Threat Information Sharing; Perspectives, Strategies, and Scenarios

15 June 2015

Tim Grance, NIST, Sarah Brown, Fox-IT, Luc Dandurand, ITU
Thomas Millar, US CERT, Pawel Pawlinski, CERT.PL

Information Sharing Benefits

- Organizations are sharing information and collaborating on its refinement for:
  - Shared Situational Awareness
  - Expanded Understanding of Threat Horizon
  - Knowledge Maturation
  - Greater Defensive Agility
  - Improved Decision-Making

Information Sharing Challenges

- Prior to Sharing
  - Establishing Trust
  - Policy, Legal, and Organizational Restrictions
  - Risk / Benefit Analysis – what to share?
- As Data is Shared
  - Collecting and classifying information
  - System interoperability
  - Preserving Anonymity
- Post Sharing
  - Classification of information
  - Generate / refine / action the intelligence

Desired Characteristics of Cyber Threat Information

- **Timely** – in time for the recipient to act
- **Relevant** – applicable to the recipient’s operational environment
- **Accurate** – correct, complete, and unambiguous
- **Specific** – providing sufficient detail and context
- **Actionable** – providing or suggesting an effective course of action

Cyber Threat Information Sources

- **Internal**
  - Intrusion Detection/Protection Systems
  - Security Information and Event Management
  - OS, network, security, and application logs
  - Personnel
- **External**
  - Open, public sharing communities
  - Government sources
  - Sector peers and business partners
  - Vendor alerts and advisories
  - Commercial Services

Cyber Threat Information Types

- **Indicators** – an artifact or observation that suggests that an attack is imminent, is underway, or may have already occurred
- **Tactics, Techniques, and Procedures** – insights related to an adversary’s behavior, conduct, and tools
- **Countermeasures** – actions to counter a specific threat
- **Adversary** – information regarding the threat agent or actor

Observations on Trust

- Trust equals knowledge, skills, experience, abilities, accuracy, integrity, reliability, commitment
- Trust gives us confidence to act
- When we trust we are more likely to share
- Trust is hard to earn, it must be cultivated
- Trust is difficult to restore if lost

Building and Maintaining Trust

- Trust is built through shared experiences
- Use sharing models that bring together contributors, participants, and consumers
  - Discuss current threats
  - Share technical insights
  - Develop mitigation strategies
  - Train, mentor, and develop skills
  - Mentor new community members
  - Develop key practices and resources

Establishing Sharing Relationships

- Define Goals, Objectives, and Scope of Sharing
  - Mission specifics; resources; approvals
- Conduct an Information Inventory
- Establish Information Sharing Rules
  - Sources; sensitivity; restrictions; marking
- Join existing Sharing Communities
  - Info actionable; mechanisms; NDAs, etc.
- Supporting an Information Sharing Capability
  - Resources; proactive measures
- Look for information that is easier to share (e.g., threats vs incidents)

Discussion Questions

1. What are the sharing barriers?
2. Overview of sharing architectures, capabilities, technical mechanisms (e.g.identity, access control, etc), and trust issues
3. How is sharing done today?
    1. Non-attributed vs attributed.
    2. Protection of shared information.
    3. Data analytics, etc.
4. Advice on how to create, maintain, and enhance sharing relationships
5. How can sharing be more scalable?
6. Specific technical and policy recommendations for the use of shared threat information. Indemnification?
7. What examples (past or future) or specific incident scenarios illustrate how sharing could realistically work to improve security and operational capability?

Achieving Meaningful Information Sharing: A Few Take-Aways

- Operate at time scales consistent with the information
- Trust leverages personal connections, operational record, legal processes
- Trust is paramount and hard to establish, but preparation helps
- As communities grow in size, trust is harder to achieve
- Organizational abilities vary greatly
- Roles and responsibilities need to be clearly articulated before sharing
- Simplicity facilitates sharing