Ασφάλεια Υπολογιστικών Συστημάτων

7ο Εξάμηνο

Μοντέλα επιθέσεων και επιτιθέμενων - Αυθεντικοποίηση οντότητας

Διδάσκων : Δρ. Παρασκευάς Κίτσος, Αναπληρωτής Καθηγητής

https://ecsalab.ece.uop.gr/

Εργαστήριο Ηλεκτρονικών Κυκλωμάτων, Συστημάτων και Εφαρμογών (ECSA Lab.)

e-mail: kitsos@uop.gr

ΚΕΦΑΛΑΙΟ 5: Μοντέλα επιθέσεων και επιτιθέμενων

Ασφάλεια Πληροφοριών & Συστημάτων στον Κυβερνοχώρο

Μοντέλα επιθέσεων και επιτιθέμενων (1/2)

Απειλή:
- Εσωτερικό περιβάλλον: (π.χ. δυσαρεστημένος υπάλληλος, αστοχία υλισμικού)
- Εξωτερικό περιβάλλον: (π.χ. κυβερνοεγκληματίας, πλημμύρα)

Επίθεση:
- Σκόπιμη: (π.χ. εκμετάλλευση αδυναμιών υλικολογισμικού)
- Μη σκόπιμη / Τυχαία: (π.χ. λανθασμένη ενέργεια)

Μοντέλα επιθέσεων και επιτιθέμενων (2/2)

Επιτιθέμενος:

- Κίνητρο
- Διαθέσιμοι πόροι
- Τεχνικές δεξιότητες
- Τεχνικές δεξιότητες / Γνώσεις
- Πρόσβαση

Γνωστές μεθοδολογίες αξιολόγησης επιθέσεων / επιτιθέμενων

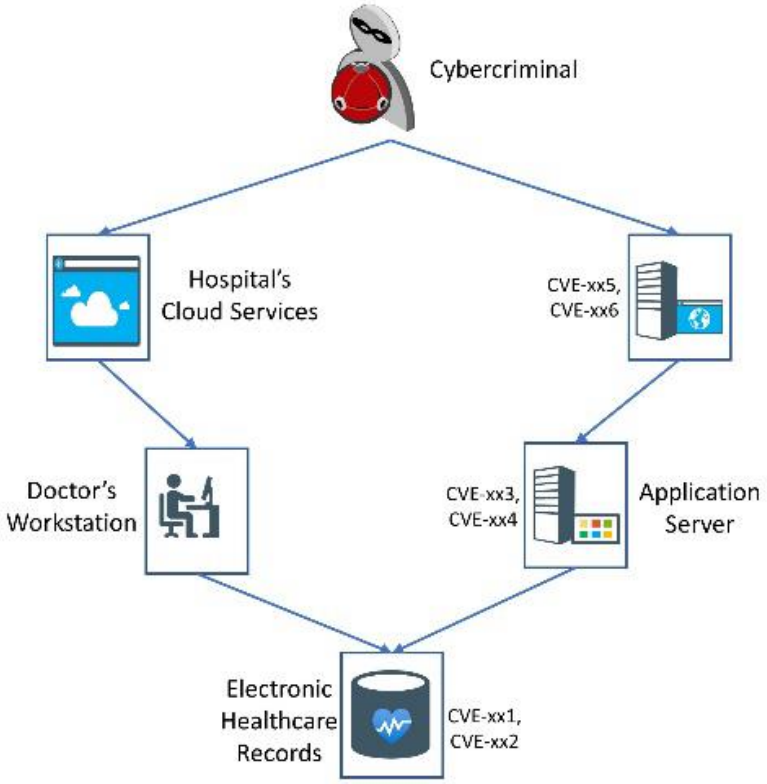
STRIDE | NIST 800-30 | Intel TAL | OCTAVE | MITRE
- PRE-ATT&CK
- TARA
- CAPEC

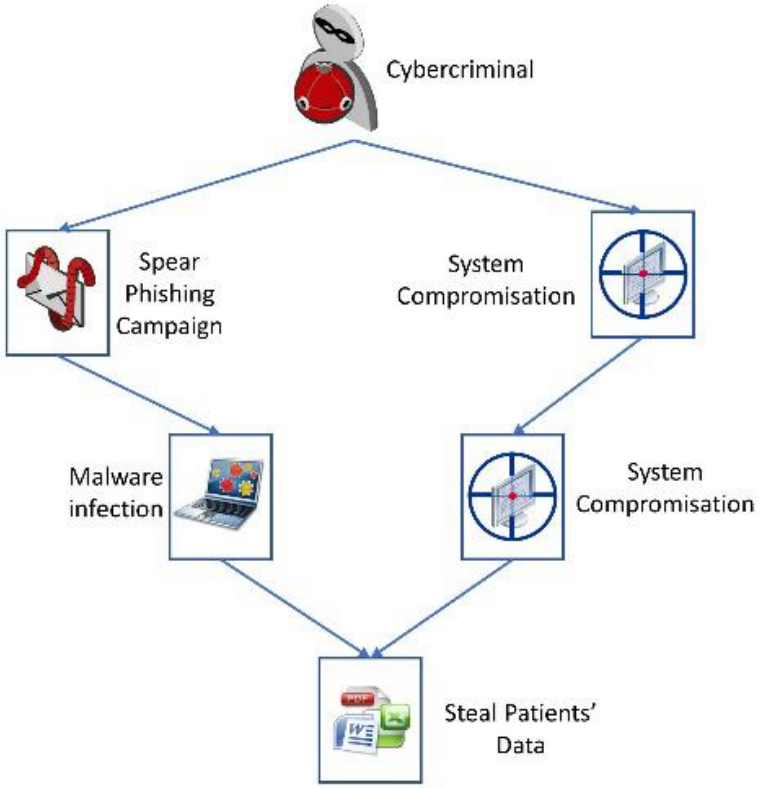
ENISA

Μοντέλα επιθέσεων και επιτιθέμενων– δένδρα επιθέσεων (1/2)

- Χρησιμοποιούνται για τη μοντελοποίηση και απεικόνιση με δομημένο τρόπο της χρονικής ακολουθίας των ενεργειών/γεγονότων μιας σύνθετης κυβερνοεπίθεσης προς ένα πληροφοριακό σύστημα
- Κάθε γεγονός τοποθετείται ως ‘φύλλο’ (leaf node) ενός δένδρου ενώ στη ‘ρίζα’ (root node) τοποθετείται ο τελικός στόχος του επιτιθέμενου
- Ανάλογα με τους λογικούς τελεστές σύγκρισης, κάθε κόμβος δύναται να είναι τύπου ***AND*** ή ***OR***
- Κάθε κόμβος δύναται να απεικονίζει ένα σύστημα, μία ευπάθεια ή/και τύπο επίθεσης επιτιθέμενου
- Χρησιμοποιούνται και σε κάποιες από τις προαναφερθείσες μεθοδολογίες

Μοντέλα επιθέσεων και επιτιθέμενων– δένδρα επιθέσεων (2/2)





Μοντέλα επιθέσεων και επιτιθέμενων – Μεθοδολογία stride (1/3)

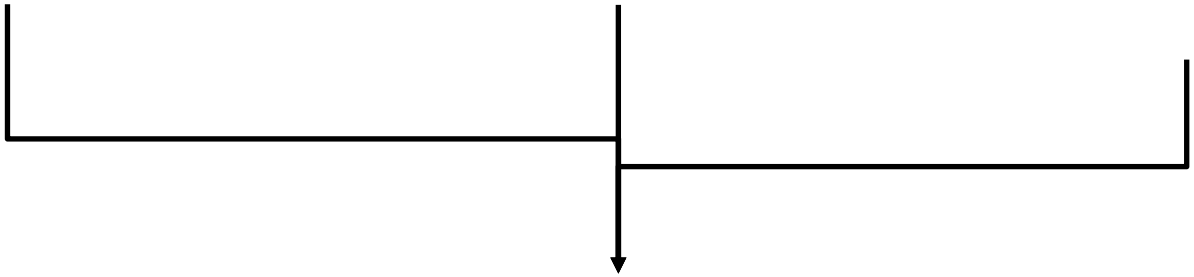
	Απειλή	Επηρρεαζόμενη ιδιότητα
S	Πλαστογράφηση (Spoofing)	Αυθεντικότητα (Authenticity)
T	Αλλοίωση (Tampering)	Ακεραιότητα (Integrity)
R	Επιβεβαίωση (Repudiation)	Μη αποποίηση ευθύνης (Non-repudiability)
I	Αποκάλυψη πληροφορίας (Information disclosure)	Εμπιστευτικότητα (Confidentiality)
D	Άρνηση υπηρεσίας (Denial of Service)	Διαθεσιμότητα (Availability)
E	Κλιμάκωση προνομίων (Elevation of Privilege)	Εξουσιοδότηση (Authorization)

Μοντέλα επιθέσεων και επιτιθέμενων – Μεθοδολογία stride (2/3)

Δημιουργία **διαγραμμάτων ροής δεδομένων (DFDs)** με σκοπό να προσδιοριστούν οι οντότητες, οι λειτουργίες και τα όρια του πληροφοριακού συστήματος

Χρήση των προκαθορισμένων τύπων απειλών/επιθέσεων STRIDE ανά πληροφοριακό σύστημα

Ανάλυση χαρακτηριστικών (π.χ. διαθέσιμοι πόροι, δεξιότητες) επιτιθέμενων, υφιστάμενων κανόνων ασφάλειας, επιπτώσεων



Αξιολόγηση απειλής

Μοντέλα επιθέσεων και επιτιθέμενων – Μεθοδολογία stride (3/3)

Κύριες παραλλαγές/προεκτάσεις μεθόδου STRIDE

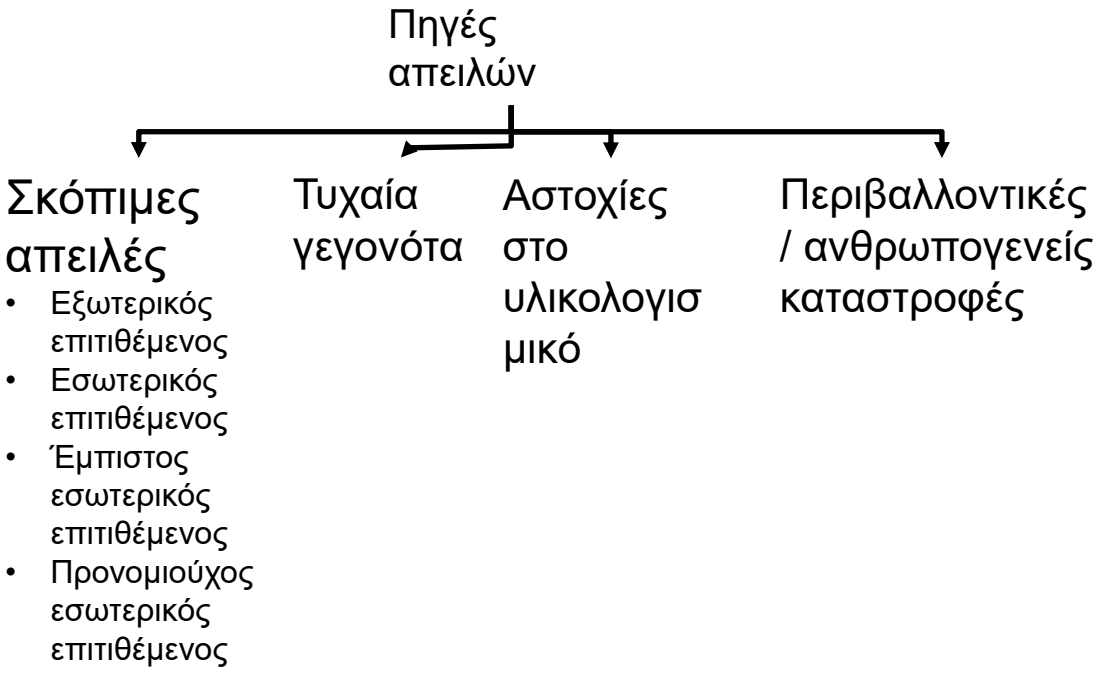
Microsoft's **DREAD**: **D**amage potential, **R**eproducibility, **E**xploitability, **A**ffected users, **D**iscoverability

- Προκαθορισμένες τιμές ανά κατηγορία απειλής
- Τύπου "*mnemonic*" - οι κατηγορίες απειλών κωδικοποιούνται αναλόγως του ονόματος της μεθοδολογίας

IDDIL/ATC: Identify the assets, **D**efine the attack surface, **D**ecompose the system, **I**dentify attack vectors, **L**ist threat actors/ **A**nalysis & assessment, **T**riage, **C**ontrols

- Δυνατότητα καταγραφής ενεργειών τύπου *"lateral movements"* μέσω δένδρων επιθέσεων

Μοντέλα επιθέσεων και επιτιθέμενων – NIST 800-30



Τακτικές, Τεχνικές και Διεργασίες (TTPs):

- Χρόνος επίθεσης
- Στόχος επίθεσης
- Διαθέσιμοι πόροι
- Σχεδιασμός επίθεσης

Μοντέλα επιθέσεων και επιτιθέμενων – Intel TAL (1/3)

Κατηγορίες επιτιθέμενων

- *Κακόβουλοι*
- *Μη κακόβουλοι*

Χρήση

- *22 προφίλ επιτιθέμενων* (π.χ. βιομηχανικοί κατάσκοποι, υπάλληλοι)
- *7 χαρακτηριστικά*

Χαρακτηριστικά επιτιθέμενων:

1. **Πρόσβαση:** Εσωτερική – Εξωτερική
2. **Αποτέλεσμα:** Κλοπή, Ζημιά, Δυσφήμηση
3. **Όρια:** Κώδικας δεοντολογίας, Νομοθετικό πλαίσιο
4. **Επίπεδο διαθέσιμων πόρων:** Χαμηλό, Επιχειρησιακό, Υψηλό
5. **Επίπεδο δεξιοτήτων:** Πολύ χαμηλό, χαμηλό, επιχειρησιακό, υψηλό
6. **Σκοπός:** π.χ. Ολική καταστροφή στόχου
7. **Βαθμός αποκάλυψης επιτιθέμενου:** Πλήρης, Μερικός, Μυστικός, Χωρίς πλάνο

Μοντέλα επιθέσεων και επιτιθέμενων – Intel TAL (2/3)

- Το 2015 η Intel τροποποίησε την εν λόγω λίστα ώστε να συμπεριλάβει και το κίνητρο (motive): ιδεολογία (ideology), εξαναγκασμός (coercion), κακοφημία (notoriety), προσωπική ικανοποίηση (personal satisfaction), οργανωτικό κέρδος (organizational gain), προσωπικό οικονομικό κέρδος (personal financial gain), δυσαρέσκεια (disgruntlement), τυχαίο (accidental), κυριαρχία (dominance) και απρόβλεπτο (unpredictable)

- Προστέθηκαν και οι παρακάτω κατηγορίες κινήτρου: κυρίως (defining motivation), συμπληρωματικό (co-motivation), δευτερεύον (subordinate motivation) δεσμευτικό (binding motivation) και προσωπικό (personal motivation)

- 21 διαθέσιμες κατηγορίες επιτιθέμενων: Αναρχικός, Ακτιβιστής, Διεφθαρμένος κυβερνητικός υπάλληλος, Δυσαρεστημένος υπάλληλος, Κυβερνο-κατάσκοπος, Εγκληματίας κλπ.

Μοντέλα επιθέσεων και επιτιθέμενων – Intel TAL(3/3)

Κατηγορία Επιτιθέμενου	Συνήθεις ενέργειες/τακτικές	Περιγραφή
Αναρχικός (Anarchist)	Βία, καταστροφή περιουσιακών στοιχείων, διακοπή επιχειρηματικών υπηρεσιών (φυσικά)	Άτομο που απαρνείται όλες τις δομές εξουσίας και δρα χωρίς αναστολές
Διεφθαρμένος κυβερνητικός υπάλληλος	Διαταραχή/διακοπή επιχειρηματικών υπηρεσιών τόσο σε φυσικό αλλά και οργανωτικό επίπεδο.	Άτομο που χρησιμοποιεί τις αρμοδιότητες της θέσης του για να αποκτήσει μέρος των πόρων ενός τρίτου φορέα/επιχείρησης.
Κυβερνο-βανδαλιστής (Cyber-Vandal)	Διαταραχή/διακοπή του δικτύου/υπολογιστών, επιθέσεις με χρήση κακόβουλου λογισμικού (malware) ή/και πειρατείας υπηρεσιών του διαδικτύου (web hijacking)	Χωρίς συγκεκριμένη ατζέντα, λαμβάνει ευχαρίστηση μέσω των παράνομων ενεργειών που διενεργεί (π.χ. εισβολή/καταστροφή) σε περιουσιακά στοιχεία τρίτων.
Δυσαρεστημένος υπάλληλος	Κατάχρηση των προσβάσεων/δικαιωμάτων με σκοπό το σαμποτάζ	Εν ενεργεία ή απολυμένος υπάλληλος με σκοπό να προκαλέσει ζημιά στην εταιρεία
Κυβερνο-πολεμιστής (Government Cyberwarrior)	Διαταραχή/διακοπή επιχειρηματικών υπηρεσιών σε φυσικό, οργανωτικό & επίπεδο υποδομών μέσω επιθέσεων με χρήση κακόβουλου λογισμικού (malware) ή/και πειρατείας υπηρεσιών του διαδικτύου (web hijacking)	Επιτιθέμενος χρηματοδοτούμενος από κράτος ικανός να επιφέρει σημαντική διαταραχή/διακοπή κρίσιμων υπηρεσιών και υποδομών σε εθνικό επίπεδο

Μοντέλα επιθέσεων και επιτιθέμενων – OCTAVE (1/2)

OCTAVE: **O**perationally **C**ritical **T**hreat, **A**sset, and **V**ulnerability **E**valuation

Κατηγορίες επιτιθέμενων:

- Με χρήση φυσικών μέσων
- Με χρήση τεχνικών μέσων
- Τεχνικά προβλήματα
- Άλλο (π.χ. φυσικές καταστροφές)

Χαρακτηριστικά απειλής:

- Επιτιθέμενος
- Επηρεαζόμενα συστήματα
- Πρόσβαση
- Κίνητρο
- Αποτέλεσμα

Αποτέλεσμα επίθεσης:

- Αποκάλυψη / τροποποίηση / καταστροφή / απώλεια πληροφορίας
- Διατάραξη καλής λειτουργίας

Μοντέλα επιθέσεων και επιτιθέμενων– OCTAVE (2/2)

Επιτιθέμενος με τεχνικά/φυσικά μέσα	Εσωτερικός (κατά λάθος)	Αποκάλυψη / Τροποποίηση / Καταστροφή / Απώλεια πληροφορίας / Διατάραξη καλής λειτουργίας
	Εσωτερικός (σκόπιμα)	
	Εσωτερικός (κατά λάθος)	
	Εξωτερικός (σκόπιμα)	
Τεχνικό πρόβλημα/δυσλειτουργία	Ελαττώματα στο λογισμικό	
	Συστημικά σφάλματα	
	Ελαττώματα στο υλισμικό	
	Κακόβουλος κώδικας	
Άλλα προβλήματα	Παροχή ρεύματος	
	Τηλεπικοινωνίες	
	Τρίτων μερών	
	Φυσικές καταστροφές	

Κατηγορίες επιτιθέμενων/απειλών σύμφωνα με την μεθοδολογία OCTAVE

Μοντέλα επιθέσεων και επιτιθέμενων – MITRE (1/3)

PRE-ATT&CK: Adversarial **T**actics, **T**echniques, and **C**ommon **K**nowledge

- Περιλαμβάνει **96 τεχνικές** αντιστοιχισμένες σε **9 τακτικές** επιτιθέμενων (συνεχώς επικαιροποιούνται…)
- Έχει επικεντρωθεί κυρίως σε εταιρικά περιβάλλοντα με υποδομή βασισμένη στο λειτουργικό σύστημα Microsoft Windows
- Χρησιμοποιείται για την αξιολόγηση της συμπεριφοράς των επιτιθέμενων που προέρχονται από το εξωτερικό περιβάλλον του οργανισμού
- Οι **Τακτικές** περιγράφουν τους επιμέρους στόχους κατά την εκδήλωση ενός σεναρίου επίθεσης (π.χ. απόκτηση αρχικής/μόνιμης πρόσβασης, εξαγωγή δεδομένων, εκτέλεση προγραμμάτων, κλοπή διαπιστευτηρίων, απομακρυσμένο έλεγχο, κλιμάκωση προνομίων). Κάθε τακτική χρησιμοποιείται ως «οδηγός» για το ποιες τεχνικές δύναται να χρησιμοποιηθούν
- Οι **Τεχνικές** περιγράφουν τον τρόπο με τον οποίο ο επιτιθέμενος πετυχαίνει τον στόχο του ή/και πιο είναι το «κέρδος» εκτελώντας μια συγκεκριμένη ενέργεια (π.χ. κλιμάκωση προνομίων→ χειραγώγηση διακριτικού πρόσβασης, τροποποίηση πολιτικής τομέα κλπ.)

Μοντέλα επιθέσεων και επιτιθέμενων – MITRE (2/3)

CAPEC: Common **A**ttack **P**attern **E**numeration and **C**lassification

- Χρησιμοποιείται από προγραμματιστές και σχεδιαστές/αναλυτές πληροφοριακών συστημάτων για το εντοπισμό των εφαρμόσιμων σεναρίων απειλών στα οποία είναι ευάλωτο το εκάστοτε πληροφοριακό σύστημα, αλλά και τους τρόπους αντιμετώπισής τους
- Τα μοτίβα των απειλών έχουν κοινά γνωρίσματα και αντιστοιχούν σε μία ή παραπάνω κατηγορίες αδυναμιών λογισμικού (Common Weakness Enumeration - CWE)
- Οι επιθέσεις ταξινομούνται σε δύο κύριους καταλόγους: μηχανισμούς (mechanisms) και τομείς (domains) μοτίβων επίθεσης. Κάθε κατάλογος έχει δενδρική δομή με κύριες κατηγορίες και υποκατηγορίες. Κάθε στοιχείο του καταλόγου, πλην των κύριων κατηγοριών, δύναται να ανήκει σε παραπάνω από μία από τις κύριες κατηγορίες

Μοντέλα επιθέσεων και επιτιθέμενων – MITRE (3/3)

TARA: **T**hreat **A**ssessment and **R**emediation **A**nalysis

- Λειτουργεί σε συνδυασμό με τη μεθοδολογία Crown Jewels Analysis (CJA) η οποία χρησιμοποιείται για τον εντοπισμό των κρίσιμων πληροφοριακών συστημάτων ενός οργανισμού.
- Αναγνωρίζει και βαθμολογεί πιθανά σενάρια επίθεσης χρησιμοποιώντας πηγές πληροφοριών όπως το CAPEC, τις κατηγορίες αδυναμιών λογισμικού (CWE), Common Vulnerabilities and Exposures (CVE) και άλλες σχετικές πηγές (π.χ. NIST)
- Για κάθε Πληροφοριακό σύστημα λαμβάνονται υπόψη: Σκοπός, αρχιτεκτονική, τεχνολογίες, χαρακτηριστικά επιτιθέμενων, υφιστάμενα μέτρα ασφάλειας, διεπαφές και ροές δεδομένων
- Τα διανύσματα επίθεσης κάθε πληροφοριακού συστήματος αξιολογούνται και βαθμολογούνται λαμβάνοντας υπόψη παράγοντες όπως η εγγύτητα, οι τεχνικές δεξιότητες και οι πόροι που απαιτούνται για την επιτυχή ολοκλήρωση του σεναρίου επίθεσης

Μοντέλα επιθέσεων και επιτιθέμενων – ENISA (1/3)

ENISA: European Union Agency for Network and Information Security

- Δημοσιεύει ανά τακτά χρονικά διαστήματα κατάλογο απειλών για συστήματα πληροφορικής και τηλεπικοινωνιών.
- Διαχωρίζονται στις **Σκόπιμες**, **Μη-σκόπιμες** και **Περιβαλλοντικές**.

Σκόπιμες:

- Εξαπάτηση, σαμποτάζ, κλοπή, εκβιασμός, τρομοκρατικές επιθέσεις κλπ.
- Λαθροακρόαση (eavesdropping), υποκλοπή (interception), υφαρπαγή (hijacking), επιθέσεις με κινούμενο όχημα (war driving), επιθέσεις επαναποστολής μηνυμάτων (replay attacks) κλπ.
- Κλοπή ταυτότητας (identity theft), αποστολή μηνυμάτων ανεπιθύμητης αλληλογραφίας (spamming), επιθέσεις άρνησης υπηρεσίας (denial of service attacks), κοινωνικής μηχανικής social engineering κλπ.
- Παραβίαση νομοθετικού/κανονιστικού πλαισίου, μη τήρηση όρων συμβολαίου, κατάχρηση δεδομένων προσωπικού χαρακτήρα, κακόβουλες ενέργειες κατά δικαστικών αρχών

Μοντέλα επιθέσεων και επιτιθέμενων– ENISA (2/3)

Μη-σκόπιμες:

- Διαρροή πληροφοριών λόγω ανθρώπινου σφάλματος ή/και μεταφοράς μέσω μη αξιόπιστων δικτύων χωρίς τις απαραίτητες προφυλάξεις
- Κακές πρακτικές διαχείρισης συστημάτων (π.χ. λανθασμένη αρχικοποίηση λειτουργικού συστήματος)
- Χρήση δεδομένων εισόδου από αναξιόπιστες πηγές.
- Μη ηθελημένη αλλοίωση δεδομένων.
- Παραλείψεις κατά την διαδικασία σχεδιασμού, ανάλυσης και υλοποίησης ενός πληροφοριακού συστήματος (π.χ. παρωχημένες διαδικασίες ανάλυσης, έλλειψη ρόλων και αρμοδιοτήτων, χρονικοί περιορισμοί).
- Ζημιές από προμηθευτές/συνεργάτες.
- Απώλεια της εμπιστευτικότητας και ακεραιότητας πληροφοριακών συστημάτων (π.χ. ψηφιακών πιστοποιητικών, πληροφοριών αποθηκευμένων σε συστήματα νεφοϋπολογιστικής)

Μοντέλα επιθέσεων και επιτιθέμενων – ENISA (3/3)

Περιβαλλοντικές:

- Διακοπές λειτουργίας κεντρικών συστημάτων (outages): Ελλείψεις/βλάβες σε υλικοτεχνικό εξοπλισμό/πόρους (π.χ. ηλεκτρικό ρεύμα, σύστημα κλιματισμού), απουσίες προσωπικού, απεργίες, διακοπές στην δικτυακή υποδομή (εσωτερικό δίκτυο, διαδίκτυο, δίκτυα κινητής τηλεφωνίας).
- Αστοχίες/δυσλειτουργίες: Βλάβες σε πληροφοριακό υλικό (π.χ. συστήματα αποθήκευσης δεδομένων), συστήματα αισθητήρων, συνδέσμων δικτύου, συστημικού λογισμικού (π.χ. προγραμμάτων υπηρεσιών νεφοϋπολογιστικής), προγραμμάτων, δικτυακός εξοπλισμός.
- Φυσικές/περιβαλλοντικές καταστροφές: Σεισμοί, πλημμύρες, πυρκαγιές, εκρήξεις, ραδιενέργεια, απειλές προερχόμενες από το διάστημα (π.χ. ηλεκτρομαγνητική καταιγίδα).

Μοντέλα επιθέσεων και επιτιθέμενων – Συγκριτική παρουσίαση (1/4)

Για την σύγκριση ορίζουμε τα παρακάτω γνωρίσματα:

- **Σκοπός – Εφαρμοσιμότητα:** Εύρος πεδίου εφαρμογής (σε επίπεδο οργανισμού, επιχειρησιακής διεργασίας ή ακόμα και μεμονωμένου πληροφοριακού συστήματος)
- **Περιβάλλον λειτουργίας (επιχειρησιακό – τεχνικό):** Ορισμένα από τα μοντέλα απειλών & επιτιθέμενων έχουν σχεδιαστεί για συγκεκριμένο περιβάλλον (π.χ. τεχνικό - ανάπτυξης λογισμικού, συγκεκριμένου λειτουργικού συστήματος) σε αντίθεση με άλλα που δύναται να εφαρμοστούν σε οποιοδήποτε επιχειρησιακό / τεχνικό περιβάλλον (ουδέτερα).
- **Βαθμός λεπτομέρειας:** Ορισμένα από τα μοντέλα ορίζουν γενικές κατηγορίες απειλών (χαμηλής λεπτομέρειας), σε άλλα ευνοείται η επεκτασιμότητα των χαρακτηριστικών του μοντέλου (μεσαίας λεπτομέρειας), σε κάποια δίνεται έμφαση στην πληρότητα του καταλόγου απειλών/προφίλ επιτιθέμενων (υψηλής λεπτομέρειας) ενώ σε μερικά το επίπεδο της πληρότητας εξαρτάται από τον τρόπο χρήσης της μεθοδολογίας.

Μοντέλα επιθέσεων και επιτιθέμενων – Συγκριτική παρουσίαση (2/4)

Για την σύγκριση ορίζουμε τα παρακάτω γνωρίσματα:

- **Επίπεδο πολυπλοκότητας:** Κάποια μοντέλα περιγράφουν βασικούς όρους και (χαμηλής πολυπλοκότητας), άλλα ορίζουν περισσότερες (μεσαίας πολυπλοκότητας), ενώ σε ορισμένες μεθοδολογίες (συνήθως σε αυτές με υψηλό βαθμό λεπτομέρειας) καθορίζονται συσχετίσεις, οι αντίστοιχοι αλγόριθμοι υπολογισμού της επικινδυνότητας ή/και εργαλεία μοντελοποίησης και προσομοίωσης (υψηλής πολυπλοκότητας)
- **Συμβατότητα:** Ορισμένα μοντέλα/μεθοδολογίες είναι πλήρως συμβατά με γνωστά πρότυπα εκτίμησης της επικινδυνότητας σε αντίθεση με άλλα που έχουν σχεδιαστεί για να λειτουργούν αυτόνομα (stand-alone).

Μοντέλα επιθέσεων και επιτιθέμενων – Συγκριτική παρουσίαση (3/4)

Μοντέλο / Μεθοδολογία	Σκοπός - Εφαρμοσιμότητα	Περιβάλλον Λειτουργίας		Βαθμός Λεπτομέρειας	Επίπεδο Πολυπλοκότητας	Συμβατότητα
		Επιχειρησιακό	Τεχνικό			
STRIDE	Συστήματος	Ουδέτερο (Αρχικά δημιουργήθηκε για ανάπτυξη λογισμικού αλλά πλέον χρησιμοποιείται και σε άλλους τομείς)	Ουδέτερο	Μεσαίο (Με δυνατότητες επέκτασης)	Μεσαίο	Υψηλή (συμβατό με NIST SP 800-30rev1)
DREAD	Συστήματος	Ουδέτερο (Αρχικά δημιουργήθηκε για ανάπτυξη λογισμικού αλλά πλέον χρησιμοποιείται και σε άλλους τομείς)	Λογισμικό	Χαμηλό	Χαμηλό	Χαμηλή
IDDIL/ATC	Συστήματος	Ουδέτερο	Ουδέτερο	Μεσαίο	Μεσαίο	Υψηλή (NIST SP 800-30, STRIDE)
NIST SP 800-30Rev1	Οργανισμού, επιχειρησιακής διεργασίας/στόχου, συστήματος	Ουδέτερο (Αν και δημιουργήθηκε για ομοσπονδιακούς οργανισμούς)	Ουδέτερο	Μεσαίο (Επεκτάσιμη καθώς υποστηρίζει την χρήση δένδρων επιθέσεων ως επιπρόσθετο επίπεδο λεπτομέρειας)	Μεσαίο	Υψηλή (Είναι διεθνώς αναγνωρισμένο πρότυπο εκτίμησης της επικινδυνότητας)

Μοντέλα επιθέσεων και επιτιθέμενων – Συγκριτική παρουσίαση (4/4)

Μοντέλο / Μεθοδολογία	Σκοπός - Εφαρμοσιμότητα	Περιβάλλον Λειτουργίας		Βαθμός Λεπτομέρειας	Επίπεδο Πολυπλοκότητας	Συμβατότητα
		Επιχειρησιακό	Τεχνικό			
Intel's TAL	Οργανισμού, επιχειρησιακής διεργασίας/στόχου, συστήματος	Ουδέτερο	Ουδέτερο	Χαμηλό	Μεσαίο	Υψηλή (NIST SP 800-30, ATT&CK)
OCTAVE/ Allegro	Οργανισμού, επιχειρησιακής διεργασίας/στόχου, συστήματος	Ουδέτερο	Ουδέτερο	Μεσαίο (επεκτάσιμο)	Μεσαίο	Χαμηλή
PREATT&CK	Συστήματος	Ουδέτερο	Συστήματος (Microsoft Windows)	Υψηλό	Χαμηλό	Υψηλή
TARA	Οργανισμού, επιχειρησιακής διεργασίας/στόχου, συστήματος	Ουδέτερο	Ουδέτερο	Χαμηλό	Μεσαίο	Υψηλή (NIST SP 800-30, ATT&CK)
CAPEC	Συστήματος	Ουδέτερο	Ουδέτερο (Έμφαση σε λειτουργικό σύστημα Microsoft Windows & nix)	Υψηλό	Μεσαίο	Μεσαία (NIST SP 800-30)
ENISA	Οργανισμού, επιχειρησιακής διεργασίας/στόχου, συστήματος	Ουδέτερο	Ουδέτερο	Μεσαίο	Μεσαίο	Χαμηλή

ΚΕΦΑΛΑΙΟ 9: Αυθεντικοποίηση οντότητας

Ασφάλεια Πληροφοριών & Συστημάτων στον Κυβερνοχώρο

Περιεχόμενα

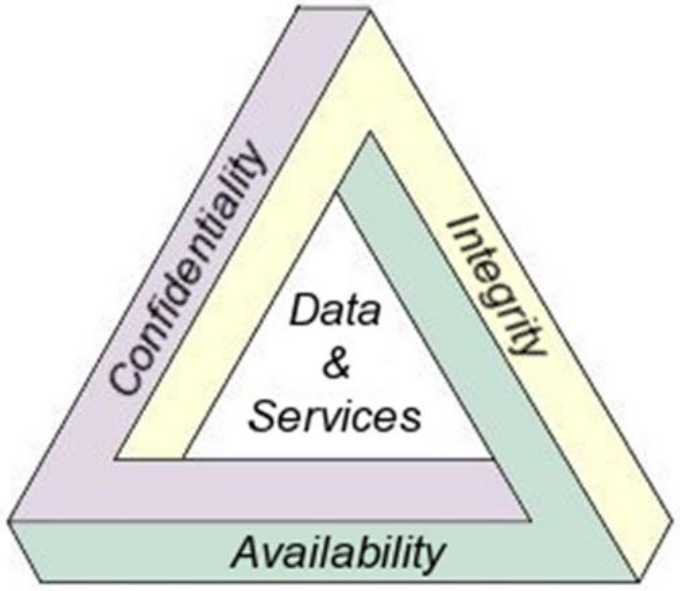
1. Εισαγωγή
2. Εννοιολογική Θεμελίωση
3. Ταυτοποίηση Χρήστη με Κωδικούς Πρόσβασης
4. Αυθεντικότητα Οντότητας με Κρυπτογραφικές Τεχνικές

Εισαγωγή

ΕΛΕΓΧΟΣ ΠΡΟΣΠΕΛΑΣΗΣ (ΓΕΝΙΚΑ)

- Προσπέλαση
  - Ροή της πληροφορίας μεταξύ υποκειμένου και αντικειμένου
- Υποκείμενο
  - Μια οντότητα που αιτείται πρόσβαση σε αντικείμενο (ή σε δεδομένα στο αντικείμενο)

- Αντικείμενο
  - Μια (παθητική) οντότητα που περιέχει πληροφορία
- Έλεγχος Προσπέλασης – Γιατί;
  - Εμπιστευτικότητα
  - Διαθεσιμότητα
  - Ακεραιότητα



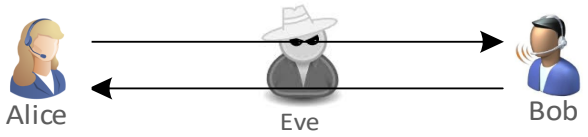
ΒΗΜΑΤΑ ΕΛΕΓΧΟΥ ΠΡΟΣΠΕΛΑΣΗΣ

1. Το υποκείμενο αποδεικνύει την ταυτότητα του, υποβάλλοντας τα διαπιστευτήρια του
   - **Τεχνικές και Τεχνολογίες Ταυτοποίησης Οντότητας** (entity authentication)
2. Έλεγχος δικαιωμάτων πρόσβασης που έχει το υποκείμενο στο αντικείμενο
   - Έλεγχος Εξουσιοδότησης (authorization)
3. Για όση ώρα αποκτά πρόσβαση στο αντικείμενο, οι ενέργειες του υποκειμένου καταγράφονται
   - Καταγραφή και Έλεγχος (logging and audit)

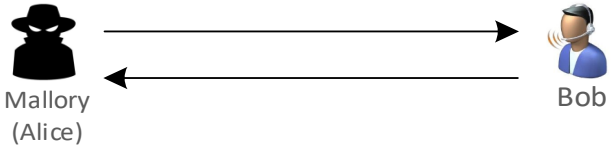
Εννοιολογική θεμελίωση

αυθεντικότητα: οντότητες και απειλές

- Eve: **Παθητικές Επιθέσεις** κατά της Εμπιστευτικότητας
  - Επιθέσεις υποκλοπής (eavesdropping, sniffing, traffic analysis, password cracking, breaking crypto keys,…)
- Mallory: **Ενεργητικές Επιθέσεις** κατά της Ακεραιότητας ή/και Αυθεντικότητας
  - Επιθέσεις τροποποίησης (modification)
  - Επιθέσεις πλαστοπροσωπίας (spoofing)
  - Επιθέσεις επανάληψης (replay)
  - Επιθέσεις ενδιάμεσης οντότητας (MIM)



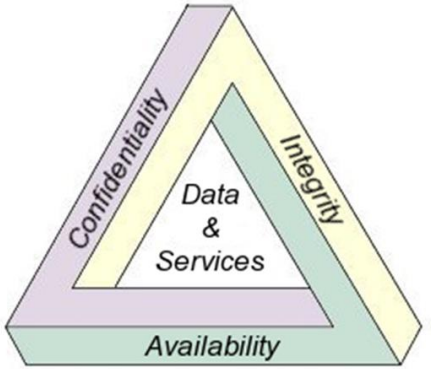
α) Επίθεση Υποκλοπής



β) Επίθεση Πλαστοπροσωπίας

γ) Επίθεση Ενδιάμεσης Οντότητας

Υπηρεσίες αυθεντικότητας & ακεραιότητας



Ακεραιότητα Δεδομένων

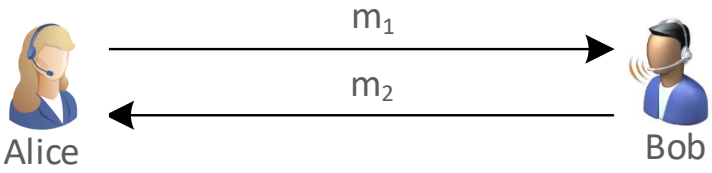
- *Είναι το μήνυμα που έλαβα ίδιο με αυτό που εστάλη;*

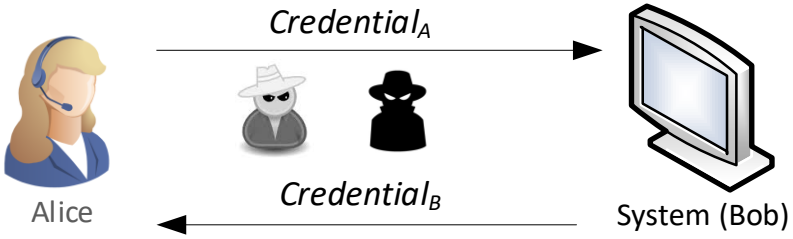
Αυθεντικότητα Μηνύματος

- *Ποιος δημιούργησε το μήνυμα που έλαβα;*

Αυθεντικότητα Οντότητας (Ταυτοποίηση)

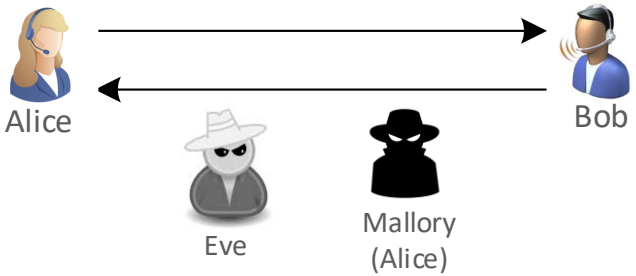
- *Με ποιον μιλάω αυτήν τη στιγμή;*



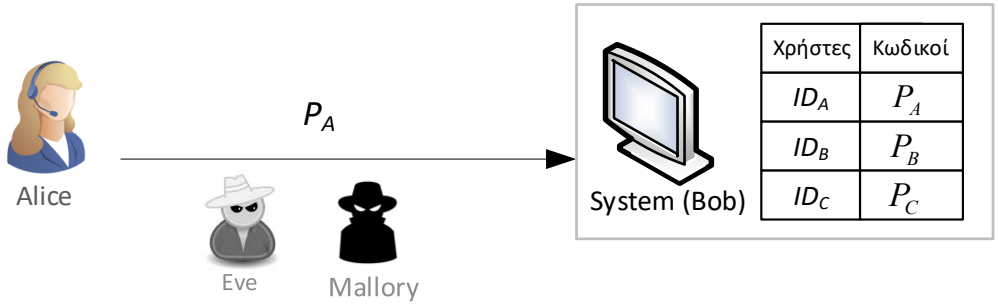


Ταυτοποίηση χρήστη ή προγράμματος

- **Ταυτοποίηση Χρήστη προς Σύστημα**
  - Κάτι που ξέρεις (SYK)
  - Κάτι που είσαι (SYA)
  - Κάτι που έχεις (SYH)
  - Ταυτοποίηση δύο ή περισσότερων παραγόντων (multi-factor)



- **Ταυτοποίηση Προγράμματος προς Πρόγραμμα**
  - Κρυπτογραφικές τεχνικές ταυτοποίησης
    - Ταυτοποίηση με Πρόκληση – Απάντηση (challenge response)
    - Ταυτοποίηση με χρονοσφραγίδες (timestamp-based)
    - Αποδείξεις μηδενικής γνώσης (zero-knowledge proofs)

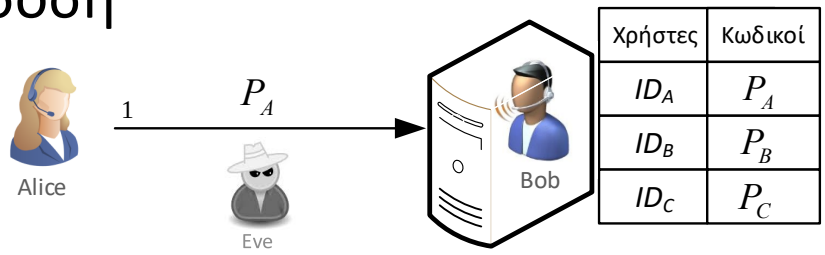


ΣΥΜΒΟΛΙΣΜΟΙ

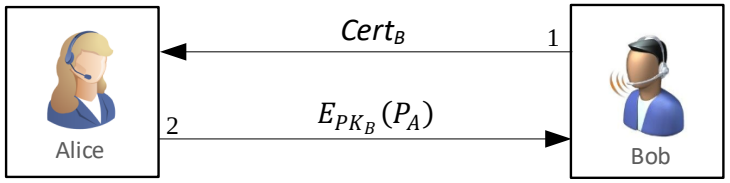
id_X	Μοναδικό όνομα της οντότητας X
m^*	Το μήνυμα m είναι προαιρετικό
r_X	Τυχαίος αριθμός που επιλέγεται από την οντότητα X
t_X	Χρονοσφραγίδα που επιλέγεται από την οντότητα X
K_{AB}	Συμμετρικό κλειδί που μοιράζονται οι *Alice* και *Bob*
SK_X	Ιδιωτικό κλειδί της οντότητας X
PK_X	Δημόσιο κλειδί της οντότητας X
$E_K(m)$	Κρυπτογράφηση του m με το συμμετρικό κλειδί K
$D_K(c)$	Αποκρυπτογράφηση του c με το συμμετρικό κλειδί K
$H(m)$	Η τιμή hash του μηνύματος m
$H_K(m)$	Η τιμή MAC του m με το συμμετρικό κλειδί K
$E_{PK_X}(m)$	Κρυπτογράφηση του m με το δημόσιο κλειδί PK_X
$D_{PK_X}(c)$	Αποκρυπτογράφηση του c με το ιδιωτικό κλειδί SK_X
$Sig_X(m)$	Η ψηφιακή υπογραφή στο μήνυμα m με το ιδιωτικό κλειδί SK_X
$Cert_X$	Πιστοποιητικό Δημόσιου Κλειδιού της οντότητας X

Ταυτοποίηση με κωδικούς πρόσβασης Απειλή: Υποκλοπή στο κανάλι επικοινωνίας

- **Απειλή**
  - Υποκλοπή κωδικού κατά τη μετάδοση
- **Ευπάθεια**
  - Μη Κρυπτογραφημένο Κανάλι
- **Αντίμετρο**
  1. Κρυπτογραφική προστασία καναλιού επικοινωνίας
     - (π.χ. SSH, SSL/TLS, IPSEC)
  2. Κωδικοί μιας Χρήσης (one-time)
     - Το Σύστημα του Lamport (1981)

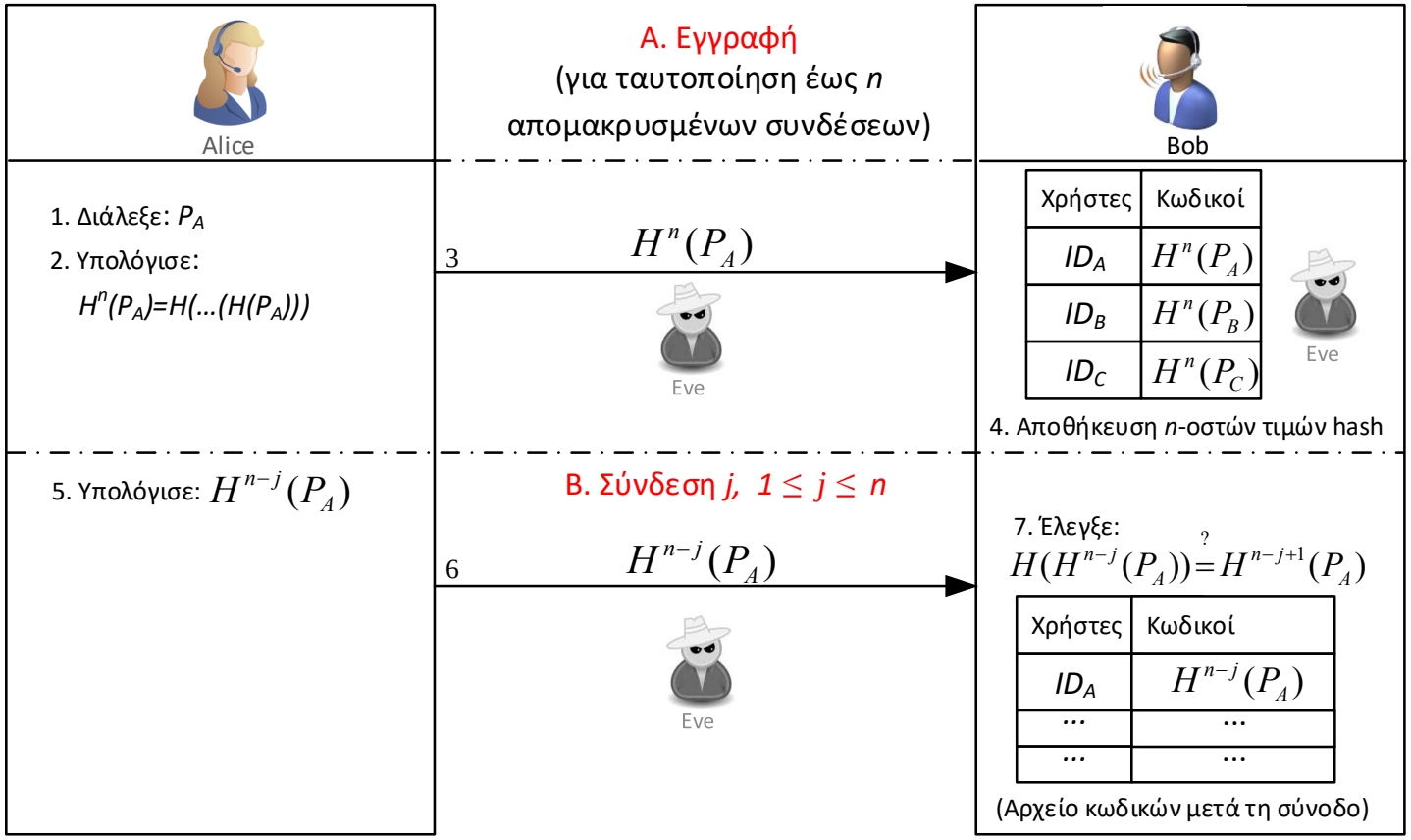


Απειλή 1 Υποκλοπή στο κανάλι μετάδοσης



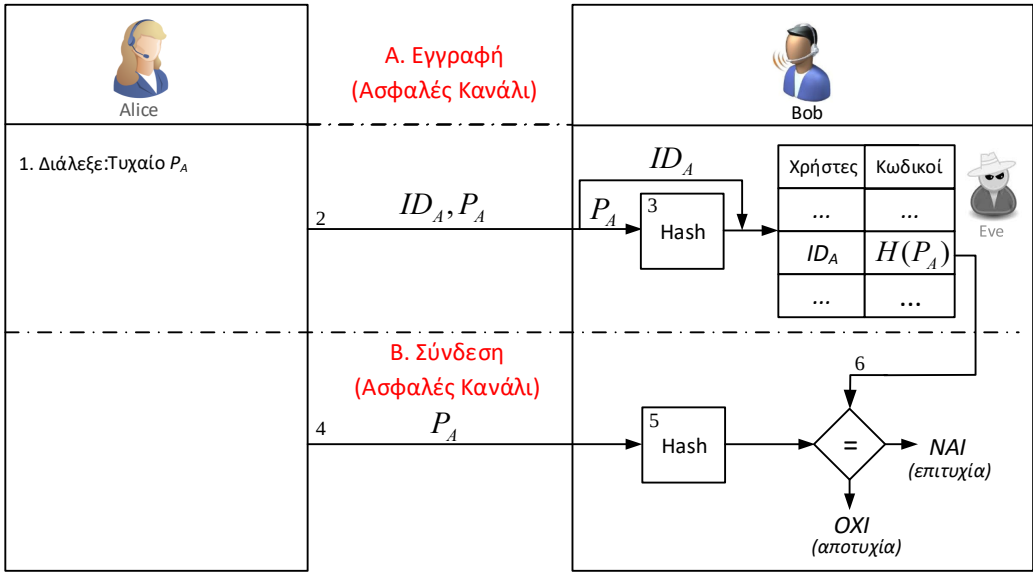
Αντίμετρο 1 – Κρυπτογράφηση Κωδικού

Ταυτοποίηση με κωδικούς πρόσβασης
Πρωτόκολλο κωδικών μιας χρήσης LAMPORT (1981)

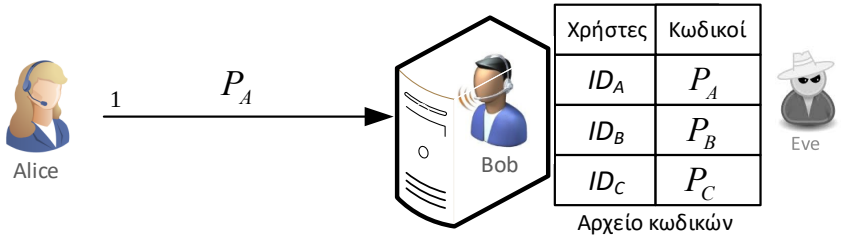


Ταυτοποίηση με κωδικούς πρόσβασης Απειλή: Υποκλοπή κατά την αποθήκευση (1/2)

- **Απειλή Α:**
  - Υποκλοπή Αρχείου Κωδικών
- **Ευπάθεια**
  - Μη Κρυπτογραφημένοι Κωδικοί
- **Αντίμετρο**
  - Κρυπρογράφηση κωδικών πρόσβασης



Σχήμα 9.5 Το Πρωτόκολλο ταυτοποίησης του Needham

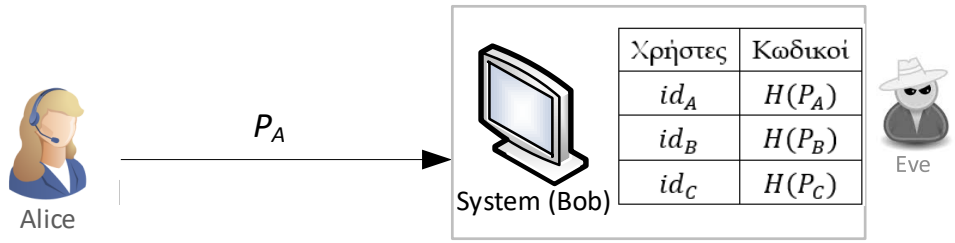


Ταυτοποίηση με κωδικούς πρόσβασης Απειλή: Υποκλοπή κατά την αποθήκευση (2/2)

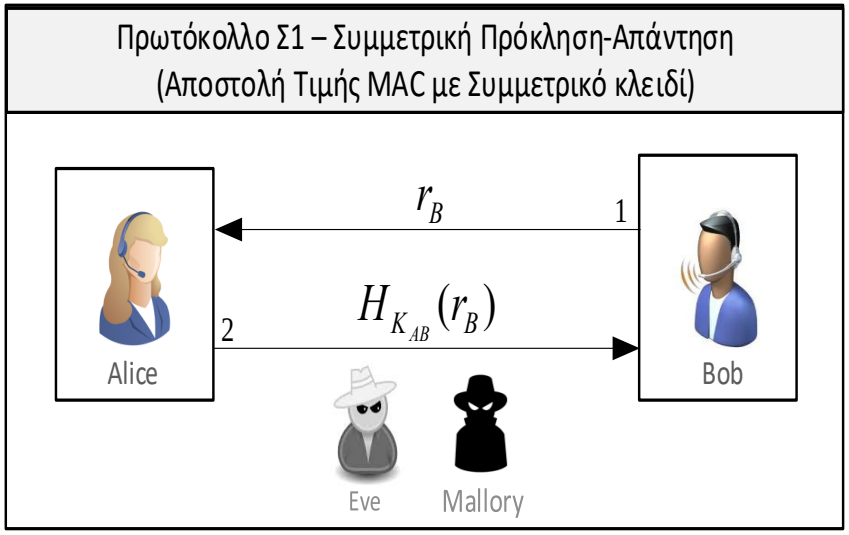
- **Απειλή Β:**
  - Επίθεση ωμής βίας ή λεξικού
- **Ευπάθεια**
  - Χαμηλή εντροπία κωδικών πρόσβασης
- **Αντίμετρο**
  - Κωδικοί υψηλής εντροπίας

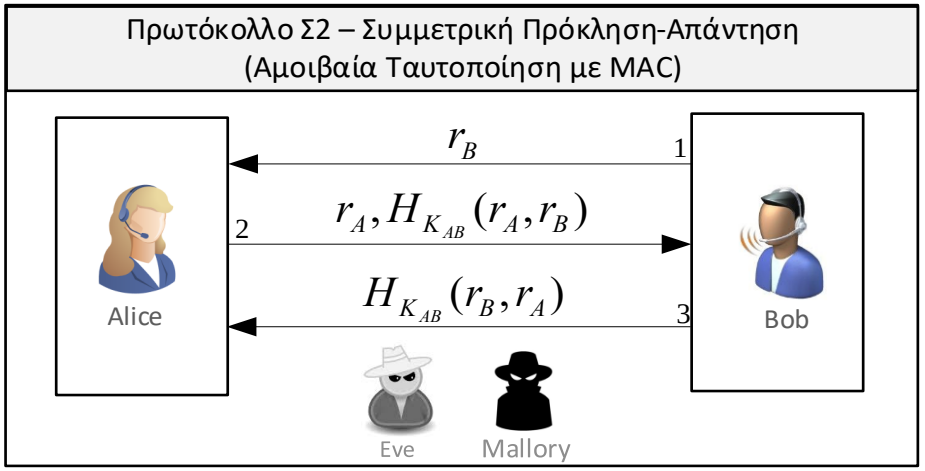
n	26 lower-case letters	36 lower-case letters and digits	62 alpha-numeric characters	95 printable characters	all 128 ASCII characters
1	30 msec.	40 msec.	80 msec.	120 msec.	160 msec.
2	800 msec.	2 sec.	5 sec.	11 sec.	20 sec.
3	22 sec.	58 sec.	5 min.	17 min.	44 min.
4	10 min.	35 min.	5 hrs.	28 hrs.	93 hrs.
5	4 hrs.	21 hrs.	318 hrs.	112 days	500 days
6	107 hrs.	760 hrs.	2.2 yrs.	29 yrs.	174 yrs.

(Morris and Thompson, 1979)

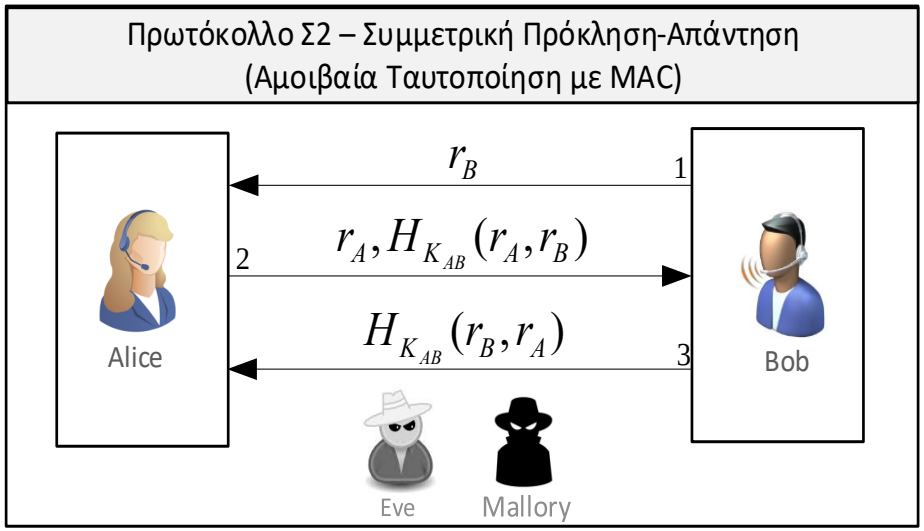


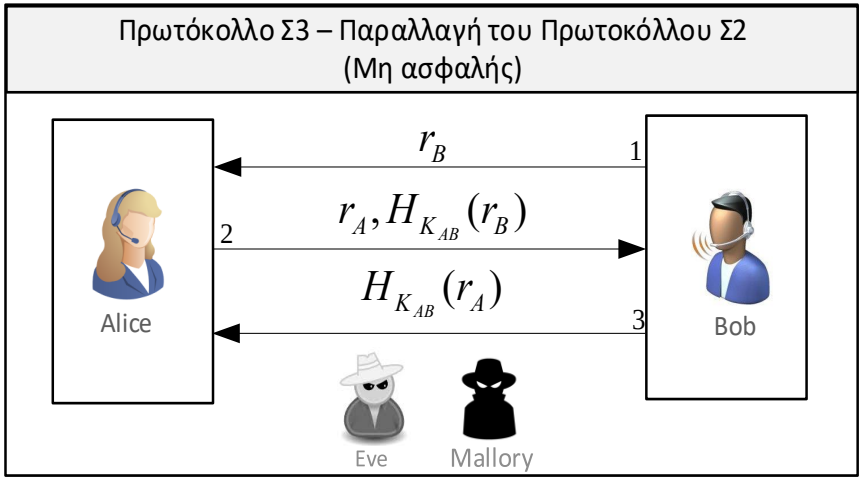
Αυθεντικότητα οντότητας με κρυπτογραφικές τεχνικές ταυτοποίηση με πρόκληση- απάντηση (συμμετρικές τεχνικές) (1/3)



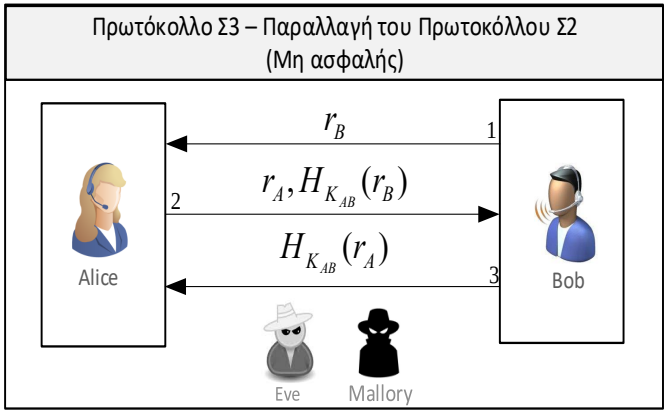


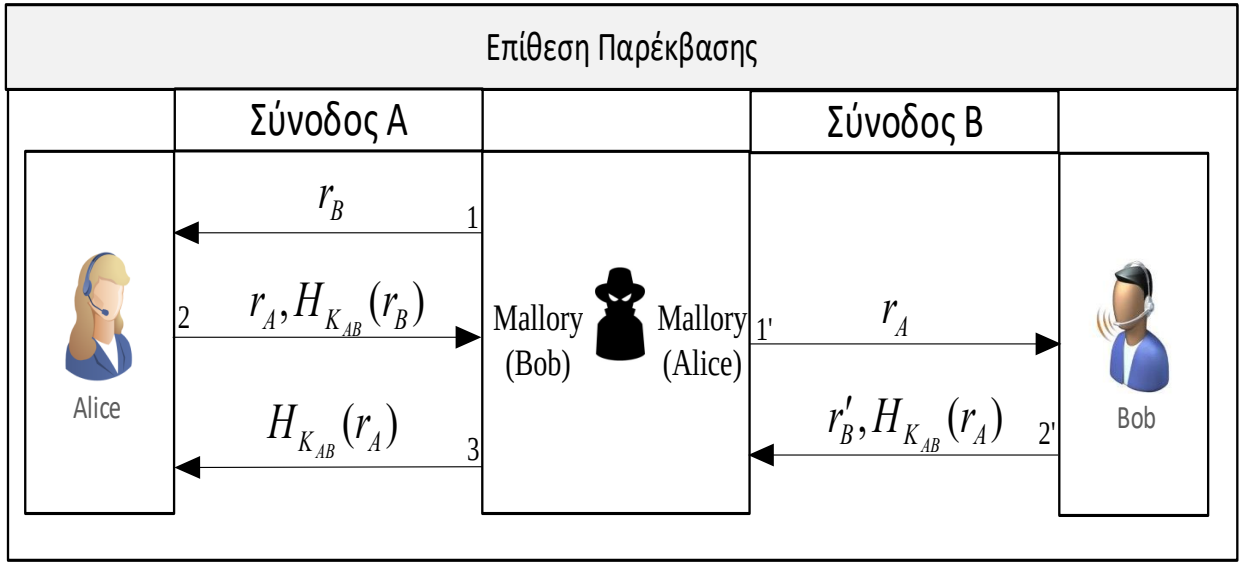
Αυθεντικότητα οντότητας με κρυπτογραφικές τεχνικές ταυτοποίηση με πρόκληση- απάντηση (συμμετρικές τεχνικές) (2/3)



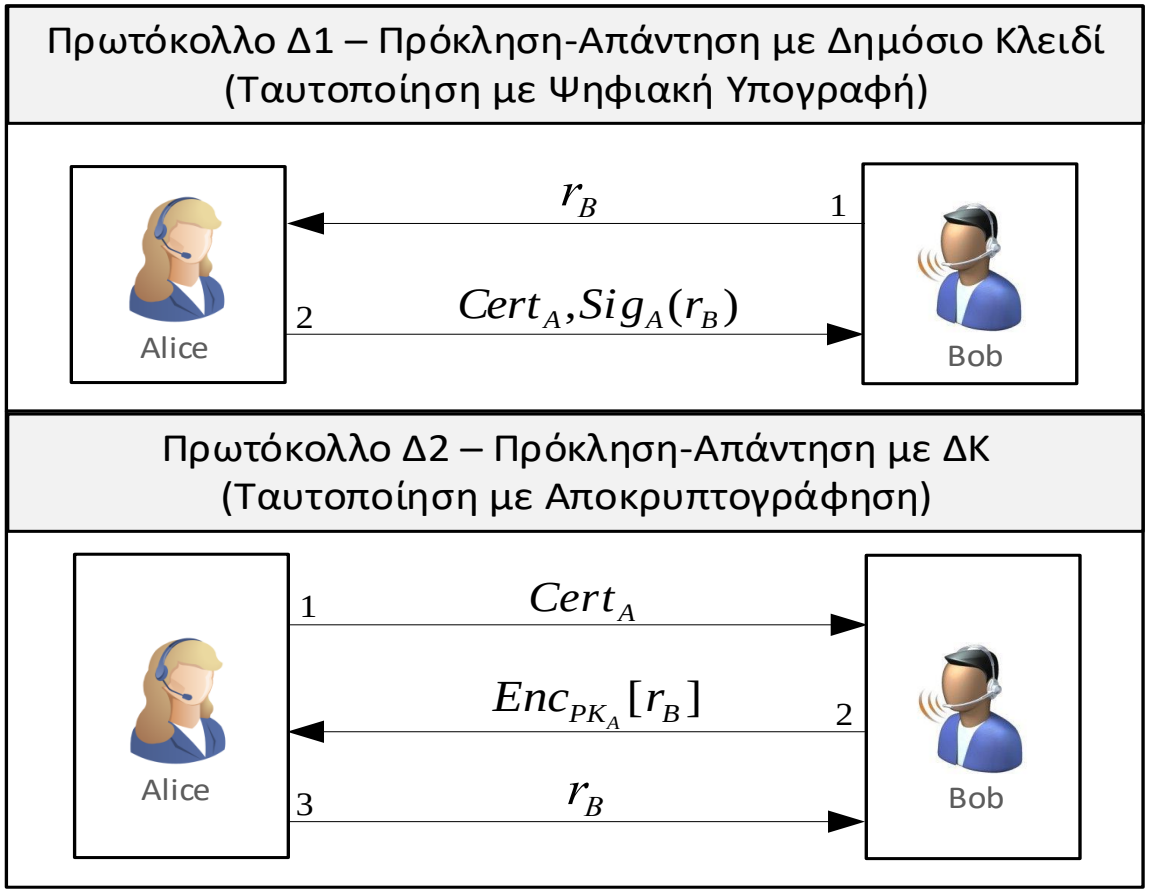


Αυθεντικότητα οντότητας με κρυπτογραφικές τεχνικές ταυτοποίηση με πρόκληση- απάντηση (συμμετρικές τεχνικές) (3/3)

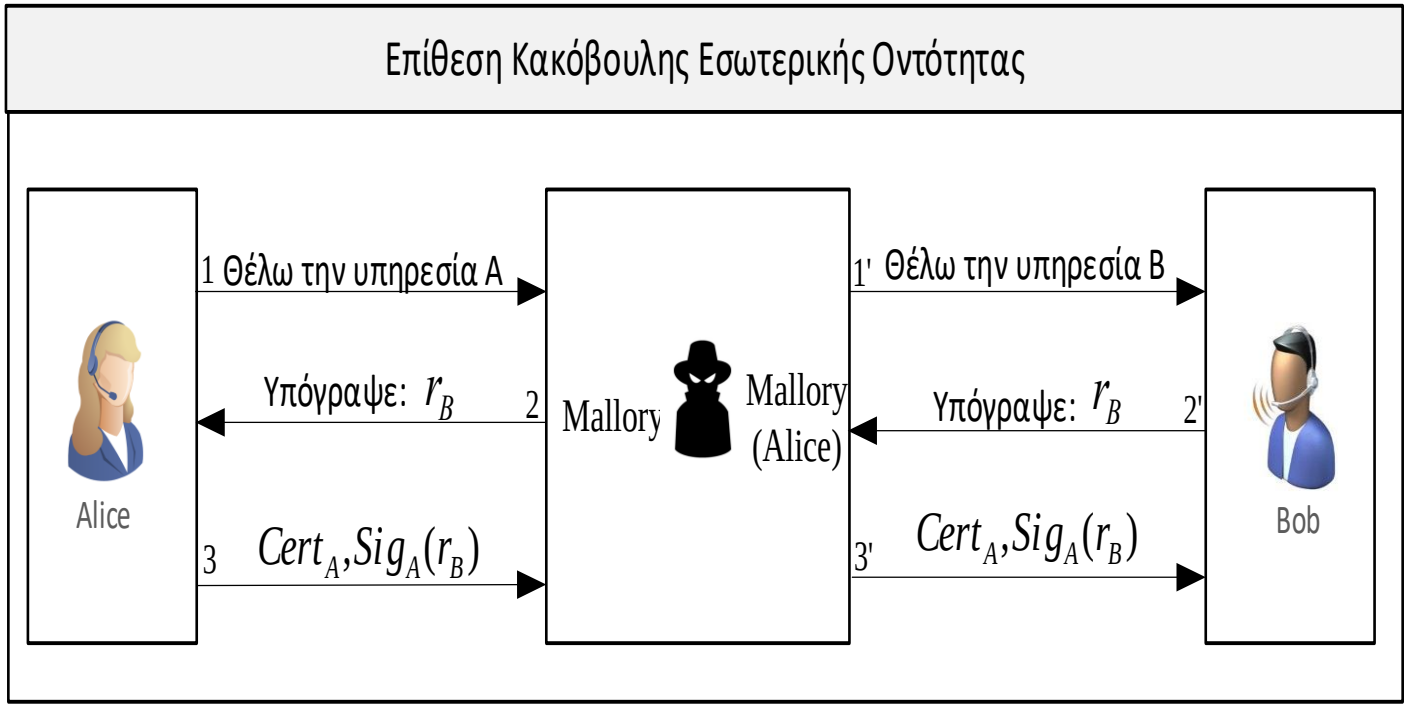




Αυθεντικότητα οντότητας με κρυπτογραφικές τεχνικές ταυτοποίηση με πρόκληση- απάντηση (τεχνικές ΔΚ) (1/2)

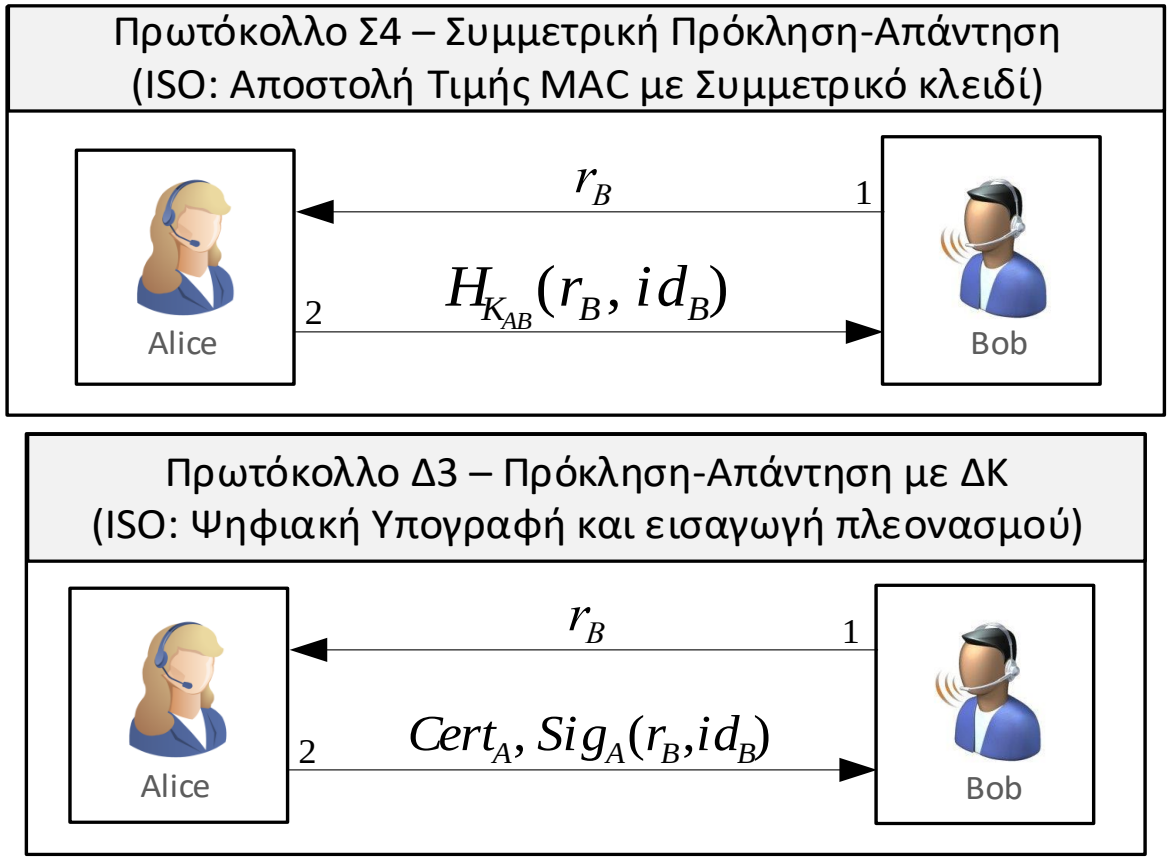


Αυθεντικότητα οντότητας με κρυπτογραφικές τεχνικές ταυτοποίηση με πρόκληση- απάντηση (τεχνικές ΔΚ) (2/2)

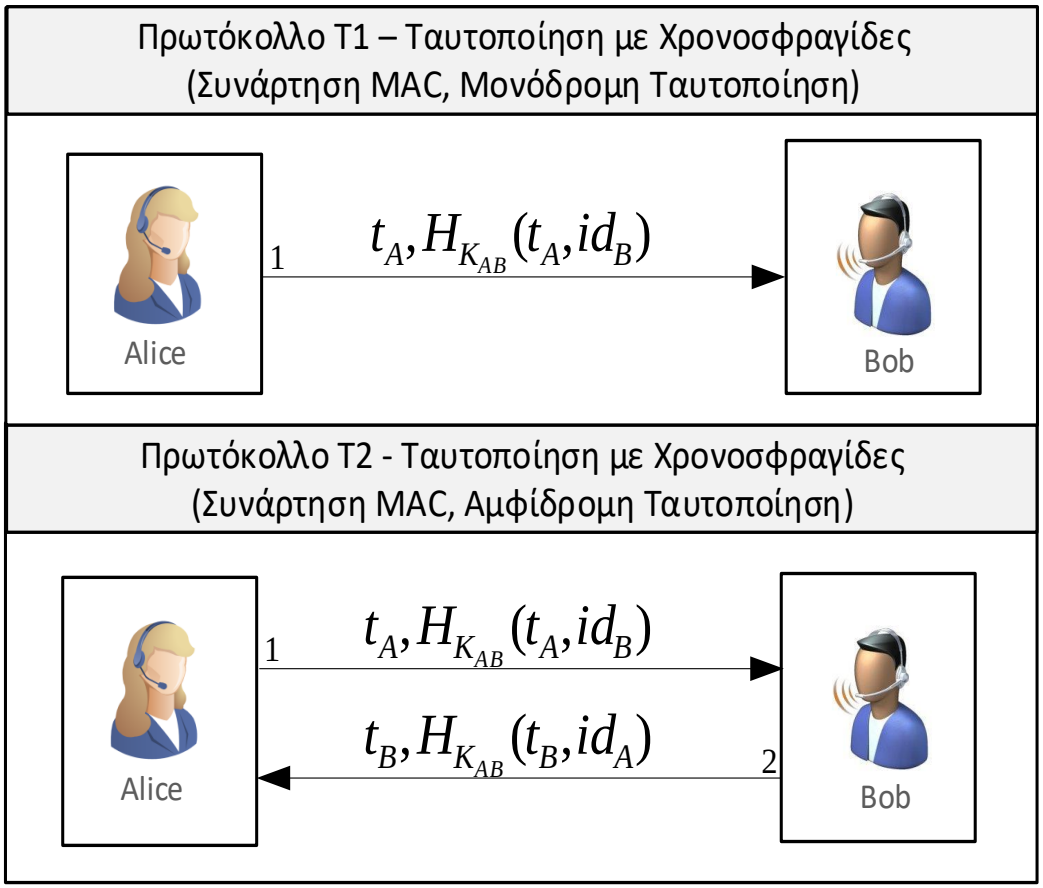


Σχήμα 9.11. Μία επίθεση σε πρωτόκολλα ταυτοποίησης

Αυθεντικότητα οντότητας με κρυπτογραφικές τεχνικές ταυτοποίηση με πρόκληση- απάντηση (χρήση πλεονασμού)



Αυθεντικότητα οντότητας με κρυπτογραφικές τεχνικές ταυτοποίηση με χρονοσφραγίδες (συμμετρικές τεχνικές)



Αυθεντικότητα οντότητας με κρυπτογραφικές τεχνικές ταυτοποίηση με χρονοσφραγίδες (τεχνικές ΔΚ)