KPMG
cutting through complexity

2ο Infocom Security

Η εξέλιξη και το μέλλον των επιθέσεων παρείσδυσης

5 Απριλίου 2012

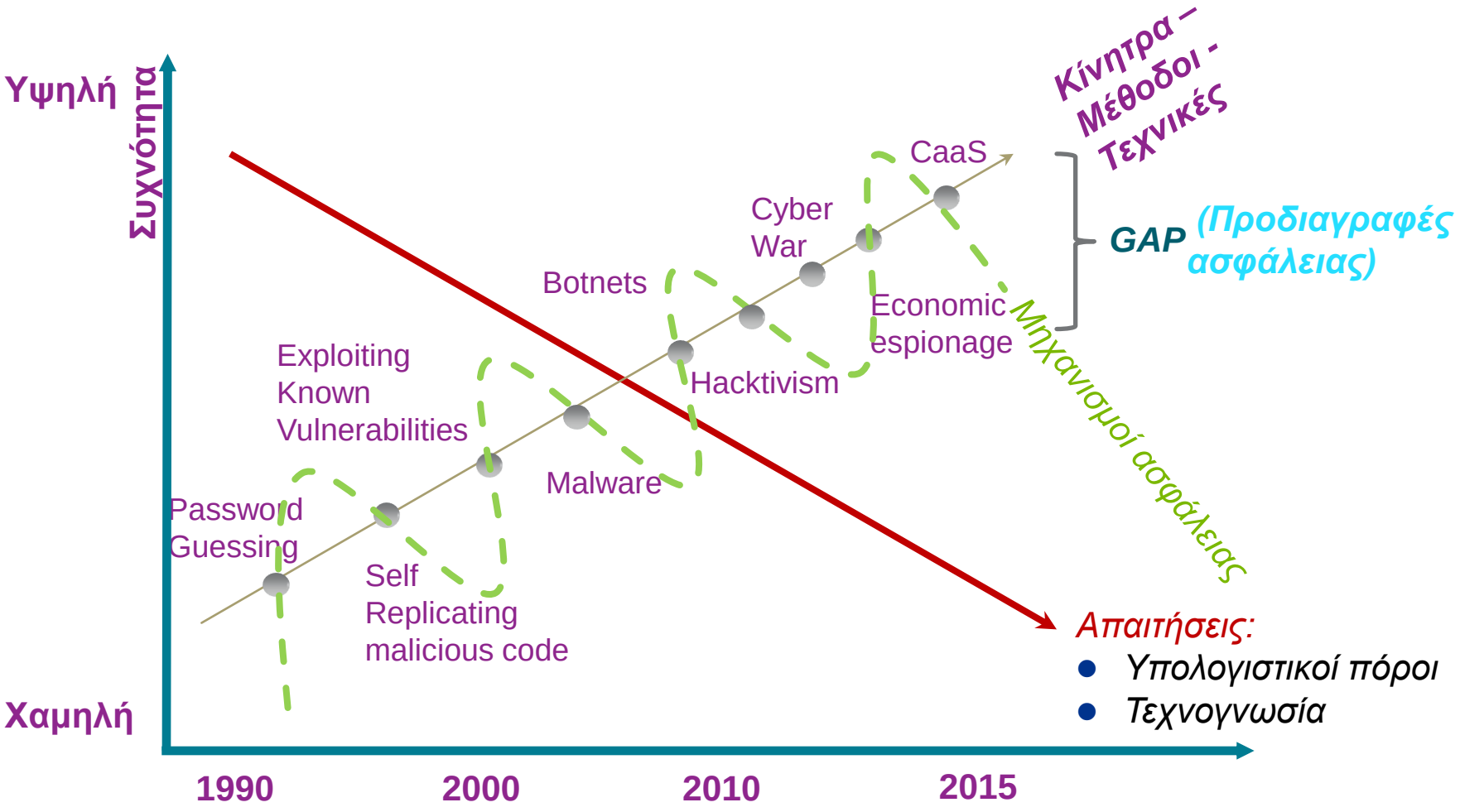
SC MAGAZINE AWARDS 2011 EUROPE WINNER

KPMG has been awarded with the Europe Awards 2011 as the information security consultancy of the year 2011 by SC Magazine

Η εξέλιξη και το μέλλον των επιθέσεων παρείσδυσης

© 2012 KPMG Σύμβουλοι ΑΕ, Ελληνική Ανώνυμη Εταιρεία και μέλος του δικτύου ανεξάρτητων εταιρειών-μελών της KPMG συνδεδεμένων με την KPMG International Cooperative ('KPMG International'), ενός Ελβετικού νομικού προσώπου. Όλα τα δικαιώματα κατοχυρωμένα.

Η εξέλιξη και το μέλλον των επιθέσεων παρείσδυσης



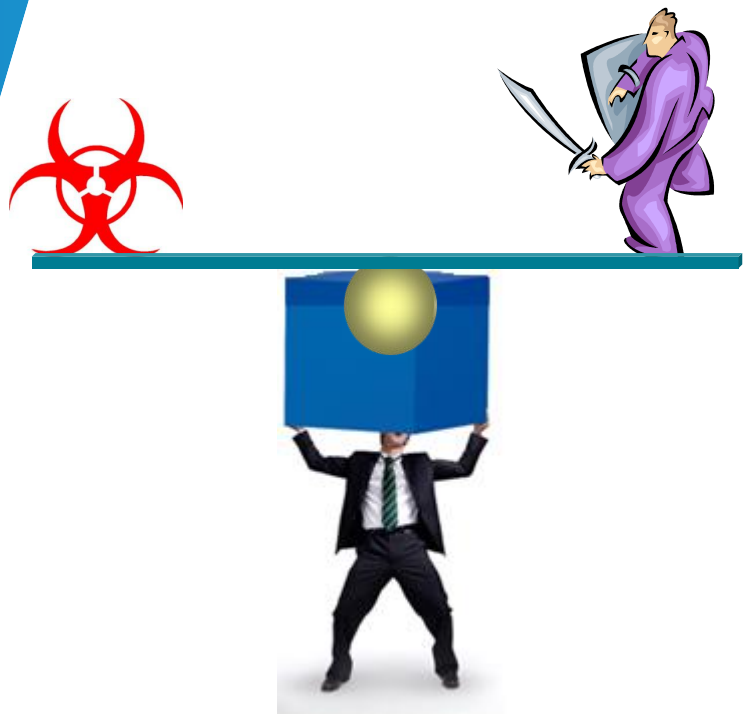
© 2012 KPMG Σύμβουλοι ΑΕ, Ελληνική Ανώνυμη Εταιρεία και μέλος του δικτύου ανεξάρτητων εταιρειών-μελών της KPMG συνδεδεμένων με την KPMG International Cooperative ('KPMG International'), ενός Ελβετικού νομικού προσώπου. Όλα τα δικαιώματα κατοχυρωμένα.

Περιεχόμενα

- Κίνητρα - Μέθοδοι - Τεχνικές
- Μηχανισμοί ασφάλειας

believe that the overall level of e-crime risk increased over the last 12 months

KPMG e-crime survey 2011



Κίνητρα (αντικειμενικοί σκοποί)

- ***Οικονομικό όφελος*** - Μη εξουσιοδοτημένες τηλεφωνικές κλήσεις [phone phreaking] (Kevin Mitnick 1998, Cyberia 2000, Dark Dante 2001)
- ***Προσωπική προβολή*** - Υποκλοπή εμπιστευτικών εταιρικών πληροφοριών (Kevin Mitnick 1990, HFM 2010)
- ***Στρατιωτική αποδυνάμωση μέσω άρνησης υπηρεσιών*** - Κυβερνο-στρατοί (Stuxnet 2009, NightDragon 2011)
- ***Οικονομικό όφελος*** - Υποκλοπή εμπιστευτικών πληροφοριών (cyber crime as a service) (Sony 2011)
- ***Προβολή κοινωνικής ατζέντας*** - Υποκλοπή απόρρητων πληροφοριών (Anonymous 2011)
- ***Προβολή κοινωνικής ατζέντας*** - Άρνηση υπηρεσιών (DOS) με σκοπό την προβολή κοινωνικής ατζέντας (GHS, Anonymous 2012)
- κ.α.

© 2012 KPMG Σύμβουλοι ΑΕ, Ελληνική Ανώνυμη Εταιρεία και μέλος του δικτύου ανεξάρτητων εταιρειών-μελών της KPMG συνδεδεμένων με την KPMG International Cooperative ('KPMG International'), ενός Ελβετικού νομικού προσώπου. Όλα τα δικαιώματα κατοχυρωμένα.

Cybercrime as a Service

- Πρόσβαση σε σταθμούς εργασίας (zombies)
- Δεδομένα προσωπικού χαρακτήρα (dubbed dumps)
- Εταιρικά εμπιστευτικά δεδομένα
- Χρήση εταιρικών πόρων (botnets)

Buy SpyEye binary with set-up and injections for $600
Buy Zeus recompile, 2 for $380
Buy customized $50 - $75
Buy for $5 each or $50 per month unlimited
One time license fee $250 + $10 for upgrades

RSA 2012 Cyber crime trends report

- Μη κοινοποιημένες αδυναμίες (zero-day exploits)
- Επιθέσεις άρνησης υπηρεσιών (DOS)

ADOBE READER	$5,000–$30,000
MAC OSX	$20,000–$50,000
ANDROID	$30,000–$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000–$100,000
MICROSOFT WORD	$50,000–$100,000
WINDOWS	$60,000–$120,000
FIREFOX OR SAFARI	$60,000–$150,000
CHROME OR INTERNET EXPLORER	$80,000–$200,000
IOS	$100,000–$250,000

Forbes Magazine, April 2011

© 2012 KPMG Σύμβουλοι ΑΕ, Ελληνική Ανώνυμη Εταιρεία και μέλος του δικτύου ανεξάρτητων εταιρειών-μελών της KPMG συνδεδεμένων με την KPMG International Cooperative ('KPMG International'), ενός Ελβετικού νομικού προσώπου. Όλα τα δικαιώματα κατοχυρωμένα.

Cybercrime as a Service (συν.)

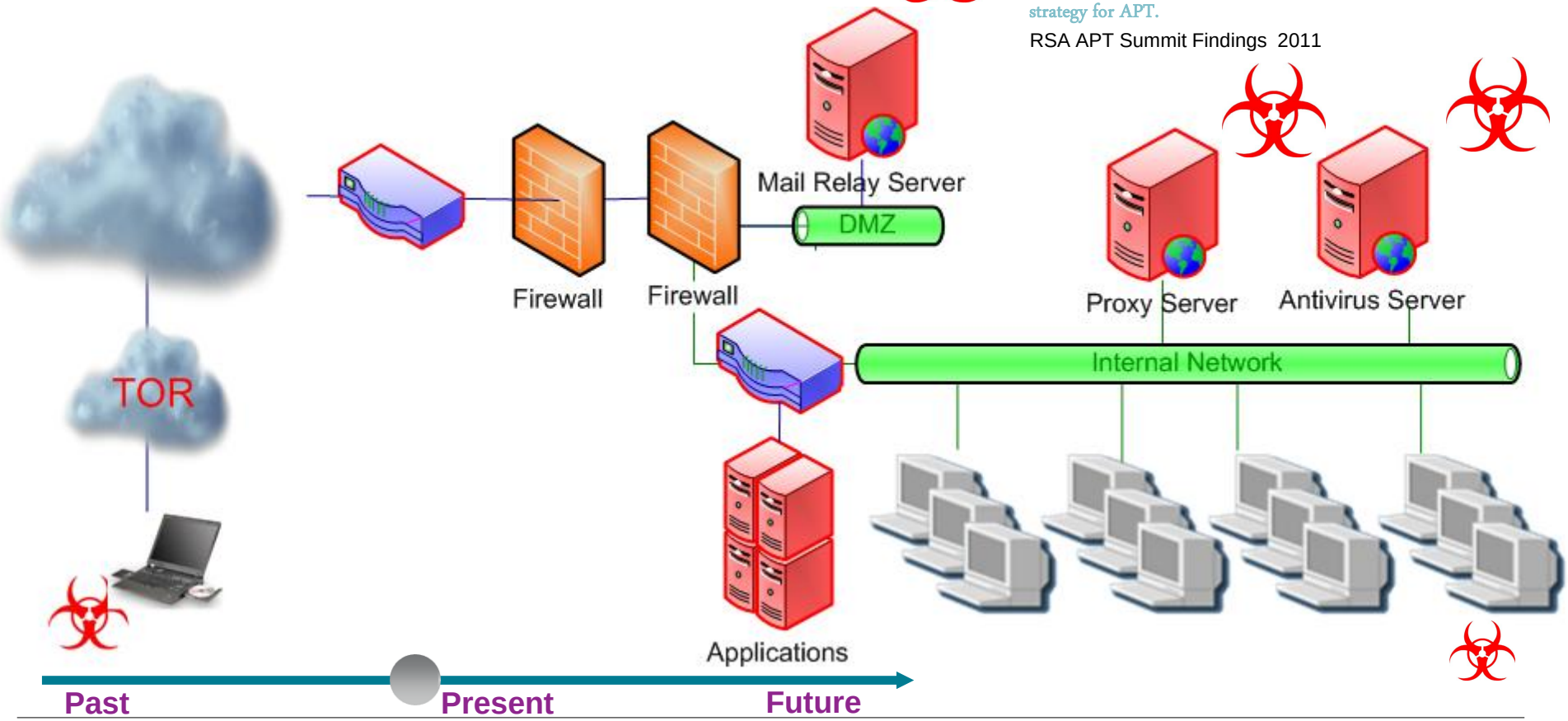
Client-side attack / Application Threat Persistent

- Αποστολή spear-phishing e-mail
- Εγκατάσταση κακόβουλου λογισμικού

54%

believe that their organization has not a threat management strategy for APT.

RSA APT Summit Findings 2011

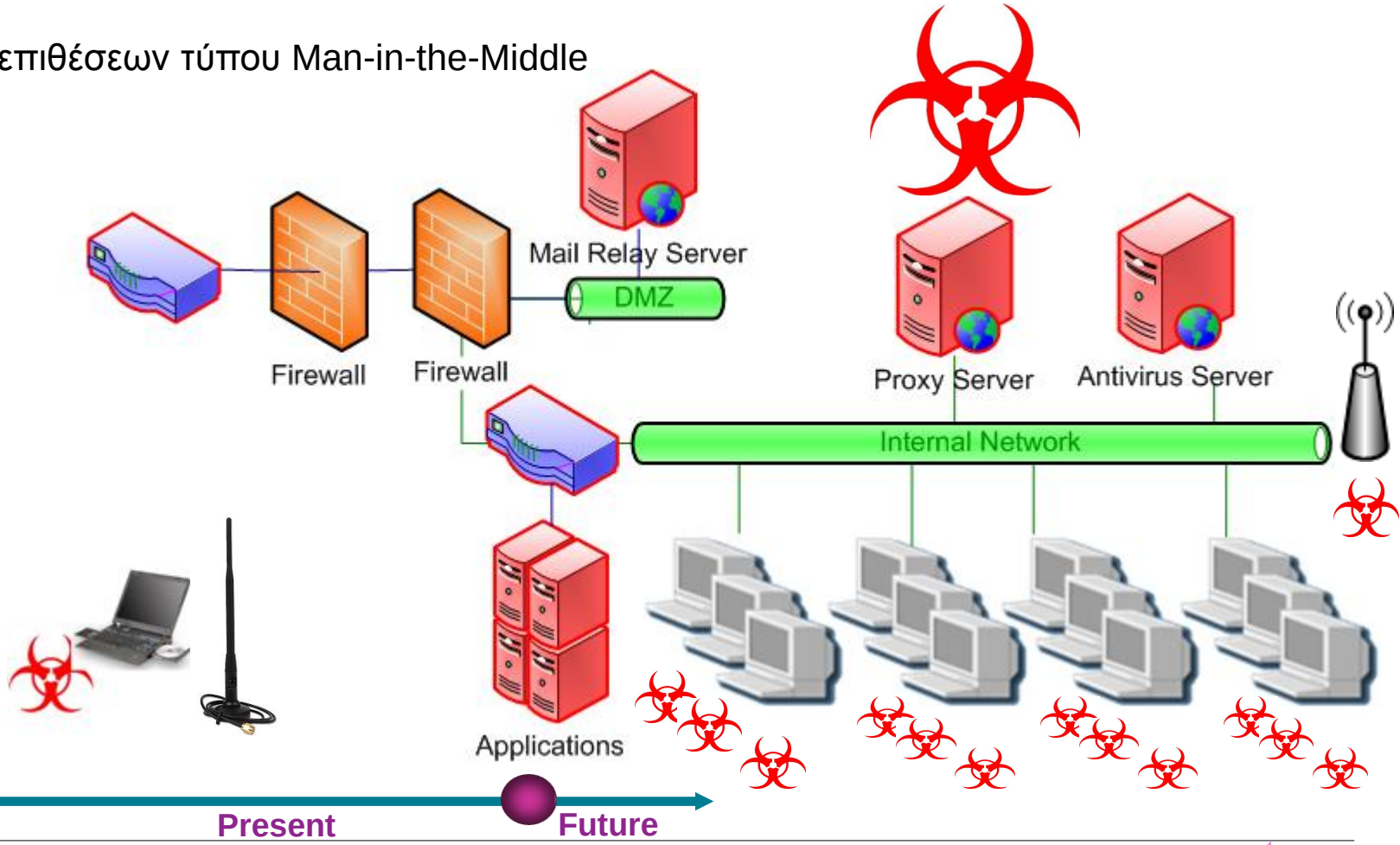


© 2012 KPMG Σύμβουλοι ΑΕ, Ελληνική Ανώνυμη Εταιρεία και μέλος του δικτύου ανεξάρτητων εταιρειών-μελών της KPMG συνδεδεμένων με την KPMG International Cooperative ('KPMG International'), ενός Ελβετικού νομικού προσώπου. Όλα τα δικαιώματα κατοχυρωμένα.

Cybercrime as a Service (συν.)

Client-side attack / Service Threat Persistent

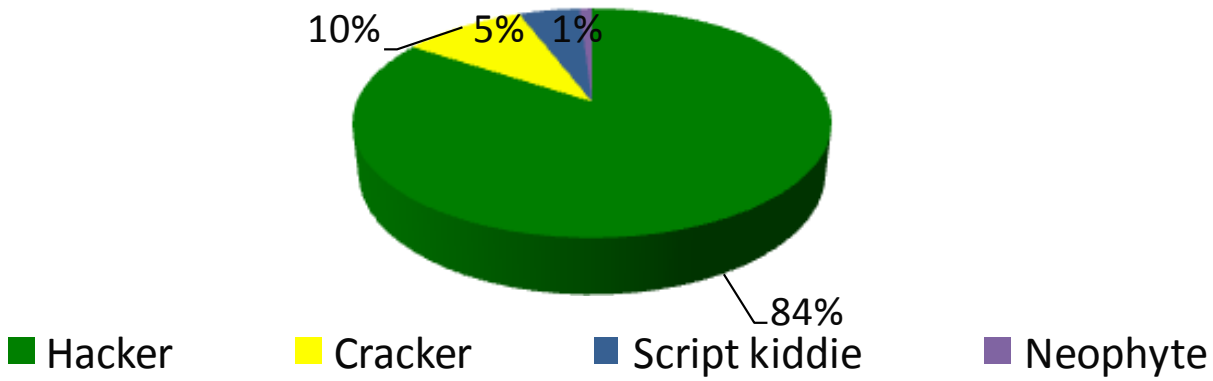
- Πρόσβαση στον ενδιάμεσο μεσολαβητή
- Εκτέλεση επιθέσεων τύπου Man-in-the-Middle



© 2012 KPMG Σύμβουλοι ΑΕ, Ελληνική Ανώνυμη Εταιρεία και μέλος του δικτύου ανεξάρτητων εταιρειών-μελών της KPMG συνδεδεμένων με την KPMG International Cooperative ('KPMG International'), ενός Ελβετικού νομικού προσώπου. Όλα τα δικαιώματα κατοχυρωμένα.

Μέθοδοι – Τεχνικές

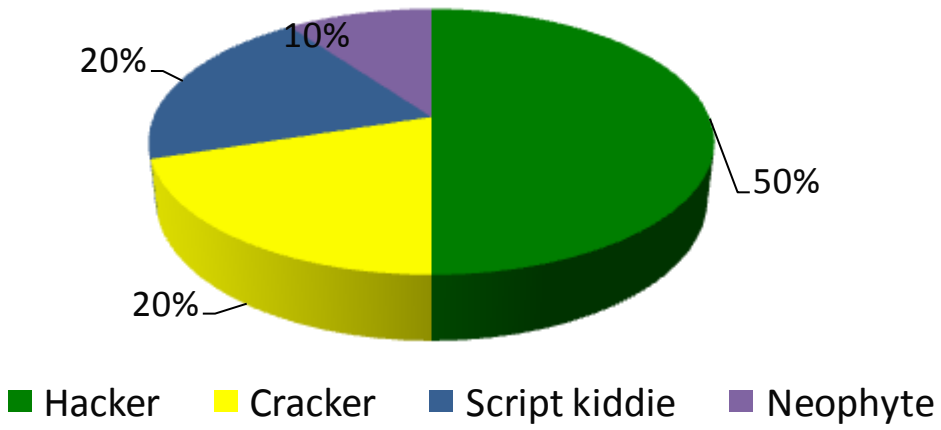
- Μη αυτοματοποιημένες τεχνικές
- Εκμετάλλευση τεχνολογικών αδυναμιών ασφάλειας (vulnerability identification and exploitation)
  - Προκαθορισμένοι, μη πολύπλοκοι κωδικοί πρόσβασης
  - Κενά ασφάλειας λόγω έλλειψης επικαιροποιημένου λογισμικού ασφάλειας
  - Μη συμμόρφωση με τις οδηγίες των προμηθευτών



© 2012 KPMG Σύμβουλοι ΑΕ, Ελληνική Ανώνυμη Εταιρεία και μέλος του δικτύου ανεξάρτητων εταιρειών-μελών της KPMG συνδεδεμένων με την KPMG International Cooperative ('KPMG International'), ενός Ελβετικού νομικού προσώπου. Όλα τα δικαιώματα κατοχυρωμένα.

Μέθοδοι – Τεχνικές (συν.)

- Αυτοματοποιημένες, με την χρήση εμπορικών εργαλείων και εργαλείων ανοικτού κώδικα
- Κοινωνική μηχανική (social engineering)
- Κατανεμημένες επιθέσεις άρνησης υπηρεσιών (DDOS)
- Σενάρια επίθεσης, αξιοποιώντας πολλαπλές τεχνολογικές αδυναμίες (attack scenarios)
- Σενάρια επίθεσης σε περιφερειακές συσκευές (BYOD)
- κ.α.



HOW DO BREACHES OCCUR?	
81%	utilized some form of hacking (+31%)
69%	incorporated malware (+20%)
10%	involved physical attacks (-19%)
7%	employed social tactics (-4%)
5%	resulted from privilege misuse (-12%)

Verizon 2012 Data breach investigations report

© 2012 KPMG Σύμβουλοι ΑΕ, Ελληνική Ανώνυμη Εταιρεία και μέλος του δικτύου ανεξάρτητων εταιρειών-μελών της KPMG συνδεδεμένων με την KPMG International Cooperative ('KPMG International'), ενός Ελβετικού νομικού προσώπου. Όλα τα δικαιώματα κατοχυρωμένα.

Κατανεμημένες επιθέσεις άρνησης υπηρεσιών

OSI	TCP /IP
Layer 7 Application	**Application** HTTP(S), Telnet, FTP
Layer 6 Presentation	**Session** e.g. RPC
Layer 5 Session	**Transport** Sockets/Steams - TLI
Layer 4 Transport	**TCP / UDP**
Layer 3 Network	**Network** IP + ARP/RA RP/ICMP
Layer 2 Data Link	**Physical Protocol** Ethernet/FDDI/PPP
Layer 1 Physical	**Transmission medium** Coax, Fiber, 10baseT..

Denial of Service Attacks

Vulnerabilities exploitation

Application flooding

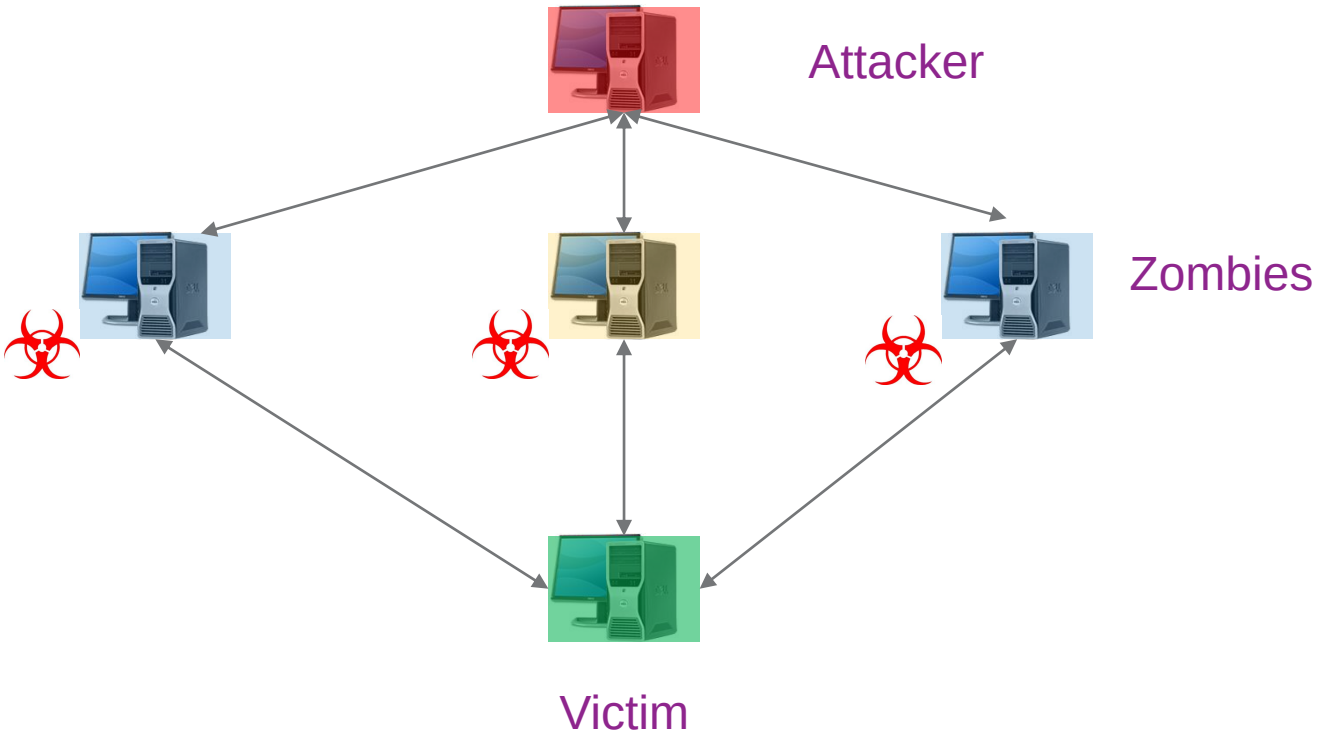
Network flooding

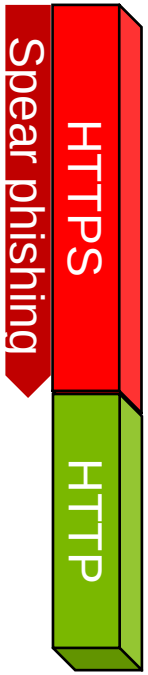
- Teardrop & smurf
- Ping of Death

Past **Present** **Future**

© 2012 KPMG Σύμβουλοι ΑΕ, Ελληνική Ανώνυμη Εταιρεία και μέλος του δικτύου ανεξάρτητων εταιρειών-μελών της KPMG συνδεδεμένων με την KPMG International Cooperative ('KPMG International'), ενός Ελβετικού νομικού προσώπου. Όλα τα δικαιώματα κατοχυρωμένα.

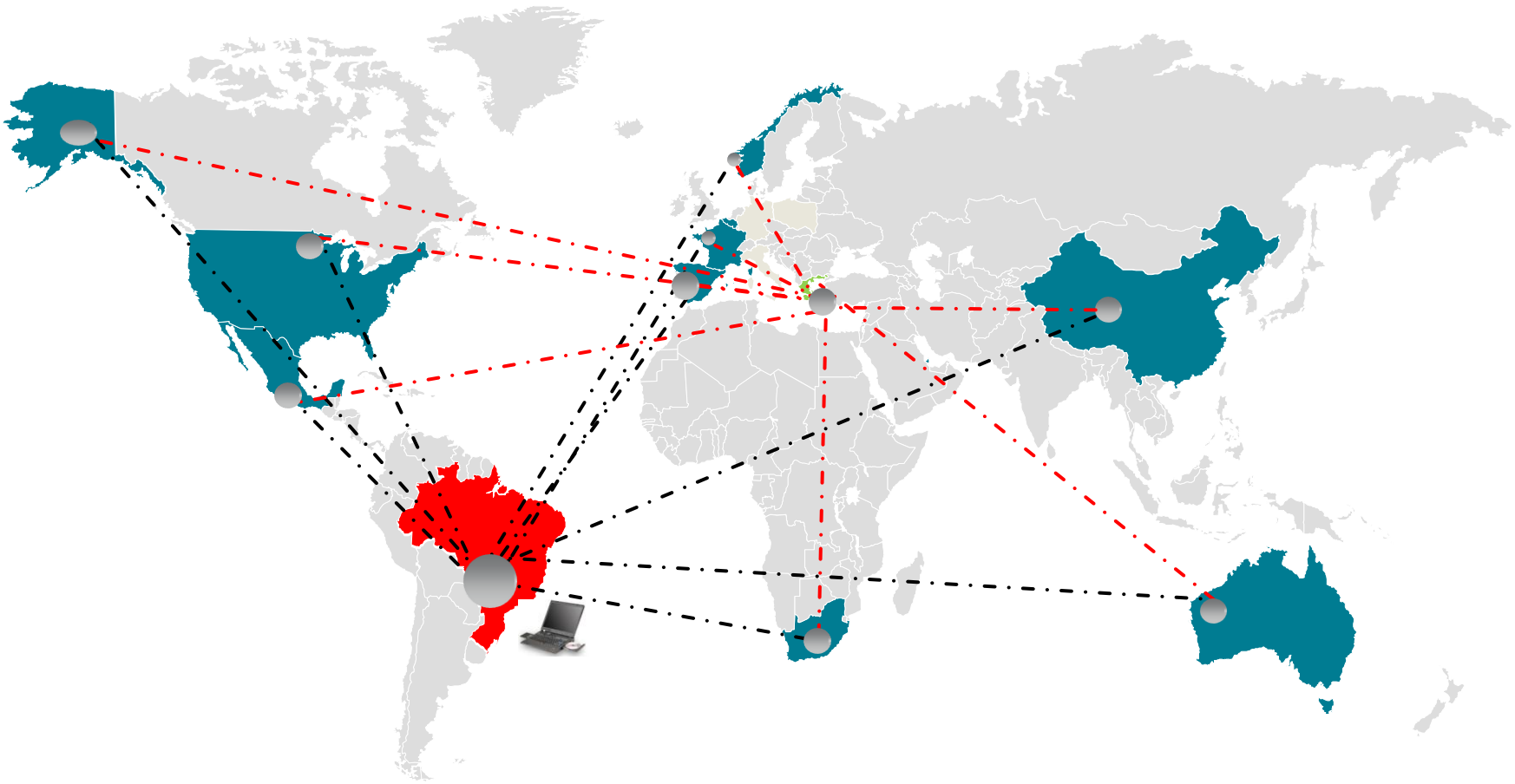
Κατανεμημένες επιθέσεις άρνησης υπηρεσιών (συν.)





© 2012 KPMG Σύμβουλοι ΑΕ, Ελληνική Ανώνυμη Εταιρεία και μέλος του δικτύου ανεξάρτητων εταιρειών-μελών της KPMG συνδεδεμένων με την KPMG International Cooperative ('KPMG International'), ενός Ελβετικού νομικού προσώπου. Όλα τα δικαιώματα κατοχυρωμένα.

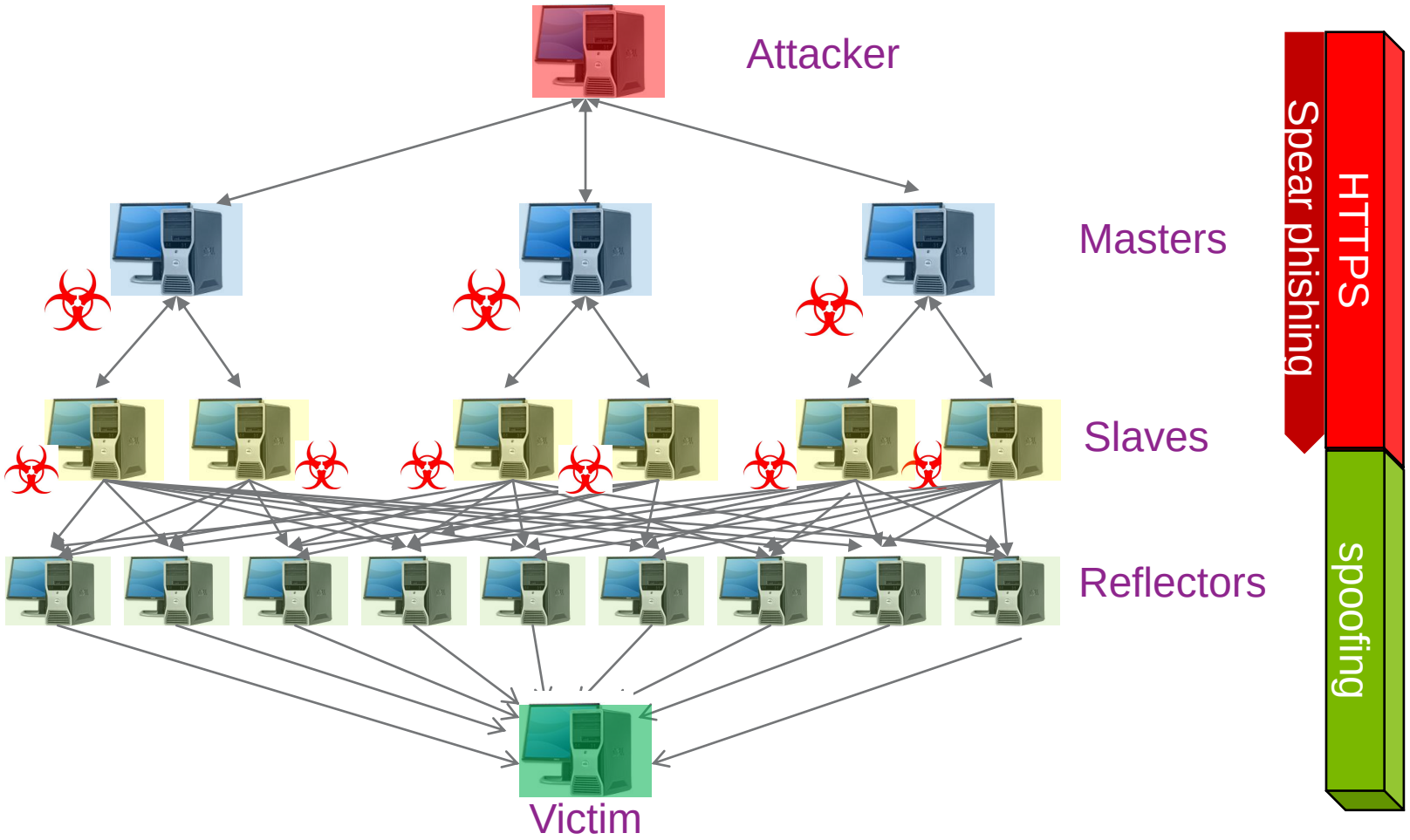
Κατανεμημένες επιθέσεις άρνησης υπηρεσιών (συν.)



Past Present Future

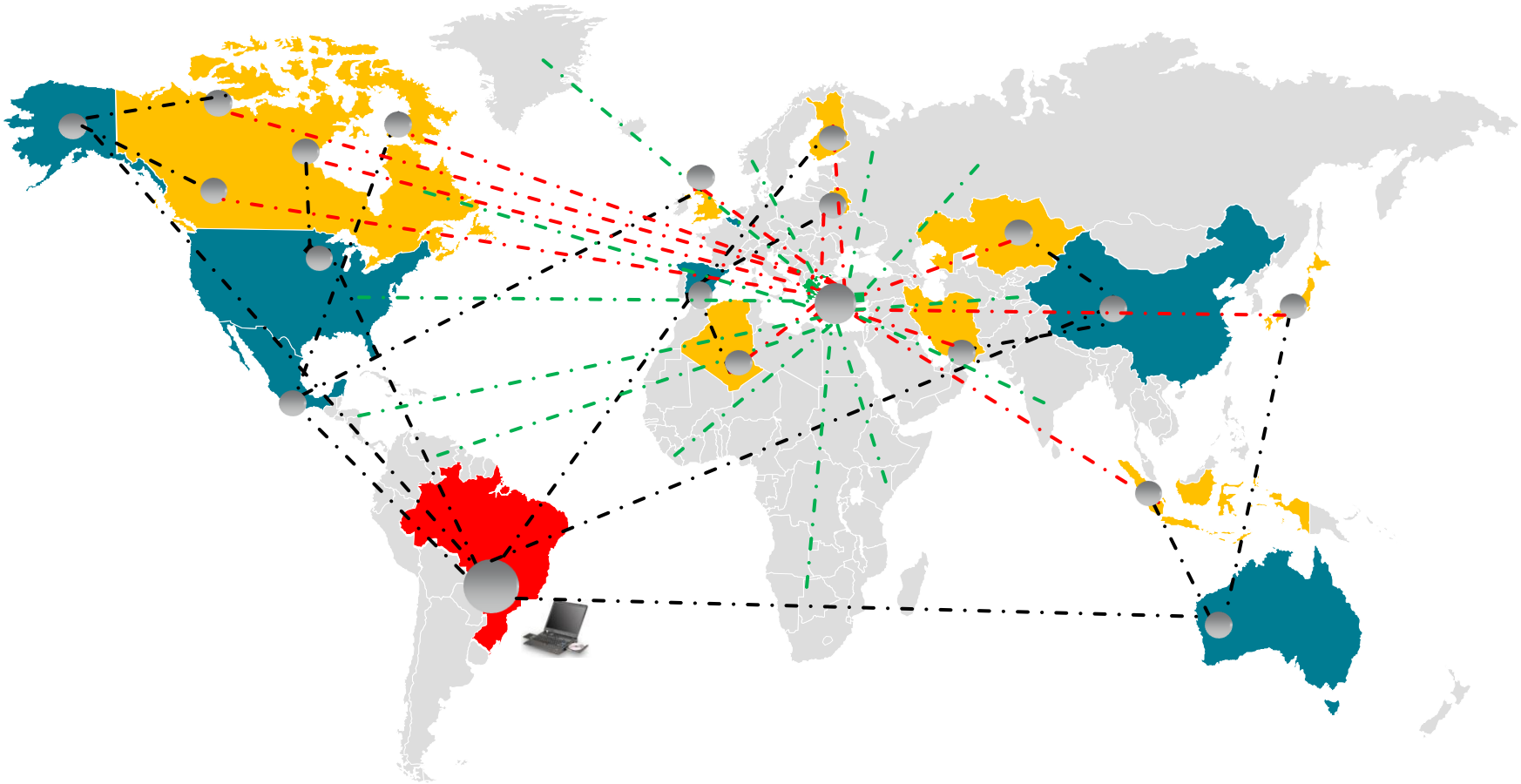
© 2012 KPMG Σύμβουλοι ΑΕ, Ελληνική Ανώνυμη Εταιρεία και μέλος του δικτύου ανεξάρτητων εταιρειών-μελών της KPMG συνδεδεμένων με την KPMG International Cooperative ('KPMG International'), ενός Ελβετικού νομικού προσώπου. Όλα τα δικαιώματα κατοχυρωμένα.

Κατανεμημένες επιθέσεις άρνησης υπηρεσιών (συν.)



© 2012 KPMG Σύμβουλοι ΑΕ, Ελληνική Ανώνυμη Εταιρεία και μέλος του δικτύου ανεξάρτητων εταιρειών-μελών της KPMG συνδεδεμένων με την KPMG International Cooperative ('KPMG International'), ενός Ελβετικού νομικού προσώπου. Όλα τα δικαιώματα κατοχυρωμένα.

Κατανεμημένες επιθέσεις άρνησης υπηρεσιών (συν.)

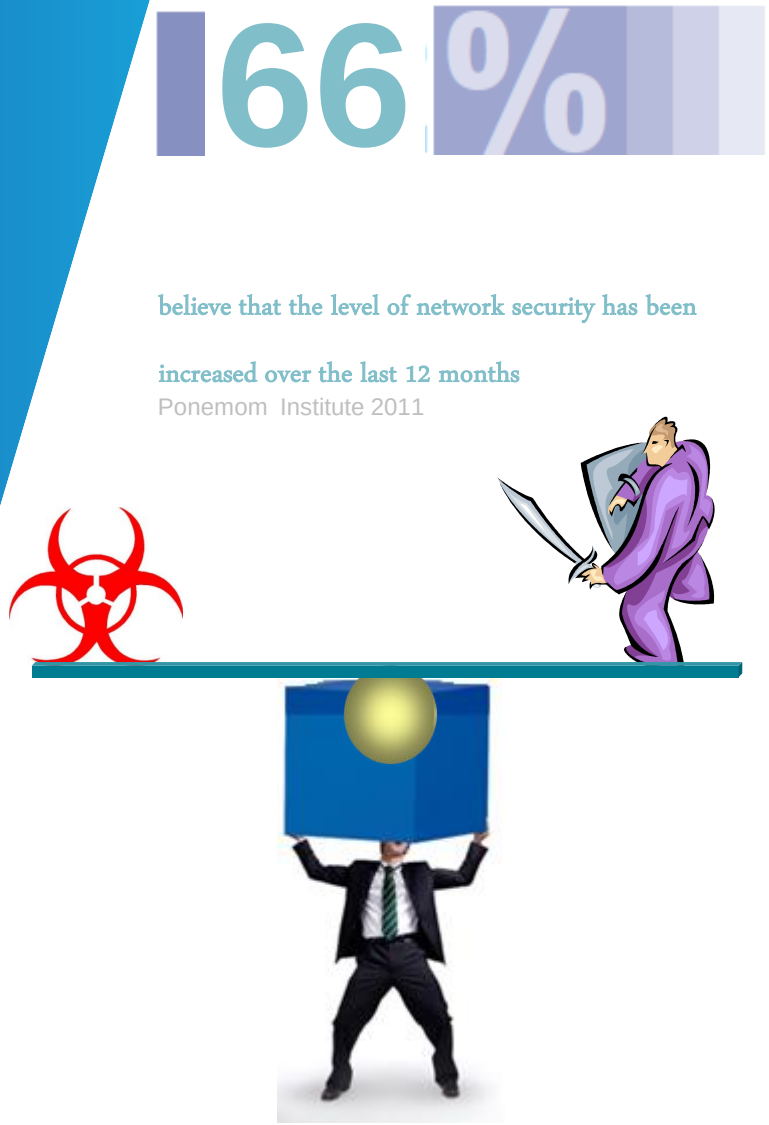


Past Present Future

© 2012 KPMG Σύμβουλοι ΑΕ, Ελληνική Ανώνυμη Εταιρεία και μέλος του δικτύου ανεξάρτητων εταιρειών-μελών της KPMG συνδεδεμένων με την KPMG International Cooperative ('KPMG International'), ενός Ελβετικού νομικού προσώπου. Όλα τα δικαιώματα κατοχυρωμένα.

Περιεχόμενα

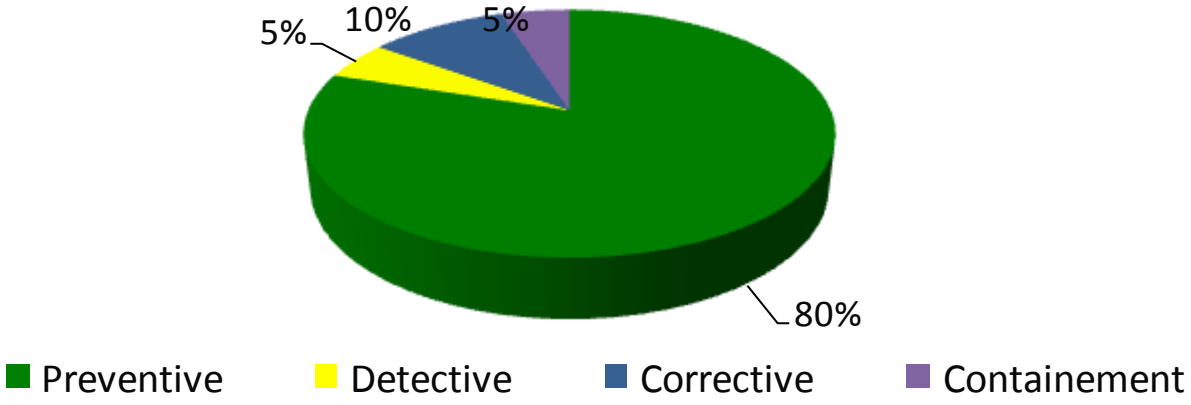
- Κίνητρα - Μέθοδοι - Τεχνικές
- Μηχανισμοί ασφάλειας



Μηχανισμοί ασφάλειας

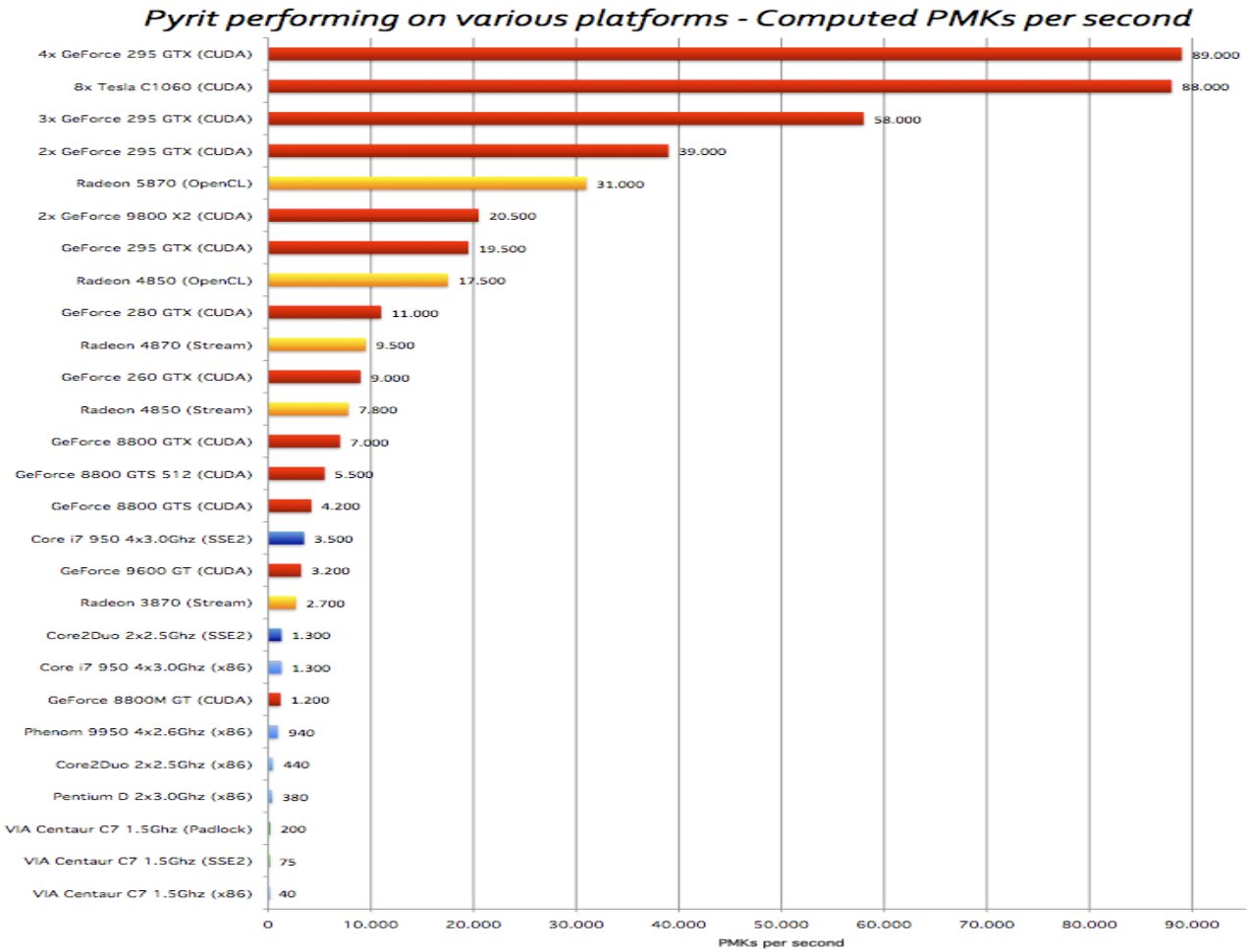
Productivity first, security later

- Τεχνολογικοί (π.χ. τοίχοι προστασίας, ιομορφικό λογισμικό, κωδικοί πρόσβασης, κτλ)
- Εφαρμογή των τεχνικών προδιαγραφών ασφάλειας των προμηθευτών
- Εκτέλεση τεχνικών ανίχνευσης τεχνολογικών αδυναμιών (vulnerability scanning)
- Αποδοχή κινδύνων *unknown – unknown / highly unlikely*



© 2012 KPMG Σύμβουλοι ΑΕ, Ελληνική Ανώνυμη Εταιρεία και μέλος του δικτύου ανεξάρτητων εταιρειών-μελών της KPMG συνδεδεμένων με την KPMG International Cooperative ('KPMG International'), ενός Ελβετικού νομικού προσώπου. Όλα τα δικαιώματα κατοχυρωμένα.

Υποκλοπή κωδικών πρόσβασης



2 billions passwords / sec

http://code.google.com/p/pyrit/

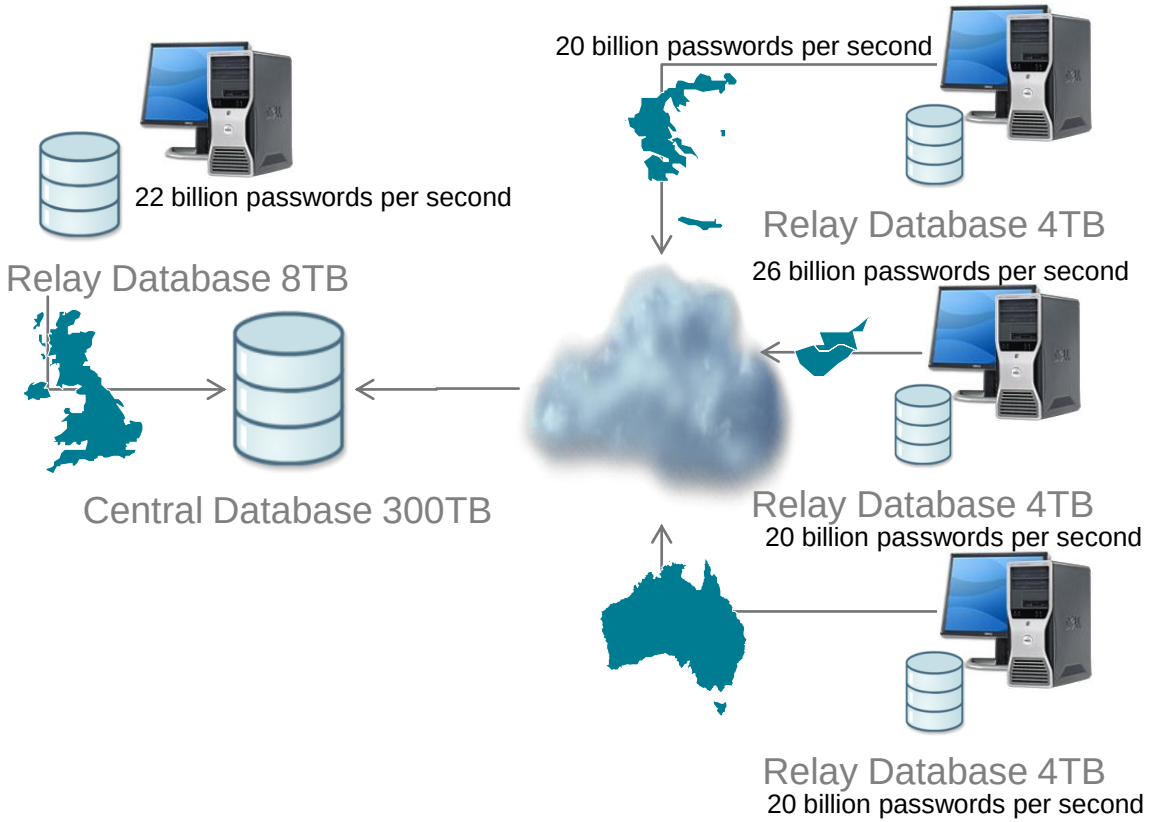
Past **Present** **Future**

© 2012 KPMG Σύμβουλοι ΑΕ, Ελληνική Ανώνυμη Εταιρεία και μέλος του δικτύου ανεξάρτητων εταιρειών-μελών της KPMG συνδεδεμένων με την KPMG International Cooperative ('KPMG International'), ενός Ελβετικού νομικού προσώπου. Όλα τα δικαιώματα κατοχυρωμένα.

Υποκλοπή κωδικών πρόσβασης (συν.)

Υποκλοπή πολύπλοκου κατακερματισμένου (NTLM) κωδικού 10 χαρακτήρων σε 24 ώρες

- 3 εργαστήρια ασφάλειας
- 32 κάρτες γραφικών
- 64 CPU Cores
- 320 TB αποθηκευτικός χώρος

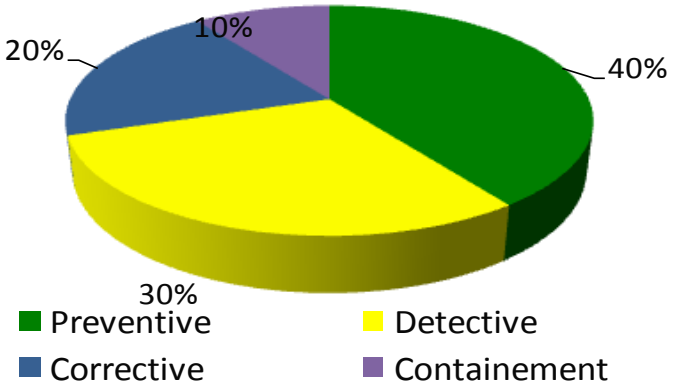


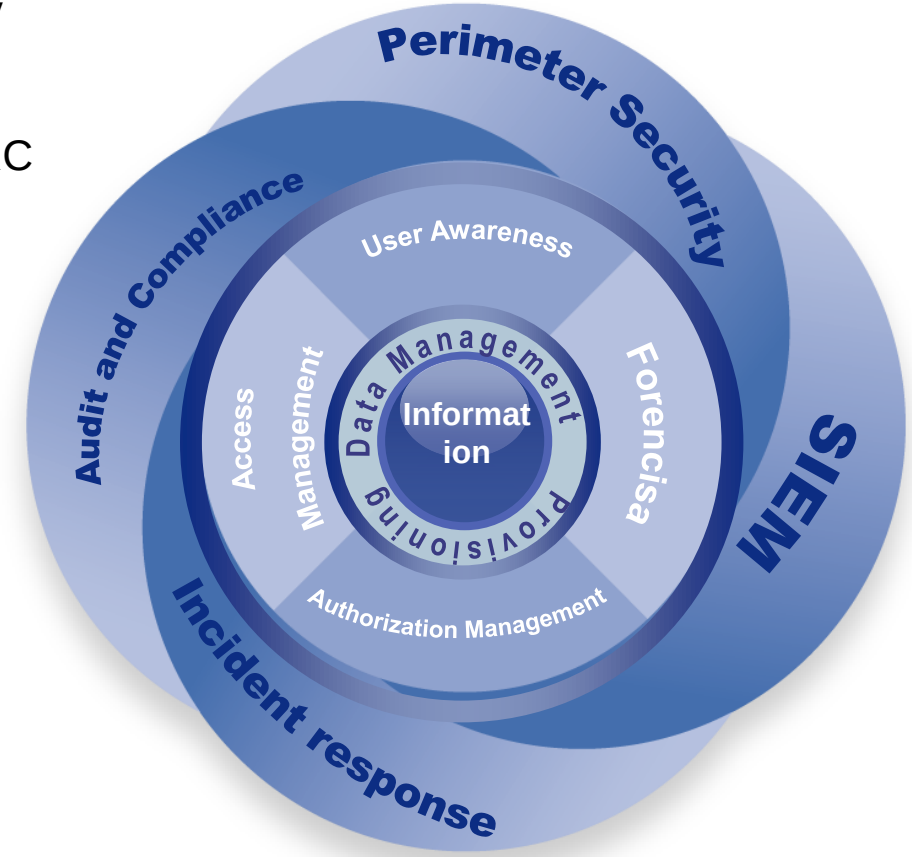
Past Present Future

© 2012 KPMG Σύμβουλοι ΑΕ, Ελληνική Ανώνυμη Εταιρεία και μέλος του δικτύου ανεξάρτητων εταιρειών-μελών της KPMG συνδεδεμένων με την KPMG International Cooperative ('KPMG International'), ενός Ελβετικού νομικού προσώπου. Όλα τα δικαιώματα κατοχυρωμένα.

Μηχανισμοί ασφάλειας (συν.)

- Υιοθέτηση κανονιστικών / θεσμικών πλαισίων ελέγχου
- Αυτοματοποιημένοι ελεγκτικοί μηχανισμοί GRC
- Βελτίωση των μηχανισμών ανίχνευσης επιθέσεων
- Βελτίωση των μηχανισμών περιορισμού πρόσβασης (least privilege)
- Εφαρμογή πολλαπλών επιπέδων ασφάλειας (defense in depth)





© 2012 KPMG Σύμβουλοι ΑΕ, Ελληνική Ανώνυμη Εταιρεία και μέλος του δικτύου ανεξάρτητων εταιρειών-μελών της KPMG συνδεδεμένων με την KPMG International Cooperative ('KPMG International'), ενός Ελβετικού νομικού προσώπου. Όλα τα δικαιώματα κατοχυρωμένα.

Μηχανισμοί ασφάλειας (συν.)

Measure security

- Αναδοχή ασφάλειας με γνώμονα την απόδοση (SROI)
- Ποσοτικοποίηση των κινδύνων (KRIs) και των μηχανισμών ασφάλειας (KCIs)
- Έλεγχοι πληροφοριακών συστημάτων Risk based / Proof-Of-Concept

Act Globally

- Εφαρμογή παγκόσμιου πλαισίου συνεργασίας (Europol, FBI, Interpol, NATO, EU CERT)
- Ανάθεση κεντρικής διαχείρισης μηχανισμών ασφάλειας σε τρίτους (consolidated SaaS)
- Πιστοποίηση ασφάλειας εφαρμογών από εξωτερικούς φορείς (attestation)

© 2012 KPMG Σύμβουλοι ΑΕ, Ελληνική Ανώνυμη Εταιρεία και μέλος του δικτύου ανεξάρτητων εταιρειών-μελών της KPMG συνδεδεμένων με την KPMG International Cooperative ('KPMG International'), ενός Ελβετικού νομικού προσώπου. Όλα τα δικαιώματα κατοχυρωμένα.

Μηχανισμοί ασφάλειας (συν.)

Operationalize security

- Ολιστική διαχείριση κινδύνων πληροφοριών
- Ενσωμάτωση μηχανισμών ασφάλειας στις καθημερινές διαδικασίες / λειτουργίες
- Υιοθέτηση κουλτούρας “hacker”

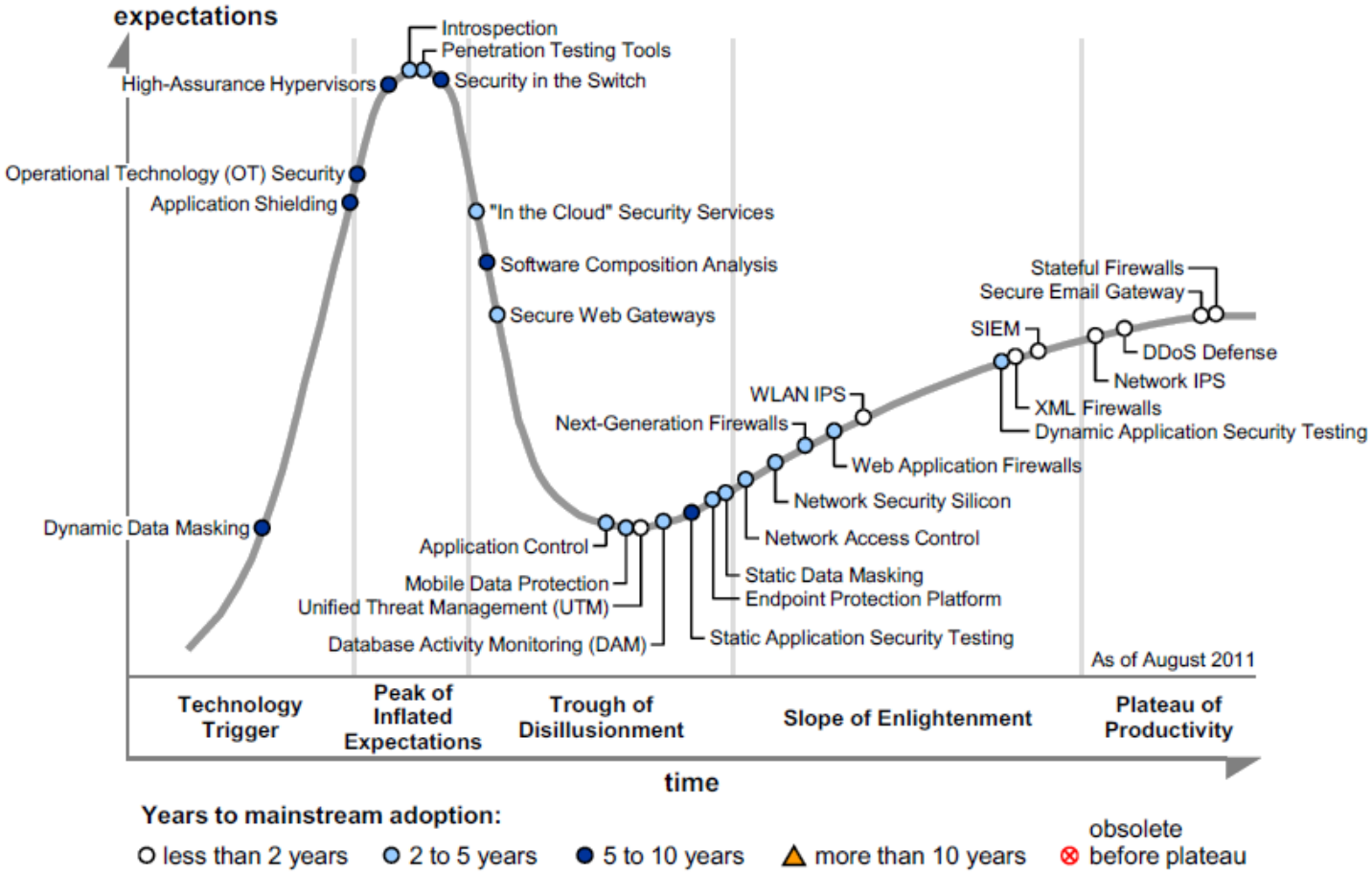
Act as though you’re already hacked

- Υιοθέτηση μηχανισμών περιορισμού επιπτώσεων
- Υιοθέτηση ισχυρών μηχανισμών πιστοποίησης (two-factor authentication) και κρυπτογράφησης
- Βελτίωση των μη-περιμετρικών μηχανισμών ασφάλειας

© 2012 KPMG Σύμβουλοι ΑΕ, Ελληνική Ανώνυμη Εταιρεία και μέλος του δικτύου ανεξάρτητων εταιρειών-μελών της KPMG συνδεδεμένων με την KPMG International Cooperative (‘KPMG International’), ενός Ελβετικού νομικού προσώπου. Όλα τα δικαιώματα κατοχυρωμένα.

Μηχανισμοί ασφάλειας (συν.)

Figure 1. Hype Cycle for Infrastructure Protection, 2011

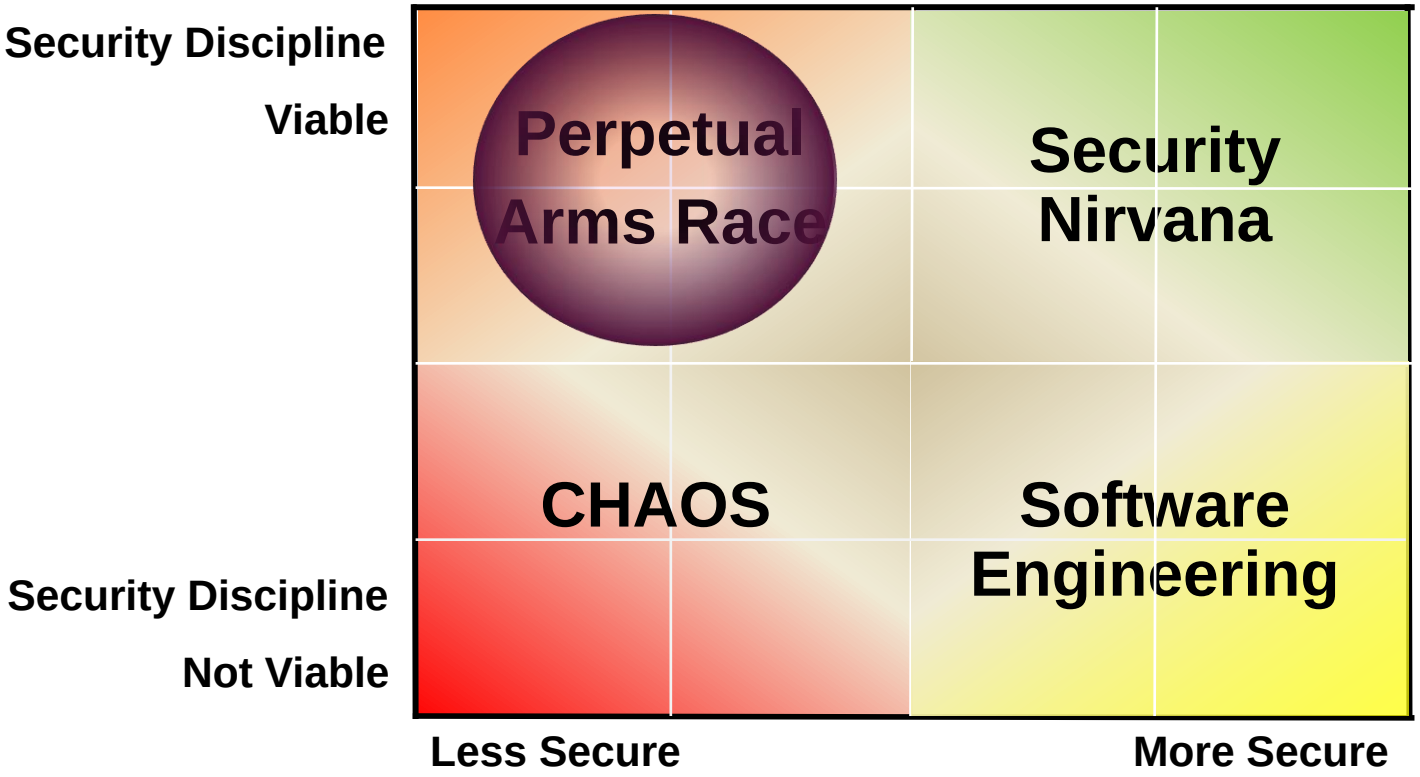


Source: Gartner (August 2011)

Past Present Future

© 2012 KPMG Σύμβουλοι ΑΕ, Ελληνική Ανώνυμη Εταιρεία και μέλος του δικτύου ανεξάρτητων εταιρειών-μελών της KPMG συνδεδεμένων με την KPMG International Cooperative ('KPMG International'), ενός Ελβετικού νομικού προσώπου. Όλα τα δικαιώματα κατοχυρωμένα.

Η εξέλιξη και το μέλλον των επιθέσεων παρείσδυσης



Source: Gartner (May 2009) Security in 2013 and Beyond

© 2012 KPMG Σύμβουλοι ΑΕ, Ελληνική Ανώνυμη Εταιρεία και μέλος του δικτύου ανεξάρτητων εταιρειών-μελών της KPMG συνδεδεμένων με την KPMG International Cooperative ('KPMG International'), ενός Ελβετικού νομικού προσώπου. Όλα τα δικαιώματα κατοχυρωμένα.

Ερωτήσεις

Στοιχεία επικοινωνίας

Χρήστος Βιδάκης, CISA, CISM, CISSP, ISO 27001 LA
Διευθυντής
Risk Advisory Services
IT Advisory
Tel.: +30 210 60 62 100
Direct line: +30 210 60 62 228
cvidakis@kpmg.gr