

Threats and vulnerabilities in Internet Telephony: Focusing on the SPIT phenomenon

Dimitris Gritzalis

June 2014 (revised)



Απειλές και Τρωτότητες στη Διαδικτυακή Τηλεφωνία: Αντιμετώπιση SPIT (SPam over Internet Telephone)



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



Εργαστήριο Ασφάλειας Πληροφοριών και Προστασίας Κρίσιμων Υποδομών
Τμήμα Πληροφορικής, Οικονομικό Πανεπιστήμιο Αθηνών

Δομή παρουσίασης

Διαδικτυακή Τηλεφωνία

VoIP και SIP

Ασφάλεια και VoIP

Περιστατικά SPIT

email spam vs. voice spam

Αντιμετώπιση SPIT

Αξιολόγηση υπαρχουσών προσεγγίσεων

Υστερήσεις και ελλείψεις

Αρχιτεκτονική antiSPIT

Προτεινόμενη αρχιτεκτονική

Ανάλυση απειλών/τρωτοτήτων SIP

Μοντελοποίηση επιθέσεων SPIT

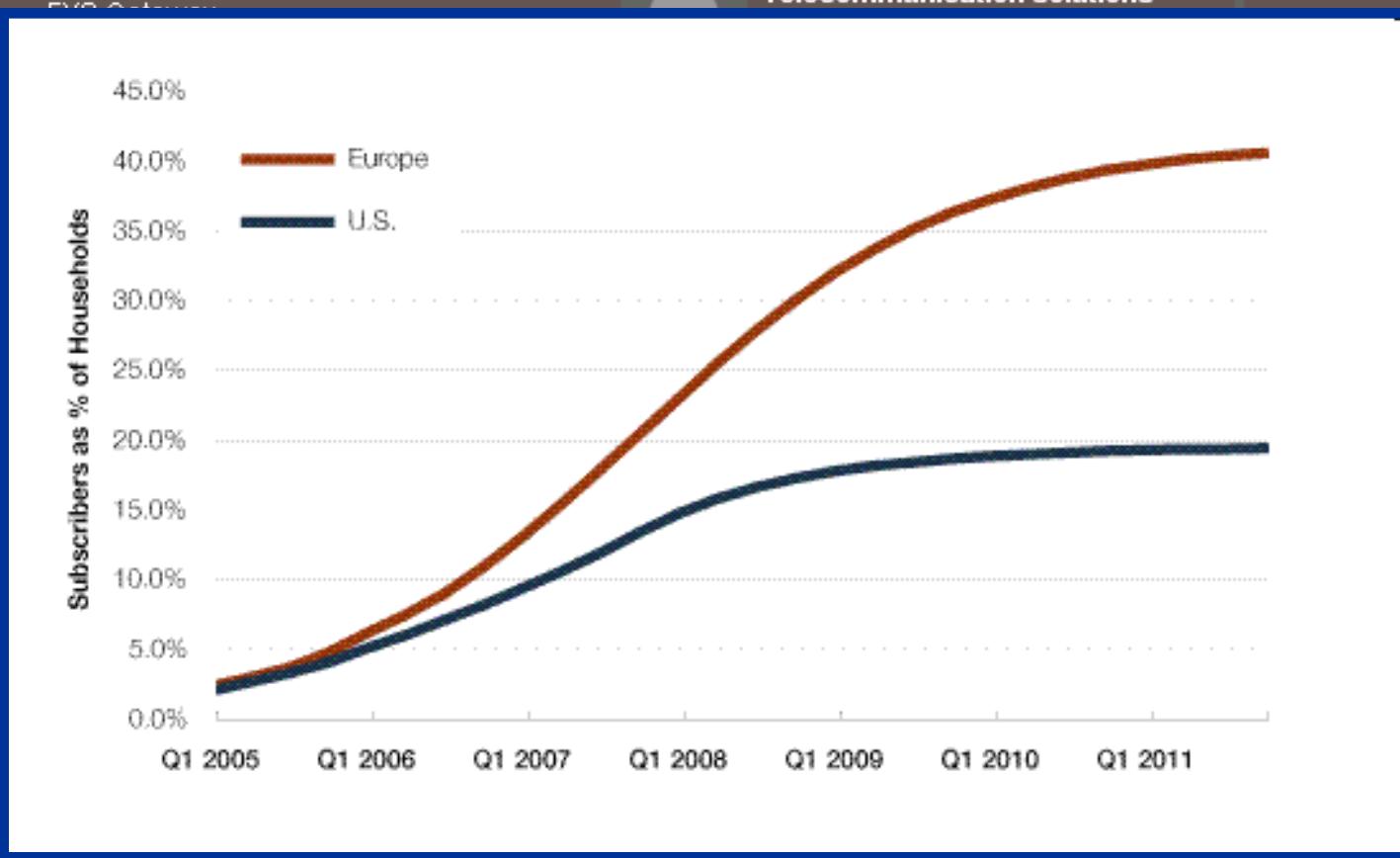
Κριτήρια ανίχνευσης SPIT

OntoSPIT

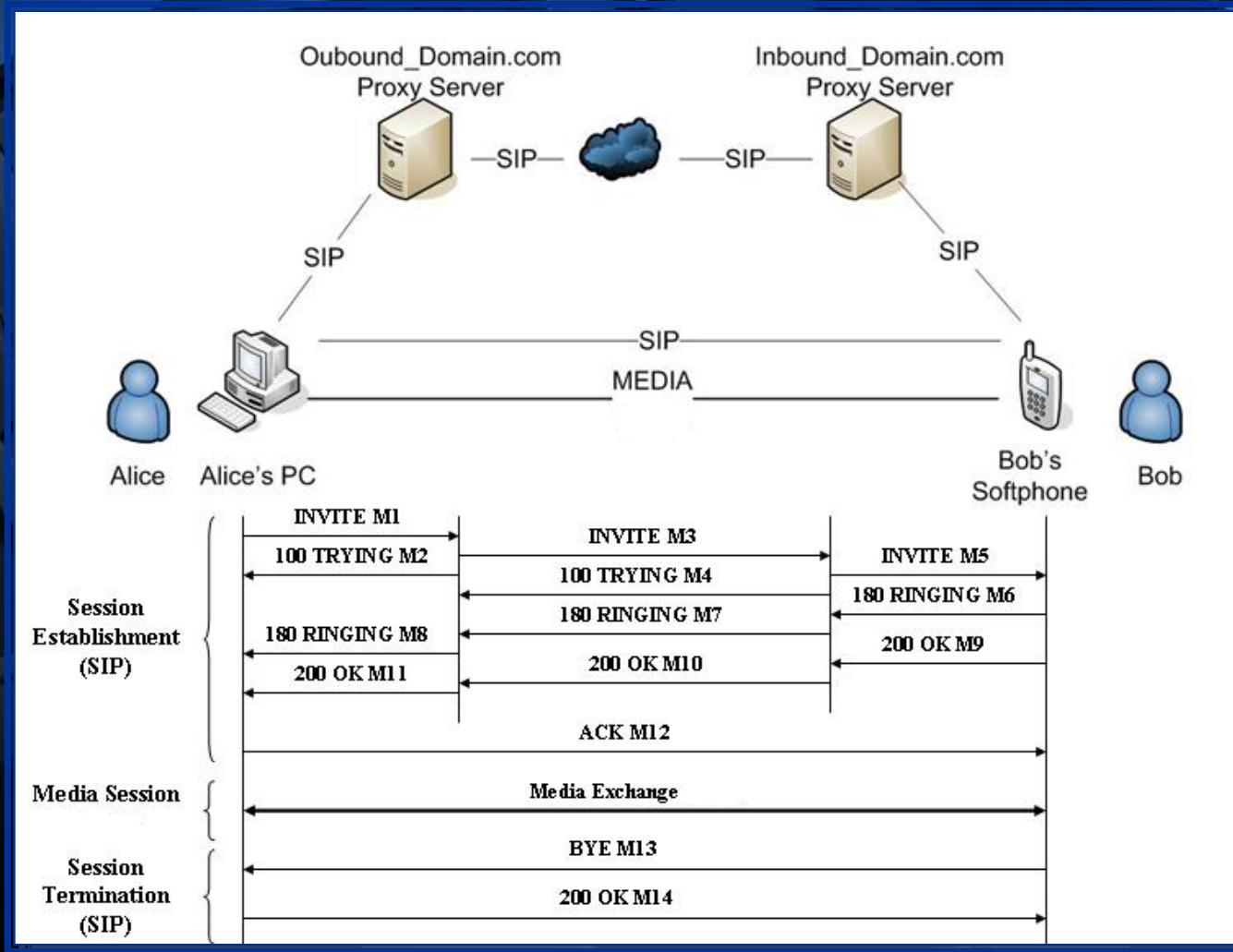
antiSPIT audio CAPTCHA

Αξιολόγηση antiSPIT

Διαδικτυακή Τηλεφωνία (Voice-over-IP)

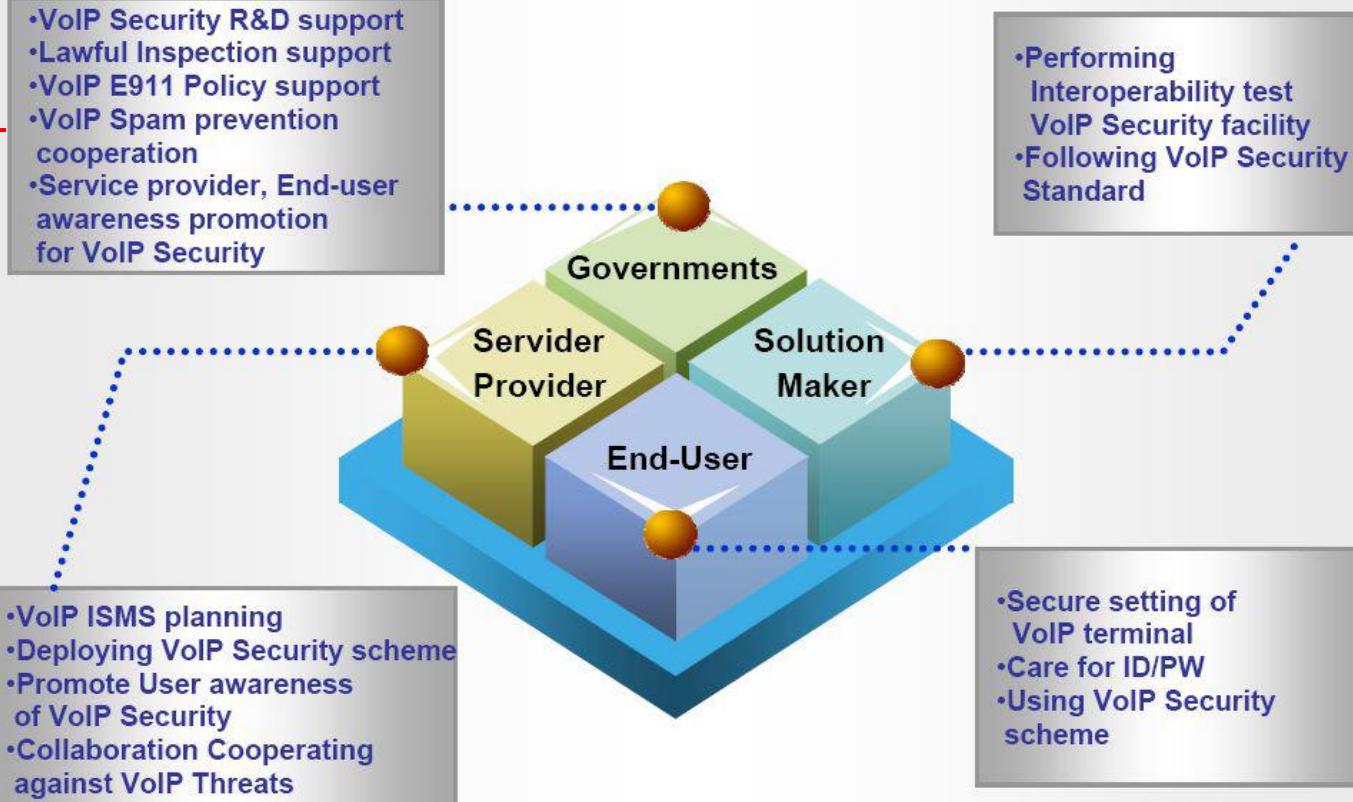


Session Initiation Protocol (SIP)



J. Rosenberg, et al., *Session Initiation Protocol*, RFC 3261, June 2002.

Ζητήματα Ασφάλειας σε VoIP



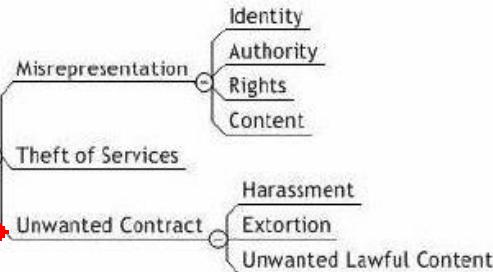
Ζητήματα Ασφάλειας σε VoIP

Ασφάλεια (ISO 17799):
Εμπιστευτικότητα - Ακεραιότητα - Διαθεσιμότητα

Confidentiality

- Call Black Holing
- Call Rerouting
- Fax Alteration
- Conversation Alteration
- Conversation Degrading
- Conversation Hijacking

Interception & Modification



SPIT

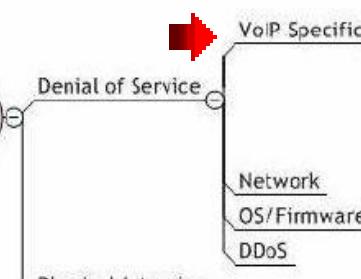
- Call Pattern Tracking
- Number Harvesting
- Fax Reconstruction
- Conversation Reconstruction

Eavesdropping

- Loss of Power
- Resource Exhaustion
- Performance Latency

Unintentional Interruption

Integrity



Availability

SPam over Internet Telephony (SPIT)

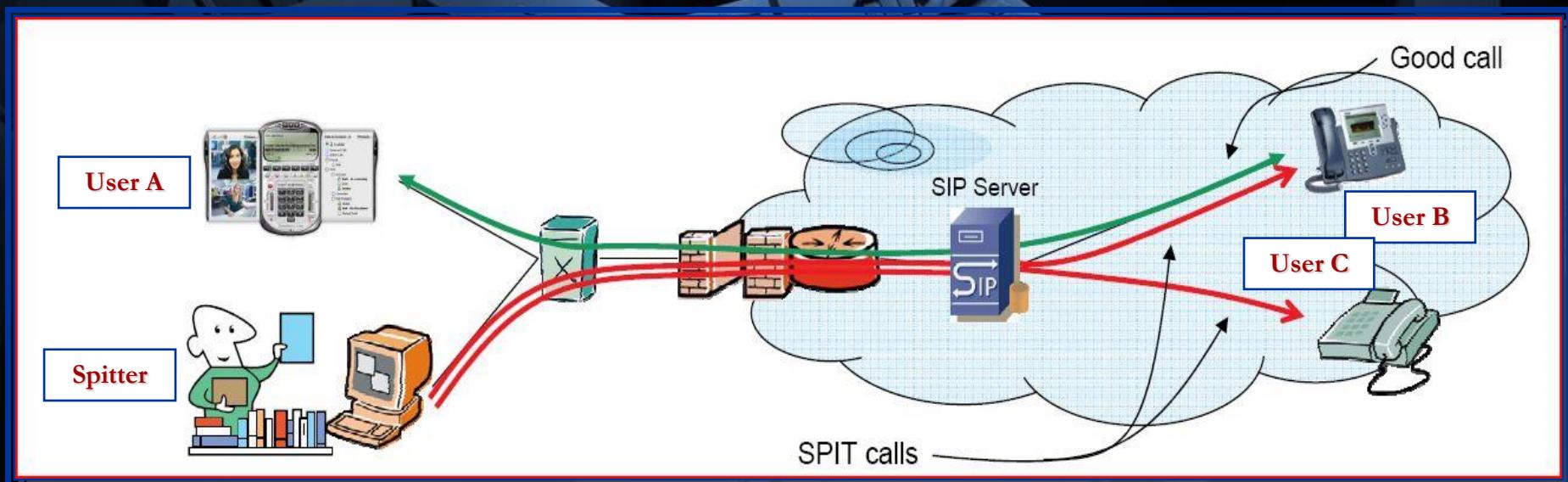
Μαζική αποστολή

απρόσκλητων

Κλήσεων

Μηνυμάτων

Αιτημάτων παρουσίας



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

Συγκλίσεις

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

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 **κείμενο**, 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.

Μηχανισμοί αντιμετώπισης SPIT

1. SPIT prevention using Anonymous Verifying Authorities:
2. SPIT mitigation through a network layer anti-SPIT entity
3. SPIT detection based on reputation and charging techniques:
4. DAPES (Domain-based Authentication and Policy-Enforced for SIP)
5. PMG (Progressive Multi Gray-Levelling)
6. Biometric framework for SPIT prevention
7. RFC 4474 (Enhancements for Authenticated Identity Management in SIP)
8. SAML (SIP Security Assertion Markup Language)
9. DSIP: Differentiated SIP
10. **VoIP SEAL** (NEC)
11. **VSD (Voice Spam Detector)** (University of North Texas)

Δυνατότητες και υστερήσεις μηχανισμών

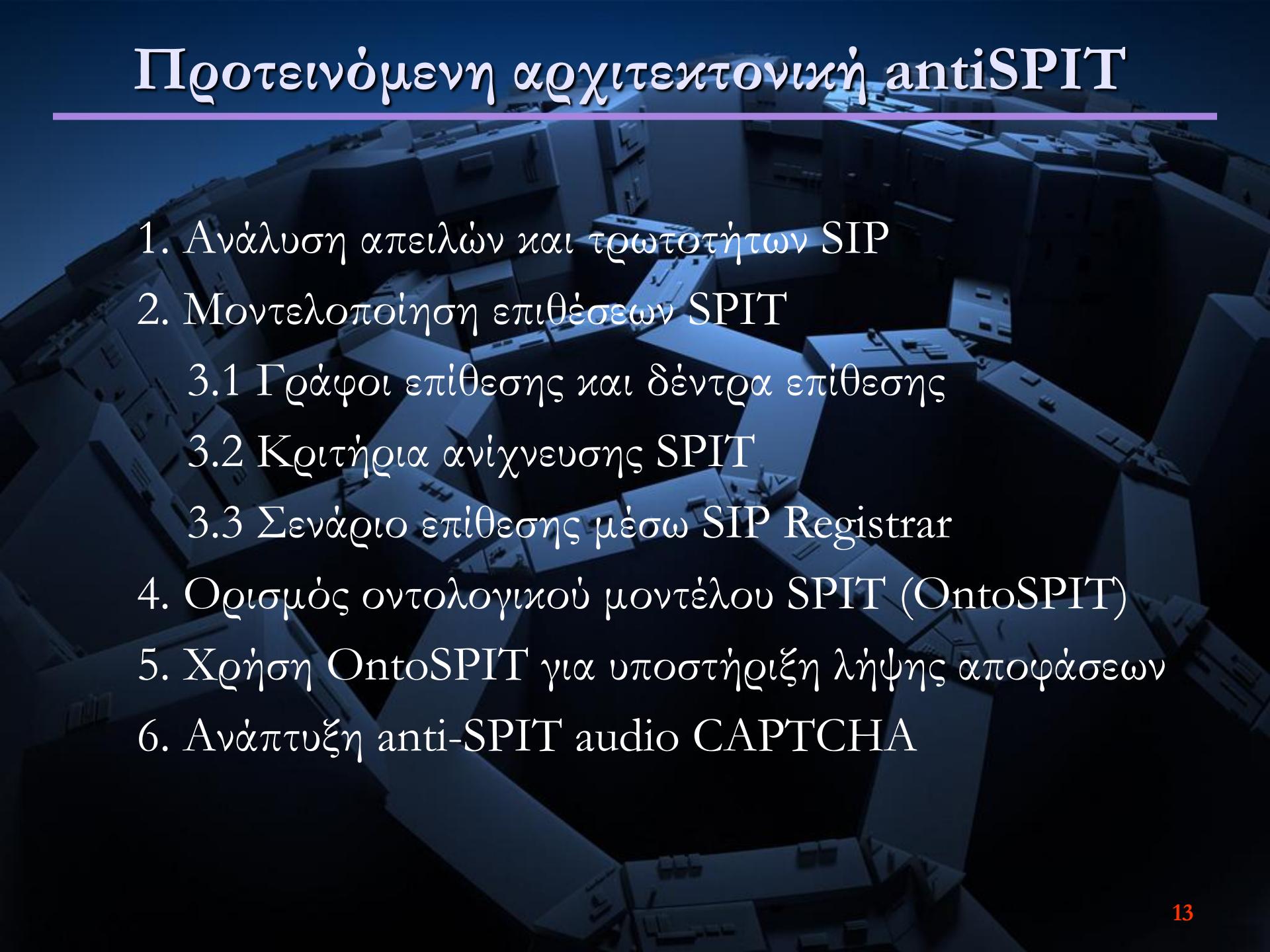
| Criteria | Percentage of SPIT calls avoided | Reliability | Promptitude | Human Interference | Resources Overhead | Vulnerabilities | Privacy Risk | Scalability | Adoption | Availability |
|---------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------|-------------------------------------|-------------------------------------|-------------------------------------|----------|--------------|
| | Anti-SPIT Mechanisms | | | | | | | | | |
| AVA | - | - | - | - | - | - | - | - | - | - |
| Anti-Spit Entity | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | - | - | <input checked="" type="checkbox"/> | - | - | - | - |
| Reputation/Charging | - | - | - | - | - | - | - | - | - | - |
| DAPES | - | - | - | - | - | - | <input checked="" type="checkbox"/> | - | - | - |
| PMG | <input checked="" type="checkbox"/> | - | - | <input checked="" type="checkbox"/> | - | - | <input checked="" type="checkbox"/> | - | - | - |
| Biometrics | - | - | - | <input checked="" type="checkbox"/> | - | - | <input checked="" type="checkbox"/> | - | - | - |
| RFC 4474 | - | - | - | - | - | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | - | - |
| SIP SAML | - | - | - | <input checked="" type="checkbox"/> | - | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | - | - |
| DSIP | - | - | - | - | - | <input checked="" type="checkbox"/> | - | - | - | - |
| VoIP Seal | - | - | - | <input checked="" type="checkbox"/> | - | - | - | - | - | - |
| VSD | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | - | <input checked="" type="checkbox"/> | - | - | - | <input checked="" type="checkbox"/> | - | - |

Marias G., Dritsas S., Theoharidou M., Mallios J., Gritzalis D., "SIP vulnerabilities and antiSPIT mechanisms assessment", in *Proc. of the 16th IEEE International Conference on Computer Communications and Networks (ICCCN '07)*, pp. 597-604, IEEE Press, USA, August 2007.

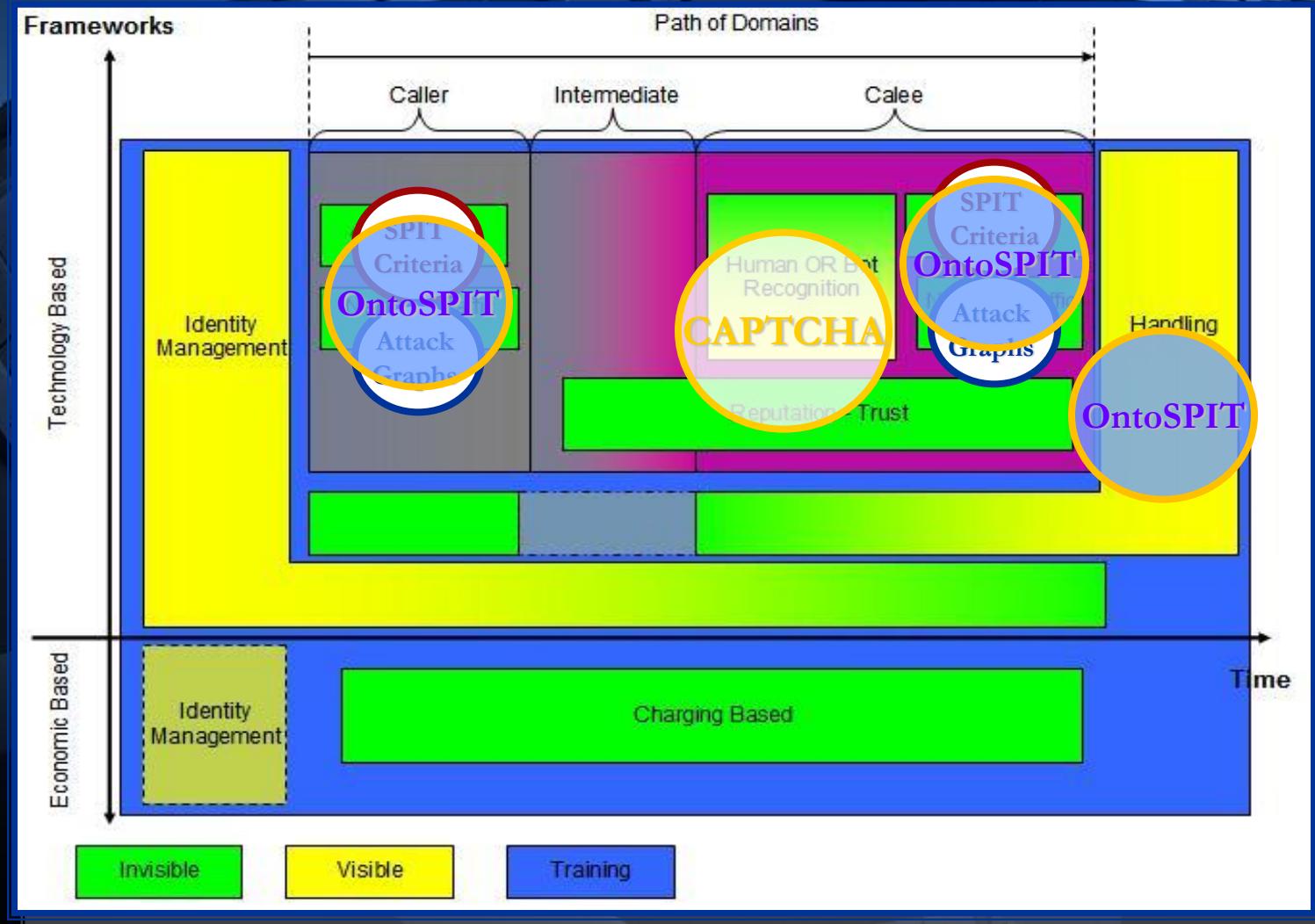
Βασικές αιτίες υστερήσεων

- Κατά κανόνα αποπειρώνται να υιοθετήσουν αντίστοιχες μεθόδους αντιμετώπισης του **email spam**.
- Αντιμετωπίζουν περιορισμένο υποσύνολο **απειλών και αδυναμιών** του SIP.
- **Εστιάζονται** και αφορούν το εκάστοτε τεχνολογικό περιβάλλον (ad-hoc προσέγγιση).
- Δεν μπορούν να αντιμετωπίσουν **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 σε **πραγματικές συνθήκες**.

Προτεινόμενη αρχιτεκτονική antiSPIT

- 
1. Ανάλυση απειλών και τρωτοτήτων SIP
 2. Μοντελοποίηση επιθέσεων SPIT
 - 3.1 Γράφοι επίθεσης και δέντρα επίθεσης
 - 3.2 Κριτήρια ανίχνευσης SPIT
 - 3.3 Σενάριο επίθεσης μέσω SIP Registrar
 4. Ορισμός οντολογικού μοντέλου SPIT (OntoSPIT)
 5. Χρήση OntoSPIT για υποστήριξη λήψης αποφάσεων
 6. Ανάπτυξη anti-SPIT audio CAPTCHA

Αρχιτεκτονική antiSPIT



Gritzalis D., Mallios Y., "A SIP-based SPIT management framework", *Computers & Security*, 2008 (to appear).

Ανάλυση απειλών και τρωτοτήτων SIP

Κατηγορία απειλών και τρωτοτήτων

Επιγραμματική περιγραφή αναγνωριζόμενων απειλών και τρωτοτήτων

Απειλές που οφείλονται σε εγγενείς τρωτότητες του πρωτοκόλλου

Αποστολή συγκεχυμένων μηνυμάτων αιτήσεων στους πληρεξούσιους εξυπηρετητές
Listening to a multicast address
Αποκάλυψη ενεργών διευθύνσεων
Αποστολή συγκεχυμένων μηνυμάτων στους εξυπηρετητές επανακατεύθυνσης
Δημιουργία πολλαπλών λογαριασμών SIP
Εκμετάλλευση stateless εξυπηρετητών
Ανώνυμοι εξυπηρετητές και B2B αντιπρόσωποι χρήστη
Αποστολή μηνυμάτων σε multicast διευθύνσεις
Εκμετάλλευση forking πληρεξούσιων εξυπηρετητών
Εκμετάλλευση της δομής μηνυμάτων και επικεφαλίδων

Απειλές και τρωτότητες που οφείλονται στις προαιρετικές συστάσεις του πρωτοκόλλου

Εκμετάλλευση εξυπηρετητών εγγραφής
Προαιρετική εφαρμογή μηχανισμών ασφαλείας
Προαιρετική χρήση και εφαρμογή μηχανισμών αυθεντικοποίησης
'Ελλειψη μηχανισμών ασφαλείας σε peer-to-peer επικοινωνία

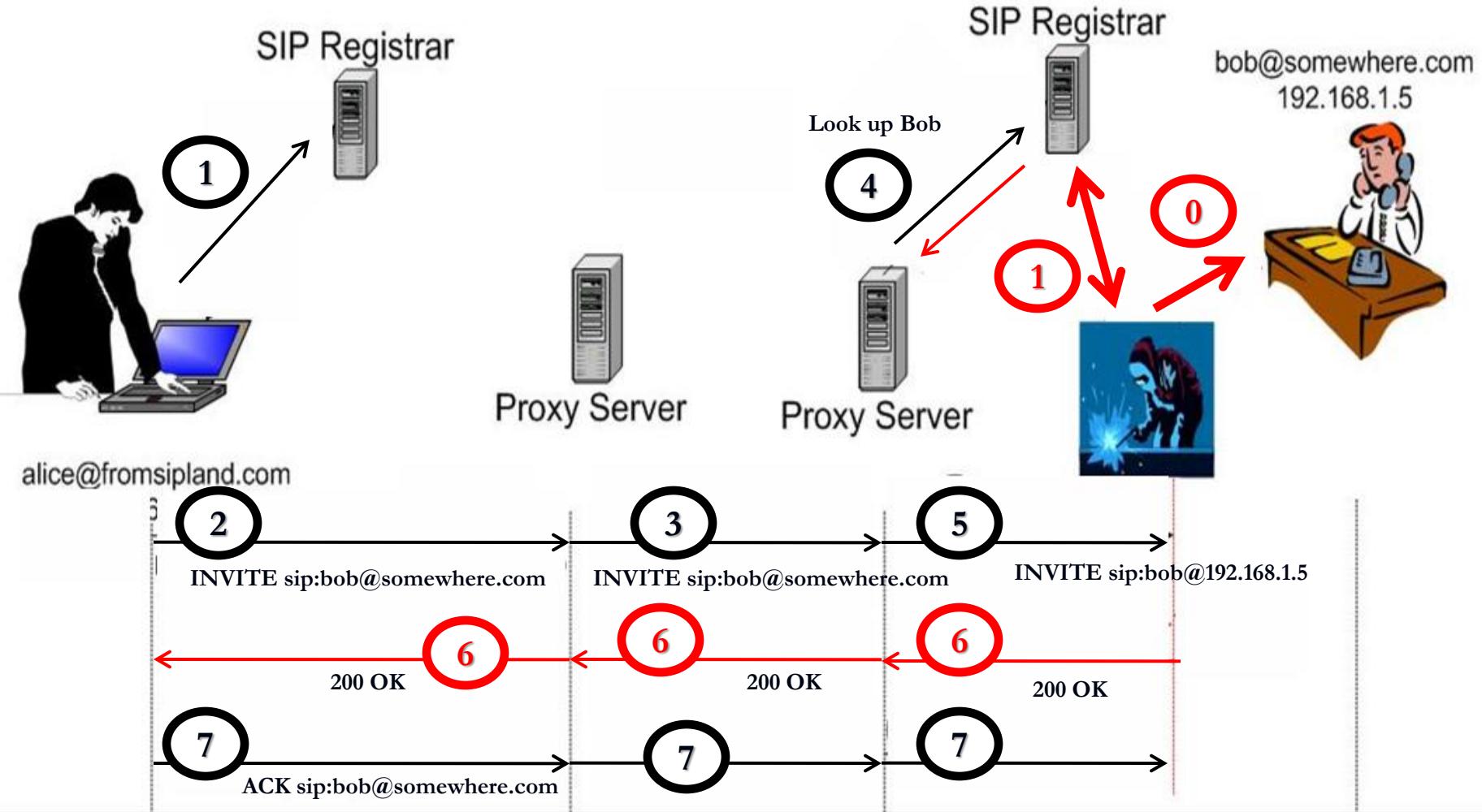
Απειλές και τρωτότητες που οφείλονται σε ζητήματα διαλειτουργικότητας του SIP με άλλα πρωτόκολλα.

Εκμετάλλευση διαδικασιών διευθυνσιοδότησης σε ένα δικτυακό τομέα

Απειλές και τρωτότητες που οφείλονται σε γενικά ζητήματα ασφάλειας

Παρακολούθηση κυκλοφορίας κοντά σε εξυπηρετητή SIP
Ανίχνευση γνωστών θυρών του SIP
Πληρεξούσιος εξυπηρετητής στο μέσο (Proxy-in-the-middle)
Εκμετάλλευση αιτήματος re-INVITE
Εκμετάλλευση πεδίου επικεφαλίδας Record-Route

Σενάριο επίθεσης μέσω SIP Registrar



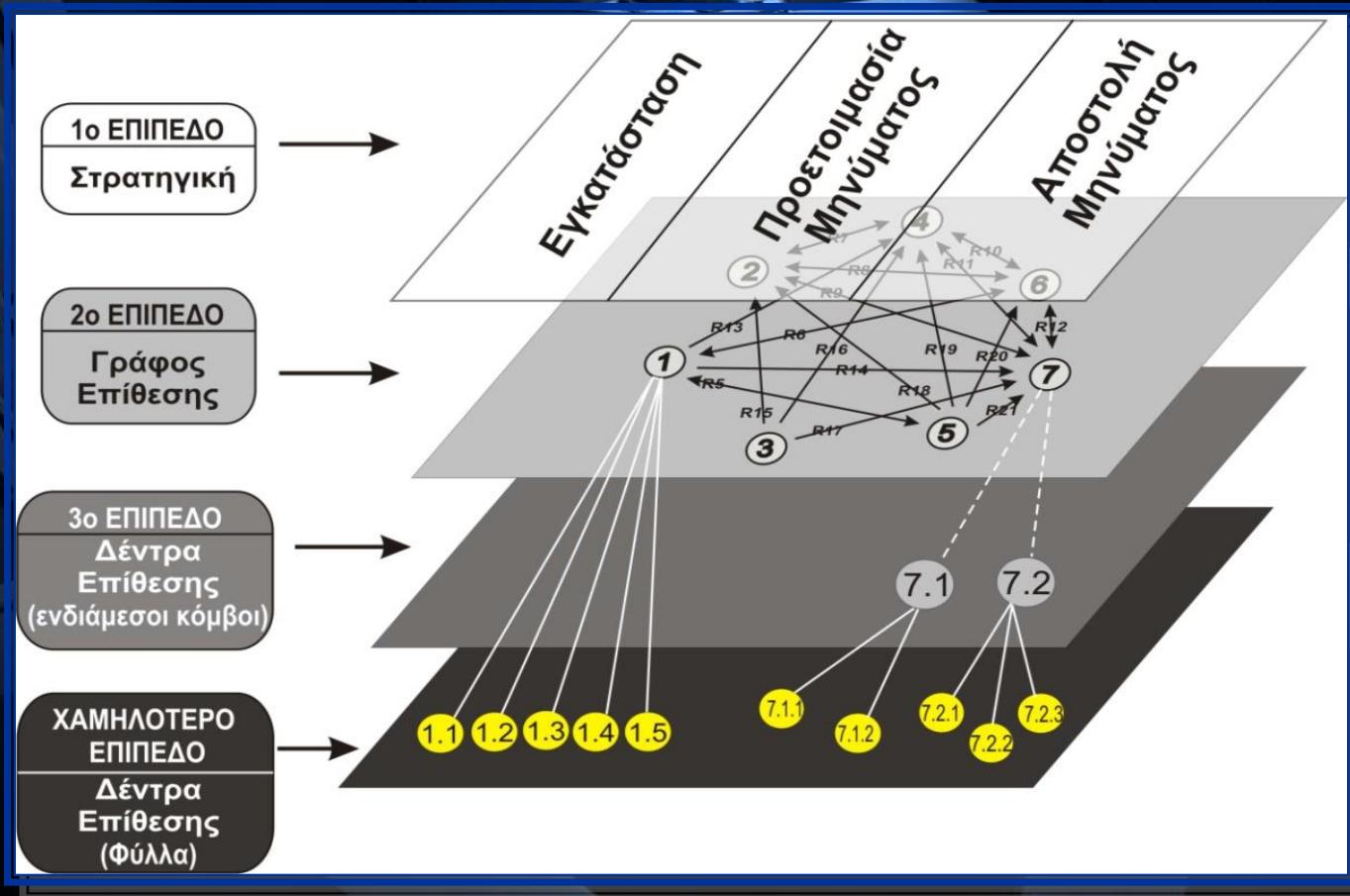
Welcome to account verification.
Please type your 16-digits card number.



Μοντελοποίηση επιθέσεων

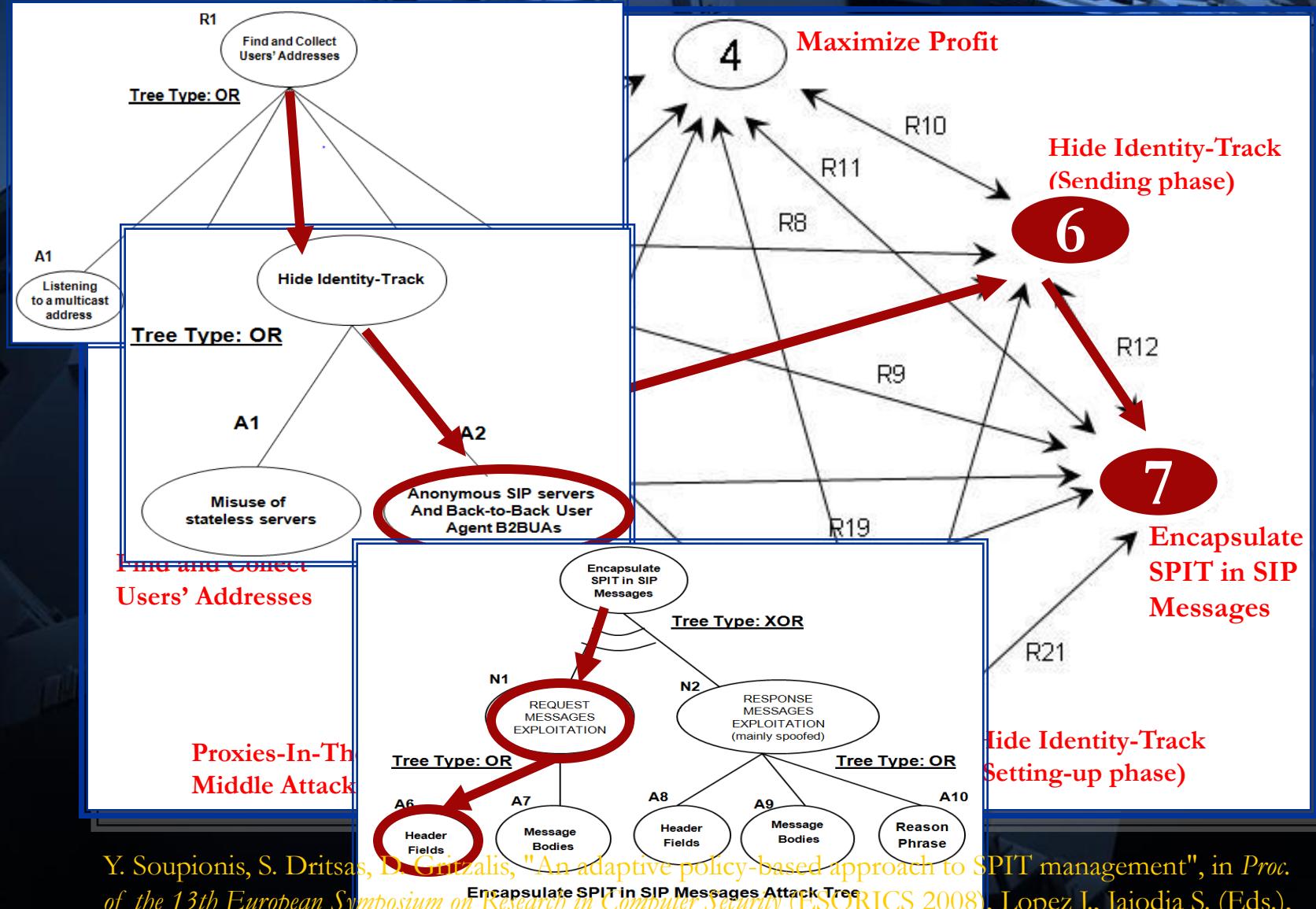
Έλλειψη ικανού πλήθους πραγματικών περιστατικών SPIT

Αναπαράσταση στιγμιότυπων (instances) προβλέψιμων περιστατικών SPIT



Mallios J., Dritsas S., Tsoumas B., Gritzalis D., "Attack modeling of SIP-oriented SPIT", in *Proc. of the 2nd IEEE-IFIP International Workshop on Critical Information Infrastructures Security (CRITIS '07)*, Lopez J., et al. (Eds.), LNCS 5141, Springer, Malaga, October 2007.

Γραφοανάλυση επίθεσης SPIT



Y. Soupionis, S. Dritsas, D. Gritzalis, "An adaptive policy-based approach to SPIT management", in *Proc. of the 13th European Symposium on Research in Computer Security (ESORICS 2008)*, Lopez J., Jajodia S. (Eds.), Springer, Malaga, October 2008 (to appear).

Κριτήρια ανίχνευσης SPIT

Κριτήρια προέλευσης μηνυμάτων-κλήσεων (SIP UserAgent-oriented)

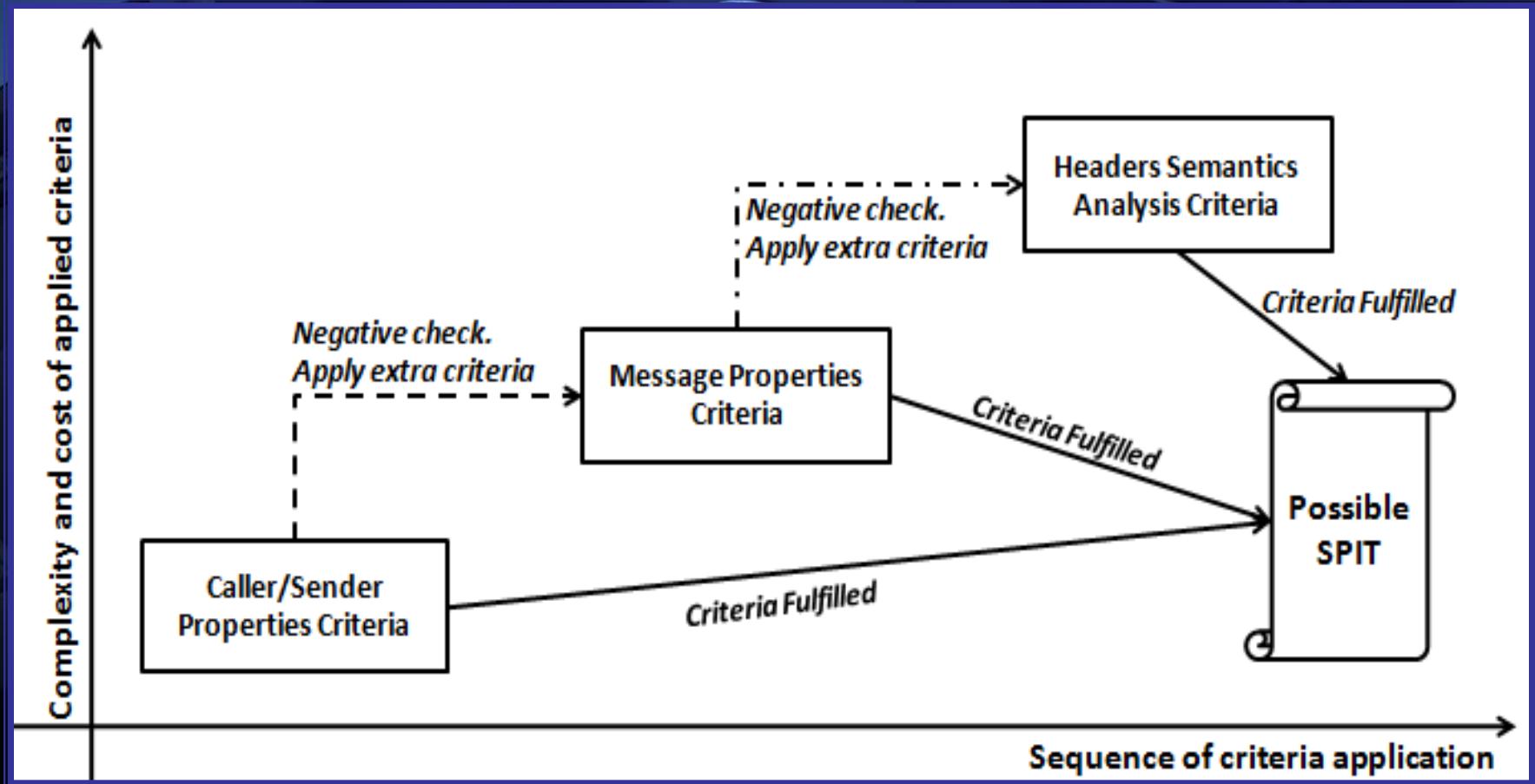
- SIP URI (Uniform Resource Identifier) του καλούντα
- IP διεύθυνση του καλούντα
- Δικτυακός τομέας (domain) του καλούντα

Μορφότυποι μηνυμάτων-κλήσεων (SIP Message-oriented)

- Διαδρομή SIP πακέτου (path traversal)
- Αριθμός κλήσεων/μηνυμάτων σε συγκεκριμένο χρονικό διάστημα
- Διάρκεια στατικών κλήσεων
- Μορφότυποι διεύθυνσης του καλούμενου
- Μικρό ποσοστό επιτυχών κλήσεων
- Μεγάλος αριθμός σφαλμάτων
- Μέγεθος SIP μηνύματος

S. Dritsas, J. Soupionis, M. Theoharidou, J. Mallios, D. Gritzalis, "SPIT Identification Criteria Implementations: Effectiveness and Lessons Learned", in *Proc. of the 23rd International Information Security Conference (SEC-2008)*, Samaratī P., et al. (Eds.), Springer, Milan, September 2008 (to appear).

Ιεραρχία εφαρμογής κριτηρίων



OntoSPIT: Οντολογία SIP-based SPIT

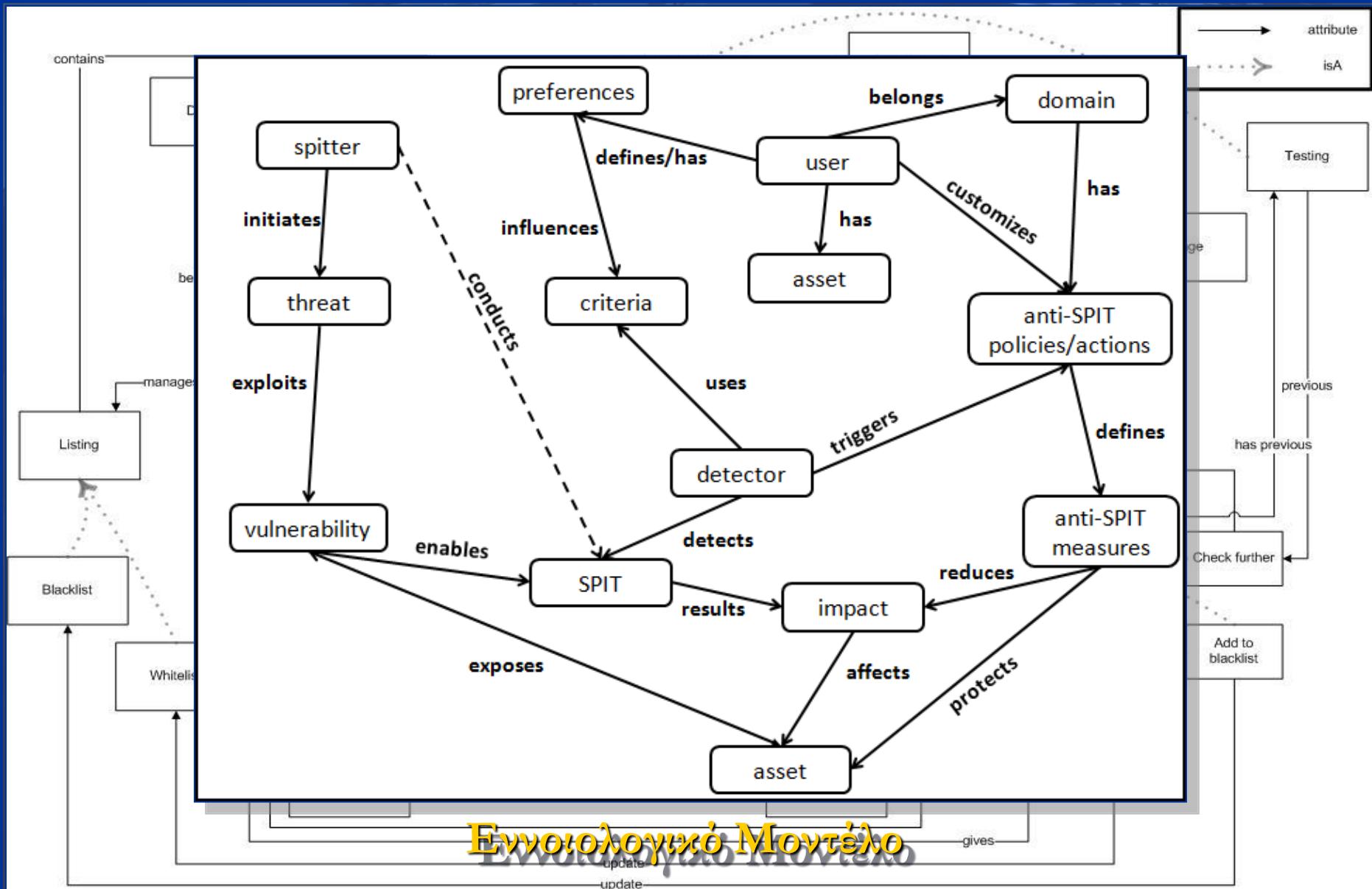
Αναπτύχθηκε μια **οντολογία** για το SIP-based VoIP πεδίο, η οποία:

Επιτυγχάνει τη σύνταξη του **λεξιλογίου** του πεδίου, καθορίζοντας την εννοιολογική του σύσταση.

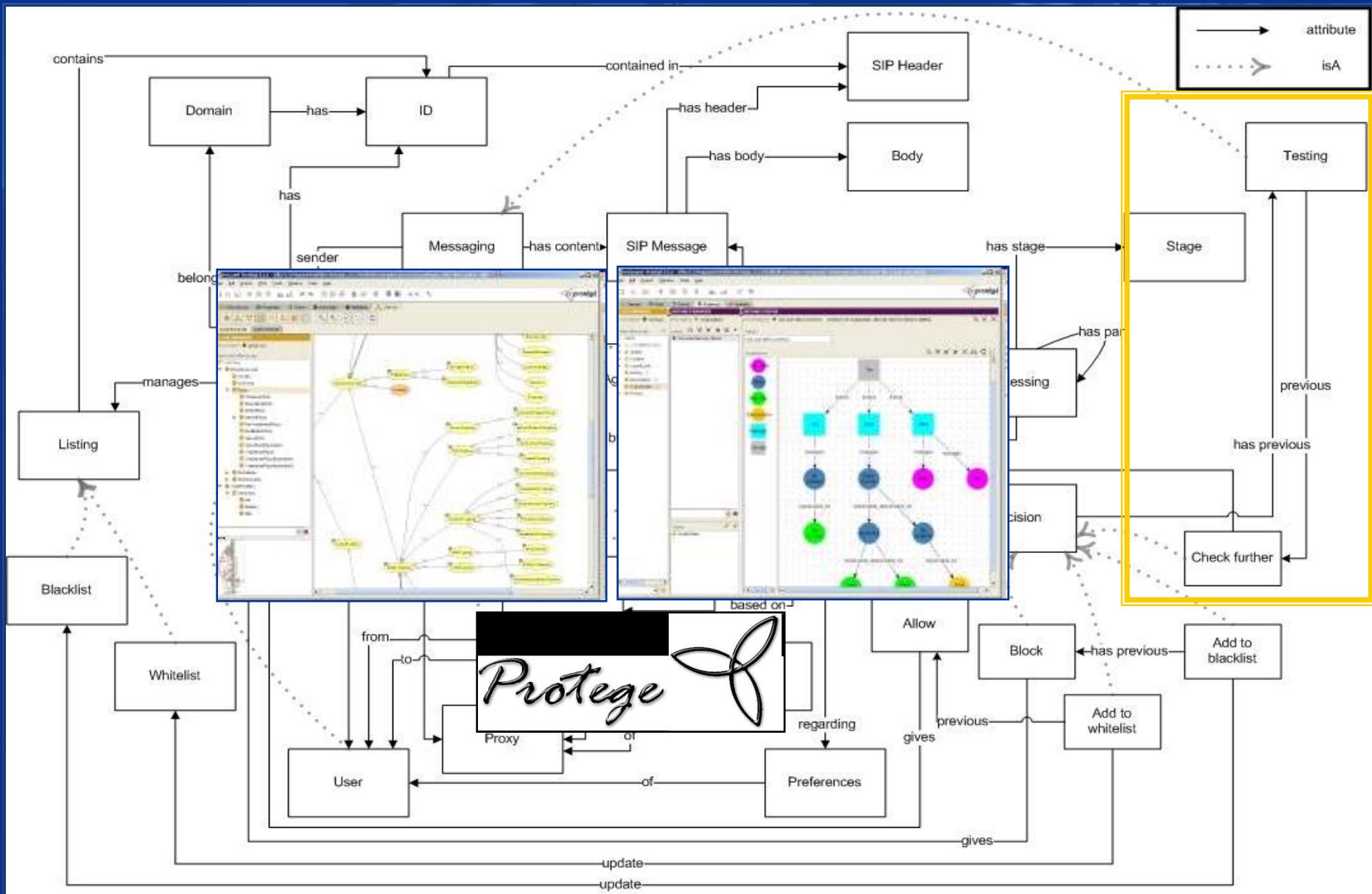
Αναπαριστά φορμαλιστικά τις **έννοιες** και τις **σχέσεις** τους στο πεδίο, διευκολύνοντας τη σε βάθος κατανόησή του.

Οδηγεί στην **υλοποίηση λύσεων** μέσω κατάλληλων μεθόδων και εργαλείων λογισμικού.

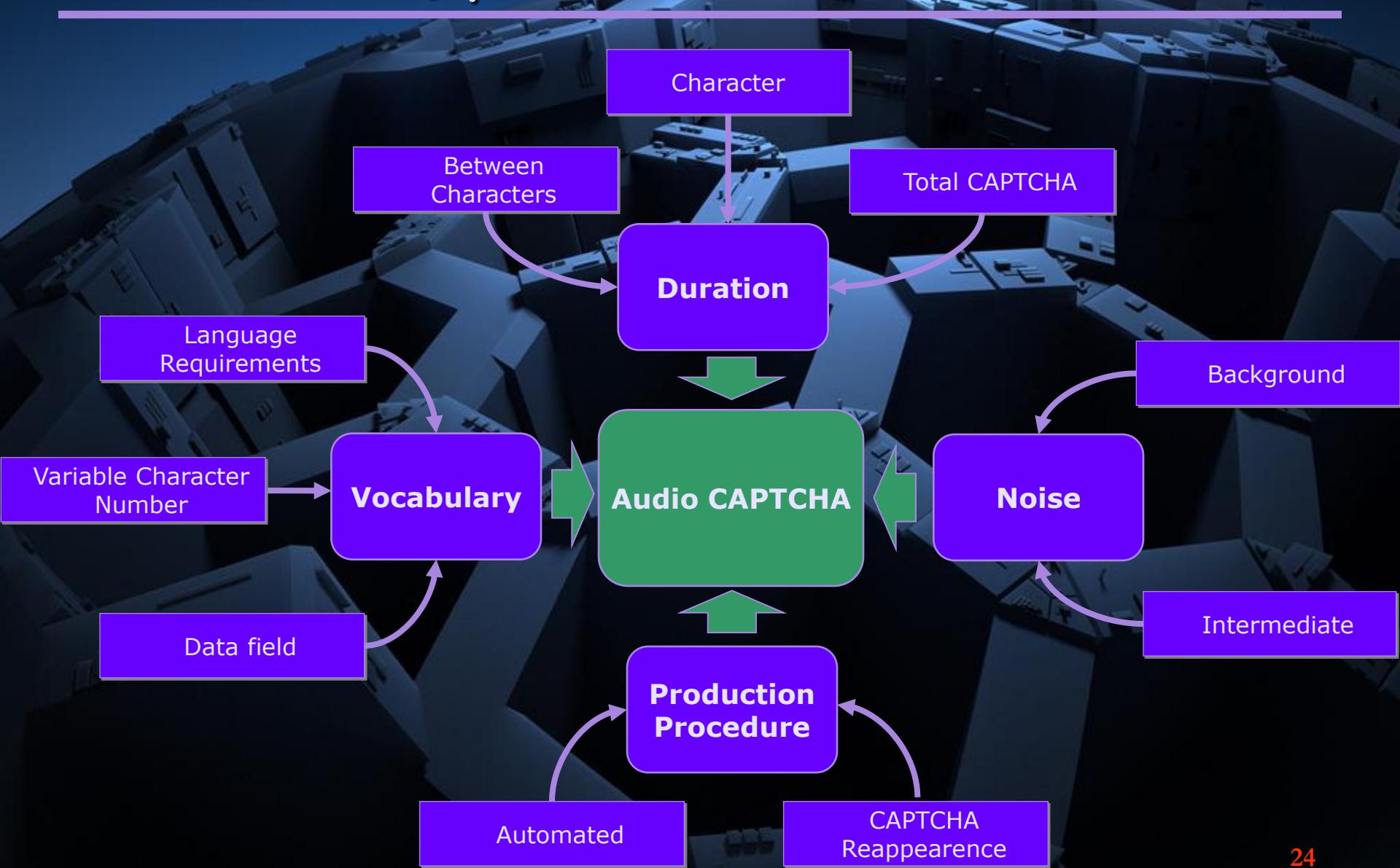
OntoSPIT: Μοντέλο και Γνώση



OntoSPIT: Διαχείριση SPIT

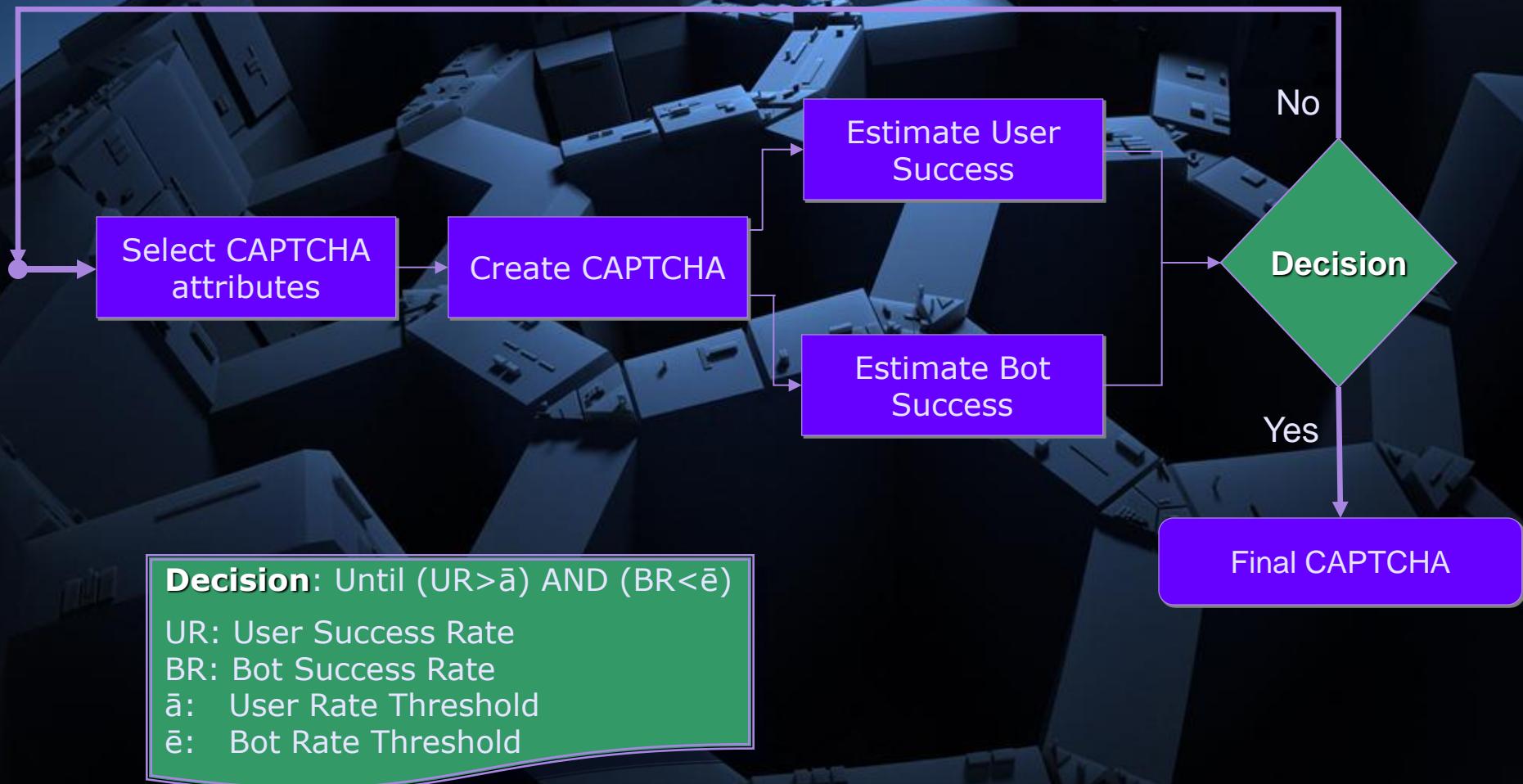


Ανάπτυξη νέου audio CAPTCHA*

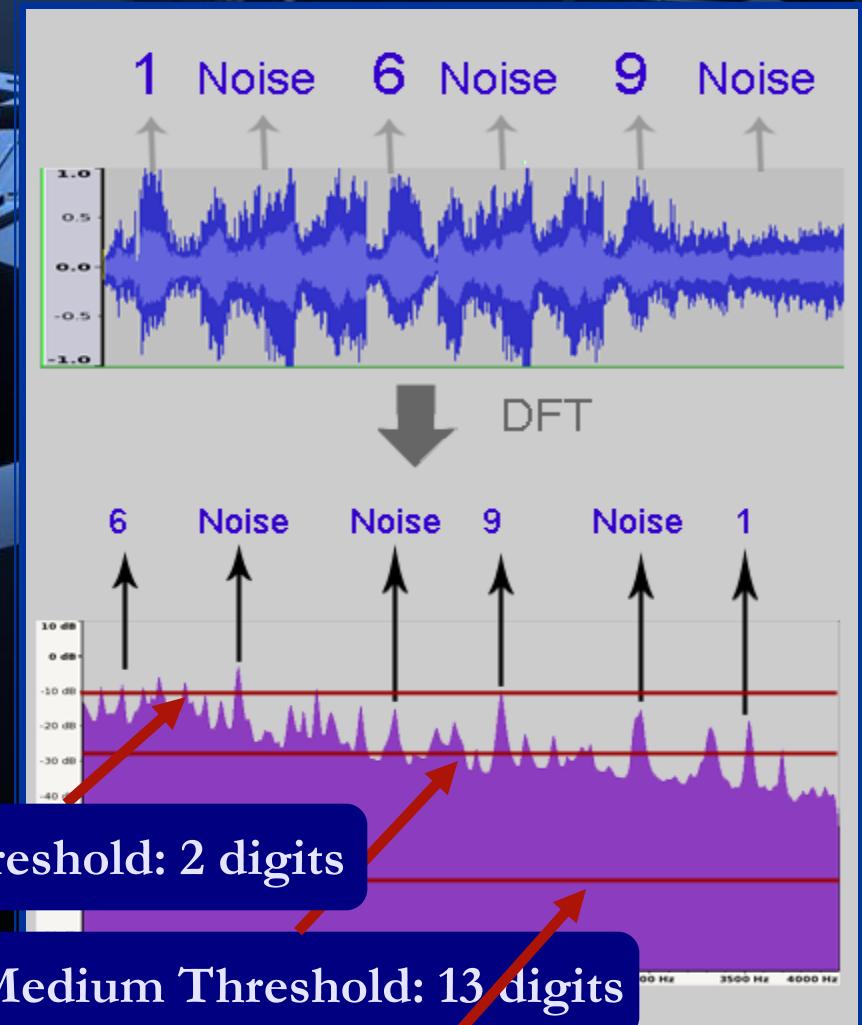
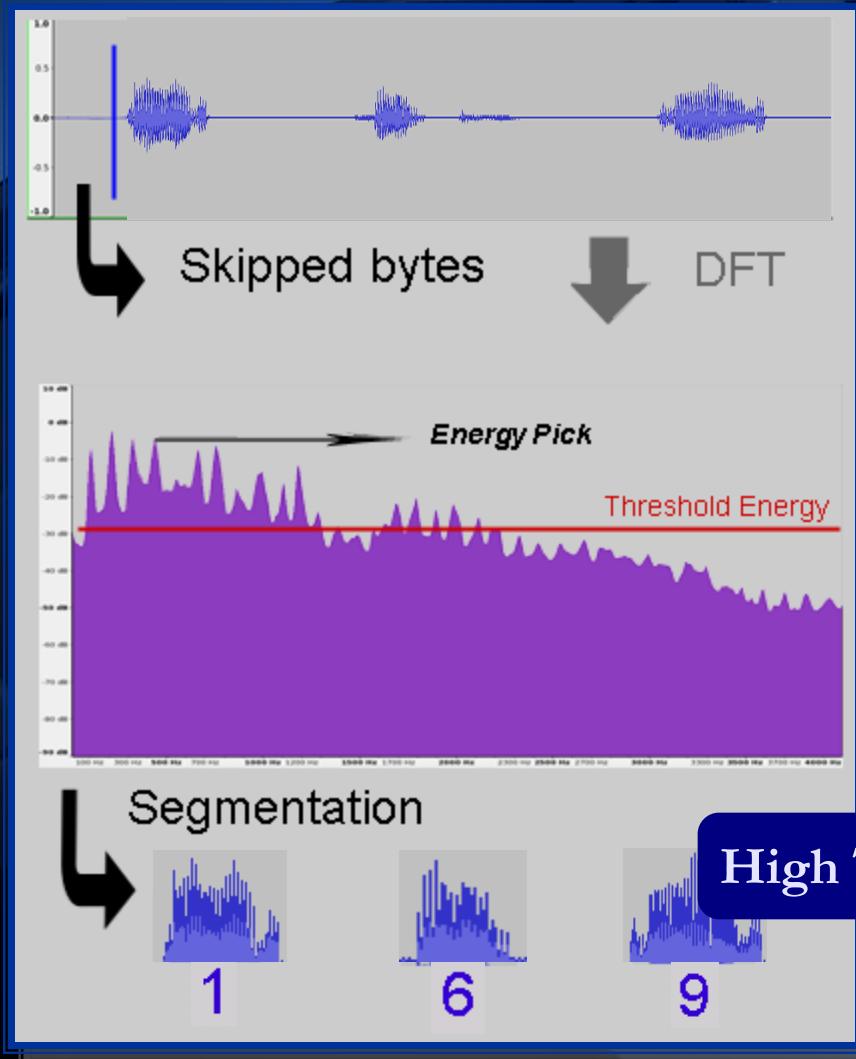


* CAPTCHA: Completely Automated Public Turing test to tell Computers and Humans Apart

Έλεγχος και αποδοχή CAPTCHA



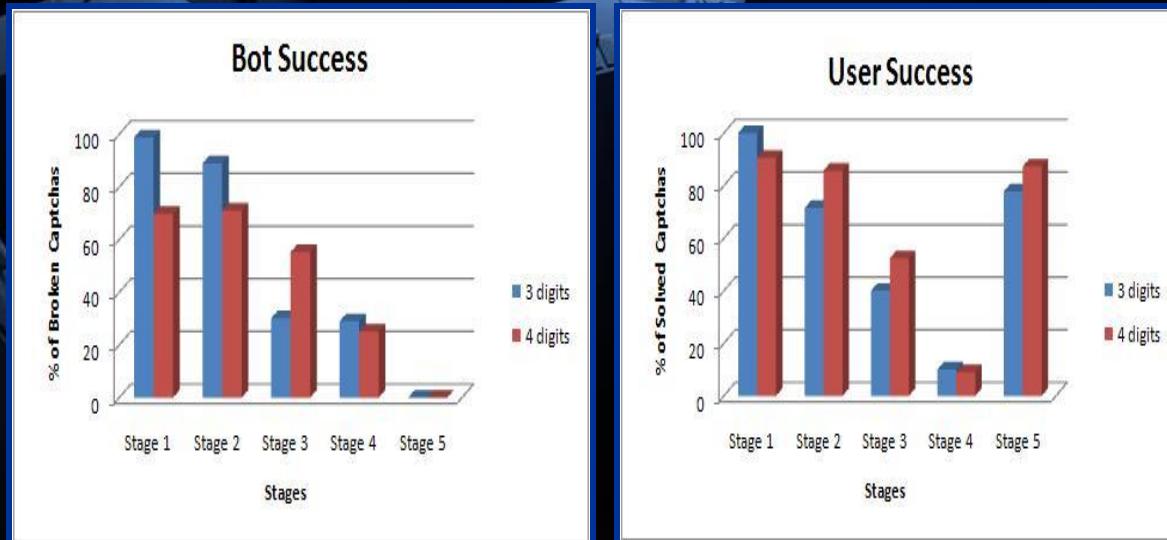
antiSPIT audio CAPTCHA



Low Threshold: 15 digits

Αρχική αξιολόγηση audio CAPTCHA

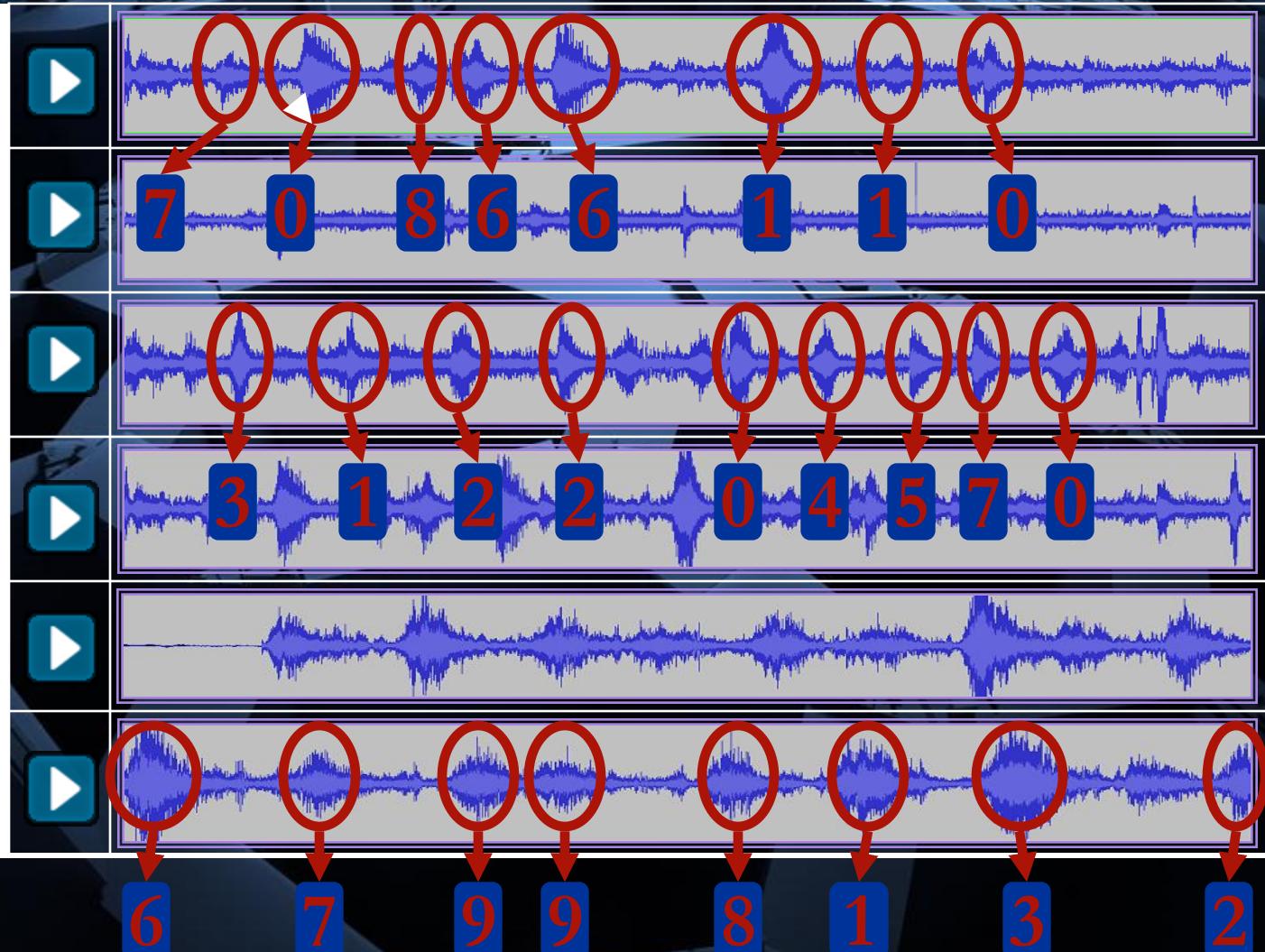
| | Πλήθος εκφωνητών | Χρονική υστέρηση | Ενδιάμεσος θόρυβος | Θόρυβος στο παρασκήνιο | Πλήθος στιγμιότυπων εκπαίδευσης |
|----------|------------------|------------------|--------------------|------------------------|---------------------------------|
| Στάδιο 1 | 1 | | | | 20 |
| Στάδιο 2 | 3 | | | | 50 |
| Στάδιο 3 | 5 | | | ☒ | 100 |
| Στάδιο 4 | 7 | ☒ | | ☒ | 100 |
| Στάδιο 5 | 7 | ☒ | ☒ | ☒ | 100 |



Soupionis Y., Tountas G., Gritzalis D., "An audio CAPTCHA for SIP-based SPIT prevention", June 2008
(in preparation).

Μείζονες υλοποιήσεις audio CAPTCHA

Recaptcha¹



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%)

Συγκριτική αξιολόγηση μηχανισμών

| SPIT Attacks | Anti-SPIT Frameworks | SPIT Prevention using Anonymous Verifying Authorities | RFC4474 | SIP SAML | Biometric Framework for SPIT Prevention | VoIP SEAL | Hidden Turing Tests | SPIT Mitigation through a Network Layer Anti-SPIT Entity | Progressive Multi Gray-Levelling | Voice SPAM Detector | DSIP | DAPES | SPIT Detection based on Reputation and Charging techniques | antiSPIT Architecture based on ontoSPIT and CAPTHCA |
|--|----------------------|--|---------|-------------------------------------|---|-------------------------------------|---------------------|--|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--|---|
| Address harvesting | | | | | | | | | | | | | | |
| Multiple Account Instantiation | | | | | | | | | | | | | | |
| Open relays and proxies | | | | | | <input checked="" type="checkbox"/> | | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | |
| Anonymity Services | | | | | | <input checked="" type="checkbox"/> | | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | |
| Obfuscating message content | | | | | | <input checked="" type="checkbox"/> | | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | |
| Support services | | | | | | <input checked="" type="checkbox"/> | | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | |
| Sending messages to multicast addresses | | | | | | | | | | | | | | |
| Exploitation of forking proxies | | | | | | | | | | | | | | |
| Exploitation of registrars servers | | <input checked="" type="checkbox"/> | | <input checked="" type="checkbox"/> | | <input checked="" type="checkbox"/> | | | | | | | | |
| Exploitation of re-INVITES request messages | | | | | | | | | | | | | | |
| Exploitation of the record-route header field | | | | | | | | | | | | | | |
| Exploitation of messages and header fields structure | | | | | | | | | | | | | | <input checked="" type="checkbox"/> |

Μερικά πρώτα συμπεράσματα...

Η επαρκής αντιμετώπιση του SPIT εξακολουθεί να απαιτεί **πολυπαραγοντική προσέγγιση**.

Η αρχιτεκτονική antiSPIT μπορεί να αντιμετωπίσει **πολύ περισσότερα είδη επιθέσεων** απ' ότι οι υπάρχουσες.

Η ontoSPIT παρέχει **λεξιλόγιο, οργανώνει** το πεδίο του SPIT και καθοδηγεί την **υλοποίηση λύσεων**.

Η γραφοανάλυση επιτρέπει τη **μοντελοποίηση** των **πιθανών επιθέσεων** και καθοδηγεί την **ανίχνευση** του SPIT.

Το audio CAPTCHA που αξιοποιεί **χροιά** εκφώνησης, τυχαίους **ενδιάμεσους** ήχους και **διασπορά** τους στο μήνυμα παρέχει ενθαρρυντική **ανθεκτικότητα** σε bot.

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., Souponis 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., Souponis 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.
5. Souponis 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, 2011.
6. Souponis Y., Tountas G., Gritzalis D., "Audio CAPTCHA for SIP-based VoIP", *Proc. of the 24th International Information Security Conference*, pp. 25-38, Springer, 2009.
7. Souponis 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, 2008.
8. Souponis 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. Souponis Y., Basagiannis S., Katsaros P., Gritzalis D., "A formally verified mechanism for countering SPIT", in *Proc. of the 5th International Conference on Critical Infrastructure Security*, pp. 128-139, LNCS-6712, Springer, 2010.
10. Souponis Y., Koutsiamanis A.-R., Efraimidis P., Gritzalis D., "A game-theoretic analysis of preventing spam over Internet Telephony with audio CAPTCHA-based authentication", *Journal of Computer Security*, Vol. 22, pp. 383-413, 2014.
11. Stachtiari E., Souponis 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 Infrastructure Security*, Springer, 2012.
12. Theoharidou M., Kotzanikolaou P., Gritzalis D., "Risk-based Criticality Analysis", in *Proc. of the 3rd IFIP International Conference on Critical Infrastructure Protection*, Springer, USA, March 2009.