Royal Holloway
University of London

Information Security: Finding the Right Balance

Fred Piper, M.Inst.ISP

Codes & Ciphers Ltd
12 Duncan Road
Richmond
Surrey
TW9 2JD

Information Security Group
Royal Holloway, University of London
Egham
Surrey
TW20 0EX

Aims of Lecture

- To enjoy ourselves
- To promote thought/discussion about the difference between theory and practice
- To suggest the importance of security cultures and the human factors of information security
- No statistics or formal analyses

What needs balancing?

- Cost of Security versus Cost of Insecurity
- Security versus Convenience
- Security versus Privacy
- Law Enforcement’s Needs versus Rights of the Individual

Some Unfortunate ‘Facts’

- There is no such thing as 100% security
- In theory there is no difference between theory and practice but in practice there is
- There is also (usually) a wide gulf between idealism and realism

An Analogy with Road Safety (1)

Why do we have a road network?

- To enable (fast) travel

Can we eliminate all accidents?

- NO

Do we try to minimise accidents?

- YES
  - Traffic lights
  - Driving tests
  - Vehicle tests
  - Fines/punishments
  - Speed limits
  - Sleeping policemen

An Analogy with Road Safety (2)

Is there an acceptable level of accidents other than none?

In theory: NO

In practice: We have to accept that accidents will happen if we want ‘fast’ travel (i.e. Faster than walking pace)

An Analogy with Road Safety (3)

Other ‘influences’ that may decide if we drive (other than safety)

- Health
- Parking
- Environment
- Public transport

An Analogy with Road Safety (4)

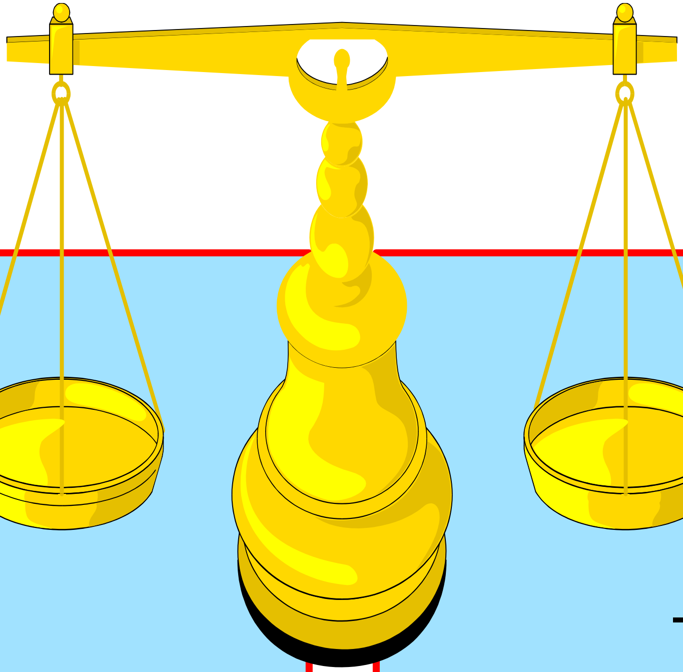
- There are agreed ‘standards’ for a worldwide infrastructure for car drivers
- Legislation exists to ‘protect’ road users from each other
- Road usage grew more slowly than use of personal computers, the Internet etc

Fundamental Question

- Is it possible to be honest/realistic about the ‘imperfect’ levels of security without causing panic or being accused of being:
  - Negligent?
  - Incompetent?
  - Irresponsible?
  - Uncaring?

- Example from personal experience
  - Encryption for a public service

A slide from the early 1980s



Security is a cost:

- To buy
- To manage

Insecurity is a cost:

- Direct losses
- Consequential losses

The objective is to minimise the sum of the two costs

Whose Costs?

Information systems may have many players including:

- Business owner
- System user
- Business customer
- System administrator

The ‘costs’ and losses may be different for each player

- A large loss for a customer may be a small loss to the business

The Innovation Process (an idealistic view?)

Inventers/Entrepreneurs/Governments

- Invent new technology
- Suggest new business applications
- Suggest ‘measures’ to improve ‘quality of life’

Friendly security professionals

- Identify ‘weaknesses’
- Suggest extra ‘features’
  - Technology
  - Procedures
  - Contracts
  - Legislation

Civil libertarians

- Consider Human Rights issues

After Launch

- Enter ‘unfriendly’ attackers
  - Criminals?
  - Academics?
- Often better resourced
- No deadlines
- What happens if they find a weakness?

Assessing Risk of Launch Time

Business Risk

- Project may be delayed or cost more in order to get the security ‘right’ (whatever that means)
- Users may not take up the service if we delay

Security Risk

- At some time, down the line, a security breach that we have not identified may occur

Pragmatic Decisions

- Unless you are exceptionally strong willed, or paranoid, the obvious conclusion is ‘let’s get the system delivered and then fix the security later if there turns out to be any problems’

Changing Vulnerability Scenario

- **Complexity of networks** means
  - No one really understands the complete system
  - No one can predict all methods of compromise
- **Connectivity/interoperability** mean
  - One person’s vulnerability may represent a threat to everyone (viruses, worms, Trojans exploit common vulnerabilities)
- Problems with patch management

Are There Tensions?

- For users:
  - Security versus convenience
- For Governments/civilians:
  - Security versus privacy
- For business:
  - Security versus business opportunities
    - Business says “go ahead”
    - Security says “slow down”

NOTE: Business usually wins!

Concerns

Employees (citizens) should ask the following about employers (Governments)

- What DO THEY SAY they do?
- What DO THEY REALLY do?
- What CAN they do?
- What WILL they do?

Companies must give assurance on all these issues

Employees' reaction will depend on the level of trust they have

User Recognition

- Three factors for identifiers
- All three methods require initial identification
- Process then confirms that person being recognised is person who registered
- Importance of registration and recovery from compromise are often overlooked

Security versus Convenience (A personal experience)

- Replacing my credit card
  - I could have been anyone
  - Does it matter?
- Fear of inconveniencing user for security

Protecting Privacy

What is involved?

- Strategic Information

  Stored Data

- Tactical Information

  Communications

- Anonymous actions

Warning

Question

If you have nothing to hide why do you care?

Possible answer

The future use of data is unknown

Who invades privacy?

Inquisitive ‘friends’

Business

Press

Government/Law Enforcement/Intelligence

Industrial Espionage

Crime/Terrorism

Why do people invade other’s privacy?

‘Noseyness’

Research/Marketing

Breaching and upholding rights?

Breaching and abusing rights?

The price of Privacy?

1. Postage stamp - letters
2. Inconvenience - E-mail
3. Inconvenience - Trash disposal
4. September 11th - Intelligence Failure

Accountability Matrix

Tools that let me see what others are doing	Tools that let others see what I am doing
Tools that stop me seeing what others are doing	Tools that stop others seeing what I am doing

Recent UK Government Leakages

There have been an unreasonably high number of recent leakages of personal data

FAQs:

- Is the Government capable of looking after confidential data?

Personal answer: YES

- Why have there been some many leakages?

Personal answer: Not treated personal data with the 'respect' it deserves

Personal Details
Do they need to be kept secret?

Some are public (for most of us)

- Name and address
- Home telephone number (if we have one)

Some are personal

- Bank balances
- Health records

Some identify us

- Passwords
- Bank account details
- National Insurance Numbers

Balance Again: Reactive or Proactive?

Knee-jerk reaction or sustainable solution?

MOD:	Laptop stolen - All laptops withdrawn
BARCLAYS:	Think Privacy (culture change!) Do you need to take this information home?

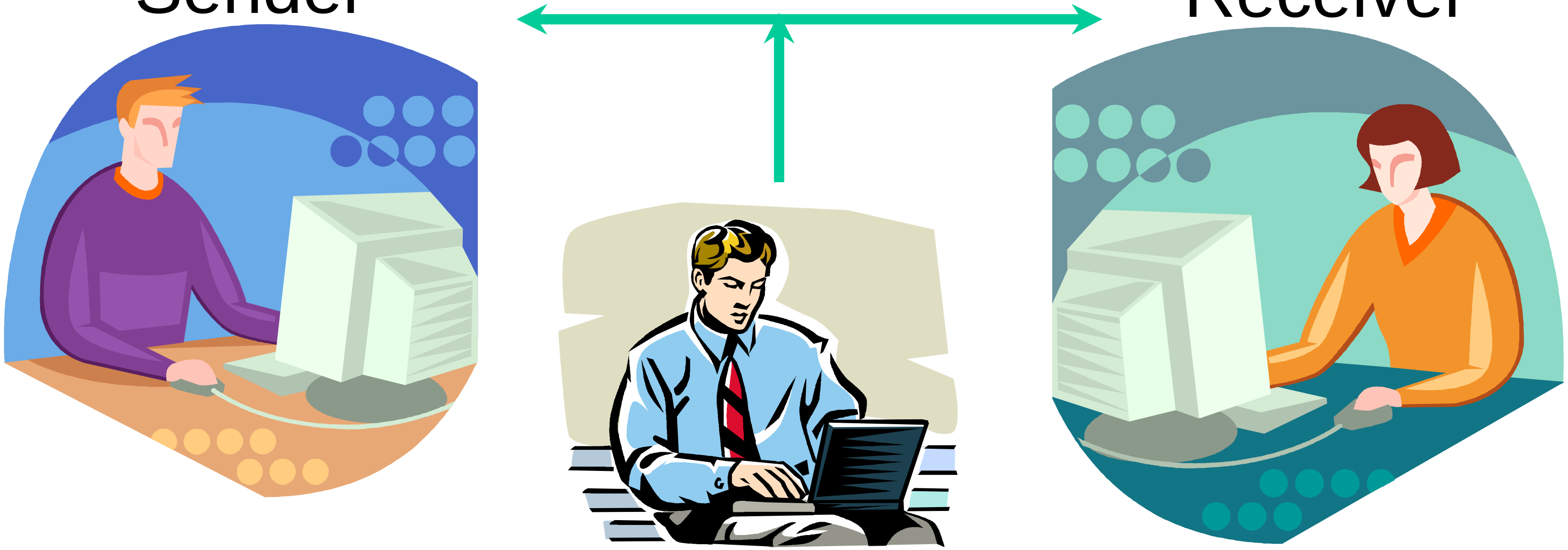
Control of Encryption

The widespread use of encryption for confidentiality has always been a cause of concern for Governments

Over simplification of objectives

- To provide strong encryption for use for ‘good’ purposes
- To be able to break encryption used for ‘bad’ purposes

Saints or Sinners ?



Sender

Receiver

Interceptor

Who are the 'good' guys ?

Law Enforcement’s Dilemmas

- Do not want to intrude into people’s private lives
- Do not want to hinder e-commerce
- Want to have their own secure communications
- Occasionally use interception to obtain information
- Occasionally need to read confiscated, encrypted information

Balance Again

Must balance:

- Rights of individuals
- Need to ‘protect’ society

Loss of Control of Encryption

- Academic papers
  - Attacks on DES
  - New algorithms
- Text books
- Need for international systems

Policy

- Defines the boundaries between behaviour that is permissible and that which is not
  - Technical level
  - Non-technical level
- Duty of care
- Protection against claim of negligence

Some Important Criteria for Policies

- Must demand compliance with regulations
- Employees must:
  - Read them
  - Understand them and believe in them
  - Be able to adhere to them

NOTE: Incomprehensible or ‘impossible’ policy requirement may ‘force’ employees to violate policy

Password Policy

- Concerns:
  - Outsiders might gain access
  - Legitimate user may be locked out
- Different concerns may ‘lead to’ different policies

Insider Threat

- Fraudulent ?
- Accidental ?
  - Laziness ?
  - Incompetence ?
  - Not understanding risk ?

Human Factors

- Profile is being raised
- Why do people break rules?
  - Evil intent
  - Unreasonable rule
  - Carelessness
  - Misunderstanding rule
- Need for professionalism
  - Understand technical and business issues
  - Understand the ‘position’ of employees (citizens)

The Challenge

- Establish a security culture where
  - Everyone accepts that security is important
  - Everyone accepts that security is their responsibility
  - Everyone is ‘onside’ with the security policy

Are we Moving in the Right Direction?

Some ‘good signs’

- Theory and practice are getting closer together
- Academia, Industry and Governments are working more closely together
- The need for professionalism from security practitioners is now accepted

Achievable or Impossible Dream?

Many positive steps in last 20 years

- Awareness
  - Got safe online
  - ISAF
- Qualifications
  - University degrees
  - $(ISC)^2$, SANS, ISACA, BCS
  - Vendors’ certificates recognising technical expertise
- Professionalism
  - IISP

CYBER?

- International
- National solutions have limited effectiveness
- ENISA
- IMPACT

Newton Minow, Speech to the Association of American Law Schools, 1985

After 35 years, I have finished a comprehensive study of European comparative law

In Germany, under the law, everything is prohibited, except that which is permitted

In France, under the law, everything is permitted, except that which is prohibited

In the Soviet Union, under the law, everything is prohibited, including that which is permitted

And in Italy, under the law, everything is permitted, especially that which is prohibited

Stay in Touch with the ISG

twitter.com/ISGNews