DOMAIN NAME HIJACKING: INCIDENTS, THREATS, RISKS, AND REMEDIAL ACTIONS

A Report from the ICANN Security and Stability Advisory Committee (SSAC)

12 July 2005

Table of Contents

Preface and Acknowledgements

This is a report by the Security and Stability Advisory Committee (SSAC) describing domain hijacking. Formed in the wake of the events of September 11, 2001, SSAC is an advisory committee to ICANN (the Internet Corporation for Assigned Names and Numbers). SSAC reports directly to the ICANN Board and advises the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems.

As part of its advisory role, the Committee offers independent advice to the ICANN board, the ICANN staff and the various ICANN supporting organizations, councils and committees as well as to the technical community at large. The Committee has no official authority to regulate, enforce or adjudicate. Those functions belong to others, and the advice offered here should be evaluated on its merits.

The Committee's membership draws from the commercial and not-for-profit sectors, has broad geographic representation and has broad representation across industry and academe (Appendix D), including all segments of the domain name system (DNS) community. The committee includes members who operate root servers, generic and country code top-level domain servers, registrars and address registries. Some members are network security experts or conduct network security research. The Committee members are volunteers, who serve without pay, each a technical contributor in his or her own organization and in the community at large. A recently appointed ICANN Fellow also serves on the Committee and is compensated by ICANN.

Because the Committee is composed of people actively working in the field, conflicts of interest arise from time to time. Committee members are expected to declare conflicts of interest, whether actual, potential or apparent, but Committee members are not required or expected to recuse themselves. In the current activity, several contributors work for registries and registrars. In all cases, the members have made their situations clear and have been careful to provide technical information without attempting to influence others on the Committee. SSAC's policy concerning conflict of interest is posted to the committee's Web site at http://ssac.icann.org. A list of contributors to this report is provided in Appendix B.

This report was written and edited by Dave Piscitello under the direction of Steve Crocker, Chairman, and the Committee, which has complete responsibility for the work, its content and its recommendations.

Executive Summary

This report by the Security and Stability Advisory Committee (SSAC) describes incidents where domain names were "hijacked". Domain hijacking refers to the wrongful taking of control of a domain name from the rightful name holder. The common use of the term encompasses a number of attacks and incidents. Incidents representative of common forms of attacks are discussed and analyzed in the report. The Committee then presents its findings and recommendations.

As the report illustrates, domain hijacking can have a lasting and material impact on a registrant. The registrant may lose an established online identity and be exposed to extortion by name speculators. Domain hijacking can disrupt or severely impact the business and operations of a registrant, including (but not limited to) denial and theft of electronic mail services, unauthorized disclosure of information through phishing web sites and traffic inspection (eavesdropping), and damage to the registrant's reputation and brand through web site defacement. The report further illustrates how incidents often affect more parties than the rightful name holder: customers, business partners, consumers of services provided by the name holder, and even parties wholly unrelated to the name holder are often "collateral damage" to hijacking incidents.

The Committee finds that domain name hijacking incidents are commonly the result of flaws in registration and related processes, failure to comply with the transfer policy, and poor administration of domain names by registrars, resellers, *and* registrants.

Finding (1) Failures by registrars and resellers to adhere to the transfer policy have contributed to hijacking incidents and thefts of domain names.

Finding (2) Registrant identity verification used in a number of registrar business processes is not sufficient to detect and prevent fraud, misrepresentation, and impersonation of registrants.

Finding (3) Consistent use of available mechanisms (Registrar-Lock, EPP authInfo, and notification of a pending transfer issued to a registrant by a losing registrar) can prevent some hijacking incidents.

Finding (4) ICANN Policy on Transfer of Registrations between Registrars specifies that "consent from an individual or entity that has an email address matching the Transfer Contact email address" is an acceptable form of identity. Transfer Contact email addresses are often accessible via the Whois service and have been used to impersonate registrants.

Finding (5) Publishing registrant email addresses and contact information contributes to domain name hijacking and registrant impersonation. Hijacking incidents described in this report illustrate how attackers target a domain by gathering contact information using Whois services and by registering expired domains used by administrative contacts.

Finding (6) Accuracy of registration records and Whois information are critical to the transfer process. The ICANN Whois Data Reminder Policy requires that registrars annually request registrants to update Whois data, but registrars have no obligation to take any action except to notify registrants. Registrants who allow registration records to become stale appear to be more vulnerable to attacks.

Finding (7) ICANN and registries have business relationships with registrars, but no relationship with resellers (service providers). Resellers, however, may operate with the equivalent of a registrar's privileges when registering domain names. Recent hijacking incidents raise concerns with respect to resellers. The current situation suggests that resellers are effectively "invisible" to ICANN and registries and are not distinguishable from registrants. The responsibility of assuring that policies are enforced by resellers (and are held accountable if they are not) is entirely the burden of the registrar.

Finding (8) ICANN requires that registrars maintain records of domain name transactions. It does not appear that all registrars are working closely enough with their resellers to implement this requirement.

Finding (9) The Inter-Registrar Transfer Policy incorporates formal dispute mechanisms. These were not designed to prevent incidents requiring immediate and coordinated technical assistance across registrars. Specifically, there are no provisions to resolve an urgent restoration of domain name registration information and DNS configuration.

Finding (10) Changes to transfer processes introduced with the implementation of the ICANN Inter-Registrar Transfer Policy have not been the cause of any known attacks against domain names. There is no evidence to support reverting to the earlier policy.

On the basis of these findings, the Committee makes the following recommendations:

Recommendation (1): Registries should ensure that Registrar-Lock and EPP authInfo are implemented according to specification. In particular, registries should confirm that registrars comply with the transfer policy and do not use the same EPP authInfo code for all domains they register.

Recommendation (2): Registries and registrars should provide resellers and registrants with Best Common Practices that describe appropriate use and assignment of EPP authInfo codes and risks of misuse when the uniqueness property of this domain name password is not preserved.

Recommendation (3): Under the current transfer policy, a losing registrar notifies a registrant upon receiving a pending transfer notice from the registry at its option. Registrars should investigate whether making this notice a mandatory action would reduce hijacking incidences.

Recommendation (4): Registrars should make contact information for emergency support staff available to other registrars, agents of registrars (resellers), and registry operators. Specifically, registrars should provide an emergency action channel. The purpose of this channel is to provide 24 x 7 access to registrar technical support staff that are authorized to assess an emergency situation, establish the magnitude and immediacy of harm, and take measures to restore registration records and DNS configuration in circumstances which merit such intervention.

Recommendation (5): Registrars should identify evaluation criteria a registrant must provide to obtain immediate intervention and restoration of domain name registration information and DNS configuration. Registrars should define emergency procedures and policy based on these criteria. This policy would complement the Transfer Dispute Resolution Policy (TDRP) and must not undermine or conflict with those policies.

Recommendation (6): ICANN, the registries, and the registrars should conduct a public awareness campaign to identify the criteria and the procedures registrants must follow to request intervention and obtain immediate restoration of a domain name and DNS configuration.

Recommendation (7): Registrars should investigate additional methods to improve accuracy and integrity of registrant records. More frequent or alternate communications might assist registrants in keeping their information up to date. Registrars should also acquire emergency contact information from registrants for technical staff who are authorized and able to assist in responding to an urgent restoration of domain name incident.

Recommendation (8): Registrars should improve registrant awareness of the threats of domain name hijacking and registrant impersonation and fraud, and emphasize the need for registrants to keep registration information accurate. Registrars should also inform registrants of the availability and purpose of the Registrar-Lock, and encourage its use. Registrars should further inform registrants of the purpose of authorization mechanisms (EPP authInfo), and should develop recommended practices for registrants to protect their domains, including routine monitoring of domain name status, and timely and accurate maintenance of contact and authentication information.

Recommendation (9): ICANN should investigate whether stronger and more publicly visible enforcement mechanisms are needed to deal with registrars that fail to comply with the transfer policy, and to hold registrars accountable for the actions of their resellers.

Recommendation (10): ICANN should consider whether to strengthen the identity verification requirements in electronic correspondence to be commensurate with the verification used when the correspondence is by mail or in person.

1 Descriptions of Incidents

Domain hijacking refers to the wrongful taking of control of a domain name from the rightful name holder. The common use of the term encompasses a number of attacks and incidents including

- impersonation of a domain name registrant in correspondence with a domain name registrar,
- forgery of a registrant's account information maintained by a registrar,
- forgery of a transfer authorization communication from a registrant to a registrar,
- impersonation or a fraudulent act that leads to the unauthorized transfer of a domain from a rightful name holder to another party, and
- unauthorized DNS configuration changes that disrupt or damage services operated under a domain name, including web site defacement, mail service disruption, pharming and phishing attacks.

Domain hijacking incidents often affect more parties than the rightful name holder. Customers, business partners, consumers of services provided by the name holder, and even parties wholly unrelated to the name holder are often "collateral damage" to hijacking incidents.

Domain hijackers have a number of motives and objectives, primarily malice and monetary gain. Modification of a registrant's information and unauthorized transfer of a domain registration can cause the registrant to lose its online identity with little recourse, or it may expose the registrant to extortion by name speculators. In several documented cases, domain hijacking caused disruption or malicious use of a registrant's Internet services. By modifying the registrant's DNS information following a successful hijacking, hijackers can have material impact on the business and operations of a registrant, including but not limited to denial and theft of electronic mail services, unauthorized disclosure of information through phishing web sites and traffic inspection (eavesdropping), and damage to the registrant's reputation and brand through web site defacement.

To illustrate the severity of the domain hijacking problem, this report examines some incidents in detail. For each incident, we describe the incident and the immediate impact on the registrant. We describe the steps that were taken to respond to the attack and the vulnerabilities in the registration process that these incidents reveal. To emphasize that these are not isolated incidents, we mention other incidents and their consequences to registrants in table form.

This report does not attempt to single out individual registrars or inter-registrar processes and protocols. It is important to note that while many of the incidents described in this report involve the .com domain, domains have been hijacked in other gTLDs and ccTLDs as well, as noted in section 1.4.

The .com domain contains a very large percentage of widely known and frequently visited names, thus .com hijackings are brought under public scrutiny more often than other TLDs. Historically, .com names have demonstrably higher resale value. Combined, these factors make .com the most attractive target for hijacking among TLDs.

The table in the sidebar illustrates the considerable disparity in perceived value a .com or .net name registration holds over the same name registered in other TLDs. As in any criminal activity, name hijackers will seek the highest value item to steal.

.COM domain names return the highest prices when brokered and resold.

Domain names for sale as of June 16, 2005 illustrates the relative values ascribed to .com, .net, .org, .info, .biz and .tv

Name	Price (in USD)
PlayerMagazine.com	$2.5 Million
PlayerMagazine.net	$300,000
PlayerMagazine.biz	$7
GamingMagazine.com	$3.5 Million
GamingMagazine.net	$400,000
GamingMagazine.biz	$7
GamingMagazine.tv	$7
PokerMachine.com	$300,000
PokerMachine.net	$60,000
PokerMachine.org	$30,000
PokerMachine.tv	$50

Sources: SuperNames, .tv corporation, sedo.com

1.1 The panix.com Incident

On January 14, 2005, Internet service provider Public Access Networks Corporation (PANIX) fell victim to a domain hijacker. The incident attracted global public attention, and is characterized by the following key events:

1. The management of the domain name, panix.com, was transferred from Dotster, Inc. (the “losing registrar”) to Melbourne IT (the “gaining registrar”), by virtue of an unauthenticated request from a Melbourne IT reseller (Fibranet), without the knowledge and consent of the registrant.
2. Melbourne IT, in response to an instruction from Fibranet, changed the name servers associated with the domain name from PANIX’s name servers to Fibranet’s name servers.

1.1.1 The Impact on Public Access Networks Corporation (PANIX)

The change to the name servers associated with the domain name panix.com resulted in the loss of service for the thousands of customers of Public Access Networks Corporation (PANIX), and therefore had a material impact on the business of PANIX. While PANIX endeavored to recover its domain name, subscriber email was forwarded to an IP address other than PANIX’s mail servers, and later delivered to a reseller’s default mail server. Mail eventually bounced or was queued for redelivery when the correct DNS configuration was restored.

PANIX minimized the impact of the attack for its customers by redirecting hosted-domain email. PANIX restored email service to mail recipients on the panix.com domain by implementing a temporary workaround and providing web mail access to subscribers via its panix.net domain.

During the course of the investigation, inflammatory and uncorroborated stories were posted across the web (see Section 1.1.5), claiming that mail sent to PANIX customers was routed to a bogus mail server run by the hijackers. Post incident analysis reveals that Fibranet, having suspected credit card fraud, locked the domain name and all panix.com email was delivered to a default mail server Fibranet maintains. (Like many service providers, Fibranet maintains service infrastructure in several locations around the world. In this case, routes and mail forwarding tables pointed to an email server in the United Kingdom, which was mistakenly reported as “owned” by attackers). PANIX has no evidence to conclude that email processed during the service outage was misused, but advised subscribers that they should consider any sensitive data mailed during this period to be compromised.

PANIX offers many Internet services to subscribers, including web hosting and UNIX command shell. PANIX customers were unable to access these services during the incident. The domain name was parked and locked, and the attacker was unable to modify the DNS configuration any further after the first DNS change had been made. Any additional malicious activities were thus thwarted.

1.1.2 Detection of and Recovery from the Incident

At approximately 1:00 a.m. EST, Saturday 17 January, 2005, PANIX discovered that the DNS configuration on their domain name panix.com was changed and attempted to contact both their sponsoring registrar (Dotster) and the registrar newly identified by the registry’s Whois service (Melbourne IT) to resolve the problem. Neither Dotster nor Melbourne IT had office staff on duty at that time, and no parties were reachable via readily-available contact numbers. Technical staff at PANIX posted messages to public mailing lists (in particular, NANOG) requesting assistance in contacting the registrars. The mobile phone number of a senior Melbourne IT staff member was obtained from the Melbourne IT website, and this staff member was contacted around 5:00 p.m. EST (Saturday evening in New York, Sunday morning in Melbourne).

Time-zone differences and office hours of the parties involved continued to encumber the recovery process. Melbourne IT was finally able to verify the details of the incident when its office opened, and the DNS and registrant information was reverted to the previously known state around 5:30 p.m. EST Sunday. Melbourne IT then asked Dotster to request that the domain name be a transferred back to Dotster through the standard transfer process. Dotster initiated this process around 2:00 a.m. EST on Monday morning, and Melbourne IT manually approved the transfer.

1.1.3 Analysis of the Incident

Analysis of the PANIX incident reveals that procedural errors contributed to the success of the hijacking. Analysis further exposes certain vulnerabilities inherent in the processes currently employed to transfer names.

1.1.3.1 Procedural errors

Under the requirements of the ICANN Inter-Registrar Transfer Policy (http://www.icann.org/transfers, informally, the “transfer policy”), a domain name may not be transferred from a losing registrar to a gaining registrar without the approval of the registrant or administrative contact. The gaining registrar is responsible for obtaining this approval. The gaining registrar is required to (1) obtain explicit authorization for a transfer from the registrant or administrative contact, and (2) authenticate the registrant or administrative contact against the information published by the Whois service of the losing registrar.

In this incident, the gaining registrar did not obtain approval from the registrant. The gaining registrar had delegated responsibility for obtaining approval to a reseller, and that reseller failed to follow the process specified by the registrar; specifically, no authentication request was issued by Fibranet to the email address of the administrative contact at panix.com.

Two available mechanisms, if used, could have prevented this hijacking incident.

The first mechanism is Registrar-Lock. A domain name on Registrar-Lock cannot be modified or transferred until the sponsoring registrar removes the lock[1]. Many registrars have implemented Registrar-Lock as a default setting for all domain names that they sponsor.

The second mechanism is the five-day transfer pending period, during which the losing registrar may take steps to verify the registrant’s intent to transfer. Upon notification of a pending transfer, the losing registrar has five (5) days to cancel the transfer, with cause. The losing registrar has the option of contacting the registrant using a standardized form (http://www.icann.org/transfers/foa-conf-12jul04.htm). In cases where the registrant explicitly denies approval of the transfer, the registrar has the opportunity to explicitly cancel the transfer.

Neither of these optional mechanisms was utilized in the case of the panix.com hijacking.

a) The domain name was not locked.

b) The losing registrar did not notify the registrant upon receiving the pending transfer notice from the registry.

[1] Where RPP is used, Registrar-Lock locks a domain name from transfers and modification. When EPP is used, Registrar-Lock usually refers to a lock on transfers, and modifications to the domain record are permitted.

Certain domain name registries use the IETF Extensible Provisioning Protocol, EPP (e.g., .org, .biz, .info). EPP provides an additional mechanism, the Domain Name Password (EPP authInfo), which might have prevented the hijacking from occurring. EPP authInfo is used by domain name registries to authenticate a registrant requesting a transfer. This password is either generated by a sponsoring registrar or provided by the registrant. A gaining registrar must obtain this password from the registrant before a transfer can be initiated.

At the time of the incident, .com did not use EPP, however VeriSign is deploying EPP in .com and .net and was preparing to do so prior to this attack[2].

1.1.3.2 Circumstances that Delayed the Recovery Process

The recovery process associated with the panix.com hijacking highlights some of the difficulties in dealing with emergency situations, and illustrates how the urgency of resolving a hijacking issue may be commensurate with the amount of harm done. In other words, the time it took to fix the panix.com issue was actually quite fast by some measures, but not fast enough when business and services are disrupted.

In this case, the recovery process was hampered by the timing of the event (possibly intentional). Transfer policies and procedures have never been designed specifically to remedy high-profile hijacking cases **requiring immediate and coordinated technical assistance across registrars.** Although Melbourne IT had 24 x 7 on-call technical and customer support, it had not envisaged a situation where a party other than a customer of Melbourne IT would need access to 24 x 7 support. [Note: Melbourne IT has since provided a public phone number on its contact page that links directly to 24 x 7 staff.]

The current registrar transfer undo procedures did not specifically address situations where:

1) An incident would occur on a weekend.

2) Incident response would require verification and investigation by parties operating in different time zones.

3) Administrative (emergency support staff) rather than office (business) contact numbers for all parties involved in an incident would be required. In general, ICANN holds contact information for office staff for all ICANN accredited registrars; however, this type of contact detail was not suited to assist in recovering from the panix.com incident.

4) Parties involved in incident response needed to share information they customarily keep private. In this incident, the gaining registrar attempted to confer with the losing registrar, the original registrant, the registry operator and the reseller to help authenticate the problem. The gaining registrar also needed to review event logs at both the registrar and its reseller.

[2] Source: VeriSign, 25 June 2005.

None of these circumstances are explicitly planned for in the current Inter-Registrar Transfer Policy, as this policy was developed to ensure a procedure for domain name holders to transfer their names from one ICANN-accredited registrar to another. The policy provides standardized requirements for registrar handling of such transfer requests from domain name holders and includes a mechanism for sharing contact details between registrar and registry staff that has been allocated to solve specific transfer problems. The policy was *not* developed to provide a mechanism for emergency support staff.

The Inter-Registrar Transfer Policy incorporates formal dispute mechanisms (the Transfer Dispute Resolution Policy) intended for handling disputes between registrars associated with a transfer that cannot be solved directly between the two parties. These business-oriented processes are appropriate when the DNS information of a domain name is unaffected, when there is no issue of service denial or interruption, and when there is less immediate urgency to restore service. While the processes may be satisfactory for resolving a transfer-related dispute in a matter of days, another mechanism may be necessary to allow restoration of service in the timely manner real-time communications networks demand.

In the panix.com incident, there was no dispute between registrars and no dispute over who was the legitimate registrant. The two registrars involved fully cooperated to resolve the problem without the use of the processes provided through the Transfer Dispute Resolution Policy. However, an officially available restoration mechanism could have minimized the effect of the hijacking as there was still a period of over 40 hours before the DNS information was corrected. The fact that the incident occurred on a weekend, the staff necessary to resolve the problem was not easily contactable, and no standard recovery procedures were defined for an incident of this kind all contributed to the length of time it took to resolve the incident.

1.1.4 Possible areas for improvement

Processes associated with name transfers must address problems exposed by the PANIX hijacking incident. Possible areas for improvement to reduce or eliminate future, similar incidents include:

1) Registrars should make contact information for emergency support staff available to other registrars, agents of registrars (resellers), and registry operators.

2) Registrars should define a mechanism to resolve an *urgent restoration of domain name registration information and DNS configuration*. For example, a policy and mechanism appear to be required to accommodate incidents where

   a) A transfer involving a change of delegation information is made in error or as a result of fraud or malice, and

   b) The registrant notifies the registry and registrars that the transfer is both unauthorized and has resulted in a service interruption.

   In such cases, the registry and both registrars must be able to identify and authenticate the registrant before they can investigate and validate any claim of fraud or malice. The registration information could be reverted to the previous state and then the domain name locked at the registry with registrar authorization while the issue is examined in detail. Such a mechanism would require a determination of what qualifies as urgent, how to determine whether the allegation of fraud is valid, and who is authorized to make this determination.

3) Registrars should improve registrant awareness of the availability and purpose of the Registrar-Lock. This feature is not uniformly appreciated nor understood, and the default setting of this status code varies depending on the registrar. Measures to consider include better online documentation, published articles, and other promotional material; a uniform default setting (or a clearly defined opt-in/opt-out process provided during registration); and a secure, intuitive and obvious method of modifying the lock setting. These initiatives may reduce hijacking incidents without causing confusion, delay, or acrimony when registrants attempt to transfer.

4) Currently, a losing registrar notifies a registrant upon receiving a pending transfer notice from the registry at its option. It is preferable for the losing registrar to use a contact point separate from the email address used by the gaining registrar to authenticate the transfer request, to minimize the risk resulting from one email address being compromised. Registrars should investigate whether making this notice a mandatory action would reduce hijacking incidences. If the objective of the transfer policy is to assure that registrars provide registrants with choice, *notification* and consent, ICANN and registrars should try to determine whether registrants would generally favor mandatory notice.

5) Registrars should consider improvements in the authentication and authorization mechanisms in protocols used for name transfers. Registries should be able to rely on system commands received from registrars without independently obtaining verification that those commands have been appropriately transmitted. In addition, registrars should implement EPP authInfo according to the transfer policy, which requires that Registrar-generated EPP authInfo codes be unique on a per-domain basis.

When a registrant claims a transfer was improper, the registrar must verify that the transfer or registration change action was in fact unauthorized. Verification requires a thorough analysis (audit) of the incident, and complete and accurate information from all involved parties. Incomplete information often frustrates investigators. Involved parties may have limited or no obligations to cooperate, produce information, or join in the investigation. Conflicting, unreliable, and uncorroborated information further complicate the process. There are also many circumstances in which a good faith dispute exists between the prior and the current domain name holders as to whether the new holder held the necessary authority to initiate a transfer. Resolving such questions can require legal rather than technical staff participation.

One means of dealing with the hijacking question would be to assign the financial and legal risks associated with fraudulent hijacking to the party most able to control the risk: the registrar closest to the wrongdoer. Holding registrars accountable in this manner would create incentives for registrar to take whatever steps are necessary to prevent the occurrence of fraudulent hijackings

1.1.5 News items and articles publicizing the incident

The following articles are representative of the coverage the PANIX domain hijack received. Some of the articles filed during the incident proved inaccurate.

ISP suffers apparent domain hijacking
http://news.zdnet.com/2100-9588_22-5538227.html

PANIX – Hijack FAQ
http://www.panix.net/hijack-faq.html

New York's Oldest ISP gets Domain-jacked
http://it.slashdot.org/it/05/01/16/0027213.shtml?tid=95&tid=172&tid=17

Australian Firm Takes Blame for U.S. Domain Name Hijack
http://www.pcworld.com/news/article/0,aid,119337,00.asp

ICANN review blames Melbourne IT for hijack
http://smh.com.au/news/Breaking/ICANN-review-blames-Melb-IT-for-hijack/2005/03/15/1110649182358.html?oneclick=true

PANIX recovers from hijack attack
http://seclists.org/lists/isn/2005/Jan/0053.html

The aftermath of a domain hijack attack
http://www.theregister.co.uk/2005/01/20/panix_recovery_continues/

1.2 The hushmail.com Incident

Another means by which the wrongful taking control of a domain name from the rightful name holder can occur does not involve an actual transfer of the name to another registrar. The following example illustrates this form of hijacking.

On Sunday, 24 April 2005, the DNS configuration for Hush Communication's Hush*mail* service was modified by an unauthorized party. The incident is characterized by the following key events:

1. An attacker convinced 1st-tier support staff at Network Solutions, Inc. to modify the administrative email contact information in Hush's registration record.
2. The attacker used the administrative contact email to submit a password reset request for the Hush Communications account to Network Solutions, Inc.
3. The attacker accessed the Hush Communications account, changed the password, and used the account to alter the DNS configuration; specifically, the attacker pointed the domain name A record to the attacker's server.
4. The attacker(s) posted a defaced home page expressly designed to embarrass Hush Communications and gain notoriety for the attacker.

This incident helps illustrate that some attacks against registrars and registrants are labeled "hijacks" but do not involve a domain name transfer in the formal sense of the word. Hushmail.com was never transferred from the rightful name holder or to a different registrar.

1.2.1 The Impact on Hush Communications

The change in the DNS configuration of the hushmail.com domain name allowed an attacker to successfully execute a web defacement attack. Hush Communications is a provider of secure email, secure web development and secure desktop services and software. The attack put Hush Communications' credibility as a security services provider into question and had a material impact on the company's reputation and brand. According to Hush Communications' CTO, Brian Smith, the negative publicity persists: months later, references to the attack still appear among the top responses at the Google and Yahoo! search engines.

During the recovery period, some Hush customers experienced an interruption of email delivery.

No unauthorized access to any of its servers was discovered, and no data managed by Hush were compromised. If the attacker had also succeeded in the modifying other contact information (for instance, the registrant and billing information), then Hush technical staff would have been unable to restore the registration and DNS information.

1.2.2 Detection of and Recovery from the Incident

Hush Communications staff discovered that its DNS configuration had been altered at approximately 10 p.m. PDT, Sunday, 24 April 2005 from a posting at the Zone-H.org web site. Users attempted to notify Hush's support via email but since the DNS configuration had been changed, this email was not delivered. An unauthorized party, identifying himself as Matt Jones, convinced 1st-level support personnel at Network Solutions to change the administrative contact email in Hush's registration record to his email account hosted at Yahoo! Network Solutions' personnel made the change. No attempt was made to reach any authorized contacts at Hush Communications using alternative contact information, e.g. telephone.

The attacker requested a password reset for the registration account, which was delivered to the attacker's email address (hushmail@ge3k.net or hushmail@jeet3k.net). The attacker reset the registration account password and again modified the administrative contact information. The attacker next modified the DNS record for www.hushmail.com to point to a web server where a defaced Hushmail.com home page was hosted. Parties visiting the defaced page saw a Hush*mail* logo, a hoax icon and a message stating, "The Secret Service is watching.-Agent Leth and Clown Jeet 3k Inc".

The defaced web site was in place less than 6 hours. The ISP that hosted the hoax page shut it down. The chronology of events that prompted the ISP to shut the page down is still under investigation by the Royal Canadian Mounted Police.

The attacker modified the administrative contact information and DNS configuration, but left the billing contact information intact. CTO Brian Smith at Hush Communications used the billing contact information to access Hush's account, reset the account password, restore the administrative contact information and restore the correct DNS configuration. Correct name resolution was available to most customers within 16 hours, but some customers continued to experience access problems for the next 72 hours while the incorrect configuration information was gradually purged from the global name service.

The hijacking occurred during a period of days when Network Solutions, Inc., was contending with denial of service (DOS) attacks directed against its name servers. Whether the DOS attack was related to the domain hijacking and intended to lend credibility to the social engineering attack on Network Solutions' support personnel is still under investigation. Network Solutions' staff were aware of the name server problems and the timing of the events, whether coincidental or intentional, aided the hijacker in his social engineering effort.

1.2.3 Analysis of the Incident

Analysis of the Hush*mail* incident reveals that vulnerabilities with the registrar's customer service security measures contributed to the success of the attack.

1.2.3.1 Customer-service security measures

In this incident, an attacker was able to socially engineer a 1st-tier customer support agent who was relatively new to the company to make a change to an administrative contact email account. The fraudster was extremely familiar with Network Solutions' customer service procedures and terminology. The attack did expose a flaw in customer support procedures that facilitated the attack: the registrant contact change procedure did not require a supervisor or registrant confirmation, and access restrictions were not in place to prevent 1st-tier support personnel from effecting a change. Network Solutions has since revised its customer support procedures. The fraudster has tried repeatedly to hijack other domain names using the same tactic, to no avail. NSI continues to work closely with law enforcement to prosecute the fraudster.

The administrative contact email account may also be used to perform a password reset on the domain registration account, which enhances its value to an attacker, and thus deserves additional consideration and stronger protection.

1.2.3.2 Circumstances That Hampered Recovery Process

The delay in resolving the Hush incident again highlighted some of the difficulties in dealing with an emergency that occurred over a weekend. Some Hushmail subscribers attempted to contact Hush's customer support by email, however, the incident occurred outside customary support hours (Monday to Friday, 9AM to 5PM Pacific Time, excluding statutory holidays). In addition, support email from users experiencing the DNS issue would not have been delivered because the DNS configuration had been altered. This highlights issues registrants must consider when specifying transfer contact email addresses.

1.2.4 Possible areas for improvement

Customer-service security policies must address problems exposed by the Hush*mail* incident. Possible areas for improvement to reduce or eliminate future, similar incidents include:

1. A registrar should identify situations where customer support should obtain supervisor approval before it satisfies a request to change a registration record. For such situations, the registrar should identify customer escalation procedures to verify the change request is authentic and authorized.
2. If a registrant's contact email address is also used as the registrant's user account, *and* the registrar offers user account self-administration (password reset or recovery), then registrars should consider stronger measures to safeguard these addresses against modification. For example, a registrar can
    a. Enforce a policy that requires a second form of authorization when a request is made to change a contact email address that can be used to perform a password reset.
    b. Keep a registrant's contact email address private (e.g., not accessible via the Whois service to unauthorized parties) if it can be used to perform a password reset on registration accounts.
    c. Require registrants to create user account names (identities) that are distinct from any contact email addresses that will be recorded in the registrant's Whois registration record (and thus have two distinct data object classes: user identity and authenticating email address).
    d. Notify more than one or all contacts (registrant, administrative, billing, and technical) when any registration information or the DNS configuration is modified for the domain name, and maintain an audit trail of contact requests and responses.
3. Registrants should provide at least one 24 x 7 emergency contact number (especially in situations where 2(a) is implemented).
4. Registrants should lock their domain names using the Registrar-Lock mechanism.
5. Registrants, especially those who are in service businesses, should consider using a second email address on a different domain for emergency purposes. Registrants should consider obtaining this emergency address from a domain that is unlikely to be tampered with, e.g., a very secure and stable service provider.

1.2.5 Sources

Hushmail.com defaced by means of DNS redirection
http://www.zone-h.org/en/news/read/id=4467/

Hushmail hit by DNS Attack
http://www.theregister.co.uk/2005/04/25/hushmail_dns_attack/

Hushmail attacked by DNS hackers
http://www.scmagazine.com/news/index.cfm?fuseaction=newsDetails&newsUID=86e229e0-2c39-44c2-8bbe-19ff34670953&newsType=New%20s

Hushmail DNS Incident
http://www.hushmail.com/login-news_dns

Mirror site of the defaced Hush*mail* home page
http://www.zone-h.org/defacements/mirror/id=2309823/

Hushmail DNS Attack Blamed on Network Solutions
http://www.eweek.com/article2/0,1759,1791152,00.asp

1.3 The HZ.com Incident

HZ.com is a wireless information portal. Operating since mid-1997, it is one of the first portals of its kind. Visitors can access information services hosted from HZ.com from any email-capable portable device (Glenayre, RIM, or Motorola pagers, and email-capable cellular phones). Information hosted at HZ.com is accessed by approximately 25,000 users.

Founder Geoff Mulligan registered this two-letter domain name in 1996. On 15 February 2005 during a casual Whois query, Mr. Mulligan discovered that the registration information for HZ.com had been modified without his knowledge or consent. The domain name had been transferred from his sponsoring registrar, AITdomains.com, to a reseller of Direct Information PVT, Limited, QNIC.com (PH Media Corporation). Mr. Mulligan's contact information had been removed and replaced with contact addresses at xyberotica.com.

Mr. Mulligan contacted AITdomains.com to notify them of the unauthorized transfer. AITdomains.com insisted that he provide proof that he was the rightful registrant. Mr. Mulligan submitted a copy of an earlier Whois registration record but AITdomains.com insisted he provide evidence that he was the name holder of record at the time of the transfer (according to their transaction records, 7 January 2005). Mr. Mulligan protested that the registrar's own audit trail of the transfer should prove his ownership, to no avail. Whois records obtained from www.whois.sc confirm that Mr. Mulligan was the name holder on 31 December 2004 (see Appendix C).

While pursuing the matter further, Mr. Mulligan was informed by both the gaining and losing registrars that they had received email correspondence from the administrative contact email address on record, authorizing the transfer request. In particular, the losing registrar, AITDomains.com, had on record an email purportedly sent from the registrant email address approving the Form of Authority (FOA) for the transfer. Mr. Mulligan did not send these email messages and investigated further. Mr. Mulligan analyzed his transaction and access logs and did not see any evidence that his mail servers had been compromised in order to send the FOA authorization. While no conclusive evidence has yet been gathered, the parties involved speculate that *some* mail server had been compromised, and the attacker had intercepted and spoofed email correspondence to hijack this and possibly 80 other domain names registered with xybererotica.com contact information. Since 80 or more domains had been transferred to the same suspected hijacker, it is likely that some intermediate mail server was compromised and used to send the transfer emails, or that spoofed emails were sent to the losing registrar directly rather than to individual mail servers at each registrant.

Mr. Mulligan asked a colleague, Ram Mohan of Afilias Ltd. for assistance. Mr. Mohan contacted the CEO of Directi Information (DBA directi.com), the gaining registrar, who was receptive to Mr. Mulligan's request to restore the domain. The history of HZ.com name holders at www.whois.sc is reproduced in Appendix C of this report to demonstrate that there was indeed enough suspicious information in the registration to justify Direct Information's decision to restore the name to Mr. Mulligan. These records also illustrate how valuable historical registration records are to parties investigating a name transfer dispute.

The CEO authorized Directi.com to return the domain name. Directi staff had earlier asked that Mr. Mulligan obtain consent from AITdomains, but AITdomains was bound by policy not to release the domain to him because he was not the registrant on record.

Ultimately, Directi.com returned HZ.com to AITdomains upon receiving sufficient notarized documents from Mr. Mulligan to satisfy its own proof of prior holder criteria. Directi also noticed a pattern of about 80 additional (presumably hijacked) domain names transferred to its sponsorship with the same registrant information (xybererotica). This evidence helped Directi make the decision to transfer the name back to Mr. Mulligan.

1.3.1 The Impact on HZ.com

While HZ.com experienced no intrusions nor service interruption during the time the domain was stolen, the rightful holder had lost control of his domain name and was essentially prevented from pursuing any business relationships (partnerships, growth and investment opportunities) in which the established identity of the service was considered a business asset.

The rightful name holder was also uncertain whether he had lost an asset with considerable speculative value. Two letter domains in .com are highly valued, especially those which have a history of repeat visitor traffic and numerous referrer links. These metrics are valued by domain name speculators. In the case of HZ.com, the name is also valuable because it is a familiar technology acronym (HertZ, the measure of electromagnetic wave frequency in cycles per second, is commonly recognized as a measure of speed of CPUs) and thus carries considerable cachet and vanity value.

1.3.2 Detection of and Recovery from the Incident

The registrant detected the name hijacking through an impromptu (non-routine) examination of the Whois registration record. Recovery was hampered by several auditing-related issues:

1. The audit records maintained by the losing registrar could not identify Geoff Mulligan, the legitimate registrant, as the name holder of record of HZ.com. Registrars are required to maintain full history of transactions, but it is possible that the correct registrant information was not collected in the first place. It is common for registrants to delegate the registration of a domain name to a third party (e.g., reseller or service provider), without ensuring that the registration includes the details of the registrant and is maintained over time.
2. The standard Whois service and registration records available to registrants do not provide any history of name holders. Geoff Mulligan could prove he was the name holder of record at one time, but could not demonstrate he was the name holder on the day the transfer request was submitted.

3. Transfer requests were submitted using email addresses of authorized contacts. In this case, the gaining registrar relied on an electronic process to obtain authorization. The transfer policy accepts consent from an individual or entity that has an email address matching the Transfer Contact email address as sole and sufficient proof of identity.
4. The name holder of record did not receive a pending transfer notification for the domain name from the losing registrar.

This incident calls attention to a conundrum involving registrant information and the Whois service; specifically, what registration information should be publicly available via the Whois service (and hence available for misuse) and what should be kept private? It may be useful to investigate methods where (and impose best common practices on registrars so that) a registrant can provide public contact information for use by the Whois service and private contact information for use in registration and transfer correspondence.

1.3.3 Analysis of the Incident

In this incident, no changes had been made to the DNS configuration, and HZ.com's services had not been affected. The theft could have gone undetected for considerably longer. It appears that the motive of this hijacking wasn't to immediately disrupt the domain holder's operation, but to acquire and resell a desirable two-letter domain name. The ultimate effect, however, would have led to grievous harm to the name holder.

In this incident, AITdomains' inability to present documentation associated with the transfer hampered restoration of the domain name to the rightful holder. Each registrar is responsible for keeping copies of documentation, including the FOA and the Transfer Contacts response because these may be required for filing and supporting a dispute under the dispute resolution policy.

1.3.4 Possible areas for improvement

Registrar auditing policies should address problems exposed by the HZ.com incident. Possible areas for improvement to reduce or eliminate future, similar incidents include:

1. Registrars should make certain resellers maintain sufficient auditing information to provide a complete chronology of name holders. This information allows registrars to conduct the equivalent of a land title search on domain names and thus facilitate and possibly expedite dispute resolutions (Note that Registrar Accreditation Agreement §3.4, Retention of Registered Name Holder and Registration Data, requires that records of all transactions be kept, see http://www.icann.org/registrars/ra-agreement-17may01.htm).
2. Registrars should augment registration records to include dates of acquisition and a history of name holders.
3. Registrars should consider whether making pending transfer notifications to registrants mandatory by losing registrars will reduce hijacking incidents like this one, and improve the process so that it is not entirely dependent on email communication (see section 6) . In the HZ.com case, the Whois records used by

the gaining registrar to validate the transfer request would have proven useful in reaching a speedier resolution. Registrars should consider sending pending transfer notifications to an additional contact point from that used by the gaining registrar for authentication.

1.3.5 Sources

The information used to document the HZ.com attack was obtained from personal correspondence between Ram Mohan, Afilias Limited, a facilitating party; Geoff Mulligan, the registrant; various parties at the gaining and losing registrars (Directi and AITdomains, respectively); and the reseller (QNIC). The email threads contained sufficient forwarded items from the reseller and sponsoring/losing registrars to corroborate the incident as related here. Many of the exchanges contained personal comments. By request and to respect all the parties' expectations of privacy, we do not provide copies or sources here.

1.4 Other Noteworthy incidents

The following table calls attention to some of the noteworthy domain hijackings. In the table, we identify the domain name, incident, nature of attack (exploit), and outcome.

Domain Name	Exploit	Outcome
Sex.com	Fax fraud used to transfer domain	Domain recovered 7 years after transfer[3]
ClubVibes.com		Recovered[4]
Commercials.com	Note 1	Recovered after attempts to resell
iFly.com	Note 1	Resold (not recovered)
Hackers.com		Resold (not recovered). Registrant suffered loss of brand.
Wifi.com		Resold (not recovered)[5]. Registrant suffered loss of brand.
Nike.com	Spoofed email used to transfer domain	Service interruption at nike.com, denial of service to innocent 3rd party (FirstNet Online) (recovered)[6]
Babayiz.biz	Unauthorized party hacked into account and blocked registrant from accessing it.	Under investigation – registrar has insufficient (audit) information to help registrant corroborate claim (see HZ.com)

[3] See http://www.gigalaw.com/articles/2003-all/hollander-2003-02-all.html

[4] From email correspondence with registrant

[5] From email correspondence with registrant

[6] See http://www.whoisfinder.com/news/200007/nike-hijacked-blames-nsi.html

Domain Name	Exploit	Outcome
2e.com	Note 1	Registrant recovered name after filing a complaint with the WIPO Arbitration and Mediation Center following lengthy arbitration process.[7]
Slsk.org	SoulSeek lost domain to unknown party. Spyware advocates lists claim new holder hosts trojan dialer program at this location.	Name not recovered. Rightful holder struggling to restore brand after site was suspected of harboring spyware downloads[8].
Ebay.de	Note 2	Domain was restored to rightful holder in approximately 40 hours [9].

Notes

1) In these three incidents, the attack methodology was the same, and is best illustrated using a concrete example, commercials.com. In this instance, the attacker found a target domain he wanted to steal where the administrative contact's email address was *not* assigned from the target domain. In this case, the administrative contact for commercials.com was rent@blinktv.net. The attacker monitored the registration status of blinktv.net. When blinktv.net expired, the attacker legally registered the domain name. The attacker had the registrar configure the DNS information for blinktv.net to point to his own servers, and all email messages addressed to "any user" @blinktv.net were delivered to his email address. The attacker requested a password reset from the registrar, which was delivered to the administrative contact email, now under control of the attacker. The attacker was able to access the registrant's account and submit a Transfer of Registrar request to move commercials.com to a new registrar.

2) A teenager claims to have visited several Web sites that described how to transfer a domain name and "on a lark", attempted to transfer several sites including Google.de, Web.de, Amazon.de and eBay.de. Only the eBay.de transfer succeeded. An automated request went to Frankfurt Internet registry, DENIC eG, which sent an automated alert to Tucows, a Canadian firm responsible for the genuine eBay site. No reply was returned, and the domain name was transferred.

[7] See http://arbiter.wipo.int/domains/decisions/html/2003/d2003-0184.html

[8] See http://www.spywareinfo.com/newsletter/archives/1003/14.php#soulseek, http://www.spywareinfo.com/articles/p2p/

[9] See http://www.internet-security.ca/internet-security-news-007/teenager-hijacks-ebay-domain.html, http://www.news24.com/News24/Technology/News/0,,2-13-1443_1583919,00.html

2 Risks and Threats Associated with Domain Hijacking

Domain hijackings pose numerous and serious threats to registrants, registrars, resellers registries, and ultimately, the end user.

To the registrant, a domain name serves simultaneously as its business location (presence) and the virtual world corollary to a business name. Whether legally accurate or not, registrants believe that "doing business online" establishes legal ownership of a domain name. From a hijacker's perspective, it only matters that the registrant ascribes value to the domain name, often in excess of any amount recoverable through legal means. At the most modest level, this is similar to the "sentimental value" of inherited jewelry to a family member. The extreme opposite exists when consumers associate brand with a domain name. Many organizations are well-known by their domain name; e.g., Amazon Corporation is popularly known as amazon.com. Many organizations go to considerable effort to protect trademark infringement and brand tarnish by registering corporate identities in across all TLDs (e.g., Dupont Corporation, Microsoft Corporation, etc.)

Because a domain name can be contextually overloaded they are valued by registrants. Once value is ascribed to a domain name, and irrespective of how it is measured or accepted in courts of law, domain names become targets for a range of exploits and criminal activities:

Theft for resale – popular registered domains are valued for their "drawing power" by individuals and organizations other than registrants. A domain name that attracted tens of thousands of hits per day is extremely attractive for online marketing of a variety of products and services, from legitimate to sordid. Operating as sex.com made millions of dollars for both the original holder Gary Kremen and hijacker Stephen Cohen, and would do so for any party that successfully registered the name and operated a similar business. Several domains of perceived value – notably, iFly.com, hackers.com and WiFi.com – were hijacked, put up for sale, and resold before any action could be taken by the registrant.

Theft for extortion – successful online concerns will pay to protect their brand. Owners of domains names will pay hijackers for the restoration of their registrant status. There is increasing evidence that both street and organized crime are involved in identity theft. If domain hijacking for extortion (or resale) becomes as lucrative a criminal activity as identity theft, fraudulent transfer requests will increase significantly.

Tarnish of brand – domain names have been used by attackers to embarrass the registrant. The web defacement of hushmail.com and the panix.com incidents put the competencies of both service providers under public scrutiny.

Fraud, Identity Theft, Monetary Theft – domain name hijackers can substitute their own authentication portals for those of a financial institution, corporate extranet or e-merchant web site and use these to collect user accounts and passwords. With stolen account information, hijackers can withdraw and transfer funds, steal identities, make online purchases.

Personal, Commercial and Political Espionage - By modifying a DNS configuration, an attacker can redirect email, IP telephony and instant messenger conversations for an entire domain so that these services pass through his own system. In *passive monitoring man in the middle* (MITM) attack scenarios, the attacker can "eavesdrop" to collect messages for offline analysis for an extended period of time without detection. In active intrusion MITM attack scenarios, the intruder can alter sender identification, impersonate senders, and alter messages and conversations.

Business Interruption (Unauthorized Loss of Domain) – a registrant's online presence is interrupted when domain names are hijacked and DNS configurations are changed. For e-merchants, the material impact can be measured in lost transactions per minute multiplied by average revenue per transaction. The losses accrued in hijacking incidents are similar to those that would accrue from a distributed denial of service attack (DDOS), or a fire or natural disaster at a brick-and-mortar shopping center. The impact to financial services and stock markets would be even more severe. Business interruption isn't only a worry for Fortune 1000 companies. Small and medium businesses can ill afford to have online businesses interrupted as well.

Collateral Damage – domain name hijacking involving service providers often has a domino effect. In the Nike incident, traffic was redirected from Nike's web servers to a web hosting company, FirstNet Online. The web hosting company was unprepared to handle the volume of traffic typically processed by Nike's server farm. FirstNet Online's facilities were overwhelmed, and the impact to its customers' web servers was the same as a denial of service attack. In the PANIX and Hush*mail* incidents, subscribers experienced partial or complete service interruptions.

Loss through Litigation – following the Nike incident, FirstNet Online sued Nike for failing to secure its domain name, and attempted to hold Nike liable for unintended usage of its facilities. Irrespective of whether suits prove to have merit or are judged to be frivolous, legal actions prove costly and expose organizations to unsought and potentially damaging publicity.

Loss of customer/confidence, customer attrition – this threat is a related outcome of any security incident where an organization's competencies are called into question. Whether a financial institution is directly responsible for a theft of account information following a domain hijacking, or whether an ISP is directly responsible for service interruption is often moot or irrelevant. Only the fact that a registrant was associated with the incident matters. Customers lose confidence and take their business to a competitor.

To the Registries, Registrars and Resellers, domain names are commodities they administer on behalf of registrants. To the extent the services of registries, registrars, and resellers are used by wrongdoers to carry out domain hijackings and related attacks, the goodwill and reputation of these entities can be damaged.

Tarnish of brand – when domains are hijacked or contested, the credibility and possibly the character of losing and gaining registrars can be called into question. If a hijacking is demonstrated to have been the result of improper or erroneous actions performed by a registrar's staff, the competency of the registrar may also be questioned.

Loss through litigation – an organization can suffer material damage from a domain name incident. If the damage can be directly attributed to a registrar's failure to meet a contractual obligation, the organization can bring suit against a registrar.

Loss of reseller business – if a reseller's actions were to prove sufficiently egregious, a registrar could cease doing business through that reseller.

Loss of accreditation and business operations – registries and registrars face compliance or legal action from ICANN if they violate their ICANN agreements, see (http://www.icann.org/correspondence/touton-letter-to-beckwith-03sep02.htm or http://www.icann.org/correspondence/twomey-to-lewis-03oct03.htm).

Loss of customer confidence, customer attrition – this threat is often a related outcome of a domain hijacking where the registrar's competencies or character are called into question.

To the end user, a domain name is a location on the Internet that offers information, commerce, and other services. Hijacked domains pose potentially serious risks to users. They can be used to deny or hijack web, mail and other Internet services; host phishing, identity theft, and other scam sites; and disseminate false or politically volatile information.

Many of these threats and consequences relate to contracts, associations, and relationships between name registration parties.

- ICANN has relationships with registries, governed by the ICANN-Registry Agreements (for example, http://www.icann.org/tlds/agreements/biz/registry-agmt-appf-11may01.htm), which includes the ability to operate a shared registration system and top level domain (TLD) name servers.
- ICANN has relationships with registrars, governed by the ICANN Registrar Accreditation Agreement (http://www.icann.org/registrars/agreements.html), which include the ability to insert and renew registration of second-level domains of the DNS in the registry.
- Registries have relationships with registrars, governed by Registry-Registrar agreements (http://www.icann.org/registrars/agreements.html). These agreements allow multiple registrars to provide Internet domain name registration services and operate SLD name servers within a top level domain.
- Registrants have relationships with registrars governed by registration agreements.

Registries and registrars are bound by their agreements with ICANN and by consensus policies developed through ICANN's Generic Names Supporting Organization (GNSO).

- Registrars have relationships with registrants, governed by a Registrar Authorization Agreement (also known as a Registrant or Registration Agreement). Under these relationships, a party ("the registrant") applies for use of a domain name. These agreements may permit registrants to apply for use of a domain name on behalf of a third party for which the registrant acts as agent (e.g., a reseller or service provider).

ICANN has no agreements with resellers, service providers, and registrants. Registries have no agreements with registrants, resellers, or service providers. It is equally important to note that no formal requirements are imposed on registrars regarding the types of agreements they enter into with resellers and service providers.

These relationships are illustrated in Figure 2-1:

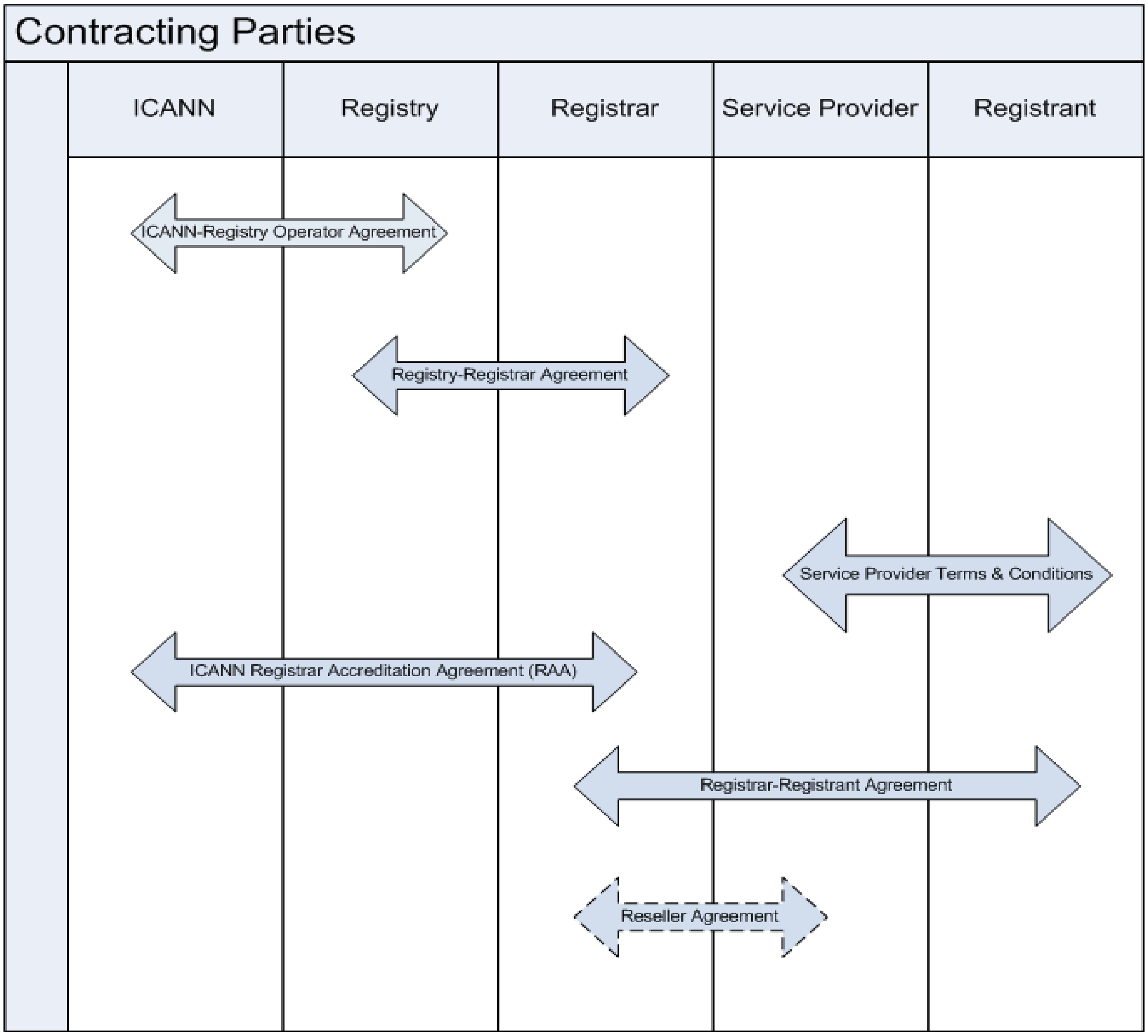
Contracting Parties
ICANN
Registry
Registrar
Service Provider
Registrant
ICANN-Registry Operator Agreement
Registry-Registrar Agreement
Service Provider Terms & Conditions
ICANN Registrar Accreditation Agreement (RAA)
Registrar-Registrant Agreement
Reseller Agreement

Figure 2-1: Registration Contracting Parties

3 Vulnerabilities Observed from Domain Hijackings

This section considers vulnerabilities in the current registrar processes that either resulted in, or present opportunities for, domain hijacking or security incidents involving domain names.

3.1 Potential for Registrant Fraud

Many domain hijackings are intentional acts involving fraud and impersonation of a domain name holder. A common attack methodology involves the substitution of a hijacker's contact information for the administrative contact information in the Whois database of the losing registrar. The gaining registrar authenticates the request from the losing registrar's Whois entry. Authentication succeeds and unless the registrant has locked the domain name or explicitly cancels the transfer, transfer authorization will succeed as well.

Hijackers perpetrate registrant fraud using several methods:

1. **Impersonation using forged credentials**. Hijackers use forged faxed requests or forged postal mail requests to modify registrant information. In certain cases, official company letterhead is stolen or copied, modified or duplicated to abet the fraud.

2. **Social engineering**. A hijacker calls a registrar or reseller support staff, and convinces support personnel to alter the registrar database record. Several incidents suggest that hijackers may create diversionary attacks or exploit operational difficulties a registrar may experience to reduce the registrar's resistance to social engineering attacks (e.g., the DOS against Network Solutions' DNS servers).

3. **Hijacking the authorized email address of an administrative contact**. Hijackers employ several methods to fake or spoof email correspondence. In one form of attack, hijackers track administrative contact email addresses, and search for an administrative contact email address that is assigned from a soon-to-be expired domain. The hijacker registers the expired domain, and then modifies the DNS configuration so that he receives all email for the domain, including that of the administrative contact of the targeted domain name. The hijacker can now impersonate the administrative contact and request a password reset on the registrant's account. The attacker intercepts the reset confirmation email, takes control of the registrant's account, and authorizes a name transfer request.

   In a second form of attack, the would-be hijacker captures Internet traffic using LAN analysis tools and searches for email user accounts and passwords. Email protocols commonly use passwords for user authentication. When these protocols are transmitted over unencrypted links (the common practice today), user identities and passwords can be captured. Attackers compare captured account information against Whois records to identify administrative contacts of exploitable domain names. Motivated and sophisticated attackers may also try to gain administrative control of email servers that are likely to relay email correspondence of domain names they want to hijack and search email messages stored on those servers for user accounts and passwords.

It is important to note that hijackers scrutinize all observable registration processes and actively monitor public information via the Whois service in preparation for an attack. This surveillance is a practice common to many forms of Internet attacks. Through observation and monitoring, attackers hope to identify a vulnerability in the registration process or registrant behavior they can exploit.

3.2 Vulnerable Aspects of Registrar Processes

Incidents mentioned in this report and documented elsewhere call attention to exploitable aspects of procedures currently implemented by registrars and resellers. This list identifies procedures that may have contributed to one or more incidents, and the scope of any vulnerability identified here may be limited to one or a few resellers and registrants. The list is reported here to help identify areas in workflows across registries, registrars and resellers that might be modified to improve the security, stability and integrity of the registration process.

1. A formal registrant authentication process is circumvented through social engineering.
2. A forged document (e.g., a fax using the name holder's company letterhead) is accepted physical proof of identity.
3. Authentication credentials are disclosed to unauthorized 3rd parties by 1st-tier support staff, or reset in a manner that abets a hijacking, and no checks-and-balances safeguard against misuse of a 1st-tier support staff's ability to access and modify registrant credentials
4. Gaining registrars use one (and often only one) form of contact, an email to administrative contact, to transmit the standard Form of Authorization (FOA) used to notify registrant of a transfer-in request.
5. Registrars fail to make the availability and purpose of domain locking mechanisms known to registrants.
6. The default setting of domain locks is not uniform across registrars.
7. A registrar or reseller fails to follow authorization processes according to the transfer policy.
8. A registrar, reseller or registrant fails to maintain accurate registrant information.
9. Registrars do not have mechanisms to handle urgent restoration of a domain name.
10. Registrars do not have sufficient contact information to assist in handling an urgent restoration of a domain name.
11. Registrars and resellers do not maintain a history of registration information.

12. Registrars do not publish best practices or set standards for auditing resellers.
13. A losing registrar is not required to notify the registrant upon receiving a pending transfer notice from the registry.
14. Registrars, registrants and resellers do not maintain alternate contact information (e.g., a contact email address for the registrant that is assigned from a domain other than the registrant's domain) for urgent communications to safeguard against circumstances where email service might not be operational in emergency situations

4 Recovery Mechanisms

This section considers the current domain name dispute resolution and recovery mechanisms, and examines how these mechanisms meet security and stability requirements for general business and contractual disputes over payment, legal disputes over ownership and use, and operational matters including an urgent recovery of a domain name.

4.1 Dispute Resolution Policies

The UDRP is available for cases of abusive registrations or cybersquatting, particularly with regard to trademarked names. A UDRP involves a cost of approximately USD $2,000, and takes at least two months to reach a decision.

The Transfer Dispute Resolution Policy (TDRP) is available to registrars to address disputes involving a transfer that has occurred. A TDRP dispute can be brought to the registry for a decision or to a third-party dispute resolution service provider.

Both dispute resolution policies are designed to provide an impartial assessment of the factual circumstances of a case in order to determine the appropriate outcome of a dispute. However, neither of these provides an immediate fix to cases of interrupted service or suspected hijacking.

4.2 Incident Response: Urgent Restoration of a Domain

Although registrars have worked together and agreed on a solution in several specific hijacking or fraud incidents, registrars may need a new communications channel and corresponding procedures to respond quickly to an operational loss of use of a domain name resulting from a transfer or DNS configuration error or hijacking. Possible elements of an urgent restoration of domain name registration information and DNS configuration include:

An **emergency action channel** – to provide 24 x 7 access to registrar technical support staff who are authorized to assess the situation, establish the magnitude and immediacy of harm, and take measures to restore registration records and DNS configuration to what is often described as “the last working configuration”. An urgent restoration of a hijacked domain may require the coordinated efforts of geographically dispersed registrars, operating in different time zones. The emergency action channel requires a **contact directory** of parties who can be reached during non-business hours and weekends. It may be useful to make support staff contacts available online, so a third party is not required to maintain and distribute the contact details.

A **companion policy to the emergency action channel –** to identify evaluation criteria a registrant must provide to obtain immediate intervention (e.g., circumstances and evidence). From these, registrars can define emergency UNDO procedures. This policy would complement the TDRP and must not undermine or conflict with policies defined therein. The circumstances which distinguish when an urgent recovery policy may be a more appropriate action than the TDRP include:

1. Immediacy of the harm to the registrant if the transfer is not reversed (e.g., business interruption, security incidents).
2. Magnitude of the harm, or the extent to which the incident threatens the security and stability of parties other than the registrant, including but not limited to users, business partners, customers, and subscribers of a registrant's services.
3. Escalating impact, or the extent to which a delay in reversing the transfer (and DNS configuration) would cause more serious and widespread incidents.

The emergency action procedures should be tested to verify they are resilient to tampering and difficult to exploit. In particular, it should be difficult or impossible for an attacker to effect a hijack or interfere with a transfer under the guise of requesting urgent restoration of a domain.

A **public awareness campaign** should be conducted to provide clear and unambiguous documentation that describes the policy and processes to registrars and registrants. This documentation should identify the criteria and the procedures registrants must follow to request intervention and immediate restoration.

5 Security Measures to Protect Domain Names

All parties have business incentives to protect domain names from hijacking and theft. Here, we consider measures registrants, registrars, registries and ICANN might take to protect domain names and minimize hijacking incidents.

5.1 Steps Registrants Can Take to Protect Domain Names

A registrant can reduce the risk of losing a domain name by taking measures to protect his registration information and name holder status. The following measures are available to registrants today. Awareness campaigns will increase registrant understanding of these opportunities and services.

To protect against unintended loss or hijacking of a domain name, a registrant should

1) Keep domain name registration records accurate and current.
2) Keep registrant account information (user identity, password, or other credentials) private, secure, and recoverable.
3) Only grant registration account access and change control to parties in the registrant's organization whose role(s) involve domain name administration.
4) Choose a registrar with hours of operation that match the needs of the registrant.
5) Keep current and accurate registrar business and emergency contact information.
6) Be familiar with and incorporate urgent restoration of domain name and DNS configuration procedures as part of business continuity policy and planning.
7) Investigate whether business interruption and losses related to a registration or DNS configuration incident are covered by insurance policies.
8) Request that domain names be placed on Registrar-Lock.
9) If a registrant's sponsoring registrar uses EPP, the registrant should use a unique EPP authInfo code for each domain name registered.
10) Request that the losing registrar contact the registrant when a transfer request is received using a contact point separate from that used by the gaining registrar.
11) Routinely check the Whois service to check if a domain name is under Registrar-Lock. Note however that this information can be as much as 24 hours out-of-date, compared to the Registrar-Lock status in the registry.
12) Routinely check domain name information to ensure that no unauthorized changes have been made to the contact information. This check can be automated using scripting tools and commercially available software. More frequent queries increase timeliness of detection and thus reduce the level of risk that a change will go unnoticed.
13) Consult with the sponsoring registrar to establish appropriate (and possibly preferred) authentication processes for removing a transfer lock or changing a domain name configuration. (We note that such added safeguards may delay or increase the

difficulty of transferring names, but this is exactly the relationship some registrants may want with a registrar.)

14) Choose a registrar who issues a transfer pending notification as its standard practice.

Registrants seeking to further reduce risk should:

15) Choose a registrar who will notify the registrant using contact methods in addition to (and in parallel with) standard email notices.

16) Specify the contact methods that must be used (e.g., any or all contacts in the registration record, including, email, telephone, messaging and paging services, fax, etc.).

Some of these services are likely to be offered by registrars as part of a basic service. Registrants that place a high value on their domain names may be willing to pay a premium for enhanced protection of registration and DNS configuration, including automated monitoring services.

5.2 Steps Registrars Can Take to Protect Domain Names

Registrars have an obligation and strong business incentives to reduce the risk of domain hijacking and loss due to mishandling of names and registration information.

To protect against unintended loss or hijacking of a domain name, registrars should consider the following measures:

1) Establish a more uniform implementation of EPP authInfo. Some registrars use a single EPP authInfo code for all domains held by the same registrant, and this is contrary to the transfer policy, which requires that Registrar-generated EPP authInfo codes be unique on a per-domain basis. Some registrars use the same EPP authInfo code for multiple (all) registrants, a practice which does not comply with the transfer policy and which effectively makes the EPP authInfo useless.

   Some registrars allow registrants to generate EPP authInfo codes for their domain names. The transfer policy does not impose any restrictions on EPP authInfo codes created by *registrants*, and by extension resellers and service providers acting as agents for registrants. While registrants and their agents are thus free to use the same EPP authInfo code for multiple domain names they hold, this practice exposes all names a registrant (or reseller) retains with that code whenever one is transferred. It may be appropriate or valuable to registrants to have the ability to create unique EPP authInfo values for each domain name registered.

2) Establish a uniform default setting of domain locks across registrars. Many registrars already automatically lock domain names. Registrars must provide sufficiently direct means to unlock domain locks, so as to not unduly deny a legitimate transfer request from a verified domain name registrant.

3) Investigate additional methods to improve accuracy of registrant records. This is admittedly a difficult task. Part of the solution lies in public awareness. ICANN's Whois Data Reminder Policy (http://www.icann.org/registrars/wdrp.htm) requires

registrars to annually present registrants with a copy of their Whois data to allow registrants an opportunity to update the data. More frequent or alternate communications might assist registrants in keeping their information up to date.

4) Collect emergency contact information from registrants, registrars, and resellers for parties who are suited to assist in responding to an urgent restoration of domain name incident. Define escalation processes (emergency procedures) that all parties agree can be instituted in events where emergency contacts are not available.

5) Consider measures to improve authentication and authorization used in all registrar business processes, but especially in these sensitive change processes:

    i) change of delegation information,

    ii) change of contact details (credentials),

    iii) change of registrant (selling the name), and

    iv) change of registrar.

6) Protect registrant information that can be used to facilitate fraud and impersonation, and theft of a domain name. As a default, treat any information that is used in registrant authentication processes as private. Consider treating this information with the same or similar measures to measures used to protect credit card or other financial information.

7) Improve auditing of resellers' compliance with record keeping requirements.

8) Ensure that resellers understand record keeping requirements of registrars (and ICANN), and improve compliance with these requirements.

9) Provide clear and readily accessible information to registrants regarding domain locking and domain name protection measures offered by registrars.

5.3 Steps Registries Can Take to Protect Domain Names

Registries, too, have an obligation and strong business incentives to reduce the risk of domain hijacking and loss due to mishandling of names and registration information. Actions registries may wish to investigate include the following:

1. Implement EPP authInfo (where not already implemented).
2. Work with registrars to establish a more secure implementation of EPP authInfo codes.
3. Monitor use of EPP authInfo codes; in particular, employ mechanisms that can detect and flag repeated use of the same EPP authInfo value across multiple registrants.
4. Work with registrars to define "best common practices" for auditing registration processing.
5. Work with registrars to improve authentication and authorization requirements for transfers and changes to Second Level Domain (SLD) name servers within the TLD.

5.4 Steps Resellers Can Take to Protect Domain Names

Although registrars are ultimately responsible for the actions of their resellers, registrars allow their resellers varying degrees of autonomy. In some cases a registrar's responsibilities may be delegated completely to a reseller. Resellers, acting as agents of registrars, thus have an obligation to reduce the risk of domain hijacking and loss due to mishandling of names and registration information.

To protect against unintended loss or hijacking of a domain name, resellers might consider the following measures:

1) Review all relevant ICANN transfer policy documentation. Request training from registrars regarding important domain transfer policies. Registrars have an obligation to provide documentation and training for resellers, to ensure that resellers conform to ICANN policies for domain names. Resellers should make sure that registrars provide documentation and training so that they can implement them at their organizations.

2) Establish a uniform default setting of domain locks. Many resellers already automatically lock domain names. Resellers must provide sufficiently direct means to unlock domain locks, so as to not unduly deny a legitimate transfer request from a verified domain name registrant.

3) Investigate additional methods to improve accuracy of registrant records. The ICANN Whois Data Reminder Policy (http://www.icann.org/registrars/wdrp.htm) requires registrars to annually present registrants with a copy of their Whois data to allow registrants an opportunity to update the data. Resellers should ask to receive reports of failures or updates to this information from registrars for the registrants that they have signed up, so that registrant records information may be kept up to date.

4) Acquire emergency contact information from registrants and registrars for parties who are suited to assist in responding to an urgent restoration of domain name incident. Define escalation processes (emergency procedures) that all parties agree can be instituted in events where emergency contacts are not available.

5) Consider measures to improve authentication and authorization used in all reseller business processes, but especially in these sensitive change processes:

   i) change of delegation information,

   ii) change of contact details (credentials),

   iii) change of registrant (selling the name), and

   iv) change of registrar.

6) Provide clear and readily accessible information to registrants regarding domain locking and domain name protection measures offered by resellers and registrars.

5.5 Steps ICANN take to minimize the negative impacts of transfers on the registrant

ICANN may need to consider developing (through its bottom-up, consensus-based policy development processes) a set of graduated penalties for registrars that fail to comply with the transfer policy (e.g. penalty for first offence, penalty for second offence etc., or penalties that increase with the time taken to rectify a fault in the registrars business process).

ICANN should publish additional consumer information that explains the domain transfers policy and processes, and identifies the areas of risk for a registrant. ICANN could provide a list of questions a registrant can ask a registrar to determine the level of authentication and protection mechanisms used to manage domain names. Another step ICANN can take is to make the SSAC report a part of the 6-month evaluation process of the transfer policy.

6 Findings and Recommendations

The Committee offers these findings and recommendations in the spirit of open review, comment and evaluation, with the expectation that they will be considered carefully before they result in action. In particular, several recommendations, if accepted, will result in future work items for the Committee as well as various parties encouraged to take action.

Overall, the Committee finds that name hijacking incidents are commonly the result of flaws in the processes implemented in support of the transfer policy, failure to comply with the transfer policy, and poor administration of domain names by registrars, resellers, *and* registrants.

Finding (1) Failures by registrars and resellers to adhere to the transfer policy have contributed to hijacking incidents and thefts of domain names.

Finding (2) Registrant identity verification used in a number of registrar business processes is not sufficient to detect and prevent fraud, misrepresentation, and impersonation of registrants.

Finding (3) Consistent use of available mechanisms (Registrar-Lock, EPP authInfo, and notification of a pending transfer issued to a registrant by a losing registrar) can prevent some hijacking incidents.

Finding (4) ICANN Policy on Transfer of Registrations between Registrars specifies that "consent from an individual or entity that has an email address matching the Transfer Contact email address" is an acceptable form of identity. Transfer Contact email addresses are often accessible via the Whois service and have been used to impersonate registrants.

Finding (5) Publishing registrant email addresses and contact information contributes to domain name hijacking and registrant impersonation. Hijacking incidents described in this report illustrate how attackers target a domain by gathering contact information using Whois services and by registering expired domains used by administrative contacts.

Finding (6) Accuracy of registration records and Whois information are critical to the transfer process. The ICANN Whois Data Reminder Policy requires that registrars annually request registrants to update Whois data, but registrars have no obligation to take any action except to notify registrants. Registrants who allow registration records to become stale appear to be more vulnerable to attacks.

Finding (7) ICANN and registries have business relationships with registrars, but no relationship with resellers (service providers). Resellers, however, may operate with the equivalent of a registrar's privileges when registering domain names. Recent hijacking incidents raise concerns with respect to resellers. The current situation suggests that resellers are effectively "invisible" to ICANN and registries and are not distinguishable from registrants. The responsibility of assuring that policies are enforced by resellers (and are held accountable if they are not) is entirely the burden of the registrar.

Finding (8) ICANN requires that registrars maintain records of domain name transactions. It does not appear that all registrars are working closely enough with their resellers to implement this requirement.

Finding (9) The Inter-Registrar Transfer Policy incorporates formal dispute mechanisms. These were not designed to prevent incidents requiring immediate and coordinated technical assistance across registrars. Specifically, there are no provisions to resolve an urgent restoration of domain name registration information and DNS configuration.

Finding (10) Changes to transfer processes introduced with the implementation of the ICANN Inter-Registrar Transfer Policy have not been the cause of any known attacks against domain names. There is no evidence to support reverting to the earlier policy.

On the basis of these findings, the Committee makes the following recommendations:

Recommendation (1): Registries should ensure that Registrar-Lock and EPP authInfo are implemented according to specification. In particular, registries should confirm that registrars comply with the transfer policy and do not use the same EPP authInfo code for all domains they register.

Recommendation (2): Registries and registrars should provide resellers and registrants with Best Common Practices that describe appropriate use and assignment of EPP authInfo codes and risks of misuse when the uniqueness property of this domain name password is not preserved.

Recommendation (3): Under the current transfer policy, a losing registrar notifies a registrant upon receiving a pending transfer notice from the registry at its option. Registrars should investigate whether making this notice a mandatory action would reduce hijacking incidences.

Recommendation (4): Registrars should make contact information for emergency support staff available to other registrars, agents of registrars (resellers), and registry operators. Specifically, registrars should provide an emergency action channel. The purpose of this channel is to provide 24 x 7 access to registrar technical support staff that are authorized to assess an emergency situation, establish the magnitude and immediacy of harm, and take measures to restore registration records and DNS configuration in circumstances which merit such intervention.

Recommendation (5): Registrars should identify evaluation criteria a registrant must provide to obtain immediate intervention and restoration of domain name registration information and DNS configuration. Registrars should define emergency procedures and policy based on these criteria. This policy would complement the Transfer Dispute Resolution Policy (TDRP) and must not undermine or conflict with those policies.

Recommendation (6): ICANN, the registries, and the registrars should conduct a public awareness campaign to identify the criteria and the procedures registrants must follow to request intervention and obtain immediate restoration of a domain name and DNS configuration.

Recommendation (7): Registrars should investigate additional methods to improve accuracy and integrity of registrant records. More frequent or alternate communications might assist registrants in keeping their information up to date. Registrars should also acquire emergency contact information from registrants for technical staff who are authorized and able to assist in responding to an urgent restoration of domain name incident.

Recommendation (8): Registrars should improve registrant awareness of the threats of domain name hijacking and registrant impersonation and fraud, and emphasize the need for registrants to keep registration information accurate. Registrars should also inform registrants of the availability and purpose of the Registrar-Lock, and encourage its use. Registrars should further inform registrants of the purpose of authorization mechanisms (EPP authInfo), and should develop recommended practices for registrants to protect their domains, including routine monitoring of domain name status, and timely and accurate maintenance of contact and authentication information.

Recommendation (9): ICANN should investigate whether stronger and more publicly visible enforcement mechanisms are needed to deal with registrars that fail to comply with the transfer policy, and to hold registrars accountable for the actions of their resellers.

Recommendation (10): ICANN should consider whether to strengthen the identity verification requirements in electronic correspondence to be commensurate with the verification used when the correspondence is by mail or in person.

Appendix A
The Four Rs: The Registry, Registrars, Resellers and Registrants

This section provides an overview of basic domain name management processes, and the roles played by the registry, registrars, resellers and registrant in each.

Overview of the Registration Process

A party wishing to register a domain name may do so by contacting a registrar. Companies operating through partnership or reseller agreements with a registrar ("resellers" and "service providers[10]") also process domain name registrations. At the time of registration, the registrant provides the registrar with technical and contact information to be associated with the domain name, and enters into a registration Agreement with the registrar.

The registrar then submits the technical and contact information associated with the domain name to the registry, which maintains the authoritative, master database of all domain names registered in a particular Top-Level Domain.

Overview of the Registrar Transfer Process

Registrants may choose to transfer their domain names from one registrar to another. Such transfers are conducted according to the Inter-Registrar Transfer Policy (see http://www.icann.org/transfers/), which has been in effect since November 2004. The policy applies to inter-registrar transfers in all unsponsored gTLDs (.biz, .com, .info, .name, .net, .org, .pro). This policy was developed to create clear guidelines for inter-registrar transfers, in response to an environment which generated frequent complaints from registrants: registrars were refusing to allow them to switch to another registrar or were imposing arbitrary conditions intended to prevent transfers out.

To transfer a domain name from one registrar to another, a registrant makes a request to the gaining registrar. The gaining registrar must take two actions. First, the gaining registrar must obtain authorization for a transfer request by requiring that the registered name holder or registrant's Administrative Contact as listed in the Whois complete a valid Standardized Form of Authorization (FOA). Second, the gaining registrar is required to verify the identity of the person submitting the Form. *By transmitting a "Transfer" command, a registrar warrants that it has completed both of these steps.*

Upon receiving the registrant's returned FOA, the gaining registrar sends a Transfer Request to the registry.

If a domain name is locked, the transfer will fail automatically at the registry, and no further action by the losing registrar is required. A registrant who wishes to transfer must

[10] The term service provider refers to an organization that offers domain name registration as one of several services to a customer, including but not limited to web hosting, email, data archival and Internet access.

explicitly request that the losing registrar remove the LOCK and then re-submit the transfer request to the gaining registrar.

If a domain name is unlocked, the registry will notify the losing registrar of the transfer request, and the transfer will proceed unless the losing registrar rejects it within five (5) days. At its discretion and option, a losing registrar may contact the registrant with notice of a pending transfer-out, to confirm the registrant’s intent to transfer the domain name to the gaining registrar. The registrant has the opportunity to reject the transfer at this point. The losing registrar also has the authority to reject the transfer in certain specific circumstances, including evidence of fraud or the existence of a pending dispute over the name.

Registry operators that use the EPP protocol (e.g., .org, .biz, .info, .name) are required to generate a unique domain name password (EPP authInfo code) for each domain name registered. In these registries, the EPP authInfo code is a required element in registrar transfers. The losing registrar must provide the EPP authInfo code to the registrant within five (5) days of the registrant’s request. The gaining registrar must then obtain this code from the registrant before a transfer-in can be initiated.

This flow is depicted in figure A-1:

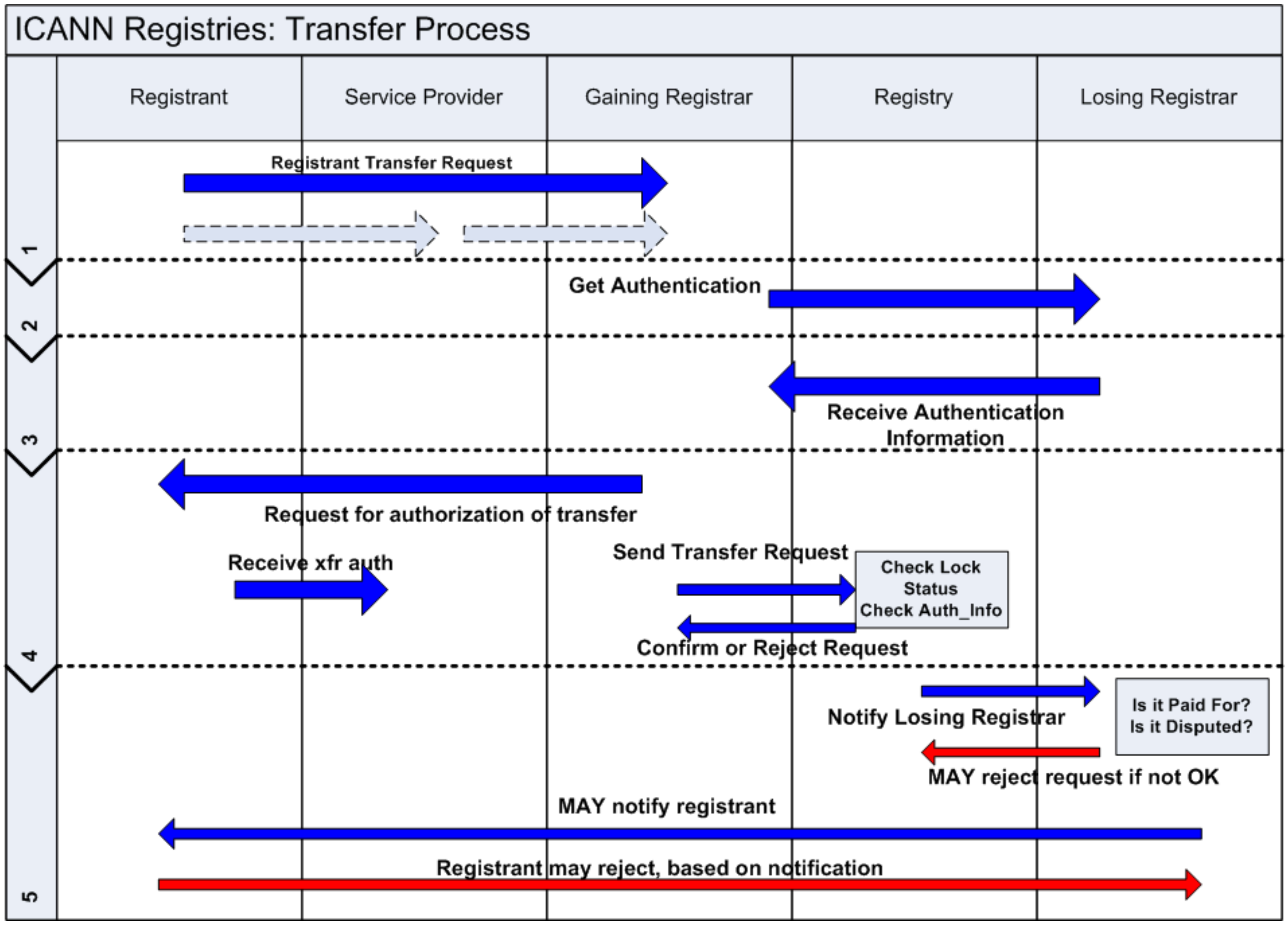
ICANN Registries: Transfer Process
Registrant
Service Provider
Gaining Registrar
Registry
Losing Registrar
1
2
3
4
5
Registrant Transfer Request
Get Authentication
Receive Authentication Information
Request for authorization of transfer
Receive xfr auth
Send Transfer Request
Check Lock Status Check Auth_Info
Confirm or Reject Request
Notify Losing Registrar
Is it Paid For? Is it Disputed?
MAY reject request if not OK
MAY notify registrant
Registrant may reject, based on notification

Figure A-1: Transfer Process

Overview of the Registrant Transfer Process

The process for transferring a domain name from one registrant to another is handled by the registrar. The process varies by registrar. There is no ICANN policy which lays out a process which must be used for registrant transfers; therefore, registrars have developed their own forms, identity validation procedures, and automated processes. Escrow devices are sometimes used in cases where a domain name is being sold.

The new registrant will enter into a registration Agreement with the registrar that defines his/her rights and responsibilities with regard to the domain name. Once the change has been accepted by the registrar, the registrar will send updated Whois information for the domain name to the registry.

Overview of the Whois Modification Process

Periodically, contact details and name server information may need to be modified or updated by the registrant. Many registrars offer online account access, so that registrants can log in and make changes to their domain information directly. In other cases, registrants may provide updates to their registrar via the registrar's support phone numbers or email addresses. Once these changes have been completed, the registrar will send the updated Whois information to the registry.

It is worth observing that many processes are dependent on the accuracy of the registrant's Whois information maintained by the registrar. If an unauthorized party succeeds in altering the registrant's contact information in the Whois database, the authenticity of any subsequent transactions can be compromised. Additionally, if a registrant has failed to maintain accurate contact information, it will be even difficult to validate the identity of the registrant or notify the registrant of pending changes.

Appendix B
Contributors

Name	**Affiliation**
Stephen Crocker	Shinkuro
David Piscitello	ICANN
Tina Dam	ICANN
Karen Lentz	ICANN
Tim Cole	ICANN
Jaap Akkerhuis	NLnet Labs
Ram Mohan	Afilias, Ltd.
Brian Smith	Hush Communications
Bruce Tonkin	Melbourne IT
Rodney Joffe	UltraDNS
Alison Mankin	Shinkuro
Mark Kosters	VeriSign
James Galvin	ElistX
Jonathan Nevett	Network Solutions
Dan Waldrun	VeriSign
Scott Hollenbeck	VeriSign
Ray Plzak	ARIN
Dan Halloran	ICANN
Richard Lau	Independent domain analyst and consultant

Appendix C
HZ.com Whois Records from WWW.Whois.sc

C.1 The Whois record for HZ.com on 31 December 2004:

```
Domain:
hz.com
Cache Date:
2004-12-31
Registrar:
THE NAME IT CORPORATION DBA NAMESERVICES.NET[11]
Domain Name:           hz.com
Registrar: THE NAME IT CORPORATION DBA NAMESERVICES.NET
Registrant Contact
Name:                  Geoff    Mulligan
Address:               3578 E Hartsel Drive #
                       Co Springs, CO 80920 US
Email Address:          geoff@coslabs.com
Phone Number:           7195932992
Fax Number:
Administrative Contact
Name:                  Geoff    Mulligan
Address:               3578 E Hartsel Drive #372
                       Co Springs, CO 80920 US
Email Address:          geoff@coslabs.com
Phone Number:           7195932992
Fax Number:
Technical Contact
Name:                      Geoff    Mulligan
Address:               3578 E Hartsel Drive #372
                       Co Springs, CO 80920 US
Email Address:          geoff@coslabs.com
Phone Number:           7195932992
Fax Number:
Record Created on........ 1995-06-15 00:00:00.000
Record last updated on... 2002-06-21 14:10:38.000
Expire on................ 2005-06-14 00:00:00.000
Domain servers in listed order:

            ns1.granitecanyon.com 205.166.226.38
            ns2.granitecanyon.com 205.166.226.38
            ns3.granitecanyon.com 65.102.83.43
            ns.coslabs.com 199.233.92.34
```

[11] AITdomains.com, a subsidiary of AIT, Inc., began operations in 1998 as N@meIT Corporation.

C.2 Altered Whois Record for HZ.com, 19 February 2005

```
Domain:
hz.com
Cache Date:
2005-02-19
Registrar:
DIRECT INFORMATION PVT. LTD., DBA DIRECTI.COM
Registration Service Provided By: QNIC
Contact: sales@qnic.com
Website: www.qnic.com
Abuse Desk Email Address: abuse@qnic.com
Domain Name: HZ.COM
Registrant:
    Xybererotica
    Xybererotica        (admin@xybererotica.com)
    Xybererotica
    Xybererotica
    null,12345
    AF
    Tel. +1.23456789
Creation Date: 14-Jun-1995
Expiration Date: 13-Jun-2006
Domain servers in listed order:
    ns.coslabs.com
    ns1.granitecanyon.com
    ns2.granitecanyon.com
    ns3.granitecanyon.com
Administrative Contact:
    Xybererotica
    Xybererotica        (admin@xybererotica.com)
    Xybererotica
    Xybererotica
    null,12345
    AF
    Tel. +1.23456789
Technical Contact:
    Xybererotica
    Xybererotica        (admin@xybererotica.com)
    Xybererotica
    Xybererotica
    null,12345
    AF
    Tel. +1.23456789
Billing Contact:
    Xybererotica
    Xybererotica        (admin@xybererotica.com)
    null,12345
    AF
    Tel. +1.23456789
Status:LOCKED
  Note: This Domain Name is currently Locked. In this status the domain name can
notbe transferred, hijacked, or modified. The Owner of this
domain name can easily change this status from their control panel. Thisfeature
is provided as a security measure against fraudulent domain namehijacking.
```

Appendix D
Citations

ICANN Inter-Registrar Transfer Policy
http://www.icann.org/transfers

ICANN Registrar Transfer Dispute Resolution Policy
http://www.icann.org/transfers

ICANN Registrar Accreditation Agreement
http://www.icann.org/registrars/ra-agreement-17may01.htm

ICANN-Registry Agreements
http://www.icann.org/registries/agreements.htm

ICANN Registry-Registrar Agreements
http://www.icann.org/registrars/agreements.html

Letter from Louis Touton to Bruce Beckwith Regarding Breach of VeriSign Registrar's Accreditation Agreement (Whois Data Accuracy) 3 September 2002
http://www.icann.org/correspondence/touton-letter-to-beckwith-03sep02.htm

Letter from Paul Twomey to Russell Lewis 3 October 2003
http://www.icann.org/correspondence/twomey-to-lewis-03oct03.htm

Standardized Form of Authorization, Domain Name Transfer:
Initial Authorization for Registrar Transfer
http://www.icann.org/transfers/foa-auth-12jul04.htm

Standardized Form of Authorization, Domain Name Transfer:
Confirmation of Registrar Transfer Request
http://www.icann.org/transfers/foa-conf-12jul04.htm