Xu Jia, Andreas Wiegenstein

I know what you coded last summer

An analysis of 450 million lines of custom ABAP code

Troopers15 Conference (SAP Security Track) March 18, 2015

Agenda

1. SAP standard und custom development
2. Custom code statistics
3. Best Practices

#SAP
#Security
#Research

Andreas Wiegenstein

- CTO at Virtual Forge
- SAP Security Researcher, active since 2003
  - Received credit from SAP for > **75** reported 0-day vulnerabilities
- Various Publications, including **DSAG** and **BSI**
- Speaker at international Conferences
  - **Troopers, BlackHat**, **DeepSec**, **Hack in the Box**, **IT Defense, RSA, DSAG, SAP TechEd**

Xu Jia

- Security Analyst at Virtual Forge
- SAP Security Researcher, active since 2006
  - Received credit from SAP for > **30** reported 0-day vulnerabilities
- Speaker at international Conferences
  - **Troopers** (2013,2014,2015)**, Sicherheit und Prüfung von SAP Systemen** (2012)

SAP

Why protect SAP systems?

- More than 248,500 companies run SAP
- SAP customers …
  - Transport > 1.1 billion flight passengers per year
  - Produce > 65% of all TV's
  - Produce > 77,000 cars every day
  - Produce > 52% of all movies
- … and …
  - 72% of the world-wide beer production depends on companies that run SAP !!!

Quelle: http://www.posters.at/the-simpsons-homer-bier_a34273.html

SAP Custom Code - basics

(All) Customers change/enhance the SAP standard

- Internal development teams
- External development teams

The development guidelines of most customers focus on

- Naming conventions

The SAP standard delivers

- Rudimentary tools for static and dynamic code analysis
- No metrics regarding volume (Lines of Code)

SAP specifics

- SAP systems run independent of operating system and database
- SAP ships a proprietary front end: SAP GUI
- Access to business data requires specific regulations
  - Authorization checks
  - Maintaining change documents
- Data of different organizations (**"Clients"**) is stored (separately) in the same database schema
- Special ABAP command to execute authorization checks: **AUTHORITY-CHECK**
- Proprietary SQL layer between ABAP and the database: **Open SQL**
- Proprietary system-to-system communication: **RFC** (Remote Function Call)

What is the biggest risk with SAP systems?

Downtime

#Statistics

"There are three kinds of lies: lies, damned lies, and statistics."

(Benjamin Disraeli)

“Don’t trust statistics you didn’t falsify yourself.”

(Unknown)

Business Code Quality Benchmark

Ongoing project analyzing the entire ABAP code of **one** selected SAP system per company

- Results from 217 companies so far
  - With diverse quality assurance processes / maturity
  - Various (corporate) size
  - With a SAP history of different length
  - From various industry sectors and countries
- Based on static code analysis
  - Performance, Rosbustness, Security, Compliance
  - Only “critical” mistakes are considered in the statistics
- Data collection done in 2013 and 2014

Business Code Quality Benchmark

Statistics - General

Companies have on average 2.08 million lines of custom code per SAP system

- Companies don't run "pure" SAP standard solutions

The most common code module types are FORMs (procedures) with 64%, followed by methods (19%)

- Most custom code is therefore **difficult to reuse**

There are on average 14,500 additional input sources due to custom code per system

- Each input / data source increases the **attack surface** of a software

78% of all user input comes via SAP GUI applications

18% of all user input comes via RFC (Remote Function Call) communication

- Malicious insiders therefore have the highest chance to find SAP vulnerabilities

Statistics – General (2)

There are **more quality issues with database access than there is database access**

- There are on average 24,635 Open SQL queries in custom code
  (21,227 **read** accesses und 3,408 **write** accesses)
- There are on average **26,147** quality issues with Open SQL queries
  (distributed across all test areas)

Only 0.3% of all SAP modules are (directly) accessible via HTTP / Internet

- Security solutions like Web Application Firewalls have limited value in SAP installations

Statistics – Security and Compliance

There is **1 critical** security / compliance issue per **1,000 lines of code**

- A typical SAP system has therefore 2,151 security / compliance issues in custom code alone.

List of the 5 most common types of security and compliance issues:

Type of vulnerability	Probability *	Occurrences **
Authorization Flaw	100 %	1.056
Directory Traversal	91 %	308
Direct Database Modification	86 %	39
Cross-Client Access	83 %	122
Open SQL Injection	70 %	15

* Probability indicates in how many analyzed systems at least one issue of this type was found

** Occurrences reflect the absolute number of critical flaws detected per system on average.

Statistics – Security and Compliance (2)

DEMO

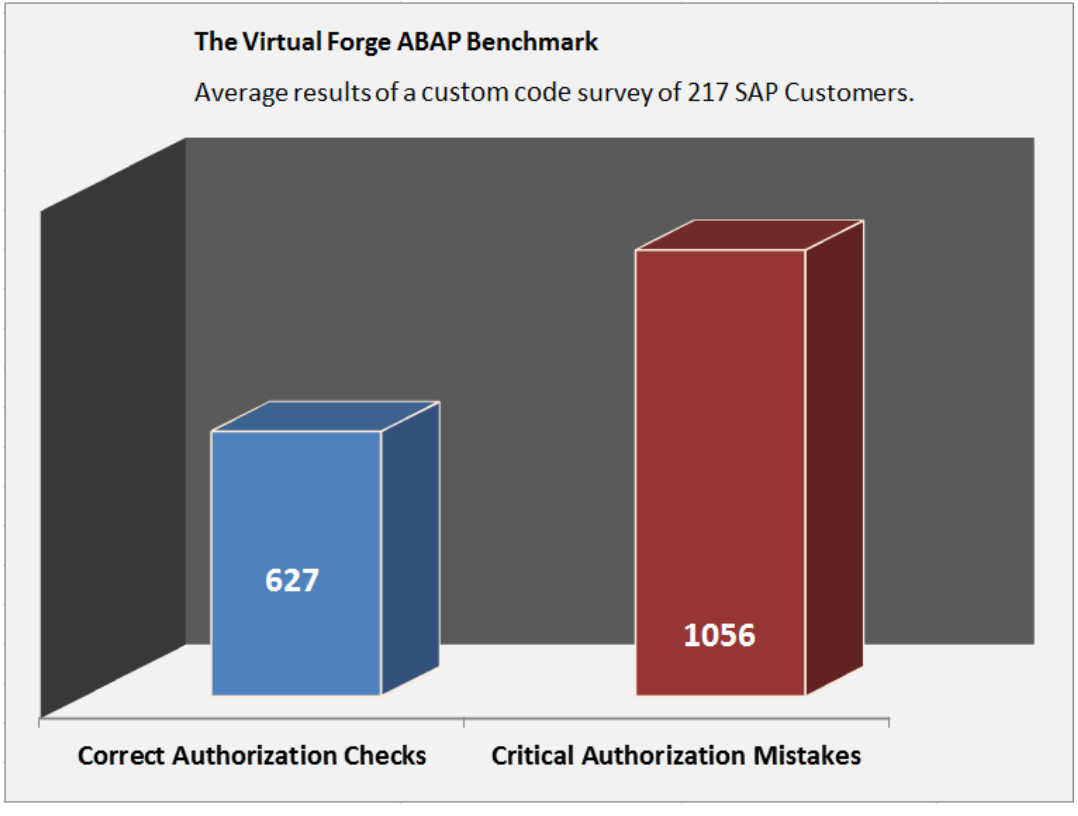
Out of the pool of critical issues, there are on average **10 vulnerabilities** per system that are so grave that a single exploit will result in **total system compromise**.

There are on average **184 proprietary authorization checks** based on **sy-uname** per system. The probability to encounter at least one proprietary authorization check is **91%**.

- „Red traffic light“ in financial audits

There are **476 RFC-enabled function modules** per system. **64%** of them are **completely lacking authority checks**.

Statistics – Security and Compliance (3)



#Best Practices

"A best practice is a method or technique that has consistently shown results superior to those achieved with other means, and that is used as a benchmark. In addition, a "best" practice can evolve to become better as improvements are discovered."

en.wikipedia.org

Best Practices

Conduct an awareness workshop for your **management**

- Without a binding process with management backup nothing will change

Set **achievable goals**

- No developer will learn 100 new secure coding practices over night

Device a plan how to deal with **legacy code**

- Corrections need time
- It's economically unviable to correct all issues

Best Practices (2)

Issue **meaningful** development guidelines

- For all relevant quality areas
- For internal **and** external development

Caution: Application security is difficult to understand for most developers

- **Regular trainings** are required in order to establish a sound security understanding

Leverage **tools** in order to check for compliance with your development guidelines

- You can only realise *testable* requirements
- Only tools will provide transparency where your company stands with regards to SAP code quality

Measure the **success** of your activities

- Success is the basis for long-term acceptance of a new process

Output

The Business Code Quality Benchmark (BCQB) by Virtual Forge is the first of its kind.

The results were used to provide guidance to companies depending on ABAP code:

- The BIZEC “APP/11” standard for ABAP security flaws is based on **BCQB**
- The BSI “ABAP Top 20 Security Risks” are based on the **BCQB**

BIZEC APP/11

BSI „ABAP Top 20“

Conclusion

If your company runs SAP, it has (statistically spoken) significant quality issues in custom code.

Your company is exposed to the following risks

- System downtime
- “Red lights” in financial / compliance audits
- Industrial Espionage
- Business data manipulation
- Backdoors

Next Steps

Next week

- Take part in our study: Business Code Quality Benchmark
- Receive a comprehensive report for one of your SAP systems

Next month

- Discuss the results with your management
- Optimize your development process

Next year

- Run you custom SAP applications more secure

Thank you for your attention.

Questions Now or later ?

@codeprofiler @xubcode

#ThingsWeFoundWhenPentestingSAP

Disclaimer

VIRTUALFORGE

VIRTUALFORGE

run your business safer