Najboljša varnost na svetu
(ampak samo za IPv6!)

Jan Bervar

jan@nil.si

VITEL 2010

Najboljše prakse varne vpeljave IPv6 v poslovna okolja IT

- Ali so grožnje v omrežjih IPv6 drugačne kot grožnje v omrežjih IPv4?
- Kako drugačne so ranljivosti samega protokola IPv6 nasproti protokolu IPv4?
- Kako protokol IPv6 vpliva na ranljivosti ostalih delov informacijsko-komunikacijskih sistemov?

VITEL 2010

Najboljše prakse varne vpeljave IPv6 v poslovna okolja IT

- Vse najboljše visokonivojske (tehnološke in procesne) prakse varovanja ostajajo iste
- Naredite inventar kontrol IPv4 in jih prenesite v IPv6
- Dodajte kontrole, specifične za IPv6 (ND, RA, kontrola tunelov)
- Dobite občutek za IPv6
- Prepoznajte omejitve današnjih varnostnih kontrol v IPv6
- Imejte plan B – pri prevelikem tveganju na delih infrastrukture počakajte z migracijo

Ranljivosti IPv6

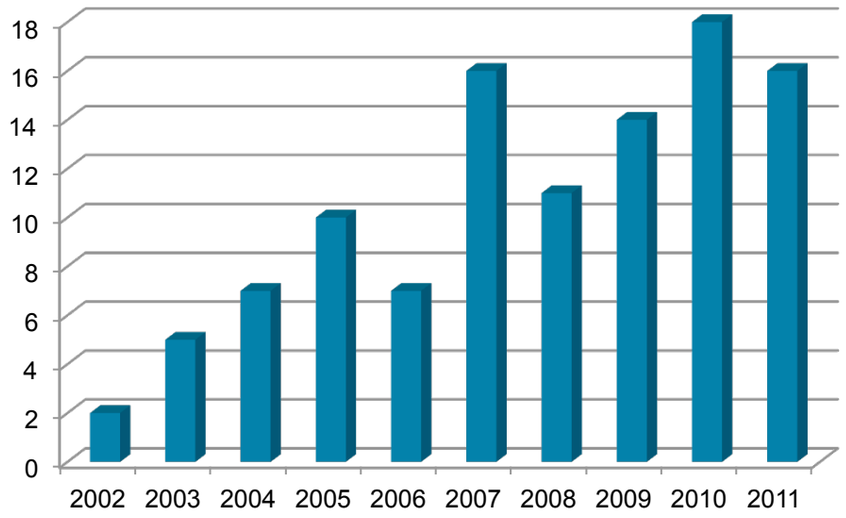
Nove stare ranljivosti

- Nepoznavanje tehnologije
- ND / RA / DHCPv6 napadi
- Izvorno usmerjanje
- Napadi na infrastrukturo (usmerjevalne protokol, kontrolno ravnino,…)
- **Implementacijske napake**

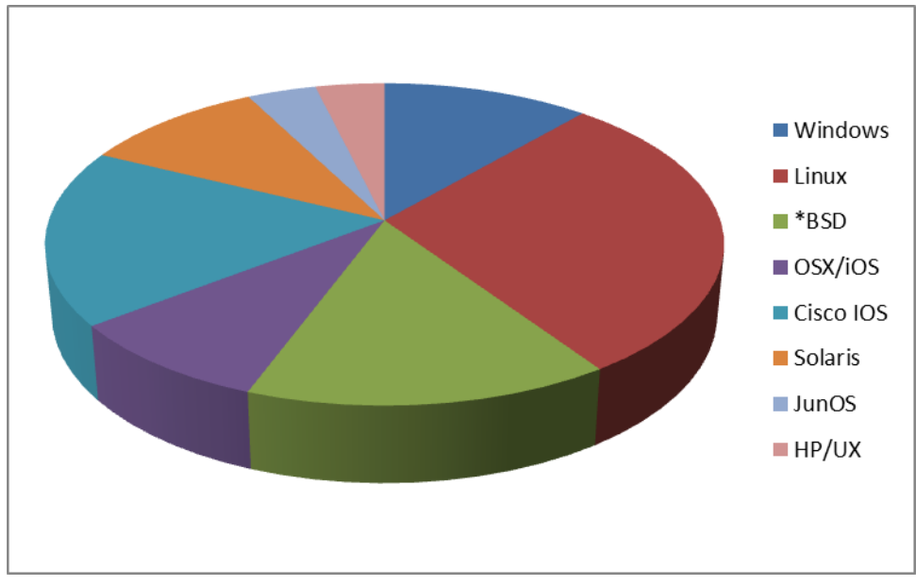
Nove ranljivosti

- Grožnje zasebnosti preko sledljivosti
- Nepričakovana povezljivost (tunelska in naravna!)

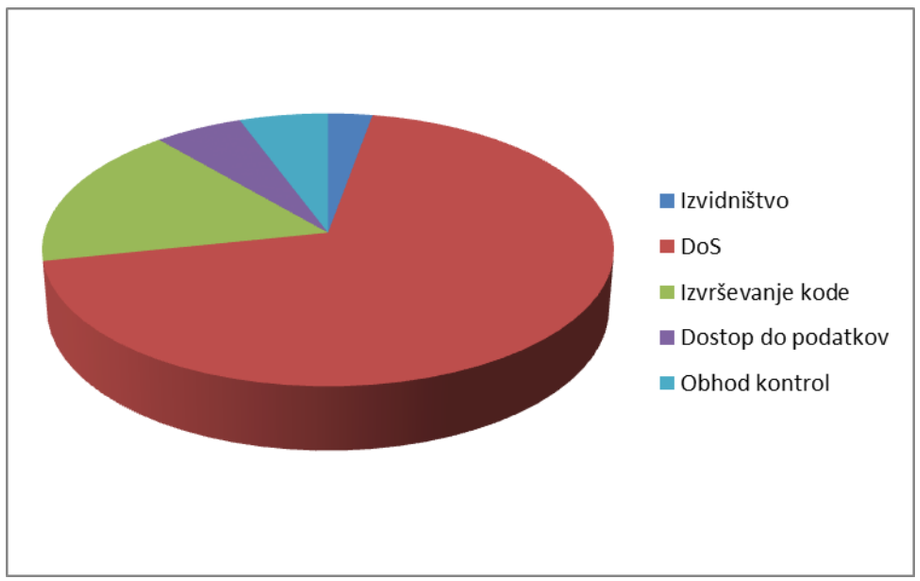
Implementacijske napake



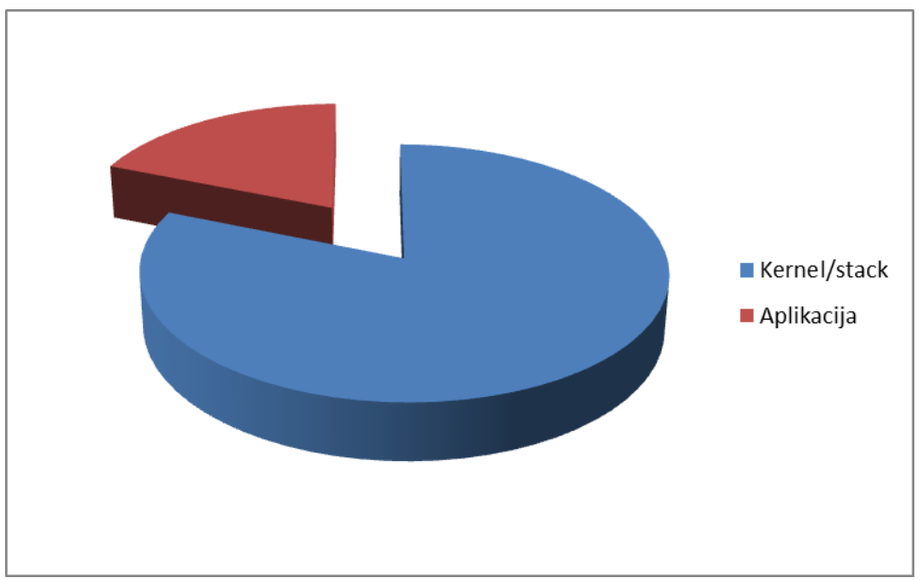
Število napak skozi leta



Napake glede na platformo

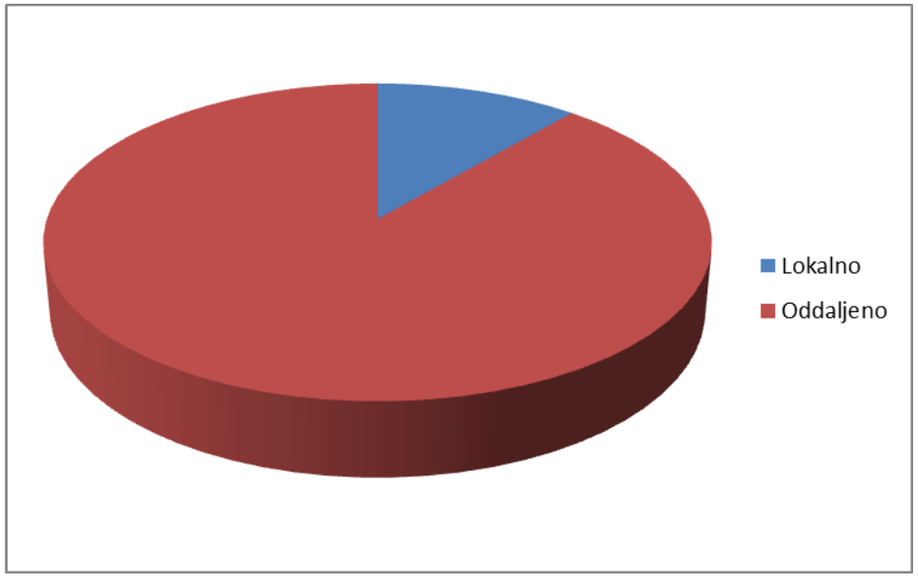


Napake glede na posledico

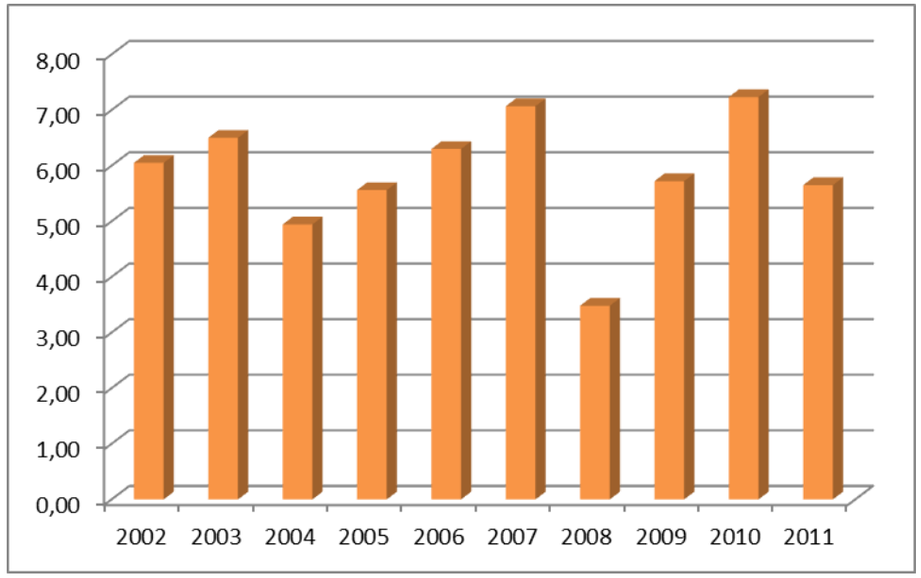


Napake glede na najdišče

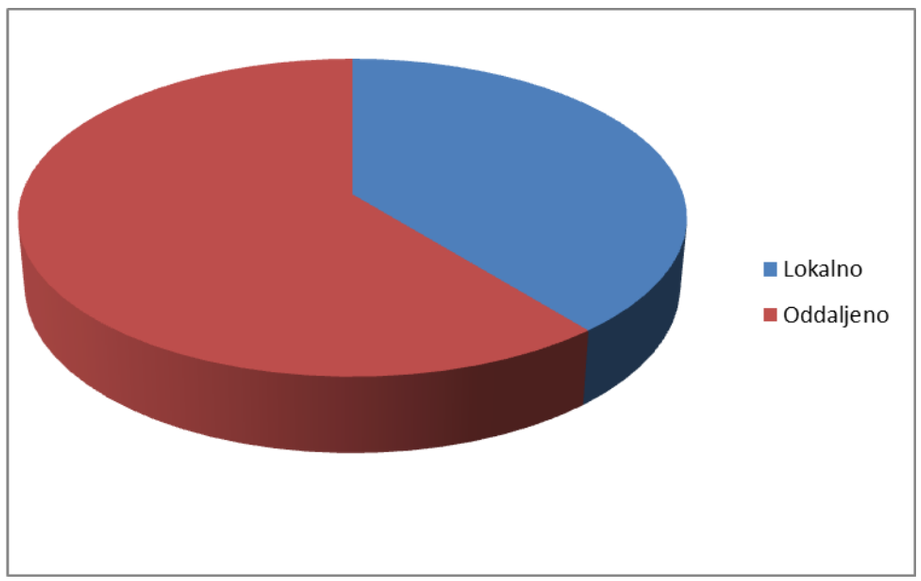
Implementacijske napake



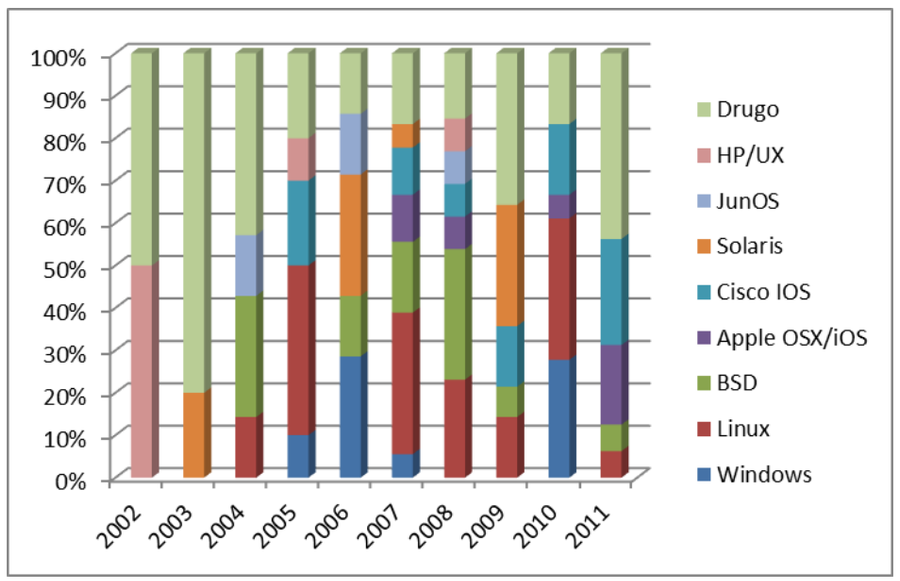
Napake glede na možnost napada



Povprečna resnost napak skozi leta



Napake glede na možnost napada (Linux)



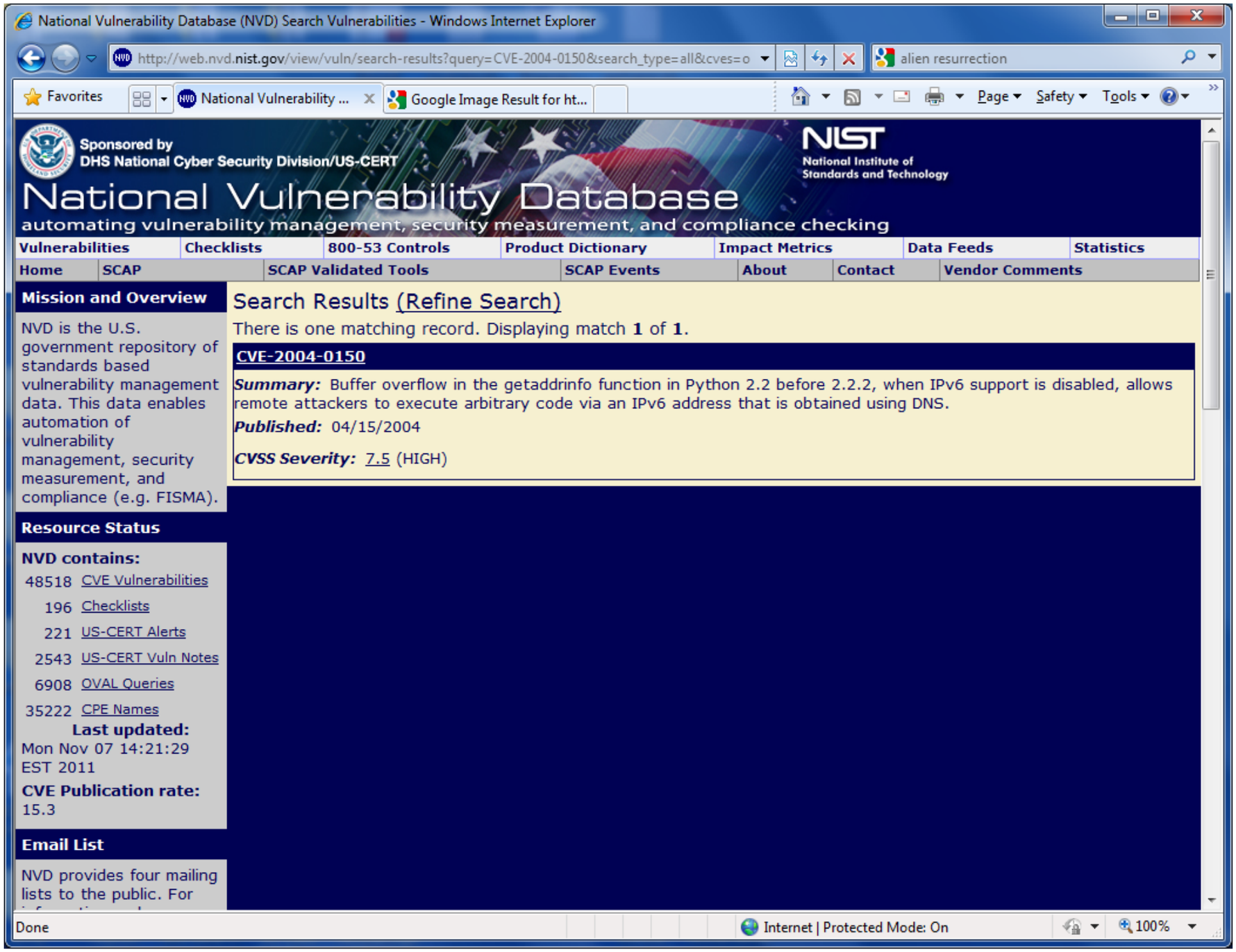
Povprečna ranljivost platform skozi leta

Zanimivi primeri

Alien Resurrection

Zanimivi primeri

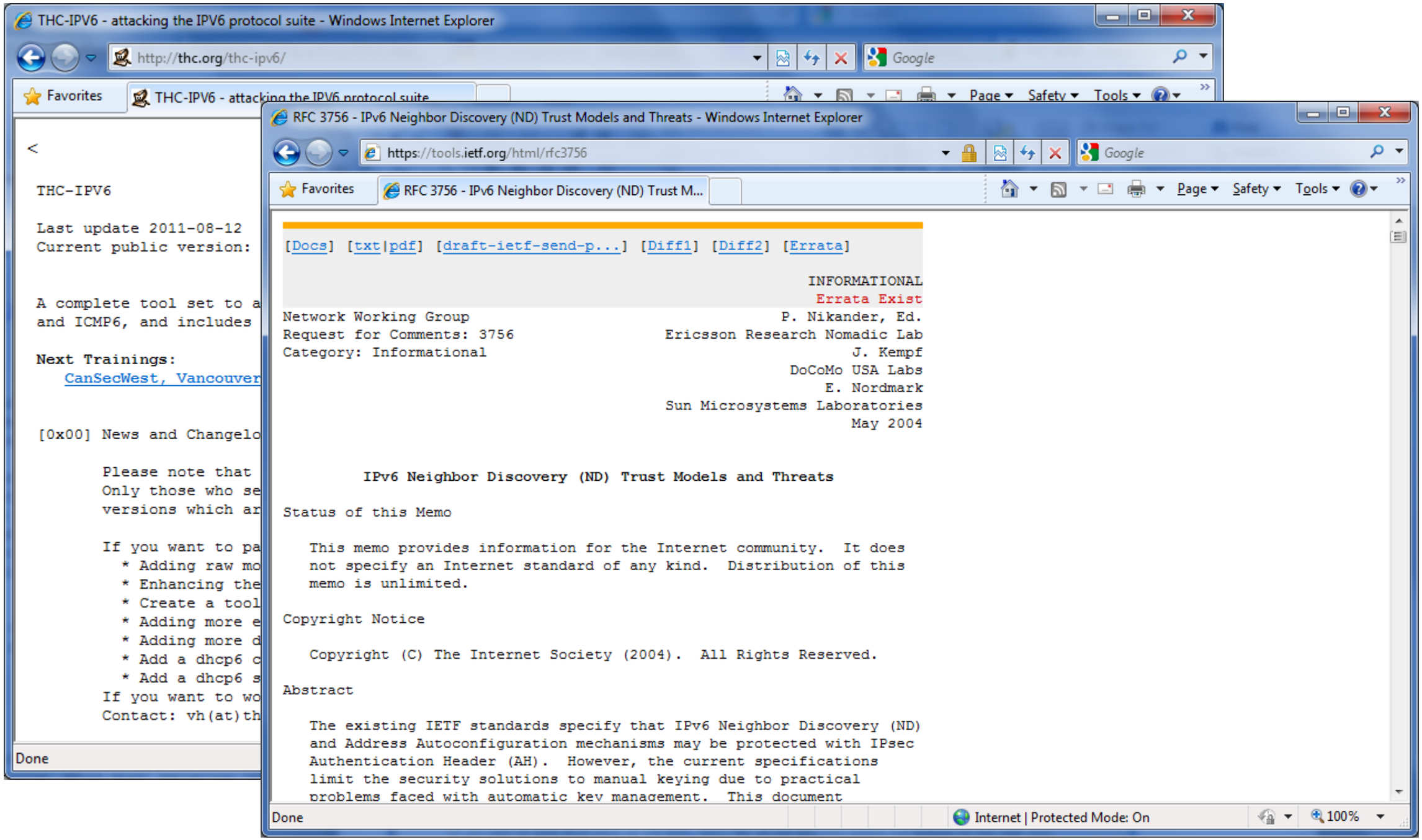
Python Code Exec



Zanimivi primeri

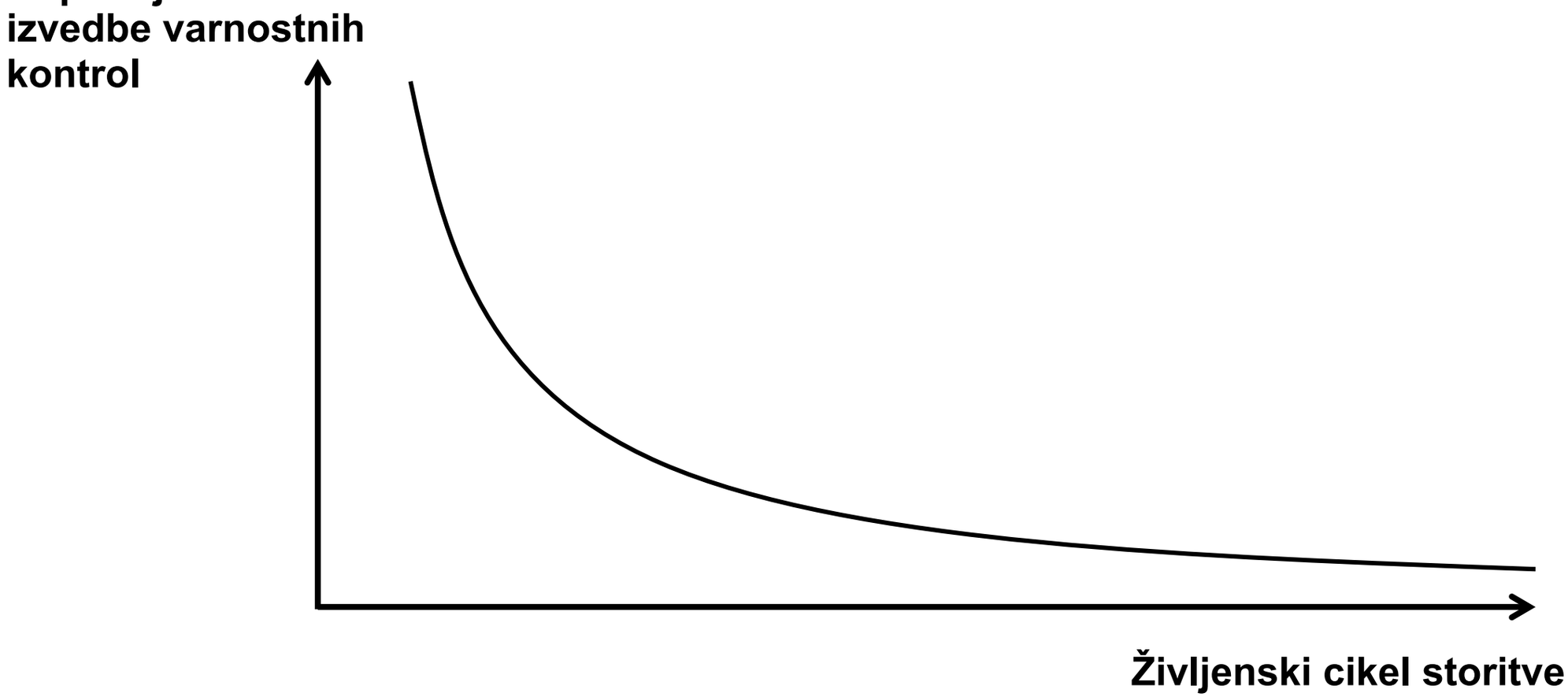
Hack the Mainframe!

Panic!


THC-IPV6 - attacking the IPV6 protocol suite - Windows Internet Explorer
http://thc.org/thc-ipv6/
Google
Favorites
THC-IPV6 - attacking the IPV6 protocol suite
Page
Safety
Tools
<
THC-IPV6
Last update 2011-08-12
Current public version:
A complete tool set to a
and ICMP6, and includes
Next Trainings:
CanSecWest, Vancouver
[0x00] News and Changelo
Please note that
Only those who se
versions which ar
If you want to pa
* Adding raw mo
* Enhancing the
* Create a tool
* Adding more e
* Adding more d
* Add a dhcp6 c
* Add a dhcp6 s
If you want to wo
Contact: vh(at)th
Done
RFC 3756 - IPv6 Neighbor Discovery (ND) Trust Models and Threats - Windows Internet Explorer
https://tools.ietf.org/html/rfc3756
Google
Favorites
RFC 3756 - IPv6 Neighbor Discovery (ND) Trust M...
Page
Safety
Tools
[Docs] [txt|pdf] [draft-ietf-send-p...] [Diff1] [Diff2] [Errata]
INFORMATIONAL
Errata Exist
Network Working Group
Request for Comments: 3756
Category: Informational
P. Nikander, Ed.
Ericsson Research Nomadic Lab
J. Kempf
DoCoMo USA Labs
E. Nordmark
Sun Microsystems Laboratories
May 2004
IPv6 Neighbor Discovery (ND) Trust Models and Threats
Status of this Memo
This memo provides information for the Internet community. It does
not specify an Internet standard of any kind. Distribution of this
memo is unlimited.
Copyright Notice
Copyright (C) The Internet Society (2004). All Rights Reserved.
Abstract
The existing IETF standards specify that IPv6 Neighbor Discovery (ND)
and Address Autoconfiguration mechanisms may be protected with IPsec
Authentication Header (AH). However, the current specifications
limit the security solutions to manual keying due to practical
problems faced with automatic key management. This document
Done
Internet | Protected Mode: On
100%

Back on track: Varni sistemi

- Varni sistemi so varno **načrtovani** in nato varno izvedeni in upravljani
- Varnost mora biti zahtevana in upoštevana od dneva 0



Zelena polja

- Vpeljava IPv6 je ena EDINSTVENIH priložnosti v vaši karieri, da stvari naredite dobro na podlagi izkušenj z IPv4
- Kaj lahko izboljšate pri izvedbi IPv6?
  - Utrjenost infrastrukture in njenih procesov
  - Topologijo (npr. razslojenost omrežja)
  - Omrežne varnostne storitve
    - Minimizacijo dostopa
    - Preverjanje protokolov
    - Kriptografsko zaščito
- Ali imamo na voljo vso tehnologijo za to? (torej tisto, ki je najboljša praksa tudi na IPv4)


FLINTS

Remember IPv4?

- Kaj so bili najlažji problemi v IPv4
  - Varnost prenosa (VPN)
  - Utrjevanje infrastrukture
- Kaj so bili največji problemi omrežne varnosti na IPv4, ki so ostali nerešeni (oziroma, pogosto neizvedeni)
  - Varnost v LAN (prestrezanje, DoS)
  - Varnost usmerjanja (prestrezanje, DoS)
  - Verifikacija protokolov in aplikacijsko filtriranje v omrežju („whitelist“ model)
  - Tuneliranje

Infrastrukturno varovanje

Cisco IOS

IPv4

- CoPP (SW/HW)
- CPPr
- iACL
- RTBH
- Overjanje usmerjevalnih protokolov
- Overjanje izvora usmerjevalnih informacij

IPv6

- CoPP (SW/HW)
- iACL
- RTBH
- Overjanje usmerjevalnih protokolov
- Filtriranje usmerjevalnih informacij
- Overjanje izvora usmerjevalnih informacij

Varovanje med varnostnimi domenami

Cisco ASA: dinamični protokoli

Podprti dinamični protokoli nad IPv4

- FTP
- SIP
- DCERPC/MSRPC
- CTIQBE
- GTP
- H.323
- ILS
- MGCP
- MMP
- PPTP
- RSH
- RTSP
- SKINNY
- SQL*NET
- TFTP
- SUNRPC
- XDMCP

Podprti dinamični protokoli nad IPv6

- FTP
- SIP

Varovanje med varnostnimi domenami

Poljubna naprava: verifikacija in minimizacija protokolov/podatkov

Verifikacija protokolov

- Odmetavanje neskladnih protokolnih enot (L3-L7)
- Težave: neskladno obnašanje v legitimnih sejah
- Rešitev IPv4: ignoriranje vseh neskladnosti
- (alternativna rešitev: normalizacija protokolov)
- Posledica: izguba dragocene kontrole pred DoS/codeexec napadi

Minimizacija protokolov/podatkov

- Prepuščanje le najnujnejših protokolnih sporočil in podatkov (whitelisting)
- Težave: kdo ve, kaj je mininalno potreben nabor?
- Rešitev IPv4: prepuščamo ves promet v seji
- (alternativna rešitev: IPS)
- Posledica: izguba pasu (ali naramnic) in posledično hitrejša izguba hlač

Varovanje med varnostnimi domenami

Cisco IPS

Podpisi nad IPv4

5343

Podpisi nad IPv6

4999

Varovanje v LAN

Dostopnost ARP Inspection, DHCP Snooping, IP Source Guard

- Catalyst 2960
- Catalyst 3570
- Catalyst 3760
- Catalyst 4500
- Catalyst 6500
- Nexus 5000
- Nexus 7000
- …

Dostopnost ND (SLAAC) Inspection

- Catalyst 6500

Implementacijske težave

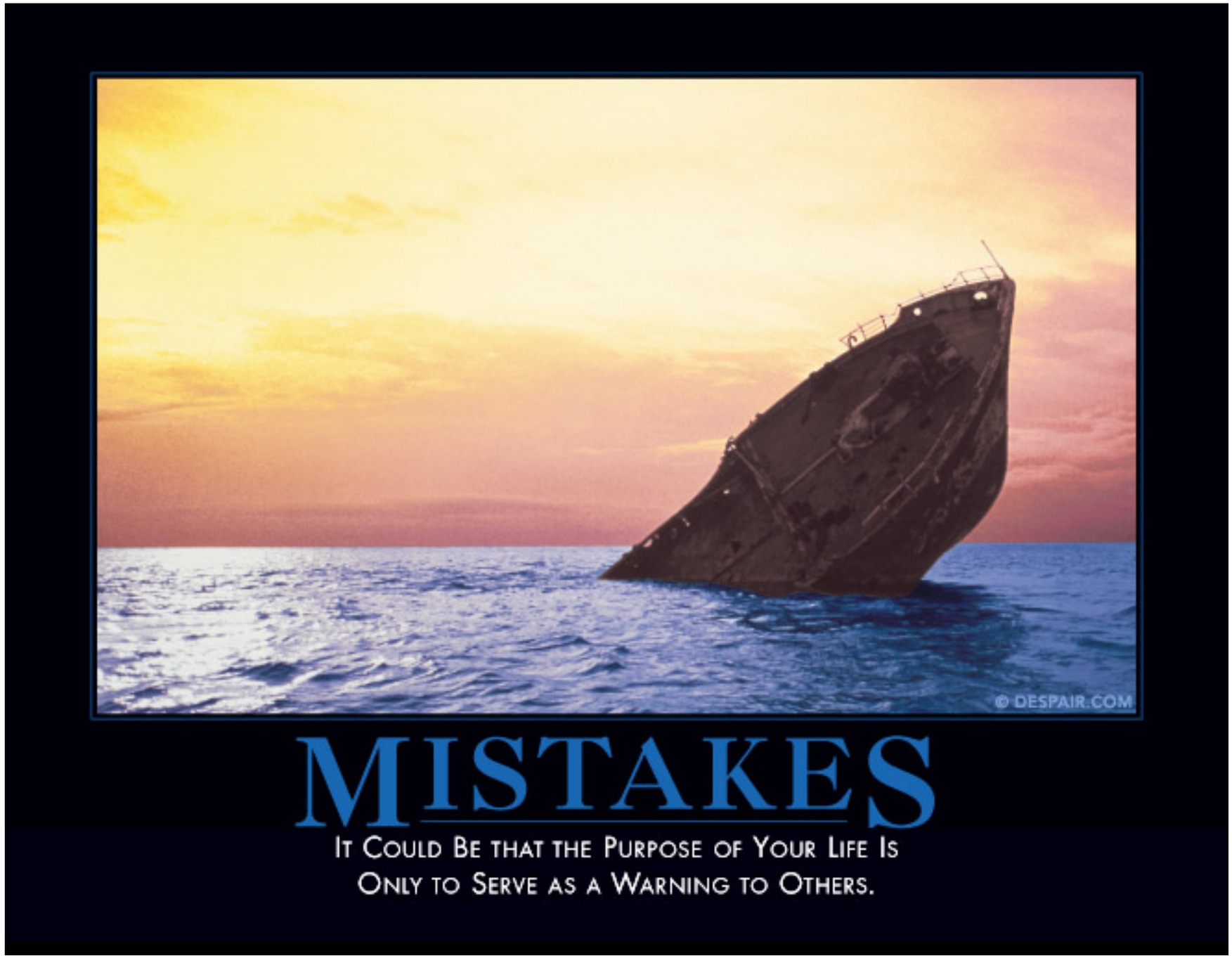
- V varnostnih mehanizmih so in bodo še nekaj časa
- Še vedno imate bistveno bolj omejen problem, kot pri IPv4, in torej luksuz, da lažje testirate
- Aktivno rešujte težave na svoji poti – konfiguracijske in v kodi (preko proizvajalca ali FOSS skupnosti); ne čakajte na druge, saj so cikli popravkov pogosto dolgi
- Cilj naj bo, da stvari vedno delajo, ne da samo delajo

Povzetek

- IPv6 ne prinaša bistveno novih tveganj, morate pa ustrezno obravnavati vsa „nova stara“ tveganja
- Najboljša varnost na svetu je ta, ki je popolnoma prilagojena svojemu okolju
- Zdaj je pravi trenutek, ki ga ne boste več imeli
- Zelo dobro analizirajte svoje tehnološke možnosti za prenos kontrol v svet IPv6
- V IPv6 svetu boste (upam!) stvari večinoma naredili bolje kot v IPv4 – znanje prenesite nazaj v IPv4!
- Give back to the community! Skupaj izboljšajmo kakovost kontrol v IPv6!

Carpe IPv6 diem!

Ali pa vsaj pustite, da se od vas učimo…



Projekte zaključimo. Odnosi trajajo.