available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

When Internet protocols and legal provisions collide: Unauthorised access and *Sierra v. Ritz*

Alana Maurushat[a], *Ron Yu*[b]

[a]*Cyberspace Law and Policy Centre, Faculty of Law, UNSW, Australia*
[b]*Gilkron Limited, Hong Kong*

Keywords:
Sierra v. Ritz
Spamming
Zone transfer
Computer misuse
Domain name system

ABSTRACT

This case note article examines the unreported decision of a U.S. court in *Sierra Corporate Design Inc. v. David Ritz* (2007) District Court, County of Cass, State of North Dakota (File No. op-05-C-01660) which deals with the unauthorised use of a domain name system zone transfer. The court ruled that access was unauthorized given the defendant's intention to obtain and divulge information found in the zone transfer.

1. Background

The trial court decision of *Sierra v. Ritz*[1] involved unauthorised use of a domain name system zone transfer. Zone transfers are generally speaking open access public information which provides data about all of the machines within a domain. Without zone transfer, you would literally have to type in an IP (internet protocol) address every time you went to a website – it is one factor contributing to the convenience of the Internet. The information may be retrieved by the use of 'host command' with the 'l' option. Zone transfers contain public information to varying degrees depending on the protocols used by an organization. Zone transfers may be disabled to the greater public with only trusted machines and senior administrators having access on a 'need to know' basis. This is a form of limited authorised public access. In Sierra's case, the zone transfer was more widely available in the sense that the system allowed zone transfers to everyone, thereby publicizing potentially private data into a public forum. There would be no way for a person accessing the zone transfer in the latter context to know whether Sierra was truly allowing shared access or whether it was merely a mis-configuration. From a technical perspective, this is a situation of authorised access to the information found in the zone transfer. From a legal perspective, the judge ruled that access was unauthorized with a large emphasis placed on the defendant's intention to obtain and divulge information found in the zone transfer.[2] David Ritz is a well-known anti-spammer. There has been debate as to whether Sierra has facilitated spam in the past. Neither of these two facts appeared to weigh into the decision. While *Sierra v. Ritz* is a civil suit, Ritz has been criminally charged with unauthorised access to a computer in North Dakota. The criminal trial is pending.

The case illustrates how the terms 'unauthorised' and 'access' do not produce a similar set of shared assumptions in the technical, legal or ethical fields. A technical researcher may falsely assume that they are operating within safe legal parameters only to discover that such parameters do not translate across fields. The technical researcher would likely assume that he/she is authorised to perform an act where technical protocols and programming convention allow for it. From a legal standpoint, authorisation and consent involve a number of factors including intention, damage, and the bargaining position of affected parties. One commentator on

[1] The judgment is unreported. A copy of the decision is accessible from private list-serves as well as from the webpages of SpamSuite.com. *Sierra Corporate Design Inc. v. David Ritz* (2007) District Court, County of Cass, State of North Dakota, File No. op-05-C-01660. *See* www.spamsuit.com.com/node/351.

[2] A detailed analysis of the case can be found on SpamSuite.com available at http://www.spamsuite.com/node/351.

0267-3649/$ – see front matter
doi:10.1016/j.clsr.2009.02.005

the decision noted that it is the equivalent of, ''Mommy, *can* I have a cookie? Sure you can have a cookie, but you *may* not.''[3] The case foregrounds a reoccurring theme: if a user interacts with a server in a way that the protocol does not prohibit but which is upsetting to the server's operator, should this be construed as ''unauthorized access'' as a matter of law?[4] This article examines, from a policy perspective, the scope of ''unauthorized access'' in computer fraud statutes within the decision of *Sierra v. Ritz*.

2. What's in a zone transfer?

The domain name system (DNS) helps users find their way around the Internet by allowing them to remember a name instead of a complex IP address.

A DNS namespace can be divided up into zones, which store name information about one or more DNS domains. For each DNS domain name included in a zone, the zone becomes the authoritative source for information about that domain.

Because of the important role that zones play in the DNS, DNS information needs to be available from more than one DNS server on the network to provide availability and fault tolerance when resolving name queries. Otherwise, if a single server is used and that server is not responding, queries for names in the zone can lead to failure to resolve the domain name.[5] Thus, secondary (or 'slave') DNS servers are also deployed.

Secondary DNS servers do not load zone-related information from local master files, which are locally edited, but instead obtain their information from the primary (or 'master') server on a regular basis.[6]

The contents of a DNS zone file can be copied from a primary DNS server to a secondary DNS server through the zone transfer process.

A zone transfer occurs, *inter alia*, when changes are saved to the primary zone file and there is a notification list or when DNS services are started on a secondary DNS server.[7] The latter may occur, for example, when a secondary DNS server starts up, has no information about the zone and therefore must immediately perform a full zone transfer.[8]

When a zone transfer is required, a (TCP) session must first be established and used for zone transfers. Then a DNS query is sent to the primary DNS server for name resolution, and a command is used to initiate the zone transfer. The server will then transfer the resource records for the zone using a series of messages (assuming that the server that requested the transfer is authorized to do so). The transfer performed may be a full or incremental one.

Once the zone transfer is complete, the secondary DNS server will update its database and return to regular operation.

As DNS zone transfers are a necessary and critical aspect of DNS operation, and can not be turned off completely, it is up to an organization to ensure that the appropriate security mechanisms are in place such as only permitting zone transfers between DNS servers and clients that actually need it.[9] Zone transfers are useful for replicating DNS data on a local DNS server in order to conserve bandwidth, to speed up requests or to make DNS data available when disconnected from the Internet.[10]

Theoretically, the zone transfer mechanism can be used to replicate a database,[11] though in actuality it is not possible to fully replicate actual database contents using a zone transfer. Replication of the contents of an actual database may only occur where an organization deliberately or accidentally places such data onto the zone transfer. This has several ramifications where the database is replicable. First, this allows others to view potentially private data. Second, this potentially allows for security vulnerabilities to be exploited. For instance, a malicious hacker could obtain a copy of a complete listing of all hosts in the domain through the DNS zone, thus making the hacker's job much easier. If a hacker could perform a DNS zone transfer the hacker could potentially launch a Denial of Service attack against that zone's DNS servers by bogging them down with multiple requests.[12] The hacker could also send erroneous information throughout the domain.[13] Normally, where there is an illicit intention, the public information from the zone transfer would be used in conjunction with information gathered from port-scans. Port-scans collect privately held information and facilitate, by their very function, unauthorised access.

Conversely, a zone transfer displays potentially useful information in determining if a company/website is facilitating illegal or unethical activity such as spam operations. Why would an anti-spammer use a zone transfer? Let us use a phone analogy. If an anti-telemarketing crusader kept getting crank calls from an organization and a particular number displays on his/her caller ID, he/she might call up the receptionist and try to get information. If the receptionist

[3] Rash, M. ''Mother, May I'' available at http://www.securityfocus.com/print/columnists/463 (last accessed January 29, 2008).

[4] Original idea expressed by Paul Ohm in the cyberprof list serve.

[5] 'Understanding zones and zone transfer' (available at: http://technet2.microsoft.com/windowsserver/en/library/940cdf9b-8e43-4b08-9a53-9fc2152644031033.mspx?mfr=true visited 23, April 2008).

[6] 'DNS Zone Management, Contacts and Zone Transfers' (available at: http://www.tcpipguide.com/free/t_DNSZoneManagementContactsandZoneTransfers.htm visited 1 May 2008).

[7] Explanation of a DNS Zone Transfer (available at: http://support.microsoft.com/kb/q164017/ visited 23, April 2008).

[8] 'DNS Zone Management, Contacts and Zone Transfers' (available at: http://www.tcpipguide.com/free/t_DNSZoneManagementContactsandZoneTransfers.htm visited 1 May 2008).

[9] 'Wiki: DNS Zone Transfers' (available at: http://wapedia.mobi/en/DNS_zone_transfer visited 22 Sept 2008).

[10] Tom Espiner DNS servers 'vulnerable to attack' *ZDNet.co.uk* Published: 25 Oct 2005 (available at http://news.zdnet.co.uk/security/0,1000000189,39233366,00.htm visited 1 May 2008).

[11] Network Working Group, 'Domain Names – Concepts and Facilities' (available at http://tools.ietf.org/html/rfc1034 visited 22, Sept 2008).

[12] 'Wiki: DNS Zone Transfers' (available at: http://wapedia.mobi/en/DNS_zone_transfer visited 22 Sept 2008).

[13] Interview with James Chan, Technical Services Manager, NetDimensions, April 18, 2008. See also: 'Why is securing DNS zone transfer necessary?' (available at: http://www.sans.org/reading_room/whitepapers/dns/868.php visited 22, April 2008).