

---

*Ανεπιθύμητη Τηλεφωνία μέσω Διαδικτύου.  
Μια νέα απειλή που αναζητά λύσεις.*

---

***Δρ. Ιωάννης Μαριάς  
Λέκτορας Ασφάλειας Υπολογιστών κ' Δικτύων  
Τμήμα Πληροφορικής  
Οικονομικό Πανεπιστήμιο Αθηνών***

*9ο ICT Forum, 29-30 Oct., 2007, Athens*

# Περιεχόμενα

---

- SPAM και SPIT
  - Διαφορές και συμπτώσεις
- Τύποι SPIT
  - Ευπάθειες και απειλές
- Anti-SPIT
  - Εύκολα ή δύσκολα;
  - Αντίμετρα και κατηγορίες τους
- Έργο SPIDER
- Συζήτηση – συμπέρασμα

# SPAM

---

## ■ Ορισμός

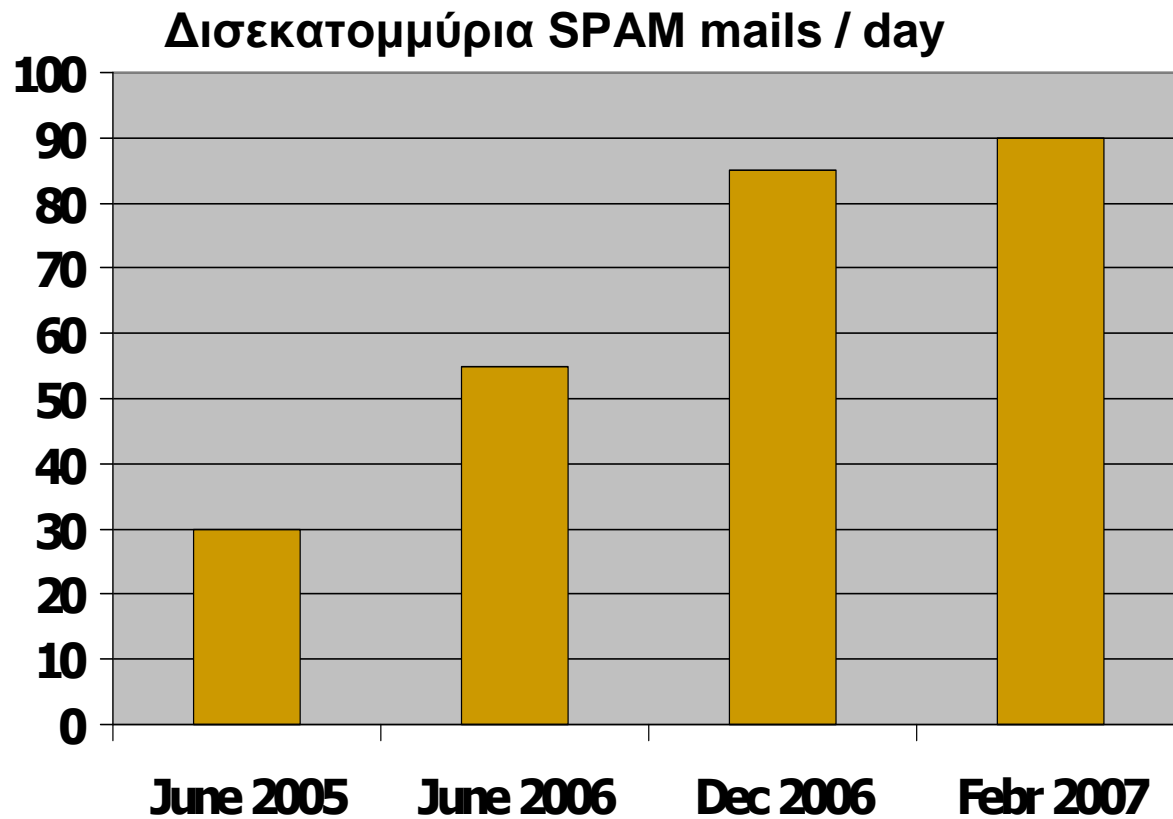
- Αυτόκλητη μαζική αποστολή (κερδοσκοπικών) e-mails

## ■ Ιστορία

- 1978 – 1ο e-mail spam σε 600 e-mail addresses
- 1994 – 1ο e-mail spam μεγάλης κλίμακας σε 6000 newsgroups
  - Εκατομμύρια αποδέκτες
- 2004 – καταδικάζεται ο N.M. σε 5 χρόνια φυλάκιση για αποστολή “Nigerian 419 spams” (Αυστραλία)

# SPAM

## ■ Ιστορία



Πηγή: Wikipedia

# SPAM

## ■ Κόστος SPAM – U.S.

|                                                                   |                        |
|-------------------------------------------------------------------|------------------------|
| <b>SPAM e-mail</b>                                                | <b>40% των e-mails</b> |
| <b>Ημερήσια αποστολή SPAM (2006)</b>                              | <b>12.4 δις.</b>       |
| <b>Ημερήσια λήψη SPAM ανά χρήστη</b>                              | <b>6</b>               |
| <b>Ετήσια λήψη SPAM ανά χρήστη</b>                                | <b>2,200</b>           |
| <b>Ετήσιο κόστος SPAM για μη εταιρικούς χρήστες του Internet.</b> | <b>\$255εκ.</b>        |
| <b>Ετήσιο κόστος SPAM για Αμερικάνικες εταιρείες (2002)</b>       | <b>\$8.9 δις.</b>      |
| <b>Πολιτείες με Anti-SPAM νομοθεσία</b>                           | <b>26</b>              |
| <b>Αλλαγή e-mail address λόγω SPAM</b>                            | <b>16%</b>             |
| <b>Ποσοστό χρηστών που απαντά σε SPAM e-mail</b>                  | <b>28%</b>             |
| <b>Ποσοστό χρηστών που αγοράζει από SPAM e-mail</b>               | <b>8%</b>              |
| <b>Εταιρικό e-mail το οποίο εκλαμβάνεται ως SPAM</b>              | <b>15-20%</b>          |
| <b>Χαμένος χρόνος εργασίας ανά SPAM e-mail</b>                    | <b>4-5 δευτ.</b>       |

Πηγή: TopTenREVIEWS, Inc.

# SPAM

- Από πού προέρχεται
  - Οι ΗΠΑ, Κίνα και Ρωσία: πλειοψηφία δ/νσεων αποστολής SPAM
  - Verizon: φιλοξενεί το μεγαλύτερο αριθμό spammers
- Σε ποιους αναφέρεται
  - 5 χώρες έχουν το 99.68% των sites που αναφέρονται σε SPAM e-mails
  - Η Κίνα φιλοξενεί το 74% αυτών

| Απρίλιος- Ιούνιος 2006 |                  |       |
|------------------------|------------------|-------|
| 1.                     | ΗΠΑ              | 23.2% |
| 2.                     | ΚΙΝΑ             | 20.0% |
| 3.                     | Ν.ΚΟΡΕΑ          | 7.5%  |
| 4.                     | ΓΑΛΛΙΑ           | 5.2%  |
| 5.                     | ΙΣΠΑΝΙΑ          | 4.8%  |
| 6.                     | ΠΟΛΩΝΙΑ          | 3.6%  |
| 7.                     | ΒΡΑΖΙΛΙΑ         | 3.1%  |
| 8.                     | ΙΤΑΛΙΑ           | 3.0%  |
| 9.                     | ΓΕΡΜΑΝΙΑ         | 2.5%  |
| 10.                    | ΗΝΩΜΕΝΟ ΒΑΣΙΛΕΙΟ | 1.8%  |
|                        | ΑΛΛΟΙ            | 25.3% |

Πηγή: Sophos S.A., U.S.

# SPAM

## ■ Περιεχόμενα SPAM e-mail

| Στατιστικά στοιχεία e-mail SPAM |                           |     |
|---------------------------------|---------------------------|-----|
| 1.                              | Προϊόντα                  | 25% |
| 2.                              | Χρηματοοικονομικά         | 20% |
| 3.                              | Ερωτικά                   | 19% |
| 4.                              | Απάτες                    | 9%  |
| 5.                              | Υγεία                     | 7%  |
| 6.                              | Internet                  | 7%  |
| 7.                              | Ελεύθερος χρόνος          | 6%  |
| 8.                              | Θρησκευτικού περιεχομένου | 4%  |
| 9.                              | Λοιπά                     | 3%  |

Πηγή: TopTenREVIEWS, Inc.

- Hoaxes – αστεία
- Annoyances – ενοχλήσεις
- Αλυσίδες
- Προώθηση προϊόντος, υπηρεσίας, ή ειδικού μηνύματος
- Απάτη
  - Advance fee fraud (Nigerian)
  - Phising
- Υποκλοπή και DoS
  - Viruses and zombies

# SPAM

## ■ Τεχνικές για αποστολή e-mail SPAM

|                                                   |                                                                            |
|---------------------------------------------------|----------------------------------------------------------------------------|
| <b>Συγκομιδή (harvesting) και επίθεση λεξικού</b> | <b>Δημιουργία λίστας-στόχου διευθύνσεων</b>                                |
| <b>Μαζικά e-mails</b>                             | <b>SPAM μέσω e-mail διεύθυνσης του αποστολέα</b>                           |
| <b>Joe job</b>                                    | <b>SPAM μέσω e-mail διεύθυνσης ανυποψίαστου χρήστη</b>                     |
| <b>Αναμετάδοση μέσω τρίτων οντοτήτων</b>          | <b>Χρήση αναμεταδοτών e-mail SPAM</b>                                      |
| <b>Εισβολή (break-in)</b>                         | <b>Εισβολή σε σύστημα ανυποψίαστου για SPAM</b>                            |
| <b>Zombies (botnets / robots)</b>                 | <b>Χρήση εγκατεστημένων προγραμμάτων σε συστήματα ανυποψίαστων χρηστών</b> |

# SPAM

---

- Μηχανισμοί αντιμετώπισης
  - Πρόληψη (prevention)
    - Πριν εκδηλωθεί
  - Εντοπισμός (detection)
    - Μετά την εκδήλωσή του
  - Αντίδραση (handling)
    - Μετά τον εντοπισμό του
    - Συνήθως ο τελικός χρήστης αποφασίζει
      - Anti-SPAM Profile

# SPAM

---

- Μηχανισμοί αντιμετώπισης
  - Πρόληψη (prevention)
    - Λευκές Λίστες (White lists)
    - Αυθεντικοποίηση αποστολέα
    - Παραποίηση της διεύθυνσης (obfuscation)
    - Πρόκληση/απόκριση (challenge/response)
    - Κουπόνι έγκρισης (consent token)
      - κόστος (υπολογιστικό/οικονομικό)
  - Εντοπισμός (detection)
  - Αντίδραση (handling)

# SPAM

---

- Μηχανισμοί αντιμετώπισης
  - Πρόληψη (prevention)
  - Εντοπισμός (detection)
    - Μαύρες λίστες
    - Ανάλυση περιεχομένου
    - Συνεργατικό φιλτράρισμα
    - Συστήματα υπολήψεων
    - Ανάλυση ίχνους
      - Ποσότητα, συχνότητα mails για αποστολή
  - Αντίδραση (handling)

# SPAM

---

- Μηχανισμοί αντιμετώπισης
  - Πρόληψη (prevention)
  - Εντοπισμός (detection)
  - Αντίδραση (handling)
    - Καραντίνα (Quarantine)
    - Περιορισμός ρυθμού (Limit Rate)
    - Απόρριψη (Reject)
    - Ετικέτα (Label)
    - Χρέωση (Charge)

# SPAM

---

- Ως τώρα συμπεράσματα:
  - Ανοικτό θέμα για μία δεκαετία
  - Μία τεχνική δεν αρκεί
    - Συνήθως συγκερασμός με φίλτρα αποφάσεων
  - Αρκετοί ISPs είναι μάλλον απρόθυμοι για συνεργασία
  - Θεσμικό πλαίσιο ισχυρό
    - απαγορεύει χρήση περιεχομένου από τρίτες οντότητες για ανάλυση
  - Ποσοστά εξαπάτησης – σημαντικά
  - Δεν διαφαίνεται bottleneck εξαιτίας των SPAMs στο Internet

# SPAM & SPIT

---

- SPIT
  - Spam over Internet Telephony
  - Αυτόκλητη μαζική (κερδοσκοπική) κλήση τηλεφωνικών αριθμών
- Ευτυχώς μόνο ελάχιστα περιστατικά ως τώρα!
  - Αλλά και στην δεκαετία 80's μόνο ελάχιστα περιστατικά SPAM
- Εκδηλώνεται σε πρωτόκολλα εγκατάστασης συνόδου για μεταφορά φωνής και πολυμέσων πάνω από το δημόσιο Internet
  - Π.χ. SIP – Session Initiation Protocol

# SPAM & SPIT

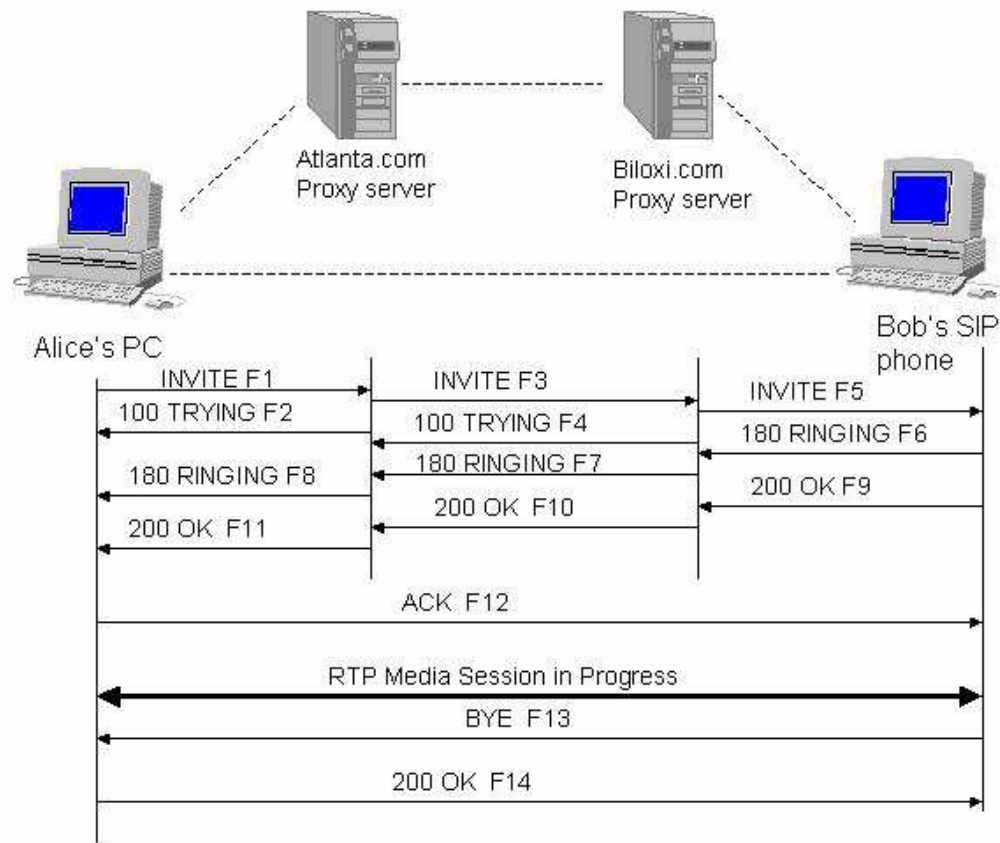
---

## ■ Τι είναι το SIP

- πρωτόκολλο επιπέδου εφαρμογής για **εγκατάσταση, τροποποίηση ή τερματισμό** συνόδων μεταξύ δύο ή περισσότερων χρηστών
- Με την εγκατάσταση συνόδου ακολουθεί η μετάδοση περιεχομένου μεταξύ των χρηστών
  - με χρήση άλλων πρωτοκόλλων (π.χ. RTP, RTSP)

# SPAM & SPIT

## ■ Αρχιτεκτονική SIP



# SPAM & SPIT

---

- Τι είναι το SIP
  - Λειτουργίες πρωτόκολλου
    - Εντοπισμός τελικού χρήστη
    - Ανταλλαγή πληροφοριών
    - Εγκαθίδρυση συνόδου
    - Τροποποίηση συνόδου
    - Τερματισμός συνόδου
    - Εγγραφή χρήστη σε καταλόγους
  - Ομοιάζει τόσο με το SMTP όσο και με το HTTP

# SPAM & SPIT

---

- Ομοιότητες ή διαφορές
  - Όλες οι τεχνικές αποστολής SPAM μπορούν να εφαρμοστούν και στο SPIT
  - Ορισμένες τεχνικές αντιμετώπισης SPAM μπορούν να εφαρμοστούν και στο SPIT
  - Μπορούν να πραγματοποιηθούν με αυτόματο τρόπο
    - SPAM: ναι
    - SPIT : ναι στο μέλλον
  - Κόστος πραγματοποίησης
    - SPAM: ελάχιστο
    - SPIT : υψηλό

# SPAM & SPIT

---

- Ομοιότητες ή διαφορές
  - Φόρτος (Bottleneck) στο δίκτυο
    - SPAM: ελάχιστο-μέτριο
    - SPIT : σημαντικό-υψηλό
  - Περιεχόμενο αυτόκλητου μηνύματος
    - SPAM: Text
    - SPIT : Text/Audio/Video/Images
  - Εκλαμβανόμενη από το χρήστη ενόχληση
    - SPAM: μέτρια
    - SPIT : υψηλή
  - SPAM σε επίπεδο περιεχομένου ενώ SPIT και σε επίπεδο σηματοδότησης

# Anti-SPIT

---

- Εύκολα ή δύσκολα;
  - Δύσκολο το φιλτράρισμα του περιεχομένου
    - Είναι πραγματικού χρόνου video/audio stream
    - Νομοθεσία περί απορρήτου
  - Εύκολο το φιλτράρισμα του signaling (SMTP/HTTP like)
    - Αλλά όχι αποτελεσματικό
    - Το πραγματικό junk μήνυμα μάλλον υπάρχει στο περιεχόμενο !!

# Anti-SPIT και έργο SPIDER

## ■ Ευρωπαϊκό έργο SPIDER

- ❑ Ασφαλής διαχείριση ανεπιθύμητων τηλεφωνικών κλήσεων μέσω του διαδικτύου
- ❑ Κατηγορία: FP6, COOP-2006
- ❑ Ημερομηνία έναρξης: 01.09.2006
- ❑ Ημερομηνία λήξης: 31.08.2008
- ❑ Συμμετοχή τμήματος Πληροφορικής Οικονομικού Πανεπιστημίου Αθηνών
- ❑ Στόχος: Σχεδιασμός και υλοποίησης μεθόδων anti-SPIT

Visit <http://projectspider.org/>

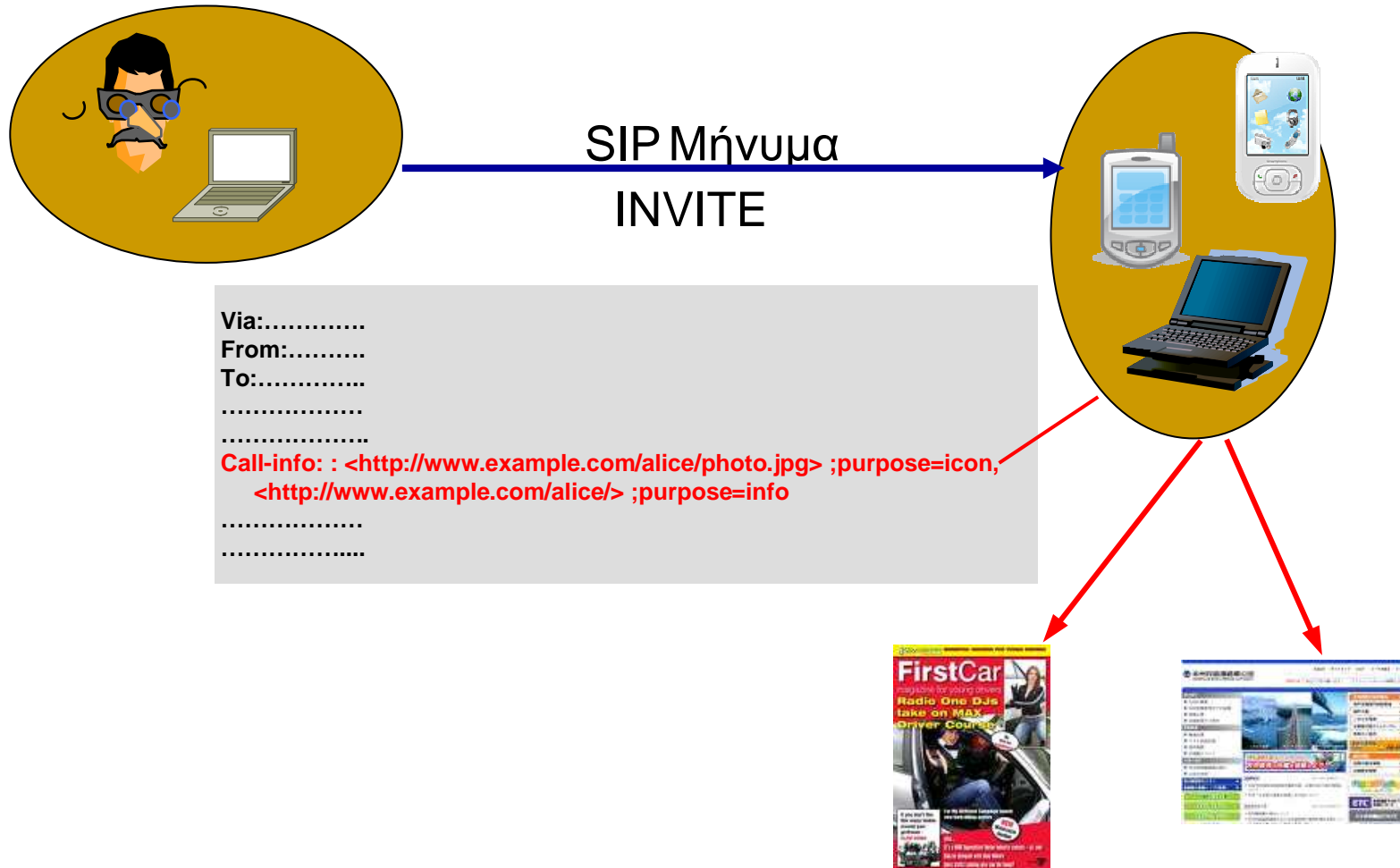
# Anti-SPIT και έργο SPIDER

---

- Ευρωπαϊκό έργο SPIDER
  - Στην πρώτη φάση το Ο.Π.Α. διακρίβωσε ευπάθειες του SIP λόγω
    - Σχεδιαστικών ατελειών στη δομή των μηνυμάτων και στη λειτουργία του πρωτοκόλλου
    - Προαιρετικών λειτουργιών που δεν υλοποιούνται στην πράξη
    - Διαλειτουργικότητας με άλλα, ευπαθή πρωτόκολλα
  - Διακριβώθηκαν πάνω από 30 ευπάθειες
    - πριν ακόμα εγκατασταθεί σύνοδος !

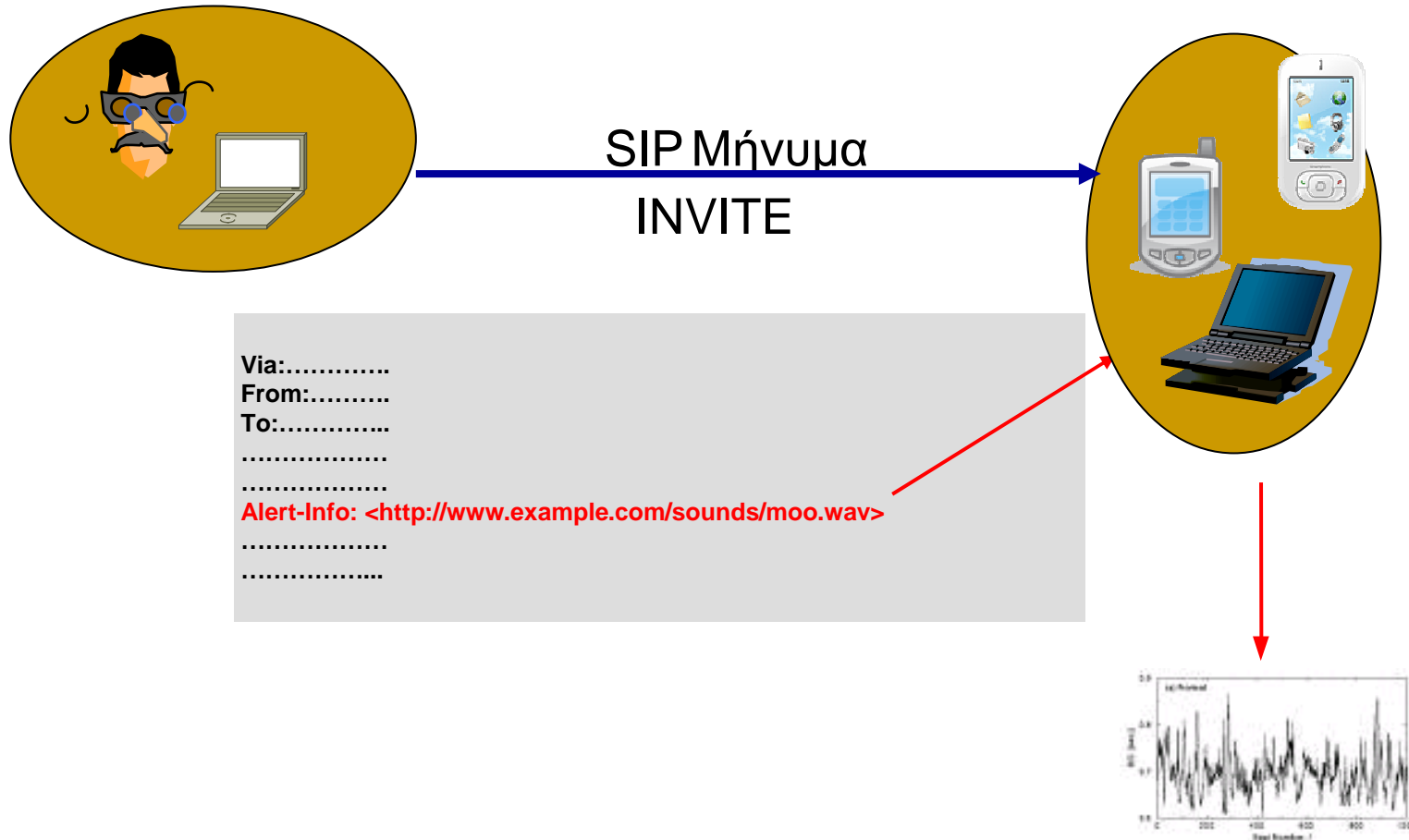
# Anti-SPIT και έργο SPIDER

## ■ Ευπάθειες SIP



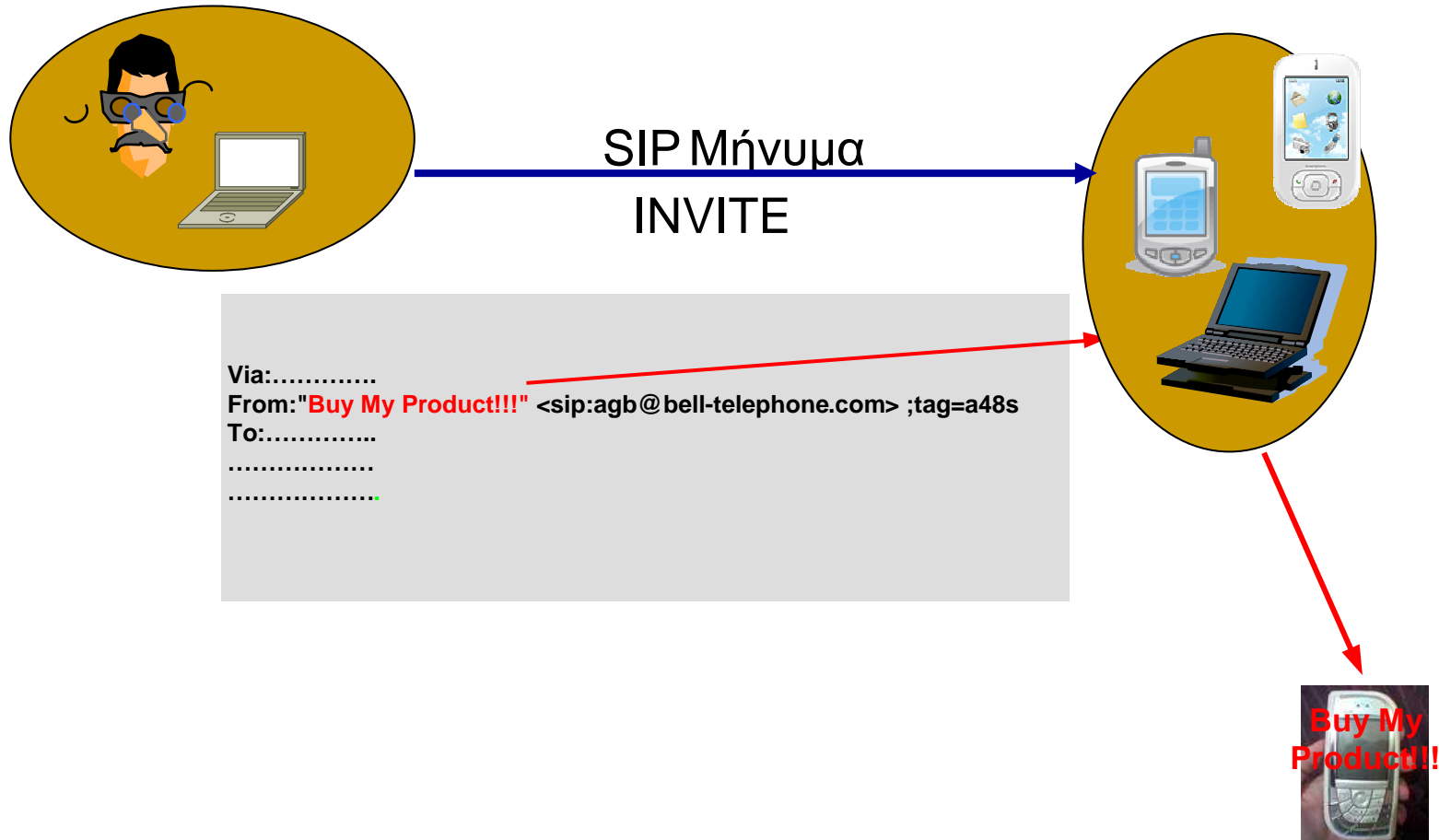
# Anti-SPIT και έργο SPIDER

## ■ Ευπάθειες SIP



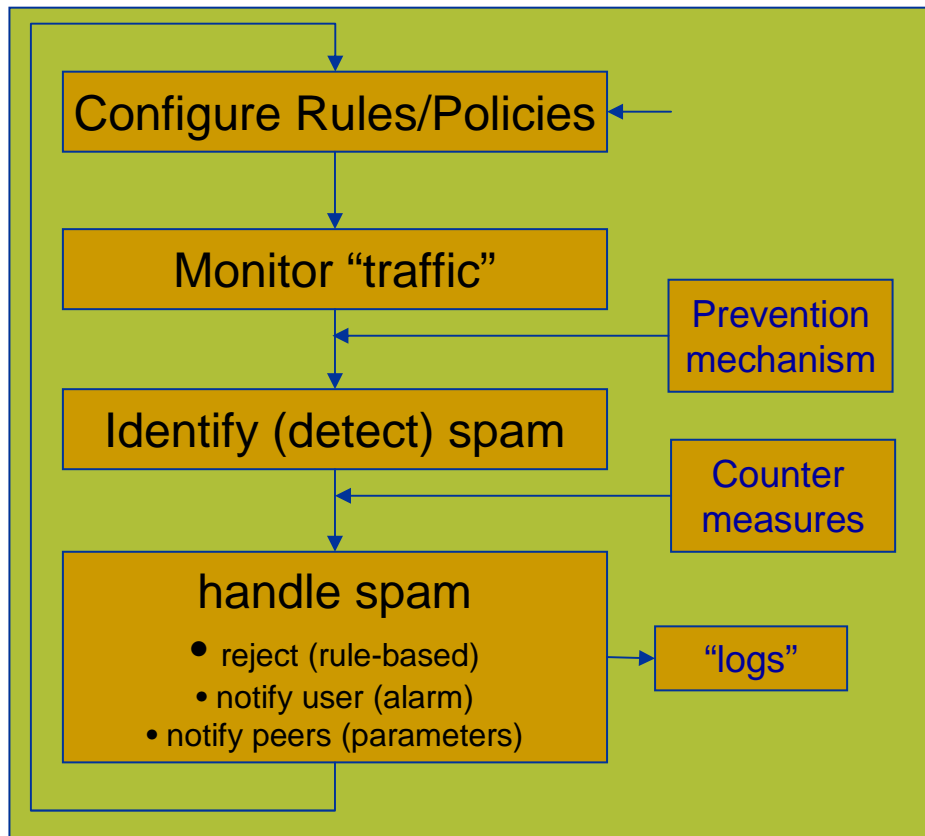
# Anti-SPIT και έργο SPIDER

## ■ Ευπάθειες SIP



# Anti-SPIT και έργο SPIDER

## ■ Αρχιτεκτονική anti-SPIT στο SPIDER



- Ανάγκη για ολοκληρωμένο πλαίσιο
  - Συμμετοχή χρήστη
  - Συνδυασμός
    - πρόληψης,
    - ανίχνευσης,
    - αντιμετώπισης
  - Συναίνεση παρόχων
  - Συνεργασία παρόχων
  - Ενδεδειγμένη αξιολόγηση
  - Θεσμικές επιταγές

# Anti-SPIT και έργο SPIDER

## ■ Κατηγοριοποίηση anti-SPIT μηχανισμών

*Αποτροπή*   *Ανίχνευση*   *Αντιμετώπιση*

|                          |                                  |                              |                                               |                                        |
|--------------------------|----------------------------------|------------------------------|-----------------------------------------------|----------------------------------------|
| Φιλτράρισμα Περιεχομένου | Συστήματα βασισμένα στη φήμη     | Υπολογιστικοί γρίφοι         | Γκρίζες λίστες                                | Ανατροφοδότηση πληροφοριών από χρήστες |
| Μαύρες Λίστες            | Παραποίηση της διεύθυνσης        | Πληρωμές με ρίσκο            | Βιομετρικό πλαίσιο πρόληψης spit              | Χρήση SIP Identity                     |
| Λευκές Λίστες            | Διευθύνσεις περιορισμένης χρήσης | Ομάδες εμπιστοσύνης          | Στατιστική ανάλυση της σηματοδότησης του VoIP | Πρόληψη του spit με χρήση της SAML     |
| Συναινετική Επικοινωνία  | Τεστ Turing                      | Κεντριοποιημένοι πάροχοι SIP | Διαφοροποιημένο SIP                           |                                        |

# Anti-SPIT και έργο SPIDER

---

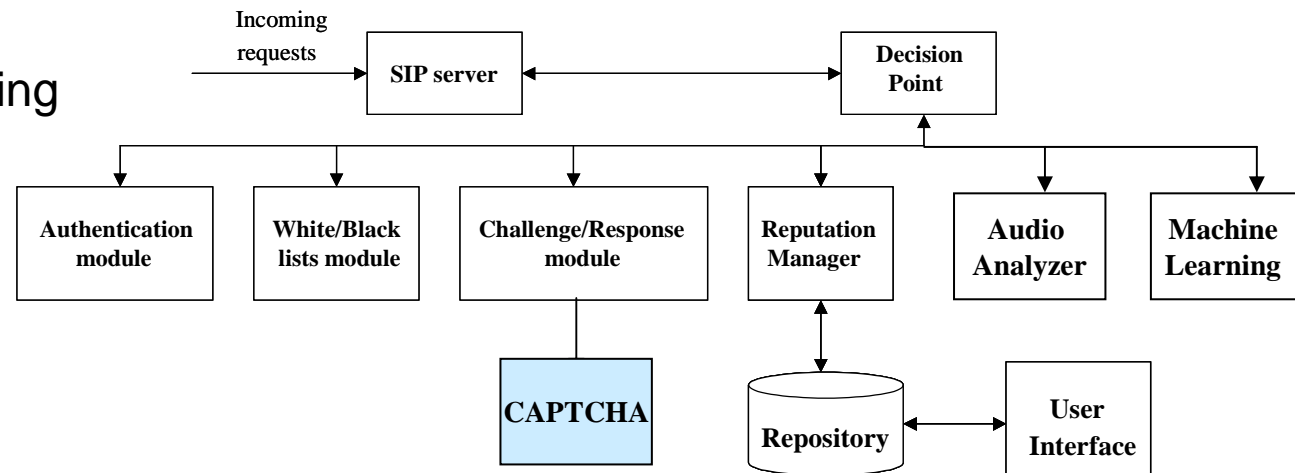
- Κριτήρια αποτίμησης anti-SPIT μηχανισμών
  - Επιτυχία
    - Ποσοστό SPIT κλήσεων που ανιχνεύεται
  - Αξιοπιστία
    - False positives / False negatives
  - Ταχύτητα ανάδρασης
  - Απαιτήσεις σε πόρους
    - Χρήστη
    - Δίκτυο
  - Οικονομικό κόστος
    - Παρόχου
  - Κλιμακοσιμότητα
  - Ιδιωτικότητα

# Anti-SPIT και έργο SPIDER

## ■ SPIDER anti-SPIT platform

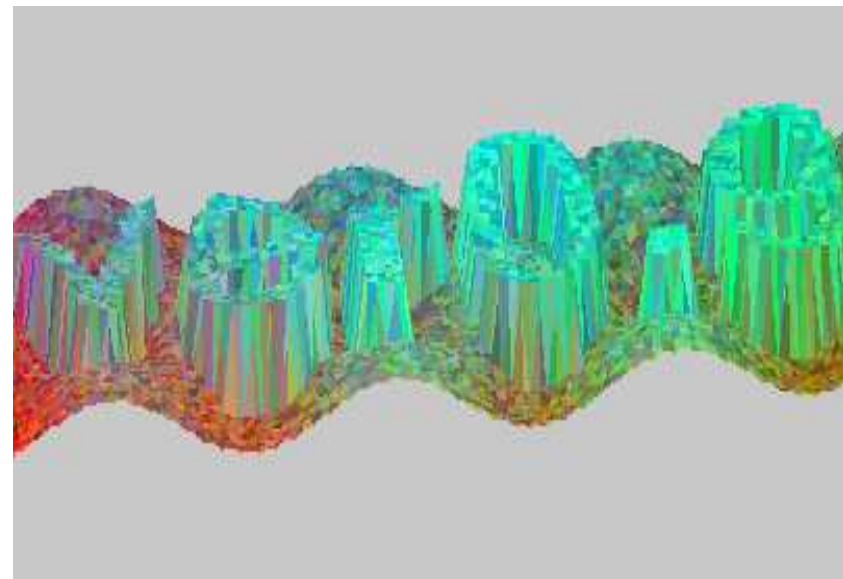
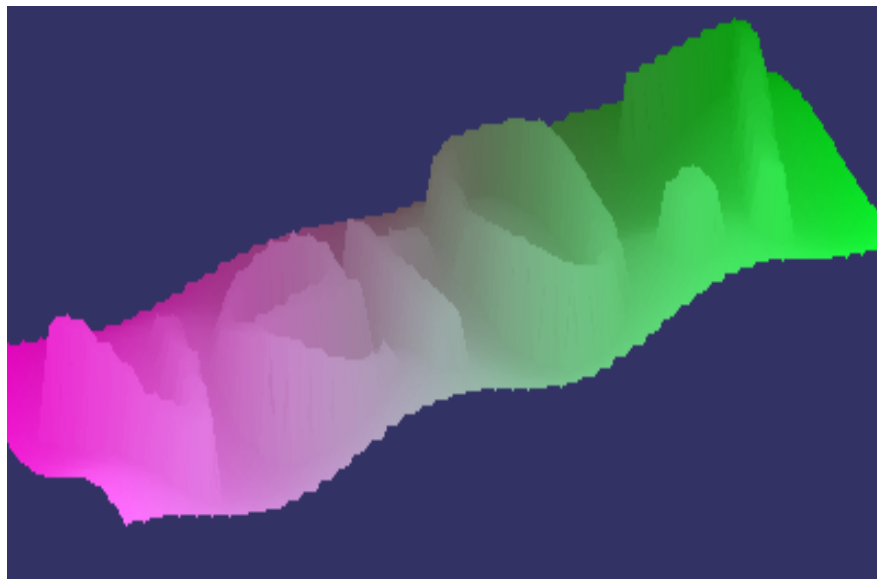
Συνδυασμός των ακόλουθων μεθόδων - τεχνικών

- ❑ Authentication
- ❑ White/Black list
- ❑ Challenge/Response
- ❑ Reputation manager
- ❑ Audio analyser
- ❑ Machine Learning



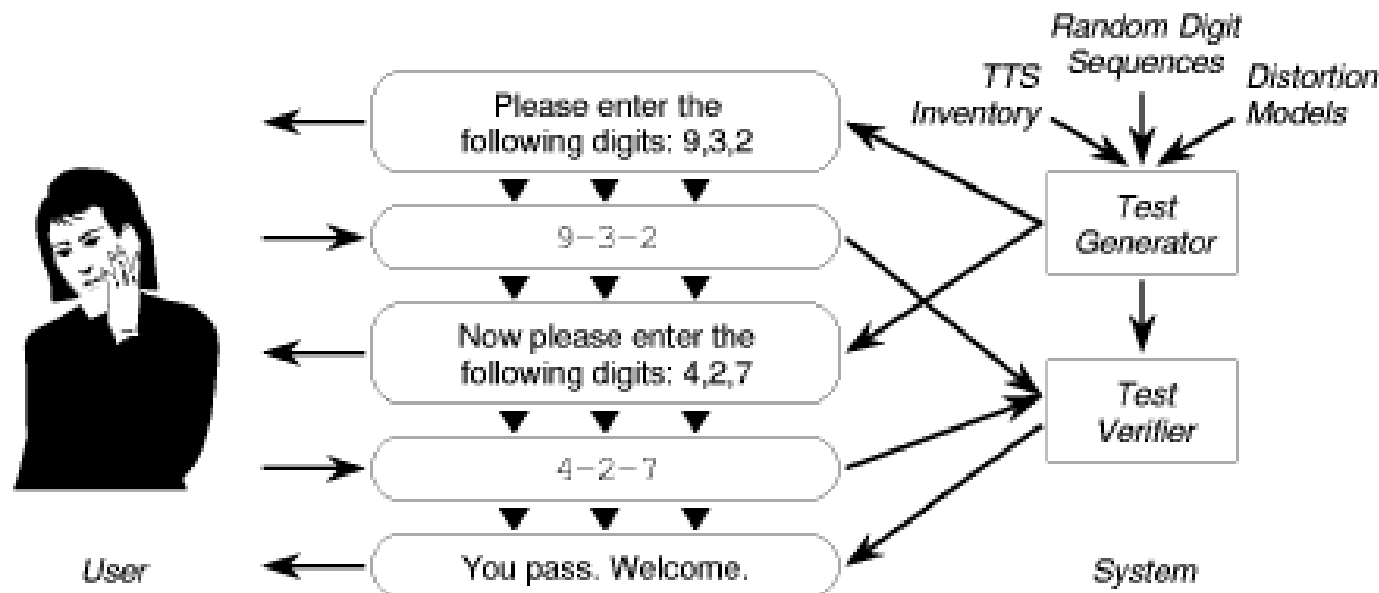
# Anti-SPIT και έργο SPIDER

- SPIDER anti-SPIT platform
  - CAPTCHA - Completely Automated Public Turing test to tell Computers and Humans Apart
  - VISUAL



# Anti-SPIT και έργο SPIDER

- SPIDER anti-SPIT platform
  - CAPTCHA - Completely Automated Public Turing test to tell Computers and Humans Apart
  - Audio



# Επίλογος

---

- Εκτιμάται ότι το SPIT είναι προ των πυλών
  - Χρειάζονται καλύτερα botnets
  - Περισσότεροι χρήστες
    - Οι VoIP χρήστες είναι υποψιασμένοι
  - Φθηνότερες χρεώσεις από παρόχους
- Για να αντιμετωπιστεί θα πρέπει οι SIP servers να έχουν ενσωματωμένο anti-SPIT
  - Επίκαιρο εφόσον τώρα αναπτύσσονται
- Συνδυασμός anti-SPIT έχει αποτέλεσμα
- Ο τελικός χρήστης δεν αντέχει SPAM και SPIT

## Συζήτηση

***Δρ. Ιωάννης Μαριάς  
Λέκτορας Ασφάλειας Υπολογιστών κ' Δικτύων  
Τμήμα Πληροφορικής  
Οικονομικό Πανεπιστήμιο Αθηνών  
marias@aueb.gr***