

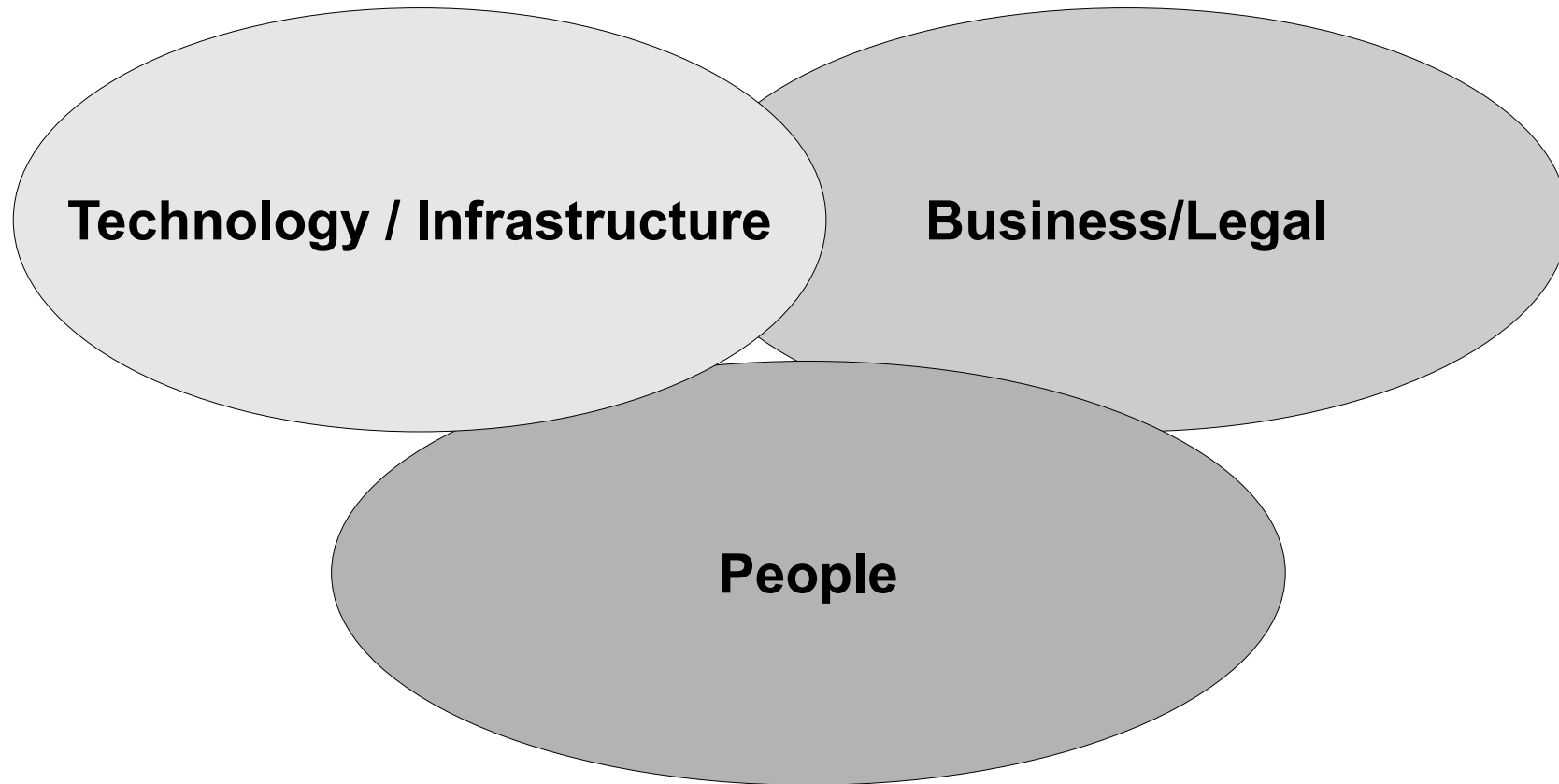
Best Practices for Secure ccTLD Registry Environment

ICANN Tech Day
June 21th, 2010

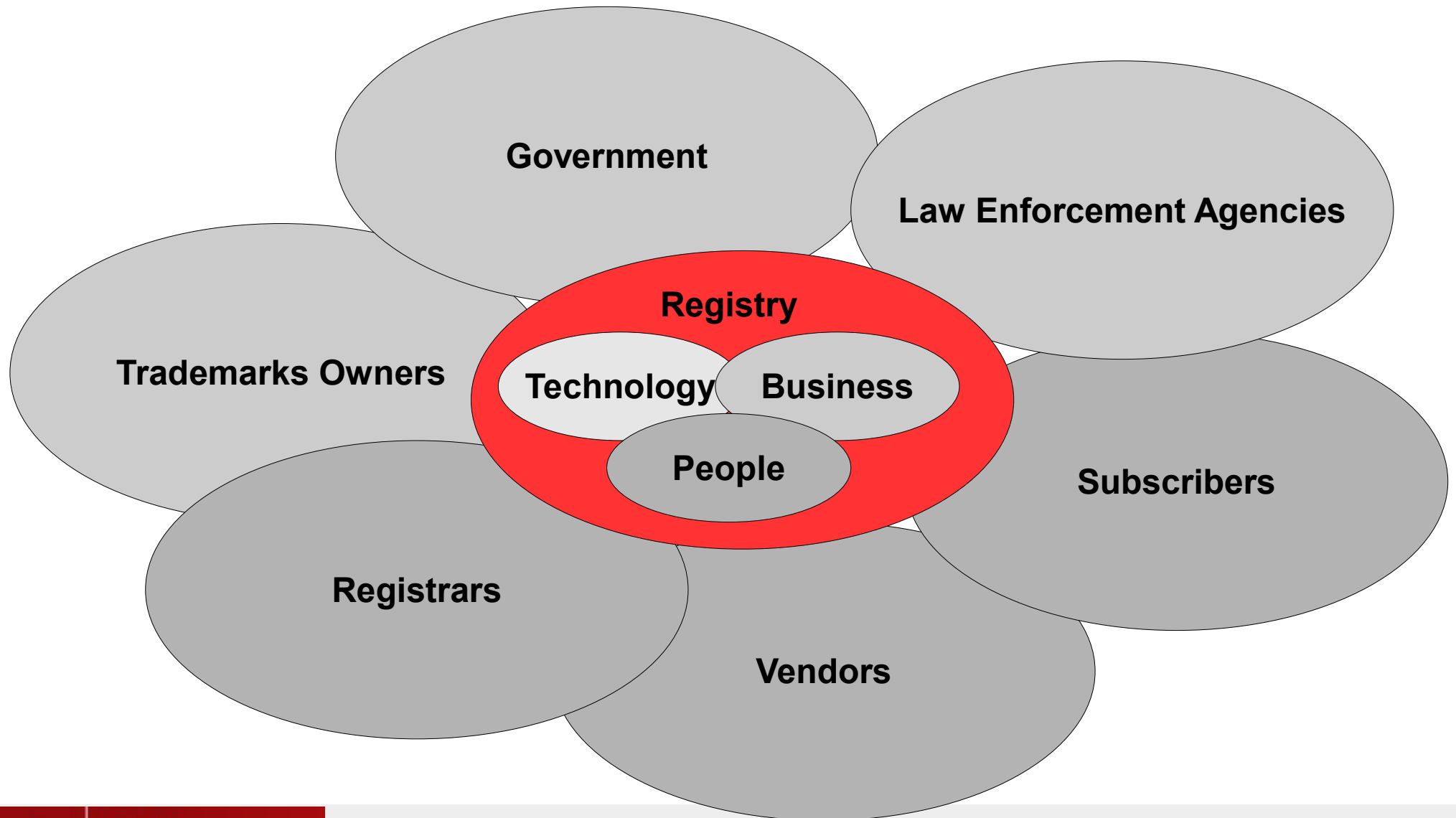
Dr. Andrzej Bartosiewicz



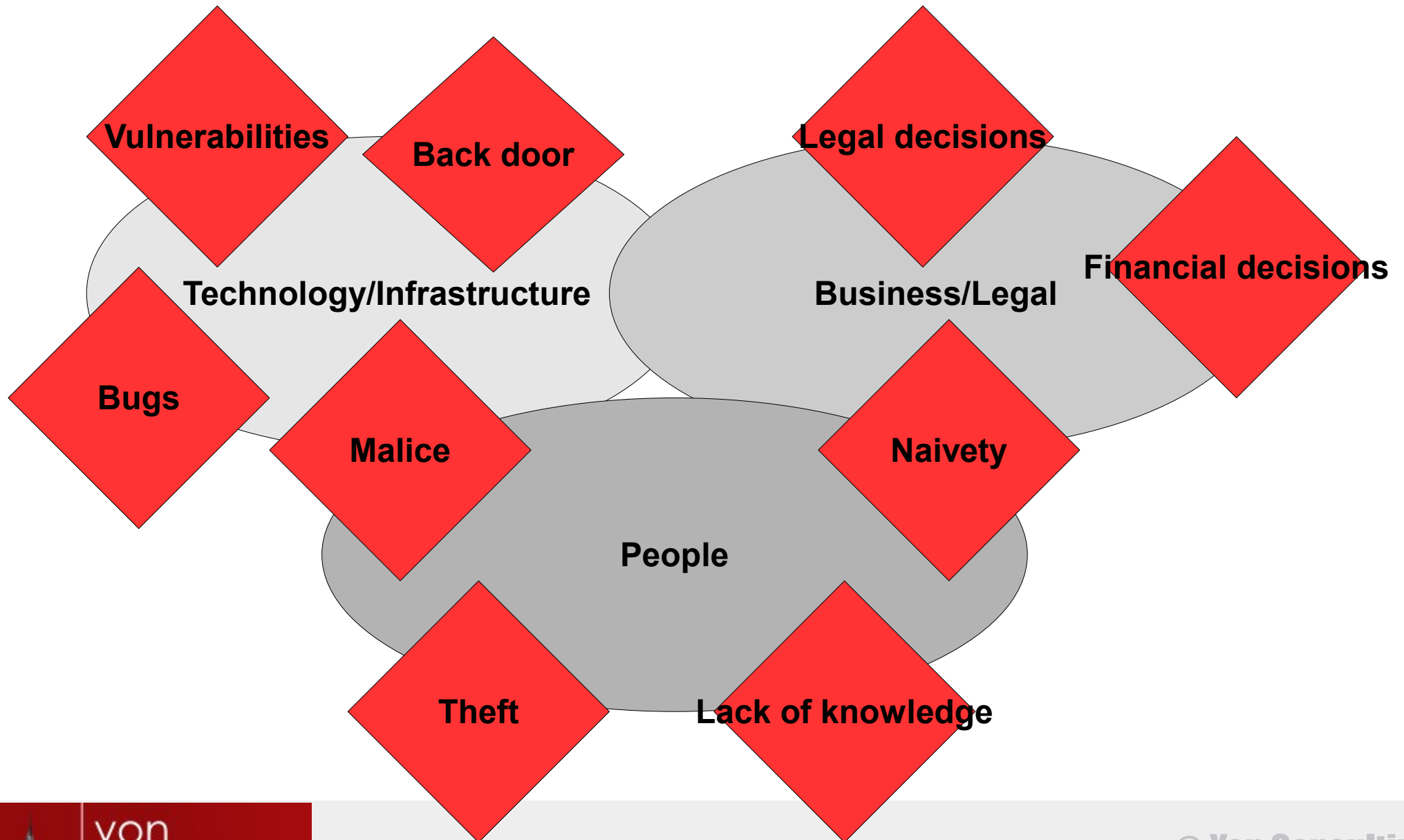
ccTLD- Environment



ccTLD-Environment



ccTLD-Environment - Threats



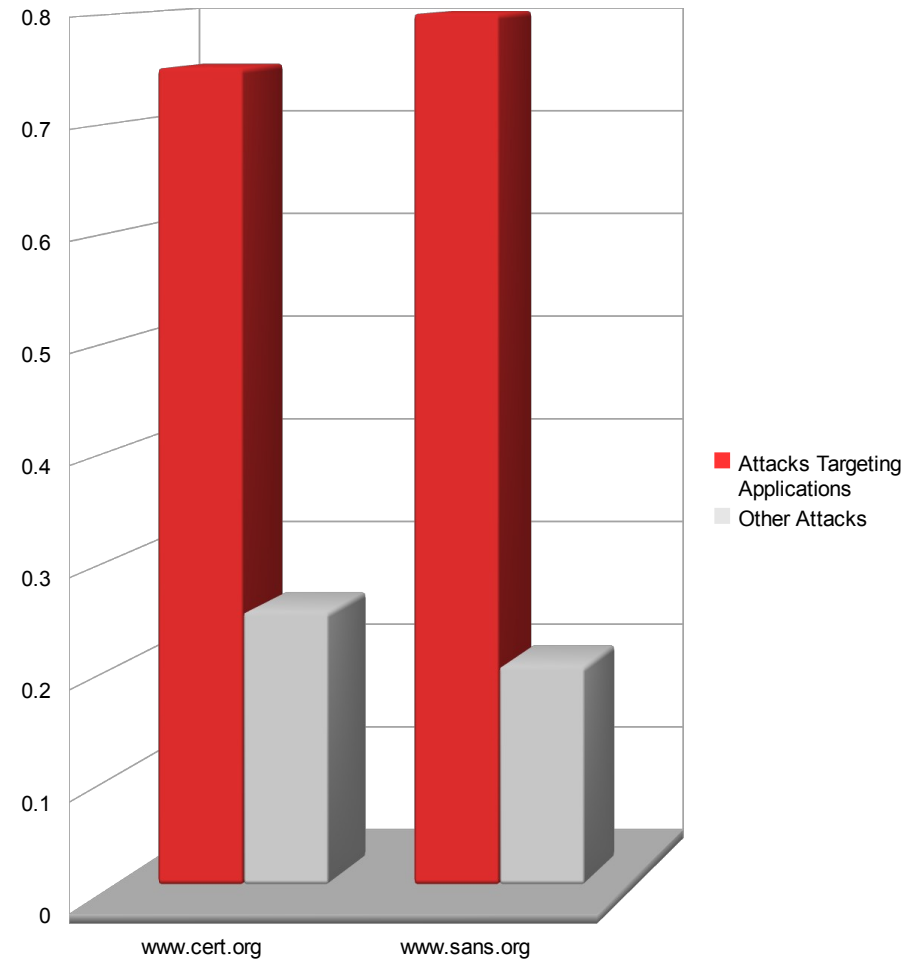
ccTLD-Environment

Technology / Infrastructure



Technical Aspect

- Application
- App/web servers
- OS
- Network
- Hardware



Application Weaknesses – Sources

- Lack of knowledge
 - Developers not aware about security (and other) issues
 - High rotation of developers
 - Many freshmen developers
 - Changing technologies
- Complexity of software development
 - Changing requirements
 - Size of a codebase
 - Growing technology stack
- Malice or laziness

Application Weaknesses

- Bugs
 - Correctness (internal incorrect execution)
 - Security vulnerabilities (external attacks)
- Bad practices
 - Performance bottlenecks (certain characteristics reveal useful information to attackers and/or allow for certain attacks)
 - Low maintainability (in long term leads to more bugs)
- Backdoors
 - 3rd party (e.g., illegal access/data gathering)

Example: SQL Injection



OH, DEAR — WHAT HAPPENED ?



OH, YES!
COOL, ISN'T IT?

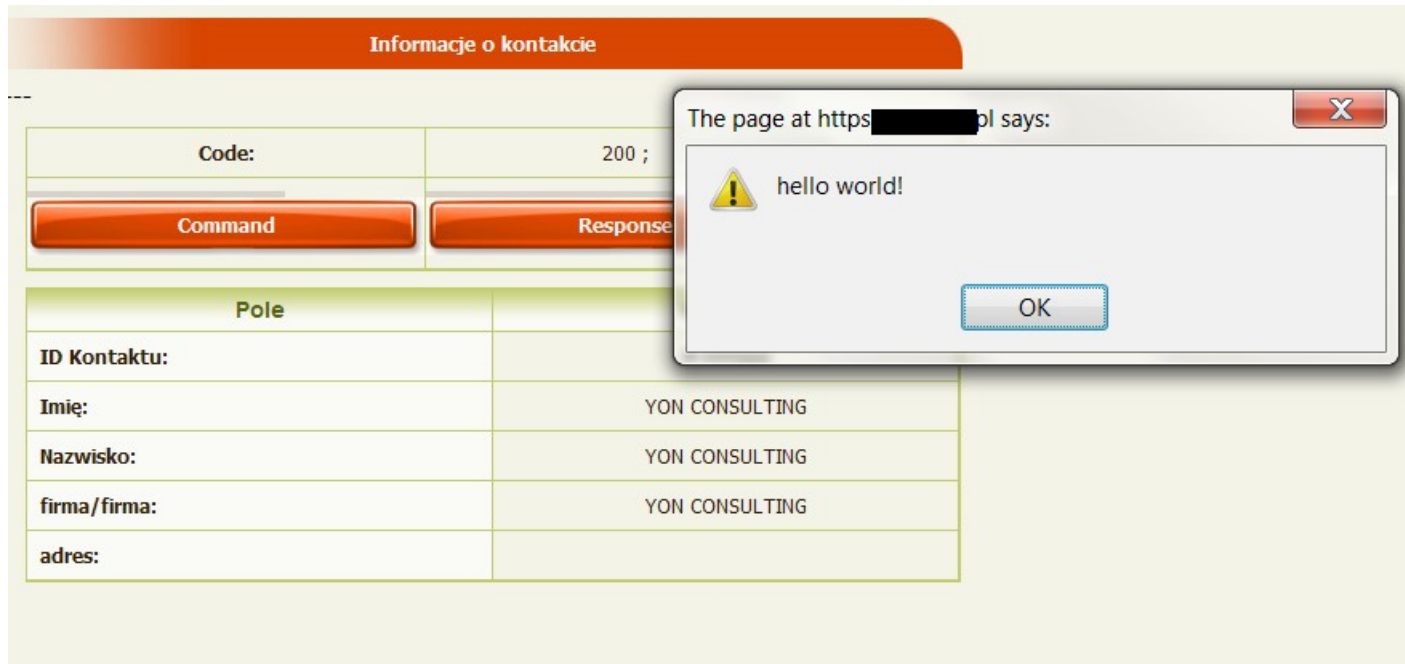


Case Study: XSS

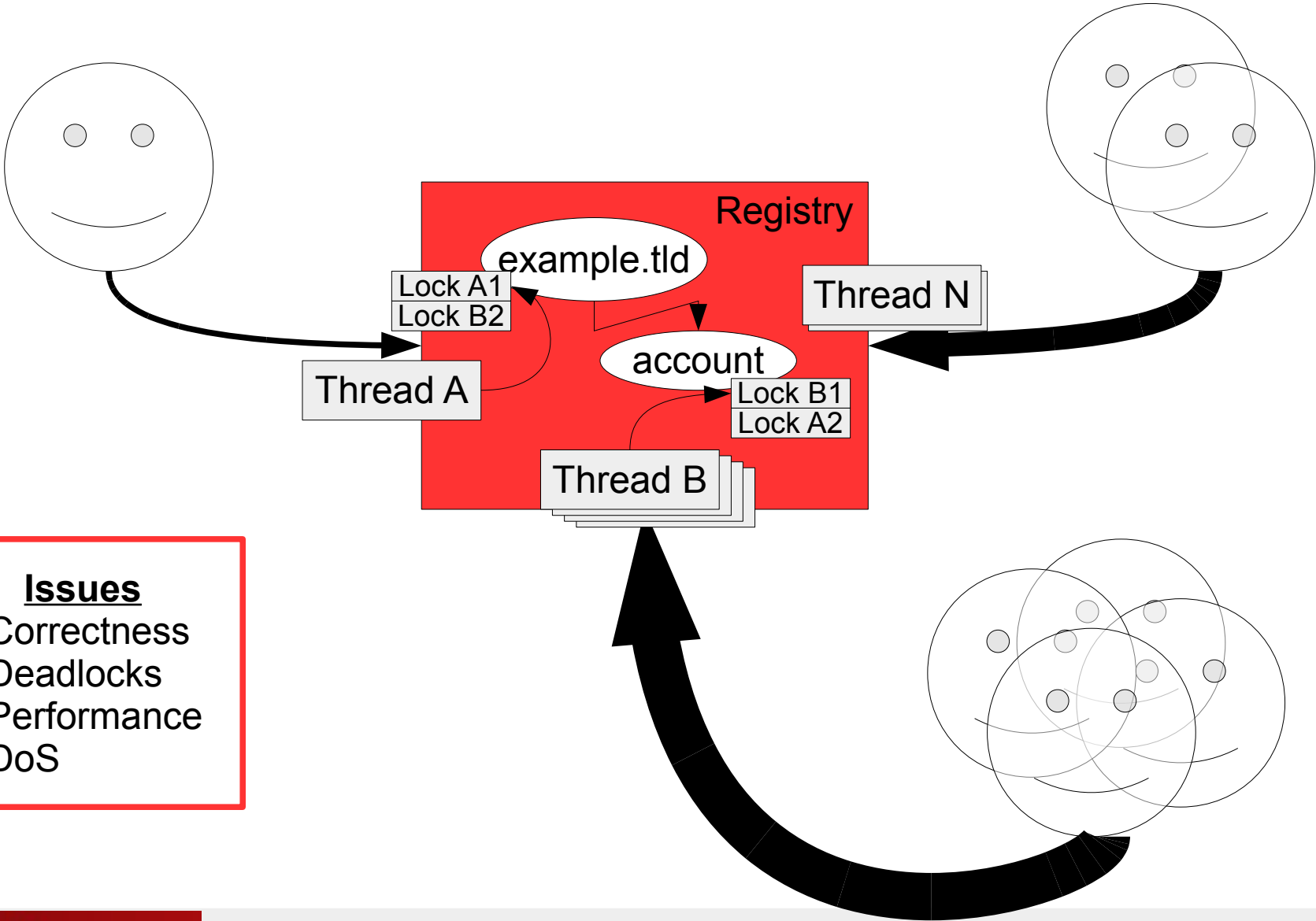
- XSS – well known vulnerability; well known methods for validation, escaping and filtering.
- Case Study: 5 TLDs and 5 Registrars checked against XSS
- Results
 - 1 TLD allowed Java Script to be injected into (WHOIS) database (no B2B-input sanitization),
 - 1 TLD allowed some fields to contain Java Script (partial B2B-input sanitization),
 - 3 of 5 Registrars allowed Java Script injection (to be stored in database, transferred to Registries as well as executed).

Example: XSS

- JavaScript entered in address field
- `<script> document.write('Hello world!') </script>` OR
- `<script> document.write('Hello world');
</script>`



Example: Concurrency/DB Issues



Example: Performance Bottleneck

- A function runs long and/or locks a domain
 - A dns-check inside a database transaction
 - Heavy processing inside a database transaction (e.g., addition/removal of many objects)
- A drop-catcher uses the issue to block other drop-catchers and increase his own chance to win
 - Unfair
 - DoS

Case Study: Backdoor

- A company suspects a backdoor
 - The first signal raised by IPS (Intrusion Prevention Systems)/IDS (Intrusion Detection Systems)
 - Oracle Forms, PL/SQL
- Manual analysis confirms the backdoor
 - The softwarehouse 'fixes' the issue
- Manual analysis reveals that the backdoor code only moved to another place
 - The softwarehouse tried to hide it was only a movement!
- What to do?
 - The entire codebase over a million lines of code

Traditional Best Practices

- Education
 - Advanced training – dedicated, expert training courses, coaching sessions, workshops.
- Software development process
 - More and more tests: Test-Driven Development (TDD), unit tests, integration tests, performance tests.
 - Continuous integration (and automated execution of tests).
- Independent verification
 - Audits: blackbox testing, code audits

Is This Enough?

Problems

- (1) Size does matter! (complexity of software development)
- (2) Program testing can be used to show the presence of bugs, but never to show their absence!

-- E. Dijkstra

Solution

Think? Why think! We have computer to do that.

-- J. Rostand

Automated Tools

- Automated testers
 - Generate test data and test suites
 - Scan applications e.g., web applications
- Tools to analyze sources, binaries without execution
 - Static analysis
- Tools to analyze execution of a program
 - Dynamic analysis

What Can The Tools Find?

- Code-level issues
 - Infinite loops, memory leaks, incorrect API usage, ...
- Security vulnerabilities
 - Injection, XSS (Cross-site scripting), XRSF (cross-site request forgery), buffer overflow, privacy violation, ...
- Multi-threaded issues
 - Deadlocks
- Innovative approaches
 - Semantic bugs, architectural and design issues
 - Transactional/database issues, algorithmic issues, performance issues...

Automated Tools – Examples

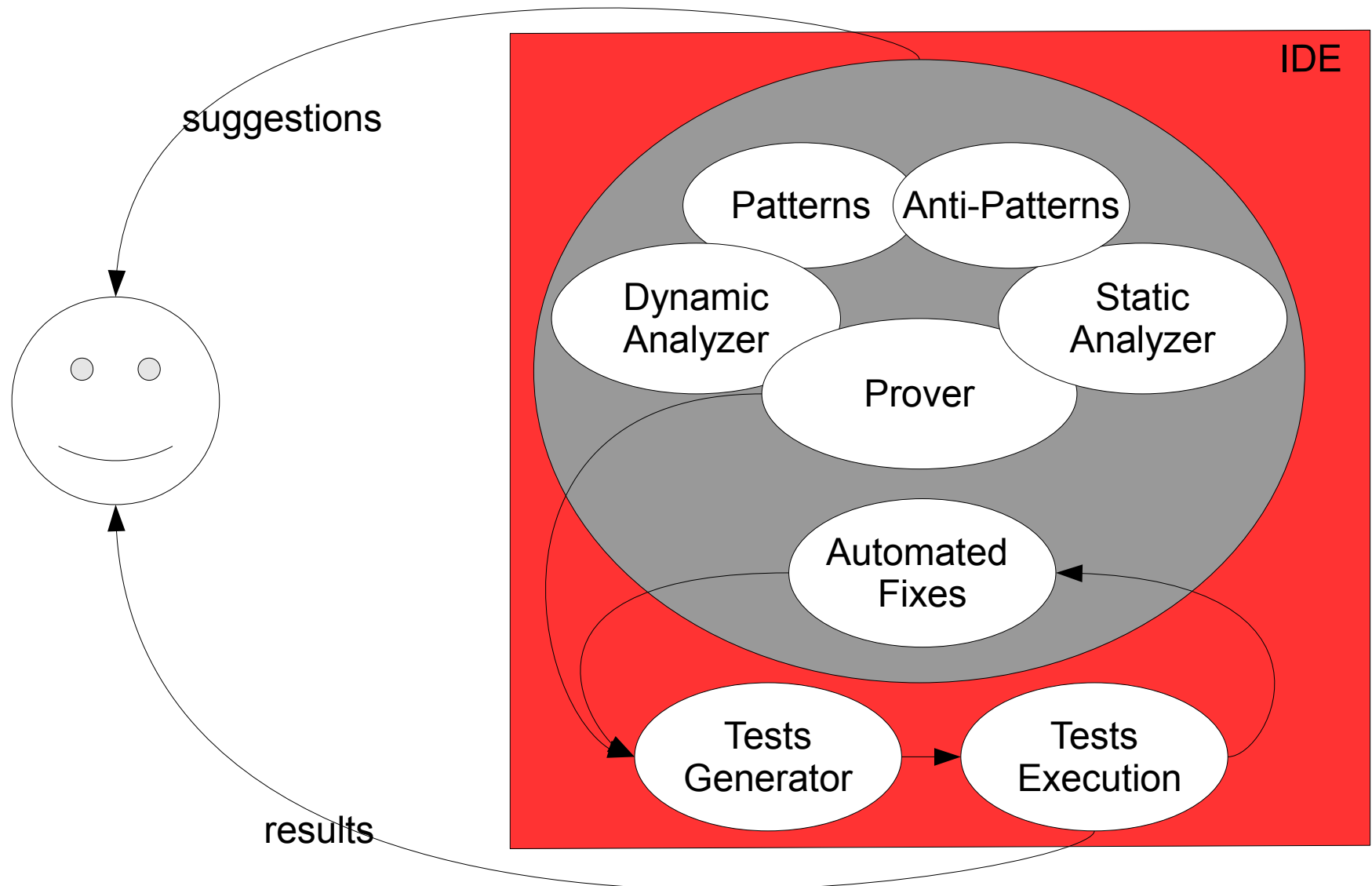
- Free

- FindBugs, Jlint, PMD, CheckStyle, WebScarab, CodeCrawler, Orizon, O2
- ...

- Commercial

- Fortify, Coverity, Klockworks, Ounce Labs (IBM), Veracode
- Yonita, release Oct. 1st
- ...

Automated Tools – The Future



ccTLD-Environment

People

Employees, Management, Contractors



Employees - Threats

- Key potential threats related to the human factor:
 - **Lack of knowledge / experience** (bad decisions, mistakes) of the employees.
 - **Disgruntled current and ex-employees** (revenge, money).
 - **Social Engineering (phishing).**
 - Management without external tight control (financial loses, corruption etc.).
 - Stolen/lost documents, laptops, pen-drives.

Lack Of Knowledge / Experience

- Employees without proper training or education.
- Administrative decisions based on not-verified documents or just on information gathered from phone conversations.
- Too complicated or not updated frequently procedures/instructions resulting in employees disregarding procedures.
- Work overload.



Lack Of Knowledge / Experience - Remedy

- Continuous trainings for the staff.
- Well defined and proved procedures and workflows.
- Up-to-date Knowledge Base + access for the employees.
- Well defined roles and responsibilities including escalation process.
- Staff monitoring, Quality assesment.

Social Engineering (Phishing)

- Wikipedia defines it as: *"is the act of manipulating people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information **gathering, fraud, or computer system access**"*
- Different ways to conduct attack: phone (including vishing), e-mail, web (using man-in-the-middle, tabnabbing), fax or in-person (not likely).
- Attack targeted on the employees on **all levels** and responsibilities (call centers, technical support and managerial staff). One of the techniques is based on the fact that we want to appear well-informed about our professional specialty.

Social Engineering (Phishing)

- TLD Registry is in the **unique situation** and can be target of phishing attack in **4 different ways**:
 - Employees of the Registry can be target of attack to gather information or execute some actions by the Registry.
 - Registrars (ccTLD Partners) can be targetted and indirectly data in the Registry database(s) stolen or compromised.
 - Domain holders can be targetted by Phishers „impersonating” Registry.
 - Domain Names can be used for Phishing.
- ccTLD Registry **must address** all four aspects of Phishing

Social Engineering - Remedy

- Educating employees / contractors about the value of information.
- Dedicated **trainings** of how Social Engineering operates and how to protect data.
- Continuous / repetitive quick-courses or remarks.
- Well defined procedures defining roles and responsibilities of employees.
- User's credentials not allowing certain actions if not part of day-to-day duties – requires escalation but safeguards TLD.
- Additional confirmation (from higher rank employee) required for certain actions.

Social Engineering: Baidu.com Has Been Hijacked

Via Registrar's Support On January 12, 2010

Gross Negligence Surfaces in Baidu Domain Hijacking Incident
Register.com employee accused of failing to enforce security checks:

a member of the Iranian Cyber Army contacted Register.com tech support via an online chat system and posing as a Baidu employee. The imposter proceeded to request the change of the contact e-mail address for the baidu.com domain. The Chinese company claims the attacker failed to provide correct identification information, but the Register.com staffer initiated the procedure either way.

Incredibly, Defendant thus changed e-mail address on file from one that was clearly a business address and contained the name of the account owner, to an e-mail address that conveyed a highly politically charged message ('antiwahabi'), with the domain name ('gmail.com') of a competitor of Baidu <http://news.softpedia.com>

Turkish Hacker Hijacks Hotmail.co.il and MSN.co.il on June 10th, 2010

It appears that the two Microsoft domains, which normally redirect users to login.live.com and il.msn.com, respectively, had their name server information altered.

The new ns1.dollar2host.com and ns2.dollar2host.com name servers, which belong to a private Web hosting company, replaced the usual ns1.msft.net and ns2.msft.net that Microsoft used for its domains.

It seems the attacker also managed to get the administrative e-mail address registered for the domains changed. The whois record for msn.co.il currently lists an @hotmail.com address, which is clearly not related to Microsoft, the Redmond giant normally using a standard @microsoft.com one for such purposes.

Disgruntled Current And Ex-Employees

- Two different reasons: malice or theft.
- (ex-)Employees may steal (copy), delete, encrypt (!) or alter data in the company's databases.
- Employees can also change credentials/passwords before they leave.



Disgruntled Current And Ex-Employees - Remedy

- Monitor all activities
- Log on all activities, do not let logs to be removed by superuser.
- Users' access and privileges:
 - Start with smallest possible privileges including technical staff.
 - Expand privileges only if necessary.
 - Remove privileges if someone leaves the company etc.
- Never give administrative privileges if not necessary.
- Organize trainings dedicated to corporate rules and legal staff.

Former Employee Steals Data

Data surrounding up to 24,000 client accounts was stolen by a former technology expert from HSBC's Swiss subsidiary, the bank has admitted. Former-HSBC employee steals data for 24,000 accounts.

Hervé Falciani, an IT specialist at the Geneva branch, is thought to have committed the theft three years ago.

The crime, which was discovered during 2009, affected accounts opened before October 2006, 9,000 of which have subsequently been closed, the bank announced.

<http://www.bobsguide.com>

To High Privileges: IT Consultant Gets 5 Years For Plundering \$2m

contractor who provided IT administration services to banks was sentenced to more than five years in prison this week after admitting he used his insider knowledge to plunder some \$2m from four financial institutions.

"Because of my position in upgrading the software, I was able to carry out this scheme without detection for nearly two-and-a-half years, from approximately August of 2006 until approximately April of 2009,"

<http://www.theregister.co>



Fired Director Of IT Accused Of Destroying Organ Donor Information Of Former Company

A former technology director who was fired from a regional organ donation center in Texas has admitted to breaking into her former employer's network and destroying more than \$94,000 worth of data. She illegally accessed the network of LifeGift just hours after bosses told her she was terminated. From the evening of November 7 through the following morning, she used a Dell laptop and her home broadband account to delete organ donation information and account invoices. She also nuked server logs in an attempt to cover her tracks.

LifeGift managers didn't disable Duann's virtual private network account and didn't change the login credentials of other employees, either. The failure made it possible for Duann to use her VPN account to reach the LifeGift network, and then use an administrator account belonging to another employee.

<http://www.theregister.co.uk>

ccTLD-Environment

Business



Business *Versus* Technology

- Broad range of business/legal decisions leading directly to software instability
 - Bad planning causes code complexity.
- Wrong communication between business/legal and software development.
- Time constraints leading to the insufficient testing.

Case Study: Landrush Of IDNs In .tel

- Registry implemented IDNs correctly, but some Registrars failed.
 - Registrant tries to register domain (in Cyrillic), going through the list of Registrars supporting IDNs for .TEL
- Registrar A doesn't support IDNs; Registrant gets information that domain is invalid (IDNA/Unicode), without further explanations.
 - Contact to CEO reveals that IDNs are not supported.
- Registrar B answers for all entered IDNs that domain is taken.
- Registrant C allows registration but domain becomes pending
 - After few hours waiting and contact with company, Registrant gets an answer that IDNs are supported excluding Cyrillic.

Contact

e-mail	info@YonConsulting.com
www	YonConsulting.com
contact	YonConsulting.tel

Follow us on Twitter @YonConsulting

