IETF MILE: Improving Incident and Information Sharing Standards

Managed Incident Lightweight Exchange (MILE) Working Group

Kathleen M. Moriarty
EMC Office of the CTO
1 November 2011

EMC² where information lives

Agenda

- Automating Incident Response Coordination
  - Protocols in use today
  - Incident Object Description Exchange Format
  - Real-time Inter-network Defense
- Managed Incident Lightweight Exchange
  - IODEF Extensions
  - Generalizing RID

Incident Information Exchanges

- National Information Exchange Model (NIEM)
- Anti-Phishing Working Group (APWG)
- Research and Education Network – Information Sharing and Analysis Center (REN-ISAC)
- Japan Computer Emergency Response Team (JP-CERT)
- Cyber Security Information Exchange Tool (CYBIET) Project
- Cloud Security Alliance CloudSIRT
- Industry, led by financial sector, asks DHS to share incident information
- DoD: NIST business use case adopted by Unified Cross Domain Management Office (UCDMO) (IODEF and RID)
- NATO is reviewing RID and IODEF in their Cyber Defense Data eXchange and Collaboration Infrastructure (CDXI)

Incident Object Description and Exchange Format (IODEF)

Background

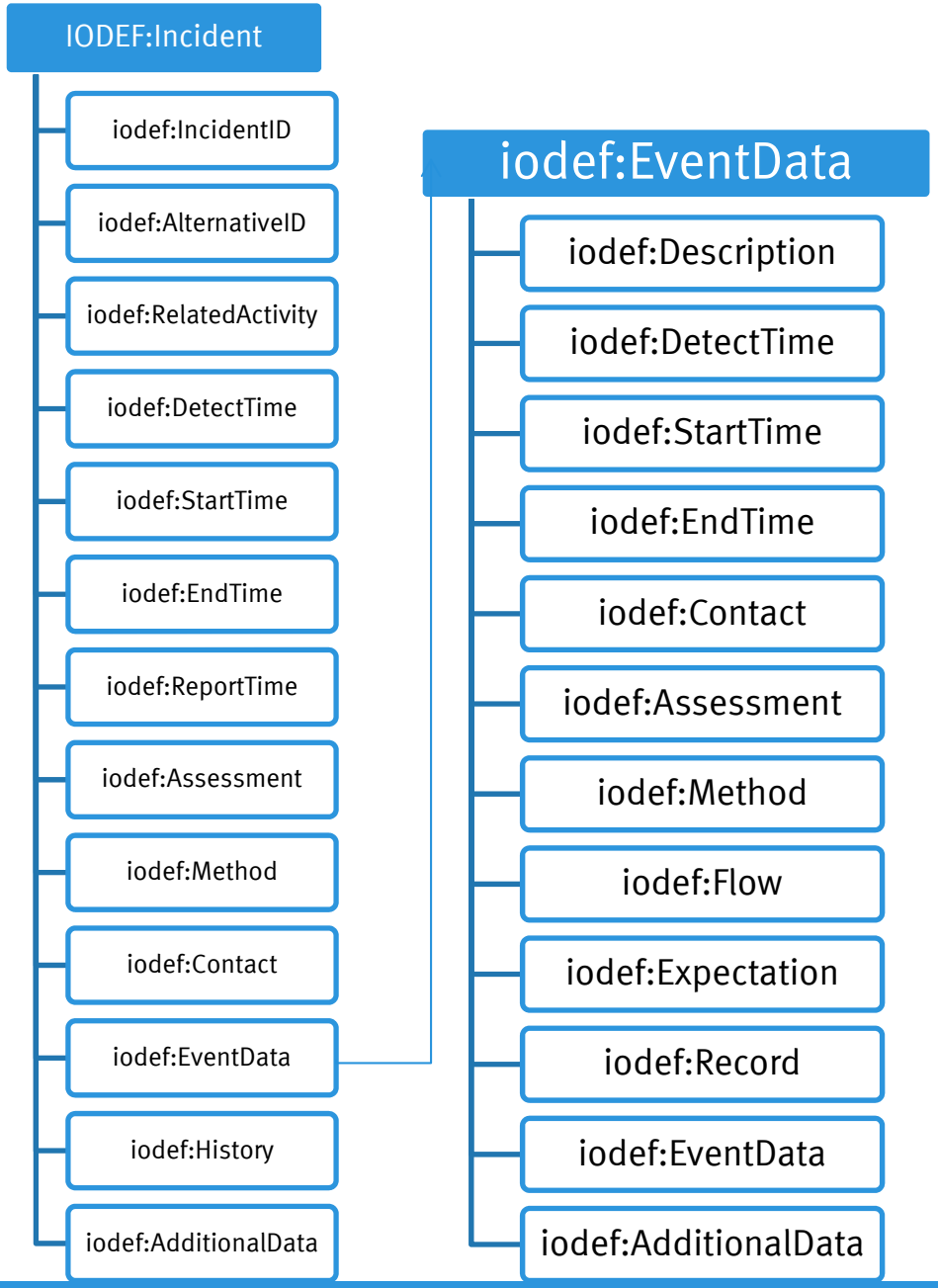
- Internet Engineering Task Force (IETF) Standard: RFC5070
- Provides a standard format to describe a security incident
- Effort led by the CERT Coordination Center (CERT/CC) out of Carnegie Mellon University
- Computer Security Incident Response Teams (CSIRTs) globally contributed to the development and evaluation of the Extensible Markup Language (XML) schema

Assumptions

- Incidents are not IDS alarms
  - "Incidents are composed of events"
- Agnostic to specific incident taxonomies
  - "Your definition/threshold of an incident may be different than mine"
- Incidents are numbered and there is state kept about them
  - "Organizations assign incident IDs and have ticketing/handling/correlation systems that process them"
- Merely a wire format
  - "Sharing is different than storage and archiving"
- Incomplete information
  - "You may require more complete information than I need, can get, or have right now"

IODEF Data Model

- CSIRT Operations
  - Incident identifiers
  - Contact Information
- Internationalization
  - Various Encodings
  - Translations
- Data handling labels
  - Sensitivity
  - Confidence
- Extensibility of attributes and adding new elements
- Timing information
- Enumeration of hosts or networks
  - e.g., IP addresses, ports, protocols, applications, etc.
- History and requested action
- Exploit and vulnerability references
- Impact expressed technically, financially, or by time
- Forensics information



EMC² where information lives

Real-time Inter-network Defense (RID)

RID Purpose and Security

- Goal: Exchange or share incident information
  - Facilitate secure communication of incident information between providers, entities, regions, or nations
  - Enable tracking of incidents as investigations evolve
  - Trace incidents to the source
  - Stop or mitigate the effects of an attack
  - Integrate with existing and future infrastructure components
- Security and Privacy Considerations:
  - Session and stored encryption
    - XML digital signatures and encryption
    - TLS used in transport
  - Authentication for single and multi-hop scenarios
  - Consortiums to establish trust relationships
  - Regional and international security and language barriers addressed via IETF Internationalization
  - Privacy: Data restriction markings, ability to optionally provide full data, anonymize data, or encrypt based on markers

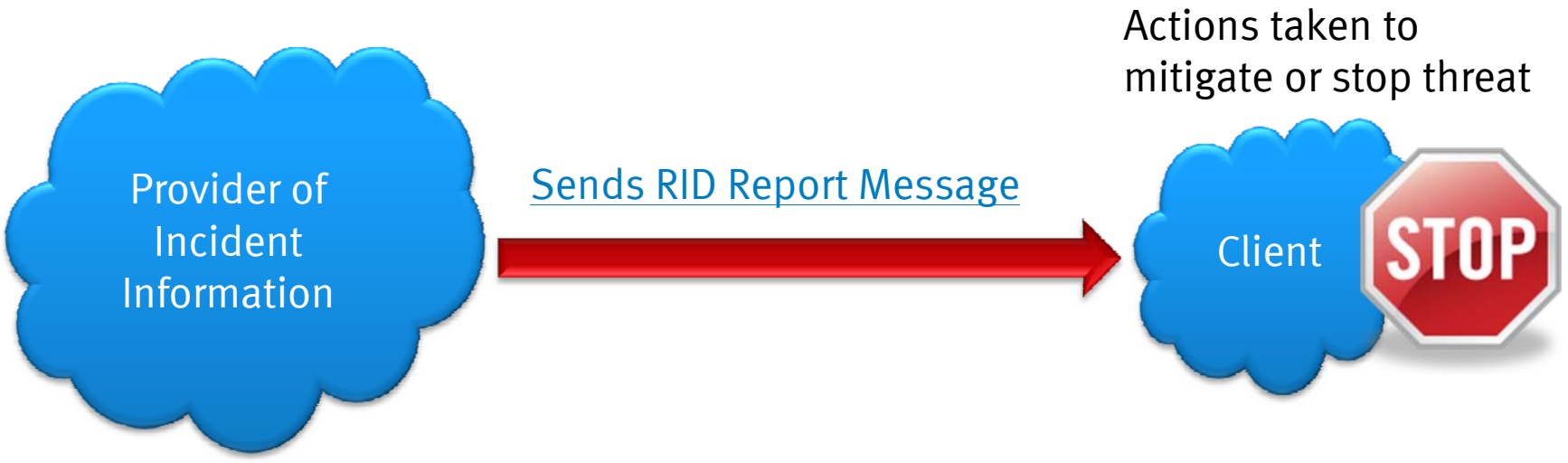
RID Message Types

- TraceRequest
- RequestAuthorization
- Result
- Investigation
- Report
- IncidentQuery

EMC² where information lives

Sharing Incident Information

IODEF, extensions to IODEF, and RID



- IODEF formatted incident report
  - May be anonymized
  - May be sent out to all clients or applicable client(s)
- Security, Privacy and policy provided via RID and transport

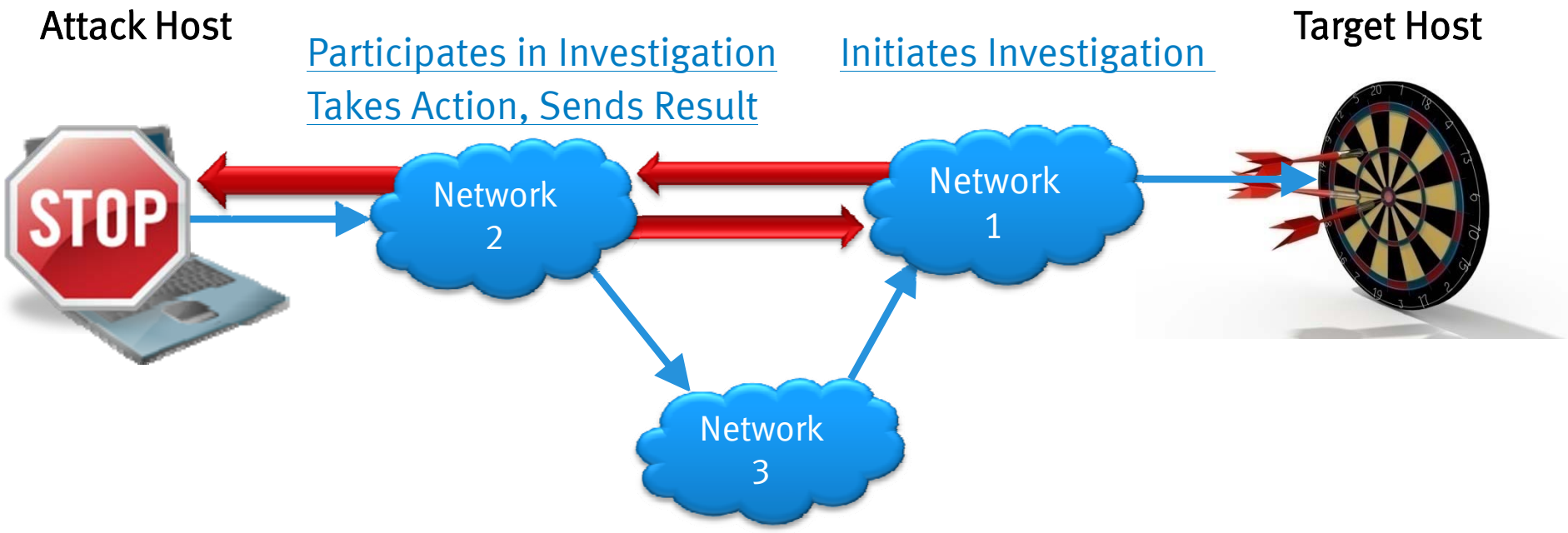
Query Incident Information

RID Exchange to Query Incident Information

- Client may be interested to know if others are seeing a specific type of incident or attack patterns
- Client sends request to Provider of Incident information
- RID Report message with IODEF document sent in response

RID: Investigation/TraceRequest Example

Investigation results in direct communication with source CSIRT



Agenda

- Automating Incident Response Coordination
  - Protocols in use today
  - Incident Object Description Exchange Format
  - Real-time Inter-network Defense
- Managed Incident Lightweight Exchange
  - IODEF Extensions
  - Generalizing RID

New Extensions to the IODEF Data Model

Drafts ready before Taipei

- Template for extensions
  - Initial draft exists
- Data Protection and Markings
  - Sensitivity and handling requirements
  - FIRST, DoD, and EMC oversight
- Integration of structured cyber security information
  - Motivated from CYBEX in ITU
  - NCIT, US CERT, MITRE, McAfee
- Mail abuse
  - MARF working group

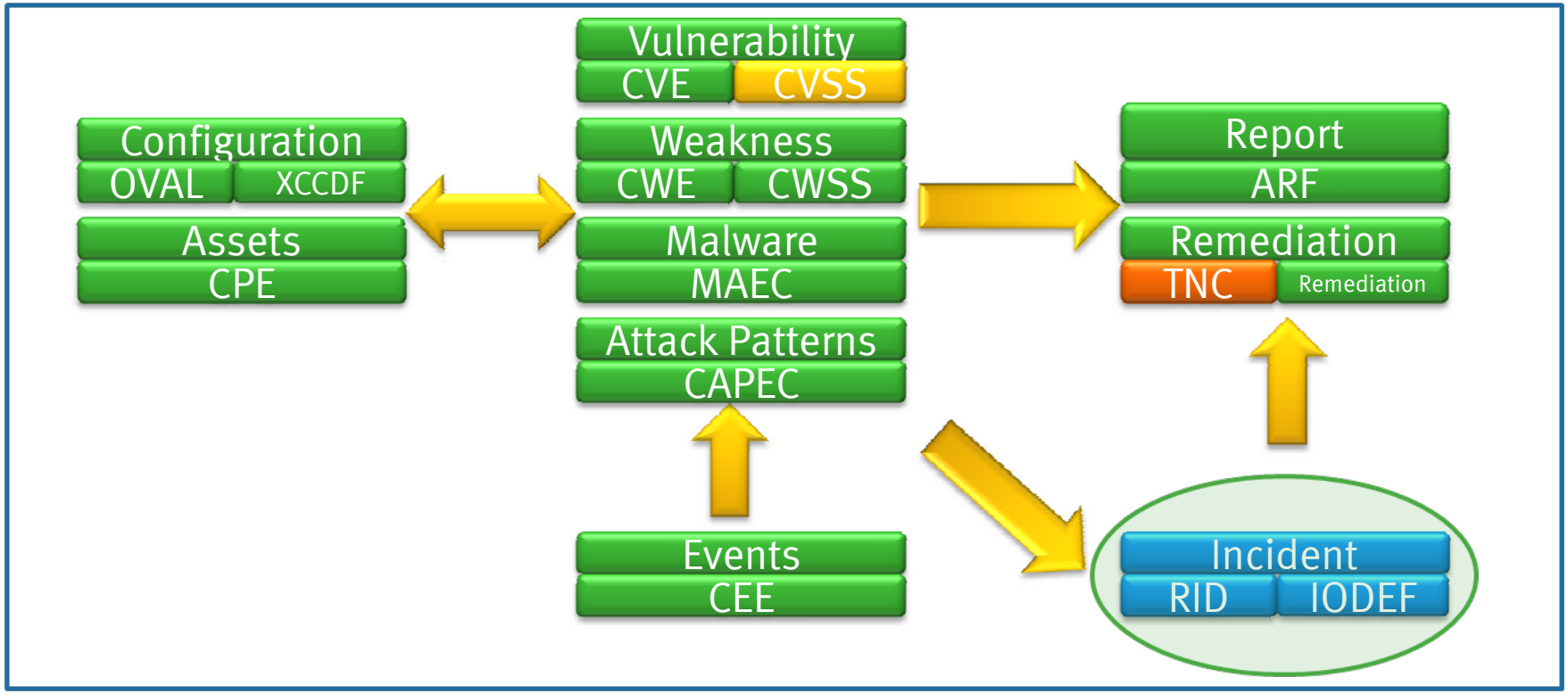
Future Work

- Financial Transactions
  - Extension exists, but review and possible re-write needed
- Virtualization
  - Represent all the data elements that need to be shared for a virtualization stack in the event of an incident
- Forensic Data
  - Korea initiative
  - Also LI-XML effort in OASIS
- Advanced Persistent Threat
- Misuse
  - Russia
- The following are not certain, from REN-ISAC
  - Malicious Code Characteristics
  - Malicious Infrastructure
  - Actor Profiles

EMC² where information lives

Structured Cyber Security Standards

Protocols and techniques encompassed in CYBEX and now IODEF



http://tools.ietf.org/html/draft-takahashi-mile-sci-01

EMC² where information lives

Data Markings

Extending marking options

- This extension will not state any handling requirements, rather provide options to mark data to enable policies to be applied as appropriate
- Retention
  - Are there retention requirements on the data included in an incident report?
- Markers for specific data types that are regulated
  - Personally Identifiable Information (PII)
    - Is PII actually contained in the incident?
    - If so, where did the PII originate?
  - Non-personally identifiable information (NPI) for GLBA
  - Credit card information for Payment Card Industry (PCI)

http://tools.ietf.org/html/draft-goodier-mile-data-markers-00

EMC² where information lives

Additional MILE work

Secure Communications and Guidance

- RID update in RFC6045-bis
  - http://tools.ietf.org/html/draft-moriarty-mile-rfc6045-bis-01
- RID Transport update in RFC6046-bis
  - http://tools.ietf.org/html/draft-trammell-mile-rfc6046-bis-01
- Generalizing RID for use by any XML schema
  - http://tools.ietf.org/html/draft-moriarty-mile-grc-exchange-01
- IODEF Guidance
  - Coming soon…

Generalizing RID

New Draft Document: GRC Report Exchange

- New draft to generalize RID for use with any XML schema
  - In an early review stage, comments and feedback are welcome!
- Related user groups:
  - Requested by ITU for Legal XML use case work with OASIS (LI-XML)
  - Requested by Governance, Risk, and Compliance XML (GRC-XML) group in OMG
  - Under review by the Emerging Specifications list for possible use
- Desire to standardize the security, policy and privacy options for incident response to these other XML formatted documents for exchange purposes

http://tools.ietf.org/html/draft-moriarty-mile-grc-exchange-01

EMC² where information lives

Summary

MILE: IODEF, RID, and new Extensions

- IODEF and RID are IETF standards with additional standardization activity in progress due to business drivers
  - Need to standardize incident formats has become more prevalent in the enterprise
    - CSIRTs at the enterprise level increasing, driven by business requirements and increases in Fraud
    - Easier to aggregate, process, and disseminate incident information within the organization
    - Requires ability to correlate incidents to system configuration & vulnerabilities (SCAP + IODEF + RID)
  - New extension formats are required to standardize exchanges for specific incident types and data classification requirements
- Increase in severity of incidents and outsourcing (Cloud) is driving the need for automation in incident response

EMC² where information lives

Q&A

THANK YOU