



Messaging Standard for Sharing Security Information

Standardisation Update

Ian Bryant

European Task Force on Computer Security Incident
Response Teams (TF-CSIRT) Seminar

Tallinn EE, 24th September 2009

TF-CSIRT Standardisation Update

- The Standardisation Process
- ISO/IEC 27035
- ISO/IEC 27010
- Questions ?



Messaging Standard for Sharing Security Information

Project JLS/2007/EPCIP/007 was co-funded by the European Commission (EC), Directorate General for Justice, Freedom and Security (DG JLS) as part of the “*European Programme for Critical Infrastructure Protection*” (EPCIP) Programme under the original title: “*Messaging standards for computer network defence warnings and alerts*”

It was performed with the support of the EC DG JLS “*Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks*” Programme

➤ **The Standardisation Process**

- ISO/IEC 27035
- ISO/IEC 27010
- Questions ?

Standardisation



“If you think of standardization as the best that you know today, but which is to be improved tomorrow; you get somewhere.”

Henry Ford 1863-1947

(American industrialist and pioneer of the assembly-line production method)

Major Standards Bodies for Information Security

- IETF
 - Internet Engineering Task Force
 - e.g. RFC2350
- ISO/IEC
 - Joint efforts between International Standards Organisation (ISO) and International Electrotechnical Commission (IEC)
 - e.g. 27xxx series
- Mitre
 - US Federally Funded Research & Development Centre (FFRDC)
 - The C*E and C*SS series
- W3C
 - World Wide Web Consortium



Other Standards Bodies (1)

- Within a specific organisation
- Within a specific country
- Within specific industry sector(s)
- Within regional transnational bodies
- Within worldwide transnational bodies



Other Standards Bodies (2)

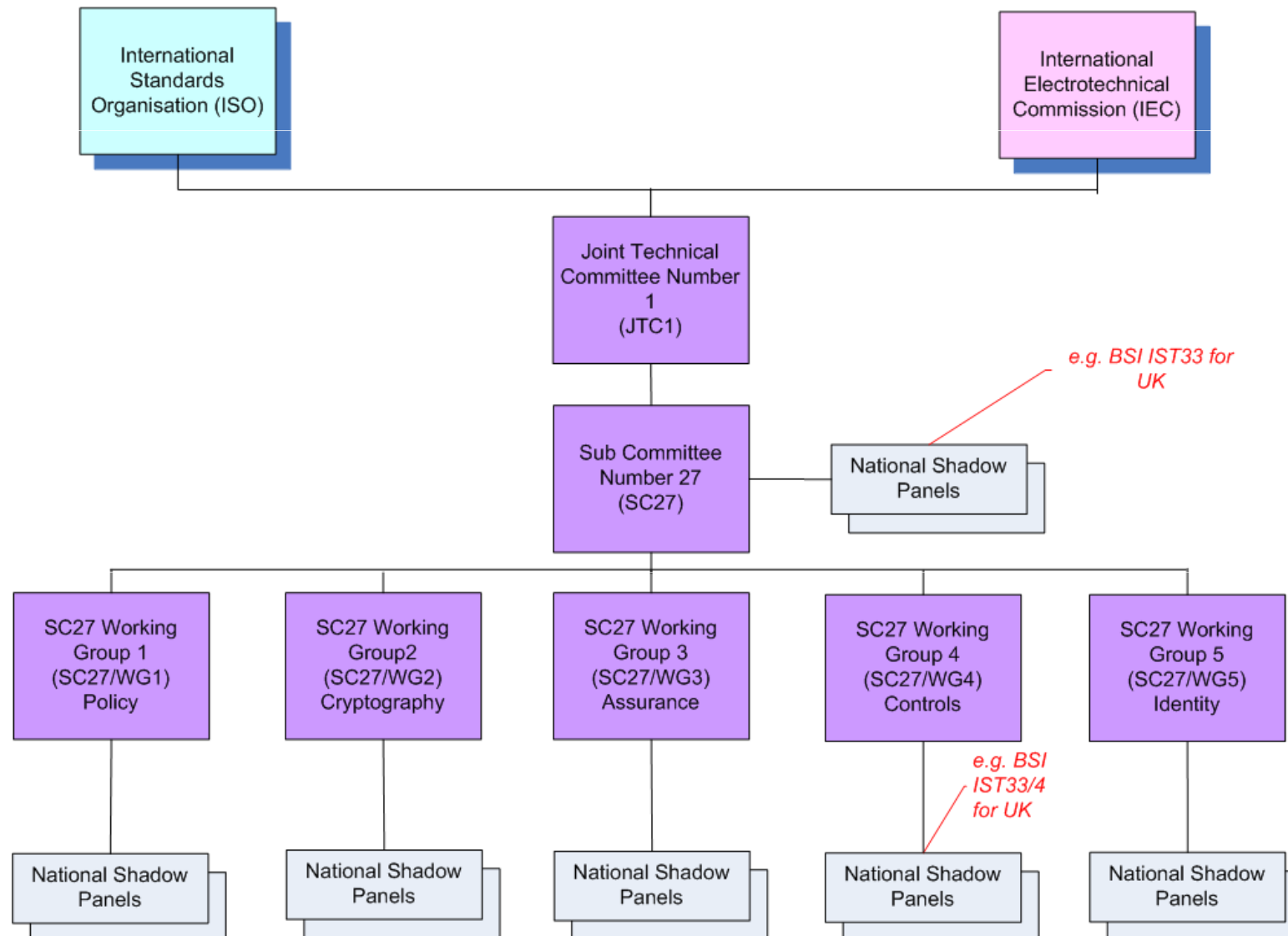
- Other bodies
 - CEN - European Committee for Standardization
 - CENELEC - European Committee for Electrotechnical Standardization
 - ECMA - European Computer Manufacturers Association
 - ETSI - European Telecommunications Standards Institute
 - IEEE - Institute of Electrical and Electronics Engineers
 - IET – Institute of Engineering and Technology
 - ITU - International Telecommunications Union
 - OASIS - Organization for the Advancement of Structured Information Standards
- Not an exhaustive list

Standardisation: Which Approach?

- Multiple possible routes to standardisation
- European focused options
 - CEN / CENELEC
 - ECMA
 - ETSI
- But strongest adoption from worldwide base
- TF-CSIRT tacitly about Information Security Frameworks
 - *De facto* lead organisation ISO/IEC (27xxx)

- **International Organization for Standardization (ISO)**
 - Founded 23 February 1947
 - Headquartered in Geneva, Switzerland
 - International-standard-setting body composed of representatives from various national standards organizations
 - Promulgates world-wide industrial and commercial standards
 - Although technically a non-governmental organization (NGO), it is consortium with strong links to governments, able to set standards that often become law, either through Treaties or National Standards
- **International Electrotechnical Commission (IEC)**
 - IEC is a not-for-profit, non-governmental international standards and conformity assessment body for all fields of electrotechnology, founded in 1906
 - IEC's own documents in 6xxxx – 7xxxx number range
 - Most work in the Information and Communications Technology (ICT) arena is carried out in conjunction with the *ISO*, through Joint Technical Committee Number 1 (JTC1)

ISO/IEC Organisation for Information Security





ISO/IEC JTC1 SC 27: Membership

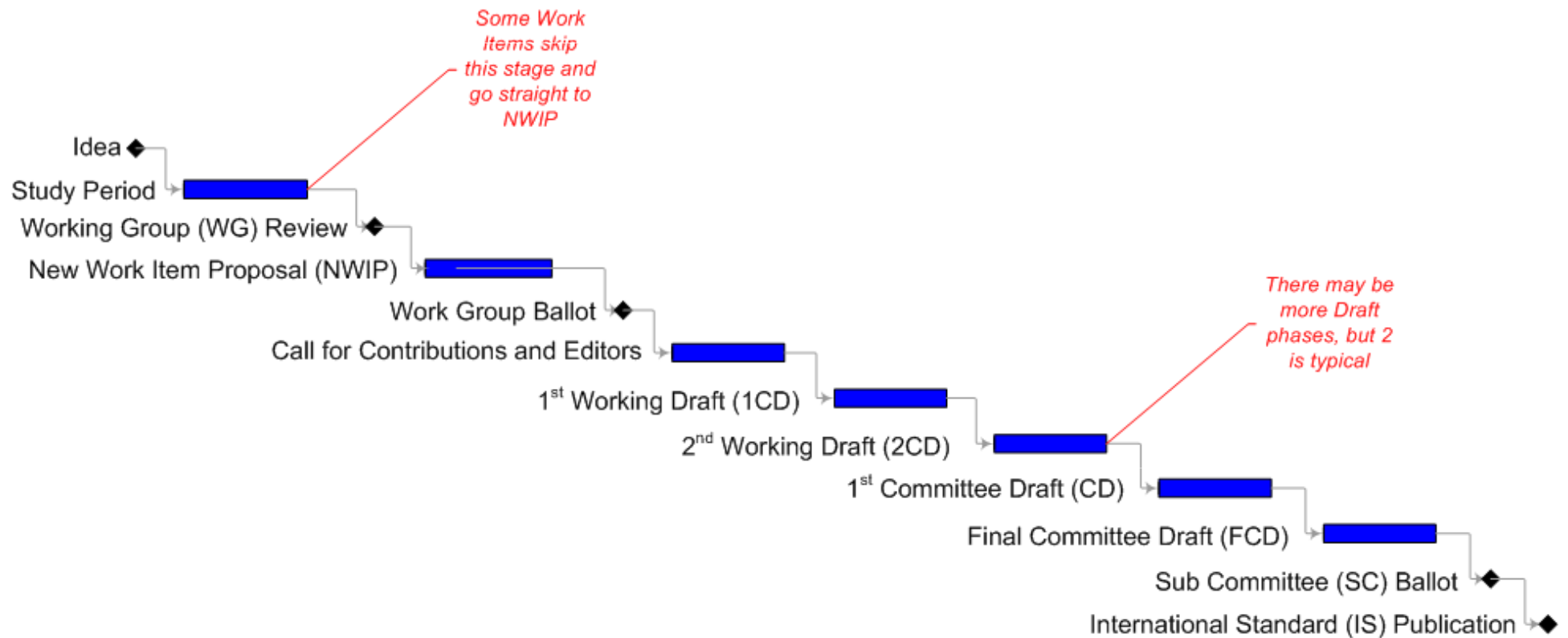
Brazil	Belgium	France	Netherlands	Sweden	USSR	
Canada	Denmark	Germany	Norway	Switzerland	China	
USA	Finland	Italy	Spain	UK	Japan	Algeria
<i>founding P-Members (18 in 1990)</i>						Venezuela
						Ireland
Russian Federation	Poland	South Africa	Kenya		Cyprus	Slovakia
Korea	Ukraine	Malaysia	Austria	New Zealand	Uruguay	Romania
Australia	Czech Republic	India	Luxembourg	Singapore	Sri Lanka	Kazakhstan
1994	1996-1999	2001	2002	2003	2005-2006	2007-2009
<i>additional P-Members (total: 40)</i>						

O-members (total: 12): Argentina, Belarus, Costa Rica, Estonia, Hong Kong, Hungary, Indonesia, Israel, Lithuania, Serbia, Thailand, Turkey

ISO/IEC Engagement Process

- Documents produced as:
 - Technical Reports
 - International Standards
- Documents normally generated by Projects, which are voluntary groupings consisting of:
 - Representatives from participating National Standards bodies
 - Additional Liaison Members from relevant communities of interest
- ISO/IEC ratification through Committees and Sub-Committees

ISO/IEC Typical Process for a Standard



- The Standardisation Process
 - **ISO/IEC 27035**
- ISO/IEC 27010
- Questions ?

Recap - History: ISO/IEC 18044 (1)

- Full title
 - ISO/IEC TR 18044:2004
 - Information technology
 - Security techniques
 - Information security incident management
- Technical Report (TR)
- Published 12-Oct-2004
- Produced under ISO/IEC JTC1 SC27

Recap - History: ISO/IEC 18044 (2)

- **Objective :**
 - Provide advice and guidance on information security incident management for information security managers and for information system managers.
- **Contains :**
 - Information on the benefits to be obtained from and the key issues associated with a good information security incident management approach (to convince senior corporate management and those personnel who will report to and receive feedback from a scheme that the scheme should be introduced and used)
 - Information on examples of information security incidents, and an insight into their possible causes
 - A description of the planning and documentation required to introduce a good structured information security incident management approach
 - A description of the information security incident management process

Recap - The Plan: ISO/IEC 27035

- Evolution of ISO/IEC TR 18044:2004
- Changes nature **from** Technical Report (TR) **to** International Standard (IS)
- Currently at Working Draft (WD) stage
- Concerns expressed by some CSIRT communities that haven't been engaged in structured manner with **either** ISO/IEC 18044 or ISO/IEC 27035 (***Draft***)
- **Previously briefed (by the current presenter) to TF-CSIRT (25th Meeting, Wien AT)**

ISO/IEC 27035: Progress Update

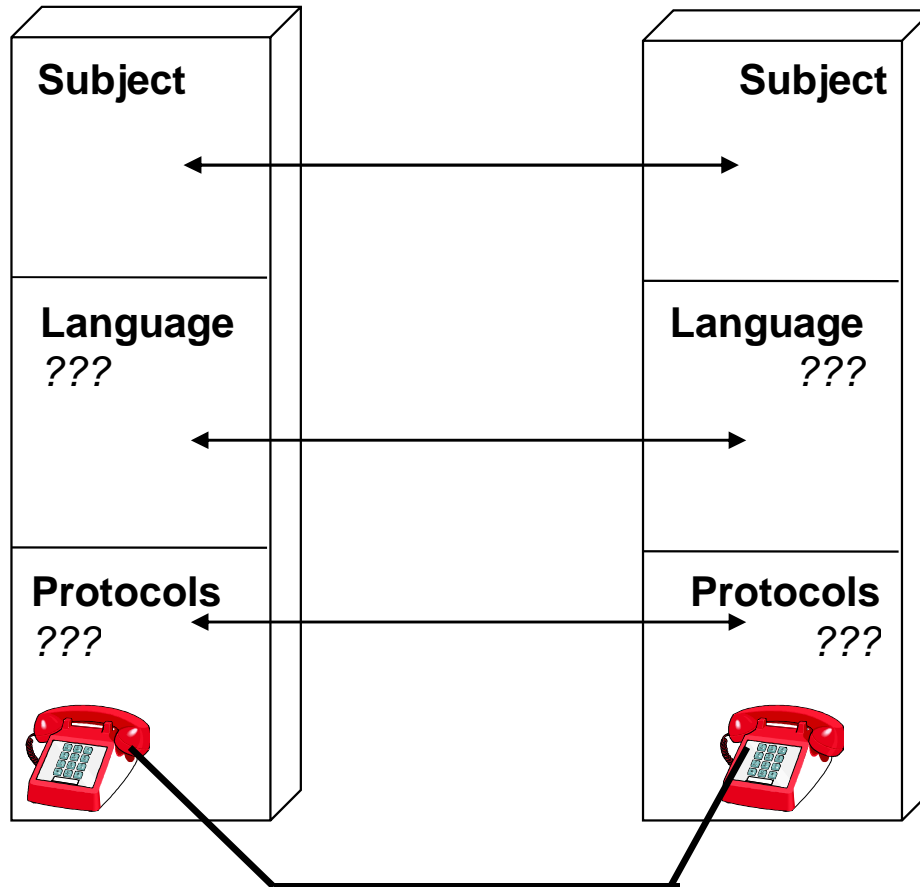
- Extensive comments made on Draft by UK
 - Significant increase proposed to Incident Taxonomy
 - Included feedback received from TF-CSIRT Members, e.g.
 - Recognition of CSIRT terminology
 - Removal of prescriptive reporting format that is not consistent with IODEF
- Good comments received from other National Bodies (e.g. JP, ZA)
- Latest Draft under review, generally Fit for Purpose

- The Standardisation Process
- ISO/IEC 27035
- **ISO/IEC 27010**
- Questions ?

Sharing Information in ISO/IEC 27xxx Context

- 27xxx assume a uniform perception of risk
 - Unlikely to be true when multiple organisations are participating
- 27xxx assume all participants can be equally trusted
- 27xxx assume all ISMS information is equally trustworthy
- 27xxx assume that all risk managers can assess the effectiveness of all security controls

Implementation Challenges to Sharing



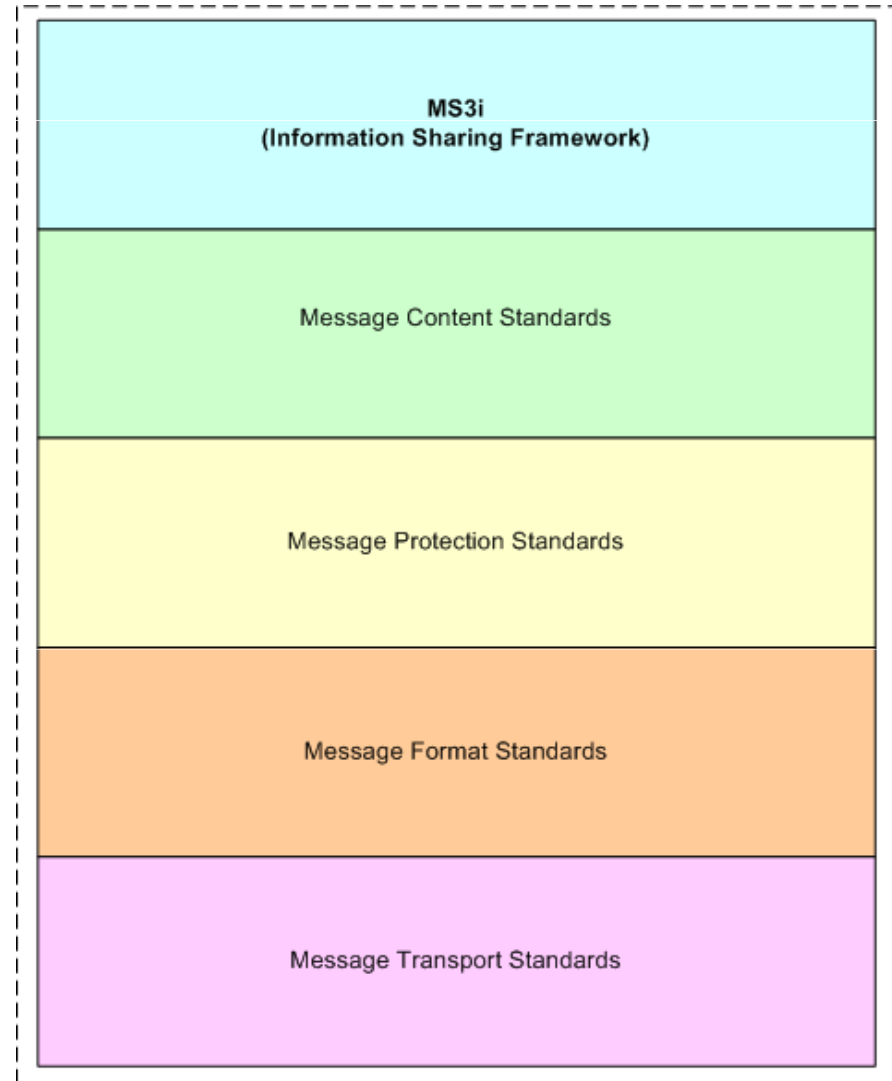


Standard for Information Sharing

- There **is** something special about trusted information sharing between organisations
 - Trusted Information Sharing needs **security management** of the sensitive **information exchanges** between organisations
- The EU funded MS3i Project studied this topic
- This work is forming the basis for a new ISO/IEC 27xxx series Draft

Standardisation: Layered Approach

- MS3i Project focus on Management Framework to support Sharing Security Information
- Expects to build upon a number of layered components for messaging information



Standardisation: Existing Coverage

- Message Transport Standards
 - *De facto* adoption of (IETF) TCP/IP
- Message Format Standards
 - *De facto* adoption of (ISO/IEC) XML
- Message Protection Standards
 - *De facto* adoption of (W3C) XML-Sig / -Enc
- Message Content Standards
 - Mainly *de facto* adoption of (Mitre) C*E

Challenge Area: Trust and Perception

*“Six Words Can Bring
Down a Prime
Minister”*



“Don't you think she looks tired?”

The Doctor of Gallifrey
25 December 2006

Perception: Cognitive Biases (1)

- Cognitive biases are patterns of deviation in judgment that occurs in particular situations, which can be:
 - Examples of evolutionary mental developments
 - e.g. adaptations that lead to more effective actions or enable faster decisions
 - Lack of appropriate mental mechanisms
 - Misapplication of a mechanism that is adaptive under different circumstances
- Cognitive Biases mean that differing people / communities will perceive **the same** information **in differing ways**



Perception: Cognitive Biases (2)

- Many noted types of Cognitive Bias
- Ones most likely to cause deviation of relevance to Information Sharing are ***Kahneman/Tversky Heuristics***:
 - Anchoring
 - Numerical estimates are skewed if seemingly similar and relevant values in recent memory
 - Availability
 - Prediction of frequencies of event or proportions within a population are skewed by how easily a seemingly similar and relevant example can be brought to mind
 - Representativeness
 - Potentially baseless assumption of commonality between objects of seemingly similar appearance or other grouping characteristics

Perception: The Impact Fallacy

- Impact is a fundamental element of Information Security Risk Assessment
- Yet in many ways not suitable for Information Sharing
 - Unlikely to be a Generic Impact, but rather influenced by Environmental Factors (Organisation, Locale, Time)
 - Intrinsic modelling problems if Low Probability / High Impact: Taleb's *Black Swan*
 - Very susceptible to Cognitive Bias, in particular prior knowledge of others' assessment Situates the Appreciation by Anchoring

Concepts of Trust



“What one needs is a way of doing the sum ... we don't know yet how to do this summation properly, but we do know certain features it should have”

Stephen Hawking, Lucasian Professor of Mathematics, Cambridge University, *(in a slightly different context – from 'Black Holes and Baby Universes' – but the principle still applies!)*

Trust: The Origins

- Trust is an evolution of the concept of signalling found in the animal kingdom
- Animals intelligent enough to speak – Human Beings – may for Machiavellian (or accidental) reasons manipulate such signals
 - May no longer be implicitly believed

- Human societies have an implicit series of Circles of Trust, typically expressed, in order of decreasing trust, as:
 - The family
 - The class
 - The nation
 - The coalition of nations
 - Humanity
- For informal and/or *ad hoc* groupings, we need a Trust Metric

Trust: Specious Reinforcement

- Guglielmo Marconi's conjectured any person could be connected to another by at most 5 people:
 - Issue also reflected by “Erdős Number”, “6 Degrees of Separation”, “Kevin Bacon Game”, “Small World problem”
- Empirical evidence is number of degrees of separation closer to 7:
 - Duncan Watts (2001) test with 48,000 emails found average number of intermediaries just over 6
 - Microsoft (2007) study of 30 billion instant messenger conversations found the average path length was 6.6
- Any model of Trust should not use linear weighting for additional instances (*de minimis* for larger values)

Trusted Information Sharing



Challenges with modelling trust in (potentially *ad hoc*) MS3i environments:

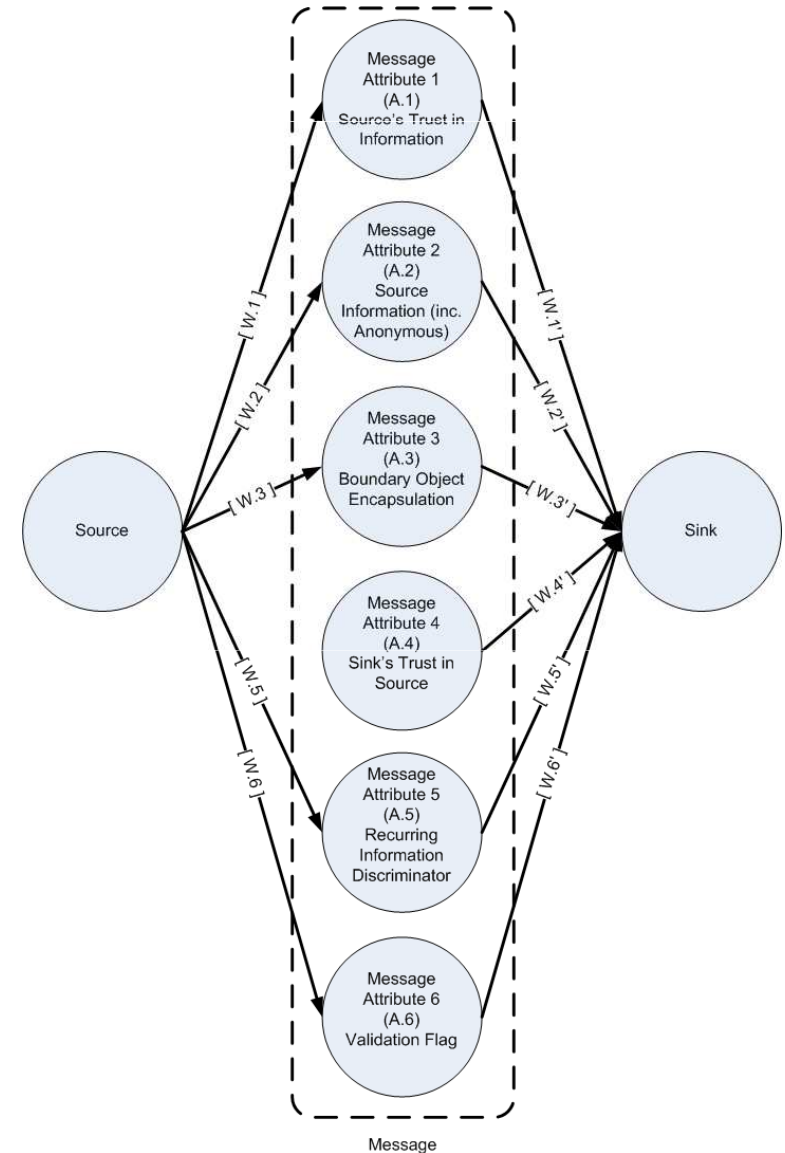
- The Communities are not necessarily aligned to the natural Circles of Trust
- The communities may not share either a common language and/or ontology
- The communities may not know trustability of *ad hoc* partners

Trust: Recipient's Implied Metric

- Recipient's degree of trust in a received statement is largely predicated on
 - The degree to which the source / message are trusted
 - The source's own trust in the statement
- Complication of risk of specious reinforcement: intrinsic tendency / underlying assumption that multiple instances of the same information from seemingly differing sources is confirmatory

Trust: MS3i Model (1)

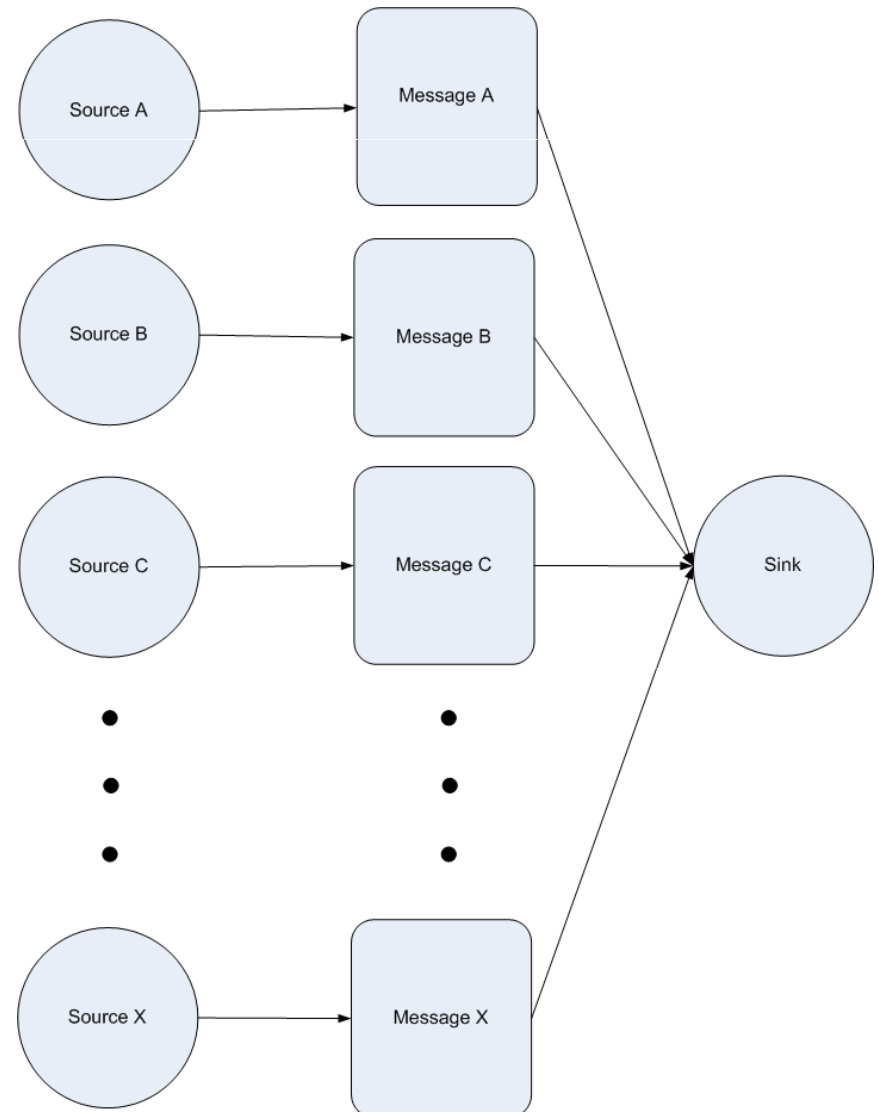
- Pareto approach: perfection would need disproportionate effort, and may not be feasible
- Model elements
 - Originators of information should assign a degree of trust in information they publish
 - All information be clearly identified with the source, ideally using a structured data format
 - But should be support for anonymous reporting, from Safety world experience



Trust: MS3i Model (2)

Model elements (contd.)

- Boundary Objects (structured information with mutual recognition across linguistic and domain boundaries) used to encapsulate information
- Both Originator and Recipient should assess how many times information previously received
- Originator or Recipient verify information independently checked
- Recipients of information should assign a subjective rating of the source



Trust: MS3i Model (3)

- Trust Metrics rely on the theories of networks and finite graphs: our modelling shows them as directed graphs (digraphs), with the nodes representing people and each edge representing the level of trust
- Noting the Hawking caveat about not knowing precisely how to perform the operation, transformation into Matroid Algebra has been omitted, but a Shape Function (Weibull CDF) has been derived :

$$U = \sum_A^x \frac{1 - e^{-\left(\frac{A \cdot W \cdot n^k}{n}\right)k}}{e}$$



ISO/IEC 27010: Scope of standard

- The Standard should specify the requirements, in terms of policies, processes, and controls, for implementing, operating, maintaining and improving the sharing of security related information. It can be used within an organisation, between organisations within a nation state and internationally.
- To align with ISO/IEC objectives, the Standard will be applicable to all types of organisations which are involved with Critical Infrastructure Protection (CIP), both public and private sector.
- The Standard will establish guidelines and general principles on how the specified requirements can be met using established messaging, and other technical, standards. It is designed to support the creation of trust when sharing sensitive and validated information, thereby encouraging the international growth of information sharing communities.



ISO/IEC 27010: Non Functional Requirements

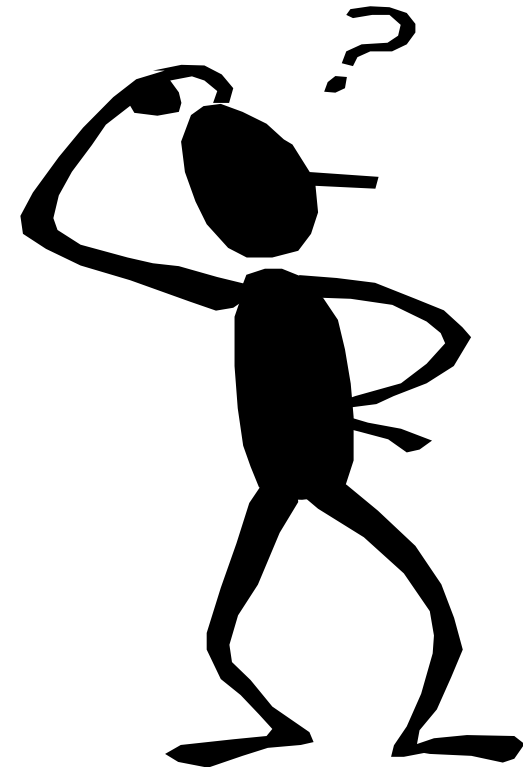
- **Trust:** The Standard should support trust in the messages received. This could include verification and validation of the information source, as well as the value of the content and how it should be handled.
- **Interoperability:** The ability of the Standard to support messages between a variety of computing systems and a variety of operational users.
- **Adoptability:** The Standard should be straightforward and cost effective to adopt, aligned to the needs of businesses and governments.
- **Robustness:** The Standard should be resistant to failures, both at a technical and understanding level.
- **Speed:** The Standard should not impose undue constraints on performance, providing the ability to deliver timely information through a number of different channels.
- **Flexibility:** Messages from a variety of sources and provenance ratings should be accommodated. Given the changing nature of information, the Standard should also be able to adapt and grow as the needs evolve.
- **Clarity:** The Standard should support the sharing of information which is in a form that is unambiguous.
- **Compliance:** The Standard should support compliance to the different regulatory and legal regimes across different sectors and member states.
- **Enabler:** The Standard should be seen as an enabler for other standards which have a need to share information and referenced where appropriate.
- **Automation:** The Standard should support the automated transfer and handling of messages, using a number of technical standards.

ISO/IEC 27010: Summary

- The MS3i Project has confirmed the need for an International Standard on trusted information sharing : work is under way to evolve such a Standard (ISO/IEC 27010)
- ISO/IEC 27010 **needs your support**
 - To ensure relevance, practicality, coverage
 - **Get involved through your National Body**
 - **Possible involvement of TF-CSIRT as Project Liaison**

TF-CSIRT Standardisation Update

- The Standardisation Process
- ISO/IEC 27035
- ISO/IEC 27010
- **Questions ?**





Contact Details

Ian Bryant

Information Assurance (IA) Advisor

MS3i Project

c/o Innovation Martlesham

Adastral Park

Martlesham Heath

Ipswich

Suffolk

IP5 3RE

ianb@ms3i.eu

+44 20 8392 5330 x2594; Desk

+44 79 7312 1924; Mobile

www.ms3i.eu