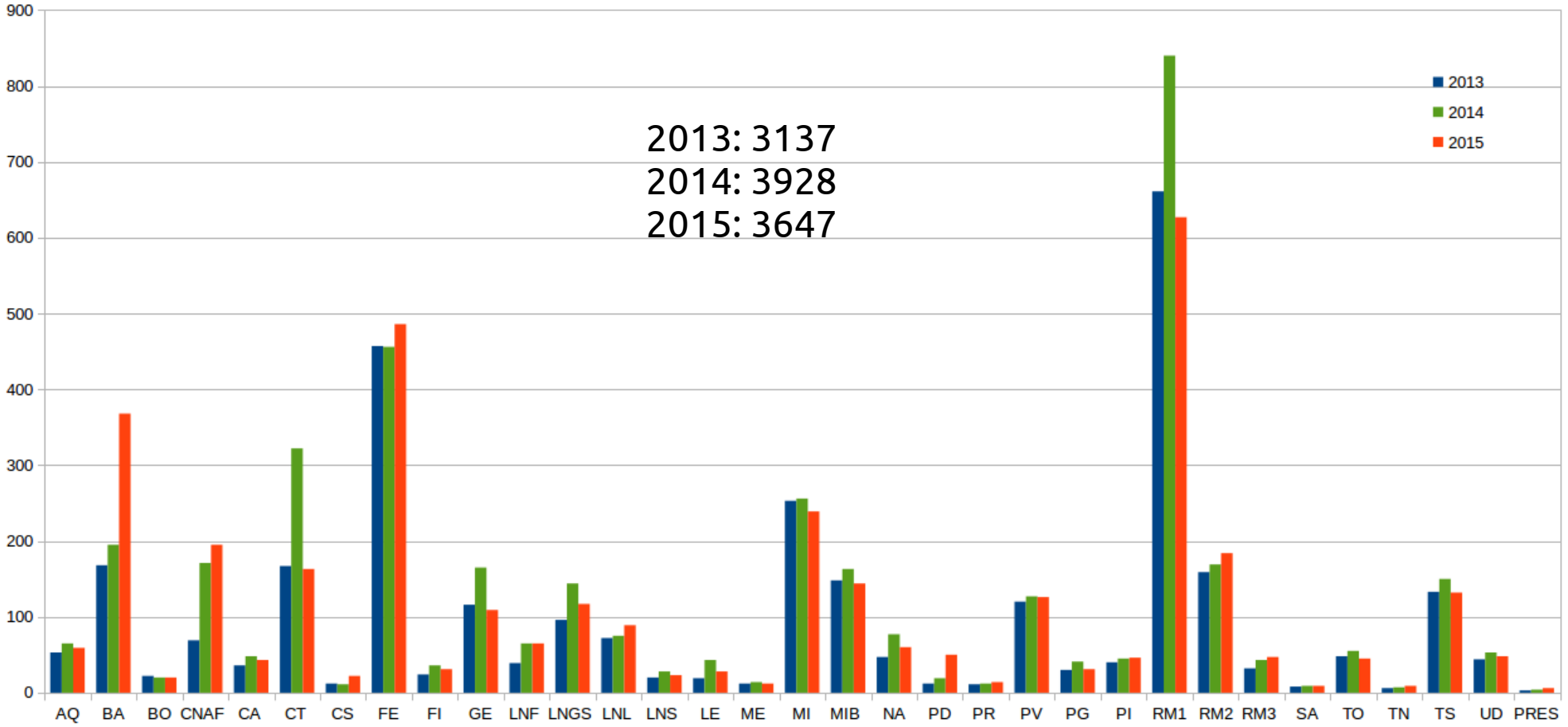
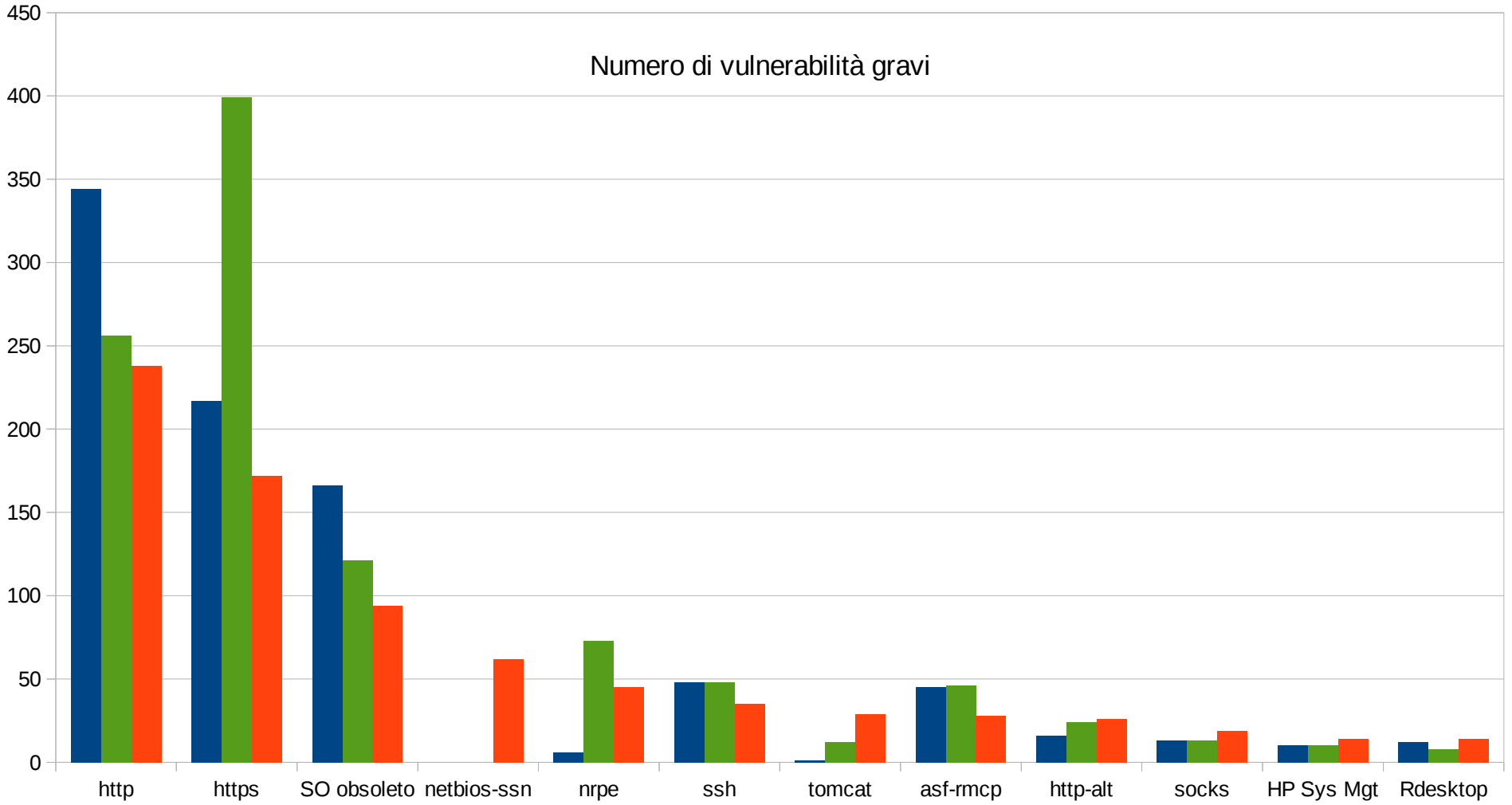
Gruppo auditing

- Franco Brasolin
- Roberto Cecchini
- Leandro Lanzi
- Antonella Monducci
- Michele Michelotto

Nodi esaminati



Vulnerabilità gravi



Vulnerabilità gravi rilevate

#	Descrizione	porta
82	Unsupported Unix Operating System	0
45	Apache HTTP Server Byte Range DoS	80
44	Nagios NRPE Command Argument Processing Enabled	5666
22	Apache HTTP Server Byte Range DoS	443
17	IPMI v2.0 Password Hash Disclosure	623
16	Apache 2.2 < 2.2.28 Multiple Vulnerabilities	80
12	OpenSSL 'ChangeCipherSpec' MiTM Vulnerability	443
11	PHP Unsupported Version Detection	80
11	IPMI Cipher Suite Zero Authentication Bypass	623
9	Unsupported Web Server Detection	80
9	PHP Unsupported Version Detection	443
7	PHP < 5.3.11 Multiple Vulnerabilities	443
7	OpenSSL 1.0.1 < 1.0.1i Multiple Vulnerabilities	8443
7	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)	3389
7	PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution	443
7	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)	3389
7	PHP < 5.3.9 Multiple Vulnerabilities	443
7	OpenSSL 1.0.1 < 1.0.1h Multiple Vulnerabilities	8443
7	OpenSSL 1.0.1 < 1.0.1g Multiple Vulnerabilities	8443
6	Apache 2.2 < 2.2.28 Multiple Vulnerabilities	443
6	OpenSSH < 4.7 Trusted X11 Cookie Connection Policy Bypass	22

Principali porte aperte

Servizio	Porta	# Vuln.	# porte aperte
ssh	22	25	2187
http	80	238	927
https	443	172	640
mysql	3306		233
ipp + printer	631 + 515		136
VNC	5900-3	5	185
ganglia (?)	8649	5	156
nrpe (nagios)	5666	44	126
smtp	25	3	92
domain	53		88
sunrpc	111		78
netbios-ssn	139	62	31
IPMI	623/u	28	19
x11	6000	2	15
ftp	21		13
tftp	69/u		10
shell / rsh	514	1	8

poodle

- Con MITM si può degradare la sessione a SSL 3.0, e sfruttare un bug per intercettarla
- È legato al protocollo, quindi non solo web
- Server web INFN vulnerabili (5/15): **247**

Eliminare poodle

- apache (**ssl.conf**)

  SSLProtocol all -SSLv3 -SSLv2

- postfix (**main.cf**)

  smtpd_tls_mandatory_protocols=!SSLv2, !SSLv3

- dovecot (**/etc/dovecot/conf.d/10-ssl.conf**)

  ssl_protocols = !SSLv3 !SSLv2

freak

- Via MITM si ottiene un downgrade della sessione ad una che usa chiavi deboli, facilmente decifrabili.
- Server web INFN vulnerabili (5/15): **51**

Eliminare freak

Configuration	Oldest compatible client
Modern	Firefox 27, Chrome 22, IE 11, Opera 14, Safari 7, Android 4.4, Java 8
Intermediate	Firefox 1, Chrome 1, IE 7, Opera 5, Safari 1, Windows XP IE8, Android 2.3, Java 7
Old	Windows XP IE6, Java 6

- Guida e generatore di configurazione:
  - v.gd/boXltP
  - v.gd/NLlCeq

logjam

- Con MITM si abbassa la connessione TLS ad una con chiave di 512 bit.
- Simile a freak, ma sfrutta un difetto del protocollo e attacca una chiave DH (invece che RSA).
- Tutti i server (web, ssh, imap, ...) che supportano DHE_EXPORT sono vulnerabili

Eliminare logjam

- Togliere il supporto agli algoritmi deboli
- Generare un gruppo DH diverso da quello standard
- Istruzioni: weakdh.org/sysadmin.html

TLS e CA

- Totale server web vulnerabili: 264
  - poodle: 247
  - freak 51
- 172 (65%!) server vulnerabili usano **CA casalinghe**
  - TCS
  - INFN CA
  - Let's Encrypt?

Miglioramenti a https

- **HTTP Strict Transport Security** (HSTS)
  - il server dice al browser di usare solo connessioni cifrate per un certo periodo
  - v.gd/h8wvSp
- **Certificati con SHA-2**
  - il supporto di certificati SHA-1 da parte dei browser sta cessando
- **Forward secrecy**
  - protegge le chiavi di sessione
  - utilizzare TLS con DHE o ECDHE

Verifica TLS

- Server: **v.gd/YACdaO**
- Browser: **v.gd/TRPyiG**

Fritto misto

- **TCS**
- **OpenVAS** vs **nessus**
- Un po' di hacking sui servizi aperti
- Censimento CA utilizzate
- Distribuzione per auditor fai-da-te
- Argomenti per il WS di Ottobre (**4-5 Novembre, Firenze**)