CV / Profil

Bernd Fix

Software & Security Architect

Jahrgang	1962
Zivilstand	verheiratet
Nationalität	Deutsch
Wohnort	Berlin

Muttersprache	Deutsch
Englisch	Fließend in Wort und Schrift

Kontakt	brf@hoi-polloi.org
	+49 160 374 3474
Webseite	https://hoi-polloi.org/~brf/
	https://de.wikipedia.org/wiki/Bernd_Fix
Github	https://github.com/bfix

Bernd Fix ist seit 1978 mit den verschiedensten Bereichen der Software-Entwicklung und den Fragen der Computersicherheit beschäftigt.

Schon während des Studiums der Physik und Philosophie an der Universität Heidelberg gründete er die Firma BrainON!, die unter anderem auch Verschlüsselungsprogramme für Behörden und Unternehmen entwikkelte. Als Sicherheits-Experte war er in den 80er Jahren auch im Bereich der Computer-Viren tätig; so geht auf ihn die nachweislich erste Bekämpfung eines Computervirus und damit die erste dokumentierte Anti-Viren-Software aus dem Jahr 1987 zurück (http://de.wikipedia.org/wiki/Antivirus).

1998 erfolgte die Überführung der BrainON! in eine schweizerische Aktiengesellschaft mit Sitz in Dornach/SO. Bis 2003 war Bernd Fix als CTO für die Software-Architektur der Produkte verantwortlich.

2003 erfolgte die Gründung der aspector GmbH mit Sitz in Zug (später in Zürich). Die Schwerpunkte der Arbeit von Bernd Fix sind die Architektur und Implementation von komplexen Software-Applikationen, das Projektmanagement sowie Computersicherheit (Verschlüsselung, digitale Signaturen, Chipkarten, Penetrationstests).

Seit 2013 lebt und arbeitet Bernd Fix in Berlin und betreut als Vorstandsmitglied der Wau Holland Stiftung verschiedenste Projekte.

Ein breites Wissensspektrum, schnelle Auffassungsgabe sowie das Interesse an schwierigen Aufgabenstellungen sind besondere Fähigkeiten, die Bernd Fix auszeichnen.

Ausbildung	Datum
Grundschule Knesebeck (Niedersachsen/DE)	1968 – 1972
Gymnasium Hankensbüttel (Niedersachsen/DE) Erlangung der allgemeinen Hochschulreife mit den Leistungskursen „Mathematik“ und „Physik“, Gesamtnote „Gut“ (1.8)	1972 – 1981
Universität Göttingen, Grundstudium der Physik und Philosophie Erlangung des Vordiploms nach Abschluss des 4. Semesters, Note „Sehr Gut“	1982 – 1985
Universität Heidelberg, Abschlussstudium Physik und Philosophie Erlangung des akademischen Grades „Diplom-Physiker“ mit einer Arbeit im Bereich „Theoretische Astrophysik“ und einer Nebenfach-Prüfung zum Thema „Philosophische Interpretationen der Quantenmechanik“, Gesamtnote „Gut“	1985 – 1989

Beruflicher Werdegang	Datum
Gründung der Firma BrainON! in Heidelberg • Selbstständige Tätigkeit als Software-Entwickler (Produkt-Entwicklung im Sicherheits-Umfeld) • Fach-Referent im Bereich Computer-Sicherheit	1987 – 1998
Verantwortlicher Software-Entwickler für das deutsche Architektur-CAD-System „SPIRIT“ (SOFT-TECH, Neustadt a.d.W.) • Schwerpunkt: 3D-Konstruktion und Visualisierung • Firmenvertreter in Standardisierungs-Gremien (STEP) • zeitweiliger Arbeitsaufenthalt in den USA bei einer Partnerfirma (Know-How-Transfer)	1989 – 1991
CTO und Geschäftsführer der BrainON AG mit Sitz in Dornach/SO • Geschäftsführer-Tätigkeit • CTO und Lead Architect für alle Software-Projekte des Unternehmens	1998 – 2003
Geschäftsführer der Firma aspector GmbH, Zug • Selbstständige Tätigkeit als Berater und Security Architect in kritischen Infrastrukturen und komplexen Umgebungen • Interne Entwicklung von Security- und Compliance-Applikationen (Produkt-Entwicklung)	2003 – 2013

Freiberufliche Tätigkeit
• Betreuung und Leitung von Projekten für die Wau Holland Stiftung, Hamburg
• Beratung / Schulung im Bereich „Computersicherheit“ und „Situational Awareness“ für Journalisten und NGOs
  • Tutor für Schulungen von „Reporter ohne Grenzen (Genf)“ und „Center for Investigative Journalism (London)“
  • Inhouse-Schulungen für Verlage / Medien
	2014 – heute

Arbeitsschwerpunkte

(Security) Architecture	Konzeption und Design von Lösung-Architekturen in anspruchsvollen und komplexen Umgebungen mit dem Schwerpunkt „Computer- und Netz-Sicherheit“, „Compliance“ und „Kryptographie / PKI“
Requirement Engineering	Moderieren, erfassen, modellieren und dokumentieren der Anforderungen an neue Software-Systeme in Zusammenarbeit mit dem Kunden.
System Specification	Detail-Design und Spezifikation der Lösungen basierend auf den Requirement Specifications des Projektes. Verifikation der Machbarkeit vor Implementationsbeginn durch Rapid Prototyping.
Implementation / Coaching	Begleitung der Implementationsphase und allfälligen Migrationsprozessen im Rahmen eines Coachings (beratende Tätigkeit) sowie Entwicklung auf verschiedenen Plattformen und Programmiersprachen (vorzugsweise Golang unter Linux)
(Security) Review	Review von konzipierten oder implementierten Software-Projekten im Sicherheits-Umfeld (inklusive aktiven Sicherheitstests und -audits) oder Evaluierungen von externen Lösungsangeboten im RfP-Prozess nach Anforderungskatalog
Documentation	Software- und Prozess-Dokumentationen im Security-Umfeld; Verfahrensdokumentationen für externe Audits und bestellte Gutachter (Gerichtsfall)

Spezielle Erfahrungen im Bereich „Computer-Sicherheit“

Kryptographie	Verschlüsselung (RSA, ECC, homomorphe Verschlüsselungen), digitale Signaturen / PKI, Hash-Verfahren, Schlüsselaustausch, Crypto-Hardware (HSM, ICSF, Chipkarten) und -Software
Netzwerk-Sicherheit	Angriffsvektoren für alle ISO-Layer (und ihre Protokolle) sowie entsprechende Devices (Router, Switches u.ä.); Firewalls, IDS, VPN, VLAN
Identity Management und Access Control	Federated Identity Management, SSO (Kerberos), SAML, 2-Factor-Authentication, Regel- und Rollen-basiertes Access Control, Provisioning,
Applikatorische Sicherheit (OS, Anwendungen)	Sicherheits-Architektur, Reviews und dedizierte PenetrationTests
Enterprise Security Architecture	Grundegende Sicherheitsanforderungen und -Architekturen in grossen Unternehmen, speziell im Bankenumfeld. Verständnis von IT-Risk und Compliance Abforderungen in komplexen IT-Infrastrukturen.

Spezielle Erfahrungen in der „Software-Entwicklung“	seit (Datum)
CSP-orientierte Entwicklung: • Golang (Linux), Limbo (Inferno)	2010
Aspekt-orientierte Programmierung (AOP): • AspectJ (Design, Implementation, Beratung, Coaching)	2001
Objekt-orientierte Programmierung (OOP): • Java (Design, Implementation) • C++(Design, Implementation) • UML (Design)	1996 1990 1994
Verantwortliche Konzeption und Umsetzung größerer Applikationen (100k+ Quellzeilen) • Übernahme der Funktion eines technischen Projektleiters (interne/externe Projekte)	1989
Plattformen/Betriebssysteme: • Unix (Schwerpunkt Linux) • z/OS (System /370); spezielle IBM-Mainframe-Kenntnisse in den Bereichen Assembler und PL/1	1998 1986

Zusätzliche Schwerpunkt-Erfahrungen / Skills

Plattformen (Hard- und Software)	• ***UNIX*** (speziell ***Linux***, Sun Solaris, IBM AIX, HP-UX u.a.) • Virtualisierung (***Docker***, Xen, VirtualBox), Android • Plan9 / Inferno • IBM Mainframe (z/OS, MVS, VM) • Chipkarten / PIC, Microcontroller
Programmier-sprachen	• ***Golang***, Limbo • AspectJ/Java, C/C++ • Perl, Python • Assembler (verschiedene Prozessoren) • PL/1
Entwicklungs-umgebungen	• ***Eclipse*** • Versionskontrollsysteme: ***git***, subversion, cvs • CI-Server (Jenkins/Hudson) • (auto-)make, ant, maven
Middleware & Integration	WebServices, Servlets, CORBA, RMI, RPC, MQ Series, JMF
Methoden / Modellierung	UML, ***XP / Scrum***, ER, AOP, OOP, RACI
Datenbanken	***MySQL***, PostgreSQL, Oracle, IBM DB2
Netzwerk	Protokolle und Hardware-Komponenten der OSI-Schichten 2 bis 4

Ausgewählte kommerzielle Projekte der letzten Jahre	Datum
System-Entwicklung (C/C++) im Bereich HPC (High Performance Computing) bei einem Finanzdienstleister in der Schweiz Unterstützung bei der Umsetzung einer Message Processing Applikation im High Performance Computing-Umfeld (Börse) auf Multicore-Architektur und RealTime-Betriebssystem.	2010
Security Architect während der Evaluations- und Konzeptionsphase für ein „Data Loss Prevention“ (DLP)-System bei einer Grossbank in der Schweiz Evaluation verschiedener DLP-Lösungsanbieter unter definierten Sicherheitsaspekten: • Sicherheit des Netzwerkverkehrs (Kommunikation der Lösungs-Komponenten untereinander) sowie der Lösungskomponenten selbst (z.B. gegen Intrusion) • Einbindung starker Authentisierungsmethoden (Smartcard, Two-Factor-Authentication) in den Management-Prozess des DLP-Systems • Eignung der Scan-Methoden (Regular Expressions, Keywords, Document and Database Matching etc.) zur Abbildung der gegebenen Compliance-Policies • Einhaltung der Sicherheits-Richtlinien beim Scannen von eMails (Personen-/Datenschutz-Richtlinien, Mission Critical Infrastructure) Konzeption zusätzlicher Sicherheits-Komponenten für den DLP-Einsatz • Kapselung der Management Console über Citrix • Einbindung der vorhandenen PK-Infrastruktur	2009 - 2010
Security Architect während der Konzeptionsphase für ein neues globales Identity Management und Access Control System einer Grossbank in der Schweiz Design einer Prozess-, Architektur- und Komponenten-Landschaft, die den komplexen und vielfältigen Compliance-, Risk- und Business-Anforderungen einer global-operierenden Bank gerecht wird: • Berücksichtigung der besondern Compliance-Anforderungen in den verschiedenen Rechtssprechungen („legal spaces“). Dies geschieht aktiv, d.h. es wird immer sichergestellt, dass nur korrekt genehmigte und zulässige/erlaubte Änderungen provisioniert werden können. Zudem wurden Mechanismen entworfen, die einen vollständigen und nachvollziehbaren Audit erlauben und durch Monitoring-/Reporting-Funktionen unterstützt werden. • Sicherstellung der Integrität, Compliance und Accountability für jeden Schritt des Workflows, speziell im Genehmigungsprozess und der Mutation von Bestandsdaten. Dies wird durch kryptographische Verfahren und regel-basierte Policies erreicht. • Effizienzsteigerung durch vollautomatische Provisionierung in die heterogene Infrastruktur und direkte Einbindung vorhandener IdM-relevanter Basistechnologien (Authentifizierung/PKI, regel-basierte Autorisierung u.ä.)	2007 - 2008
Security-Review einer Offshore-IT-Plattform Technischer Review und Klärung von Detailfragen im Rahmen einer Entwicklungs-Plattform für Offshore-Entwickler, die im Auftrag einer Grossbank (im Ausland) arbeiten: • Prüfung der Grundkonzeption und des technischen Basis-Layouts (Netzwerk-Design/-Komponenten) • Ermittlung und Bewertung von Angriffsvektoren (initiiert durch „malicious“ Offshore-Mitarbeiter) • Detailabklärungen wie z.B. LPAR Separation unter IBM z/OS	2007

Ausgewählte Projekte der letzten Jahre	Datum
Entwürfe einer Lösungs-Architektur für den Integritätsnachweis von Logdateien Erstellung alternativer Konzepte für die Integration von Logdateien in den Integritätsnachweis des Langzeit-Archives. Die Konzepte hatte die speziellen Compliance- und Accountablility-Anforderungen im Bankenumfeld zu berücksichtigen.	2006
Technische Projektleitung und Konzeption der Lösungs-Architektur für den Integritätsnachweis im digitalen Langzeit-Archiv einer Grossbank Dieses Projekt realisiert den gesetzlich geforderten Nachweis der Unversehrtheit (Integrität) von geschäftsbücher-relevanten Dokumenten in elektronischen Langzeit-Archiven (GeBüV) und berücksichtigt die zusätzlichen (Compliance-)Anforderungen einer Grossbank: • „Offene Architektur“, d.h. es wurden ausschliesslich (quell-)offene, validierte und anerkannte kryptographische Standards und Verfahren verwendet. • Hohe Performance (tägliches Volumen: > 10 Mio. Dokumente) • Migrationsfähigkeit von rund 140TB Archivbestand • Gerichtsfähiger Integritätsnachweis (Evidence Record) einzelner elektronischer Dokumente auf Anforderung, ohne Dokumente anderer Kunden einzubeziehen (Bankgeheimnis) Nach der Konzeptionsphase wurde das Projekt während der Implementations- und Einführungsphase unterstützend begleitet und eine Verfahrens-Dokumentation des Gesamtprozesses gestellt.	2004 - 2006
Konzeption und Implementation eines Prototypen für ein Testwerkzeug im Bereich „Zahlungsverkehr“ Generierung und automatische (periodische) Ausführung von Buchungsaufträgen in der IT-Testumgebung. Durch das anschließend ebenfalls automatische Überprüfen der jeweils generierten Buchungsdaten durch die vielfältigen und verzahnten Einzelprozesse (Applikationen) kann das korrekte Zusammenspiel der einzelnen Komponenten geprüft werden. • Servlet-basiertes GUI für Administration und Benutzung • Import von Testbuchungen aus vorhandenen Quellen • Verwendung der CORBA-Middleware für die Kommunikation mit den Buchungskomponenten • Reporting-Funktionalität	2003 - 2004

Ausgewählte Community / Open-Source-Projekte	Datum
Projektleitung für ein neues Social Media Framework (Python) Community-Projekt mit Entwicklern aus Europa, Amerika und Australien zur Erstelung einer neuartigen sozialen Netzwerkwerk-Applikation mit speziellen Sicherheits-Merkmalen (Profil-Verschlüsselung mit ECC, homomorphe Verschlüsselung, ...)	2012
Design und Implementation eines High-Secure-Submission-Systems **`http://github.com/bfix/sid/`** golang-basiertes System zur geschützten Einreichung von Dokumenten mittels einer Webapplikation über das Tor-Netzwerk (https://torproject.org). Erstellt im Auftrag und in Zusammenarbeit mit australischen Universitäten und Forschungseinrichtungen.	2011 - 2012

Ausgewählte Open-Source-Projekte	Datum
J9P/StyxLib **http://github.com/bfix/j9p/** The J9P development framework is designed to ease the integration of legacy or non-9P services into 9P networks. It is a pure Java implementation and will run on various hard- and software platforms. The J9P/StyxLib framework enables Java developers to publish namespaces (virtual filesystems) based on the 9P/Styx protocol (Plan9/Inferno). Every namespace entry (file or directory) is associated with a handler (Java class) that controls the behavior and content of the entry. By developing customized handlers, you can integrate legacy or other non-9P services into a 9P network by mapping the service functionality to file operations. A generic 9P server (with pure Java implementation of 9P) as well as example namespaces („dbfs“) are included.	2009
Cyfer **http://hoi-polloi.org/~brf/projects/Cyfer/index.html** Cyfer is an OpenPGP implementation for newer Nokia Communicators (9500/9300). OpenPGP is a standard (RFC 2440) for exchanging signed and/or encrypted messages (via eMail). It is used by applications like GnuPG (GNU Privacy Guard) and others.	2006
DynaWorks **http://hoi-polloi.org/~brf/projects/DynaWorks/index.html** DynaWorks is a Java-based framework to develop GUI applications for PalmOS devices. It provides an efficient and compact source code library for GUI handling and database access and currently supports multiple Java2™ implementations (J9/IBM and KVM/Sun).	2000 - 2001

Ältere Projekte (interne Produktentwicklungen)	
PC-DES: Datei und Verzeichnis-Verschlüsselung unter MS-DOS Design und Implementation der Security-Applikation „PC-DES“ (Verschlüsse-lungsprogramm nach DES-Verfahren) für den Einsatz in Behörden, Unternehmen und im privatem Umfeld. Die Applikation wurde aktiv über Partner vermarktet und 1990 vom Partner übernommen und weiterentwickelt.	1987 - 1989
WAS: Virtueller Modellbau für Architekten Design und Implementation des Computeranimations-Systems „WAS“ für die Bauindustrie und Architekten. Einsatz auch in Behörden (Polizei) zur Tatort-Rekonstruktion und -Begutachtung.	1992 - 1995
MOPS: Messe-Organisations- und Planungs-System Design und Implementation der Messeplanungs-Software „MOPS“ für Messegesellschaften; Kundenbetreuung und Schulung; Systempflege. MOPS war diese Jahre das zentrale visuelle Planungs- und Organisations-Instrument der Deutschen Messe AG, Hannover (CeBIT), der Messe München (Systems) sowie weiterer kleiner Messeveranstalter.	1995 - 2003
CADalog: Elektronischer Ersatzteil-Katalog System zum Identifizieren von Ersatzteilen in komplexen Maschinen (Flugzeug- und Maschinenbau) durch visuelles Navigieren in einem 3D-Modell oder in 2D-Explosionszeichnungen mit steigender Detaillierung.	1996 - 2003