Domain Name Hijacking
A Preliminary Report

Security and Stability Advisory Committee

Mar del Plata

April 5, 2005

Headlines

- Panix.com was hijacked on 15 Jan 2005
  - action returned it after 48 hours
- Gaining Registrar and Reseller at fault
- We say the problem is (also) systemic
- Other domain names have been hijacked
  - hz.com is an equally compelling story
- Room for improvement

Outline

- Hijackings
  - Details on two hijackings - panix.com, hz.com
  - Nightmare scenarios
- The transfer process
  - Opportunities for error and mischief
  - The recent change
  - Potential improvements
- The Recovery process and improvements
- Tentative Recommendations

Security problem

- Unauthorized disclosure, alteration, insertion or destruction of domain name data
- Data includes:
  - Domain name record information
    - A records, MX records, etc.
  - Name Server information (e.g NS records)
  - Domain name holder information
  - Domain name contact information
  - Registrar

Panix.com incident

- Unauthorized change to the DNS information including A records and MX records, and name holder information
- Impact
  - website and email services ceased
    - Major impact on business operations

Root cause of panix.com

- Failure to authenticate the registrant by the gaining registrar
- Registrar transfer initiated by a third party through a domain name service provider
- Once domain name transferred at the registry level, the registrant information was changed at the new registrar, and the DNS nameserver for the domain name was changed
- New DNS nameserver contained default A and MX records that were different from the original

Hijacking of hz.com - 1

- First identified by registrant February 16, 2005
- Caught by a random Whois check
  - there was no indication that the domain was hijacked
  - classic man-in-the-middle capture
- Losing registrar claimed transfer was legitimate
  - refused to share original email to registrant
- Registrant asked to prove transfer not authorized(!)
  - How do you prove what you did not do?
- Losing registrar took no responsibility for the problem
- Registry had no registrant records
- Occurred *after* transfer dispute time period

Hijacking of hz.com - 2

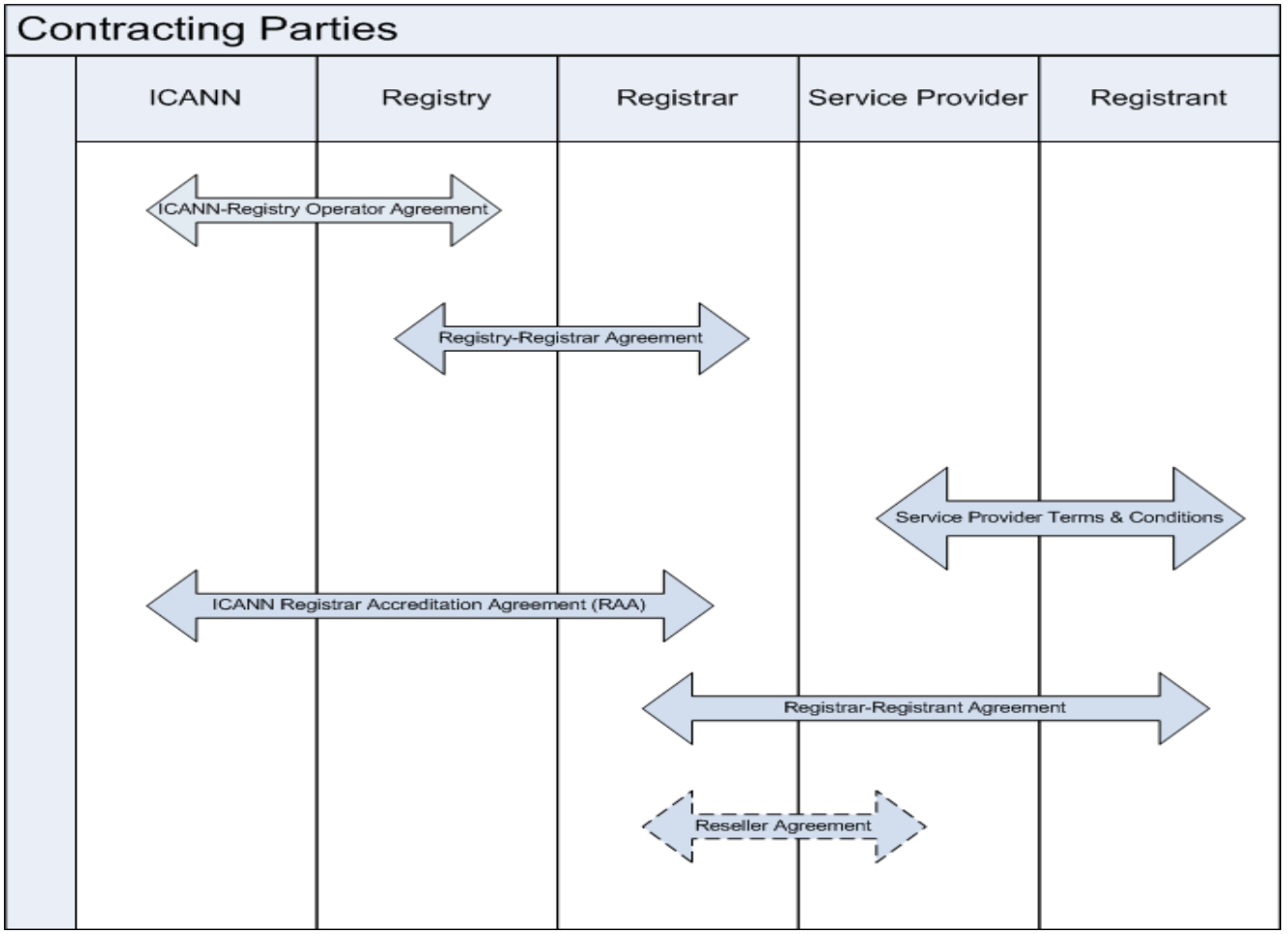
- No “Whowas” service
- Registrant believes the losing registrar’s mail servers or systems were compromised, resulting in transfers with no notice
- Direct intervention with CEO of gaining registrar led to domain being returned to registrant
- Gaining registrar had noticed 80 other cases
  - no place to report; no clearinghouse; no security alert mechanism
- Caveat Emptor still reigns

Nightmare Scenarios

- Immediate loss of a domain is visible
- Man-in-the-middle could be worse
  - Read all the mail both in and out
  - Alter critical information for selected targets
  - Likely to remain undetected for a while
    - Perhaps a very long time

Entities involved for a gtld name

- ICANN
- Registry operator
- Registrars
- Domain name service providers
- Registrants
- Other domain name contacts



Registry security

- Registries use authentication to control registrar access to the registry database
  - e.g source IP address, password, and digital certificates
- Registrars can create and administer records in the registry database
- A registrar may only alter records where they are designated as the registrar for that record in the database
- Registry: database, WHOIS service, top level nameserver (e.g .com)
  - Controls direct access to above systems
- Nameserver information for each domain name and the IP addresses of nameservers is paramount

Registrar security

- Registrars hold credentials for access to registry database
  - Maintains data on domain name holder (registrant), and admin, tech and billing contacts, as well as data for service providers (resellers)
- Data includes name, address, phone, fax, email and extra authentication information (e.g passwords, credit cards, etc) for the above contacts, as well as access control information (which contact has which privileges to change information)
- Most of the contact information is made public
- May operate a nameserver for a particular domain name (which holds records such as A records, and MX records that support services such as web sites and email)
- Common security issues are inaccurate data on domain name holder and other contacts
- Common authentication techniques are username, password, sending unique code to contact email address, and other information (such as mother's maiden name etc)

Service provider security

- Domain name service providers, typically operate a nameserver that hold the A and MX records, and provide associated services such as email, and web hosting
- Have credentials for access to registrar systems
- Manage multiple domain name records via registrar
- Maintain authentication data for domain name holders and other contacts
- Most important data is the domain name records in the nameservers

Registrant security

- Hold credentials for access to either a domain name service provider or registrar
- May authorise other parties as admin, tech or billing contacts
- May provide credentials to other parties
- Ultimately should authorise all changes to a domain name record

Contacts

- Domain name contacts (e.g admin, tech, billing) may hold credentials for more than one domain name
- Commonly have technical knowledge to maintain a domain name record on behalf of a registrant
- Relationship with registrant not always clear

Common registrant issues

- Registrant not the official domain name holder (licence holder)
  - Often the registration of a domain name has been delegated to another party, and that party inserts their information as the registrant
- Poor management of credentials
  - Held insecurely on a PC or laptop
  - Prone to phishing, spyware etc
  - Provided to other contacts or additional parties
- Lack of clear delegation of authority to a domain name contact
  - Eg: Tech contacts may decide to change DNS information or transfer between registrars or service providers
- Lack of understanding of industry structure and transfer mechanisms

Risk magnitude of security breach

- Registry (may affect all records in zone)
- Registrar (may affect all records under management of registrar in registry)
- Domain name service provider (may affect all records under management within registrar database)
- Registrant (all records held by registrant)
- Domain name contact (all records where they hold authentication information)
- Some registries, registrars, and service providers manage more than a million records

Of course, the hijack of a single name could risk millions of users

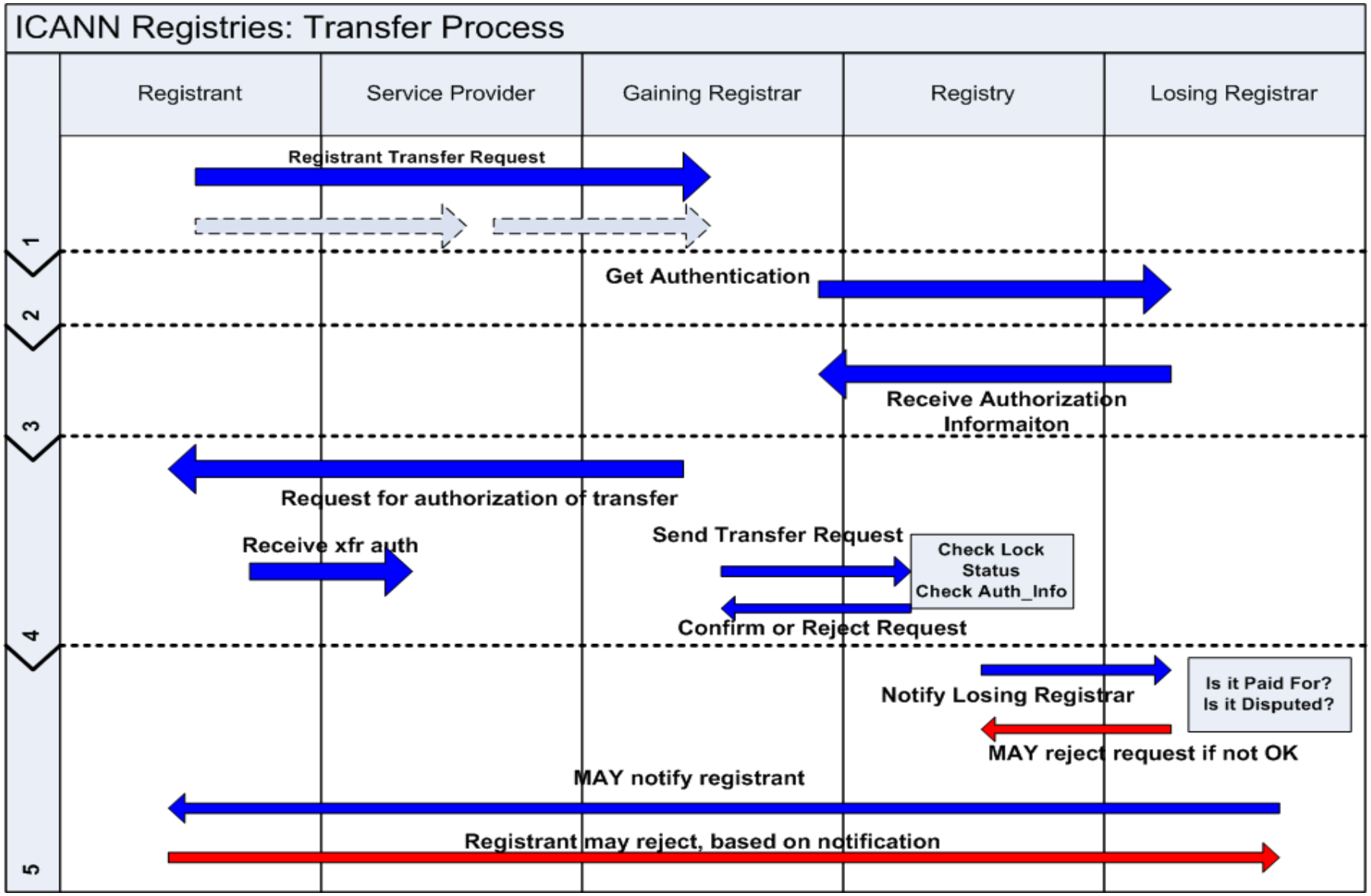
Transfers

- Transfers relate to a transfer of control at different levels of the system
- Common transfers include:
  - Between registrars at the registry
  - Between domain name service providers at the registrar (ie, no Whois record change, no Registry notice) … and no transfer fee
  - Between registrants at a registrar or a domain name service provider

Transfer issues

- Authentication – need to authenticate the parties in a transfer transaction
- Authorisation – need to ensure that each party is fully aware of the meaning of the transfer transaction and gives approval for the transfer
- Protection – additional mechanisms to prevent an unauthorised transfer

Transfer Process



Recent transfers policy change (1)

- Transfers process supports the ability for a gaining registrar to initiate a transfer, and the ability for a losing registrar to reject a transfer
- Requirement of standard text to ensure that a registrant authorises a transfer and authorises cancelling a transfer

Recent transfers policy change (2)

- Explicit reasons where a losing registrar can cancel a transfer without authorisation from the registrant
  - non-payment of the domain
  - UDRP dispute
- Explicit additional protection mechanisms available to the registrant
  - Ability to request the name be locked
  - Auth-info password for EPP registries

Previous industry practice

- Prior to the refinement of the transfers policy it was common practice for a losing registrar to reject a transfer without explicit authorisation from the registrant
- Losing registrars would send a message to the registrant advising of the impending transfer, and if this message was ignored the transfer would be rejected

Relationship of policy change to panix.com incident

- Change in policy did not affect panix.com
  - losing registrar did not send a notice to the registrant of the impending transfer

Relationship of policy change to hz.com incident

- Change in policy did not affect hz.com either
  - losing registrar sent a notice to the registrant email, but real registrant did not get the email

Industry issues

- Lack of education to registrants regarding availability of lock (and auth-info where available).
- Lack of facilities provided by registrars (and domain name service providers/resellers) to support management by the registrant of lock and auth-info
- Improper use of lock and auth-info by registrars

What could prevent the panix.com incident

- Gaining registrar properly authenticating the registrant and gaining authorisation from the registrant
- Registrant placing the name on lock
- Losing registrar contacting the registrant to confirm that the transfer was authorised
- Registry implementing auth-info password

What could prevent the hz.com incident

- Losing registrar properly ensuring that registrant email was not spoofed
- Additional authorization method(s)
- Registrant placing the name on lock
- Registry implementing auth-info password

Failure to Lock a Domain

- Registry doesn’t provide the service
  - Registrar doesn’t provide the service
- Registrar doesn’t explain it well enough
- Registrant doesn’t understand the value
- Registrant can’t figure out how to do it

The Auth Mechanism

- Some Registrars use(d) the same Auth code for all registrants(!)
- Some Registrars do not provide the Auth Code on request (even though contract requires it)
- Some Registrars provide incorrect Auth Codes, multiple times (intentional or accident?), or registrant's don't ask for the right credentials (e.g password for access to registrar, rather than auth-code in the registry database)

The Recovery Process

- Aimed at contractual disputes
  - Doesn't distinguish between loss of use of a domain, failure to transfer a domain when properly authorized, or failure to make changes to nameserver or other details
- May take weeks
- ICANN's enforcement is usually private

The Emergency Recovery Process

- Urgent action for operational emergencies
  - Not documented.
  - Key people who know each other talk on private channels
  - No clear authority to fix things. All ad hoc.
  - No documented escalation path
- The records of who has registered a domain name at various periods of time is distributed across all the registrars that have ever been responsible for that name

Potential Fixes to the Recovery Process

- A new channel and corresponding procedures to fix urgent operational loss of use problems versus disputes over contracts, charges, etc.
  - The distinction is in the magnitude and immediacy of the harm
- 24/7 contacts

Protection Now and in the Future

- Insurance to cover business impact from a domain name problem?
- Need a range of mechanisms that trade off ease of use versus quality of protection
  - Some might not cost very much
- Need much better visibility and education
  - This should be a discriminator in the marketplace

Tentative Recommendations

- Campaign for public awareness
  - Domain name risks and management of credentials
  - Domain name lock and auth-info mechanisms
  - Levels of service (contact hours, authentication techniques)
- Require Losing Registrar to send notification to the Registrant, in addition to Gaining registrar getting authorisation
  - Currently it's optional
  - Refinement of existing policy, not a reversal
- Development of emergency action channels
- Development of more visible enforcement
- Emergency "UnDo" procedure being pushed

Domain Name Hijacking
A Preliminary Report

Security and Stability Advisory Committee

Mar del Plata

April 5, 2005

Transfer process (1)

- Gaining registrar initiates a transfer at the registry after receiving authorisation from the registrant
- Registrant is identified from the WHOIS information held at the losing registrar
- Gaining registrant authenticates the registrant by sending an email to the registrant (or admin) contact, and receiving a reply from that contact
- Registrant (or admin) contact authorises the transfer by agreeing to standard text explaining the transfer

Transfer process (2)

- It is common for a domain name service provider/reseller (or tech contact) to initiate a transfer at the registrar on behalf of the registrant
- Often the service provider/reseller has control of the registrant credentials (e.g email address)
- In some cases registrars delegate to a reseller the task of gaining authorisation from the registrant as the reseller often holds authentication information for the registrant

Transfer process (3)

- When a registry receives a transfer request, two checks are available:
  - Check if domain name has been locked by the losing registrar
  - Check the auth-info password for the domain name
    - Part of the EPP protocol used by .biz, .info, .us, .au etc
    - Not yet used for .com, .net
- If either check fails, the transfer is rejected by the registry
- Transfer is also not possible within 60 days of registration or registrar transfer (except to reverse)

Transfer process (4)

- If the request passes the registry check, the losing registrar is notified
- Notification via range of means including email and online reports (EPP supports a message queue at the registry)
- Losing registrar has 5 days to reject the transfer

Transfer process (5)

- Losing registrar may reject a transfer, without authorisation from the registrant, for a range of specified reasons including:
  - Lack of payment for the domain
  - UDRP dispute
- Losing registrar may authenticate and receive authorisation from the registrant using standard form of authorization to reject a transfer on the basis of the registrant's wishes