Cybersecurity in 2012-2015:

The new challenges to be faced by Registries and Registrars. How to profit from cyber security?

Dr. Andrzej Bartosiewicz

Yonita Inc., CEO

YONITA

4th International conference for ccTLD registries

Are YOU prepared for Cyber Attack?

Recent examples of cyber-attacks

11 August 2011 Last updated at 10:05 GMT

Hong Kong share trading hit by hackers

Trading in seven stocks listed on the Hong Kong stock exchange was suspended on Wednesday after a hacking attack.

The attack was aimed at a website run by the exchange used to tell traders about company announcements.

The site was shut and trading in seven firms due to make announcements via the website was suspended for half a day.

Several stock exchanges have been hit by hackers in 2011

Shares in HSBC, Cathay Pacific, China Power International and the Hong Kong exchange itself were among those suspended.

Cyber crime, cyber terrorism and cyber warfare

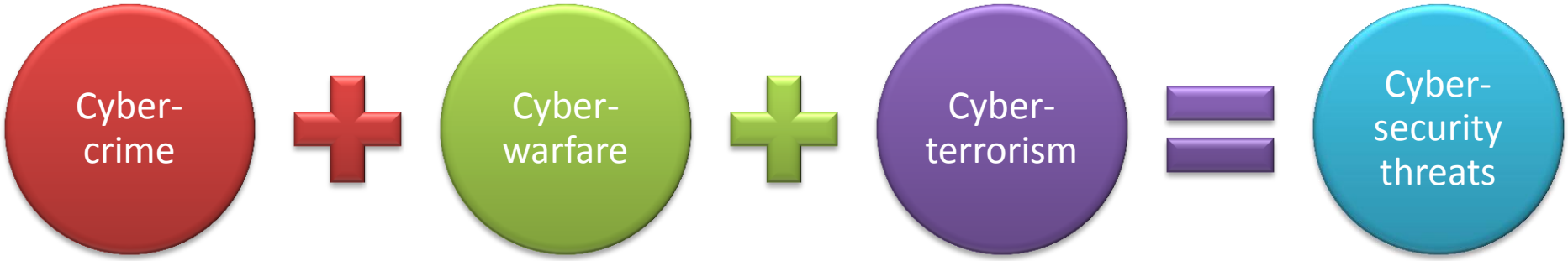
Types of the cybersecurity threats

CYBERSECURITY THREATS

YONITA

4th International conference for ccTLD registries

Hacking is a “pure” criminal activity only?



criminal activity: most common activity today, in most cases concealed;

cyberwarfare: probably already in place; some countries already prepared to launch cyberattack on enemy’s infrastructure

cyberterrorism: already in place, developing fast and become more and more dangerous in upcoming years

Cyber-crime

- **Cybercrime** is any criminal act committed by a person with knowledge of computers who uses this information to accomplish acts of identity theft, intellectual property theft, terrorism, vandalism, credit and debt card fraud, and other forms of computer-related crimes.
- Hacking is defined as **intentionally** accessing a computer **without authorization** or exceeding authorization in order to access restricted information.

Cyber-terrorism

- **Cyber-terrorism** is a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in **violence, destruction and/or disruption** of services to create **fear** by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda.

FEDERAL GOVERNMENT, THE FBI

Cyber-warfare

- **Cyberwarfare** - Actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption

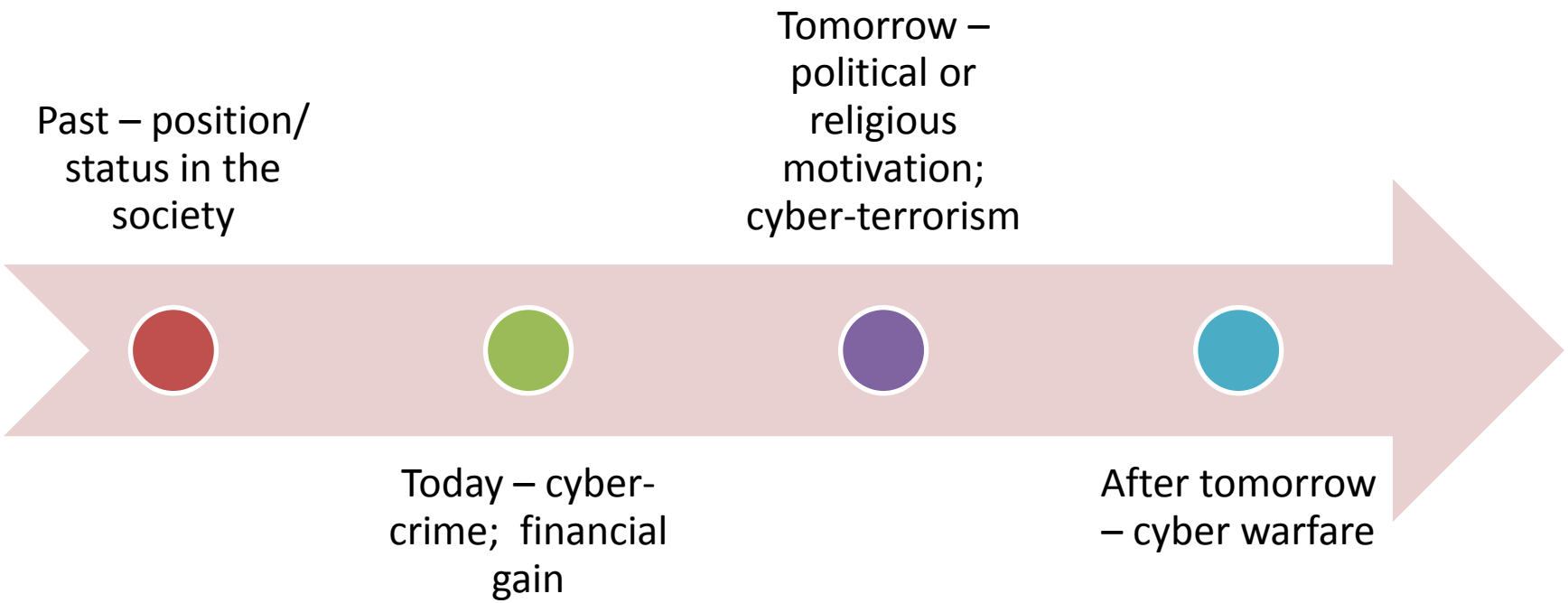
RICHARD A. CLARKE

- Cyberwarfare refers to politically motivated (and sponsored) hacking to conduct sabotage and espionage.

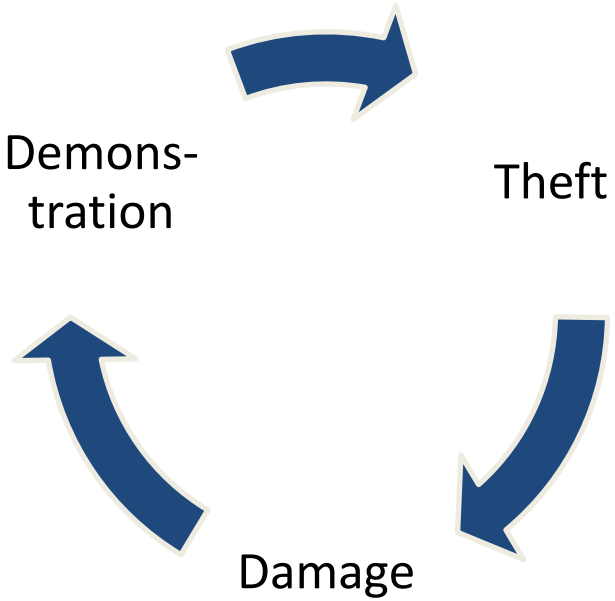
Cyber-warfare example: Stuxnet, Iran

- Highly specialized malware payload; designed to target only Siemens **SCADA** systems that are configured to control and monitor specific industrial processes.
- Stuxnet appears to be designed to sabotage the **uranium enrichment facility** at Natanz by destroying centrifuges (device performing isotope separation). Stuxnet may have physically destroyed up to 1000 centrifuges (10 percent)
- "serious nuclear accident" occurred at the site in the first half of 2009
- *"They succeeded in creating problems for a limited number of our centrifuges with the software they had installed in electronic parts."* MAHMOUD AHMADINEJAD

Cyber-attacks: evolution



Slide partially based on Dr. Paul Wagner's presentation



SOURCES, OBJECTIVES, MOTIVATION AND TOOLS

Threat sources

- **Hackers and Crackers** (individuals who illegally break into other computer systems to damage the system or data, steal information, or cause disruption of networks for personal motivations - monetary gain or status)
- **Criminals** (individuals or gangs who illegally break into other computer systems primarily for financial gain)
- **Terrorist activity** (unlawful destruction, disruption, or disinformation of digital property to intimidate or coerce governments or societies in the pursuit of goals that are political, religious or ideological)
- **Governments**
- **Industrial espionage** (discover proprietary information on financial or contractual issues, or to acquire classified information on sensitive research and development efforts)
- **Insiders** (disgruntled employees working alone to use their access to compromise the system)

Objectives of Cyber Attack

- **Loss of Integrity** (corrupted data, lost data)
- **Loss of Availability** (loss of system functionality and operational effectiveness)
- **Loss of Confidentiality** (unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization)
- **Theft** (information stolen especially financial or personal data, R&D documents)
- **Physical Destruction** (ability to create actual physical harm or destruction through the use of IT systems; i.e. SCADA systems)

Motivation

- Financial
- Non-financial

Motivation

- Challenge, ego, “fame”
- Illegal information disclosure, blackmail
- Monetary gain
- Unauthorized data alteration
- Destruction of information, exploitation and revenge
- Sabotage (to gain competitive advantage)
- Industrial or corporate espionage
- Government led intelligence and economic espionage

Tools of Cyber Attacks

- Infrastructure is targeted:
  - Service flooding - Distributed Denial of Service Attack (DDoS)
  - Vulnerabilities detection + system intrusion / break-ins
  - Backdoors
  - Trojan horses and viruses
  - Botnets
  - 3rd party infrastructure is targeted (example: domain hijacking, DNS hijacking)

- Humans are targeted:
  - Social engineering: Phishing & E-mail Spoofing
  - Blackmail or physical assault on an employee

Tools of Cyber Attacks

example: Phishing

- using social methods to infect users with non-vulnerability based malware (such as Trojans and keyloggers) or to steal user privileged information by requesting the user to provide it and making the user believe they are surfing a genuine site.

Tools of Cyber Attacks

example: domain hijacking

Domain hijacking or **domain theft** is the process by which registration of a currently registered domain name is transferred without the permission of its original registrant, generally by exploiting a vulnerability in the domain name registration system.

Register.com settles Baidu domain hijacking lawsuit

Kevin Murphy, November 25, 2010, 14:28:53 (UTC), Domain Registrars

Register.com has apologised to Chinese portal company Baidu for allowing its domain, baidu.com, to be hijacked by the Iranian Cyber Army hacker group.

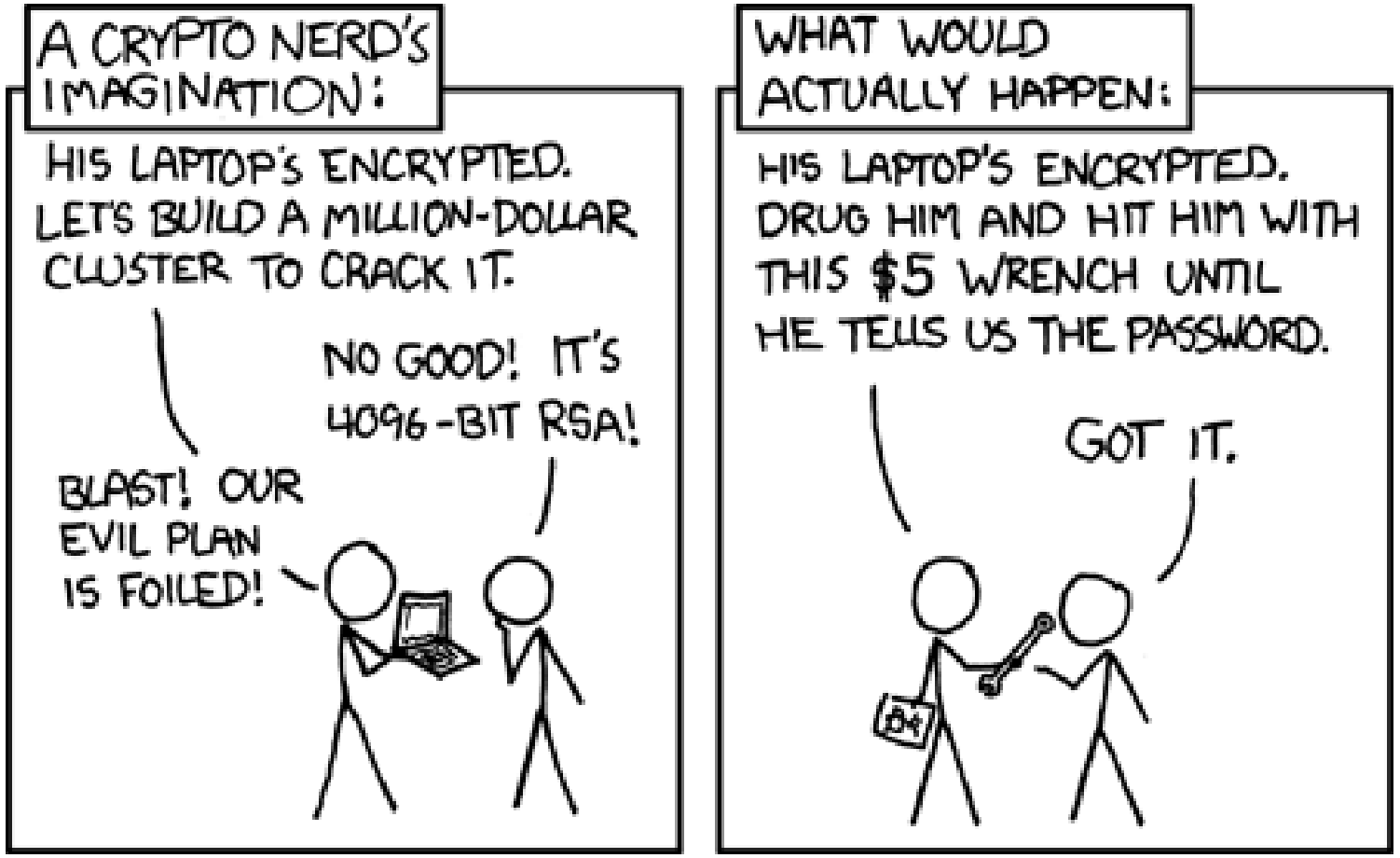
If Baidu's complaint was to be believed, the hackers took over baidu.com with a trivial social engineering attack that relied upon a Register.com tech support employee being asleep at the wheel.

The company is one of China's largest internet firms, employing over 6,000 people and turning over well over $600 million a year. But for the period of the hijack, visitors to baidu.com instead just saw the hackers' defacement message instead.

The registrar had argued in court that its terms and conditions released it from liability, but the judge didn't buy it.

> After an internal investigation, we found that the breach occurred because Register's security protocols had been compromised. We have worked with United States law enforcement officials and Baidu to address the issue. We sincerely apologize to Baidu for the disruption that occurred to its services as a result of this incident.

YONITA



http://imgs.xkcd.com/comics/security.png

Are you using **TWO-MAN RULE** in your infrastructure? The two-man rule is a control mechanism designed to achieve a high level of security for especially critical material or operations. Under this rule all access and actions requires the **presence of two authorized people at all times.**

Critical Infrastructure

Roles of the Registry

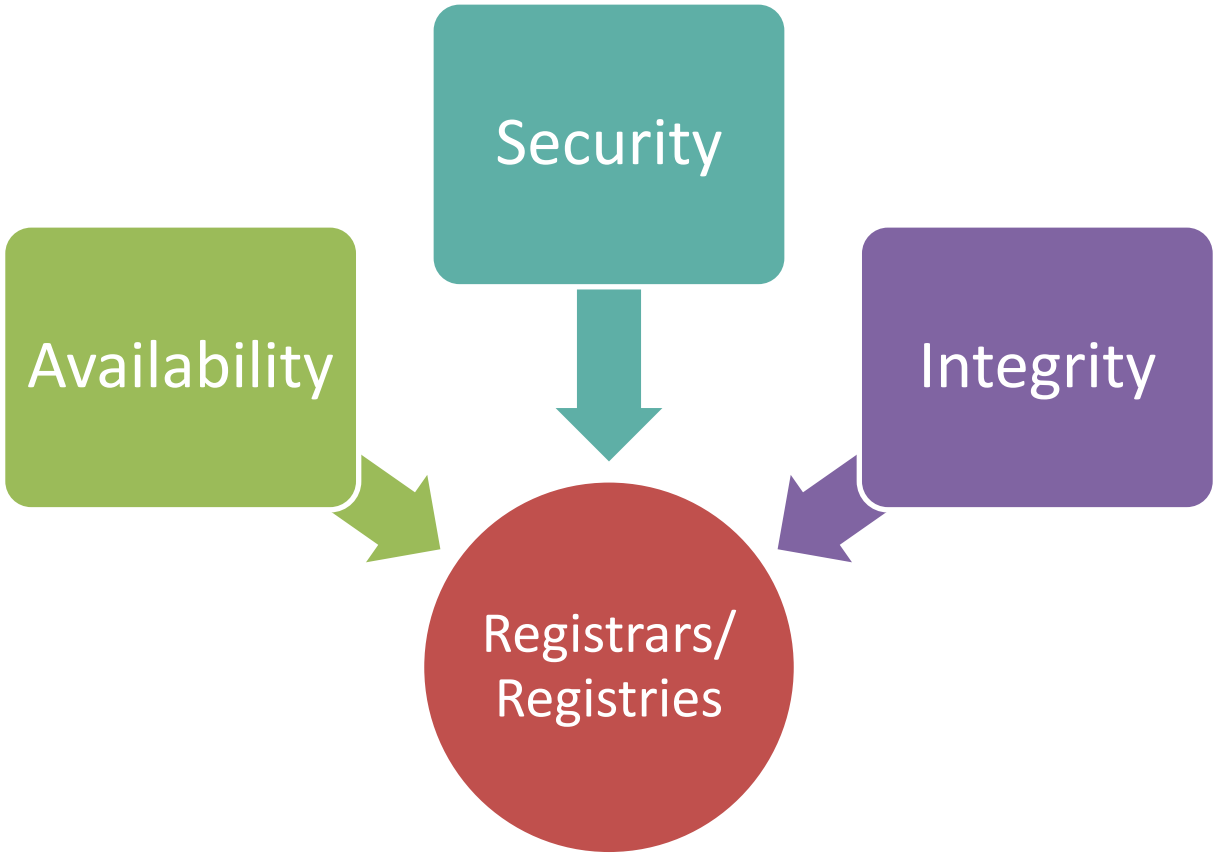
Roles of the Registrars

CHALLENGES FOR REGISTRIES AND REGISTRARS

YONITA

4th International conference for ccTLD registries

Expectations from Registrars and Registries



Roles of the Registry

Protect DNS	• from DDoS attacks on the whole zone • from DNS spoofing of individual zones (domains)
Protect data (users, domains, financial)	• from loss of internal integrity of data • from attacks targeted to steal data • from domain hijacking
Protects from outages	• from natural disasters and industrial catastrophes

Roles of the Registrars

Protects data (users, domains, financial)

- from loss of internal integrity of data
- from attacks targeted to steal data
- from domain hijacking

Protects from outages

- from natural disasters and industrial catastrophes

Necessary costs of Cybersecurity

	Registrars	ISPs	Registries
DNS robustness, stability and ANYCAST		$	$$$$
Monitoring (data integrity + service availability)		$$	$$$$
DNSSEC	$	$	$$$$
Data protection: Infrastructure & software	$	$$	$$$$
Availability: protection from outages	$	$$	$$$$

YONITA

4th International conference for ccTLD registries

Challenges to be faced by both Registries and Registrars

Intensified Hacker attacks to:

- Steal personal data
- Take control of domain names to disrupt business or use hijacked domains for unlawful purposes
- Disrupt services (locally)

Cybererrorism:

- Cyberterrorism should be perceived as threat by Registries. Attack on the country's infrastructure can be combined with attack on the TLD Registry.

SECURITY - COST OR OPPORTUNITY?

Are YOU prepared for…
making money on security?

Cybersecurity in upcoming years – just the cost or business opportunity?

- For most domain registrants (doman holders), cybersecurity of their domains, on-line applications and web-pages, technical infrastructure is only the necessary cost.
- For Registrar and Registries cybersecurity can be both cost and the business opportunity.

Today, most Registries and Registrars miss the opportunity to make revenue on the additional security for domain name holders.

Business opportunities in upcoming years for…

	Registrars	Registries
WHOIS Privacy Protection	YES	NO
Domain Lock Services	YES	Maybe
DNSSEC support	YES	Maybe
SSL Certificates	YES	Maybe
Domains/URL Security Scanning - On-line application vulnerabilities	YES	YES
Domains/URL Security Scanning - Malware detection	YES	YES

Domains/URL Security Scanning -

On-line application vulnerabilities

- Web Scanner is aimed at detecting security vulnerabilities in web sites and online applications.
- example: **Yonita Web Scanner** performs dynamic verification of web applications based on automated tests generated by the Smart Test Generator and Randomized Data Generator.

.regia

photos, videos, music
ANKABOOT
عنكبووت
Connect and Share

az

YONITA

Provided by Registry

- Free service – whole zone scan
- Paid service through Registrars

Provided by Registrar

- Pay per scan

Domains/URL Security Scanning -

On-line application vulnerabilities

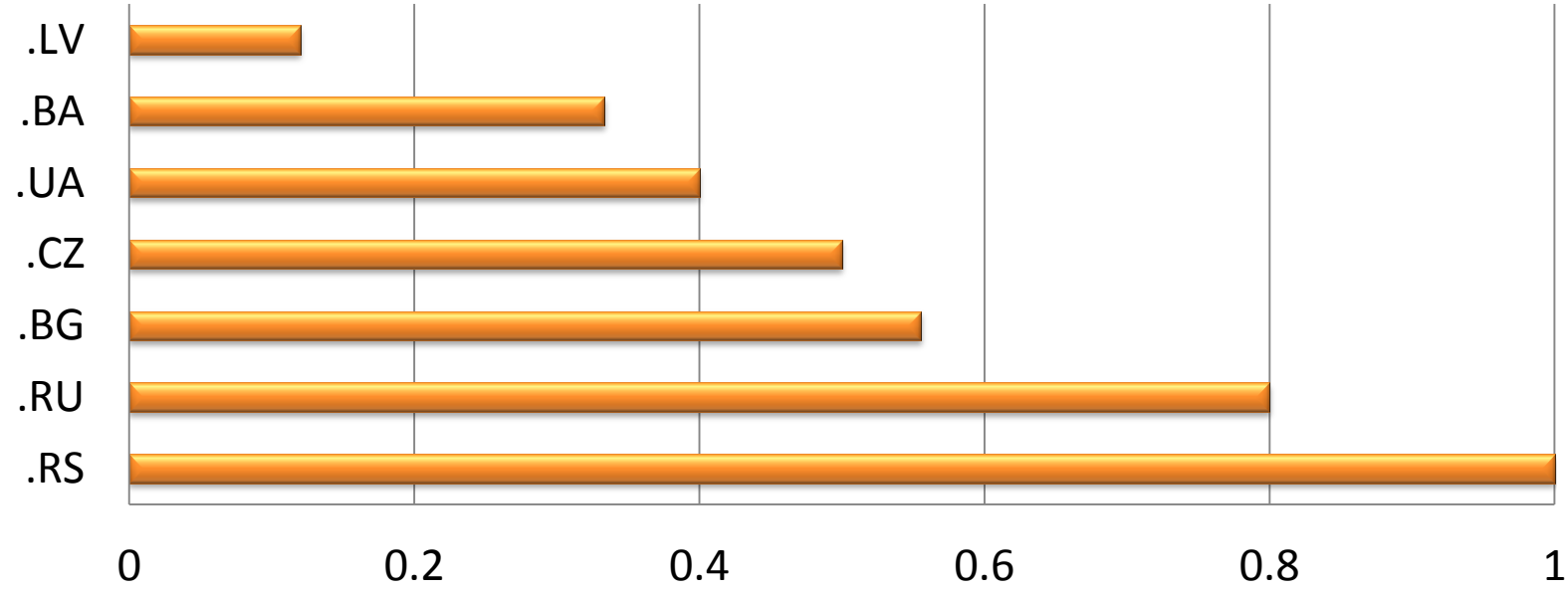
Defects in authentication and authorization	Defects in session management	Cross-site Scripting (XSS)	Cross-site Request Forgery
Defects in forward and redirect mechanisms	Content spoofing	Buffer overflow	Script injection
OS command injection	SQL injection	CRLF injection	Direct object references

YONITA

4th International conference for ccTLD registries

Domains/URL Security Scanning

CRITICAL VULNERABILITIES (TYPES) / DOMAIN*
August 2011



	.RS	.RU	.BG	.CZ	.UA	.BA	.LV
CRITICAL	1	0.80	0.56	0.50	0.40	0.33	0.12

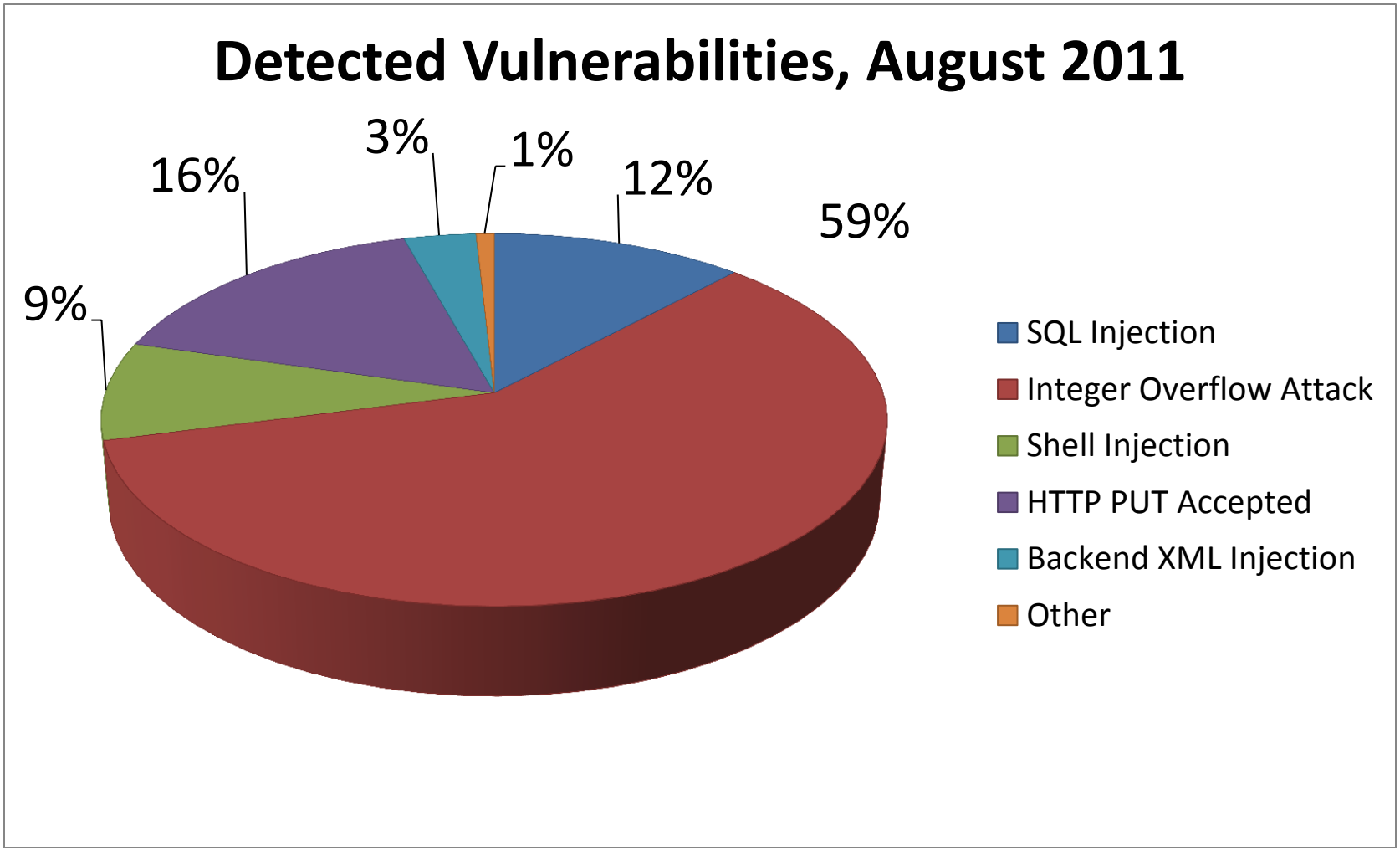
**) based on Alexa list, ccTLD domains only*

YONITA

Full report will be available @ end of September

4th International conference for ccTLD registries

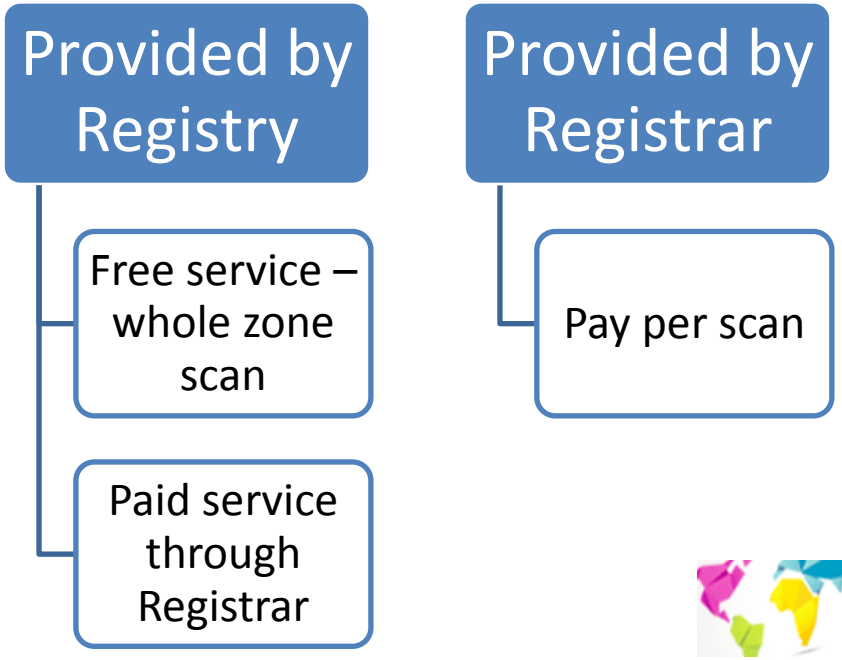
Domains/URL Security Scanning



Domains/URL Security Scanning –

Malware detection

- to help prevent websites from infecting other websites.
  - automatic malware scanning service with every domain name registration
- examples: McAfee agreement with .XXX ($8 million deal); VERISIGN MalDetector



YONITA

4th International conference for ccTLD registries

WHOIS Privacy Protection

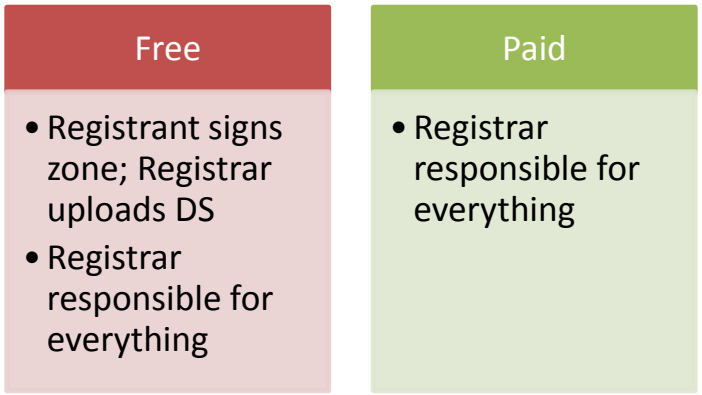
- A user buys privacy from the company, who in turn replaces the user's info in the WHOIS with the info of a forwarding service (for email and sometimes postal mail, done by a proxy server).
- Pricing: $4-$10/yr + processing fees (i.a. disputes)
- Providers: “Domain by Proxy” (GoDaddy), eNOM, WhoisGuard and many more
- Some TLDs (including XXX, US, CA, AG, CO.NZ, SE, TC, TK, TW, IT, JOBS, JP) do not allow WHOIS Privacy Protection

Domain Lock

- Domain Lock is a **status code** that can be set on an Internet domain name by the sponsoring registrar of the domain name to prevent unauthorized, unwanted or accidental changes to the domain name.
  - The Extensible Provisioning Protocol (EPP) specifies both client (registrar) and server (registry) status codes that can be used to prevent unintended registry changes: *Delete, Transfer and/or Update*
- Types:
  - Registrar Lock: usually free of charge; protects against accidental transfers/deletions; no real protection; *high volume/low value*
    - all gTLDs, many ccTLDs
  - Registry Lock: more secure, required additional secure, authenticated process (i.a. manual); *low volume/high value*
    - examples: .COM, .AF, .CX, .GS, .GY, .KI, .NF, .NL., .PR, .US and .TL

DNSSEC support

- DNSSEC is an addition to the Domain Name System (DNS) protocols; it is designed to add security to the DNS to protect it from certain attacks, such as any data modification attack (e.g. cache poisoning). It is a set of extensions to DNS, which provide origin authentication of DNS data, data integrity and authenticated denial of existence.
- Registry – provides the free of charge service through EPP
- Registrar:
  - Registrars can either pass Delegation Signer (DS) (the only correct approach from security point of view) only or complete the whole process of keys generation and signing (less secure but easier to sell)
  - Can be offered for free or as a part of the paid service (like GoDaddy's "Premium DNS Account")



Dr. Andrzej Bartosiewicz, CEO of Yonita Inc.

Ph.D. in Informatics, Warsaw University of Technology. Expert in domain names, security and trademarks protection, telecommunication. Author of more than 200 publications and presentations.

Over 15 years of experience in the information and communication technology business, including 12 years of experience in senior managerial positions.

- Director and Chairman of CENTR (2006-2010).
- Rapporteur and Chairman of ITU-T in the field of “Internationalized Domain Names” (2005-2008)
- Head of .PL Registry (2001-2010)

Yonita.com
+1 650 249 3707
andrzej@Yonita.com

T: @bartosiewicz
FB: @abartosiewicz

Yonita, Inc.
800 West El Camino Real
Suite 180
Mountain View, CA 94040

YONITA

4th International conference for ccTLD registries