



An APWG Industry and Law Enforcement Data Policy Project

eLENS:

The Emergent
Law Enforcement
Network Security
Initiative

Bridging the Gaps
in eCrime
Data Sharing

The APWG logo is the letters 'APWG' in a bold, white, sans-serif font, centered within a dark green rectangular box with a thin white border. The background of the entire slide is a satellite map of Europe with numerous green lines radiating from the center, suggesting a network or data flow.

APWG

Committed to Wiping Out
Internet Scams and Fraud

April 2009

Correspondent Authors Contact Data:

Erin E. Kenneally, [erin@elchemy.org]
TechLaw Specialist, U. of California San Diego, and CEO, eLCHEMY, Inc.

Patrick Cain, [pcain@antiphishing.org]
Research Fellow, APWG; and President, The Cooper-Cain Group, Inc.

Randy Vaughn, [rl_vaughn@baylor.edu]
Baylor University; and Chair, APWG eCrime Researchers Summit

Disclaimer: PLEASE NOTE: The APWG and its cooperating investigators, researchers, and service providers have provided this message as a public service, based upon aggregated professional experience and personal opinion. These recommendations are not a complete list of steps that may be taken to avoid harm from phishing. We offer no warranty as to the completeness, accuracy, or pertinence of these recommendations with respect to any particular registrar's operation, or with respect to any particular form of criminal attack. Please see the APWG website – <http://www.apwg.org> – for more information.

eLENS Initiative Project Summary

The Emergent Law Enforcement-Network Security Initiative (eLENS) is an effort sponsored by the APWG that endeavors to take responsibility for helping to bridge the eCrime data-sharing gap between public law enforcement, private network security, investigative intelligence, network measurement and experimentation, and related policy. While the operational lines between these entities are blurring, there is no corresponding policy to guide and coordinate what is occurring informally and on an *ad hoc* basis. The eLENS effort will initially develop and promote uniform data exchange guidelines that address the full life cycle of information flows: discovery, acquisition, sharing, and disclosure. This will take into account the legality of capturing, observing, and sharing network activity, including the proper roles of the various stakeholders, and observance of evidentiary chain-of-custody principles to ensure resulting actions are ethically and legally actionable.

The three foundational tasks for the eLENS effort are 1) inventory and coalesce existing solution(s) to our defined problems from across the globe; 2) where gaps or deficiencies exist, develop reference guidance and processes for the orderly exchange of network and eCrime information; and 3) generate community dialogue on these recommendations from relevant stakeholders before revising and publishing them for practical use.

This effort will be composed of a number of small groups completing parallel tasks to allow for the efficient use of subject matter specialists and to minimize large-scale introductory adventures. The initial small groups may be (1) process models for sharing information; (2) description of acceptable sharing data formats and standards; and (3) identification of common sharing dynamics -- how and what to collect --- for specific situations and events. Other groups will be chartered and operate as they are identified.

The effort is targeted to complete in calendar year 2009. Some groups may operate into the future as situations warrant. Parties interested in participating in this effort should contact the APWG or one of the eLENS initiative's leaders.

eLENS Initiative Programmatic Motives

Counter-eCrime research and data exchange, in its present state, is highly inefficient, error-prone and burdened with uncertainty and doubt about the forensic utility and, in the jurisprudence dimensions, admissibility of much electronic crime event data. The eCrime and security researchers self-organize into a multitude of vetted research groups which are often based on listservs, private forums, or *ad hoc* wikis. Inter-researcher sharing may include topics of many forms, including: anecdotal observations of network abuse; independent malware sample sharing and analysis; and discussions of general trends.

Such research communities integrate well into the fast pace of security research. However, research communities do not always succeed in producing actionable intelligence for legal agencies or other consumers. In fact, most counter-eCrime research communities attempt to operate in a manner that inhibits data disclosure to external entities. The fusion of disparate data sources into a larger, more complete picture is routinely necessary to analyze the entire eCrime situation, but nearly prohibitive given contemporary eCrime data exchange impediments.

This process of data fusion attempts to overcome the barriers to reducing Internet-based criminal activities by promoting secure and effective communications between all counter-eCrime interests. Guidelines, which outline acceptable discovery, collection, and disclosure of eCrime event data (and co-opted data precipitated from eCrime events), need to be in place in order to facilitate and coordinate legally acceptable data discovery and collection mechanisms required to fight the criminal pandemic facing Internet commerce. As both the techniques and loci of eCrime can mutate rapidly, proactive countermeasures require the automated distribution of usable empirical intelligence.

Merely collecting and distributing eCrime intelligence is not sufficient to add significant improvement to counter-eCrime operations. Systematic cooperation between Law Enforcement and Network Security professionals requires clearly communicated procedures, organization, and management of data fusion and exchange through continuous review and incremental improvements of the system processes. Additionally, a successful eLENS system must identify the communities of interests, define their scopes of action, and recruit their participation in the development and operation of an effective system.

Of course, many assumptions and goals are present. No system is without cost, and a worthwhile system must meet a need and simultaneously not blockade effective advancements in countering eCrime. Other assumptions for the success of an eLENS initiative are:

- 1) The process of data fusion and exchange between researchers and enforcement agencies is complicated by a variety of constraints and carries inherent risks, but is not impossible.

- 2) Not all researchers are aware of effective data collection methods, which can result in increased infrastructure security and in the prevention and prosecution of electronic crime, but most are willing to adapt their methods to align with the needs of law enforcement.
- 3) Law enforcement will benefit from additional, well-structured data and collection methods which reputable sources can provide.
- 4) Empirical counter-eCrime and network measurement practices, which demonstrably increase the effectiveness of legal proceedings and policies against eCrime, will motivate additional researcher contributions and evolve the normative reliance on empirical measurement. The consequence will be improved research quality and capabilities, and more just decision making.
- 5) Properly designed and managed counter-eCrime methods, combined with clearly communicated procedures for data exchange, can facilitate cooperation between government, commercial, and researcher interests in a manner that is consistent with the constraints and concerns of each community.

eLENS Initiative Goals

It is important to set reasonable, measurable goals that will drive the successful achievement of an effective eLENS system. For example, goals for the first stage of an effective eLENS should focus on achieving a foundation that provides:

- 1) An implementation that can clearly communicate the rules governing the collection and distribution of data in a manner consistent with proper legal requirements.
- 2) Open procedures and policies which provide transparency into the methodologies for data discovery, collection, distribution, and disclosure.
- 3) Feedback to researchers that communicates the utility and quality of their data and data collection methods in a manner that will facilitate effective and timely submission and subsequent distribution.
- 4) A method for ensuring the privacy of all system constituents without restricting their abilities to share data.
- 5) Security measures to ensure the integrity, confidentiality, and availability of the system and its contributors, which strongly mitigates against inappropriate distribution of data or exposure of data sources.

- 6) A design that will allow data exchange using accepted security data protocols and that will not add complexity to the workloads of any of the system consumers.
- 7) Dynamic procedures which can adapt to mutations of existing eCrime dynamics as well as to novel species of eCrime.

eLENS Data Sharing Actors and Roles

For practically-useful eCrime data to be efficiently shared, each stakeholder must agree on the expectations of the exchange and trust the information flow. eLENS envisions that the cognizant parties in an eCrime data sharing system include.

- Detector. The party that detects and reports an eCrime event is identified as a detector. Many events will have multiple detectors.
- Initial Investigator. This is the party that performs triage or initial investigation on an eCrime event. They should be knowledgeable about the important data to capture or identify how that data will traverse through the system.
- Downstream Collaborator. This party may or may not also be a detector for this event. Collaborators receive investigative data for advice, fusing with other sources, statistics generation, or further empirical or investigative research.
- Law Enforcement (LE) Investigator. This stakeholder is an agent of the government, and may receive eCrime information for investigative or evidentiary purposes.
- Notified Parties. Some groups have no investigative or research interest but may need to be informed of the event so they can commence other activities. Examples include a victim of an eCrime or a phished financial institution. This group encompasses all stakeholders not already identified.

Note that some actors will engage multiple roles for a single event or a set of inter-related events. For example, a *LE Investigator* may be a *downstream collaborator* and may also have been the *detector*.

The intent of the eLENS Initiative is to provide guidance to these parties so as to set levels of expectations, address concerns, and identify requirements across and between all parties. By preempting common procedural hurdles with normative solution options, eLENS aims to more efficiently and effectively avoid the risks that permeate our current data sharing approaches.

The Initial Tasks

This initiative involves five initial tasks grouped into three categories.

1. The first category is to seek out an existing solution. Its sole task is to survey the global eCrime fighter community and identify programs, projects, and documents that inform or provide the output for which this Initiative aims. The goal is steward and coalesce existing, practicable and competent work-product, and to avoid duplication and redundancy. Initial inventorying has not yet identified all candidate solutions.

2. The second category is to develop the guidance and processes necessary for efficient data sharing. This category is composed of at least three tasks, summarized below.

- (A) Develop a legal framework and guidance for private organizations to distribute or exchange eCrime data to other stakeholders, taking into account regulatory and legal parameters, specifically including privacy, intellectual property, confidentiality, and community ethics standards.
- (B) Identify or develop technical means to collect, package, and transport electronic data between parties.
- (C) Define multiple reference documents to guide a Detector party on the appropriate and necessary information to collect for a variety of eCrime applications, such that the resultant information product is sufficient and worthwhile to a downstream investigator, LEA or other constituent decision maker.

3. The third category of tasks comprises initial disclosure, iterative gathering and responding to commentary, and eventual authoritative publication of the guidance in an appropriate forum.

Other tasks will be initiated as necessary as the initiative progress and initial work completes.

Summary

As the Internet provides the communication artery for government, commerce, and society, threats and crimes leveraging Internet infrastructure cannot be ignored; the effectiveness of legal proceedings must be increased; it is critical that our tactical and strategic decision makers operate from reliable information; and, cooperation between networks, researchers and law enforcement is necessary. The eLENS framework provides a mechanism for proactively achieving the common goals of reduced crime and increased security.

Participation Information

For more information, or to participate in this initiative, please contact one of the eLENS initiative leaders or APWG Secretary General Peter Cassidy at pcassidy@antiphishing.org.