Data Privacy for data in transit and
The Semantic Web

Mike Davies

Where it all comes together:
Data privacy at rest vs in transit

+ **Personal data at rest**
  - Stored within a company’s network

+ **Personal data in transit**
  - Moved either within a public or private network

+ **Industry and regulations has focused on the former**
  - Rather than the latter
The Semantic Web

- The Semantic web will make it easier to get data on any subject from the internet
- Data privacy will be impacted as the fog of information becomes clearer
- Fraudsters will use these tools to steal identities by looking at multiple sources ("Phoraging")
- Where security needs to be applied to protect privacy
SSL – SSL Certificates used externally

- Customer
- Fraudster
- Company
- SSL
- Secure Shopping
- VeriSign
- SSL

VeriSign Confidential
SSL – SSL Certificates used Internally

- Partner
- Customer
- Employee
- Company
- Administrator
- Fraudster
- MPKI for SSL
How much value to a fraudster is there in data?

Value of data

- Public Information
- Low value private data
- High value private data

Consumer interaction
- With site

Public Message boards / articles
- Enquiries
- Registrations for events or newsletters, Brochures
- Private Message boards
- Healthcare records
- Financial payments data
So who says where the security line should be?

+ Privacy line position is very clear
  ▪ Name and Address (email or physical) is personal data

+ Position of Security line depends on following
  ▪ 1) Regional or country Data protection laws
    – i.e. UK data protection act of 1998
  ▪ 2) Best practice in standards
    – i.e. BS 7799, ISO 27001
  ▪ 3) Potential or perceived threat
    – Currently “Potential threat vs value of data vs cost of solution”
    – Should be “Potential brand or equity damage vs cost of solution”
1) Regional or country based Data Protection laws

+ Current laws in Europe all based on EU Privacy Directive
  - and then interpreted by the member states

+ In UK became “Data Protection Act of 1998”
  - Over 8 years old

+ The “dummies guide to DP law” says…
  - “Personal Data should be protected to an appropriate level of security
    dependant on the potential for and implications of misuse”

+ In 1998 “the Security Line” was drawn
  - the internet has changed a little since then!
1) EU Law based on “Physical world” (Postal Model)
1) Regional or country based Data Protection laws

+ Decisions were made on the “postal model”
  ▪ but one major difference

+ Consumer “feels” like they are “in the store”
  ▪ Not reliant on a trusted third party to deliver (i.e. Royal Mail)
  ▪ Even use the term “domain”

+ At best creates a “duty of care” for Site Owner
  ▪ To ensure that customers are safe

+ At least implies that the Site Owner should be worried
  ▪ Brand and equity issues if there is a compromise
2) Best Practice in standards

+ British Standards BS7799
  - Dictates best practice for online security

+ Standards only, no legal requirement
  - However very influential in EMEA
2) Best Practice in standards

+ EU Safe Harbour Standard
  - EU initiative to ensure security when personal data leaves EU

+ “Packets” of data could travel outside of EU
  - On their route over the internet within EU

+ EU Safe Harbour states
  - “Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction”

+ This could ALONE give us enough reason to say that best practice states that you should encrypt ANY personal data
3) Potential or perceived threat

+ **Percieved threat to low value personal data is changing**
  - Cost of processing power very different to 1998
  - Potential to build illegal “database” of personal data real
  - Use geo location software to correlate information?

+ **“Packet sniffing”**
  - Originally used for credit card data
  - Searches all data going into a site for known characteristics
  - No reason why it can’t be used for other data sets

+ **Looking for real life examples but could be used for**
  - Corporate espionage  Spammers
  - Fraud  Press
  - Blackmail  Burglary
3) Potential or perceived threat - Privacy Policy

SECURITY STATEMENT
We have taken all reasonable steps to have in place appropriate security measures to protect your information.
To: enquiries@Honeymoonholidays.co.uk
From: mikedavies@heatmail.co.uk
Subject: Brochure request

Please help!!!!

We are looking for a holiday destination for our honeymoon from the 1st October 2006 to 15th October 2006. Can you suggest anywhere?

We would also really like to see a printed copy of your brochure or at worse a .pdf we can print out here

If .pdf please email to: mikedavies@heatmail.co.uk

If Physical copy please send to: 111 Main Street, Chiswick, London, W4 1AA, UK

Alternatively if you have a representative who can call me to discuss you can get me on 0208 511 7856.

Thanks!

Mike Davies
3) Example Threat 1 – Similar example in US
3) Example threat 2 – Spammers

To: enquiries@Honeymoonholidays.co.uk
From: mikedavies@heatmail.co.uk
Subject: Brochure request

Please help!!!!

We are looking for a holiday destination for our honeymoon from the 1st October 2006 to 15th October 2006. Can you suggest anywhere?

We would also really like to see a printed copy of your brochure or at worse a .pdf we can print out here

If .pdf please email to: mikedavies@heatmail.co.uk

Alternatively if you have a representative who can call me to discuss you can get me on 0208 511 7856.

Thanks!

Mike Davies
3) Example threat 3 – Government

Pentagon sets its sights on social networking websites
09 June 2006

Pentagon's National Security Agency, which specializes in eavesdropping and code-breaking, is funding research into the mass harvesting of the information that people post about themselves on social networks. And it could harness advances in internet technology - specifically the forthcoming "semantic web" championed by the Web standards organization W3C - to combine data from social networking websites with details such as banking, retail and property records, allowing the NSA to build extensive, all-embracing personal profiles of individuals.
3) Example threat 4 – Entrepreneurs
Some questions for the ICO

+ Do you feel that companies should protect consumer data in transit?

+ If so, do you think the Data Protection law gives you adequate powers to enforce protecting data in transit?
Data Privacy for data in transit and The Semantic Web

Mike Davies