Content, Trust and Security

- **What has knowledge representation to do with security?**

Graham Klyne
Head of Strategic Research, MIMEsweper Group
and
Nine by Nine

- **To conduct an e-commerce transaction: trust must be established**

Security and Trust

- **“Security makes trust work”**

  ...or is it...

- **“Trust makes security work”**

  ...?

Authentication is Key

- **Focusing on authentication, reliability of information and non-repudiation**
  - **Confidentiality is a different issue**
- **Knowing with whom one is dealing ...**
  ... is needed to establish a level of trust
  ... is basis of evidence for non-repudiation

Keys for Authentication

- **Cryptosystems use mathematical models to offer near-*certainty* about a party's identity, subject to certain assumptions:**
  - **The private key is known only to the authenticated party**
  - **The public key used matches the private key**
  - **Key processing systems are not subject to external manipulation**
  - **The identity of the authenticated party is properly established and associated with the key pair**
- **If any assumption is violated, all bets are off**
- **Security from cryptosystems alone is "brittle"**
- **Secure systems are difficult to set up and use**

Weight of Evidence

- **Legal systems rarely deal with certainties:**
  - **Witnesses lie**
  - **Documents are forged**
  - **Performance is evaded**
  - **Contract parties are fooled**
- **Dealing with uncertainty:**
  - **"beyond reasonable doubt", or**
  - **"balance of probabilities"**
- **Available evidence is assessed as a whole**
  - **Information from several sources**
  - **One item of evidence rarely dominates**
  - **Any evidence can be challenged**

Risk Management

- **Balancing risk, cost and benefits**
  - **Credit card companies do this for billions of transactions, with pitifully weak basic security mechanisms**
- **Assessing "real-world" information**
  - **"Would you buy a used car from this person?"**
- **Dealing with uncertainty leads to:**
  - **Greater security**
  - **Greater tolerance of incorrect assumptions**

Assessing Risk

- **Using a range of information**
  - **Reputation**
  - **Previous interactions**
  - **References/testimonials from trusted parties**
  - **Third party indemnities**
  - **Verifiable facts**
  - **Credibility of claims made**
- **Need to deal with unstructured information**
- **The affairs of people don't usually fit precise mathematical models**
- **Ultimately, e-commerce is "affairs of people".**

Combining elements

- **Open standards for information exchange**
  - **IETF: protocols**
  - **W3C: data formats**
- **Leveraging years of research:**
  - **Knowledge representation**
  - **Expert systems**
  - **Inference systems, logic programming**
  - **Machine learning**
- **Adopts the web's open-world model**
  - **Combining information from a variety of sources**
  - **New assertions can be added at any time, any place, any where; scaling to millions+ of assertions**
  - **Provision for non-monotonic reasoning**

And There's More...

- **Ad-hoc micro-mobile networks**
  - **Bluetooth**
  - **Walk up / walk by**
  - **Continual exchanges with new systems**
- **Realizing the potential of wireless hardware**
- **Invisible, involuntary information exchange needs invisible, involuntary protection**
- **Instant messaging protocols for information exchange using “low grade bandwidth”**

Summary: Security and Content

- **Quoting Bruce Schneier:**
  - **"Security is a process, not a product." [Crypto-gram, May 2000]**
- **A security process must access content, not just protocols and raw data**
  - **Application data is a major content-borne security risk**
- **Who owns your data: you or your application vendor?**
  - **"An end-to-end architecture for content"**
  - **Cross platform, cross application access to information**
  - **Allowing full analysis of information content**