PROTECTING IDENTITY IN THE DIGITAL ERA

Robin Wilton
Corporate Architect (Federated Identity)
Sun Microsystems
robin.wilton@sun.com
+44 705 005 2931
http://blogs.sun.com/racingsnake
Aim of this presentation

• To 'set the scene' for subsequent discussions of identity security
• To outline the relevant characteristics of identity
• To look at identity theft, its scope and its modes
• To build shared understanding on specific examples
• To position technology appropriately amongst the applicable countermeasures
Topics

- Scope and characteristics of identity abuse
- An 'industry example'
- The challenge we face
- What does Identity consist of?
- Identity theft life-cycle and attack vectors
- Possible counter-measures in theory and practice
Scope and Characteristics of identity abuse

- Identity theft and identity fraud are a factor in:
  > Money-laundering and financial fraud
  > Vulnerability of the online 'critical national infrastructure'
  > Other aspects of organised crime

- These activities are:
  > Organised
  > International
  > A 'commercial' enterprise
  > Facilitated by Internet technologies
  > It is tempting (but, I believe, wrong) to conclude that the solution is therefore primarily technical.
'Name this Industry' ...

1 - 'Mining' of raw materials

2 - Bulk sale, cross-border shipment

3 - Reprocessing; consumer value-add

4 - Re-export, cross-border

5 - Convert Assets to Goods

6 - Re-sell cross-border to monetise
Retail Card 'Skimming' Case Study

- Details captured in North America
- 'Consolidated' in SE Asia
- Cards personalised in S Asia
- Physically shipped to EU
- Goods bought for shipment to Central Europe

- In other industries, this would be a normal supply chain...
- Organised entities operate in the theft, trafficking and exploitation of identities, for financial gain and other ends
- No single law-enforcement agency has the jurisdiction, resources or inclination to investigate or prosecute this crime (which one...?)
The Challenge We Face

“As long as we persist with

- C17th. notions of sovereignty
- C18th. judiciary and
- C19th. law enforcement

the C21st. will belong to organised crime.”

Jeffrey Robinson
Writer on Money-laundering and Organised Crime
What does Identity consist of?

- A three-layer model for Identity Data:
  - Attributes
  - Entitlements
  - Credentials
  ... support assertions about ...
  - “History”
  - Authorisation
  - Identity

- Assertions about Identity are, essentially, assertions that the person presenting credentials is the person to whom they were issued at a point in the past.
- This reveals an implicit 'chain of trust', which must be intact if we are to trust an identity assertion.
- Identity Theft is the act of subverting that chain of trust at some point.
Identity Theft Life-cycle and Attack Vectors

Planning
- Targeting, Research

Setup
- Materials and Attack Tools

Attack
- Capture exploitables data
- 1st/2nd Stage exploitation

Collect

Defraud
- Shut down, Remove evidence
- Sell expertise

Post-attack

Each of these usually has 'bulk' and 'individual' attack variants

Technical
- Keystroke logging, DNS spoof/poison, wireless sniffing

Physical
- Disk theft, 'trash analysis', insider attack
  (abuse of authorised access)

“Social Engineering”
- Phishing, email scams, 'trusted source', duress,
  'politically exposed positions'
Countermeasures and their Positioning

- It is tempting to see “technology” or “legislation” (or both) as the definitive solution to identity theft.
- However, that is likely to fail tests of practicality, scalability, and 'portability' across jurisdictions (for instance, regulations relating to 'Breach Notification').
- Each 'regulatory regime' (country, industry...) has a characteristic 'profile', to which technology needs to be fitted as appropriate:

Regulatory Regime “A”
- Best Practice
- Self-regulation
- Legislation

Differing balances of technical and other measures

Regulatory Regime “B”
- Best Practice
- Self-regulation
- Legislation
Mitigations by Attack Vector – Some Examples

- As one might expect, the mitigations for identified attack vectors vary, include both technical and non-technical measures, and often overlap. The table below gives some examples:

<table>
<thead>
<tr>
<th>Attack type</th>
<th>Attack Vector</th>
<th>Description</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical</td>
<td>Wireless intercept</td>
<td>War-driving', open wireless access points, 'Evil Twin' attack</td>
<td>Wireless encryption, MAC filtering, user education</td>
</tr>
<tr>
<td>Physical</td>
<td>Trash Analysis'</td>
<td>Collecting (and aggregating) identity data which has been discarded without adequate protection (documents, disks, tapes)</td>
<td>User education, use of document shredding, secure file delete, asset disposal policies, audit</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>Phishing</td>
<td>Luring individuals to reveal personal data</td>
<td>User education, browser toolbars, improved (e.g. multi-factor) authentication</td>
</tr>
</tbody>
</table>
Life-cycle and Attack Vectors – Further Reading

- My source for much of this analysis is the Liberty Alliance, through its ID Theft 'Special Interest Group'
- The SIG's first two pieces of output are freely available through the links below:
- Also, see how this recent case-study of identity theft and fraud at 'street level' has got into the mainstream media: who, why and how...
Some Advantages of a Federated Approach

- Federation makes strong authentication available as a 'shared service', capitalising on the user's 'most trusted' relationships
- The layered model for identity data provides functional separation
- Permission-based exchange of user attributes (allowing user consent and privacy to be addressed)
- Reduced need to move sensitive data from place to place

- The federated model provides a much better online analogue for 'real-world' trust relationships
Some Closing Thoughts...

- Why do people rob banks?
  > “Because that's where the money is...”
  > People steal identities because they are of value – and a 'clean' identity with excellent credit and strong credentials is all the more valuable
  > Every increase in the 'strength' of credentials requires greater care in the initial registration process
  > How do you issue someone with a 'new' biometric?

- Tackling Identity Theft requires a holistic approach:
  > Legislation, Regulation, Best Practice, Technology, Process and User Behaviour are all factors
  > Systematic analysis of identity data, attack vectors and mitigations is an essential foundation – and is possible
THANK YOU

Robin Wilton
Corporate Architect (Federated Identity)
Sun Microsystems
robin.wilton@sun.com
+44 705 005 2931
http://blogs.sun.com/racingsnake