in the protocol

- Still being pushed by CESG in hospital "pilot projects"

DTI Proposals

Only GAK CA's (and signatures) will be recognised by law

Goverment is allowed secret access to GAK'd keys

- Access is granted by request, not by court-ordered warrant
- GAK accesses/usage must be kept secret

Non-UK (non-GAK) signatures will not be recognised

- Under the EU digital signature reciprocity rules, UK signatures will not be recognised anywhere else
- "We need to make sure all our laws and rules are e-commerce friendly"

DTI Proposals (ctd)

UK companies/individuals are given a choice:

- Submit to warrantless secret surveillance of private communications

or

- Opt out of e-commerce

"This is not mandatory key escrow"

DTI were awarded the 1998 Big Brother Award (national government category) for their efforts

GAK Problems

Critically dependent on the honesty of criminals in complying with GAK requirements

Trivially defeated by

- Use of non-GAK software
- Double encryption with strong crypto hidden by GAK crypto
- Use of doctored GAK software (Clipper protocol failure)
- "If the sender and receiver collaborate to defeat KR [key recovery], there is no technical method from preventing this" — NSA study on key recovery

Many keys can't be GAK'd

- Session keys are set up and discarded on the fly
- Securely transporting this continuous flood of keys to a GAK centre is practically impossible

GAK Problems (ctd)

Building the infrastructure is well beyond the state of the art

- Law enforcement requires 24/7 access to keys, usually in real time
- After 10 years of work on X.509 we can't even move public keys around yet

Handing over keys demonstrates a lack of presumption of privacy → no warrant necessary

- ECPA ruled that cordless phones, radio communications have no expectation of privacy

NSA Study on Key Recovery

"Threat and Vulnerability Model for Key Recovery", February 1998

- Rogue users will bypass any KR mechanism
- Rogue KR agents/LE agents pose "the most formidable threat"

Summary of report: GAK won't have any effect on the bad guys, and greatly jeopardises the good guys

- Governments will try to implement it anyway

German government:

> "A US-style 'key recovery' system cannot be reconciled with national security interests"

GAK in Practice

Example of centrally-managed key centre: Bank with 25,000 employees

- Used centrally-managed mainframe passwords
- 30 full-time employees barely coped

GAK schemes are vastly more complex than this simple password example

Convervative US estimate is 90M keys escrowed per year

- Using the banking key centre figures, this would require 100,000 people to manage
- A secret shared by 100,000 people isn't terribly secret

GAK in Practice (ctd)

The fact that GAK is so far beyond the state of the art is probably the biggest protection against it being implemented any time soon