

An aerial, high-angle view of a server farm. The server racks are arranged in a circular pattern, creating a central void. The lighting is dim, with a blueish tint, suggesting a nighttime or low-light environment. The perspective is from directly above, looking down into the center of the circular arrangement.

VoIP Infrastructures: The SPIT threat

Dimitris Gritzalis

February 2012



11^ο Συνέδριο για θέματα Ασφάλειας και Άμυνας
Αθήνα, 28-29 Φεβρουαρίου 2012

Υποδομές Διαδικτυακής Τηλεφωνίας: Η απειλή του SPIT

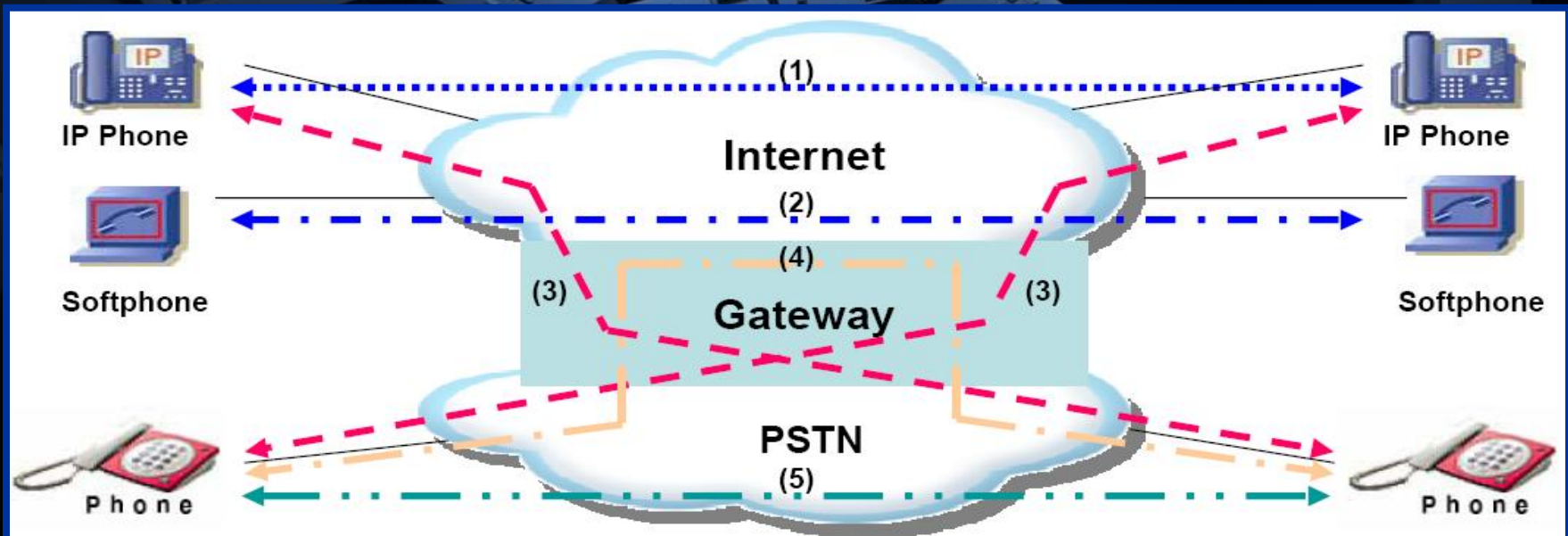
Καθηγητής Δημήτρης Γκρίτζαλης (dgrit@aueb.gr, www.cis.aueb.gr)



Διευθυντής Διαπανεπιστημιακής Ερευνητικής Ομάδας
Ασφάλειας Πληροφοριών & Προστασίας Κρίσιμων Υποδομών
Τμήμα Πληροφορικής, Οικονομικό Πανεπιστήμιο Αθηνών

Διαδικτυακή Τηλεφωνία (Voice-over-IP)

- Σύγκλιση δικτύων δεδομένων και δικτύων φωνής.
- Οι τεχνολογίες **Voice-over-IP (VoIP)** αποτελούν υποδομή για την πραγματοποίηση **τηλεφωνικών κλήσεων μέσω Διαδικτύου**.
- Βασίζονται σε πρωτόκολλα, όπως το **Session Initiation Protocol (SIP)** για τη σηματοδότηση και το **RTP** για τη μεταφορά φωνής ή πολυμεσικού περιεχομένου.



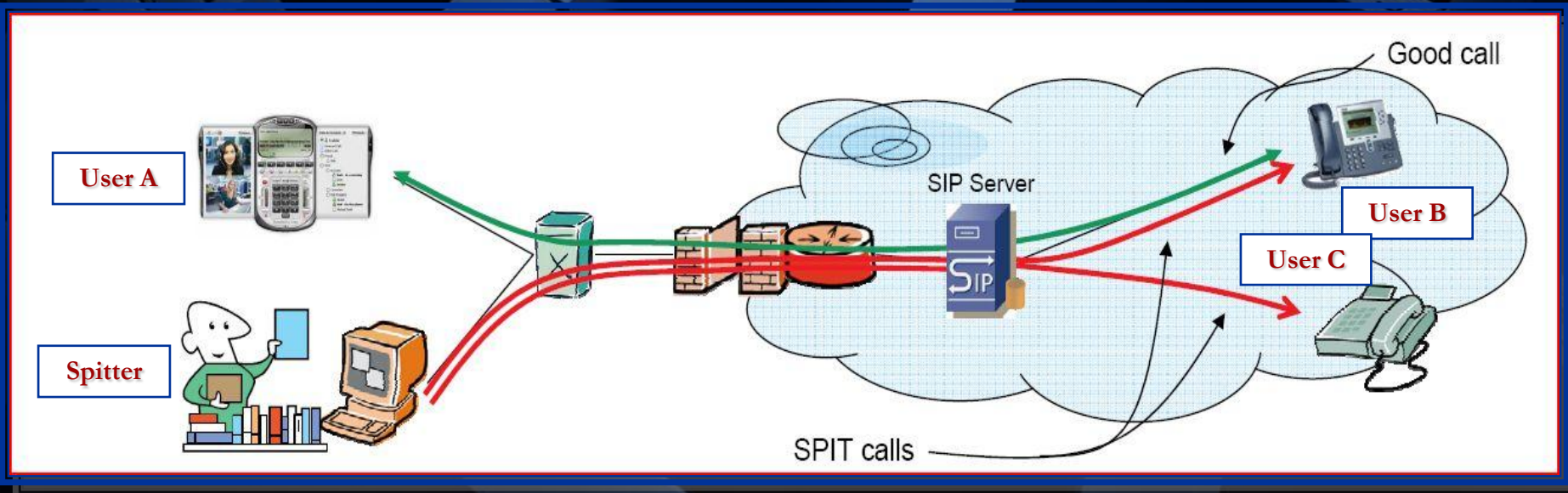
SPam over Internet Telephony (SPIT)

Μαζική αποστολή

απρόσκλητων

Κλήσεων
Μηνυμάτων

Αιτημάτων παρουσίας



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

Συγκλίσεις

- **Κοινά κίνητρα**, πχ. αναζήτηση οικονομικού κέρδους ή άσκηση επιρροής.
- **Κοινές** τεχνικές δημιουργίας, πχ. αυτόματη παραγωγή μαζικών μηνυμάτων/κλήσεων χαμηλού κόστους, χρήση πραγματικών διευθύνσεων τελικών χρηστών, συλλογή διευθύνσεων κλπ.

Αποκλίσεις

- Η επικοινωνία με email είναι ουσιαστικά **ασύγχρονη**, ενώ η VoIP επικοινωνία είναι κυρίως **σύγχρονη**.
- Στο περιβάλλον VoIP μη εύλογες καθυστερήσεις **δεν είναι** (ούτε) τεχνικά **αποδεικτές**.
- Το email spam αποτελείται κυρίως από **κείμενο** (ίσως και εικόνες), ενώ το SPIT κυρίως από **ήχο** και **εικόνα** (πολύ λιγότερο από κείμενο).
- Μια SPIT κλήση συνήθως δημιουργεί εντονότερη **ενόχληση** στο χρήστη.



Τεχνολογίες αντιμετώπισης SPIT

1. Ανάλυση περιεχομένου (Content Filtering)
2. Μαύρες ή/και λευκές λίστες (Black-White Lists)
3. Επικοινωνία βασισμένη στη Συγκατάθεση (Consent-based com's)
4. Συστήματα Εμπιστοσύνης (Reputation Systems)
5. Απόκρυψη Διεύθυνσης (Address Obfuscation)
6. Διευθύνσεις Περιορισμένης Χρήσης (Limited-use Addresses)
7. Τεχνικές Απόκρισης (Turing Tests, Computational Puzzles)
8. Τεχνικές Εισαγωγής Κόστους (Payments at Risk)
9. Νομοθετικές ή κανονιστικές δράσεις (Legal Action)
10. Κύκλοι Εμπιστοσύνης μεταξύ Παρόχων (Circles of Trust)
11. Κεντρικοί Πάροχοι (Centralized SIP Providers)

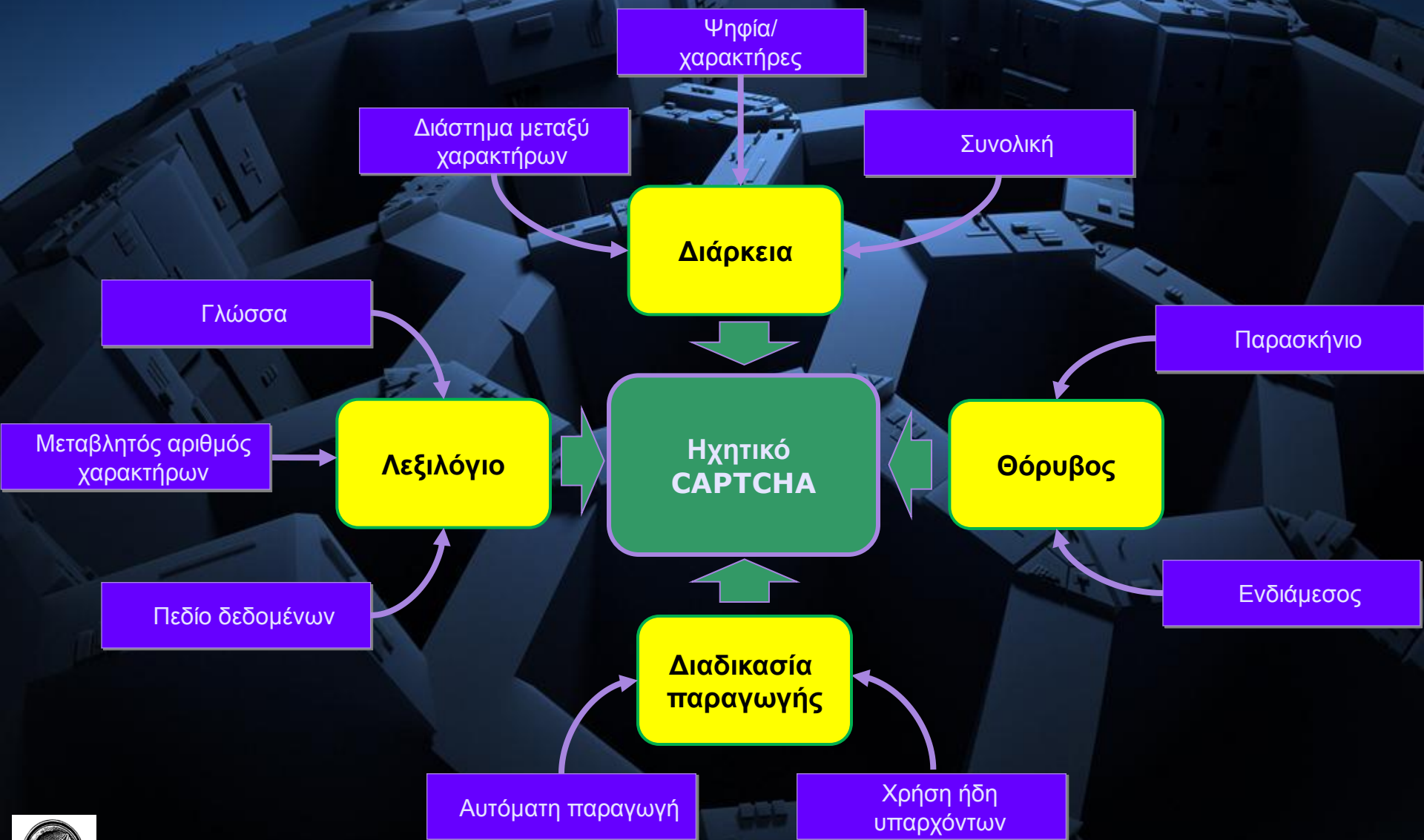


Σήμερα (2012): Ανεπαρκής αντιμετώπιση, γιατί οι υπάρχοντες μηχανισμοί...

- ... κατὰ κανόνα αποπειρώνται να υιοθετήσουν αντίστοιχες μεθόδους αντιμετώπισης του **email spam**.
- ... αντιμετωπίζουν περιορισμένο υποσύνολο **απειλών και αδυναμιών** του SIP.
- ... **εστιάζουν** στο ελάχιστο τεχνολογικό περιβάλλον (ad-hoc προσέγγιση).
- ... δεν μπορούν να αντιμετωπίσουν επαρκώς **καινούργια σενάριο** SIP επιθέσεων.
- ... απαιτούν **συνδυασμό** τεχνικών (πολυπαραγοντικότητα) σε κάθε **στάδιο** μιας SIP κλήσης.
- ... δεν μπορούν να προσφέρουν δυνατότητες **πρόληψης, ανίχνευσης και αντιμετώπισης** του SPIT.
- ... δεν μπορούν να αξιολογηθούν, ακόμη, σε **πραγματικές συνθήκες**.



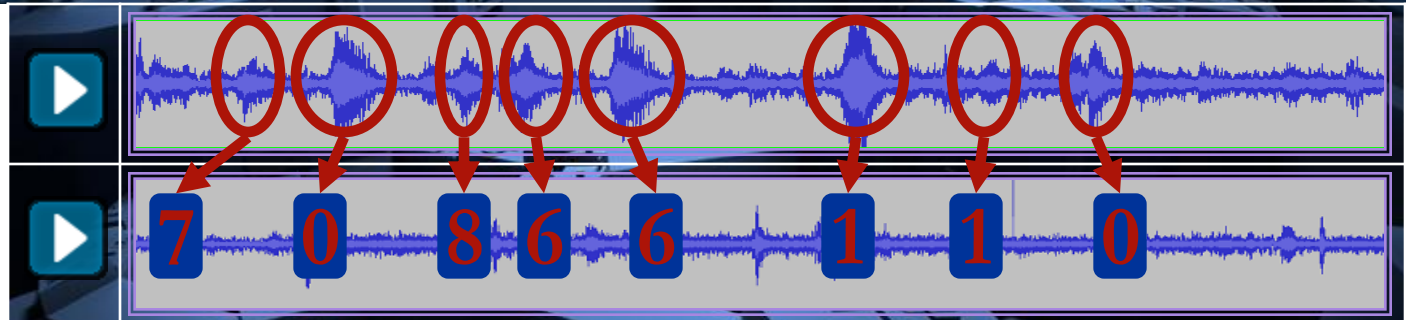
Ηχητικά CAPTCHA*



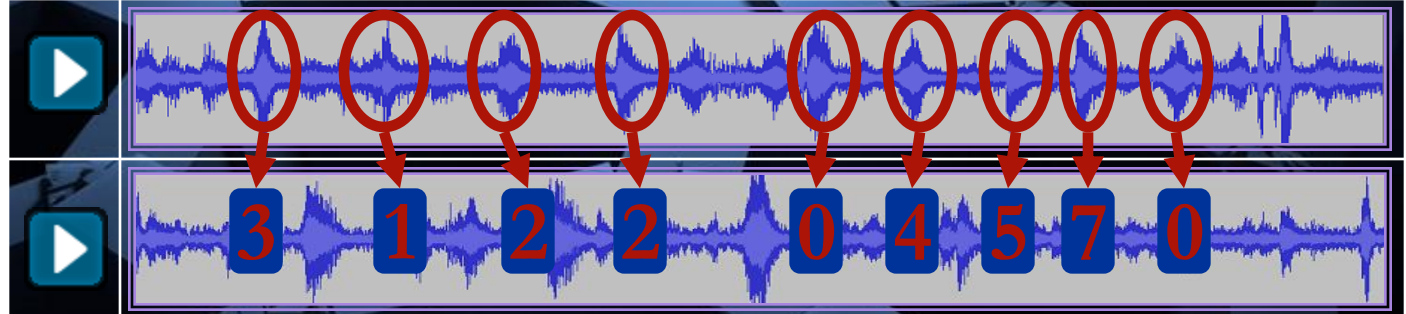
* CAPTCHA: Completely Automated Public Turing test to tell Computers and Humans Apart

Υλοποιήσεις ηχητικών CAPTCHA

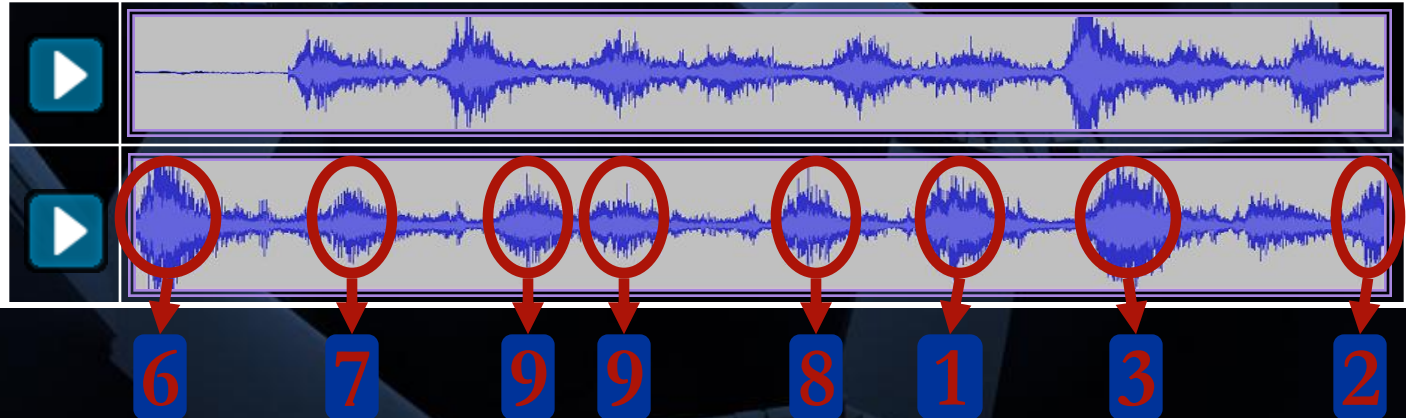
Recaptcha¹



Google²



MSN³



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%)

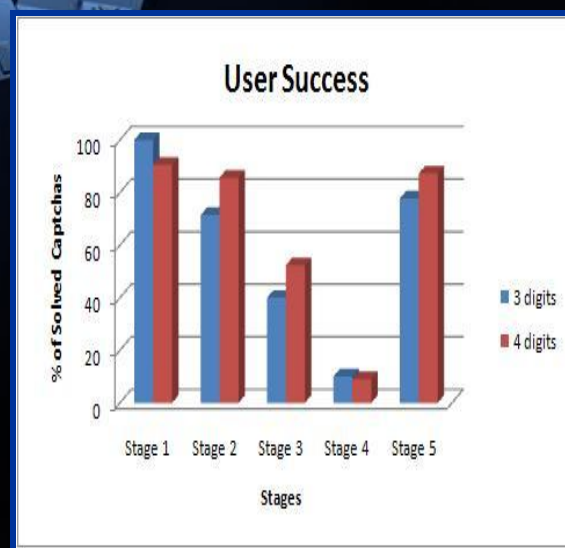
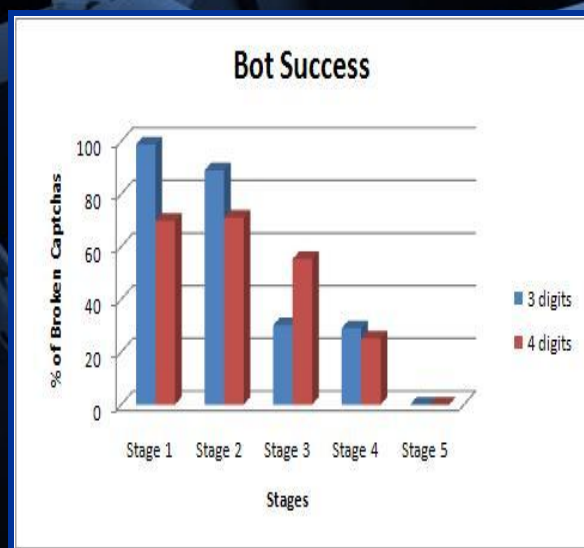
Σύγκριση διαθέσιμων λύσεων ηχητικών CAPTCHA

Ηχητικό CAPTCHA	Google	MSN	Recaptcha	eBay	Secure image captcha	Mp3Captcha	Captchas.net	bokehman	slashdot	Authorize	AOL	Digg
Χαρακτηριστικά												
Ποσοστό επιτυχίας χρήστη	60%	80%	50%	95%	98%	98%	98%	98%	95%	95%	95%	95%
Background θόρυβος	Φωνές, ήχος	Φωνές, ήχος	Ήχος	Φωνές, ήχος	Ήχος	Όχι	Όχι	Όχι	Όχι	Όχι	Φωνές	Ήχος
Ενδιάμεσος θόρυβος	Ήχος	Ήχος	Όχι	Όχι	Όχι	Όχι	Όχι	Όχι	Όχι	Όχι	Ήχος	Όχι
Πεδίο δεδομένων	0-9	0-9	Λέξεις	0-9	A-Z, a-z, 0-9	A-Z, a-z, 0-9	a-z, 0-9	A-Z, a-z, 0-9	Λέξεις	A-Z, a-z, 0-9	A-Z, a-z, 0-9	A-Z, a-z, 0-9
Πλήθος χαρακτήρων στιγμιότυπου	5-10	10	10-20	6	4	4	6	4	<9	5	8	5
Σπάνια επανεμφάνιση	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι	Όχι	Ναι	Ναι	Ναι
Διαδικασία παραγωγής	Άγνωστη	Άγνωστη	Άγνωστη	Άγνωστη	Αυτόματη	Αυτόματη	Αυτόματη	Αυτόματη	Άγνωστη	Άγνωστη	Άγνωστη	Άγνωστη
Γλώσσες εκφώνησης	Πολλές γλώσσες	Πολλές γλώσσες	en	Πολλές γλώσσες	en	en, fr, it, de	en, de, it, nl, fr	en	en	en	en	en
Διαφορετικοί εκφωνητές	Ναι	Όχι	Ναι	Όχι	Ναι	Όχι	Όχι	Όχι	Όχι	Όχι	Ναι	Όχι
Διάρκεια (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



Αρχιτεκτονική νέου* ηχητικού CAPTCHA

	Πλήθος εκφωνητών	Χρονική υστέρηση	Ενδιάμεσος θόρυβος	Θόρυβος στο παρασκήνιο	Πλήθος στιγμιότυπων εκπαίδευσης
Στάδιο 1 ▶	1				20
Στάδιο 2 ▶	3				50
Στάδιο 3 ▶	5			☑	100
Στάδιο 4 ▶	7	☑		☑	100
Στάδιο 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)*, Per-nul G. (Ed.), pp. 153-160, Austria, August 2011.

Κατευθυντήρια συμπεράσματα

- ✓ Η εξάπλωση της χρήσης του VoIP εισαγάγει **νέες επιχειρηματικές δραστηριότητες** και **εφαρμογές**, αλλά και **νέες απειλές**.
- ✓ Η επαρκής αντιμετώπιση του SPIT απαιτεί **πολυ-παραγοντική προσέγγιση** - δεν επαρκούν μόνο υπάρχουσες **anti-spam τεχνικές**.
- ✓ Οι τεχνικές anti-SPIT πρέπει να στοχεύουν στην αντιμετώπιση **περισσότερων και νέων ειδών επιθέσεων** απ' ότι οι υπάρχουσες.
- ✓ Το audio CAPTCHA που αξιοποιεί **χρoιά** εκφώνησης, τυχαίους **ενδιάμεσους** ήχους και **διασπορά** τους μέσα στο μήνυμα, παρέχει ενθαρρυντική **ανθεκτικότητα** απέναντι σε bots.





Από τη θεωρία στην πράξη...

ΣΦΙΓΕ Consortium (sphinx.vtrip.net)

1. Virtual Trip
2. Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης
3. Δημοκρίτειο Πανεπιστήμιο Θράκης
4. Οικονομικό Πανεπιστήμιο Αθηνών

Χρηματοδότηση

Γενική Γραμματεία Έρευνας & Τεχνολογίας

Ε.Π. Ανταγωνιστικότητα & Επιχειρηματικότητα

Δράση Εθνικής Εμβέλειας ΣΥΝΕΡΓΑΣΙΑ



ΣΦΙΓΕ: Αναμενόμενα αποτελέσματα

- Αξιοποίηση τεχνολογιών αιχμής

- ✓ Ανάπτυξη υπηρεσίας πρόληψης αυτοματοποιημένων επιθέσεων SPIT
- ✓ Ενσωμάτωση της υπηρεσίας σε υπάρχουσες εταιρικές υπηρεσίες
- ✓ Αποτίμηση απόδοσης και αξιολόγηση αποτελεσματικότητας της υπηρεσίας
- ✓ Μελέτη οικονομικών και κοινωνικών επιπτώσεων και ανάλυση απαιτούμενου κανονιστικού πλαισίου

Τεχνολογίες αιχμής

- **Audio CAPTCHA**
- **Formal Model Checking**
- **Privacy Enhancing Technologies (PET)**





Μεταβαίνοντας, **συνεργατικά**,
από τη **θεωρία** στην **πράξη**,
για την ανάπτυξη
εύρωστων ψηφιακών υποδομών
και **διαδίκτυακών υπηρεσιών**



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. Soupionis Y., Basagiannis S., Katsaros P., Gritzalis D., “A formally verified mechanism for countering SPIT”, in Proc. of the 5th International Conference on Critical Information Infrastructure Security (CRITIS-2010), pp. 128-139, LNCS-6712, Springer, Greece, September 2010.
4. Gritzalis D., Mallios J., “A SIP-based SPIT management framework”, *Computers & Security*, Vol. 27, No. 5-6, pp. 136-153, 2008.
5. Gritzalis D., Marias G., Rebahi Y., Soupionis Y., Ehlert, S., “SPIDER: A platform for managing SIP-based spam over Internet Telephony”, *Journal of Computer Security*, Vol. 19, No. 5, pp. 835-867, 2011.
6. 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.
7. Kandias M., Mylonas A., Virvilis N., Theoharidou M., Gritzalis D., “An Insider Threat Prediction Model”, *Proc. of the 7th International Conference on Trust, Privacy and Security in Digital Business*, pp. 26-37, Springer (LNCS 6264), Spain, 2010.
8. Soupionis Y., 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, 2011.
9. 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, 2009.
10. 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, 2008.
11. 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.
12. Stachtari 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, 2012.
13. 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, 2012.