Andreas Wiegenstein

VIRTUALFORGE
we harden your software

SAP GUI Hacking (V1.0)

Troopers Conference 2011, Heidelberg

Who am I

VIRTUALFORGE
we harden your software

Andreas Wiegenstein

- CTO and founder of Virtual Forge, responsible for R&D
- SAP Security Researcher, active since 2003
- Speaker at SAP TechEd 2004, 2005, 2006, DSAG 2009, BlackHat 2011
- Co-Author of "Secure ABAP Programming" (SAP Press)

Virtual Forge GmbH

- SAP security product company based in Heidelberg, Germany
- Focus on (ABAP) application security services
  - ABAP Security Scanner
  - ABAP Security Guidelines
  - ABAP Security Trainings
  - SAP Security Consulting

Belief: "Our SAP system is secure."

VIRTUALFORGE
we harden your software

- Roles & Authorizations
- Segregation of Duties
- Secure Configuration & System / Service Hardening
- Encryption
- Secure Network Infrastructure
- Password Policies
- Patch Management
- Identity Management
- Single Sign-on

Reality-Check

VIRTUALFORGE
we harden your software

"...and this is our ABAP security department."

VIRTUALFORGE
we harden your software

1. ABAP, the SAP GUI and everything

- Proprietary language, exact specification not (freely) available
- Platform-independent code
- Client separation built-in
- Integrated auditing capabilities
- System-to-System calls via SAP Remote Function Call (RFC)
- Client-Server communication via SAP GUI (DIAG protocol)
- Various programming paradigms:
  - Programs & Forms, Reports, Function Modules, Dynpros
  - Classes & Methods, Business Server Pages, Web Dynpro ABAP
- Integrated platform-independent SQL Standard: Open SQL
- Built-in authentication, roles and (explicit) authorization model
- Thousands of well-known standard programs and database tables
- 150+ Million Lines of Code in an ECC6.0 System

SAP GUI

VIRTUALFORGE
we harden your software

- Proprietary fat client, provided and maintained by SAP
- Available as Windows executable and Java application
- Client-Server Communication via DIAG protocol
- DIAG can be encrypted with SNC, but is only compressed by default
- Renders ABAP Dynpros and is the default SAP user interface
- Provides methods to interchange files with the SAP application server
- Execution of screen-events can be scripted

VIRTUALFORGE
we harden your software

2. SAP GUI Attacks originating from the Server

ABAP Functions that access the SAP GUI client

VIRTUALFORGE
we harden your software

- Function Module `WS_EXECUTE`
  - Executes an operating system command on the client
- Function Module `GUI_UPLOAD`
  - Uploads a file from the Client to the Server
- Function Module `GUI_DOWNLOAD`
  - Downloads a file from the Server to the Client
- Class `CL_GUI_FRONTEND_SERVICES`
  - Provides various other functions
    - Directory listing, access to clipboard, etc
- Underlying ABAP Commands
  - `CALL METHOD OF`
  - `CALL` *`cfunc`*

DEMO

Mitigation(s)

VIRTUALFORGE
we harden your software

- Install SAP GUI 7.20
  - Restrict access to client-side ressources
- New security center in SAP GUI for Windows 7.20

  (https://service.sap.com/sap/support/notes/1483525)

- More on SAP GUI Security
  - "Secure Configuration SAP Netweaver Application Server ABAP"
  - https://service.sap.com/~sapidb/011000358700000968282010E.pdf

VIRTUALFORGE
we harden your software

3. SAP GUI Attacks originating from the Client

Client-side Manipulations

VIRTUALFORGE
we harden your software

- Forceful Browsing in SAP GUI !
  - Manipulate disabled fields and buttons
- Cross-Site Scripting in SAP GUI applications !!!
  - Not nice, but rare
- SAP GUI scripting
  - Scripting of SAP GUI events

DEMO

Mitigation(s)

VIRTUALFORGE
we harden your software

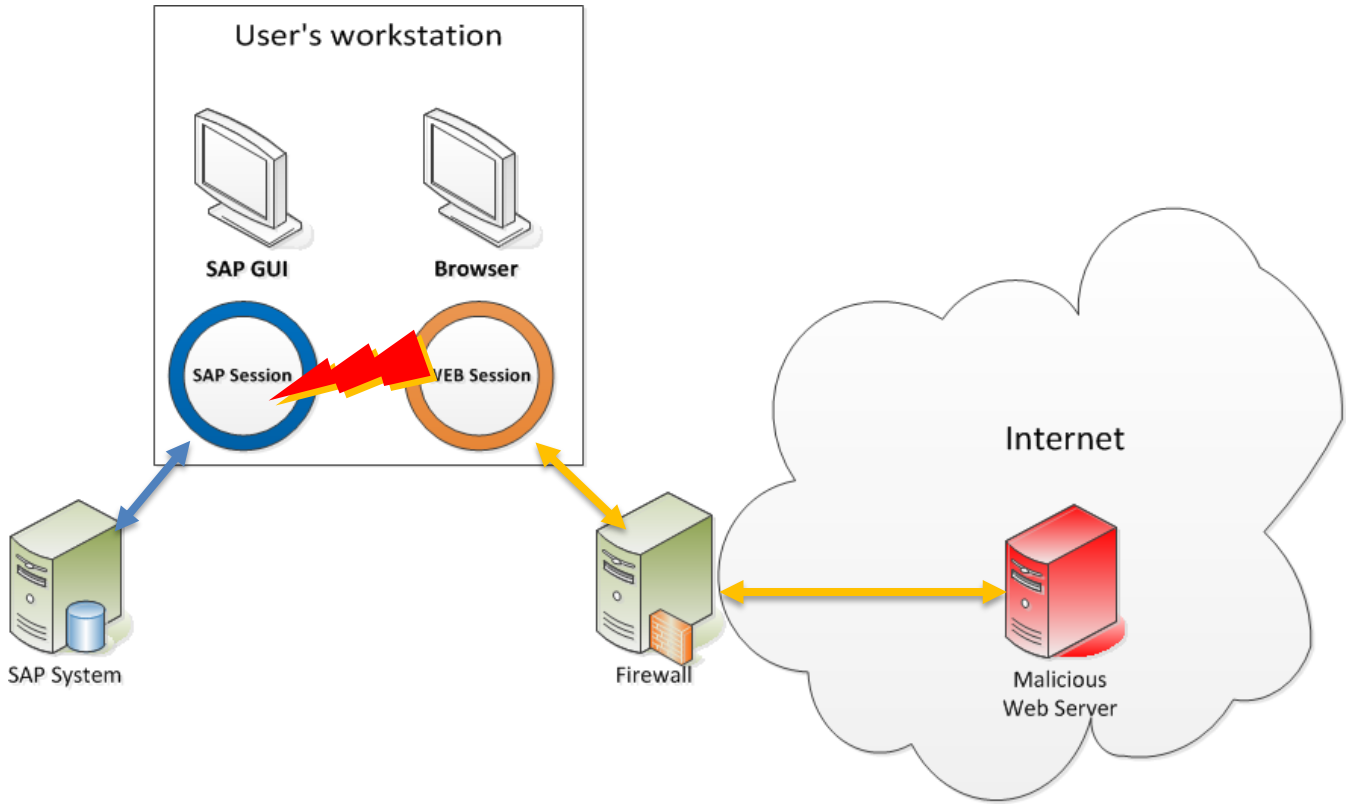
- Do not transport important data by client-roundtrips
- Make sure you use HTMLViewer Control (`CL_DD_DOCUMENT`) securely
- Disable SAP GUI scripting
  - See "SAP GUI Scripting Security Guide"
  - http://www.sdn.sap.com/irj/scn/index?rid=/library/uuid/3099a575-9cf4-2a10-9492-9838706b9262

VIRTUALFORGE
we harden your software

4. SAP GUI Attacks originating from the Internet

VIRTUALFORGE
we harden your software

- Cross-Application Request Forgery with SAP Shortcuts
  - Allows malicious Web sites to fire SAP GUI events



DEMO

Mitigation(s)

VIRTUALFORGE
we harden your software

- Read SAP Security Notes 1397000 & 1526048
  - (https://service.sap.com/sap/support/notes/1397000)
  - (https://service.sap.com/sap/support/notes/1526048)

SAP / ABAP Security Information

VIRTUALFORGE
we harden your software

Organizations

BIZEC
BUSINESS SECURITY

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

Literature

"Secure ABAP-Programming"
(German only)
SAP Press 2009

If you find new zero days

secure@sap.com

VIRTUALFORGE
we harden your software

Questions?

http://www.VIRTUALFORGE.com

Andreas.Wiegenstein@virtualforge.com

VirtualForge GmbH
Speyerer Straße 6
69115 Heidelberg
Deutschland

Phone: + 49 (0) 6221 86 89 0 - 0
Fax: + 49 (0) 6221 86 89 0 - 101

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 author assumes no responsibility for errors or omissions in this document. The author does 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 author 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.