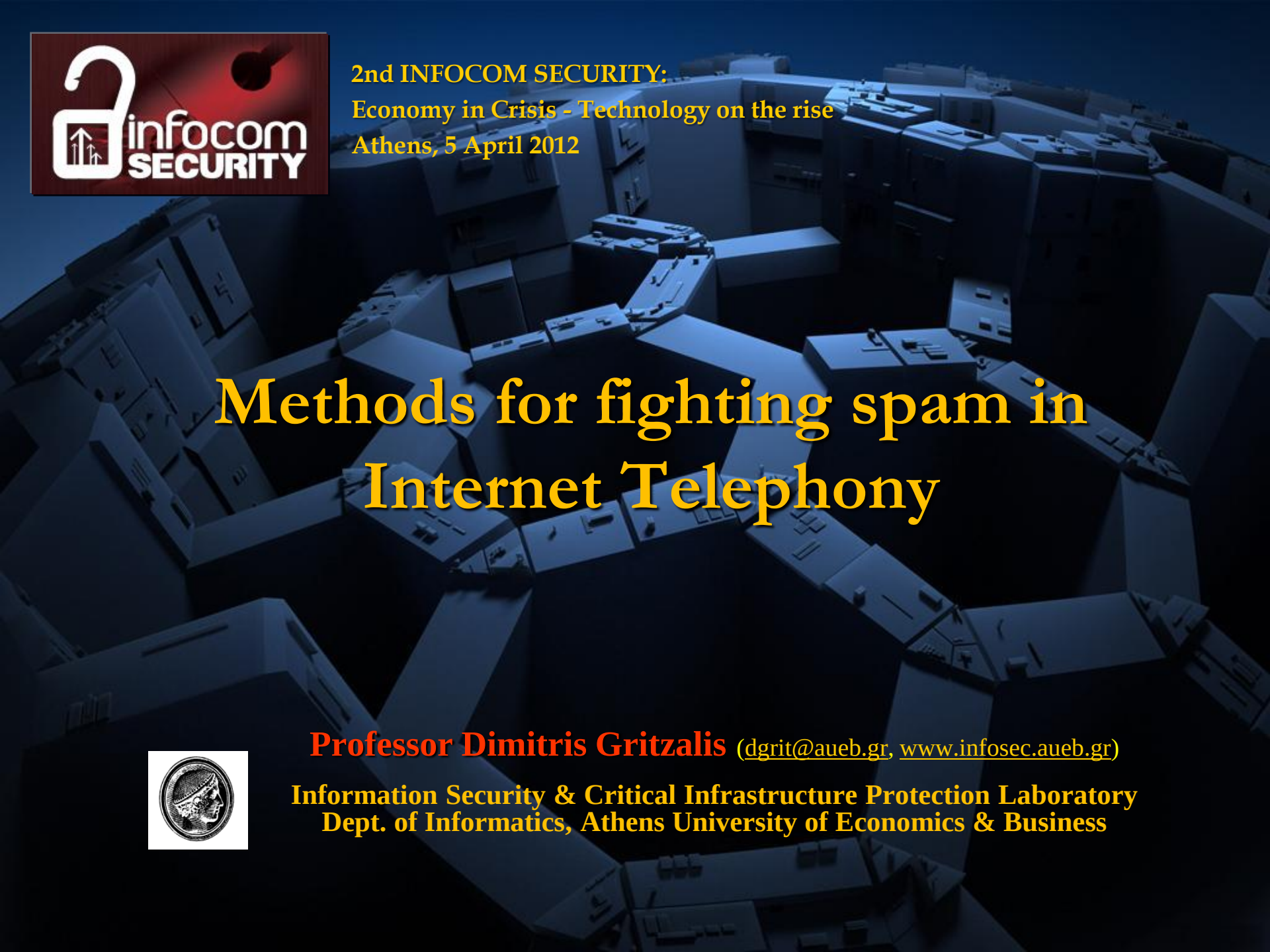
Methods for fighting spam in Internet Telephony

Dimitris Gritzalis
Athens University of Economics & Business



2nd INFOCOM SECURITY:
Economy in Crisis - Technology on the rise
Athens, 5 April 2012

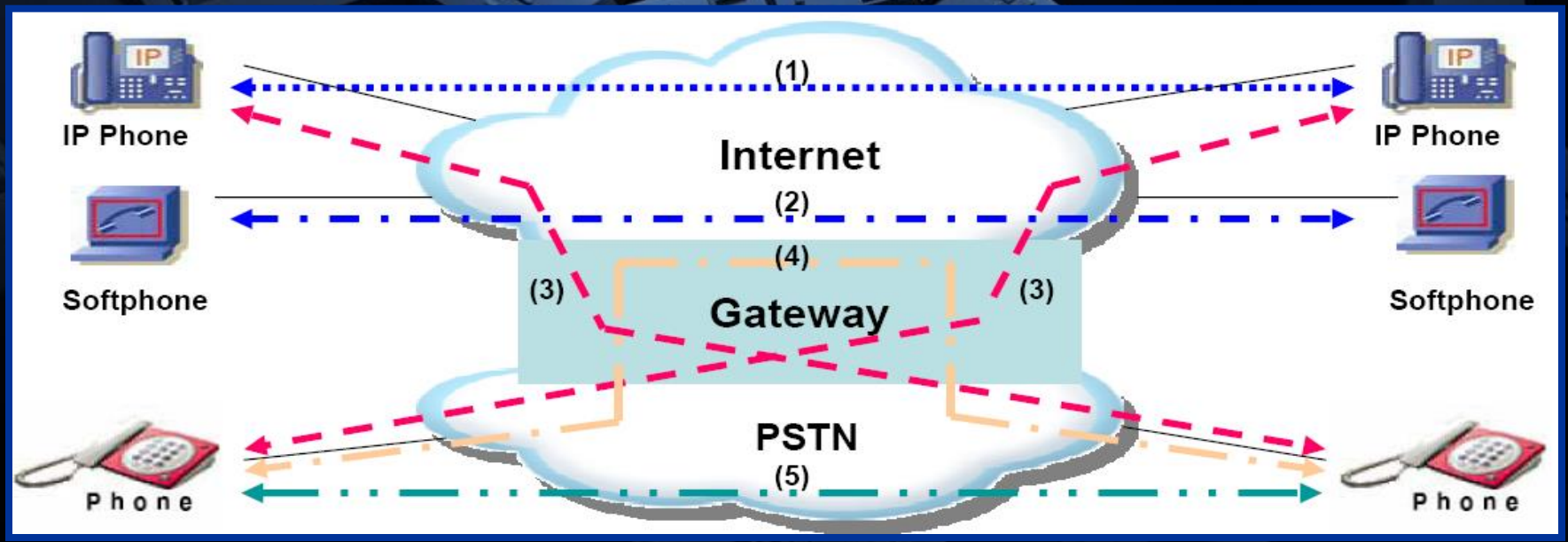
Methods for fighting spam in Internet Telephony

Professor Dimitris Gritzalis (dgrit@aueb.gr, www.infosec.aueb.gr)

Information Security & Critical Infrastructure Protection Laboratory
Dept. of Informatics, Athens University of Economics & Business

Internet Telephony (Voice-over-IP)

- Convergence of **data networks** and **voice networks**.
- **Voice-over-IP (VoIP) technologies** pose as an infrastructure for making **phone calls over the Internet**.
- These are based on protocols, such as the **Session Initiation Protocol (SIP)** for signaling and the **RTP** for voice transfer or multimedia content.



The looming threat : SPam over Internet Telephony (SPIT)

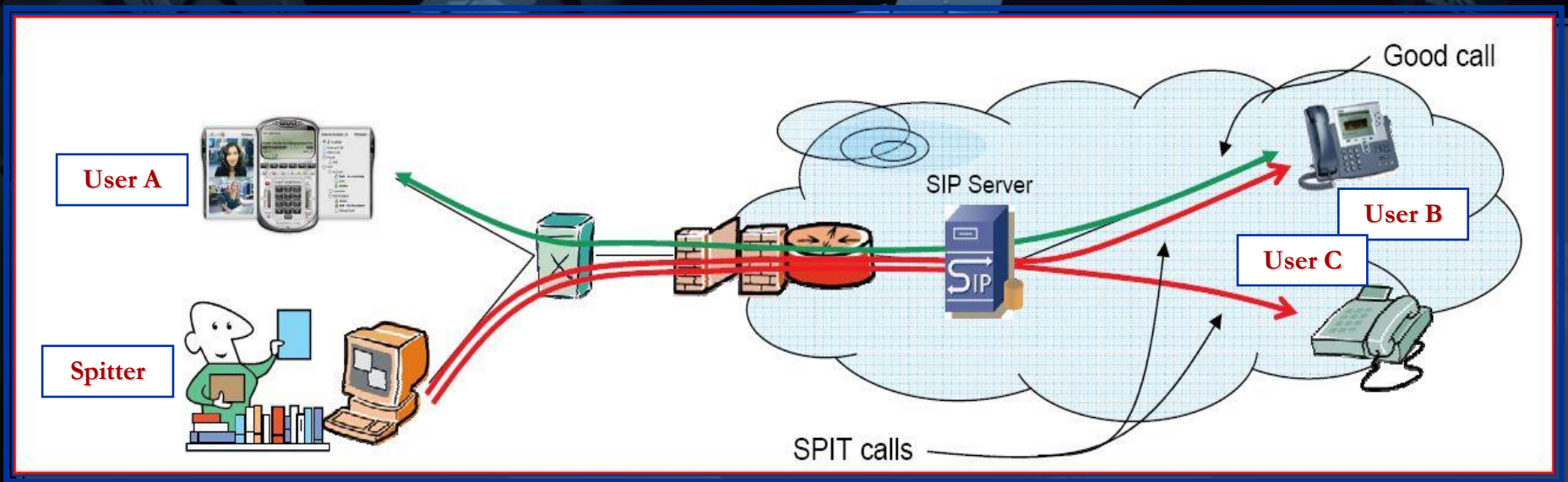
Mass mailing

Unsolicited

Calls

Messages

Presence queries



email spam (spam) vs. voice spam (spit)

Convergences

- **Common incentives**, e.g. seeking financial gain or influence.
- **Common** creative techniques, e.g. automatic production of mass messages/low cost calls, use of real addresses of end-users, collection of addresses etc.

Deviations

- Communication by email is essentially **asynchronous**, while VoIP communication is mainly **synchronized**.
- In the VoIP environment unreasonable delays **are not** (even) **technically acceptable**.
- Spam email is mainly composed of **text** (perhaps images as well) while SPIT is primarily composed by **sound** and **image** (far less by text).
- A SPIT call usually creates a more intensive **disturbance** to the user.

SPIT Mitigation techniques

1. Content Filtering
2. Black-White Lists
3. Consent-based com's
4. Reputation Systems
5. Address Obfuscation
6. Limited-use Addresses
7. Turing Tests, Computational Puzzles
8. Payments at Risk
9. Legal Action
10. Circles of Trust
11. Centralized SIP Providers

Today (2012): Inadequate mitigation because existing mechanisms …

… typically attempt to adopt similar methods of **email spam** mitigation.

… deal with a limited subset of **threats and vulnerabilities** of SIP.

… **focus** on each technological environment (ad-hoc approach).

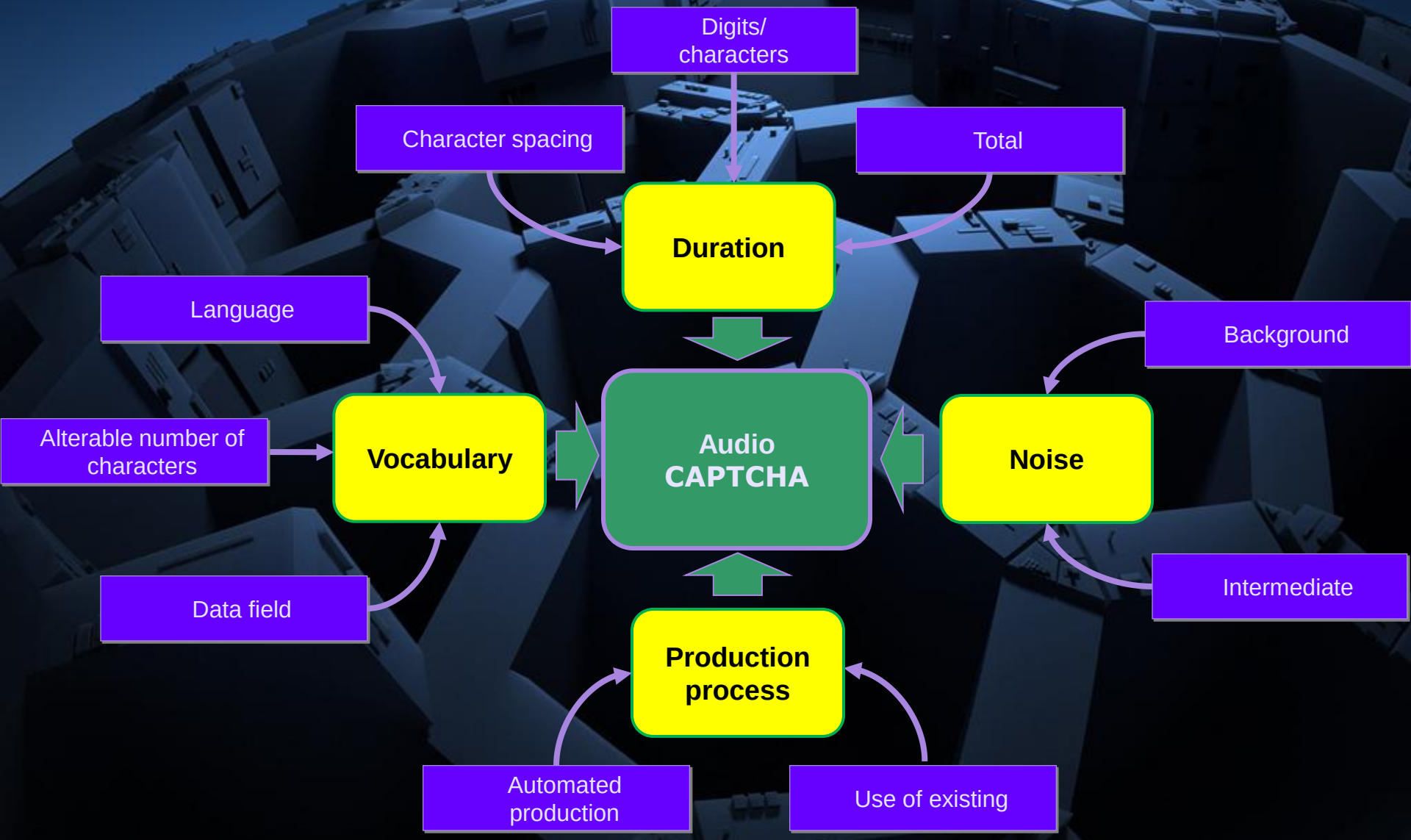
… are unable to cope sufficiently with **new scenarios** of SIP attacks.

… require a **combination** of techniques (multi-factorial) in every **phase** of a SIP call.

… are unable to offer **prevention, detection** and **mitigation** capabilities of SPIT.

… are unable to be evaluated, yet, in **real time conditions**.

Audio CAPTCHA*



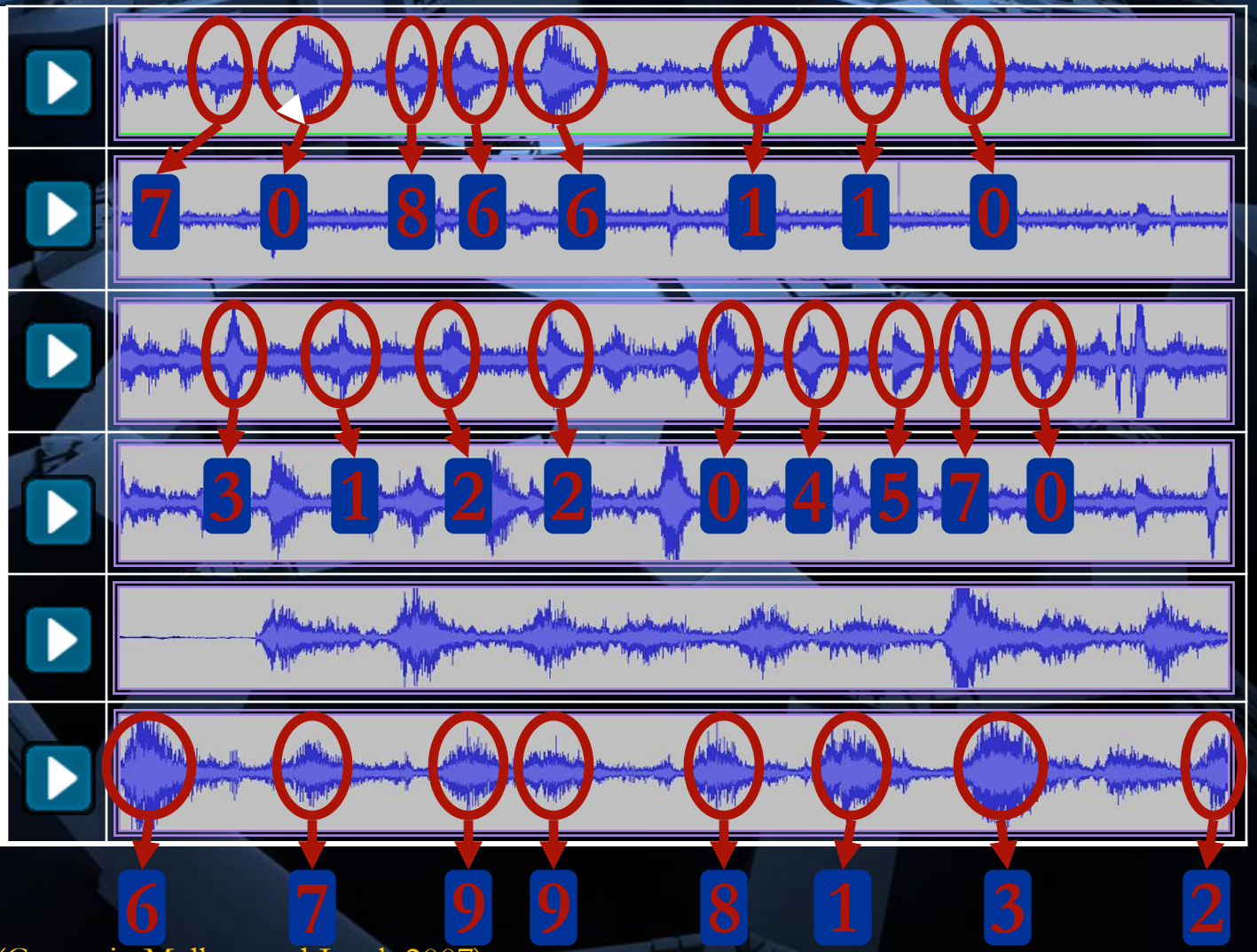
* **CAPTCHA**: **C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part

Implementations of audio CAPTCHA

Recaptcha[1]

Google[2]

MSN[3]



1. http://recaptcha.net (Carnegie Mellon and Intel, 2007)
2. http://gmail.com (Google, 2008) **(Vorm bot access rate: 33%)**
3. https://accountservices.passport.net/reg.srf (Microsoft, 2008) **(Vorm bot access rate: 75%)**

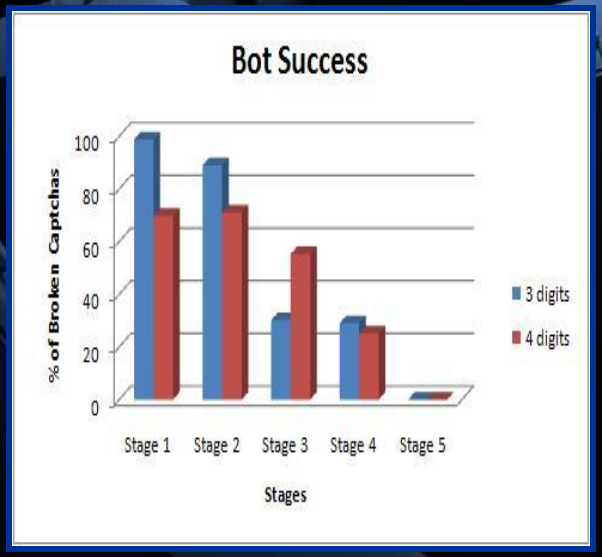
Comparison of available solutions based Sound CAPTCHA

Audio CAPTCHA Characteristics	Google	MSN	Recaptcha	eBay	Secure image captcha	Mp3Captcha	Captchas. net	bokehman	slashdot	Authorize	AOL	Digg
User's Success rate	60%	80%	50%	95%	98%	98%	98%	98%	95%	95%	95%	95%
Background noise	Voice, sound	Voice, sound	Sound	Voice, sound	Sound	No	No	No	No	No	Voice	Sound
Intermediate noise	Sound	Sound	No	No	No	No	No	No	No	No	Sound	No
Data field	0-9	0-9	Words	0-9	A-Z, a-z, 0-9	A-Z, a-z, 0-9	a-z, 0-9	A-Z, a-z, 0-9	Words	A-Z, a-z, 0-9	A-Z, a-z, 0-9	A-Z, a-z, 0-9
Number of characters in a snapshot	5-10	10	10-20	6	4	4	6	4	<9	5	8	5
Rare reappearance	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Production process	Unknown	Unknown	Unknown	Unknown	Automated	Automated	Automated	Automated	Unknown	Unknown	Unknown	Unknown
Speaker voice	Multiple languages	Multiple languages	en	Multiple languages	en	en, fr, it, de	en, de, it, nl, fr	en	en	en	en	en
Different speakers	Yes	No	Yes	No	Yes	No	No	No	No	No	Yes	No
Duration(sec)	0:10-0:15	0:05-0:09	~0:04	~0:04	~0:04	~0:04	~0:08	0:04-0:05	0:03-0:04	0:05	0:10	0:08

Soupionis Y., "*Preventing Spam over Internet Telephony (SPIT) with the use of Security Policies and Audio CAPTCHA*", Ph.D. thesis, Dept. of Informatics, Athens University of Economics & Business, Greece, 2011.

Architecture of the *new** Audio CAPTCHA

	Number of speakers	Time delay	Intermediate noise	Background noise	Number of training snapshots
Phase 1	1	x	x	x	20
Phase 2	3	x	x	x	50
Phase 3	5	x	x	☑	100
Phase 4	7	☑	x	☑	100
Phase 5	7	☑	☑	☑	100



* Soupionis J., Gritzalis D., "ASPF: An adaptive anti-SPIT policy-based framework", in *Proc. of the 6th International Conference on Availability, Reliability and Security* (ARES-2011), Pernul G. (Ed.), pp. 153-160, Austria, August 2011.

General conclusions

- ✓ The widespread use of VoIP introduces **new business activities** and **applications**, but also **new threats**.
- ✓ The adequate mitigation of SPIT requires a **multi-factorial** approach - existing **anti-spam techniques** alone are not sufficient.
- ✓ Anti-SPIT techniques must aim at the mitigation of **even more and new attack types** rather than existing ones.
- ✓ The audio CAPTCHA that capitalizes the **tone** of voice, random **intermediate** sounds and their **distribution** within the message, provides encouraging **resistance** against bots.

References

1. Dritsas, S., Tsoumas, B., Dritsou, V., Konstantopoulos, P., Gritzalis, D., "OntoSPIT: SPIT Management through Ontologies", *Computer Communications*, Vol. 32, No. 2, pp. 203-212, 2009.
2. Gritzalis, D., Katsaros, P., Basagiannis, S., Soupionis, Y., "Formal analysis for robust anti-SPIT protection using model-checking", *International Journal of Information Security*, Vol. 11, No. 2, pp. 121-135, 2012.
3. Gritzalis, D., Mallios, J., "A SIP-based SPIT management framework", *Computers & Security*, Vol. 27, No. 5-6, pp. 136-153, 2008.
4. Gritzalis, D., Marias, G., Rebahi, Y., Soupionis, Y., Ehlert, S., "SPIDER: A platform for managing SIP-based spam over Interent Telephony", *Journal of Computer Security*, Vol. 19, No. 5, pp. 835-867, 2011.
5. Soupionis, J., Gritzalis, D., "ASPF: An adaptive anti-SPIT policy-based framework", *Proc. of the 6th International Conference on Availability, Reliability and Security*, pp. 153-160, Austria, August 2011.
6. Soupionis, Y., Tountas, G., Gritzalis, D., "Audio CAPTCHA for SIP-based VoIP", *Proc. of the 24th International Information Security Conference*, pp. 25-38, Springer (IFIP AICT 297), Cyprus, May 2009.
7. Soupionis, Y., Dritsas, S., Gritzalis, D., "An adaptive policy-based approach to SPIT management", *Proc. of the 13th European Symposium on Research in Computer Security*, pp. 446-460, Springer, Spain, October 2008.
8. Soupionis, Y., Gritzalis, D., "Audio CAPTCHA: Existing solutions assessment and a new implementation for VoIP telephony", *Computers & Security*, Vol. 29, No. 5, pp. 603-618, 2010.
9. Stachtiari, E., Soupionis, Y., Katsaros, P., Mentis, A., Gritzalis, D., "Probabilistic model checking of CAPTCHA admission control for DoS resistant anti-SPIT protection", *Proc. of the 7th International Conference on Critical Information Infrastructures Security*, Springer (LNCS 7722), Norway, September 2012.
10. Tassidou, A., Efraimidis, P., Soupionis, Y., Mitrou, L., Katos, V., "User-centric privacy-preserving adaptation for VoIP CAPTCHA challenges", *Proc. of the 6th International Symposium on Human Aspects of Information Security and Assurance*, Greece, June 2012.
11. Kandias, M., Virvilis, N., Gritzalis, D., "The insider threat in Cloud Computing", *Proc. of the 6th International Workshop on Critical Infrastructure Security*, pp. 93-103, Springer (LNCS 6983), Switzerland, 2011.