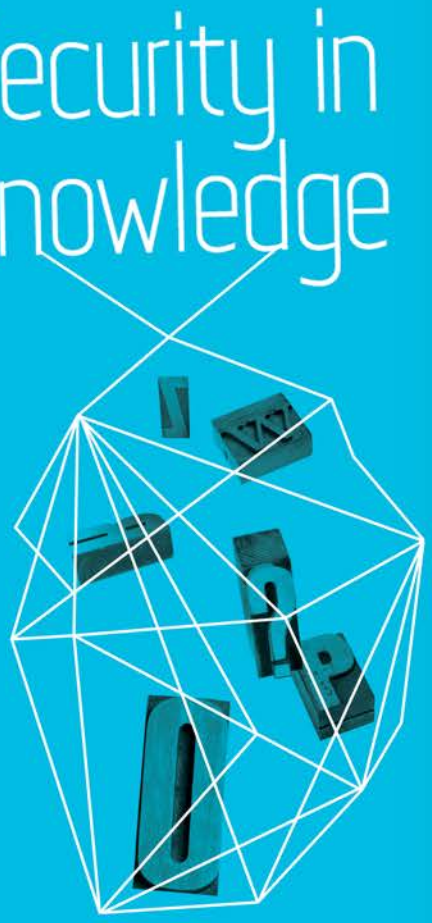
RSA CONFERENCE ASIA PACIFIC 2013

THE STATE OF SAP SECURITY 2013: VULNERABILITIES, THREATS AND TRENDS



Alexander Polyakov
ERPScan

Session ID: DAS-T03

Session Classification: Intermediate

Agenda

- SAP: Intro
- SAP: vulnerabilities
- SAP: threats from the Internet
- Critical SAP services
- Known incidents
- Future trends and predictions
- Conclusions

Agenda

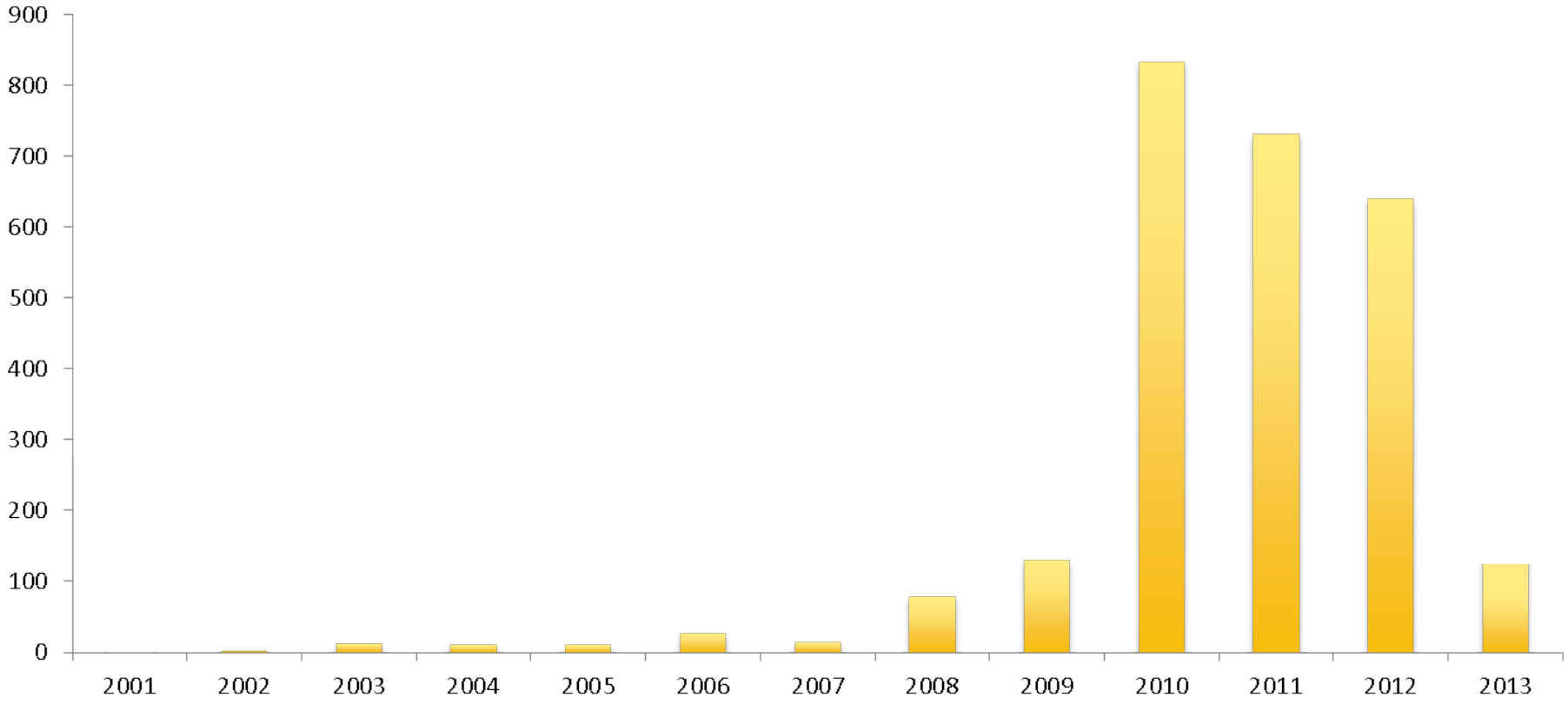
- The most popular business application
- More than 180000 customers worldwide
- 74% of Forbes 500 run SAP

Why SAP security?

- Espionage
  - Stealing financial information
  - Stealing corporate secrets
  - Stealing supplier and customer lists
  - Stealing HR data
- Sabotage
  - Denial of service
  - Modification of financial reports
  - Access to technology network (SCADA) by trust relations
- Fraud
  - False transactions
  - Modification of master data

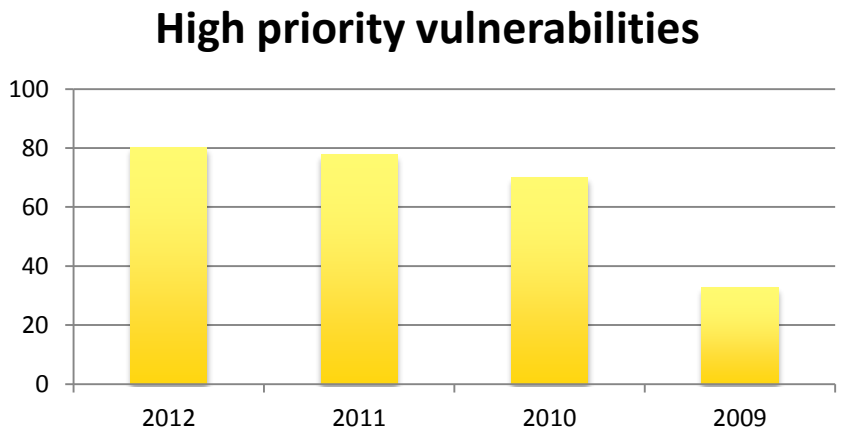
SAP Vulnerabilities

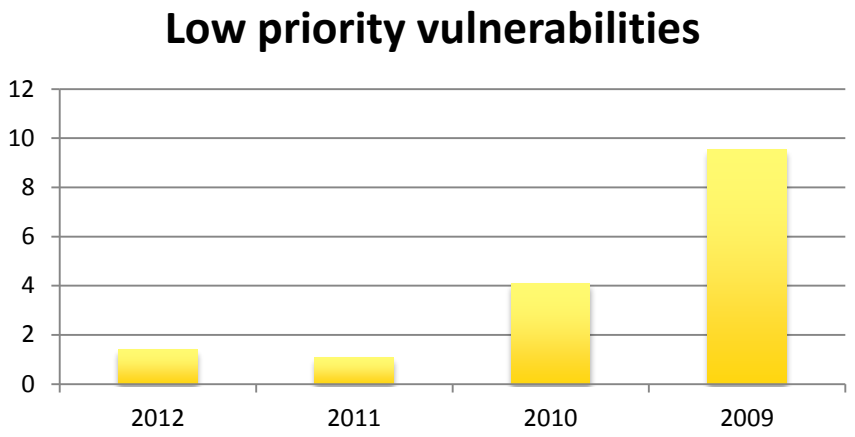
Security notes by year

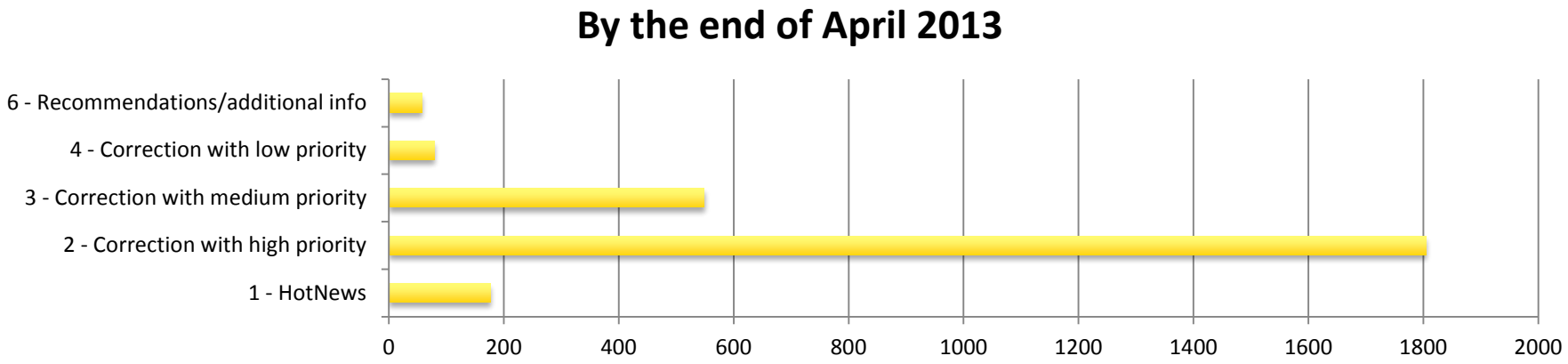


More than 2600 in total

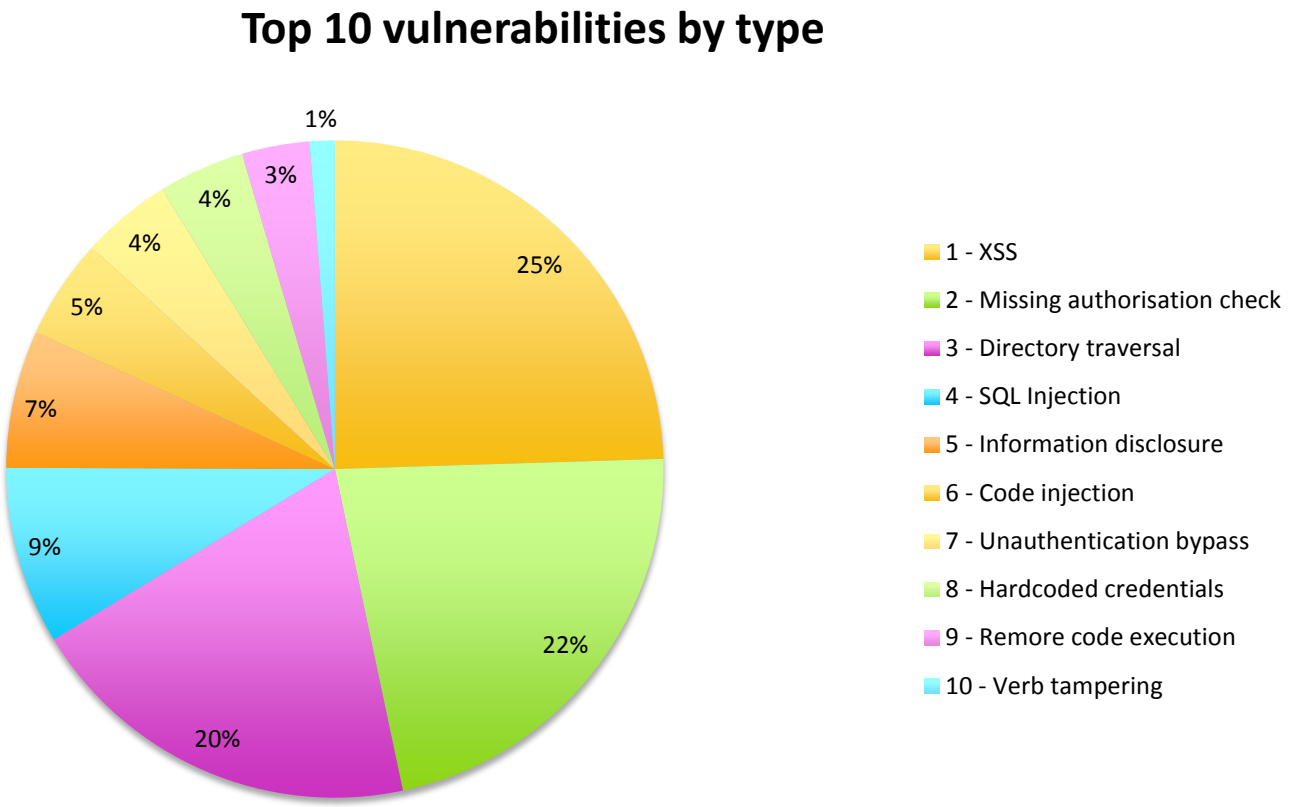
Security notes by criticality







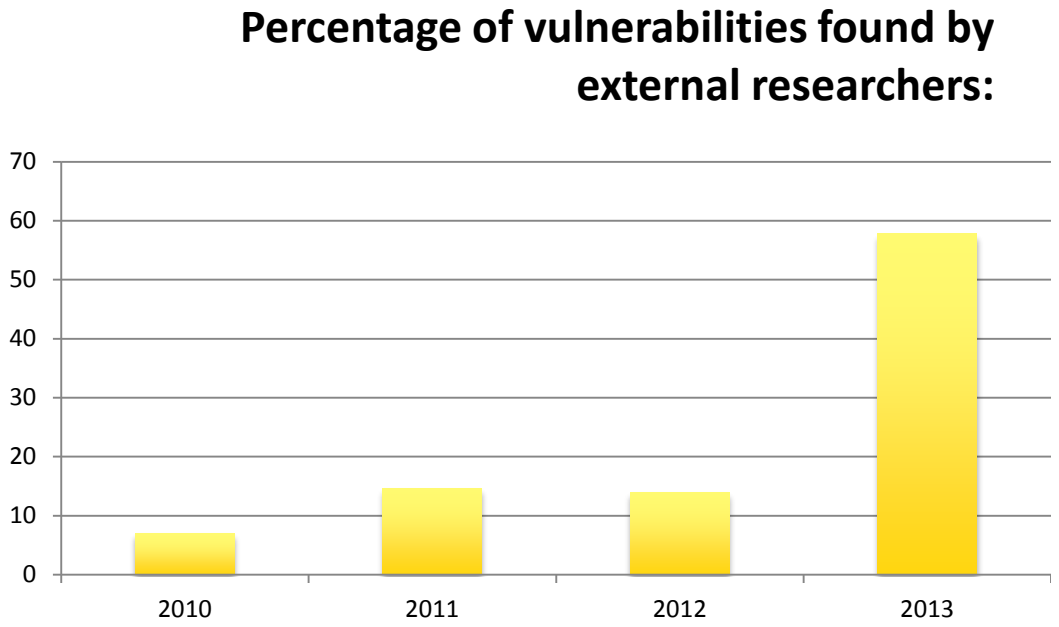
Security notes by type



Acknowledgments

Number of vulnerabilities
found by external researchers:

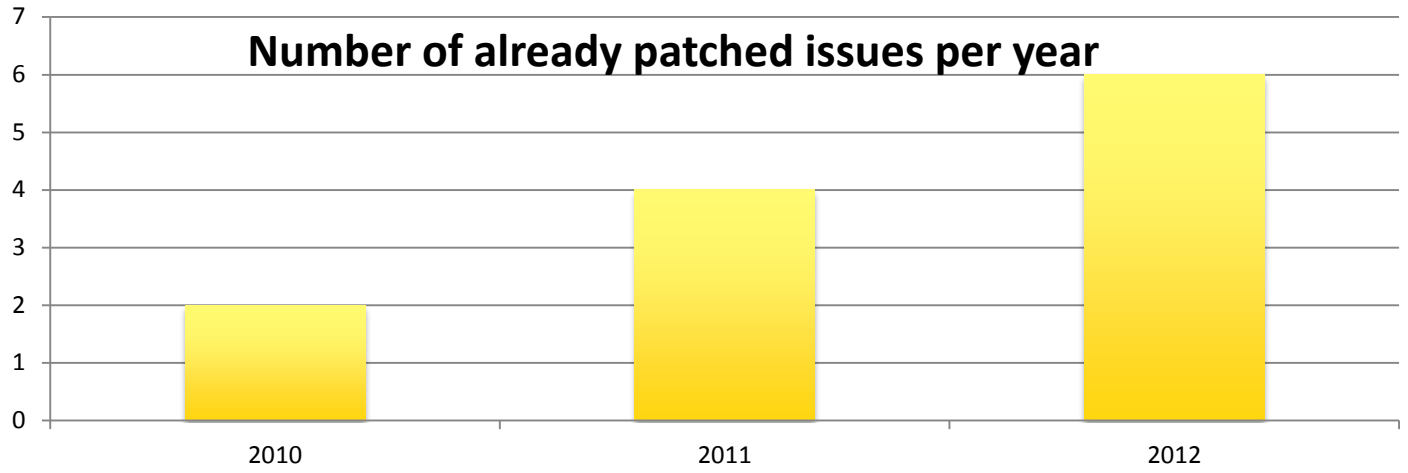
- 2010 - 58
- 2011 - 107
- 2012 - 89
- 2013 - 52



The record of vulnerabilities found by external researchers was cracked in January 2013: 76%

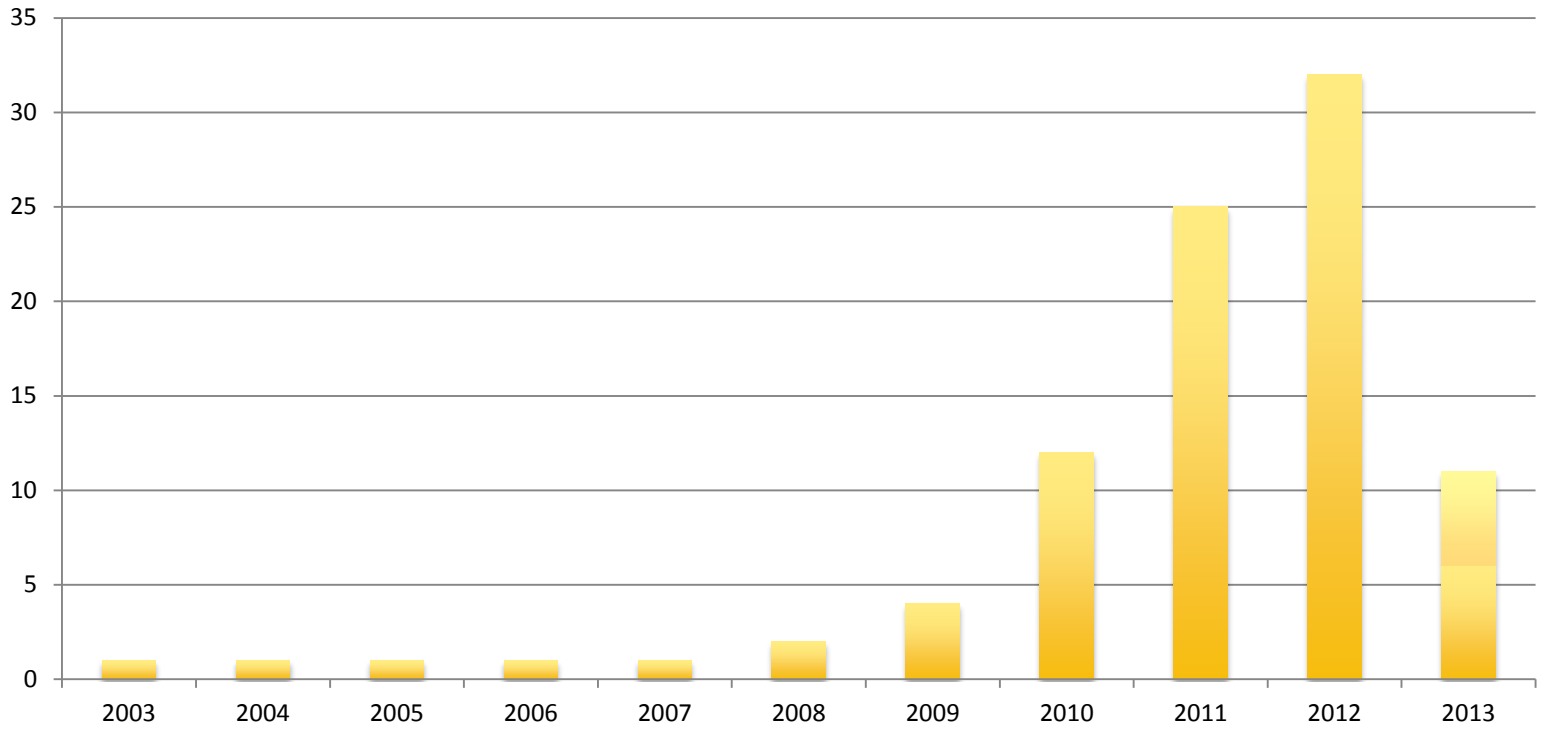
Acknowledgments

- More interest from other companies



** Number of vulnerabilities that were sent to SAP but were rejected because they were already found before by other company of SAP internal code review.*

SAP security talks at conferences



Talks about:

- **Common:** SAP Backdoors, SAP Rootkits, SAP Forensics
- **Services:** SAP Gateway, SAP Router, SAP NetWeaver, SAP GUI, SAP Portal, SAP Solution Manager, SAP TMS, SAP Management Console, SAP ICM/ITS
- **Protocols:** DIAG, RFC, SOAP (MMC), Message Server, P4
- **Languages:** ABAP Buffer Overflow, ABAP SQL Injection, J2EE Verb Tampering, J2EE Invoker Servlet
- **Overview:** SAP Cyber-attacks, Top 10 Interesting Issues, Myths about ERP

Almost every part of SAP was hacked

Top 5 SAP vulnerabilities 2012

1. SAP NetWeaver DilbertMsg servlet SSRF (June)
2. SAP HostControl command injection (May)
3. SAP SDM Agent command injection (November)
4. SAP Message Server buffer overflow (February)
5. SAP DIAG buffer overflow (May)

SAP NetWeaver DilbertMsg servlet SSRF

Espionage:	Critical
Sabotage:	Critical
Fraud:	Medium
Availability:	Anonymously through the Internet
Ease of exploitation:	Medium
Future impact:	High (New type of attack)
CVSSv2:	10 (according to ERPScan researchers)
Advisory:	http://erpscan.com/advisories/dsecrg-12-036-sap-xi-authentication-bypass/
Patch:	Sap Note 1707494
Authors:	Alexander Polyakov, Alexey Tyurin, Alexander Minozhenko (ERPScan)

SAP HostControl command injection

Espionage:	Critical
Sabotage:	Critical
Fraud:	Critical
Availability:	Anonymously through the Internet
Ease of exploitation:	Easy (a Metasploit module exists)
Future impact:	Low (Single issue)
CVSSv2:	10 (according to ERPScan researchers)
Advisory:	http://www.contextis.com/research/blog/sap-parameter-injection-no-space-arguments/
Patch:	SAP note 1341333
Author:	Contextis

SAP J2EE file read/write

Espionage:	Critical
Sabotage:	Critical
Fraud:	Critical
Availability:	Anonymously
Ease of exploitation:	Medium
Future impact:	Low
CVSSv2:	10 (according to ERPScan researchers)
Advisory:	https://service.sap.com/sap/support/notes/1682613
Patch:	SAP Note 1682613
Author:	Juan Pablo

SAP Message Server buffer overflow

Espionage:	Critical
Sabotage:	Critical
Fraud:	Critical
Availability:	Anonymous
Ease of exploitation:	Medium. Good knowledge of exploit writing for multiple platforms is necessary
CVSSv2:	10 (according to ERPScan researchers)
Advisory:	http://www.zerodayinitiative.com/advisories/ZDI-12-112/
Patch:	SAP Notes 1649840 and 1649838
Author:	Martin Gallo

SAP DIAG Buffer overflow

Espionage:	Critical
Sabotage:	Critical
Fraud:	Critical
Availability:	Low. Trace must be on
Ease of exploitation:	Medium
CVSSv2:	9.3 (according to ERPScan researchers)
Advisory:	http://www.coresecurity.com/content/sap-netweaver-dispatcher-multiple-vulnerabilities
Patch:	SAP Note 1687910
Author:	Martin Gallo

- SAP and the Internet

SAP on the Internet

- Companies have SAP Portals, SAP SRMs, SAP CRMs remotely accessible
- Companies connect different offices (by SAP XI)
- Companies are connected to SAP (through SAP Router)
- SAP GUI users are connected to the Internet
- Administrators open management interfaces to the Internet for remote control

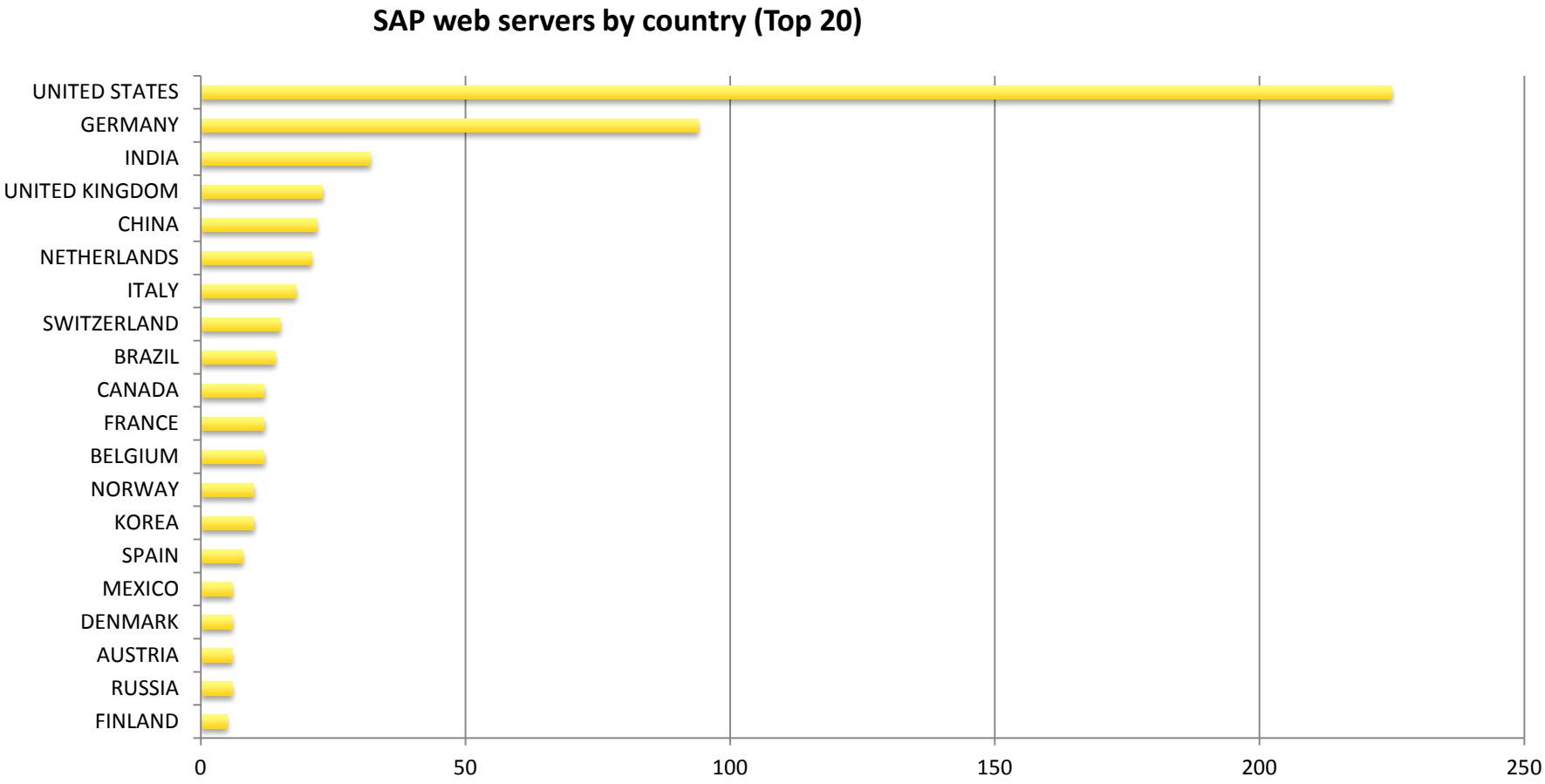
Almost all business applications have web access now

Google search for web-based SAPs

- As a result of the scan, **695** unique servers with different SAP web applications were found (14% more than in 2011)
- 22% of previously found services were deleted
- 35% growth in the number of new services

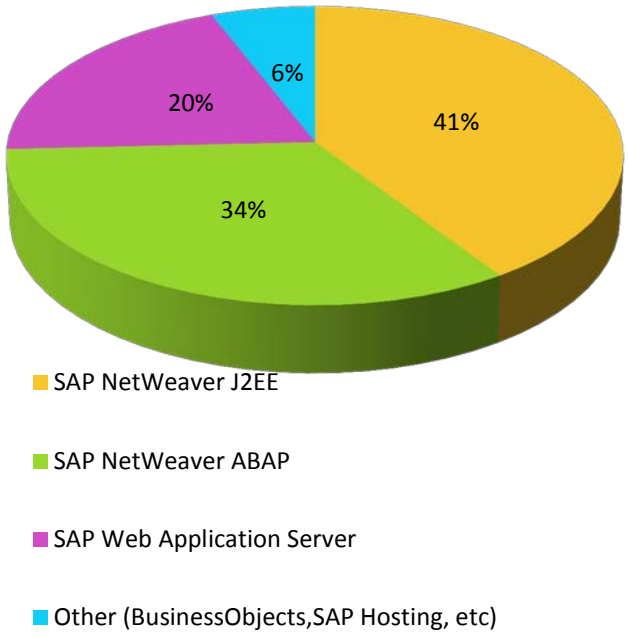
Application server type	Search string
SAP NetWeaver ABAP	Inurl:/SAP/BC/BSP
SAP NetWeaver J2EE	Inurl:/irj/portal
SAP BusinessObjects	inurl:infoviewapp

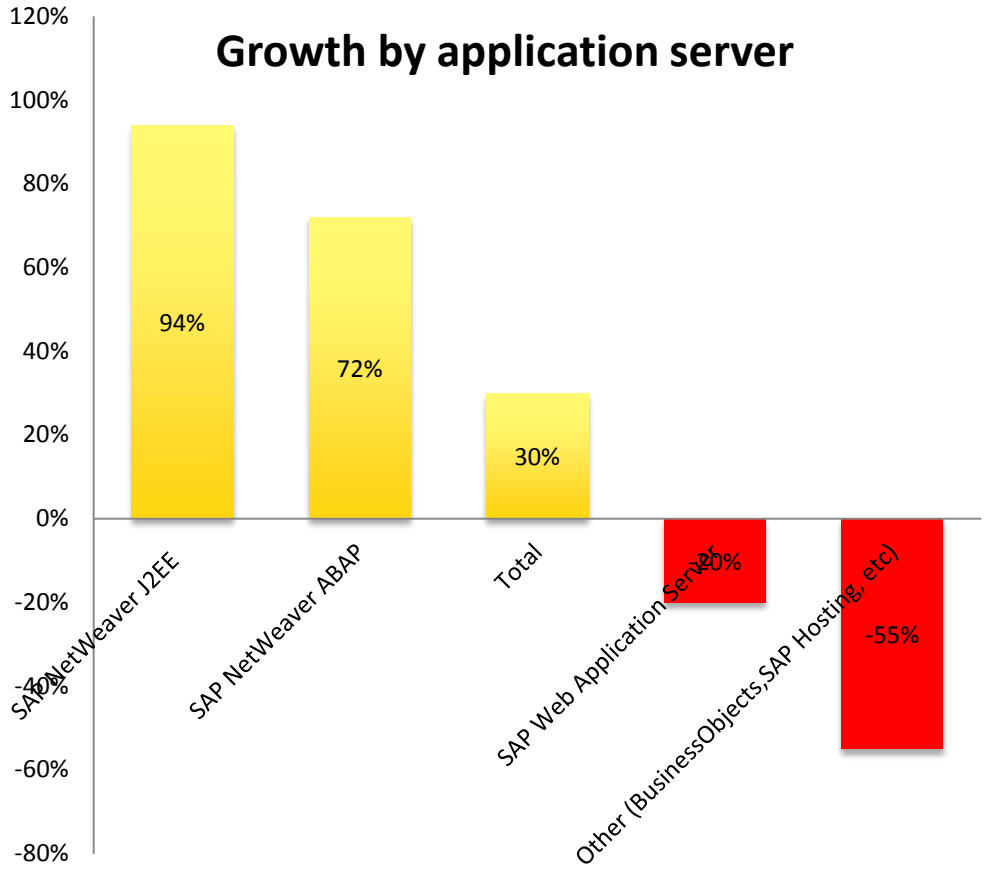
Google search by country



Shodan scan

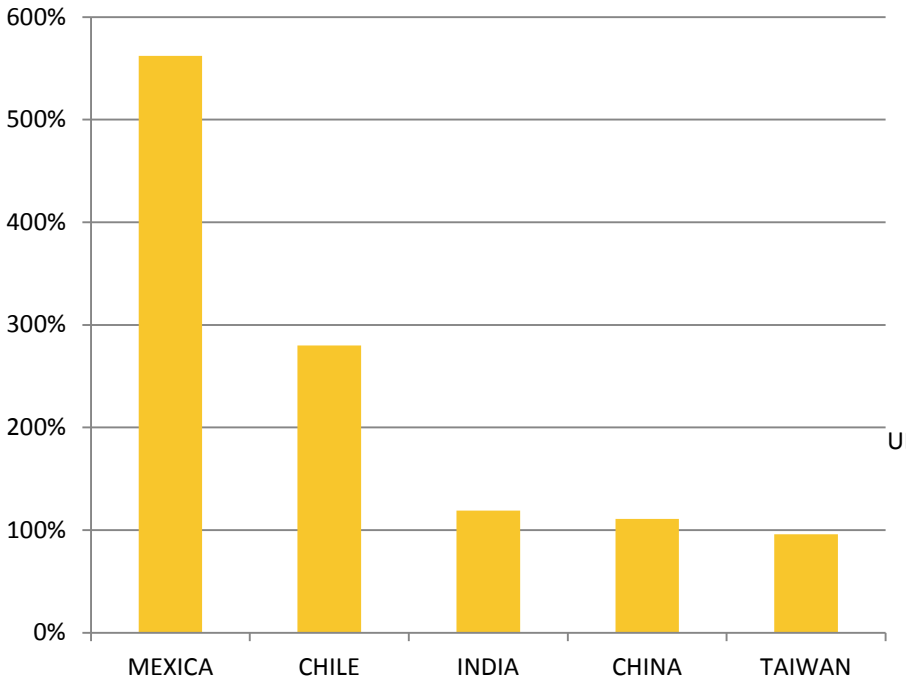
A total of 3741 server with different SAP web applications were found



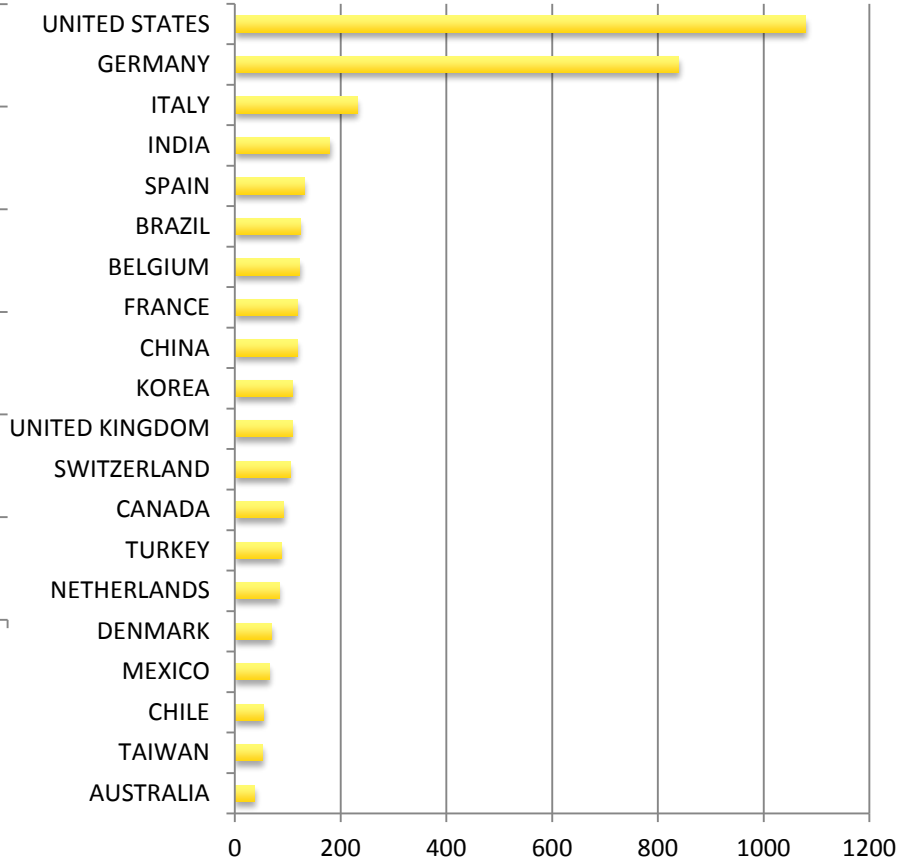


Shodan scan by country

Growth of SAP web servers (Top 5)

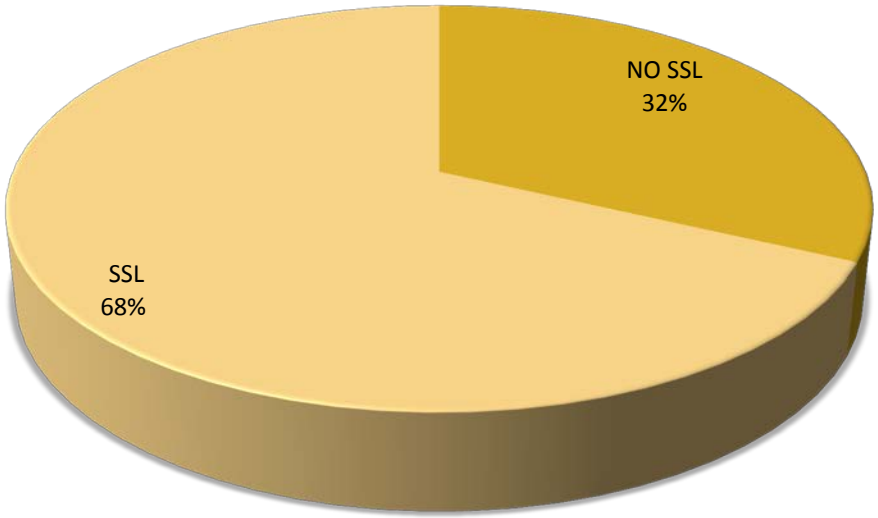


SAP web servers by country (Top 20)



Internet Census 2012 scan

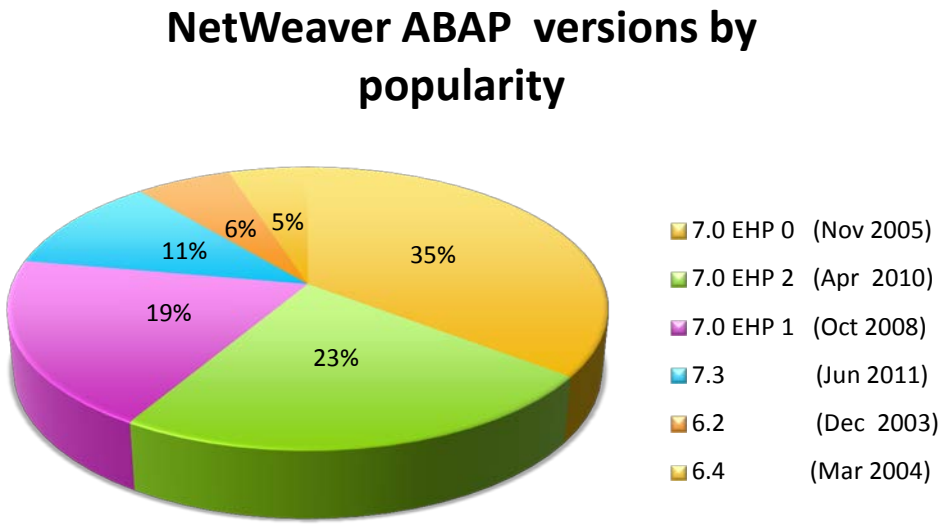
- Not so legal project by Carna Botnet
- As a result, **3326** IPs with SAP web applications



SAP NetWeaver ABAP - versions

- 7.3 growth by 250%
- 7.2 growth by 70%

- 7.0 loss by 22%
- 6.4 loss by 45%



The most popular release (35%, previously 45%) is still NetWeaver 7.0, and it was released in 2005!

But security is getting better.

NetWeaver ABAP – information disclosure

- Information about the ABAP engine version can be easily found by reading an HTTP response
- Detailed info about the patch level can be obtained if the application server is not securely configured
- An attacker can get information from some pages like /sap/public/info

6% (was 59%) of servers still have this issue

SAP NetWeaver ABAP – critical services

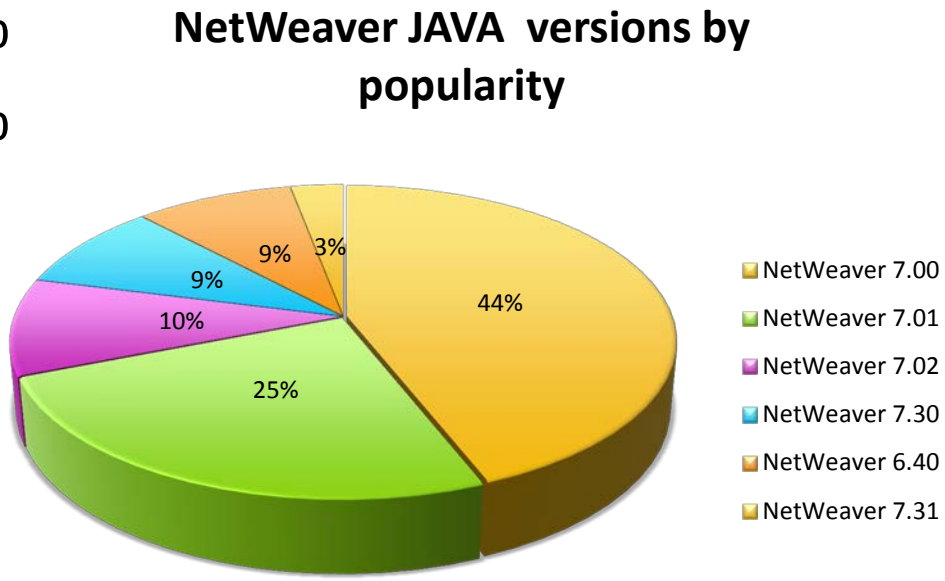
- Execute dangerous RFC functions using HTTP requests
- NetWeaver ABAP URL – /sap/bc/soap/rfc
  - Can be protected by Security Note 1394100: Access to RFC-enabled modules via SOAP
- There are several critical functions, such as:
  - Read data from SAP tables
  - Create SAP users
  - Execute OS commands
  - Make financial transactions, etc.
- By default, **any user can have access to this interface** and execute the RFC_PING command. So there are 2 main risks:
  - If there is a default username and password, the attacker can execute numerous dangerous RFC functions
  - If a remote attacker obtains any existing user credentials, they can execute a denial of service attack with a malformed XML packet
  - Can be protected by Security Note 931252: Authority Check for Function Group SRFC

Secure Configuration of SAP NetWeaver Application Server Using ABAP

SAP NetWeaver J2EE - versions

- 7.31 growth from 0 to 3%
- 7.30 growth from 0 to 9%
- 7.02 growth by 67%

- 7.0 loss by 23%
- 6.4 loss by 40%



The most popular release (44%, previously 57%) is still NetWeaver 7.0, and it was released in 2005!

But security is getting better.

SAP NetWeaver J2EE – information disclosure

- Information about the J2EE engine version can be easily found by reading an HTTP response.
- Detailed info about the patch level can be obtained if the application server is not securely configured and allows an attacker to get information from some pages:
  - /rep/build_info.jsp 26% (61% last year)
  - /bcb/bcbadmSystemInfo.jsp 1.5% (17% last year)
  - /AdapterFramework/version/version.jsp 2.7% (a new issue)
- To secure your SAP system, use these SAP Security Notes:
  - 1503856: Potential information disclosure relating to server info
  - 1548548: Missing authentication in Business Communication Broker
  - 1679897: PI SEC: Potential information disclosure in PI AF

SAP NetWeaver J2EE – critical services

- NetWeaver J2EE URL: /ctc/ConfigTool (and 30 others)
- **Can be exploited without authentication**
- There are several critical functions, such as:
  - Create users
  - Assign a role to a user
  - Execute OS commands
  - Remotely turn J2EE Engine on and off
- Was presented by us at BlackHat 2011
- To protect your system, use SAP Security Note:
  - 1589525: Verb Tampering issues in CTC

It was found that 50% (was 61%) of J2EE systems on the Internet have the CTC service enabled.

- From Internet to Intranet

Disclaimer

- ** Some numbers are approximate (mostly less than in real world) due to the very high amount of resources needed to fully analyze the Internet for SAP services with detailed numbers. We use optimized scan approach, which will be described in the whitepaper. More precise numbers will be published next month, after all the scans are finished and the results are fully analyzed.*

SAProuter

- Special application proxy
- Transfers requests from Internet to SAP (and not only)
- Can work through VPN or SNC
- Almost every company uses it for connecting to SAP to download updates
- Usually listens to port 3299
- Internet accessible (approximately 5000 IPs)
- http://www.easymarketplace.de/saprouter.php

Almost every third company have SAProuter accessible from internet by default port.

SAProuter: known issues

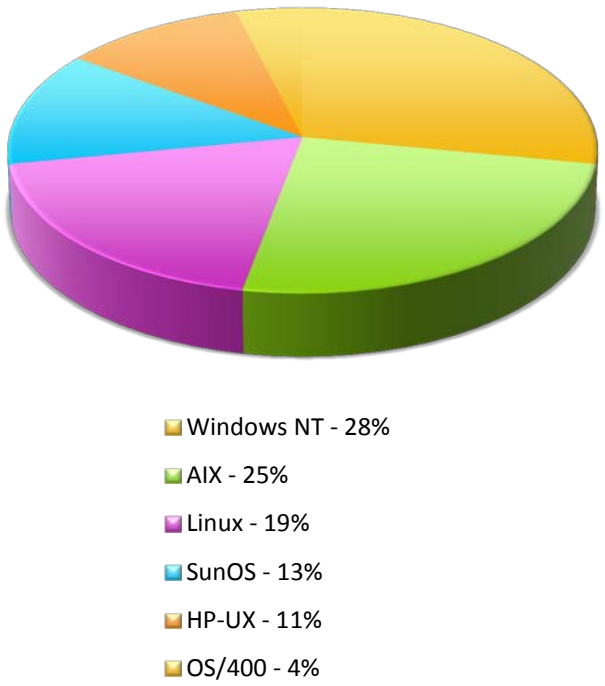
- Absence of ACL – 15%
  - Possible to proxy any request to any internal address
- Information disclosure about internal systems – 19%
  - Denial of service by specifying many connections to any of the listed SAP servers
  - Proxy requests to internal network if there is absence of ACL
- Insecure configuration, authentication bypass – 5%
- Heap corruption vulnerability

Port scan results

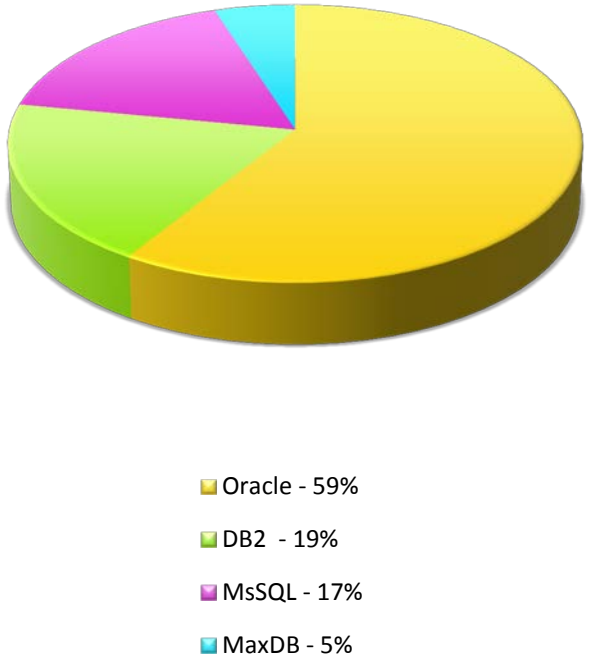
- Are you sure that only the necessary SAP services are exposed to the Internet?
- We were not
- In 2011, we ran a global project to scan all of the Internet for SAP services
- It is not completely finished yet, but we have the results for the top 1000 companies
- We were shocked when we saw them first

Popular OS and DB

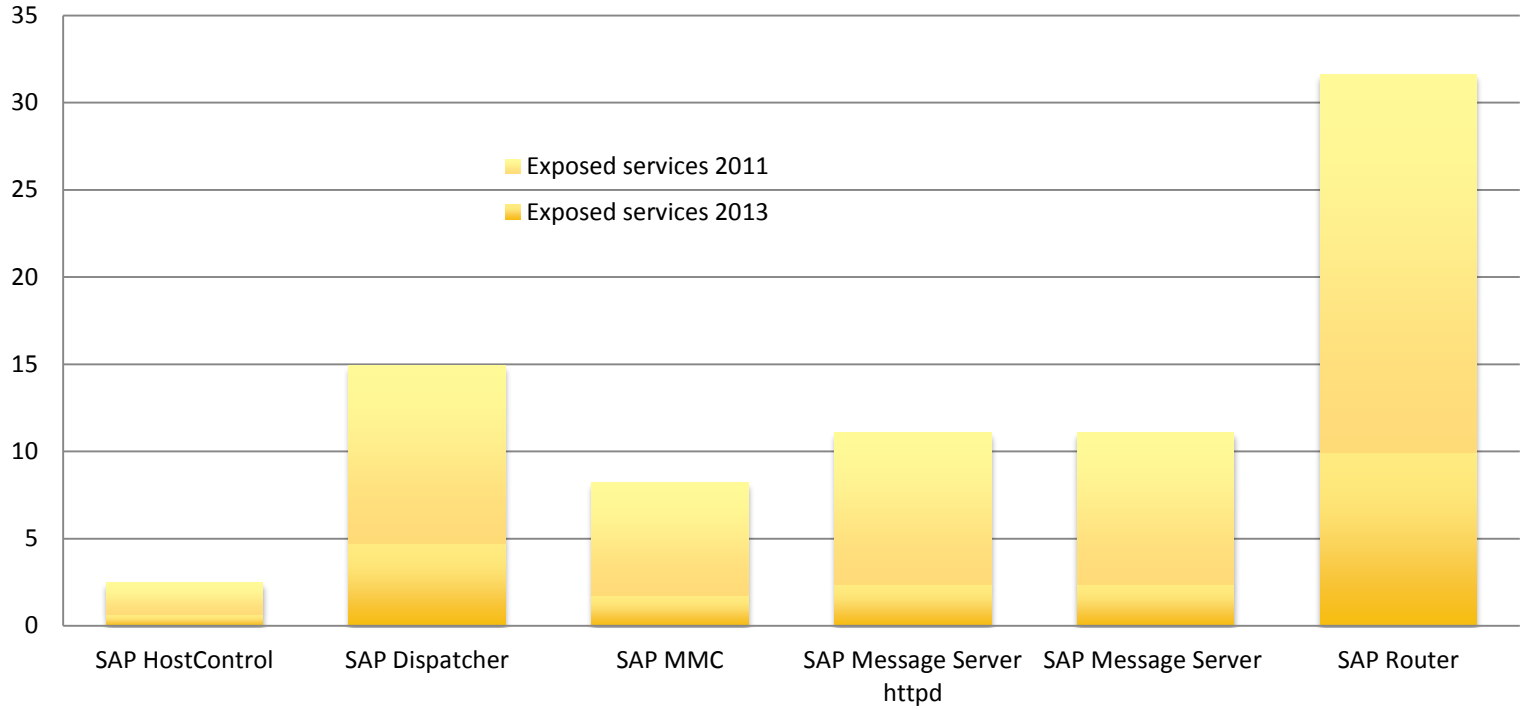
Popular OS for SAP



Popular RDBMS for SAP Backend

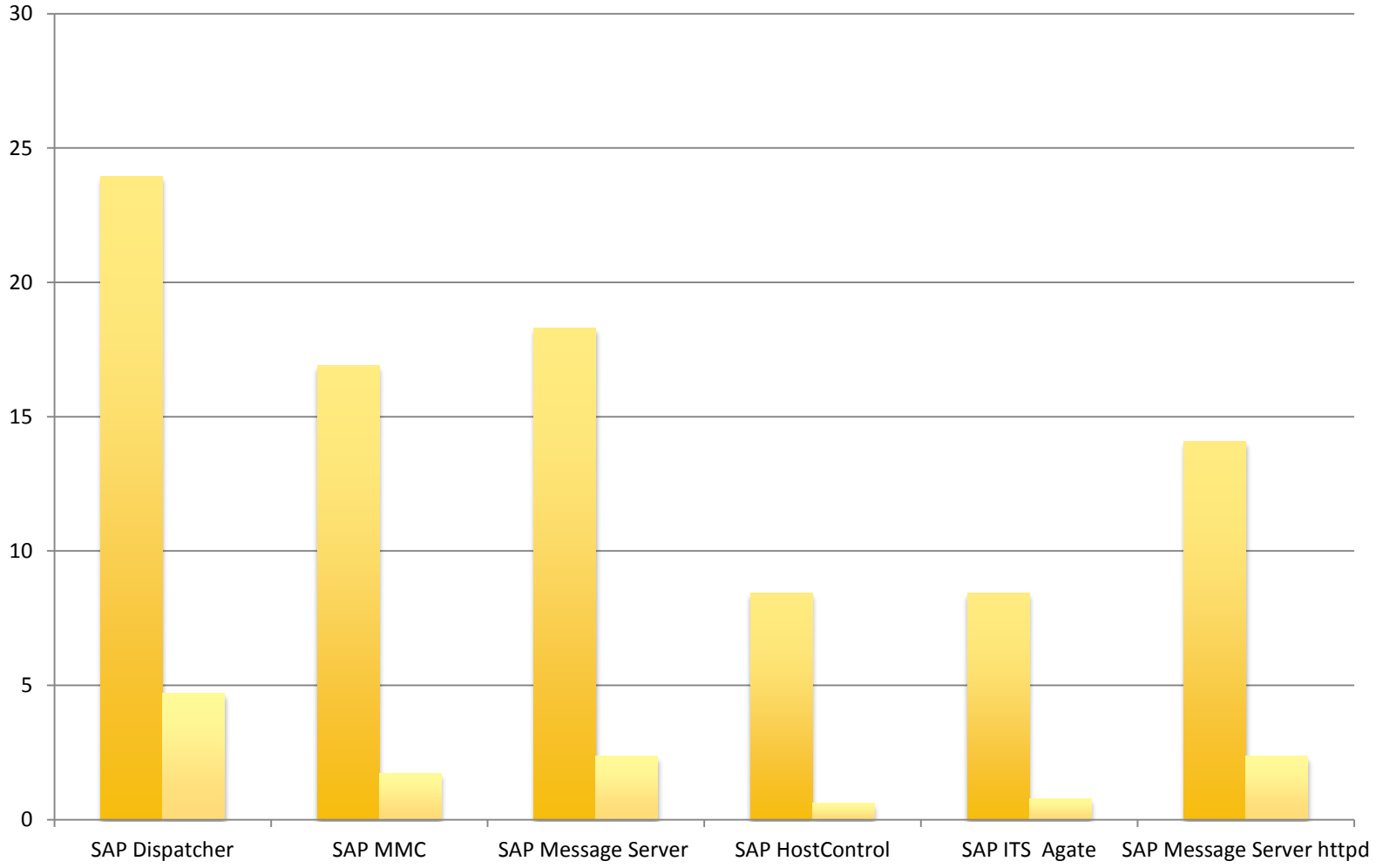


Port scan results



The listed services should not be accessible from the Internet

Singapore vs. Average



SAP HostControl service

- SAP HostControl is a service which allows remote control of SAP systems
- There are some functions that can be used remotely without authentication
- Issues:
  - Read developer traces with passwords
  - Remote command injection
- **About every 120th (was 20th) company is vulnerable REMOTELY**
- **About 35% systems assessed locally**

SAP Management console

- SAP MMC allows remote control of SAP systems
- There are some functions that can be used remotely without authentication
- Issues:
  - Read developer traces with passwords
  - Read logs with JsessionIDs
  - Read information about parameters
- **About every 40th (was 11th) company is vulnerable REMOTELY**
- **About 80% systems locally**
- To secure your system, use SAP Security Notes:
  - 927637: Web service authentication in sapstartsrv as of Release 7.00
  - 1439348: Extended security settings for sapstartsrv

SAP Message Server

- SAP Message Server – load balancer for App servers
- Usually, this service is only available inside the company
- By default, the server is installed on the 36NN port
- Issue:
  - Memory corruption
  - Information disclose
  - Unauthorized service registration (MITM)
- **About every 60th (was every 10th) company is vulnerable REMOTELY**
- **About 50% systems locally**

SAP Message Server HTTP

- HTTP port of SAP Message Server
- Usually, this service is only available inside the company
- By default, the server is installed on the 81NN port
- Issue: unauthorized read of profile parameters
  - Fixed by SAP Security Note 916398: HTTP access control for Message Server
- **About every 60th (was every 10th) company is vulnerable REMOTELY**
- **About 90% systems locally**

SAP Dispatcher service

- SAP Dispatcher - client-server communications
- It allows connecting to SAP NetWeaver using the SAP GUI application through DIAG protocol
- Should not be available from the Internet in any way
- Issues:
  - There are a lot of default users that can be used to connect and fully compromise the system remotely
  - Also, there are memory corruption vulnerabilities in Dispatcher
- **About every 20th (was 6th) company is vulnerable REMOTELY**
- To secure your system, use SAP Security Note:
  - 1741793: Potential remote termination of running work processes

But who actually tried to exploit it?

Known incidents related to SAP security and internal fraud

- Exploit market interest
- Anonymous attacks
- Insider attacks
- Evil subcontractors and ABAP backdoors

Market Interest

- Whitehat buyers and sellers
  - Companies like ZDI buy exploits for SAP
  - Only in 2012 ZDI publish 5 critical SAP issues
- Whitehat buyers and different sellers
  - Companies who trade 0-days say that there is interest from both sides
- Black market
  - Anonymous attack?
  - Why not?

Market Interest

Re: 0day remote vuln selling SAP / Linux Kernel / PHP etc...

From: Ferdinand Klinzer <Klinzer () gmx de>
Date: Thu, 8 Feb 2007 10:26:54 +0100

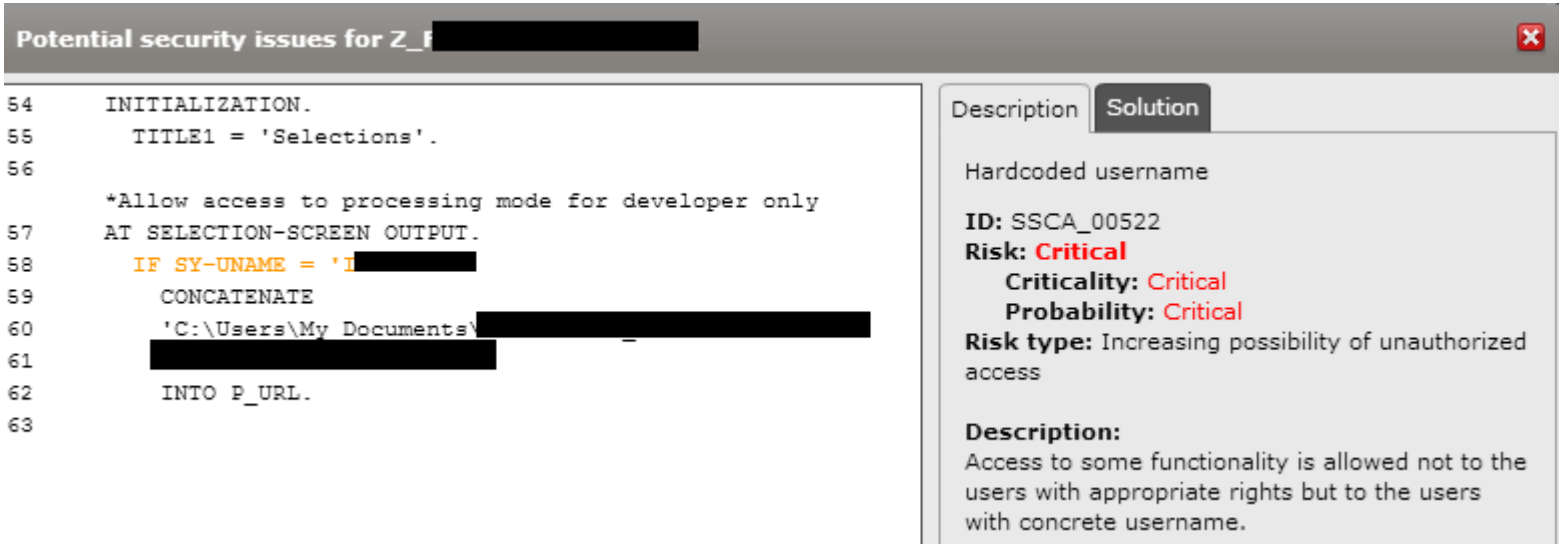
```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

So Snacker,

Where can i see your price list?
In euro or $ ?
```

Insider attacks

- The Association of Certified Fraud Examiners (**ACFE**) survey showed that U.S. organizations lose an estimated **7**% of annual revenues to fraud.
- Real examples that we met:
  - Salary modification
  - Material management fraud
  - Mistaken transactions

Evil subcontractors and ABAP Backdoors

- They exist!
- Sometimes, it is possible to find them



What has happened already?

- AutoCAD virus (Industrial espionage)
  - http://www.telegraph.co.uk/technology/news/9346734/Espionage-virus-sent-blueprints-to-China.html
- Internet-Trading virus (Fraud)
  - Ranbys modification for QUICK
  - http://www.welivesecurity.com/2012/12/19/win32spy-ranbyus-modifying-java-code-in-rbs/
- News resources hacking (Sabotage)
  - http://www.bloomberg.com/news/2013-04-23/dow-jones-drops-recovers-after-false-report-on-ap-twitter-page.html

What is next?

- Just imagine what could be done by breaking:
  - One SAP system
  - All SAP systems of a company
  - All SAP systems in a particular country
  - Everything

SAP strategy in app security

- Now security is the number 1 priority for SAP
- Implemented own internal security process SDLC
- Security summits for internal teams
- Internal trainings with external researchers
- Strong partnership with research companies
- Investments in automatic and manual security assessment of new and old software

Future threads and predictions

- Old issues are being patched, but a lot of new systems have vulnerabilities
- Number of vulnerabilities per year is going down compared to 2010, but they are more critical
- Number of companies which find issues in SAP is growing
- Still, there are many uncovered areas in SAP security
- SAP forensics can be a new research area because it is not easy to find evidence now, even if it exists

Forensics as a new trend for 2013

- If there are no attacks, it doesn't mean anything
- Companies don't like to share information about data compromise
- Companies are not capable of identifying attacks
  - Only 10% of systems use security audit at SAP
  - Only 2% of systems analyze them
  - Only 1% do correlation and deep analysis

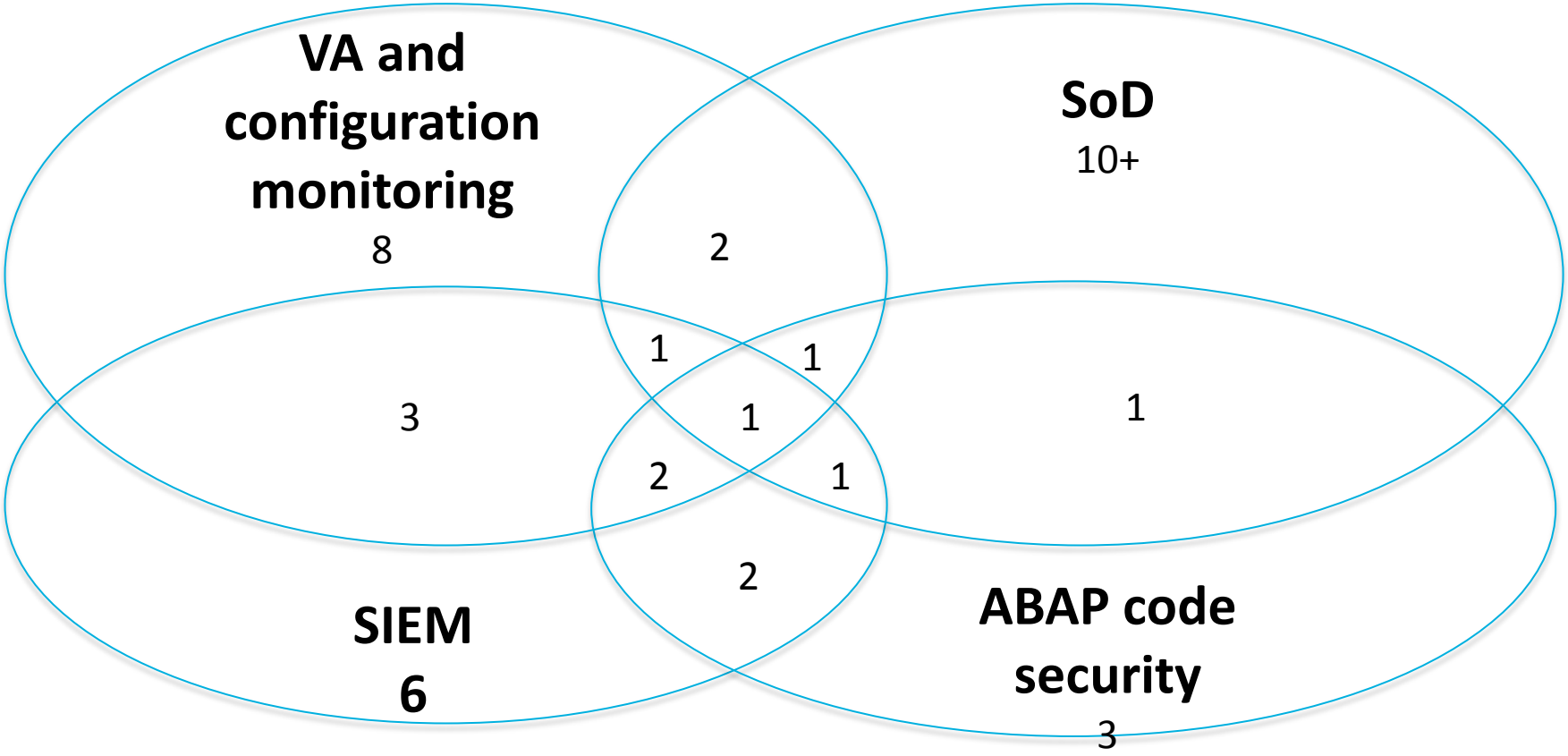
** Based on the assessment of over 250 servers of companies that allowed us to share results*.

Forensics as a new trend for 2013

- ICM log icm/HTTP/logging_0 70%
- Security audit log in ABAP 10%
- Table access logging rec/client 4%
- Message Server log ms/audit 2%
- SAP Gateway access log 2%

** Based on the assessment of over 250 servers of companies that allowed us to share results.*

SAP Security tools



* We did not compare the quality of the tools and their coverage. For example, SIEM capabilities for SAP can be found in many SIEM solutions, but they cover 10% of all log file types. The same applies to Vulnerability assessment: we collected tools that have general scan capabilities including SAP as well as only SAP related. SAP checks in those tools can amount to 10 to 7000.

Conclusion

- - The interest in SAP platform security has been growing exponentially, and not only among whitehats
- + SAP security in default configuration is getting much better now
- - SAP systems can become a target not only for direct attacks (for example APT) but also for mass exploitation
- + SAP invests money and resources in security, provides guidelines, and arranges conferences
- - unfortunately, SAP users still pay little attention to SAP security
- + I hope that this talk and the report that will be published next month will prove useful in this area

Conclusion

- Issues are everywhere

  but the risks and the price

  of mitigation are different

Future work

I'd like to thank SAP Product Security Response Team for their great cooperation to make SAP systems more secure. Research is always ongoing, and we can't share all of it today. If you want to be the first to see new attacks and demos, follow us at @erpscan and attend future presentations:

- **End of June – Release of "SAP Security in Figures 2013"**
- **July 30 –Talk and Exhibition at BlackHat USA (Las Vegas, USA)**
- **September 10-12 – BlackHat Trainings (Istanbul, Turkey)**

Questions?