Andreas Wiegenstein and Xu Jia

VIRTUALFORGE
we harden your software

Ghost In The Shell

Troopers13, March 11th – 15th, Heidelberg

The researchers

VIRTUALFORGE
we harden your software

Andreas Wiegenstein

- SAP Security Researcher, active since 2003
  - Received Credits from SAP for more than 20 reported 0-day Vulnerabilities
- Speaker at international Conferences
  - **SAP TechEd** 2004 (USA & Europe) / 2005 (USA) / 2006 (USA), DSAG 2009
  - **BlackHat** 2011 (Europe), **Hack in the Box** 2011 (Europe)
  - **Troopers** 2011, 2012, 2013, **RSA** 2012 (USA), **IT Defense** 2013
- Co-Author of „Sichere ABAP Programmierung" (SAP Press)

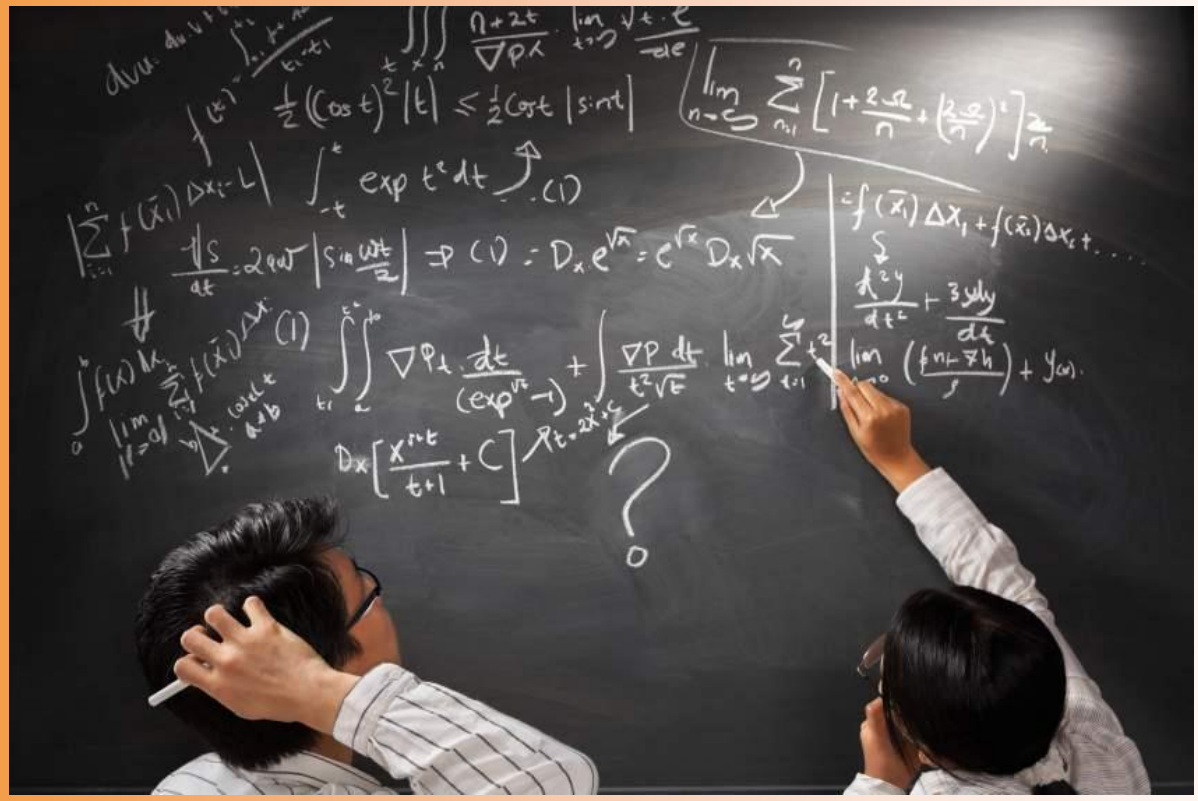
Xu Jia

- SAP Security Researcher, active since 2006
  - Received Credits from SAP for more than 15 reported 0-day Vulnerabilities
- Speaker at SAP-focused Conferences
  - **Sicherheit und Prüfung von SAP Systemen** 2012

CONTENTS

VIRTUALFORGE
we harden your software

SAP Technology Basics



Source: http://www.productiveflourishing.com/wp-content/uploads/2011/03/Simplifying-Complexity.jpg

SAP in (Business) Numbers

VIRTUALFORGE
we harden your software

Why protect SAP Systems?

- More than 176,000 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 !!!

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

SAP in (Technical) Numbers

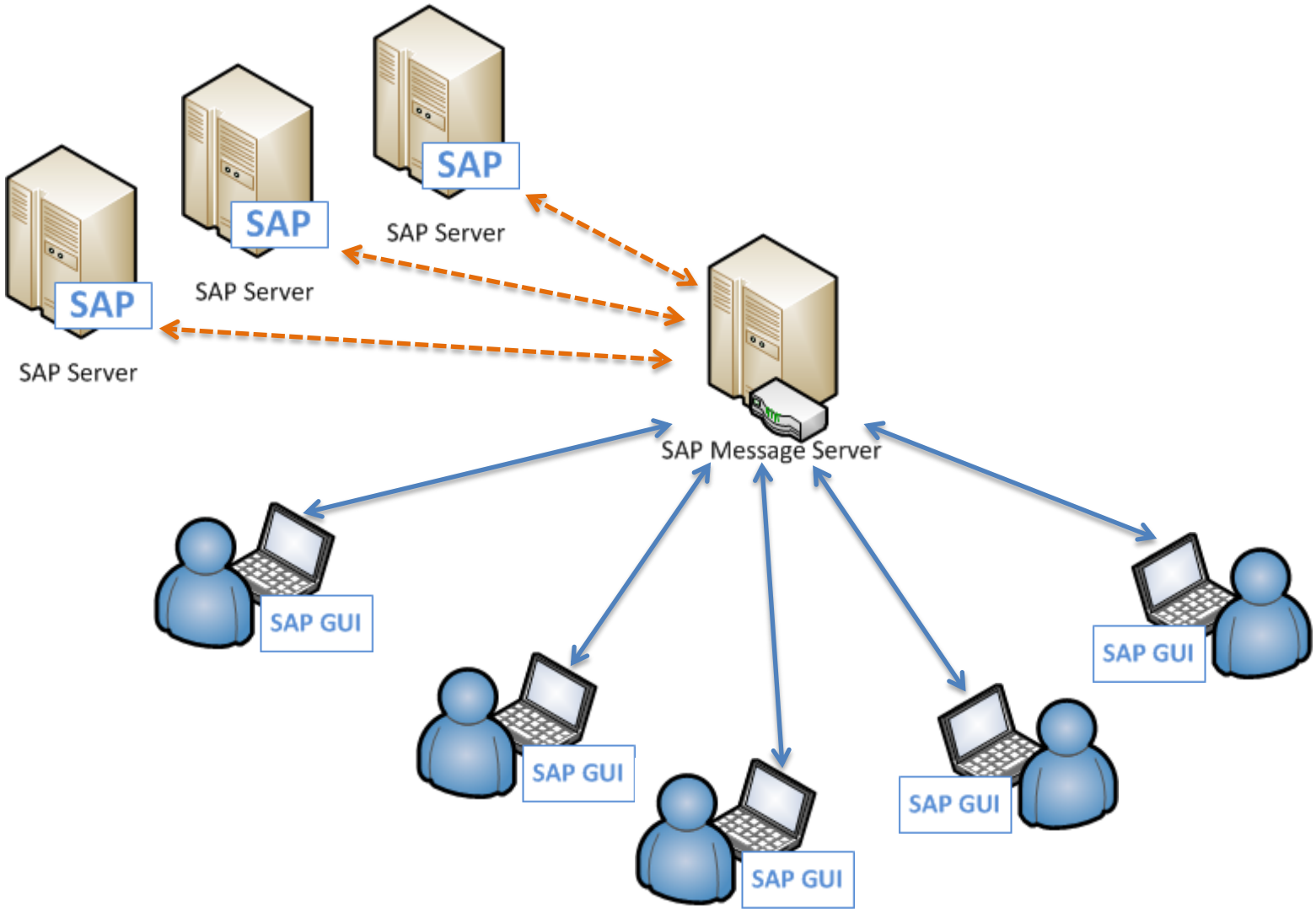
VIRTUALFORGE
we harden your software

How many … exist in Release … ?	Release	Answer
… DB tables	Basis 7.20	~ 81,000
*… SLOC**	Basis 7.20	~ 37.9 Mio
… Executable programs	Basis 7.20	~ 38,000
… DB tables	ECC 6.0	~ 384,000
*… SLOC**	ECC 6.0	~172.8 Mio
… Executable programs	ECC 6.0	~221,000

* SLOC = Source Lines of Code

Classic SAP Architecture

VIRTUALFORGE
we harden your software



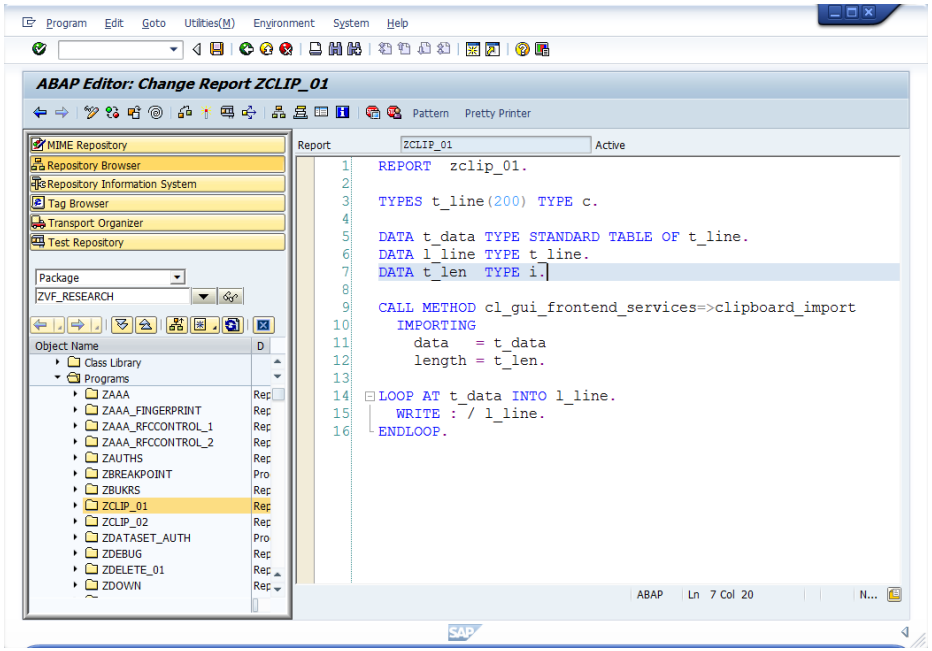
SAP GUI Users

VIRTUALFORGE
we harden your software

Who works with SAP GUI and why?

- Employees
  - Daily work

    (running multi-million $ Companies)
- Administrators
  - System Maintenance & Configuration
  - User Maintenance
- Developers
  - Write custom ABAP Code (extend standard Solutions)



In short:

- Users with a wide Range of Privileges work with SAP GUI.
- User Access to SAP Backend is still done via SAP GUI in 99% of the Cases

SAP GUI Application

VIRTUALFORGE
we harden your software

What is SAP GUI?

- Proprietary (Fat) Client
  - EXE Running on Windows (a Java Version is also available)
  - Access to Client OS (file system, shell, registry, clipboard, …)
  - Scriptable
- Proprietary Communication Protocol (DIAG)
  - Up- and download of files and data from screen elements
  - Data is transferred in a compressed format

Summary:

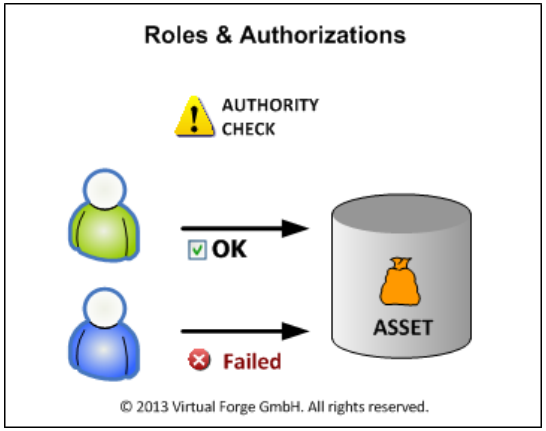
- SAP GUI is a powerful tool that manages data transfers between frontend and backend

SAP Security / Forensic Basics

VIRTUALFORGE
we harden your software

Roles and Authorizations

- Restrict User Access to Data and Business Logic

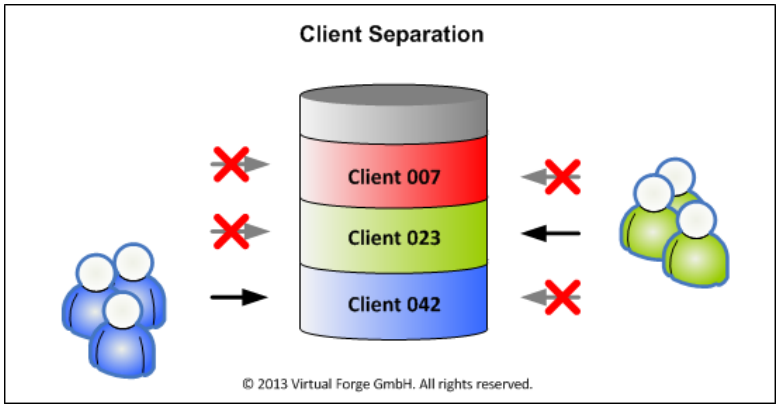


Accountability

- Log Changes to relevant Data
- Trace DB Access, Program Execution, …

Client Separation

- Protect Data of different Organizations on the same SAP System



Very few monitoring tasks are active all the time.

Audit Information System / Security Audit Log (should be active)

- (Failed) (Remote) Logon Events, Server Events
- Program execution, Debugging
- User maintenance
- …

System Trace (not active, due to high data volume)

- List of performed authorization checks and their results
- List of executed OSQL commands
- …

Ghost in The Shell

VF Advisory: **SAP-GHO-01**

SAP Note: 1529235

Advisory: 03.11.2010

Fix Date: 27.09.2011

CVSS Base Score: 6.0

CVSS Base Vector: AV:N/AC:M/AU:S/C:P/I:P/A:P

VF Advisories: **SAP-ZONE-01, SAP-ZONE-02**

SAP Note: 1560489

Advisory: 18.01.2011

Fix Date: 27.09.2011

CVSS Base Score: 6.0

CVSS Base Vector: AV:N/AC:M/AU:S/C:P/I:P/A:P

Mechanics of the Ghost

Passive Request Forgery (PRF)

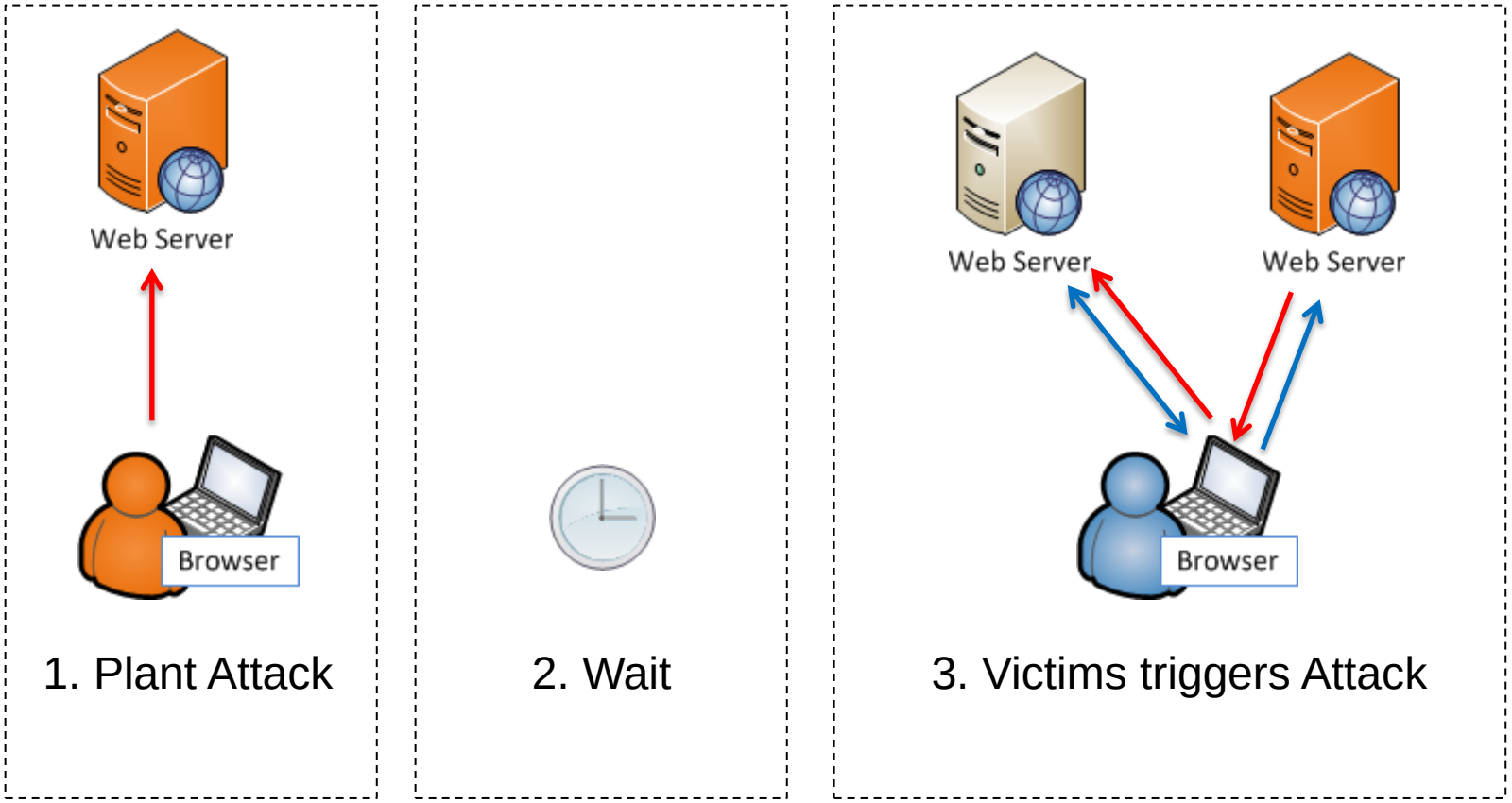
- Attack User Session through Trap
- Examples:
  - Cross-Site Request Forgery
  - Cross-Application Request Forgery (Troopers 2011)

Active Request Forgery (ARF)

- Attack User Session immediately
- Examples:
  - Ghost in the Shell

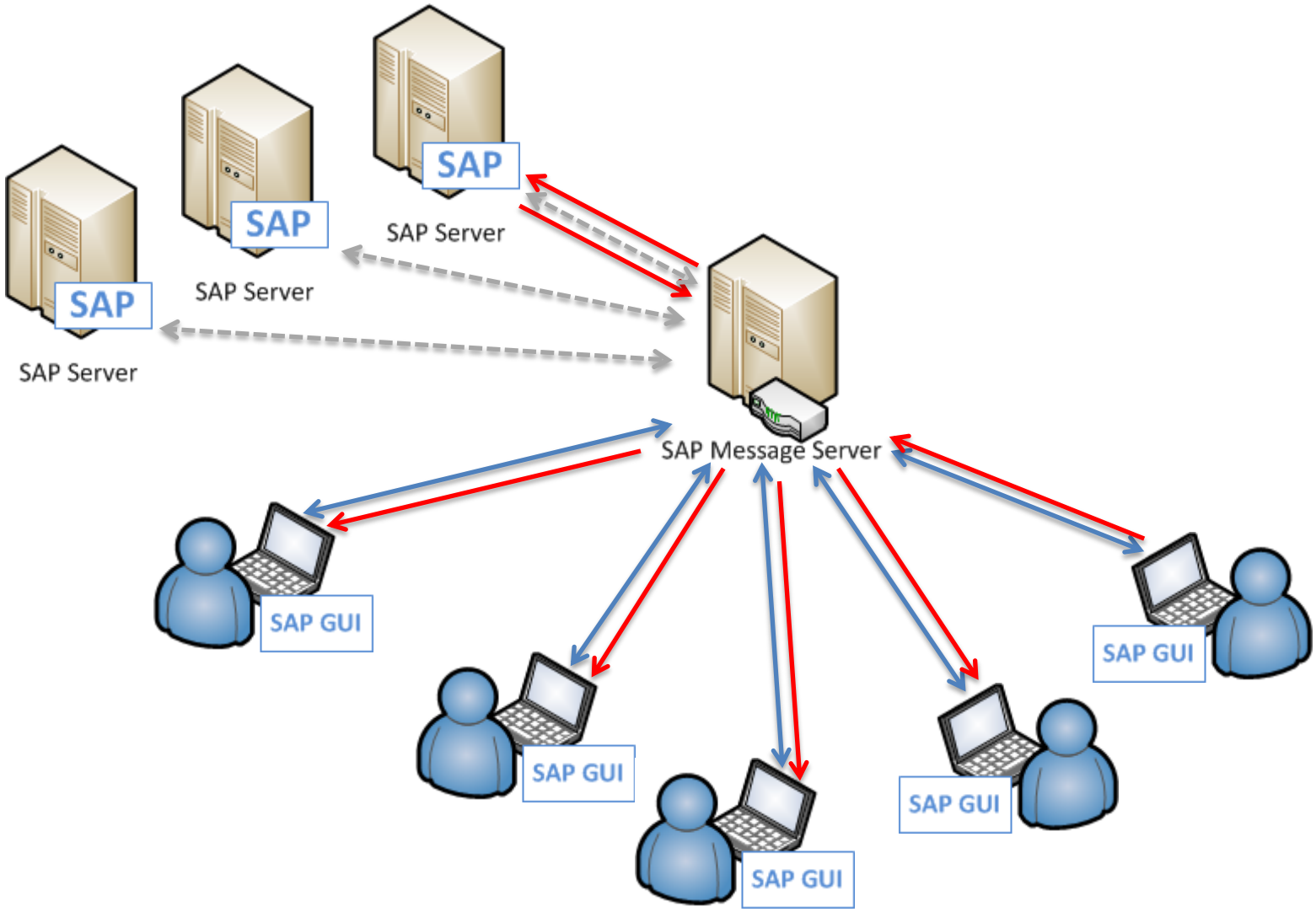
PRF is asynchronous. Be patient.

VIRTUALFORGE
we harden your software



ARF is synchronous. Much better!

VIRTUALFORGE
we harden your software



Summary

SAP Security Recommendations

VIRTUALFORGE
we harden your software

ABAP Security Resources

VIRTUALFORGE
we harden your software

Links

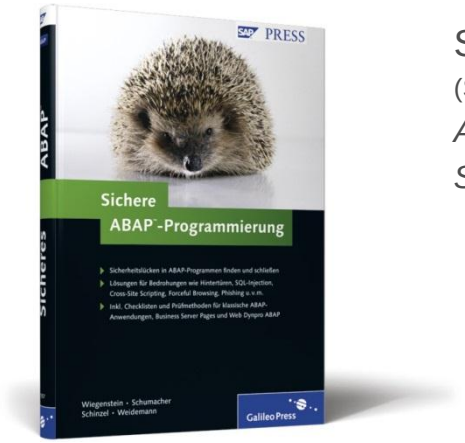
SAP Security Advisories researched by Virtual Forge
http://www.codeprofilers.com/index.php/advisories.html

Organizations

BIZEC
BUSINESS SECURITY

BIZEC – Business Security Initiative
http://www.bizec.org

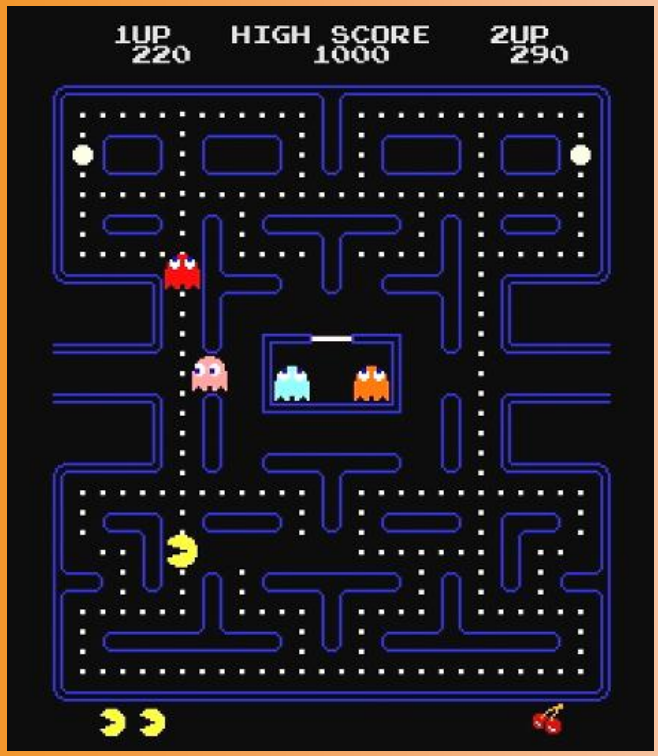
Literature



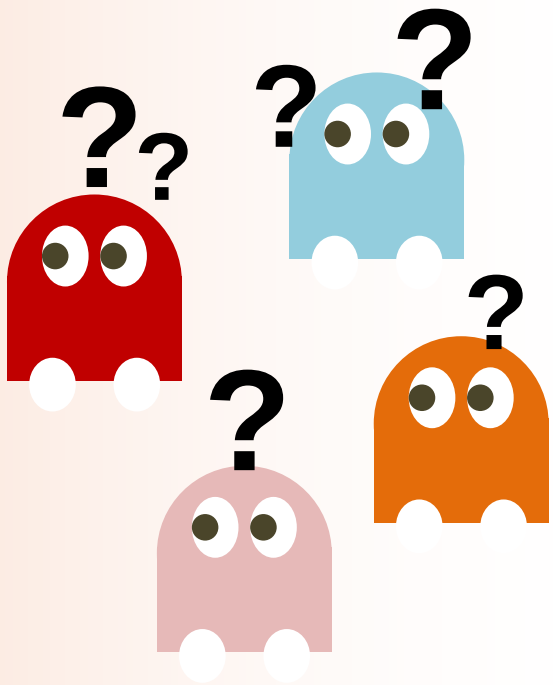
Sichere ABAP-Programmierung
(SAP PRESS, 372 S., 2009)
Andreas Wiegenstein, Markus Schumacher, Sebastian Schinzel, Frederik Weidemann

VIRTUALFORGE
we harden your software

Questions?



Source http://ostatic.com/pacman/screenshot/1



VIRTUALFORGE
we harden your software

Contact Information

VIRTUALFORGE GmbH

contact@virtualforge.com

Web: http://virtualforge.com

Phone: + 49 (0) 6221 86 89 00

Twitter: @codeprofiler

Disclaimer

SAP, R/3, ABAP, SAP GUI, SAP NetWeaver and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.

All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only.

The authors assume no responsibility for errors or omissions in this document. The authors do not warrant the accuracy or completeness of the information, text, graphics, links, or other items contained within this material. This document is provided without a warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

The authors shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of this document or the consumption of beer.