

Requirements Focussed Security

Dr. Simon Foley
Department of Computer Science,
University College Cork, Ireland
www.cs.ucc.ie/~s.foley



University College Cork

Overview

User Focus

Business Focus

Federation Focus



The Technology Focussed Network

Overview

User Focus

Business Focus

Federation Focus



Security should not be driven only by technical concerns.

Focus on the needs of users, businesses and their federations.

Overview

User Focus

Business Focus

Federation Focus

User Focussed Security



Security Policy Requirements Elicitation

Overview

User Focus

Business Focus

Federation Focus

Policy elicitation often driven by technical concerns.

- Technical policies designed by technical people.
- Based on the system artifacts with which users interact: groups, roles, transactions, etc.

Should consider needs of individuals and their relationships.

- Balance individuals' requirements [eg, Multilateral Security].
- Include human issues.

How can we address this?

TIMES ONLINE

- NEWS
- COMMENT
- BUSINESS
- MONEY
- SPORT
- LIFE & STYLE
- TRAVEL
- DRIVING
- ART
- UK NEWS
- WORLD NEWS
- POLITICS
- SCIENCE
- ENVIRONMENT
- WEATHER
- TECH & WEB

Where am I? > Home > News > Tech & Web

From The Times
July 6, 2009

Wife of Sir John Sawers, the future head of MI6, in Facebook security alert

Michael Evans, Defence Editor

Diplomats and civil servants are to be warned about the danger of putting details of their family and career on social networking websites. The advice comes after the wife of Sir John Sawers, the next head of MI6, put family details on Facebook — which is accessible to millions of internet users.

Lady Sawers disclosed details such as the location of the London flat used by the couple and the whereabouts of their three children and of Sir John's parents. She put no privacy protection on her account, allowing any of Facebook's 200 million users in the



EXPLORE TECH & WEB

- > PERSONAL TECH
- > THE WEB
- > GADGETS & GAMING

TECH CENTRAL

Latest posts on the blog
[View RSS feed](#)

TOKYO ROBOT SHOW

Trust Management Policy Elicitation

Overview

User Focus

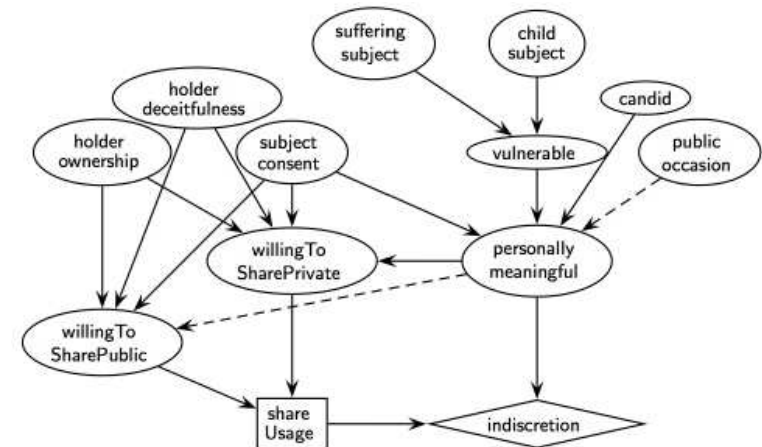
Business Focus

Federation Focus

Use qualitative analysis methods from social sciences to elicit trust management policy for photograph sharing.

- Explore user-experience through semi-structured interviews.
- Qualitative analysis elicits policy requirements.
- Model the result in a Bayesian Network.

User requirements more complex than basic access controls.



[S.N. Foley, V.M. Rooney. *Qualitative Analysis for Trust Management*. International Security Protocols Workshop, Cambridge UK, April 2009.]

Overview

User Focus

Business Focus

Federation Focus

Business Focussed Security



Managing Security

Overview

Siloed security driven by technical concerns.

User Focus

Business Focus

Federation Focus

- Technical mechanisms designed by technical people.
- Based on the system artifacts: groups, roles, transactions, etc.

Should align security with business strategy.

- Secure critical business processes, not just technologies
- Security threats are inevitable, need to manage the risk.



www.dilbert.com scottadams@aol.com

© 2007 Scott Adams, Inc./Dist. by UFS, Inc. 11-4-07

Security Risk Management

Overview

User Focus

Business Focus

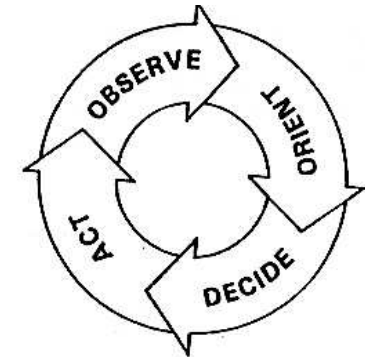
Federation Focus

Use *Enterprise Risk Management* (ERM) to manage (operational) risks related to security:

- security mechanisms as controls that mitigate known risks in meeting objectives of business process,
- tests that audit efficacy of risk mitigation,
- catalogues of best practice controls.

Security as an ongoing process:

- measure, prioritize, mitigate,
- security risk metrics and aggregation.



[S.N. Foley. *Security Risk Management using Internal Controls*, ACM Workshop on Information Governance, 2009]

Risk Management of Network Access Controls

Overview

User Focus

Business Focus

Federation Focus

Security controls should be compliant with best practice.

- *1.2.1.a Verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data. [PCI-DSS]*

Semantic configuration models facilitate automated reasoning:

- Analysis of n-tier network for shadowing, redundancy, etc.
- Encode catalogues of best practice [PCI-DSS, NIST-800-41, NIST-800-44, RFC-3330, RFC-1918].
- Autonomic configuration based on catalogue search.

[S.N. Foley and W.M. Fitzgerald. *An Approach to Autonomic Security Policy Configuration using Semantic Threat Graphs*. IFIP WG 11.3 Working Conference on Data and Applications Security 2009. Springer LNCS 5645.]

Overview

User Focus

Business Focus

Federation Focus

Federation Focussed Security



Security Policy

Overview

User Focus

Business Focus

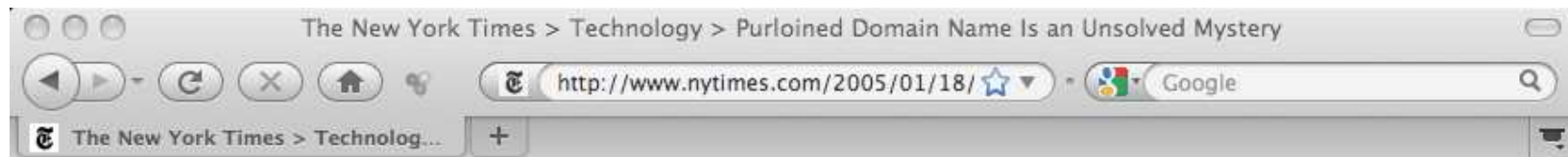
Federation Focus

Centralized policy, closed system.

- Centralized authority, controlled by administrator.
- Principle of no privilege.
- Opportunity to subvert administrator usually small.

Distributed policy, open system.

- Decentralized authority across multiple stakeholders.
- Principle of flexible privilege
- Opportunity to subvert stakeholder intentions?



The New York Times
nytimes.com



January 18, 2005

Purloined Domain Name Is an Unsolved Mystery

By TOM ZELLER Jr.

It was yet another reminder of how vulnerable a company's brand name can be in the world of electronic commerce.

In the space of about 48 hours over the weekend, Panix.com, New York City's oldest commercial Internet service provider, saw its name slip out of its control and become the center of an international cyberhunt to get it back. Whether maliciously or inadvertently, the company's main domain name - panix.com - had somehow been transferred to a company in Australia.

Mail to users with a panix.com address was suddenly being sent to a server computer in Canada that had no relation to the company. And in Vancouver, Wash., Panix's registrar - the broker responsible for securing rights to the domain name and administering its use - was completely unaware that the name had been pinched.

Secure Coalitions

Overview

User Focus

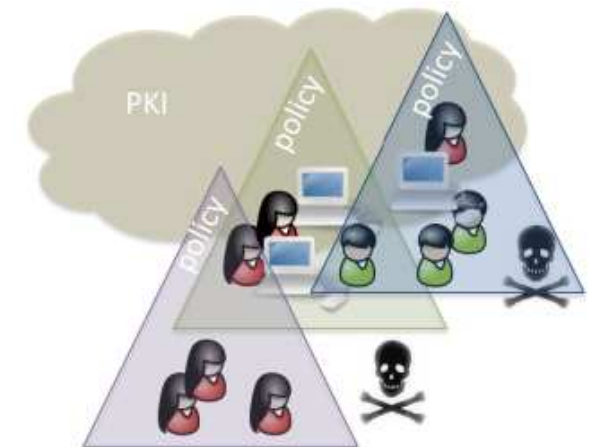
Business Focus

Federation Focus

Federation as coalition of principals/federations.

- coalition policy govern actions,
- coalition formation governed by participants,
- policy decentralized/distributed across network,
- principal of governed flexible privilege.

In the absence of a centralized authority, the actions of a malicious principal/coalition should not be able to circumvent policy.



[H. Zhou and S.N. Foley, *A Framework for Establishing Decentralized Secure Coalitions*. IEEE Computer Security Foundations Workshop, 2006.]