


*Ground Systems and the Challenge of  
Creating Collaborating I-A  
Communities via the Internet Research  
and Standards*

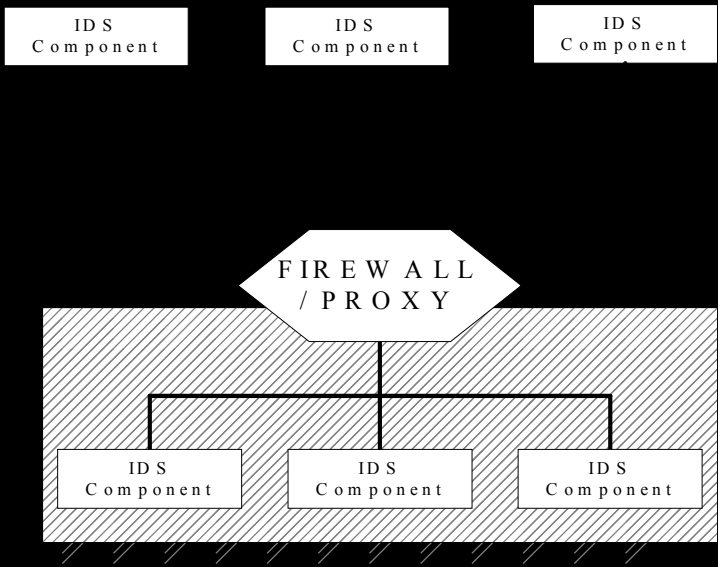


Ground Systems Architecture  
Workshop (GSAW) 2002  
El Segundo, CA, March, 2002

Joe Betser  
betser@aero.org

# *Motivation*

- Ground systems increasingly COTS-based
  - IA and security key in many GS projects
  - Increased connectivity
  - Multiple communities
- Intrusion detection is becoming widespread
  - Many different proprietary systems
  - Volume of data reported increasing
- Automation and interoperability are needed
  - Collect information in central repository
  - Collate and filter data
  - Automate response
- **Learn from the Process for Related Challenges**



## Innovation

- The first attempt at globally interoperable IDS protocols
- Incorporation of input from numerous stakeholder communities including: Research, Commercial, Academic, Government, and International

## Impact

- Create **global** Internet IDS protocols and data structures to enable IDS component communication in **global** enterprises
- IETF: Ubiquitous **global** dissemination of usage & interoperability -- a condition for advancement in standards track
- “Rough Consensus and Running Code”

## Schedule

		CIDF
1998	+	IETF IDWG Established
1999	+	Charter, Spec/Req design
2000	+	Reqs, IDMEF, IAP
2001	+	IDXP
2002	+	Interoperability testing

Standards track progress

# *Innovation*

- The first attempt at globally interoperable IDS protocols - **IEEE DISCEX Demonstrations, 13 June, 2001**
- Incorporation of input from numerous stakeholder communities including: **Research, Commercial, Academic, Government, and International**

# *Timeline*

- 1998 - Point-Solution IDSs
- 1998 - CIDF (Lunt, Staniford, Porras, et al)
- 1998 - IETF IDWG Established
- 1999 - Charter, Spec/Req, Design
- 2000 - Reqs, IDMEF, IAP
- 2001 - IDXP
- Interoperability Testing
- 2002 - Standards Track Progress
- Correlation, Response

# *Impact*

- Create **global** Internet IDS protocols and data structures to enable IDS component communication in **global** enterprises
- Ubiquitous **global** dissemination of usage & interoperability -- a condition for advancement in standards track
- “Rough Consensus and Running Code”

# *The IDS Process*

- IP infrastructure under attack
- IDS sensors/mgrs communicate via IDMEF/IDXP
- IDS information correlated by managers
- Detection drives response

# *Technical Approach*

- Develop widely used IDS Internet protocols
  - IETF IDWG (Intrusion Detection W/G)
    - Message structures and communication protocols
- Participation of Cisco, NAI, HP, Boeing, IBM, ISS, MITRE, MSFT, etc.
- 3 IETF meetings per year and interim IDWG meetings, much work done over email

# *The IETF*

- Standards body for the Internet
- Divided into Working Groups
- “Rough Consensus and Running Code”

# *The IDWG*

- Intrusion Detection Working Group
- Develop a common way to communicate
  - Message Format (XML)
    - IDMEF (Intrusion Detection Message Exchange Format)
  - Transport protocol
    - IDXP (Intrusion Detection eXchange Protocol)

# *The Hoover Institute*

- Bird's eye perspective on the challenge
- 1999 Conf on Cyber-Crime and Terrorism
- Multiple Communities and disciplines:
  - Technical, Policy, Law-enforcement, Legal, Government, Commercial, Civil Liberties
  - Diversity of cultures and approaches

# *Lessons Learned*

- Knowing what we know today, 5 years into the process, we draw several constructive conclusions that can serve other contributors who wish to embark on large collaborative research and standardization activities:
- It is critical to have the research results on fairly stable ground before standardization could proceed.
- Requirements must be specified for the working group and its desired products as early as practical.
- Standardization must involve all key stakeholders in the success of the deployed standard. This includes, and is not limited to, research contributors, industry vendors, and user organizations.

# *Lessons Learned (cont)*

- The standardization process must create and engage reference implementations and interoperability testing as the process advances. Continual feedback is used to improve the specifications, implementations, and research prototypes.
- Additional leverage can be obtained by using existing and emerging standards (BEEP) to enhance the new protocol standard (IDXP).
- The IETF mode of operation, i.e. “Rough Consensus and Running Code” is an excellent framework to achieve ubiquitous penetration of Internet IA protocols and data structures for all communities.
- Continual feedback and interaction among the stakeholder communities will enhance the success of both research and engineering.

# *Lessons Learned*

- Tough to build global consensus
- Wide spectrum of agendas among participants
- Strong collaboration with forward momentum
- Researchers and vendors participate
- Extraordinary leverage and tech transfer
- A lot can be accomplished with bright students

# *Publications*

- IETF drafts: Reqs, IDMEF, IDXP, Tunnel
- IEEE DISCEX
- IEEE SRDS
- ACSAC
- Hoover Institute Proceedings
- Future: Interoperability Reports

# *Acknowledgements*

- Silicon Defense
  - Stuart Staniford
- HMC
  - Mike Erlinger et al
- Aerospace
  - Andy Walther
  - Alan Foonberg
  - Dave Evans
  - Charlie Lavine
- IETF members
  - Dave Curry
  - Dipankar Gupta
  - Herve Debar
  - Darren New
  - Marshall Rose
  - John C. C. White
  - Paul Osterwald