

1. Name of the Technology and the Corporation Supporting It

Product: **Peer Offering Service** (distribution of authorized content)

Company: **Exploit Systems Inc.**
Palo Alto, CA
info@exploitsystems.com
www.exploitsystems.com

RFI Contact: Todd Souvignier
Co-Founder and CTO
Exploit Systems, Inc.
todd@exploitsystems.com

NOTE: Information presented in this report is based in good faith on information provided by the company offering the technologies described. No independent 'due diligence' has been carried out to verify the original source information.
--

2. The Applicable Technology Application Area and Overview

Exploit Systems Inc. holds the view that the “anti-piracy approach to P2P is an incomplete solution” and their approach is designed to fill P2P query systems with massive amounts of responses that point to legitimate offerings on legitimate sites. Exploit Systems Inc. holds the view that this would simultaneously:

- * Ensure a legitimate alternative for acquiring copyrighted files
- * Swamp query results leading to unauthorized copies of copyrighted works with a deluge of query results pointing to legitimate copies of those same works, thus flushing away “pirate” trading of files.

The *Peer Offering Service* (POS) being developed by Exploit Systems is based around a query engine that can generate and offer responses to P2P queries. This engine is implemented as part of a distributed application, called *Clone Farm*, that interfaces with P2P networks. Query responses generated within the Clone Farm can point to copies of specific requested files that are hosted by agreement with content owners, behind a Storefront e-commerce system that is also provided by Exploit Systems. Currently, all of the system components are in alpha-testing.

3. Detailed Technology Description

3.1 Network Architecture

Exploit Systems stated “Information available only under terms of NDA”. However, from descriptions provided in parts of the response it can be deduced that the Clone Farm consists of server systems ‘attached to’ P2P networks from a multitude of non-contiguous IP addresses but under central control of Exploit Systems.

3.2 Scalability

Exploit Systems’ proposal encompasses several distinct system components. The approach relies directly on P2P systems regarding what might be termed the ‘consumer-facing’ interface. Then there is the separate e-commerce system interface, for which scalability is currently under test. No information is provided on the scalability of the Clone Farm. The response indicates that the scale of legitimate content available depends on the extent to which content providers utilize the system and the extent to which files that utilize the system are ‘seeded’ into P2P networks.

3.3 Protocol Identification

While POS is not designed to “identify” P2P protocols, the Clone Farm clearly needs to interface with specific P2P networks. Currently, interfaces are available into the FastTrack and Gnutella protocols (although information was not provided as to which FastTrack versions are supported).

3.4 Granularity of Protocols

Clone Farm feeds responses into the P2P network corresponding to queries that can be associated with requests for specific content items. Thus the granularity is at the query-response level. Additionally, responses would point to legitimate copies of the requested files, where these had been provided under rights holder agreements.

3.5 Content Identification

Not applicable – the system is based around processing of query traffic.

3.6 Examination of Network Packets or File Content

Exploit Systems’ response states “Not Applicable” presumably because traffic flows and packets are not subjected to a network-centric analysis. However it can be anticipated that Clone Farm nodes receiving queries from the P2P network would process those queries for the purposes of providing a response – in much the same way as a standard P2P node would, i.e. by supplying a pointer to a file corresponding to the request.

3.7 Distribution System

Exploit Systems' POS is designed to work with the Gnutella protocol and the FastTrack protocol (which version is unclear).

3.8 Resilience of the Technology to Countermeasures

Exploit Systems provided several possible threats and their analysis of the significance of these including:

- * IP blocking of CloneFarm nodes. Non-contiguous IP blocks are used, together with an IP migration strategy.
- * DoS attacks against CloneFarm. The application is distributed and incorporates timeouts and IP-blocking to hinder DoS attacks. Additional security measures are claimed, but not disclosed.

3.9 Testing and Installed Base

Exploit Systems' technology is at "alpha-test" and the installed base is "under Non-Disclosure".

3.10 Competitive Approaches

Exploit Systems claims no direct competitor. The company also claims advantages for its P2P-based legitimate distribution system in terms of leveraging P2P for efficient distribution of authorized files.

3.11 Third-Party Components

In terms of the POS core systems, Exploit Systems presents a self-contained proposal. Third-party DRM and payment systems would be needed within the e-commerce aspect of the system. Access to authorized content is another aspect of the overall system – but this is not covered in the response document. Authorisation is often based on territorial licensing arrangements.

4. Intellectual Property

Exploit Systems has filed for US and international patents on the Clone Farm and associated parts of their system.

5. Corporate Characteristics

Exploit Systems is a privately held California corporation based in Palo Alto. The company was founded in 2001 and has twelve full-time staff plus contract engineering resource of eleven further staff. Financial information and customer base is available "only under Non-Disclosure".

6. Pilot Testing

The company states that systems should be available for testing following July 2003 on terms that would be negotiated on a case-by-case basis with clients. Pro-bono arrangements are precluded.

7. Commercial Terms

Terms are negotiable "Under Non-Disclosure"

8. Other Information

N/A