Eesti Internet
Eesti Interneti SA

eeTLD WHOIS accuracy conception

New methods in domain registrant's personal identification

Marek-Andres Kauts

Estonian Internet Foundation

Chairman of the Management Board and CEO

Abstract: eeTLD and Estonian Internet Foundation

Estonian Internet Foundation: private organization with multi-stakeholder PDP body-s

- No “domain law”
- Registrations are open to everyone, incl private persons and foreign residents
- Total number of domains 66 500, incl IDN 1300

Registry-registrar model, 41 registrars, incl 9 ICANN accredited registrars

- EPP
- Registry-registrar contract
- Guarantee deposite, contractual penalties for incidents

Domain registry software F.R.E.D.

Staff 14 people

Problems regarding WHOIS accuracy

1. Unidentified registrants
2. Irredeemability of the application
3. No audit trail

Lack of consumer trust and confidentce: Consumers use WHOIS data to establish the legitimacy of those engaged in e-commerce. Inaccuracy WHOIS database decreases their trust to e-commerce.

Cyber security and cybercrime experts make extensive use of WHOIS to thwart and respond to a varied set of threats. Information contained within inaccurate WHOIS is invaluable or misleading in these efforts.

Anonymous registrations increase number of malicious domains: *"All things being equal, scammers prefer registrars with "no questions asked" registration. The less information a scammer needs to provide, the better."* Mapping the Mal Web. McAfee 2010

eeTLD WHOIS accuracy conception

1. All the registrants are identified
2. Applications are collected to the registry
3. Audit trail to the application and registrant

Methods of registrant identification:

1. International registrant's personal identification: Domain registrant’s personal identification via bank transfer.
2. Domestic registrant's personal identification: Estonian smart-card ID

Domain registrant's personal identification via bank transfer

Primarily used for identifying foreign registrants who have no Estonian IDcard/Mobile-ID

Based on international anti-money laundering conventions and protocols:

- FATF Forty Recommendations and Special Recommendations on Terrorist Financing
- Egmont Group of Financial Intelligence Units
- IBAN / SWIFT standards

FRED and EPP protocol modified by Estonian Internet Foundation

Personal identification via bank transfer doesn't have significant effect on ease of use and usability of the registry services

The “chain of trust” between the registrant and the registry I

The DRBT establishes a chain of trust, which is linked on the basis of the following legislation, documents and requirements.

I Registrant – Registrant’s bank

FATF 40+9 recommendations and other measures within the anti-money laundering framework contained in laws that regulate activities of banks and credit institutions on the national level.

II Registrant’s bank – Registrar’s bank

SWIFT or IBAN standards applicable to international bank transfers and requiring provision of personal identification data to the receiving bank.

The particular FATF 40+9 recommendation that the receiving bank must make sure that the paying bank complies with the personal identification requirements.

The “chain of trust” between the registrant and the registry II

III Registrar's bank – Registrar

Contract concluded between the registrar's bank and the registrar.

Contract concluded between the registrar and the registry (Estonian Internet Foundation), including guarantee deposits and contractual penalties.

IV Registrar – Estonian Internet Foundation

Contract concluded between the registrar and the registry (Estonian Internet Foundation), including guarantee deposits and contractual penalties.

Modified EPP protocol enabling addition to the query of a copy of the bank’s account statement / payment order and its communication to the registry simultaneously with domain registration.

DNSSec and identified registrants

1. DNSSec creates a chain of trust between the Internet-user and registry.

2. Accurate WHOIS data with registrants identified enables to create a chain of trust between the registry and registrant – private person or legal entity

3. Connecting these two chains of trust creates a chain of trust between the Internet user and domain registrant, private person or legal entity. WHOIS with identified registrants lengthens the DNSSec chain of trust to private person or legal entity responsible for use of the specific domain name.

Thank You!

Questions ...

marek-andres.kauts@internet.ee