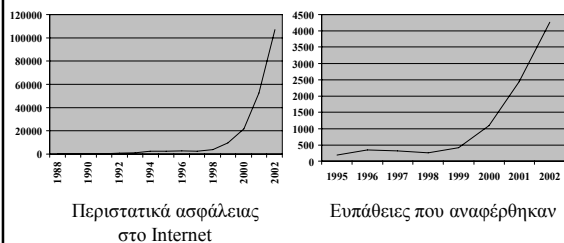


Ασφάλεια στο διαδίκτυο

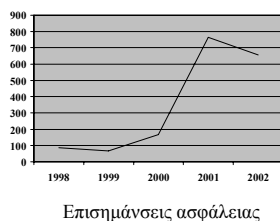
- Πρώτο μείζον πρόβλημα: 1988
 - Επίθεση με το «σκουλήκι» έθεσε εκτός λειτουργίας το 10% των υπολογιστών του Internet (6.000 από 60.000)
 - Δημιουργία της ομάδας CERT (Computer Emergency Response Team)
 - » 6 περιστατικά το 1988
 - » 2412 περιστατικά το 1995 με επιπτώσεις σε 12.000 δικτυακές περιοχές

Ασφάλεια στο Διαδίκτυο



Πηγή: CERT

Ασφάλεια στο Διαδίκτυο



Πηγή: CERT

Λόγοι αύξησης περιστατικών

- Οι υπολογιστές του Internet έχουν πολλαπλασιαστεί
- Οι χρήστες ομοίως
- Παρέχονται πολύ περισσότερες υπηρεσίες
- *Κάθε υπολογιστής, χρήστης και υπηρεσία παρέχει θαυμάσιες ευκαιρίες στους επίδοξους εισβολείς*

Επιθέσεις μέσω ηλεκτρονικού ταχυδρομείου

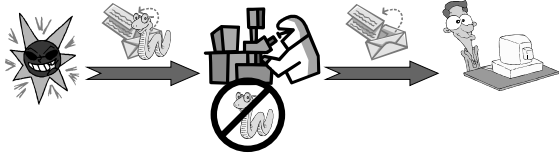
- Αρχικά: ηλεκτρονικό ταχυδρομείο = απλό κείμενο
- Συνέχεια: δυνατότητα επισύναψης εγγράφων
 - Οι χρήστες αποθηκεύουν σε αρχείο και ανοίγουν με την κατάλληλη εφαρμογή
- «Ευχρηστία»
 - Οι εφαρμογές ηλεκτρονικού ταχυδρομείου επιτρέπουν άμεση εκτέλεση της σχετιζόμενης εφαρμογής και εμφάνιση του εγγράφου, χωρίς ενδιάμεση αποθήκευση
 - Τα αρχεία προγραμμάτων θεωρούνται και αυτά έγγραφα
 - «Φιλική» παρουσίαση ονομάτων των εγγράφων

Επιθέσεις μέσω ηλεκτρονικού ταχυδρομείου

- Ο «κακός» επισυνάπτει έγγραφο-πρόγραμμα και το μεταμφιέζει σε άλλο τύπο εγγράφου
- Ο ανυποψίαστος χρήστης ανοίγει το έγγραφο, εκτελώντας έτσι το πρόγραμμα του κακού
 - Αποστολή μηνυμάτων σε άλλους
 - Αποστολή πληροφοριών στον «κακό»
 - Σβήσιμο αρχείων ή μόλυνσή τους
 - Μετάδοση μόλυνσης σε άλλους υπολογιστές

Επιθέσεις μέσω ηλεκτρονικού ταχυδρομείου - αντιμετώπιση

- Έλεγχος των συνημμένων εγγράφων
 - Για γνωστά επικίνδυνα προγράμματα
 - Για απόπειρες απόκρυψης του πραγματικού ονόματος
 - Αυτόματη μετονομασία των συνημμένων εγγράφων
 - Κατά προτίμηση στους κεντρικούς υπολογιστές διακίνησης ηλεκτρονικού ταχυδρομείου



Επιθέσεις μέσω ηλεκτρονικού ταχυδρομείου - Αντιμετώπιση

- Εγκατάσταση προγραμμάτων προστασίας στους υπολογιστές των χρηστών
- *Εναισθητοποίηση των χρηστών*
 - Να φαίνονται τα πλήρη ονόματα των αρχείων
 - Πρώτα να αποθηκεύετε τα αρχεία και κατόπιν να τα εκτελείτε
 - Μην ανοίγετε συνημμένα με άγνωστη προέλευση ή αν έχετε αμφιβολίες για το περιεχόμενό τους

Ασφάλεια σε προγράμματα πλοήγησης

- Τα πρώτα προγράμματα πλοήγησης απλά παρουσίαζαν κείμενο και εικόνες και προσέφεραν δυνατότητες πλοήγησης
- Οι νέες εκδόσεις κάνουν πολύ περισσότερα εκτελώντας κώδικα
 - Javascript, Java, ActiveX, plugins, κ.λπ.
- *Ουσιαστικά εκτελούμε κώδικα για τον οποίο δεν είμαστε σίγουροι*

Ασφάλεια για Javascript

- Απλή γλώσσα για ενεργή συμπεριφορά
- Πιθανά προβλήματα
 - Ανάγνωση ή τροποποίηση στοιχείων του προγράμματος πλοήγησης
 - » Π.χ. Αλλαγή αρχικής σελίδας, προσθήκη σελιδοδεικτών
 - Αποστολή μηνυμάτων
 - Ανάγνωση στοιχείων του συστήματος
 - » Ανάγνωση του αρχείου συνημτικών
 - Ανάγνωση ή τροποποίηση στοιχείων άλλων προγραμμάτων Javascript που εκτελούνται σε άλλα παράθυρα του προγράμματος πλοήγησης
- Η Javascript δεν έχει τυπικό μοντέλο ασφάλειας, βασίζεται στους κατασκευαστές

Ασφάλεια για Javascript

- Ορισμός επιπέδων προστασίας για διάφορα αντικείμενα και δικαιωμάτων για τα προγράμματα Javascript
 - UniversalBrowserRead, UniversalBrowserWrite, UniversalBrowserAccess
 - UniversalFileRead
 - UniversalPreferencesRead, UniversalPreferencesWrite
 - UniversalSendMail
- Οι κατασκευαστές των προγραμμάτων πλοήγησης δεν ελέγχουν πάντα όλες τις περιπτώσεις
 - `window.open('about:javascript', 'stealProperties');`

Ασφάλεια για Javascript

- Πολιτική ίδιας προέλευσης
 - Ένα πρόγραμμα Javascript δεν μπορεί να διαβάσει ή να γράψει μεταβλητές άλλου προγράμματος, εκτός αν προέρχονται από τον ίδιο εξυπηρέτη
 - Παράδειγμα
 - » Πρόγραμμα στη σελίδα URL <http://company.com/dir/page.html>

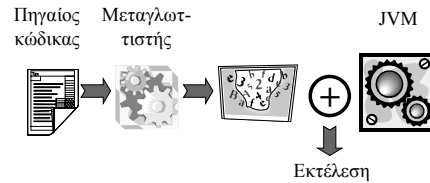
URL	Αποτέλεσμα	Λόγος
http://company.com/dir2/this.html	✓	
http://company.com/dir3/dir4/that.html	✓	
http://www.company.com/dir/pg.html	✗	Διαφορετικοί εξυπηρέτες
file:///D:/myPage.htm	✗	Διαφορετικό πρωτόκολλο
http://company.com:8080/dir/etc.html	✗	Διαφορετική θύρα

Ασφάλεια για Javascript

- Η πολιτική ίδιας προέλευσης είναι πολύ περιοριστική
 - » www1.ibm.com, www2.ibm.com
 - » www.symantec.com, www.sarc.com
- `document.domain = "ibm.com";`
- Υπογεγραμμένα προγράμματα
- Εξαγωγή, εισαγωγή διαδικασιών
- Απαγόρευση διαρροής ευαίσθητων πληροφοριών
 - Το πρόγραμμα πρέπει να έχει πρόσβαση σε πληροφορίες, δεν πρέπει όμως να τις στείλει στο δίκτυο
 - «Σεσημασμένες» πληροφορίες (*tainted information*)
 - Υπολογισμοί που περιλαμβάνουν σεσημασμένες πληροφορίες δίνουν σεσημασμένα αποτελέσματα
 - Ο χρήστης ειδοποιείται για προσπάθειες διαρροής σεσημασμένων πληροφοριών

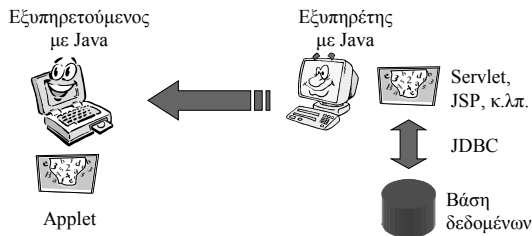
Ασφάλεια για Java

- Πλήρης γλώσσα προγραμματισμού
- Οι εφαρμογές μπορούν να εκτελεστούν αυτόνομα (applications) ή στο περιβάλλον ενός προγράμματος πλοήγησης (applets)



Η Java στους εξυπηρέτες

- Προγράμματα Java μπορούν να εκτελεστούν και στους εξυπηρέτες



Java – Πιθανά προβλήματα

- Διαρροή πληροφοριών
- Διαθεσιμότητα πόρων (Denial of Service)
- Ακεραιότητα πληροφοριών (καταστροφή, παραθοροά)
- Ενόχληση του χρήστη

Πόρος	Διαρροή	Διαθεσιμότη.	Ακεραιότητα	Ενόχληση
Σύστημα αρχείων	✓	✓	✓	✓
Δίκτυο	✓	✓	✓	✓
Μνήμη	✓	✓	✓	✓
Συσκευές εξόδου				✓
Συσκευές εισόδου	✓	✓		✓
Διαχείριση διεργασιών		✓		✓
Περιβάλλον χρήστη	✓		✓	✓
Κλήσεις συστήματος	✓	✓	✓	✓
Επίπεδο άμυνας Java	Υψηλό	Χαμηλό	Υψηλό	Χαμηλό

Java – Μοντέλο ασφάλειας

- Κώδικας που εμπιστευόμαστε
- Κώδικας που δεν εμπιστευόμαστε
- Η εκτέλεση του κώδικα που δεν εμπιστευόμαστε γίνεται σε ένα περιβάλλον αυξημένης ασφάλειας το *sandbox*



Java – Τι απαγορεύεται

- Ανάγνωση, διαγραφή, μετονομασία, έλεγχος ύπαρξης, αναφορά ιδιοτήτων αρχείων
- Δημιουργία ή αναφορά περιεχομένων για καταλόγους
- Σύνδεση προς διαφορετικό υπολογιστή από τον εξυπηρέτη προέλευσής του και δημιουργία θυρών προς υποδοχή συνδέσεων
- Δημιουργία παραθύρου πρώτου επιπέδου χωρίς προειδοποίηση ότι πρόκειται για ανασφαλή εφαρμογή
- Συλλογή πληροφοριών για τον χρήστη (όνομα, προσωπικός κατάλογος)
- Ορισμός ιδιοτήτων του συστήματος
- Εκτέλεση προγραμμάτων
- Τερματισμός της εκτέλεσης της εικονικής μηχανής
- Φόρτωση δυναμικών βιβλιοθηκών
- Δημιουργία και πρόσβαση νημάτων ελέγχου εκτός των δικών της
- Δημιουργία περιβάλλοντος φόρτωσης κλάσεων ή διαχείρισης ασφαλείας
- Δημιουργία διαδικασιών ελέγχου δικτύου π.χ. URLStreamHandlerFactory
- Ορισμός κλάσεων που ενσωματώνονται στις κλάσεις του υπολογιστή

Java – Τι επιτρέπεται

- Κεντρική μονάδα επεξεργασίας
- Μνήμη
- Οι προγραμματιστές θεωρούν το μοντέλο περιοριστικό
 - Προσωρινά αρχεία
- Στη δεύτερη έκδοση της Java μία ψηφιακά υπογεγραμμένη εφαρμογή μπορεί να ζητήσει περισσότερα προνόμια με επιβεβαίωση από τον χρήστη
 - Όσο αυξάνονται τα προνόμια, τόσο μειώνεται η ασφάλεια

Java – Ασφάλεια μέσω σχεδιασμού της γλώσσας

- Η Java είναι αντικειμενοστρεφής γλώσσα με *πακέτα, κλάσεις, στιγμιότυπα, μεταβλητές*

Πληροφορία	Προσπελάσσεται από
Ιδιωτική μεταβλητή	Την ίδια την κλάση
Προστατευμένη μεταβλητή	Την ίδια την κλάση, τις υποκλάσεις και κλάσεις στο ίδιο πακέτο
Δημόσια μεταβλητή	Όλες τις κλάσεις
Εξ ορισμού συμπεριφορά	Την ίδια την κλάση και κλάσεις στο ίδιο πακέτο

Java – Ασφάλεια μέσω σχεδιασμού της γλώσσας

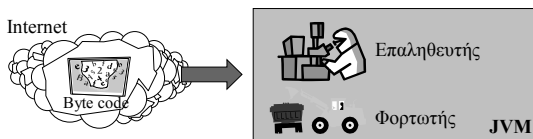
- Δήλωση αντικειμένων και μεθόδων ως *final* – δεν μπορούν να τροποποιηθούν ή να επανορισθούν
- Τα όρια των πινάκων ελέγχονται σε κάθε πρόσβαση
- Η μετατροπή τύπων είναι ιδιαίτερα περιορισμένη
- Οι μεταβλητές δεν μπορούν να χρησιμοποιηθούν πριν αρχικοποιηθούν
- Η αυτόματη συλλογή απορριμμάτων ελευθερώνει τη μνήμη που δεν χρειάζεται

Τα τμήματα του Sandbox



- Επαληθευτής: ασφάλεια μορφής και τύπων δεδομένων
- Φορτωτής κλάσεων: φορτώνει δυναμικά κλάσεις από το περιβάλλον εκτέλεσης
- Διαχειριστής ασφαλείας: αποτρέπει ενδεχομένως επισφαλή λειτουργικότητα

Sandbox – Ο επαληθευτής

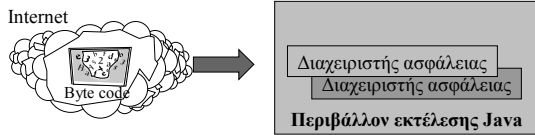


- Ο επαληθευτής είναι τμήμα του περιβάλλοντος εκτέλεσης, απροσπέλαστο για τα προγράμματα, και ελέγχει:
 - Αν η μορφή του κώδικα είναι σωστή
 - Αν ο κώδικας παραποιεί δείκτες, παραβιάζει περιορισμούς πρόσβασης ή χρησιμοποιεί λάθος πληροφορίες τύπων
 - Έλεγχος συνέπειας εκδόσεων κλάσεων
 - » Διαγραφή μεθόδων που χρησιμοποιούνται
- Η διαδικασία είναι σχετικά χρονοβόρα
 - Πολλές φορές διαρκεί περισσότερο από το «κατέβασμα»

Sandbox – Ο επαληθευτής

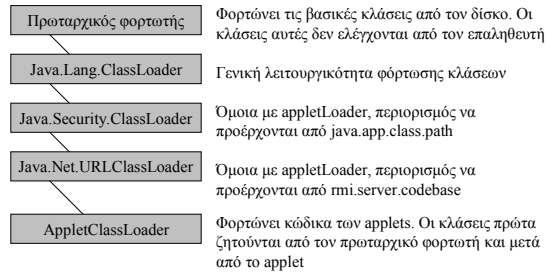
- Μετά το πέρας της επαλήθευσης είναι βέβαιο ότι:
 - Το αρχείο έχει τη σωστή μορφή
 - Δεν θα υπάρξει υπερχείλιση ή εξάντληση της σμίκρας
 - Όλοι οι τύποι των παραμέτρων είναι σωστοί
 - Δεν υπάρχουν παράνομες μετατροπές τύπων δεδομένων
 - Οι προσπελάσεις σε μεταβλητές υπακούνε στους κανόνες πρόσβασης της γλώσσας (public, private, κ.λπ.)
 - Οι αναγνώσεις και εγγραφές σε καταχωρητές είναι έγκυρες

Sandbox – Φορτωτής κλάσεων



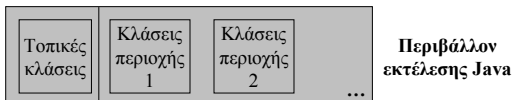
- Πιθανότητα πρόβλημα ασφάλειας
- Πιθανώς όμως και όχι!
- Τελικά εξαρτάται από το πόσο εμπιστευόμαστε τον συγγραφέα

Sandbox – Φορτωτής κλάσεων



Sandbox – Φορτωτής κλάσεων

- Περιοχές ονοματολογίας
 - Μία κλάση μπορεί να χρησιμοποιείται από πάνω από μία εφαρμογές δικτύου
 - » *Εύρεση/Μετοχή* σε λεξικό ρημάτων και εφαρμογή χρηματιστηρίου
 - Η ίδια κλάση μπορεί να είναι ενσωματωμένη στη Java και να χρησιμοποιείται από εφαρμογή
- Μπορεί να ορίζεται περιοχή ονοματολογίας



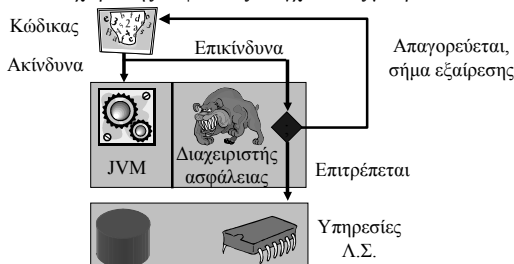
Κατά την αναφορά σε κλάσεις ελέγχονται και πάλι πρώτα οι ενσωματωμένες κλάσεις και κατόπιν οι κλάσεις στην περιοχή ονοματολογίας

Sandbox – Φορτωτής κλάσεων

- Έλεγχος αν η κλάση έχει φορτωθεί – αν ναι, επιστρέφεται η φορτωμένη
- Απόπειρα φόρτωσης της κλάσης από τον πρωταρχικό φορτωτή
- Έλεγχος αν ο φορτωτής έχει το δικαίωμα δημιουργίας της κλάσης
- Διάβασμα της κλάσης σε έναν πίνακα από bytes, είτε από το δίκτυο είτε από αρχεία
- Δημιουργία του αντικειμένου και των μεθόδων
- Προσδιορισμός των κλάσεων που απαιτούνται άμεσα από την κλάση (π.χ. πρόγονοι, εκφράσεις αρχικοποίησης) και έλεγχος γι' αυτές
- Έλεγχος του αρχείου κλάσης από τον επαληθευτή

Sandbox – Διαχειριστής ασφάλειας

- Οι βιβλιοθήκες της Java παρέχουν πλήρη λειτουργικότητα
- ... η οποία δεν πρέπει να είναι προσπελάσιμη στον καθένα!
- Ο διαχειριστής ασφάλειας ελέγχει ποιος μπορεί να κάνει τι



Sandbox – Διαχειριστής ασφάλειας

- Λειτουργία διαχειριστή
 - Ένα πρόγραμμα Java καλεί μία εν δυνάμει επικίνδυνη λειτουργία στη διασύνδεση της Java
 - Ο κώδικας βιβλιοθήκης της Java ρωτά τον διαχειριστή ασφάλειας αν επιτρέπεται ή όχι
 - Αν όχι, δεν εκτελείται η λειτουργία και δημιουργείται ένα σήμα εξαιρέσης που διαδίδεται στη στοιβιά εκτέλεσης
 - Αν ναι, η διαδικασία εκτελείται κανονικά
- Στην απόφαση συμμετέχουν ο χρήστης και η προκαθορισμένη πολιτική