Testing Security Properties of Web Services

Achim D. Brucker
achim.brucker@sap.com
joint work with
Lukas Brügger (ETH Zurich)

SAP AG, SAP Research, Security & Trust
Vincenz-Priessnitz-Str. 1, 76131 Karlsruhe, Germany

May, 2nd

Abstract

Today's large enterprise systems are service-oriented, i. e., they are built by composing independent components, called services, that encapsulate a certain business functionality. Service-oriented enterprise system impose many challenges in general and in particular with respect to their security. The dynamic nature of service-oriented systems as well as the fact that a service-oriented system is usually composed out of services from many different providers, makes these system a particular interesting target for model-based or specification-based testing approaches.

In this talk, we will motivate the challenges of testing service-oriented systems in general and, in particular, we will present an approach for modeling and (conformance) testing security policies for Web services. Our approach is based on previous work in using HOL-TestGen for conformance testing of security policies.

Agenda

1 Motivation and Introduction

2 Testing Web Services 101

3 Case study: A Simple Health Record Service

4 Future Work: Web Service Compositions

5 SAP Research

Has Sony been Hacked this Week?

http://hassonybeenhackedthisweek.com/

Time-line of the Sony Hack(s) (excerpt):

2011-04-20	Sony PSN goes down
2011-05-21	Sony BMG Greece: data of 8300 users leaked
2011-05-23	Sony Japanese database leaked
2011-05-24	Sony Canada: roughly 2,000 leaked
2011-06-05	Sony Pictures Russia
2011-06-06	Sony Portugal
2011-06-20	20th breach within 2 months, 177k email addresses leaked

(http://hassonybeenhackedthisweek.com/history)

Has Sony been Hacked this Week?

`http://hassonybeenhackedthisweek.com/`

Time-line of the Sony Hack(s) (excerpt):

2011-04-20	Sony PSN goes down
2011-05-21	Sony BMG Greece: data of 8300 users leaked
2011-05-23	Sony Japanese database leaked
2011-05-24	Sony Canada: roughly 2,000 leaked
2011-06-05	Sony Pictures Russia
2011-06-06	Sony Portugal
2011-06-20	20th breach within 2 months, 177k email addresses leaked

(http://hassonybeenhackedthisweek.com/history)

Consequences:

- account data of close to 100 million individuals exposed
- over 12 million credit and debit cards compromised
- more than 55 class-action lawsuits
- costs of $ 170 million only in 2011

Costs of Computer Hacks

TJX Company, Inc. (2007)	$ 250 million
Sony (2011)	$ 170 million
Heartland Payment Systems (2009)	$ 41 million

> A hack not only costs a company money, but also its **reputation** and the **trust** of its customers. It can take years and millions of dollars to repair the damage that a single computer hack inflicts.

(http://financialedge.investopedia.com/financial-edge/0711/Most-Costly-Computer-Hacks-Of-All-Time.aspx)

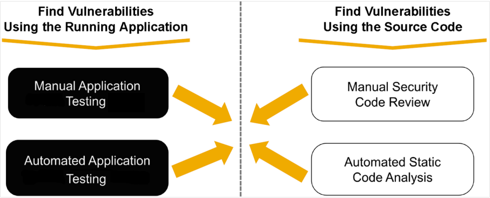
Observation

The two main causes are:

- “bad” programming
  resulting in: SQL Injections, XSS, backdoors, . . .
- configuration errors:
  inactive access control, data leakage, . . .

Countermeasures:

- (Security) Training
- Static (source code) analysis
- (Specification-based) Testing


Find Vulnerabilities
Using the Running Application
Find Vulnerabilities
Using the Source Code
Manual Application Testing
Automated Application Testing
Manual Security Code Review
Automated Static Code Analysis

SAP RESEARCH

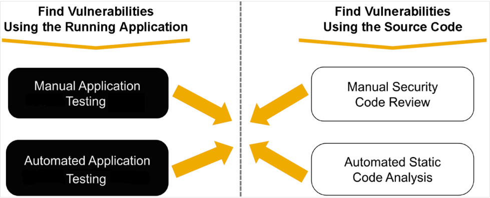
Observation

The two main causes are:

- "bad" programming
  resulting in: SQL Injections, XSS, backdoors, . . .
- configuration errors:
  inactive access control, data leakage, . . .

Countermeasures:

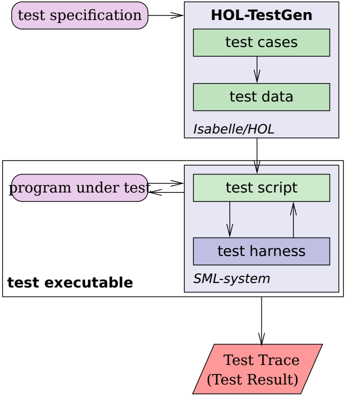
- (Security) Training
- Static (source code) analysis
- (Specification-based) Testing


Find Vulnerabilities
Using the Running Application
Find Vulnerabilities
Using the Source Code
Manual Application Testing
Automated Application Testing
Manual Security Code Review
Automated Static Code Analysis

SAP RESEARCH

HOL-TestGen

- HOL-TestGen:
  - specification-based testing
  - based on Isabelle/HOL
- HOL (Higher-order Logic):
  - “Functional PL with Quantifiers”
  - plus libraries on Sets, Lists, . . .
- Interactive User Interface:
  - user interface of Isabelle
- Test harness/driver
  - automatically generated for SML
  - others via foreign language interface
- Applications:
  - Unit testing
  - Sequence testing
  - Security policies (firewall policies)



SAP RESEARCH

The HOL-TestGen Workflow

The HOL-TestGen workflow is basically fivefold:

1. *Step I:* writing a test theory (in HOL)
2. *Step II:* writing a test specification
   (in the context of the test theory)
3. *Step III:* generating a test theorem (roughly: testcases)
4. *Step IV:* generating test data
5. *Step V:* generating a test script

And of course:

- building an executable test driver
- and running the test driver

SAP RESEARCH

A Simple Test Theory

```
theory List_test
imports Main begin
  consts is_sorted:: "('a::ord) list ⇒bool"
  primrec "is_sorted []      = True"
          "is_sorted  (x#xs) = case xs of
                                   []  ⇒ True
                                 | y#ys ⇒((x < y) ∨(x = y))
                                         ∧ is_sorted xs"

  test_spec "is_sorted (prog (l::('a list)))"
    apply(gen_test_cases prog)
  store_test_thm "test_sorting"

  gen_test_data "test_sorting"
  gen_test_script "test_lists.sml" list" prog
end
```

Agenda

1 Motivation and Introduction

2 Testing Web Services 101

3 Case study: A Simple Health Record Service

4 Future Work: Web Service Compositions

5 SAP Research

Today’s World is Distributed

Modern applications are built

- by composing (black-box) services
- are re-composing happens relatively often
- require complex security configurations

There are

- widely adopted standards (e. g., WSDL)
- powerful frameworks for building Web Services

Idea:

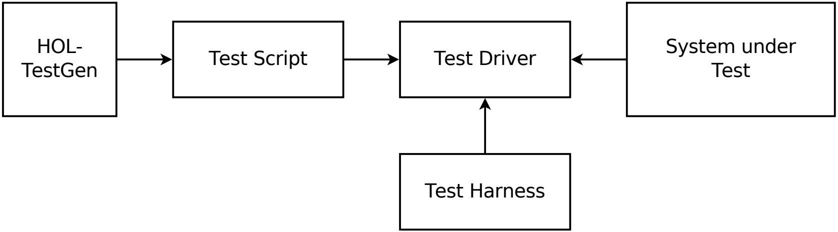
- Let’s try to apply HOL-TestGen in this scenario

Necessary steps:

- model Web Service Application API in HOL
- connect HOL-TestGen to a Web service Framework

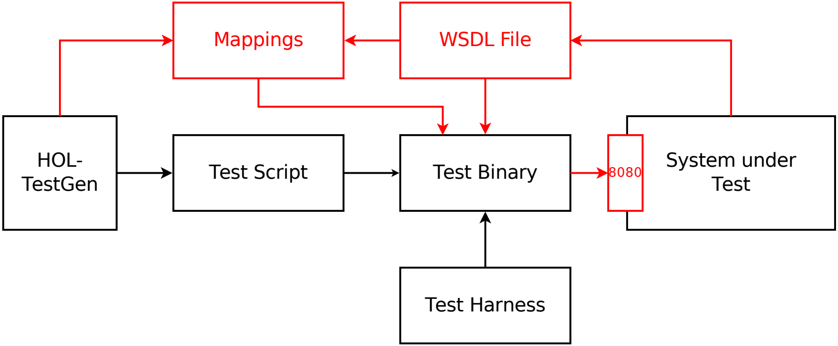
SAP RESEARCH

Local Testing Setup



SAP RESEARCH

Remote Testing Setup



Provide support for the .net/mono framework:

- Add support for F# code generator to Isabelle (HOL-TestGen)
- Develop Test Harness in F#
- Use the WSDL toolchain for C# (F# not stable yet)

SAP RESEARCH

Agenda

1 Motivation and Introduction

2 Testing Web Services 101

3 Case study: A Simple Health Record Service

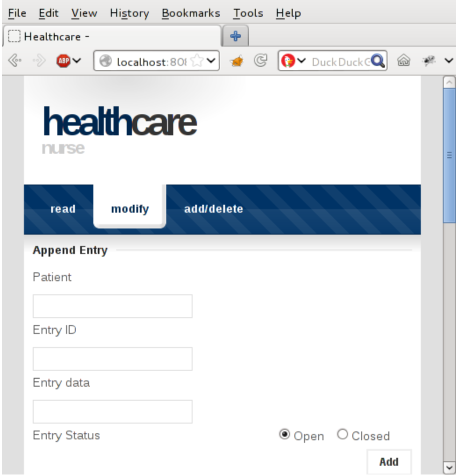
4 Future Work: Web Service Compositions

5 SAP Research

SAP RESEARCH

Case Study: Overview

- HealthCare web service
- Policy conformance testing
- Data handled:
  - Summary care records
  - Entries
  - Legitimate Relationships



Append Entry

Patient

Entry ID

Entry data

Entry Status ● Open ○ Closed

Add

Case Study: Policy

- Role-based access control
  - Nurse
  - Clinical practitioner
  - Clerical
- Legitimate relationships
- Sealed envelopes

Demo: Unit Test Scenario

Three users:

- Alice: Nurse
- Bob: Clinical Practitioner
- Charlie: Clerical

Example test case:

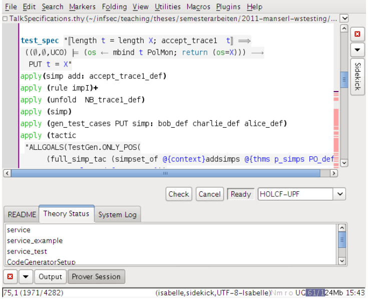
- createSCR Charlie Smith
- addLR Charlie Smith 0 {Bob, Charlie}
- appendEntry Bob Smith (Open, 1, "Entry content")
- readSCR Bob Smith
- readEntry Alice Smith 1

Demo: Sequence Test Scenario

Test specification:

- 1st operation: createSCR
- 2nd operation: addLR
- 3rd operation: appendEntry
- 4th operation: readEntry or readSCR

⇒ 88 generated test data


File Edit Search Markers Folding View Utilities Macros Plugins Help
□ TalkSpecifications.thy (~/infsec/teaching/theses/semesterarbeiten/2011-manserl-wstesting/...
Sidekick

```
test_spec "⟦length t = length X; accept_trace1  t⟧ ⟹
 ((∅,∅,UC0) ⊨ (os ← mbind t PolMon; return (os=X))) ⟶
  PUT t = X"
apply(simp add: accept_trace1_def)
apply (rule impI)+
apply (unfold  NB_trace1_def)
apply (simp)
apply (gen_test_cases PUT simp: bob_def charlie_def alice_def)
apply (tactic
 "ALLGOALS(TestGen.ONLY_POS(
      (full_simp_tac (simpset_of @{context}addsimps @{thms p_simps PO_def
```

Check
Cancel
Ready
HOLCF-UPF
README
Theory Status
System Log

service
service_example
service_test
CodeGeneratorSetup

75,1 (1971/4282) (isabelle,sidekick,UTF-8-Isabelle)Nm r o UG 61/124Mb 15:43

SAP RESEARCH

Agenda

1 Motivation and Introduction

2 Testing Web Services 101

3 Case study: A Simple Health Record Service

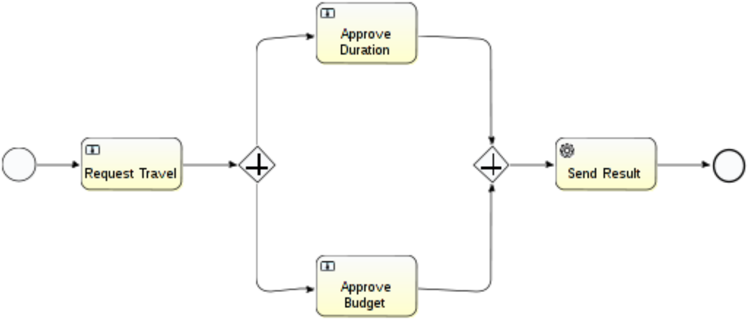
4 Future Work: Web Service Compositions

5 SAP Research

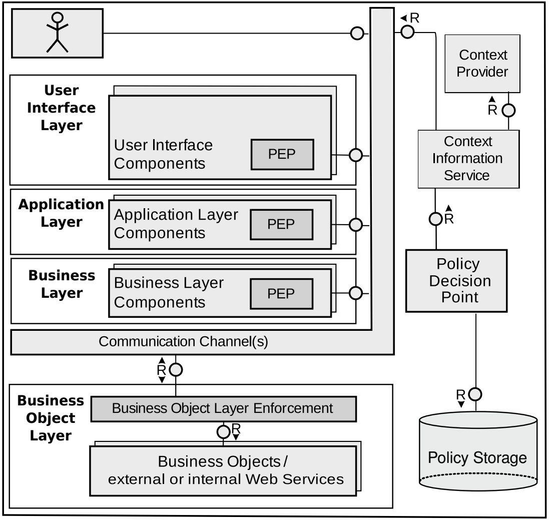
SAP RESEARCH

Web Service Compositions

Many Applications are process-driven



A Typical SOA/Process-based Architecture

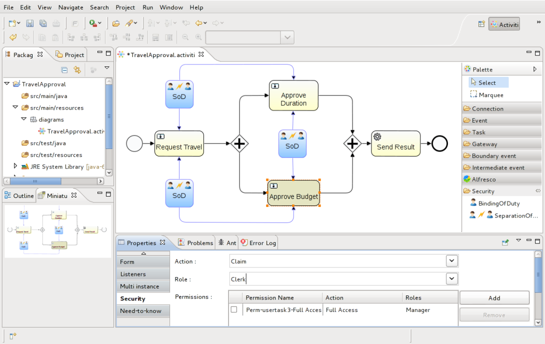

R
Context Provider
R
User Interface Layer
User Interface Components
PEP
Context Information Service
R
Application Layer
Application Layer Components
PEP
Policy Decision Point
Business Layer
Business Layer Components
PEP
Communication Channel(s)
R
R
Business Object Layer
Business Object Layer Enforcement
R
Business Objects / external or internal Web Services
Policy Storage

SAP RESEARCH

Using BPMN Models for Testing

Integrating HOL-TestGen and a BPMN tool provides a

- graphical way of writing test specifications
- interactive way of exploring the test space / test cases (coverage!)



Action : Claim

Role : Clerk

Permissions :

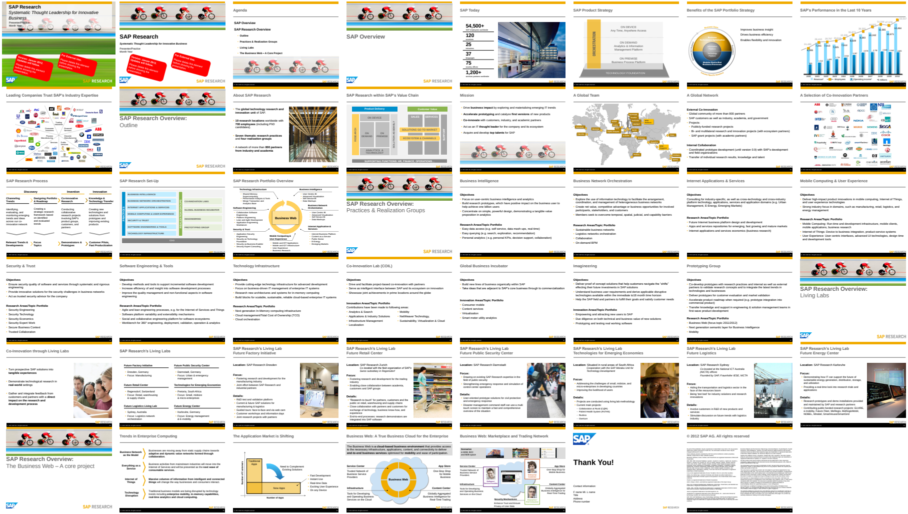
	Permission Name	Action	Roles
□	Perm-usertask3-Full Acces	Full Access	Manager

SAP RESEARCH

Outline

1. Motivation and Introduction
2. Testing Web Services 101
3. Case study: A Simple Health Record Service
4. Future Work: Web Service Compositions
5. SAP Research

SAP Research: An Overview


SAP Research
Systematic Thought Leadership for Innovative Business
SAP Research
Agenda
SAP Overview
SAP Today
SAP Product Strategy
Benefits of the SAP Portfolio Strategy
SAP's Performance in the Last 10 Years
Leading Companies Trust SAP's Industry Expertise
SAP Research Overview: Outline
About SAP Research
SAP Research within SAP's Value Chain
Mission
A Global Team
A Global Network
A Selection of Co-Innovation Partners
SAP Research Process
SAP Research Set-Up
SAP Research Portfolio Overview
SAP Research Overview: Practices & Realization Groups
Business Intelligence
Business Network Orchestration
Internet Applications & Services
Mobile Computing & User Experience
Security & Trust
Software Engineering & Tools
Technology Infrastructure
Co-Innovation Lab (COIL)
Global Business Incubator
Imagineering
Prototyping Group
SAP Research Overview: Living Labs
Co-Innovation through Living Labs
SAP Research's Living Labs
SAP Research's Living Lab Future Factory Initiative
SAP Research's Living Lab Future Retail Center
SAP Research's Living Lab Future Public Security Center
SAP Research's Living Lab Technologies for Emerging Economies
SAP Research's Living Lab Future Logistics
SAP Research's Living Lab Future Energy Center
SAP Research Overview: The Business Web – A core project
Trends in Enterprise Computing
The Application Market is Shifting
Business Web: A True Business Cloud for the Enterprise
Business Web: Marketplace and Trading Network
Thank You!
© 2012 SAP AG. All rights reserved

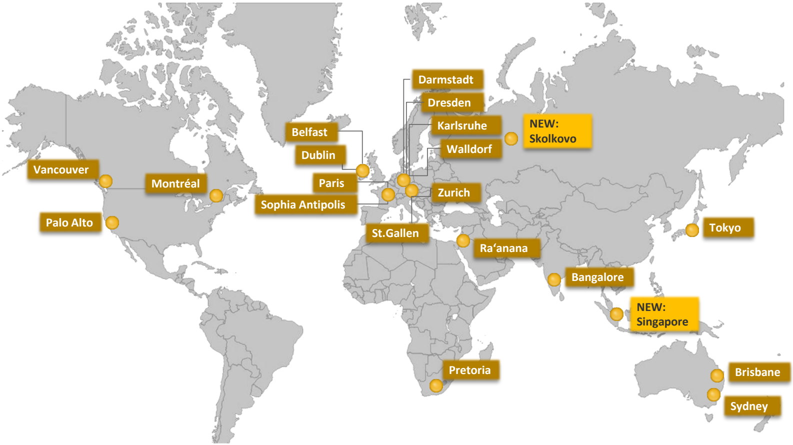
SAP RESEARCH

About SAP Research

- The global technology research and innovation unit of SAP.
- 19 research locations worldwide with 700 employees (SAP: > 54 500).
- Seven thematic research practices and four realization groups
- A network of more than 800 partners from industry and academia

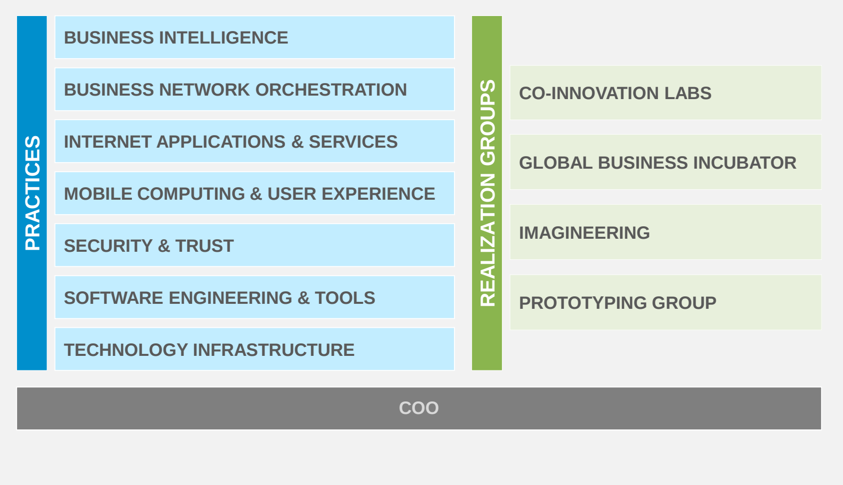
SAP RESEARCH

SAP Research Locations



SAP RESEARCH

SAP Research Set-up



PRACTICES

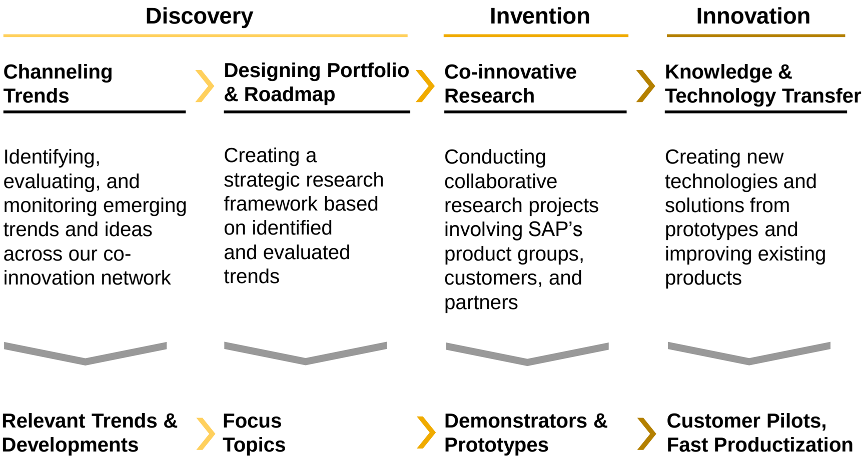
- BUSINESS INTELLIGENCE
- BUSINESS NETWORK ORCHESTRATION
- INTERNET APPLICATIONS & SERVICES
- MOBILE COMPUTING & USER EXPERIENCE
- SECURITY & TRUST
- SOFTWARE ENGINEERING & TOOLS
- TECHNOLOGY INFRASTRUCTURE

REALIZATION GROUPS

- CO-INNOVATION LABS
- GLOBAL BUSINESS INCUBATOR
- IMAGINEERING
- PROTOTYPING GROUP

COO

SAP Research Process



Discovery

Channeling Trends

Identifying, evaluating, and monitoring emerging trends and ideas across our co-innovation network

Relevant Trends & Developments

Designing Portfolio & Roadmap

Creating a strategic research framework based on identified and evaluated trends

Focus Topics

Invention

Co-innovative Research

Conducting collaborative research projects involving SAP’s product groups, customers, and partners

Demonstrators & Prototypes

Innovation

Knowledge & Technology Transfer

Creating new technologies and solutions from prototypes and improving existing products

Customer Pilots, Fast Productization

SAP RESEARCH

Research vs. Development

An Exaggerating and Simplified View

	Research	Development
Time horizon:	3–5 years	0.5 years
Work mode:	“it’s ready, when it’s ready”	SCRUM with 4 week tacts
Technologies:	no limitations	limited selection
Process:	flexible	rigorous SDL
Results:	papers (knowledge), patents (IP), small prototypes	mission critical, large products (> 10 MLOC)
Support:	best efforts	> 20 years

The Researchers Dilemma

> A research should drive the future of the company
> but
> not act as extended work bench.

The three main challenges are:

- Timing
- Knowing the right persons
- Resources

Personally, I have experience with

- Top-down: (large) transfer projects (likely to result in high visibility)
- Bottom-up: (small) personal collaborations (likely to generate impact)

Personal Experiences

> People do not refer to (trust) organizations,
> they refer to (trust) other people!

Advise:

- Try to become an expert the key decision people refer to (trust).
- Do networking across your reporting line
  (talk to the people on the same floor, building, etc.)

Some example stories:

- Mobile
- Advanced access control models
- Static code analysis and testing

SAP RESEARCH

Thank you!

© 2012 SAP AG. All rights reserved

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft, Windows, Excel, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, System i, System i5, System p, System p5, System x, System z, System z10, System z9, z10, z9, iSeries, pSeries, xSeries, zSeries, eServer, z/VM, z/OS, i5/OS, S/390, OS/390, OS/400, AS/400, S/390 Parallel Enterprise Server, PowerVM, Power Architecture, POWER6+, POWER6, POWER5+, POWER5, POWER, OpenPower, PowerPC, BatchPipes, BladeCenter, System Storage, GPFS, HACMP, RETAIN, DB2 Connect, RACF, Redbooks, OS/2, Parallel Sysplex, MVS/ESA, AIX, Intelligent Miner, WebSphere, Netfinity, Tivoli and Informix are trademarks or registered trademarks of IBM Corporation.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Adobe, the Adobe logo, Acrobat, PostScript, and Reader are either trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.

HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

Java is a registered trademark of Sun Microsystems, Inc.

JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

SAP, R/3, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP BusinessObjects Explorer, StreamWork, 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.

Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius, and other Business Objects products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Business Objects Software Ltd. Business Objects is an SAP company.

Sybase and Adaptive Server, iAnywhere, Sybase 365, SQL Anywhere, and other Sybase products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Sybase, Inc. Sybase is an SAP company.

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

The information in this document is proprietary to SAP. No part of this document may be reproduced, copied, or transmitted in any form or for any purpose without the express prior written permission of SAP AG.

This document is a preliminary version and not subject to your license agreement or any other agreement with SAP. This document contains only intended strategies, developments, and functionalities of the SAP® product and is not intended to be binding upon SAP to any particular course of business, product strategy, and/or development. Please note that this document is subject to change and may be changed by SAP at any time without notice.

SAP assumes no responsibility for errors or omissions in this document. SAP 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.

SAP 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 these materials. This limitation shall not apply in cases of intent or gross negligence.

The statutory liability for personal injury and defective products is not affected. SAP has no control over the information that you may access through the use of hot links contained in these materials and does not endorse your use of third-party Web pages nor provide any warranty whatsoever relating to third-party Web pages.