



**SPIT: Still another  
emerging Internet threat**

**Dimitris Gritzalis**

**October 2009**



Τμήμα Πληροφορικής  
Οικονομικό Πανεπιστήμιο Αθηνών

# SPIT

(SPam over Internet Telephony)

## Μια νέα διαδικτυακή απειλή

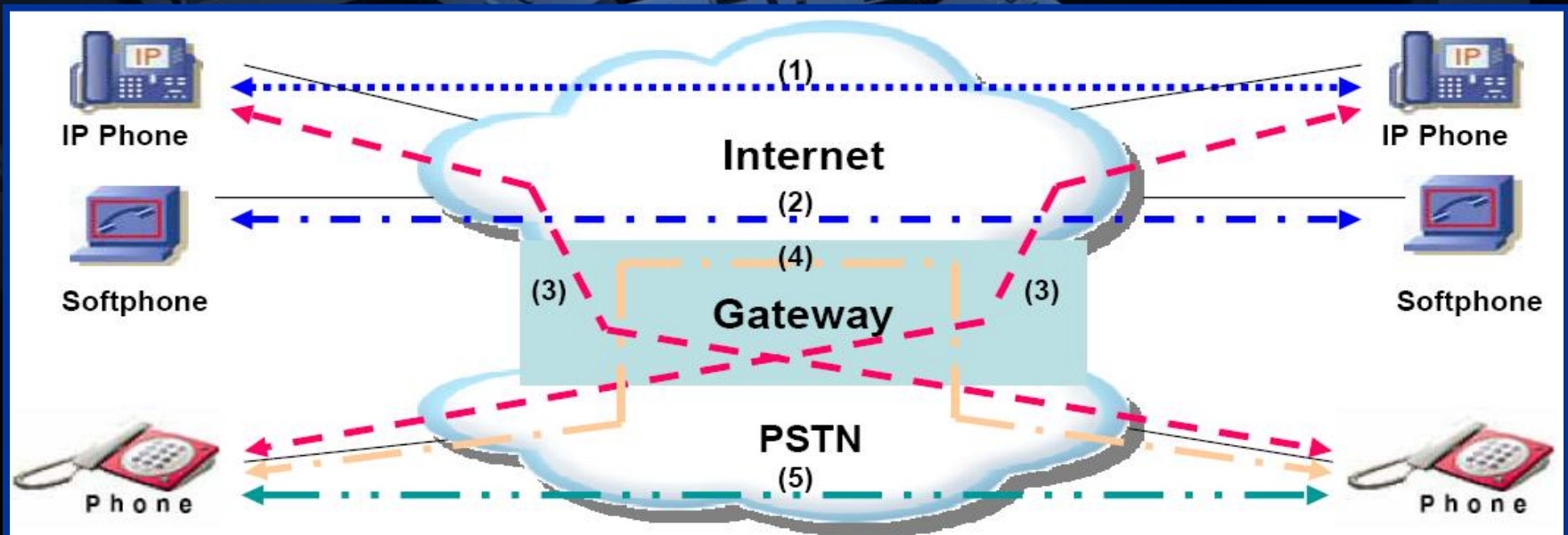
**Καθηγητής Δημήτρης Γκρίτζαλης**

([dgrit@aub.gr](mailto:dgrit@aub.gr), [www.cis.aub.gr](http://www.cis.aub.gr))

Διευθυντής Διαπανεπιστημιακής Ερευνητικής Ομάδας  
Ασφάλειας Πληροφοριών και Προστασίας Κρίσιμων Υποδομών

# 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 τα **Session Initiation Protocol (SIP)** και **H.323** για τη σηματοδότηση και το **RTP** για τη μεταφορά φωνής ή πολυμεσικού περιεχομένου.



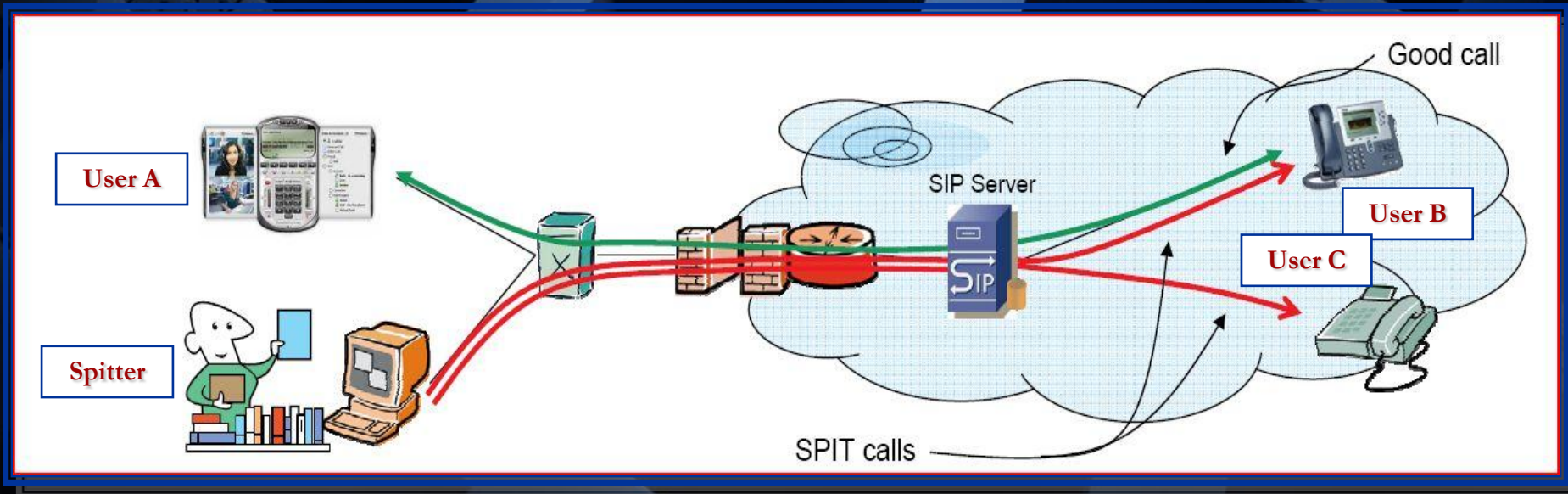
# SPam over Internet Telephony (SPIT)

Μαζική αποστολή

απρόσκλητων

Κλήσεων  
Μηνυμάτων

Αιτημάτων παρουσίας



“ Welcome to account verification.  
Please type your 16-digits card number ”



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

---

## Συγκλίσεις

- **Κοινά κίνητρα**, πχ. αναζήτηση οικονομικού κέρδους ή άσκησης 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** στις διάφορες φάσεις των συνόδων.
- Στο περιβάλλον VoIP μη εύλογες καθυστερήσεις **δεν είναι** (ούτε) τεχνικά **αποδεκτές**.
- Το email spam αποτελείται κυρίως από **κειμένο**, ίσως και εικόνες, ενώ το SPIT κυρίως από **ήχο** και **εικόνα** και πολύ λιγότερο από κείμενο.
- Μια SPIT κλήση συχνά δημιουργεί εντονότερη **ενόχληση** στο χρήστη.



# Μέθοδοι 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)

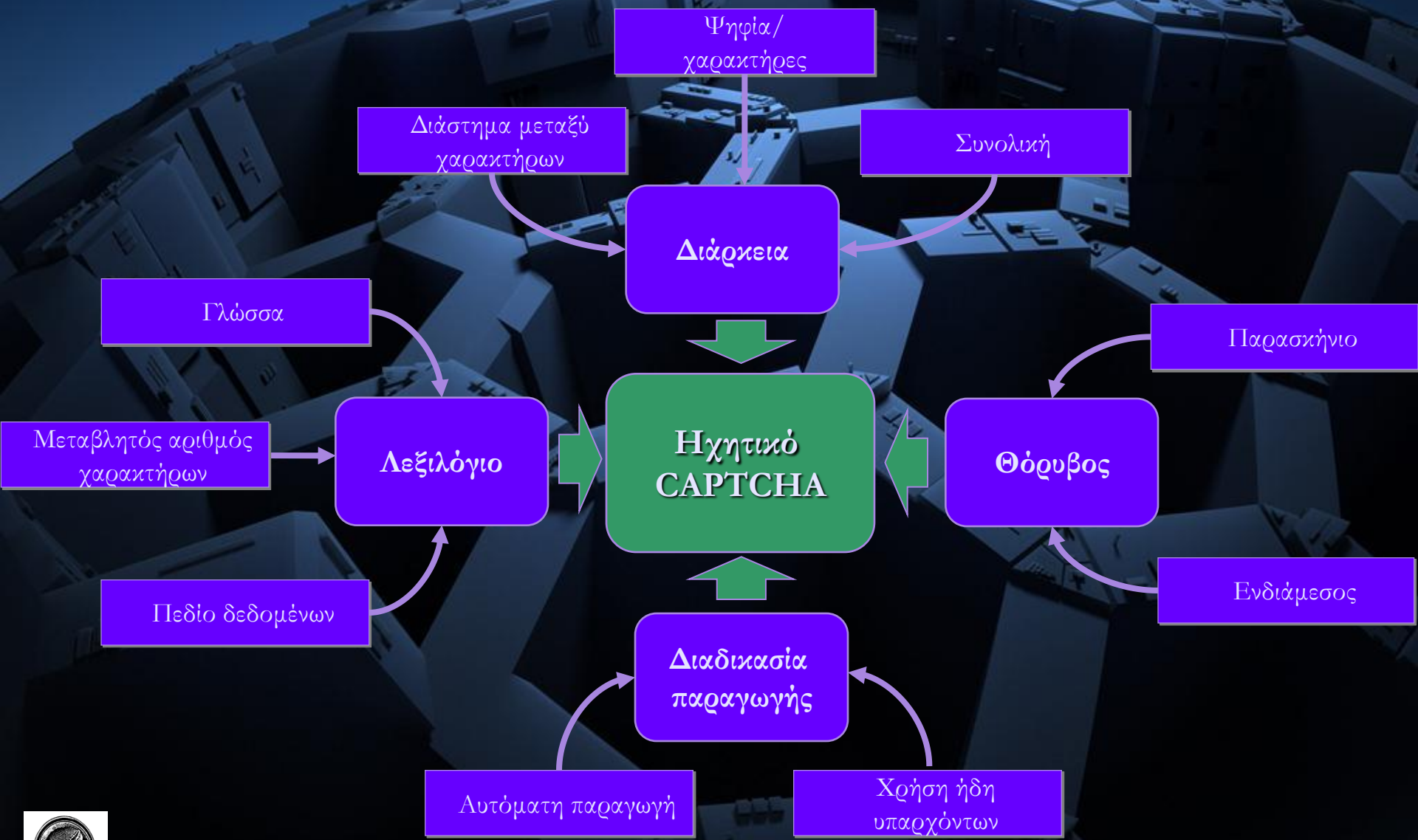


# Ανεπαρκής αντιμετώπιση, γιατί οι υπάρχοντες μηχανισμοί...

- ...κατά κανόνα αποπειρώνται να υιοθετήσουν αντίστοιχες μεθόδους αντιμετώπισης του **email spam**.
- ...αντιμετωπίζουν περιορισμένο υποσύνολο **απειλών και αδυναμιών** του SIP.
- ...**εστιάζουν** και αφορούν το εικάστοτε τεχνολογικό περιβάλλον (ad-hoc προσέγγιση).
- ...δεν μπορούν να αντιμετωπίσουν **καινούργια σενάρια** 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**.



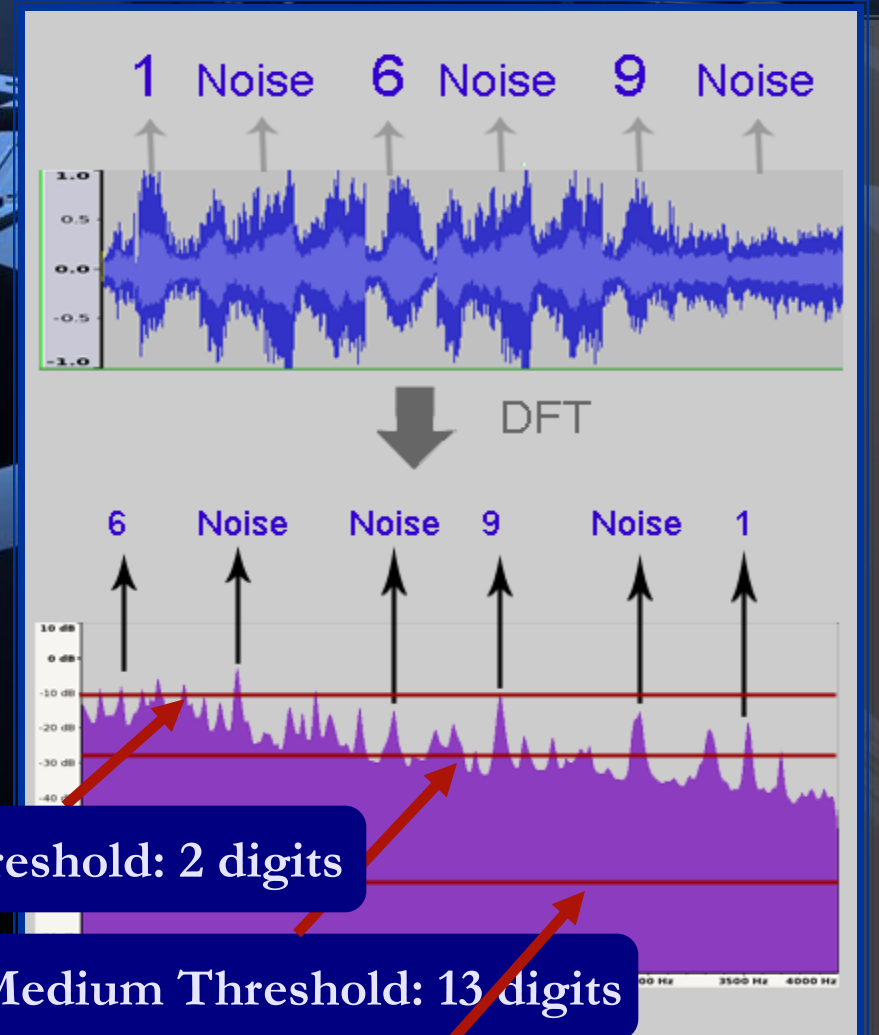
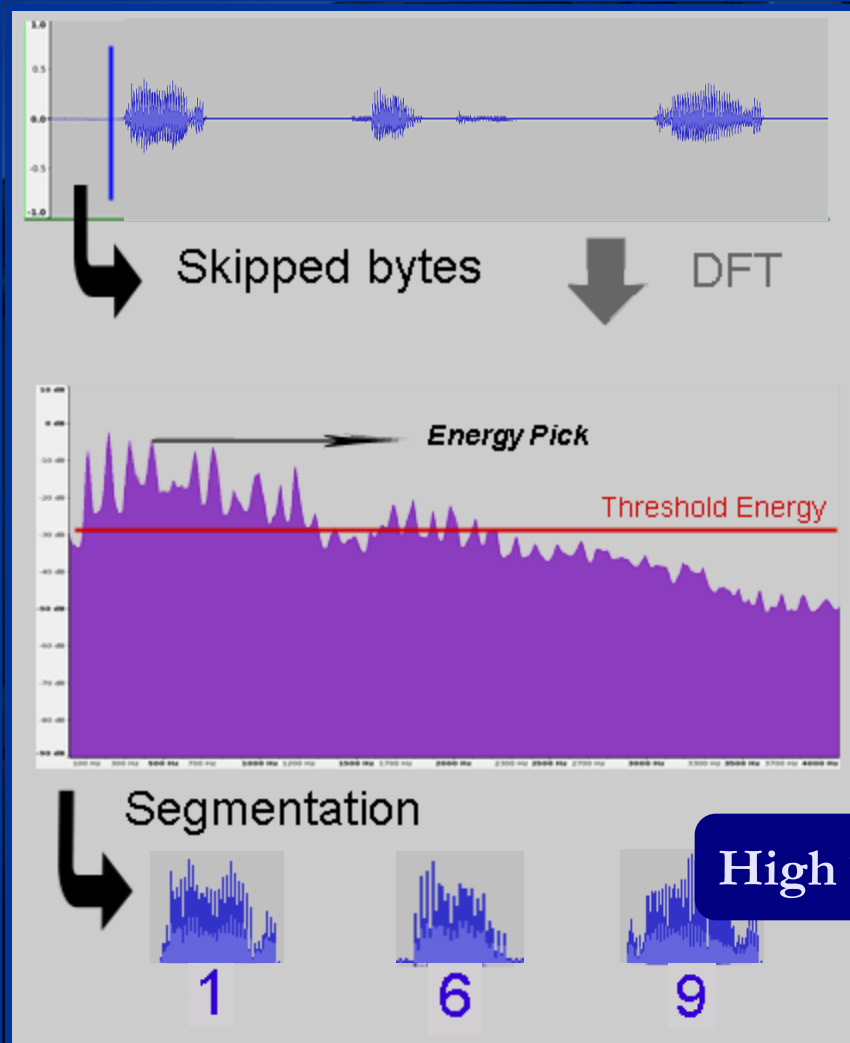
# Audio CAPTCHA\*



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



# Anti-SPIT audio CAPTCHA



High Threshold: 2 digits

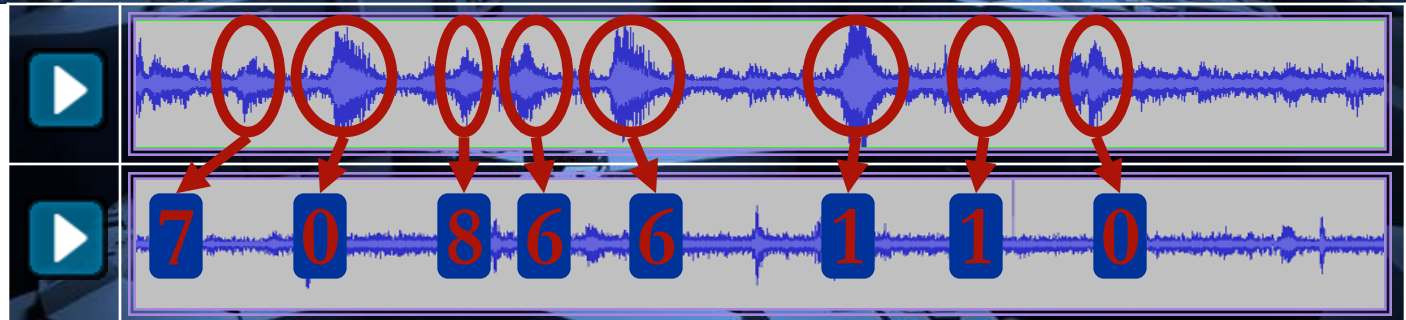
Medium Threshold: 13 digits

Low Threshold: 15 digits

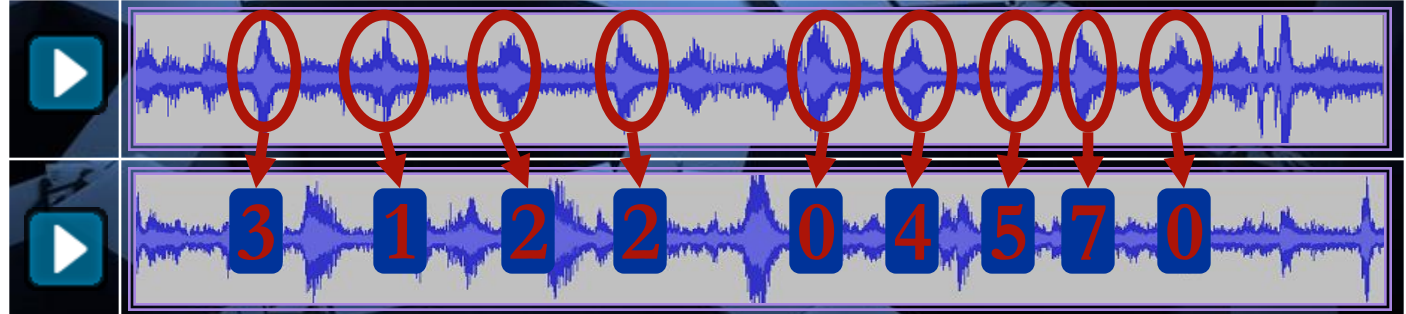


# Βασικές υλοποιήσεις audio CAPTCHA

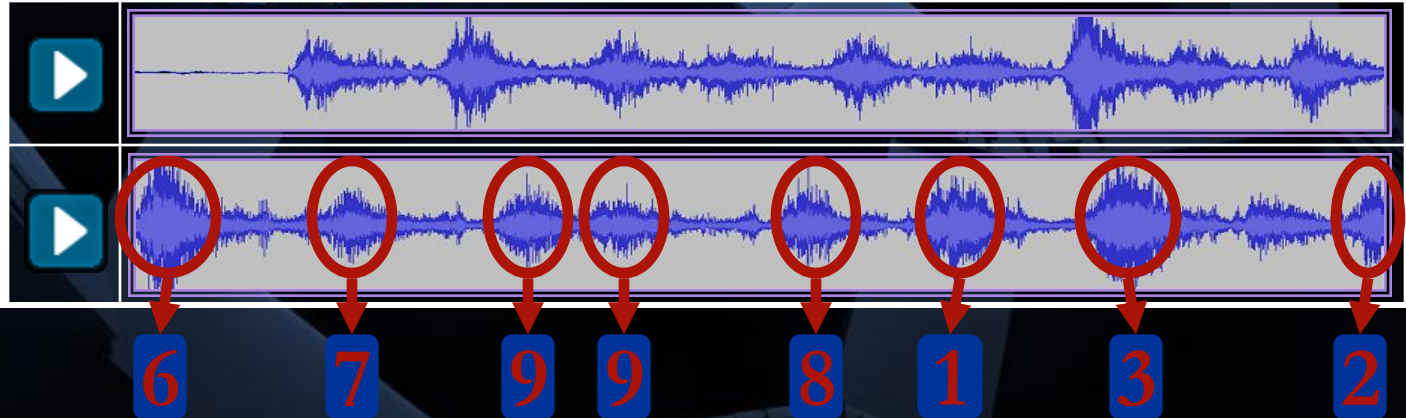
Recaptcha<sup>1</sup>



Google<sup>2</sup>



MSN<sup>3</sup>



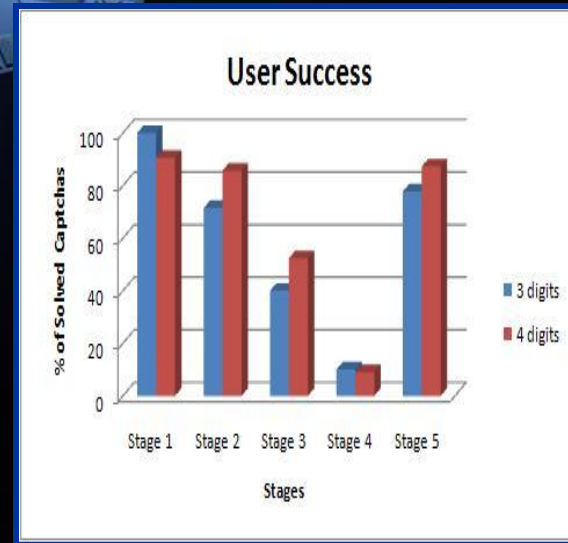
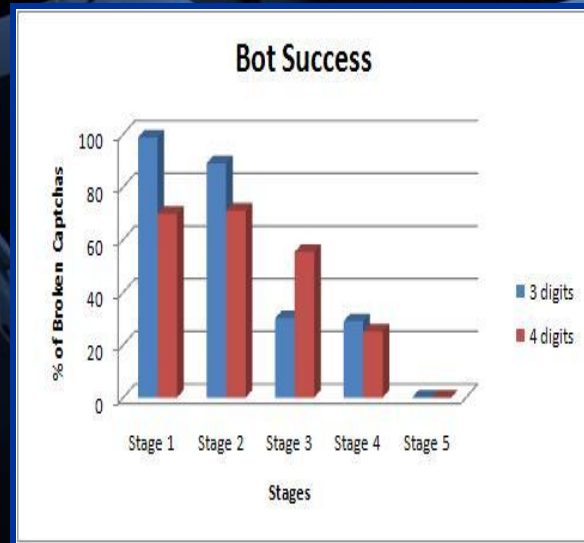
1. <http://recaptcha.net> (Carnegie Mellon and Intel, 2007)

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%)

# Αρχική αξιολόγηση audio CAPTCHA

	Πλήθος εκφωνητών	Χρονική υστέρηση	Ενδιάμεσος θόρυβος	Θόρυβος στο παρασκήνιο	Πλήθος στιγμιότυπων εκπαίδευσης
Στάδιο 1 	1				20
Στάδιο 2 	3				50
Στάδιο 3 	5			<input checked="" type="checkbox"/>	100
Στάδιο 4 	7	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	100
Στάδιο 5 	7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	100



# Πρώτα συμπεράσματα

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



## References

1. Dritsas S., Mallios J., Theoharidou M., Marias G., Gritzalis D., "Threat analysis of the Session Initiation Protocol, regarding spam", in *Proc. of the 26<sup>th</sup> IEEE International Performance Computing and Communications Conference*, pp. 426-433, IEEE Press, 2007.
2. 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.
3. Dritsas S., Soupionis J., Theoharidou M., Mallios J., Gritzalis D., "SPIT Identification Criteria Implementations: Effectiveness and Lessons Learned", in *Proc. of the 23<sup>rd</sup> International Information Security Conference*, pp. 381-395, Springer, 2008.
4. Gritzalis D., Mallios J., "A SIP-based SPIT management framework", *Computers & Security*, Vol. 27, No. 5-6, pp. 136-153, 2008.
5. Mallios J., Dritsas S., Tsoumas B., Gritzalis D., "Attack modelling of SIP-oriented SPIT", in *Proc. of the 2<sup>nd</sup> International Workshop on Critical Information Infrastructures Security*, pp. 299-310, Springer, 2007.
6. Marias J., Dritsas S., Theoharidou M., Mallios J., Gritzalis D., "SIP vulnerabilities and antisipit mechanisms assessment", in *Proc. of the 16<sup>th</sup> IEEE International Conference on Computer Communications and Networks*, pp. 597-604, IEEE Press, 2007.
7. Soupionis Y., Tountas G., Gritzalis D., "Audio CAPTCHA for SIP-based VoIP", *Proc. of the 24<sup>th</sup> International Information Security Conference*, pp. 25-38, Springer, 2009.
8. Soupionis Y., Dritsas S., Gritzalis D., "An adaptive policy-based approach to SPIT management", *Proc. of the 13<sup>th</sup> European Symposium on Research in Computer Security*, pp. 446-460, Springer, 2008.
9. Theoharidou M., Kotzanikolaou P., Gritzalis D., "Risk-based Criticality Analysis", in *Proc. of the 3<sup>rd</sup> IFIP International Conference on Critical Infrastructure Protection*, Springer, 2009.
10. Theoharidou M., Stougiannou E., Gritzalis D., "A CBK for Information Security and Critical Infrastructure Protection", in *Proc. of the 5<sup>th</sup> IFIP Conference on Information Security Education*, pp. 49-56, Springer, 2007.