

# How safe and reliable are information systems?

Dr. Ian Brown

Department of Computer Science, UCL

Children: Over Surveilled, Under Protected

LSE

27 June 2006

## Against industry practice...

- Child databases such as RYOGENS and NOTIFY meet best-practice standards
- Users access system over secure Web links
- Web application communicates securely with firewalled database server
- All accesses logged
- Users only able to access info to which they have legitimate access

## Will industry practice suffice?

Prof. Martyn Thomas: “**almost every IT supplier in the world today is incompetent...** the typical rate of delivered faults after full user acceptance testing from the main suppliers in the industry over many years has been steady at around 20 faults per thousand lines of code. We know how to deliver software with a fault rate that is down around 0.1 faults per thousand lines of code and the industry does not adopt these techniques.” *Evidence to Home Affairs Select Committee, 24/2/2004*

# Security requirements

- Data held securely to prevent unauthorised access and modification
- Extensive protection against data loss or corruption
- Resistant to Denial of Service attacks
- All transactions must be logged and monitored

# Measuring system security requirements

1. Scale and complexity
2. Number of users
3. Sensitivity of data
4. Connections to other systems, particularly untrusted
5. Connectivity to the Internet
6. Attractiveness as target

## Evaluation Assurance Level

- Part of internationally-recognised “Common Criteria” govt security standards
- Complex, sensitive, widely used and connected systems should be EAL 6+
- UK certified products list contains no operating systems, firewalls, networking software or databases at EAL 4+

# Insider fraud

<i>Information required</i>	<i>Price paid to 'blagger'</i>	<i>Price charged to customer</i>
Occupant search/Electoral roll check (obtaining or checking an address)	not known	£17.50
Telephone reverse trace	£40	£75
Telephone conversion (mobile)	not known	£75
Friends and Family	£60 – £80	not known
Vehicle check at DVLA	£70	£150 – £200
Criminal records check	not known	£500
Area search (locating a named person across a wide area)	not known	£60
Company/Director search	not known	£40
Ex-directory search	£40	£65 – £75
Mobile telephone account enquiries	not known	£750
Licence check	not known	£250

Source: “What price privacy?”, Information Commissioner, May 2006

# Function creep: Police National Computer

1974	Stolen Vehicles		
	Broadcast	Fingerprints	
1979	Vehicle owners	Criminal names	Disqualified drivers
	Missing persons	Crime patterns	
1984	Convictions history		
	Stolen property	Transaction logs	Combined directory
1989	Marine craft	Firearms	ANPR systems
	PHOENIX index	VODS vehicle search	Sex offenders
1994	Motor insurance	QUEST	
	jurors	FSS link	CRB link
1999	Drivers database	Disaster recovery	MOT rollout
2004			

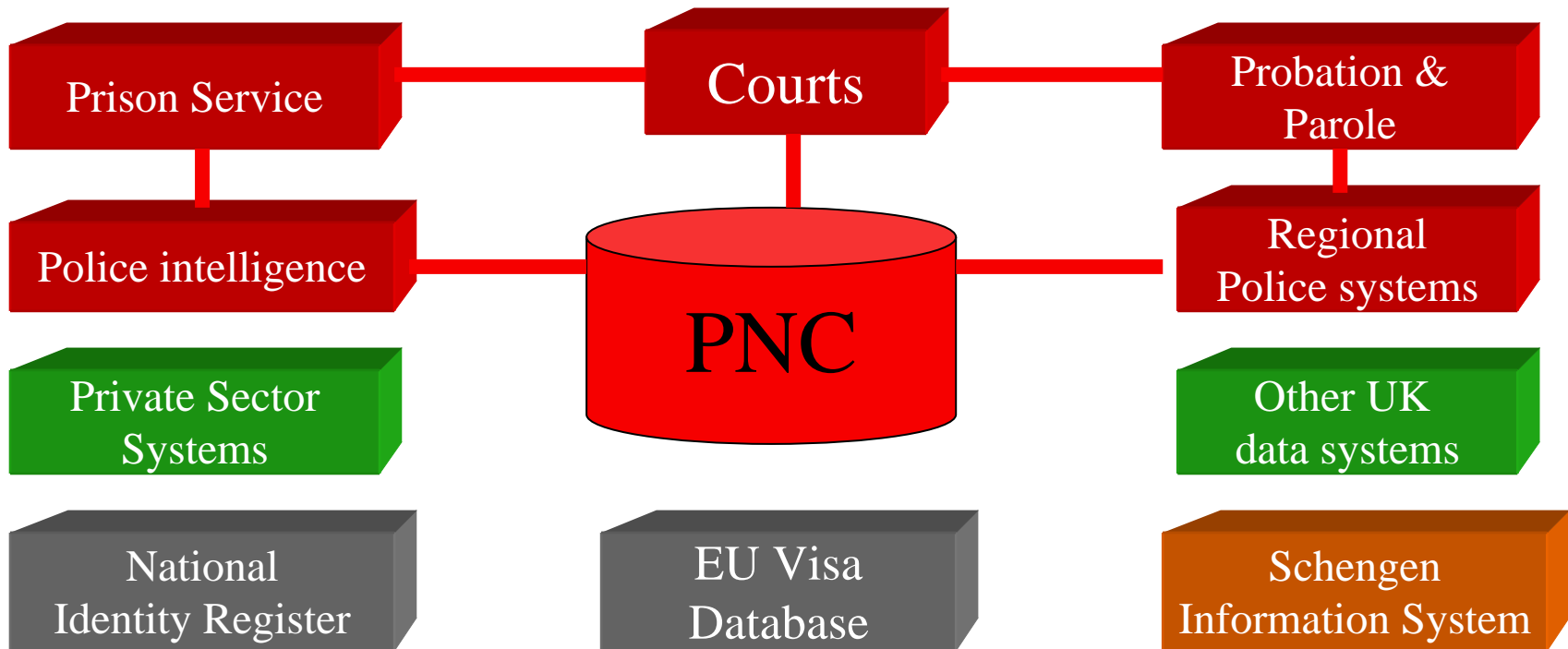
Source: Simon Davies, LSE

# The Police National Computer

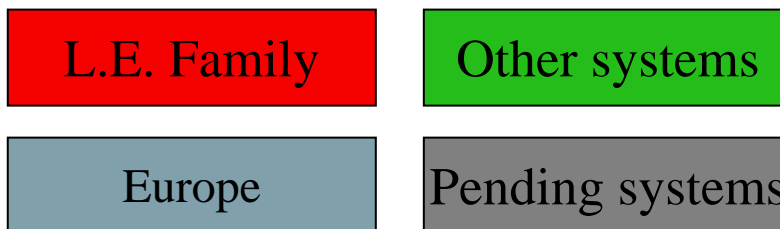
1974	Basic data storage & retrieval
1979	Data analysis
1984	National access
1989	Data Matching
1994	Free text search
1999	National interoperability
2004	Mobile access

Source: Simon Davies, LSE

# The Police National Computer



## Legend



# Conclusions

- Industry best practice is not good enough for secure govt systems – why should it be secure enough for sensitive info on children?
- Insider attacks extremely hard to defend against
- Function creep is inevitable – computers are *fantastic* at gathering and crunching data (if not actually making sense of it)