

# Virtualising privacy



Martin Sadler  
martin.sadler@hp.com

hp labs bristol

# Descriptions that capture intent



- There is increasing attention on languages that capture intent around notions of privacy and trust
- How useful are they?
- Prejudice: descriptions without enforcement mechanisms aren't interesting
- Thesis: by tackling issues around enterprise privacy statements and how we might provide assurance, we can do a much better job of enforcement than we do today

# From hp's online privacy statement



**Technology:** *Some HP Web pages are P3P-enabled, which allows you additional control over your personal information.*

**Processes:** *HP is a founding sponsor of the Council of Better Business Bureau's BBBOnline Privacy Program, the "gold standard" for privacy certification.*

**Principles:** *HP has also self-certified its privacy practices as consistent with U.S.-E.U. Safe Harbor principles: Notice, Choice, Onward Transfer, Access and Accuracy, Security, and Oversight/Enforcement.*

# So there is lots of complexity



- But is there any real choice?

*At hpshopping.com, for example, we offer one cookie called "hpshopping." It is a permanent cookie designed to give those customers who choose to register with hpshopping.com a personalized experience, including a greeting and remembering your shopping cart. Customers can browse with cookies turned off, **but you can purchase only if you accept the cookie.***

- Most consumers and businesses just want things taken care of – a role for trusted 3<sup>rd</sup> parties

# Can technology help to build trust?



- What might we like to be able to do?
  - test whether or not a particular statement holds
    - who gets to test?
  - monitor (continuous testing)
  - enforce (prevent violations)
- And we want to do this for more than toy examples
  - should we give up because it's too hard?
- So what do we need to pay attention to?
- **And what implications does this have for how we describe intent?**

# Properties to pay attention to



- Scale

- policy doesn't usually sit in one place
- is created by multiple individuals
- often described in terms of defaults and exceptions

**we need better data management**

- Federation

- data does need to cross boundaries between jurisdictions and organisations

**we need much more practical notions of ownership and responsibility**

# Properties to pay attention to



- Assurance

- how do we know everything is as it “should be”?

policy needs to carry information that helps to provide assurance



hp labs focus

- Escalation and resolution

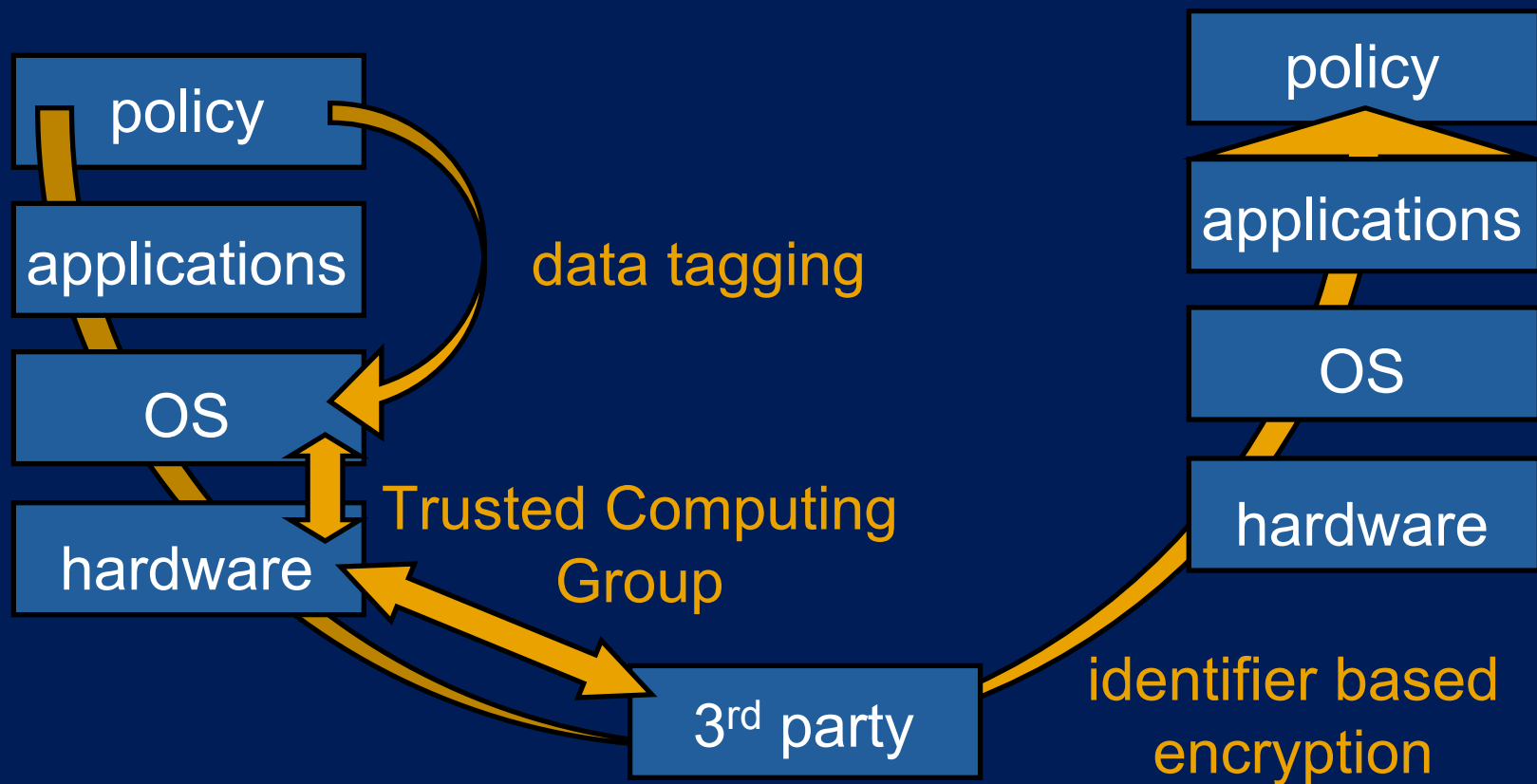
- inconsistency is resolved by managers
- not all violations are equal
- lots of people processes

we need support for events and integration with management processes

# Virtualisation



- Establishing the abstractions that might help us marry together high level notions with underlying mechanisms



# Data tagging



- Applications don't do a good job when it comes to security
- Expect the world of web services to be worse
- Idea: have the underlying OS/platforms enforce policy on data irrespective of what applications do – keep policy (tags) firmly attached to data
- How: (one idea) rewrite machine code to preserve tags, check and enforce policy

# Trusted Computing Group



- Hardware support to “prevent” cheating
- From which we can build chains of trust
- Industry consortium
- PCs to servers to PDAs to mobile phones to ...

# Identifier based encryption (IBE)



- Barrier: change our (locked in) thinking over identity and the ideas of public key cryptography, overcome the complexities of PKI
- IBE: based on public information from a trust authority, Alice can use *any* string she likes as a public key for Bob, string can be:
  - an email address, URL, ...
  - a date
  - terms and conditions
  - a program

Alice



Bob



Trust Authority(s)

change in roles

RSA: decryptor centric

IBE: encryptor centric

identity as evidence

# How might this all work?



- Rather than check (P3P) whether a website is going to respect my wishes
- I encrypt my personal information (using multiple trusted 3<sup>rd</sup> parties) with the terms and conditions (events, ...) I want the website to comply with, and the encryption string remains as a tag
- Enterprises accredit applications with 3<sup>rd</sup> parties, the 3<sup>rd</sup> parties release decryption keys
- Data tagging mechanisms ensure only accredited applications get to use the data; if the information is transferred, it is re-encrypted
- TCG mechanisms ensure platforms will do as they say they will

# What next?



- We have a good handle on the underlying mechanisms
- (Amongst) the interesting things to do:
  - a policy language based on assurance and the transfer of responsibility (rather than just a static view of access control)
    - data, tag-as-program, tag-as-terms&conditions, trust-authority
    - policy as specified by the consumer (rather than provider), and perhaps more about the relationship between providers and trust authorities



**i n v e n t**