Ασφάλεια και ΕΛ/ΛΑΚ

Πάτροκλος Αργυρούδης Δημήτρης Γλυνός
Νίκος Τσαγκαράκης

census
IT security research, development and services
{argp, dimitris, ntsag}@census.gr

Ημερίδα ΕΛ/ΛΑΚ, Σχολή Ικάρων
23 Οκτωβρίου 2009

Περίγραμμα

Εισαγωγή

- Ψηφιακή ασφάλεια: η ικανότητα προστασίας πληροφοριών από αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένες προσβάσεις
- Βασικές έννοιες
  - Εμπιστευτικότητα: μη εξουσιοδοτημένη ανάγνωση, ιδιωτικότητα, μυστικότητα
  - Ακεραιότητα: μη εξουσιοδοτημένη μεταβολή
  - Διαθεσιμότητα: άρνηση παροχής υπηρεσιών, υπηρεσίες/πληροφορίες άμεσα προσπελάσιμες (από εξουσιοδοτημένους χρήστες)
- Ασφάλεια δεδομένων, συστημάτων και δικτύων
- Συμβολή τεχνολογιών και εργαλείων ΕΛ/ΛΑΚ

Σημασία της ασφάλειας

- Οργανισμοί, εταιρίες και ιδιώτες
  1. Τεράστια αύξηση των μαζικών κλοπών προσωπικών δεδομένων (στοιχεία ταυτοτήτων, ιατρικών ιστορικών, πιστωτικών καρτών, ...)
  2. Νομοθεσία που επιβάλει τη δημοσιοποίηση περιστατικών παραβίασης της ασφάλειας
  3. Μεγάλες οικονομικές ζημίες από τις παραβιάσεις
  4. Πλήγμα υπόληψης το οποίο είναι αδύνατο να υπολογιστεί
- 2001-2002: παραβιάσεις στο Πεντάγωνο, στη NASA και σε συνολικά 98 κυβερνητικά δίκτυα των Η.Π.Α. από τον Gary McKinnon
- 2003: το σκουλήκι Slammer διείσδυσε στο πυρηνικό εργοστάσιο Davis-Besse (Η.Π.Α.) και το παρέλυσε
- 2006: παραβίαση του Υπουργείου Γεωργίας (Η.Π.Α.)
- 2007: μερική παράλυση των συστημάτων του Υπουργείου Εμπορείου (Η.Π.Α.) για ένα μήνα

Σημασία του ΕΛ/ΛΑΚ για την ασφάλεια

- Ανοικτός κώδικας σημαίνει περισσότεροι και λεπτομερέστεροι έλεγχοι για προβλήματα ασφάλειας
- Το ανοικτό μοντέλο ανάπτυξης υποχρεώνει τους προγραμματιστές να γράφουν καλύτερο/καθαρότερο κώδικα και να ακολουθούν τα πρότυπα
- Ταχύτερη διόρθωση των κενών ασφάλειας
- Οι διαφορές μεταξύ των διανομών συμβάλλουν στην ασφάλεια
- Ευκολότερος εντοπισμός κακόβουλων λειτουργιών
- Βέβαια, τα παραπάνω μπορούν να οδηγήσουν σε ένα λανθασμένο αίσθημα ασφάλειας
  - Το ΕΛ/ΛΑΚ είναι δυνητικά ασφαλέστερο
  - Οι τακτικοί έλεγχοι από τρίτους είναι απαραίτητοι και στο κλειστό και στο ανοικτό λογισμικό

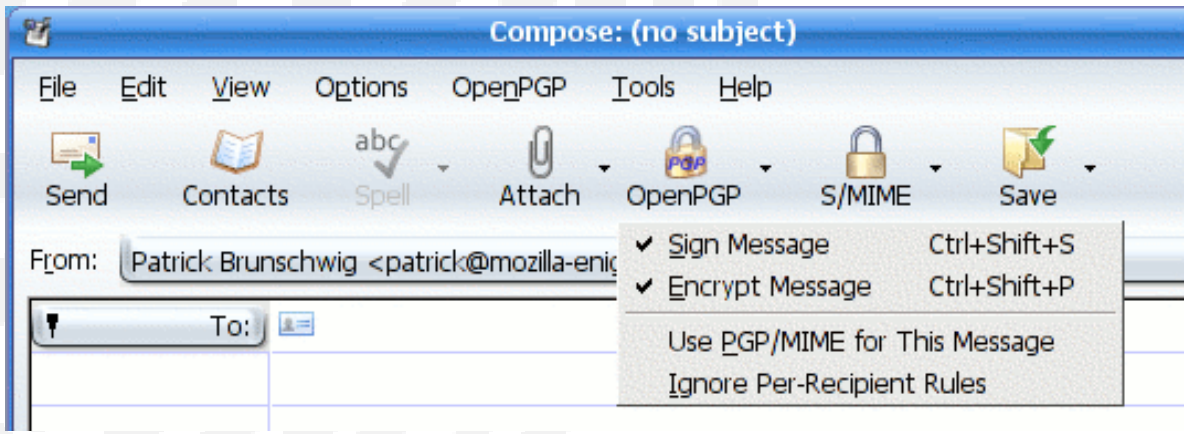
Ασφάλεια δεδομένων

Κρυπτογραφία

- Ένας αλγόριθμος κρυπτογράφησης διασφαλίζει την εμπιστευτικότητα (κυρίως) των δεδομένων
- Πολύ δύσκολο να σχεδιαστεί σωστά συνεπώς προϋποθέτει τη δυνατότητα ελέγχου από τρίτους (ανοικτός σχεδιασμός)
- Πολύ δύσκολο να υλοποιηθεί σωστά (ανοικτός κώδικας)
- Παράδειγμα προς αποφυγή: ο αλγόριθμος A5/1 των δικτύων κινητής τηλεφωνίας (GSM)
  - Πρακτικές επιθέσεις σε πραγματικό χρόνο υπό ανάπτυξη
- Παραδείγματα προς μίμηση: PGP (GnuPG), SSL (OpenSSL, OpenVPN), SSH (OpenSSH), IPsec (FreeS/WAN, Openswan)
  - Όλα βασισμένα σε ανοικτούς αλγορίθμους και λογισμικό

Ψηφιακές υπογραφές

- Εφαρμογή ασύμμετρων κρυπτοσυστημάτων
- Έλεγχος ακεραιότητας μηνύματος, ταυτοποίησης αποστολέα, μη αποποίηση ευθύνης
- Δεν προσφέρουν εμπιστευτικότητα
- GNU Privacy Guard (GnuPG ή GPG)
  - Εργαλείο της γραμμής εντολών
  - `$ gpg --output test.txt.sig --detach-sig test.txt`
  - `$ gpg --verify test.txt.sig test.txt`
- Thunderbird Enigmail



Κρυπτογράφηση μέσων αποθήκευσης

- Η κλοπή ενός φορητού Η/Υ είναι απλά κλοπή υλικού και όχι προσωπικών δεδομένων
- Μία παραβίαση συνεπάγεται σε χρόνο μη λειτουργίας και όχι σε κλοπή δεδομένων
- TrueCrypt: υποστηρίζει εικονικούς δίσκους αποθηκευμένους σε ένα αρχείο ή ολόκληρους δίσκους και κατατμήσεις
  - Παρέχει τη δυνατότητα αληθοφανούς άρνησης υποστηρίζοντας ένθετους κρυπτογραφημένους τόμους
- EncFS: δεν απαιτεί αλλαγές στον πυρήνα, κρυπτογραφεί καταλόγους και αρχεία, όχι κατατμήσεις ή ολόκληρους δίσκους
- dm-crypt: μέρος του πυρήνα, υποστηρίζει ολόκληρους δίσκους, κατατμήσεις, της κατάτμησης εναλλαγής (swap), καθώς και εκκίνηση από κρυπτογραφημένες κατατμήσεις

Ασφάλεια συστημάτων

Ακεραιότητα του συστήματος αρχείων

- Tripwire, Samhain: ανίχνευση μη εξουσιοδοτημένων αλλαγών στο σύστημα αρχείων μέσω κρυπτογραφικών συναρτήσεων σύνοψης
  - Βάση με τις συνόψεις όλων των αρχείων
  - Καταγραφή ιστορικού σε κεντρικό διακομιστή
- Υπογεγραμμένα πακέτα λογισμικού για προστασία από μη εξουσιοδοτημένη εγκατάσταση προγραμμάτων
  - Μέσω ψηφιακών υπογραφών
  - Καθιερωμένη πρακτική σε όλες τις δημοφιλής διανομές (Red Hat, Fedora, Debian, openSUSE, Gentoo, ...)
- Υπογεγραμμένα εκτελέσιμα αρχεία για προστασία από μη εξουσιοδοτημένη εκτέλεση προγραμμάτων
  - Έλεγχος της υπογραφής από τον πυρήνα σε κάθε κλήση εκτελέσιμου αρχείου

Τεχνολογίες περιορισμού

- `chroot(2)`: περιορισμός διεργασιών
  - Ως προς το μέρος του συστήματος αρχείων που μπορούν να έχουν πρόσβαση
- Jails -- φυλακές (FreeBSD): επεκτείνουν το μοντέλο του `chroot(2)` με την εικονικοποίηση
  - της πρόσβασης στο σύστημα αρχείων
  - των χρηστών
  - του υποσυστήματος δικτύωσης
- Συστήματα εικονικοποίησης: δυνατότητα ταυτόχρονης χρήσης του υλικού από πολλά λειτουργικά συστήματα
  - VirtualBox, Xen, QEMU, Bochs

Διαχείριση προνομίων

- Οι σημαντικότερες σύγχρονες εφαρμογές ΕΛ/ΛΑΚ ακολουθούν την αρχή ελαχίστων προνομίων, π.χ. OpenSSH
  - Η εφαρμογή χρησιμοποιεί ακριβώς τα προνόμια που χρειάζεται, αποδεσμεύοντας τα επιπλέον προνόμια σταδιακά
- Security-Enhanced Linux (SELinux): ανοικτή υλοποίηση κατά-απαίτηση (mandatory) πολιτικής ασφάλειας
  - Η προσπέλαση δεδομένων και πόρων επιτρέπεται μόνο σε υποκείμενα που τα έχουν ανάγκη για να εκτελέσουν τις εργασίες τους
- grsecurity: σύνολο τροποποιήσεων για τον πυρήνα με στόχο τη βελτίωση της ασφάλειας
  - Διαχείριση προνομίων με ρόλους και υλοποίηση της αρχής ελαχίστων προνομίων για ολόκληρο το σύστημα
  - PaX: τυχαιοποίηση διευθύνσεων και μη εκτελέσιμες σελίδες μνήμης

Τεχνολογίες αποτροπής εκμετάλλευσης

- Τυχαιοποίηση των διευθύνσεων των σελίδων μνήμης:
  - της στοίβας και του σωρού
  - αυτών που δεσμεύονται με mmap(2) (βιβλιοθήκες, malloc(3) κ.α.)
  - του κώδικα μιας εφαρμογής
- Μη εκτελέσιμες σελίδες μνήμης
  - ExecShield (Red Hat)
  - W^X (OpenBSD)
- Κατά τη μεταγλώττιση (gcc)
  - `gcc -D_FORTIFY_SOURCE=2 -O2`: ανίχνευση (απλών) σφαλμάτων υπερχείλισης μνήμης
  - `gcc -Wformat=2`: έλεγχος προσδιοριστών μορφής
  - `gcc -fstack-protector`: προστασία δεδομένων της στοίβας

Ασφάλεια δικτύων

Επίπεδο δικτύου

- Αναχώματα ασφάλειας (firewalls) επιπέδου δικτύου
- Φιλτράρισμα IP πακέτων από την επικεφαλίδα τους για την υλοποίηση της πολιτικής ασφάλειας
- Καταστασιακή λειτουργία (stateful): εξελισσόμενη εσωτερική βάση προηγούμενων πακέτων για κάθε επικοινωνία
- Μη καταστασιακή λειτουργία (stateless): κάθε πακέτο εξετάζεται απομονωμένα
- netfilter/iptables (σύντομα nftables): μέρος του πυρήνα (Linux), βιβλιοθήκη για ανάπτυξη προσαρμοσμένων εφαρμογών (libnetfilter)
- ipfw ή ipfirewall: FreeBSD, Mac OS X και υποστήριξη για Windows (wipfw)
- pf ή packet filter: OpenBSD, FreeBSD, NetBSD, Core Force (Windows)

Επίπεδο εφαρμογής

- Αναχώματα ασφάλειας (firewalls) επιπέδου εφαρμογής
- Διεξοδικός έλεγχος των περιεχομένων των πακέτων στο επίπεδο εφαρμογής (π.χ. HTTP, telnet, FTP, ...)
  - Υλοποίηση σύνθετων πολιτικών ασφάλειας
- Ουσιαστικά λειτουργούν ως εκπρόσωποι/πληρεξούσιοι της εφαρμογής πελάτη εξασφαλίζοντας τη συμμόρφωσή του στην πολιτική ασφάλειας
- Firewall Toolkit (FWTK, 1993): ανοικτό με στόχο τη βελτίωση του λογισμικού αναχωμάτων (χρηματοδότηση από το DARPA)
- Zorp: Python για τον ορισμό σύνθετων κανόνων, πολλά πρωτόκολλα (HTTP, FTP, SSL, telnet, whois, ...), άδεια χρήσης GPL
- ModSecurity, WebKnight: εξειδικευμένες λύσεις για προστασία εφαρμογών ιστού

Συστήματα ανίχνευσης εισβολών/επιθέσεων

- Αυτόματοι μηχανισμοί ελεγκτικής παρακολούθησης (auditing)
  - Αντιπρόσωπος: συλλογή πληροφοριών από τη δικτυακή κίνηση ή από το ιστορικό ενός Η/Υ
  - Αναλυτής: ανίχνευση επιθέσεων
  - Αγγελιοφόρος: ειδοποίηση του διαχειριστή, λήψη αντιμέτρων
- OSSEC: ανάλυση αρχείων καταγραφής ιστορικού (iptables, OpenSSH, Samba, sendmail, Postfix, Apache, MySQL, PostgreSQL, MS IIS, ...), κεντρική διαχείριση
- Snort: ανάλυση δικτυακής κίνησης, ανίχνευση επιθέσεων μέσω των γνωστών χαρακτηριστικών τους, δυνατότητα λήψης αντιμέτρων (π.χ. σταματώντας πακέτα)
- Prelude: συλλογή πληροφοριών, συσχέτιση, αντιστοίχιση, συμβατό με σχεδόν όλα τα ΕΛ/ΛΑΚ συστήματα ανίχνευσης

Κυβερνοπόλεμος

Ορισμός κυβερνοπολέμου

- Εκτεταμένες ζημίες και όχι απλή αναστάτωση/ενόχληση
- Επιθέσεις σε μονάδες υποδομής, π.χ. σε ηλεκτροπαραγωγικούς σταθμούς
- Οι στρατιωτικές δυνατότητες εξαρτώνται από τη σύμπραξη
  - διεργασιών στο πεδίο του κυβερνοχώρου, και
  - υλικού εξοπλισμού στο κινητικό πεδίο
- Συνεπώς στρατιωτικές δυνατότητες μπορούν να εξουδετερωθούν από επιθέσεις στο πεδίο του κυβερνοχώρου
- Δύο βασικοί προσδιορισμοί
  - Οι επιθέσεις διεξάγονται παράλληλα με συμβατικές πολεμικές επιχειρήσεις
  - Απροσδόκητες επιθέσεις σε μονάδες υποδομής μέσω του Διαδικτύου

Περιστατικά

- 2002-Σήμερα; Κίνα/Η.Π.Α. (Titan Rain)
  - Οργανωμένες επιθέσεις και παραβιάσεις (Lockheed Martin, NASA, Redstone Arsenal, ...)
- 2007 Αραβικές χώρες/Δανία
  - Η ομαλή λειτουργία της Διαδικτυακής υποδομής αποκαταστάθηκε μετά από δύο εβδομάδες
- 2007 Ρωσία/Εσθονία
  - Το δεύτερο μεγαλύτερο περιστατικό, επιθέσεις εναντίων οργανισμών, τραπεζών, υπουργείων, ...)
- 2008 Ρωσία/Γεωργία
  - Παρόμοιο μοντέλο με αυτό της Εσθονίας
- 2009 Β. Κορέα/Ν. Κορέα
  - Καταστροφή τηλεπικοινωνιακής υποδομής, διαγραφή δεδομένων από υπολογιστές συγκεκριμένων προσώπων

Ασύμμετρος ψηφιακός πόλεμος

- Στον παραδοσιακό πόλεμο μια χώρα πολεμά μία άλλη
- Στον ασύμμετρο ψηφιακό πόλεμο μερικοί άνθρωποι πολεμούν εναντίων μίας χώρας
- Κατανεμημένες επιθέσεις και δυνατότητα χρήσης της υποδομής του εχθρού για παραπέρα επιθέσεις
- Χαμηλό κόστος της απαραίτητης τεχνολογίας και τεχνογνωσίας
- Δυνατότητα άμεσης επαφής με τα υψηλότερα επίπεδα του κέντρου έλεγχου του εχθρού
- Πυρομαχικά: (άγνωστα) κενά ασφάλειας και προγράμματα εκμετάλλευσης για αυτά
- Αποτελεσματική άμυνα βασισμένη στα πλεονεκτήματα του ΕΛ/ΛΑΚ

Οπλοστάσιο ΕΛ/ΛΑΚ

- nmap: ανακάλυψη/συλλογή πληροφοριών για απομακρυσμένα συστήματα και δίκτυα
  - Ενεργές υπηρεσίες και τους αριθμούς έκδοσής τους
  - Τύπο και έκδοση λειτουργικού συστήματος
  - Χαρτογράφηση δικτυακής τοπολογίας
  - Δυνατότητες διαφυγής από συστήματα ανίχνευσης (π.χ. μέσω επιλογών χρονισμού)
  - Δυνατότητες επέκτασης χωρίς αλλαγή του πηγαίου κώδικα μέσω της γλώσσας Lua
- Nessus/OpenVAS: ανίχνευση γνωστών κενών ασφάλειας
  - Τρωτότητες λογισμικού, προεπιλεγμένα συνθηματικά, λάθη ρύθμισης
- Metasploit: πλατφόρμα ανάπτυξης και χρήσης προγραμμάτων εκμετάλλευσης τρωτοτήτων
  - Αυθαίρετο κώδικα (shellcode) για πλήθος συστημάτων/αρχιτεκτονικών και λειτουργιών

Συμπεράσματα

- Η σημασία της ψηφιακής ασφάλειας μεγαλώνει καθώς μεγαλώνει η εξάρτησή μας από τα ψηφιακά μέσα
- Ο κυβερνοπόλεμος είναι πραγματικότητα και έχει απτά αποτελέσματα
- Το ΕΛ/ΛΑΚ και οι πρακτικές ανάπτυξής του συμβάλλουν στην ασφάλεια
- Πλήθος από εργαλεία ασφάλειας ΕΛ/ΛΑΚ για κάθε ανάγκη και χρήση
- Απαραίτητος ο τακτικός έλεγχος της ασφάλειας από τρίτους
  - Δικτυακής υποδομής, εφαρμογών (πηγαίου κώδικα), πολιτικών ασφάλειας

Παραπομπές

John Micklethwait, editor

Marching off to cyberwar

The Economist, December 2008

Raphael S. Mudge and Scott Lingley

Cyber and air joint effects demonstration

U.S. Air Force Research Laboratory, August 2007

Johnny Ryan

iWar: A new threat, its convenience and our increasing vulnerability

NATO Review, winter 2007

Kevin Poulsen

Slammer worm crashed Ohio nuke plant network

www.securityfocus.com/news/6767, August 2003

Mark Dowd, John McDonald and Justin Schuh

The art of software security assessment

Addison-Wesley, 2006

Debian Wiki

Debian hardening options

http://wiki.debian.org/Hardening, 2009