Bridging Technical Possibilities With Policy Technicalities

Montreal, QC
June 24, 2003
Past, Present, and Future

• The Whois policies of today are severely constrained by the Whois protocol of yesterday.
• In the future, CRISP will allow greater flexibility for policy.
• The questions should no longer be “How do we do this?” but “What do we want?”
The Past

• Whois was first described in RFC 812 in 1982.
  – It was titled “Nicname/Whois”
  – Its IANA port registration is under the “Nicname”.
  – RFC 812 describes Whois over NCP, not IP.
• By comparison, the first RFC to describe DNS was published in 1983.
• RFC 954, the most current specification for Whois, spends more text describing who from ARPANET & MILNET should be in the database than describing the protocol itself.
The Present

• Nickname/Whois is used for many types of data:
  – domain registration data
  – IP address allocation data
  – Routing policy data
  – others… many we don’t even know about
The Present Users

• Nicname/Whois users are no longer just a couple of node operators on ARPANET. They are:
  – Intellectual property holders
  – Law enforcement
  – Service providers
  – Network operators
  – Registrars
  – Registrants
  – DNS users
  – Abusive users
The Future

• The CRISP working group of the IETF is working on a new specification for use by registries of Internet resources.

• It is applying what we have learned about operating services over the Internet from the 20 intervening years to the problems of today.
CRISP Goals

• Access controls
  – allows service operators to differentiate between the varying types of users

• Internationalization (I18N)
  – provides a user experience beyond ASCII and creates an environment for localization (L10N).

• Decentralized
  – facilitates navigation between repositories without requiring aggregation of data
Authentication vs. Authorization

- **Authentication** – the process used to verify the identity of a user
- **Authorization** – the access policies applied to a user based on authentication
- Authentication mechanisms facilitate authorization schemes.
Today’s Authentication

• Anonymous
  – because RFC 954 assumes all users to be equal

• Source IP address
  – this is an artifact of the Internet Protocol and was never intended as an authentication mechanism

• Hence, the authorization policies of today are limited.
Modern Authentication and Authorization

• Authentication mechanisms
  – passwords, one-time passwords, digital certificates, references

• Authorization schemes
  – user-based, sequence-based, chain-based, attribute-based, time-based, referee-based
Passwords

• An old idea still valid in today’s world.
  – Newer technologies allow passwords to be passed securely on unencrypted channels.
  – The user experience is the same.

• Passwords allow for the well understood user-based authorization schemes.
One-time Passwords

• One-time password systems are cryptographic mechanisms designed to keep pass phrases from being sent in the clear over unencrypted sessions.
  – However, their design limits their use to a finite number of authentications with both parties keeping track of the number of uses.
  – But the user experience is not much different than normal passwords.

• This allows for sequence-based authorization
  – access may be changed based on the number of times a user authenticates.
Digital Certificates

• Use a branch of mathematics called public key cryptography to conduct authentication.
  – Used in conjunction with TLS, they also allow for server authentication and session encryption.
• Facilitate the following authorization schemes:
  – user-based
  – chain-based
  – attribute-based
  – time-based
Certificate Chains

Authorization can be based on one of the certificates in the chain.

• Example:
  – If the certificate is signed by the “lea CA”
    • Allow access to all contact data
  – If the certificate is signed by the “regr CA”
    • Allow access only to all domain and registrant data
Attributes in Certificates

- Information attributes in certificates are cryptographically secure.
- Example:
  - If the “Type” attribute in the certificate equals “LEA”
    • Allow access to all contact data
  - If the “Type” attribute in the certificate equals “Registrar”
    • Allow access only to all domain and registrant data
Referrals

- The CRISP protocols allow a server to pass extra information via a client to a referent server.
- This information may contain authentication data, thus allowing a referee-based authorization policy.
Conclusion

- CRISP will allow much more than is currently possible with Nicname/Whois.
- The question should no longer be:
  - How do we do this?
- The question should be:
  - What do we want?