# PWG -Imaging Device Security (IDS) Working Group

August 4, 2011

Camas, WA

PWG F2F Meeting

Joe Murdock (Sharp)

Brian Smithson (Ricoh)

# Agenda

| | |
|---|---|
| 9:00 – 9:15 | Administrative Tasks |
| 9:15 – 9:30 | NAC Attributes |
| 9:30 – 10:00 | NIAP |
| 10:00 – 11:00 | TNC Document review |
| 11:00 – 11:15 | Short Break |
| 11:15 – 12:30 | Black Hat Embedded Security session web cast |
| 12:30 – 13:15 | IAA and Security Model |
| 13:15 – 13:30 | Summary |

# Administrative Tasks

- Select minute-taker
- Introductions
- IP policy statement:
  *"This meeting is conducted under the rules of the PWG IP policy". If you don't agree, there's wine and beer tasting down south.*
- Approve Minutes from May 12 conference Call

# IDS WG Officers

- IDS WG Chairs
  - Joe Murdock (Sharp)
  - *Brian Smithson (Ricoh)*
- IDS WG Secretary:
  - *Brian Smithson (Ricoh)*
  - *IDS is on the lookout for a new secretary*
- IDS WG Document Editors:
  - HCD-ATR: Jerry Thrasher (Lexmark)
  - HCD-NAP: Joe Murdock (Sharp), Brian Smithson (Ricoh)
  - HCD-TNC: Ira McDonald (Samsung)
  - HCD-HR (Health Remediation): Joe Murdock (Sharp)
  - HCD-NAP-SCCM: Joe Murdock (Sharp)
  - IDS-Log: Mike Sweet (Apple)
  - IDS-IAA: Joe Murdock (Sharp)
  - IDS-Model: Ira McDonald, Joe Murdock, Ron Nevo

# Action Items

| Action Item # | Entry date | Assignee | Type | Action | Status | Disposition |
|---|---|---|---|---|---|---|
| 33 | 12/10/2009 | Randy Turner Ron Nevo | SHV | Randy Turner will contact Symantec (when appropriate) to encourage discussion with the PWG about a SHV. | | |
| 34 | 12/10/2009 | Randy Turner Ron Nevo | Remediation | Investigate Symantec's products and their method(s) to "remediate noncompliant endpoints." | | Need to indicate to Symantec that we really don't need too much proprietary information from them, but want to give them our information. |
| 44 | 3/11/2010 | Jerry Thrasher Ira McDonald Brian Smithson | NEA Binding | TCG TNC Binding document | P | Make it a TCG document, not an IETF NEA document |
| 80 | 2/3/2011 | Joe Murdock, Brian Smithson | WG admin | Update the description of the IDS WG to include scope that is larger than just NAC/NAP/etc. | | do this after Mike makes the new PWG web site and wiki pages |
| 81 | 2/3/2011 | Joe Murdock | IDS-LOG | Find the user role definitions in the IA&A or schema documents and import them into the LOG document | P | |
| 92 | 4/6/2011 | Michael Sweet | IDS-LOG | Update the rational section to higher-level statements | P | see 4/6/2011 minutes |
| 95 | 5/26/2011 | Joe Murdock | IDS-IAA | Make all of the identification UUIDs in the schema required elements | P | need to merge with symantic model version |
| 96 | 5/26/2011 | Joe Murdock | IDS-Model | Expand scenarios into use cases for security-related cases | | |

# Stable Documents

- HCD-Assessment-Attributes

  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-idsattributes10-20110127.pdf
  - Stable (needs a binding prototype)
- HCD-NAP Binding

  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-napsoh10-20100930.pdf
  - Stable
- HCD-NAC Business Case White Paper
  - ftp://ftp.pwg.org/pub/pwg/ids/white/tb-ids-hcd-nac-business-case-20100422.pdf
    - Final
- IDS Charter

  ftp://ftp.pwg.org/pub/pwg/ids/charter/ch-ids-charter-201100503.pdf
  - Updated charter approved by Steering Committee

# Active Document Status

- HCD-TNC Binding
  - Initial Draft still under development
- HCD-Health Remediation

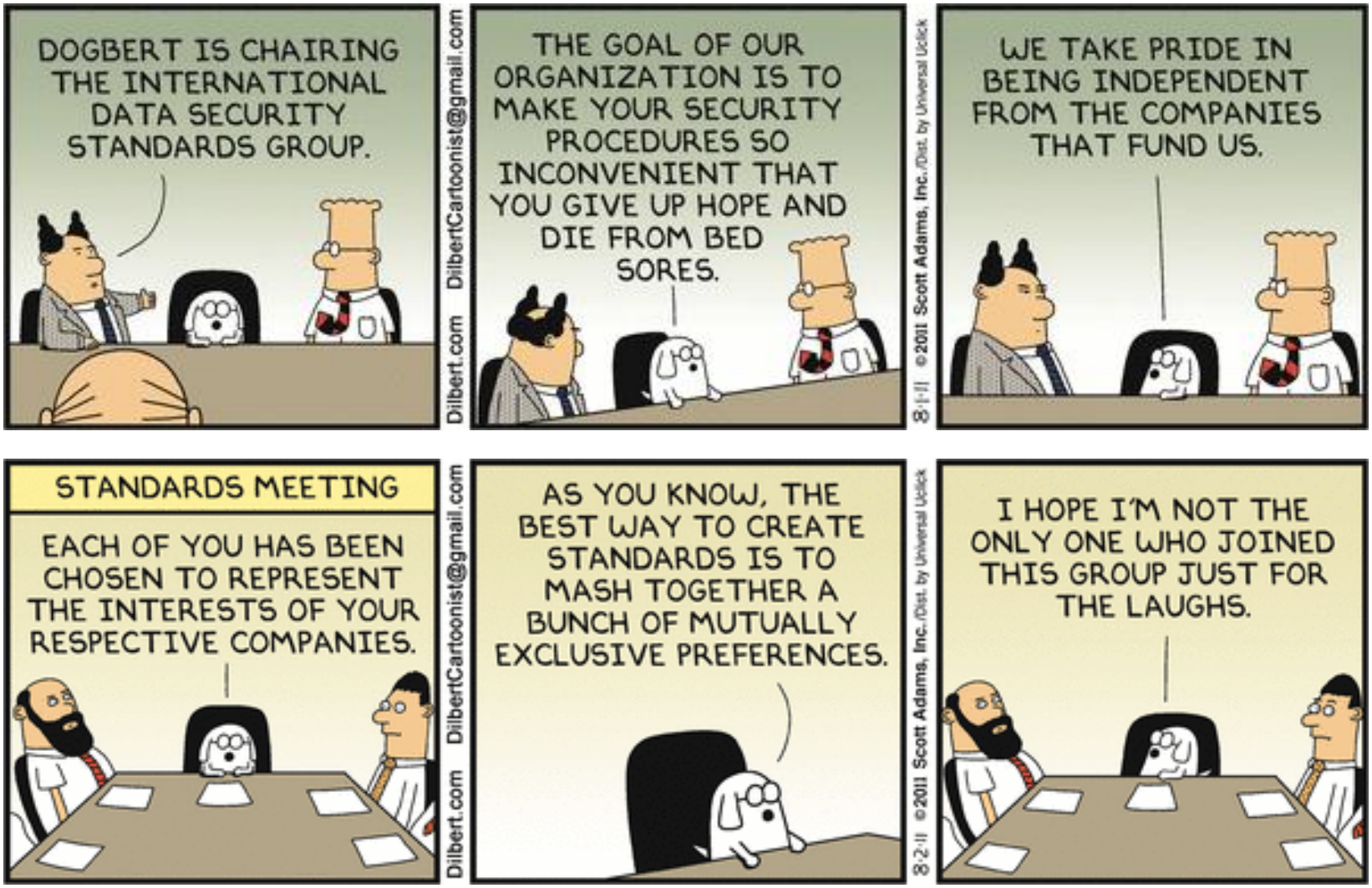
  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-remediation10-20100930.pdf
  - Initial Draft
- IDS-Log

  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-log10-20110326.pdf
  - Draft
- IDS-Identification-Authentication-Authorization

  ftp://pwg@ftp.pwg.org/pub/pwg/ids/wd/wd-ids-iaa10-20110801.pdf
  - Draft
- IDS-Model

  ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-model10-20110524.pdf
  - Draft

# What we're doing



# NAC Attribute Extensions

- After discussion with Steve Hanna and TNC teams, it was decide to drop the attributes
  - HCD_SecurityLog_URI (string)
    - The HCD_SysLog_URI attribute is a variable length string that specifies the location(s) where the HCD's system log is to be stored. Locations are provided as a URI and MUST conform to RFC 2396. When multiple locations are provided, the log is to be written to locations in the order indicated by the list, starting with the first provided location. If no explicate HCD_SysLog_URI locations have been defined by a system administrator, the system default internal log location MUST be returned
  - HCD_SecurityLog_Enabled (boolean)
    - The HCD_SysLog_Enabled attribute is a Boolean value that indicates if system logging is enabled for the device. If system logging is disabled (HCD_SysLog_Enabled = FALSE) then any value set for HCD_SysLog_URI is ignored.
  - IDS_Authentication_Service_URI Attribute
    - The HCD_SysLog_Enabled attribute is a variable length string that identifies the server(s) or service(s) the HCD will use to authenticate itself, users and remote devices or services.

# NIAP Support

- NIAP is not interested in our Supporting Documents proposal
- They are interested in working with us on defining a new tailored Protection Profile
- Is this something the group wants to take on?

# HCD-TNC Binding

- HCD-TNC Binding Specification Review
  Live review

# Black Hat Session

Today, everything from kitchen appliances to television sets come with an IP address. Network connectivity for various hardware devices opens up exciting opportunities. Forgot to lower the thermostat before leaving the house? Simply access it online. Need to record a show? Start the DVR with a mobile app. While embedded web servers are now as common as digital displays in hardware devices, sadly, security is not. What if that same convenience exposed photocopied documents online or allowed outsiders to record your telephone conversations? A frightening thought indeed.

The risk of insecure embedded web servers has been amplified by insecure networking practices. Every home and small business now runs a wireless network, but it was likely set up by someone with virtually no networking expertise. As such, many devices designed only for LAN access are now unintentionally Internet facing and wide open to attack from anyone, regardless of their location.

Leveraging the power of cloud based services, Zscaler spent several months scanning large portions of the Internet to understand the scope of this threat. Our findings will make any business owner think twice before purchasing a 'wifi enabled' device. We'll share the results of our findings, reveal specific vulnerabilities in a multitude of appliances and discuss how embedded web servers will represent a target rich environment for years to come.

Register for the webcast at:

https://www.blackhat.com/html/bh-us-11/bh-us-11-uplink.html

# IDS IAA

- IDS-IAA Specification Review

  ftp://pwg@ftp.pwg.org/pub/pwg/ids/wd/wd-ids-iaa10-20110801.pdf
  ftp://pwg@ftp.pwg.org/pub/pwg/ids/wd/wd-ids-iaa10-20110801_rev.pdf

  Schema and WSDL
  ftp://ftp.pwg.org/pub/pwg/ids/wd/schema/PwgSecurity.wsdl
  ftp://ftp.pwg.org/pub/pwg/ids/wd/schema/PwgSecurityOpMsg.xsd
  ftp://ftp.pwg.org/pub/pwg/ids/wd/schema/Security.xsd
  ftp://ftp.pwg.org/pub/pwg/ids/wd/schema/SecurityOperations.xsd

# Wrap up

- Review of new action items and open issues
- Conference call / F2F schedule
  - Next Conference call August 25, 2011
- Adjournment