A Plague of Plug-ins

Thomas Ball

Microsoft Research

May 2011

Plug-ins

- The why and wherefore of plug-ins
- Problems of composition
  - Isolation
  - Connectedness
  - Dependences
  - Protocols
  - Feature Interaction
- Other thoughts
  - Smart phone
  - Cloud computing
  - Human-based computation

Car Plug-ins

http://www.bing.com/search?q=after+market+car+stereo&src=ie9tr

after market car stereo - Bing

Shop for **after market car stereo**

2006 GMC Canyon Car Stereo
$315.00

2006 Toyota Camry Car Stereo
$265.00

2008 Acura TL Car Stereo
$495.00

2004 Nissan Quest Car Stereo
$395.00

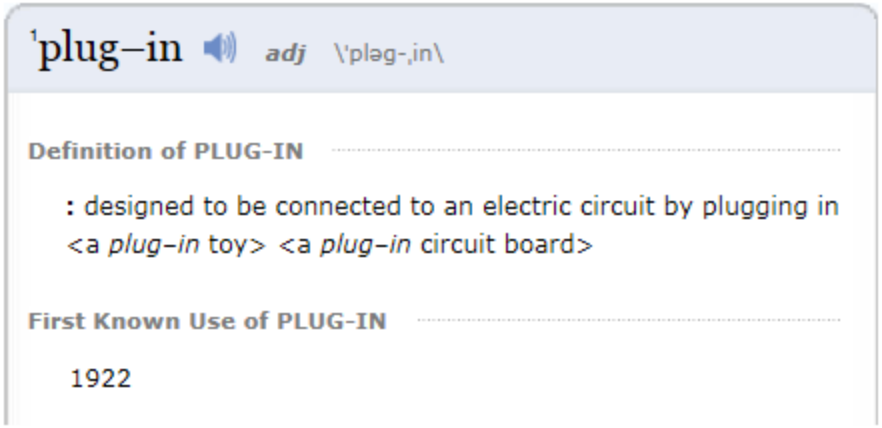
bing.com/shopping

Guide to **Aftermarket Car Stereo** Wiring | eHow.com

A common form of customization for **car** owners is **aftermarket** additions to their **car stereo** system. There are many options for creating a custom system from speakers ...

www.ehow.com/way_5700933_guide-**aftermarket-car-stereo**-wiring.html

Plug-in



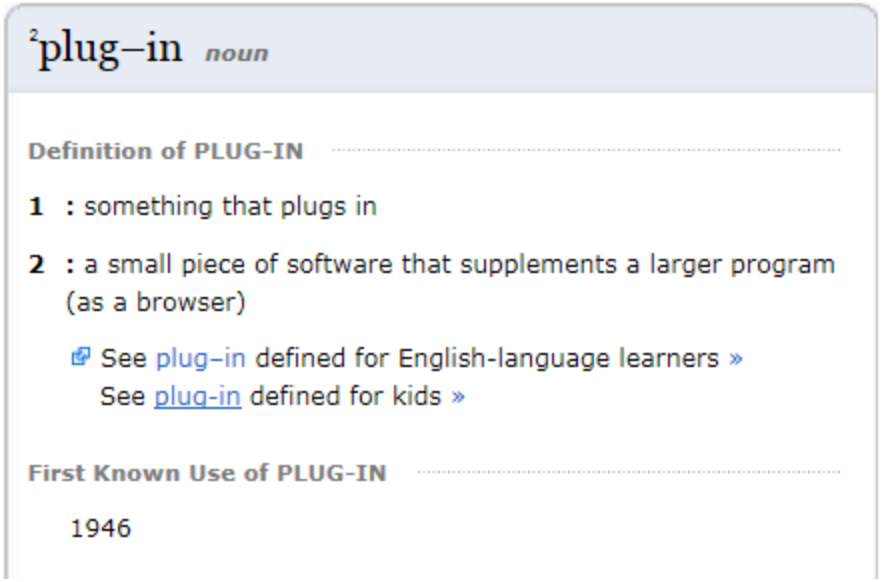
¹plug–in *adj* \ˈpləg-ˌin\

Definition of PLUG-IN

: designed to be connected to an electric circuit by plugging in
<a *plug–in* toy> <a *plug–in* circuit board>

First Known Use of PLUG-IN

1922



²plug–in *noun*

Definition of PLUG-IN

1 : something that plugs in

2 : a small piece of software that supplements a larger program (as a browser)

See plug–in defined for English-language learners »
See plug-in defined for kids »

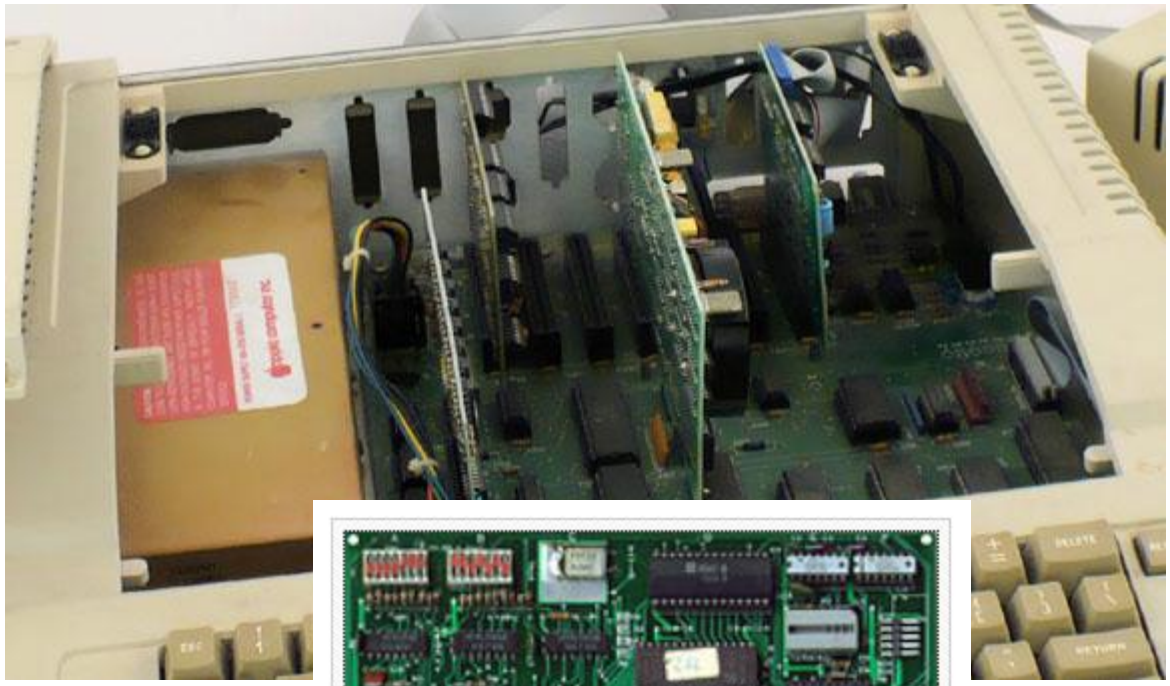
First Known Use of PLUG-IN

1946

Plug-ins are aftermarket extensions of a product that

- Give consumers more choice
- From a market of plug-in producers

My Start With A Very Pluggable Computer, 1979



Apple II serial interface card that required cutting and soldering to reconfigure. The user would cut the wire trace between the >< cones at X1 and X3 and solder the <> cones together at X2 and X4.

1981-1986

IBM 5150 as of 1981

Intel 386

Intel 80386 DX rated at 16 MHz

Produced	From 1985 to September 2007
Common manufacturer(s)	Intel AMD IBM
Max. CPU clock rate	12 MHz to 40 MHz
Min. feature size	1.5µm to 1µm
Instruction set	x86 (IA-32)
Package(s)	132-pin PGA, 132-pin PQFP; SX variant: 88-pin PGA, 100-pin PQFP

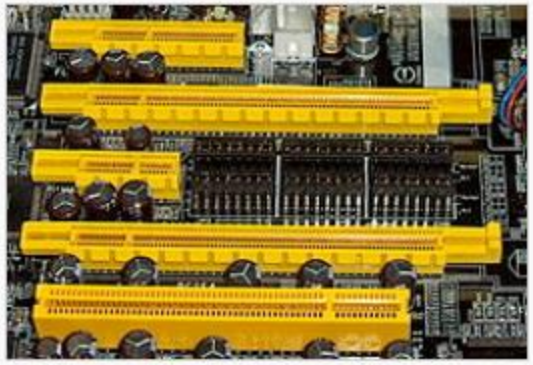
The Pluggable PC Platform

Conventional PCI

PCI Local Bus

Three 5 V 32-bit PCI expansion slots on a motherboard (PC bracket to left)

Year created	July 1993
Created by	Intel
Supersedes	ISA, EISA, MCA, VLB
Superseded by	PCI Express (2004)
Width in bits	32 or 64
Capacity	133 MB/s (32-bit at 33 MHz) 266 MB/s (32-bit at 66 MHz or 64-bit at 33 MHz) 533 MB/s (64-bit at 66 MHz)
Style	Parallel
Hotplugging interface	Optional



PCI Express slots (from top to bottom: ×4 , ×16, ×1 and ×16), compared to a traditional 32-bit PCI slot (bottom), as seen on DFI's LanParty nF4 SLI-DR.

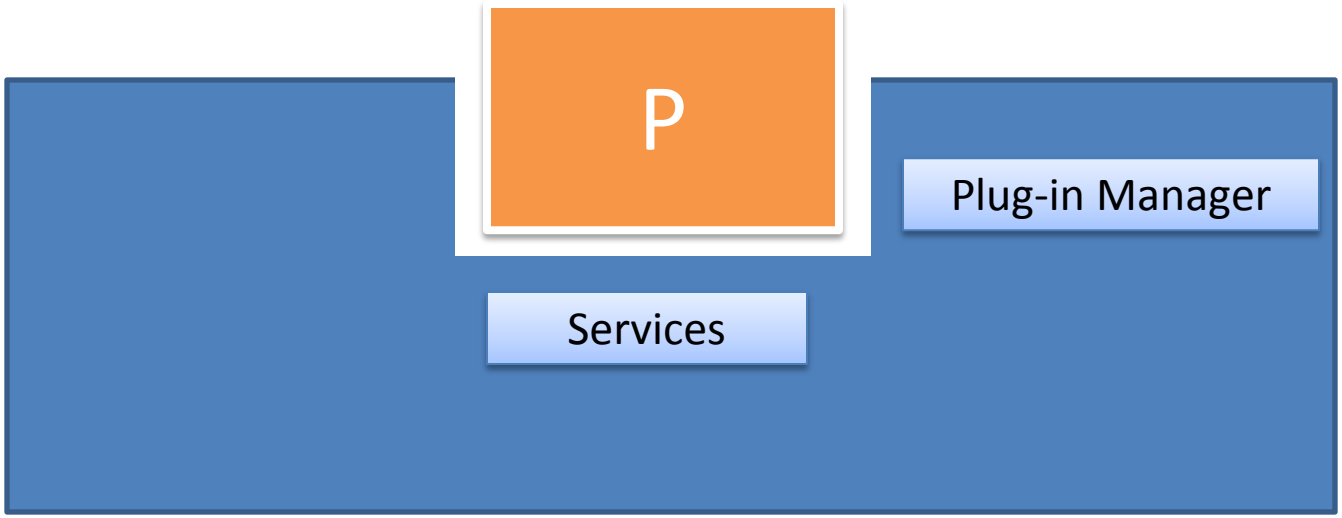
A USB Standard Type A plug, the most common USB plug

USB
The ultimate plug-in enabler!

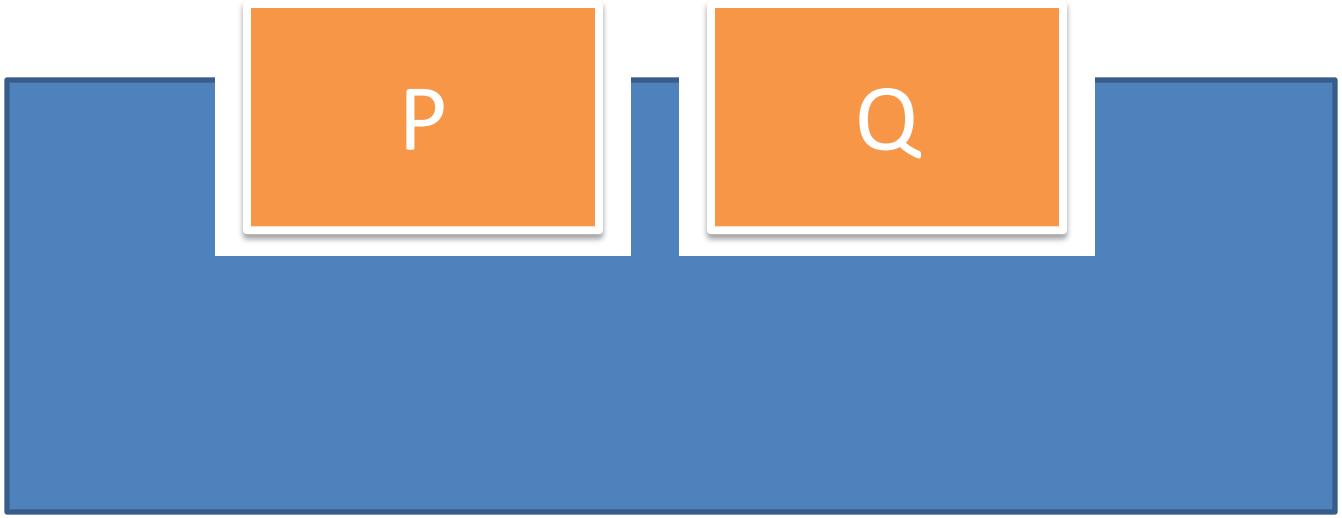
Cup is not included

Pluggable Platforms: Compare/Contrast

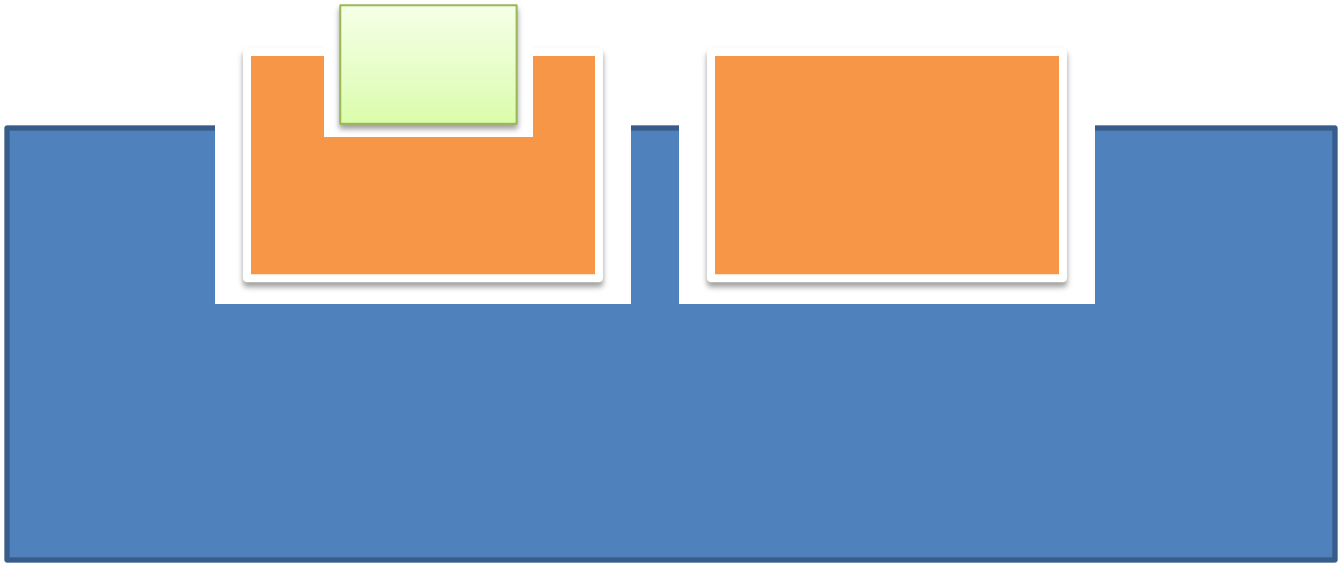
Plug-ins



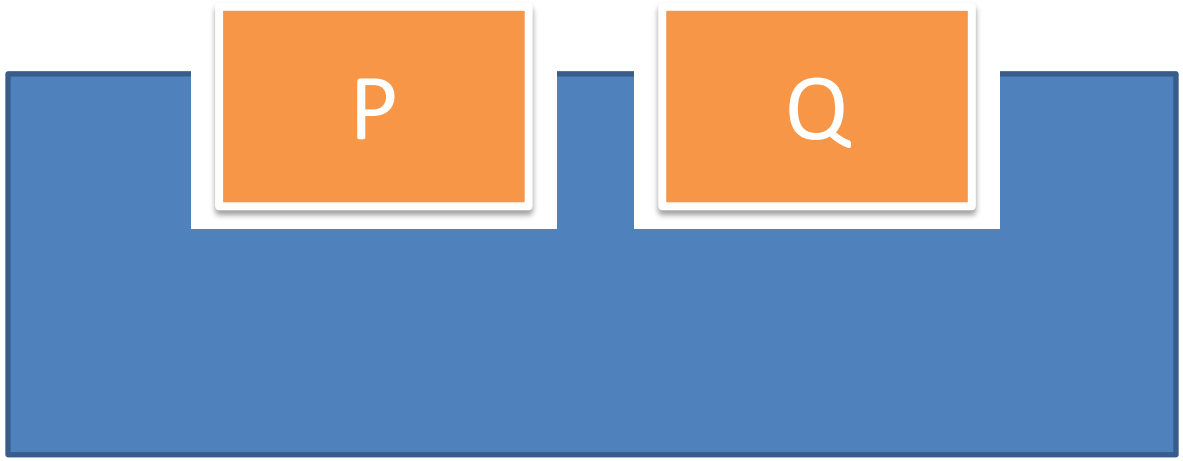
Plug-ins



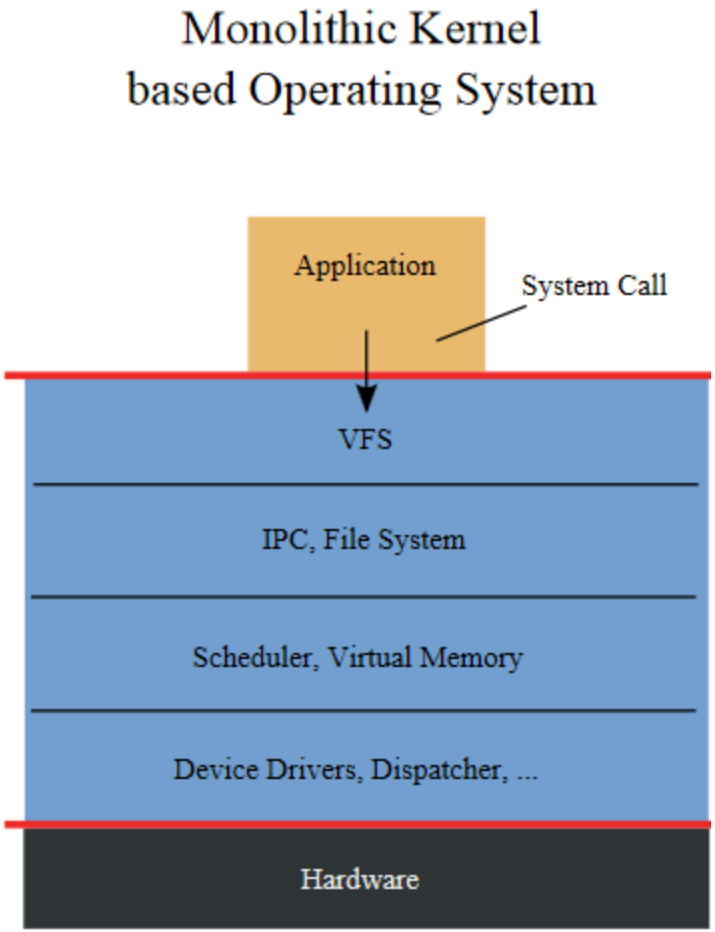
Plug-ins



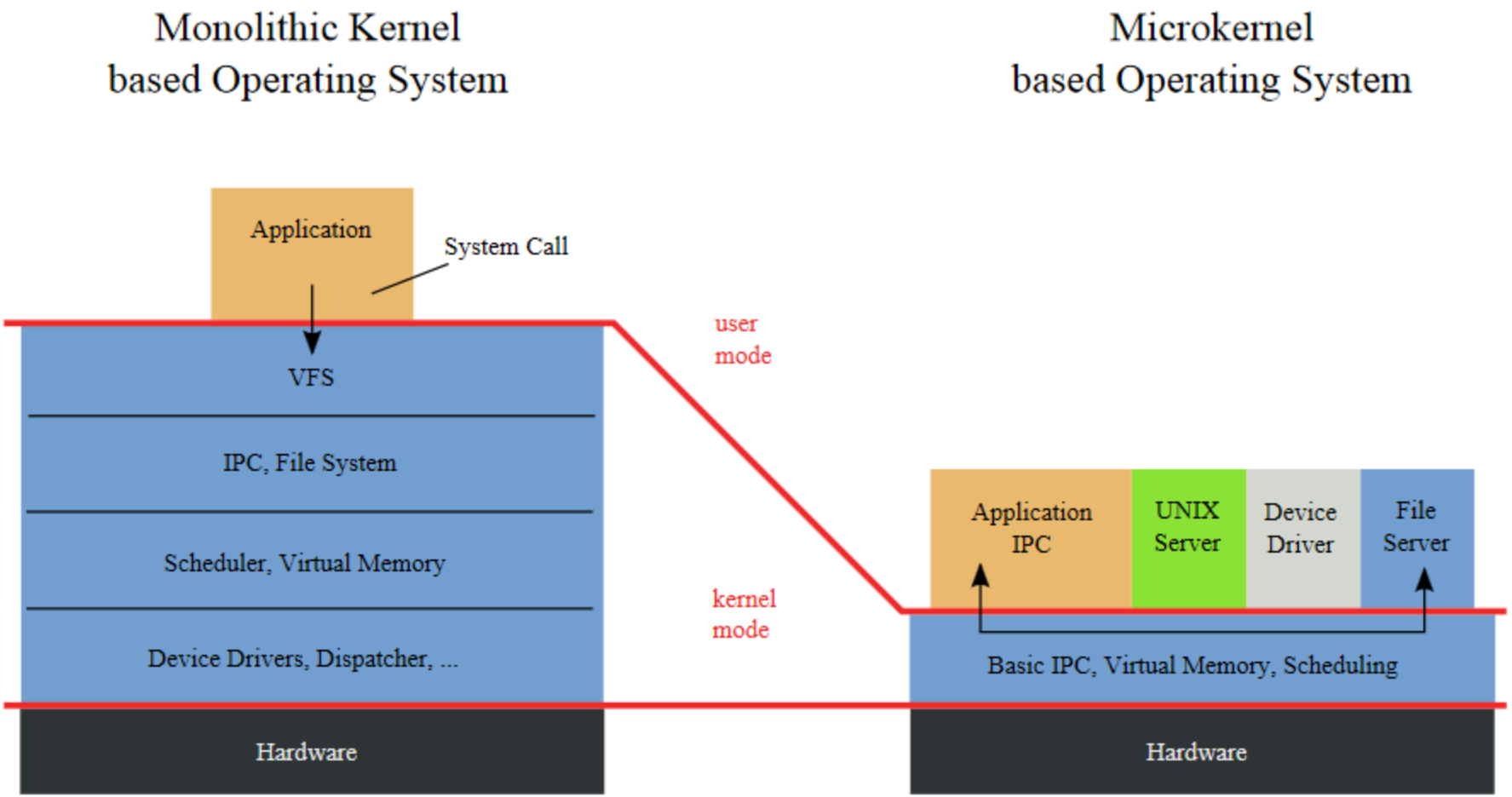
Isolation



1980s: BSD Unix to Microkernels



1980s: BSD Unix to Microkernels

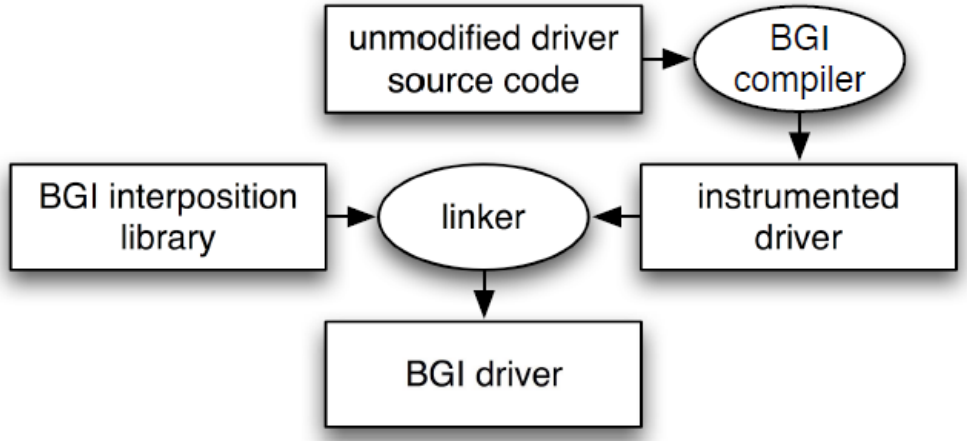


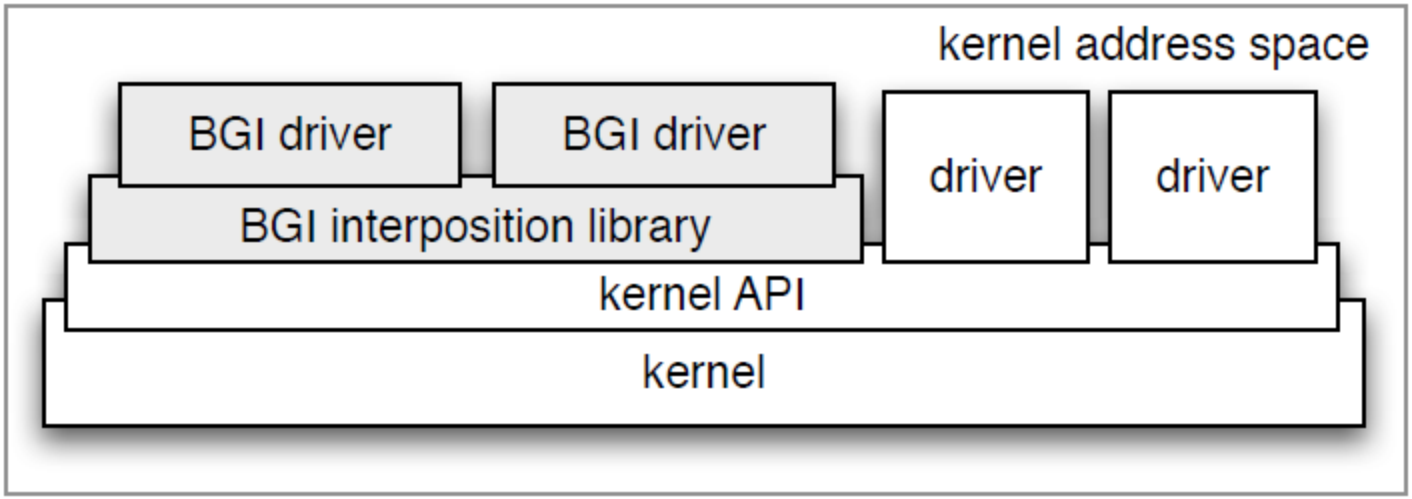
Software Isolated Programs

- Shared memory
  - Java, C#: safe user-level prog. language
  - Cyclone, Sing#: safe systems prog. language
  - Instrumentation (BGI, next slide)

- Message passing (distributed systems)
  - Bell Labs' 5ESS
  - Modern web services/platforms

Byte-Granularity Isolation for Kernel Drivers (MSR Cambridge)





SOSP 2009

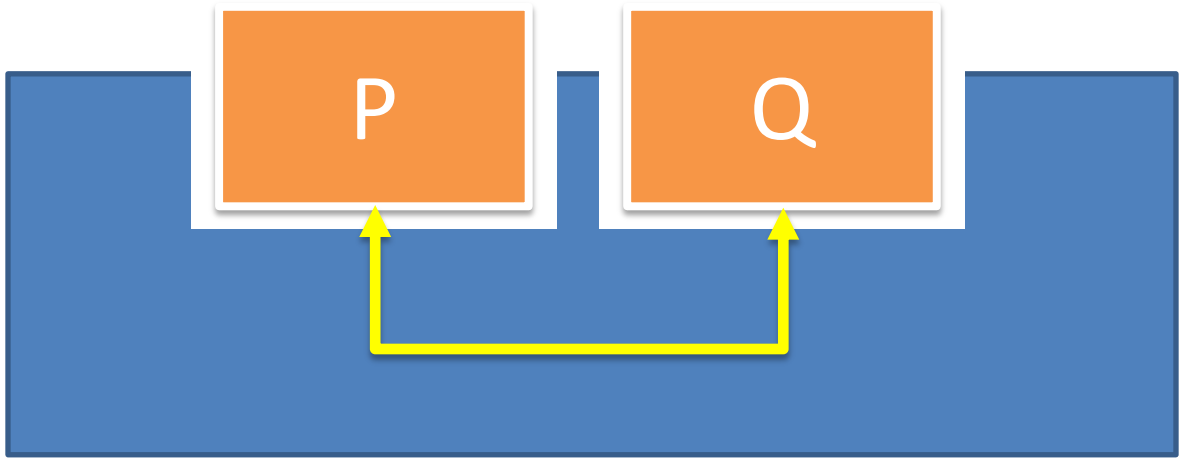
Tab Isolation

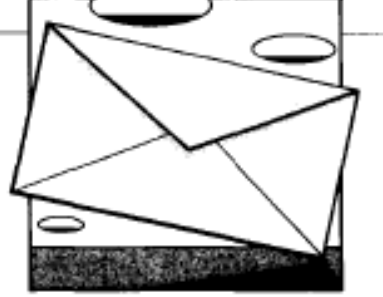
The browser as operating system

"IE8 runs the browser frame and tabs in separate processes, which prevents glitches and hangs from bringing down the entire browser and leads to higher performance and scalability."

"In IE8-9, tabs run without permissions to install software, modify settings, or change files of any user."

Connectedness





Connecting Tools Using Message Passing in the Field Environment

Steven P. Reiss, *Brown University*

Field connects tools with selective broadcasting, which follows the Unix philosophy of letting independent tools cooperate through simple conventions. Field demonstrates that this simple approach is feasible and desirable.

Steven P. Reiss: Connecting Tools Using Message Passing in the Field Environment. IEEE Software 7(4): 57-66 (1990)

Reiss' Field IDE

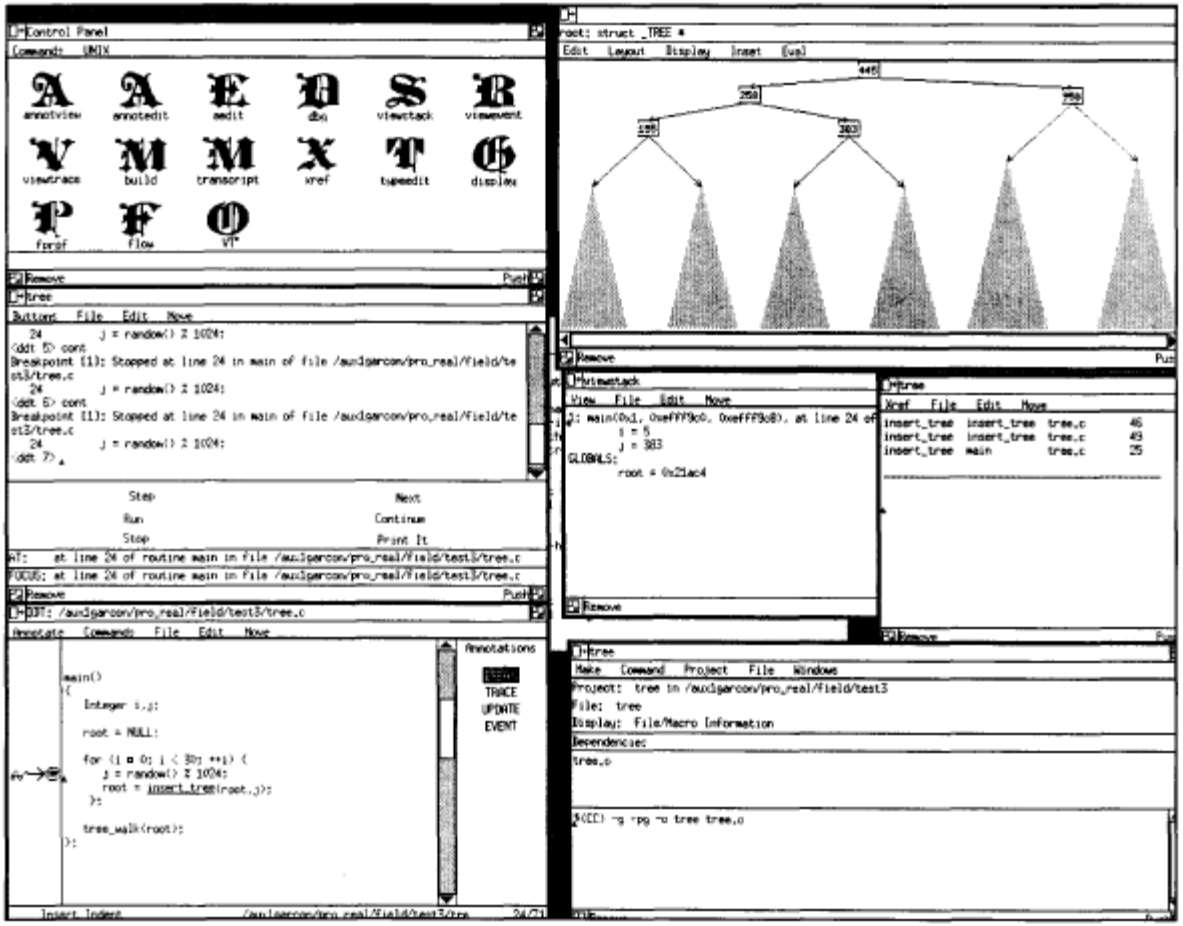
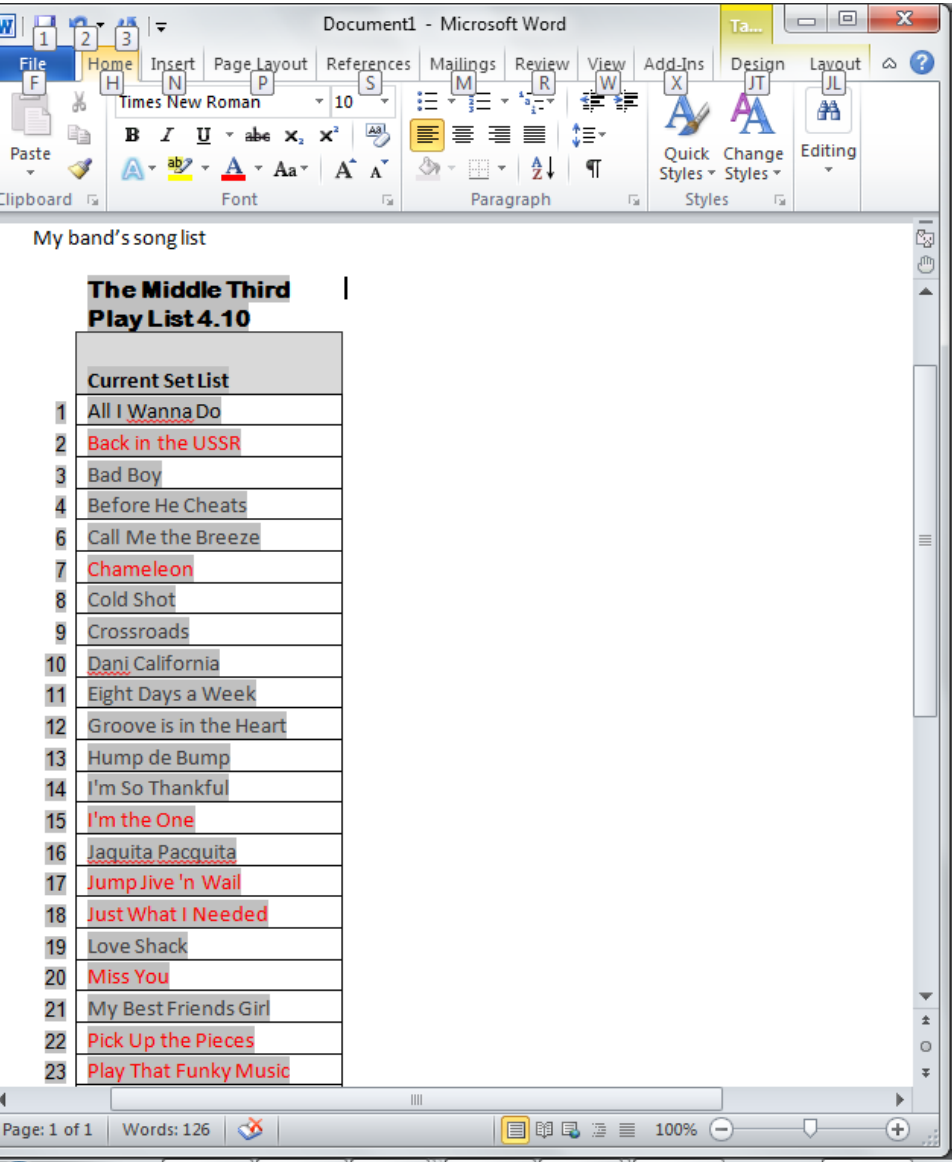
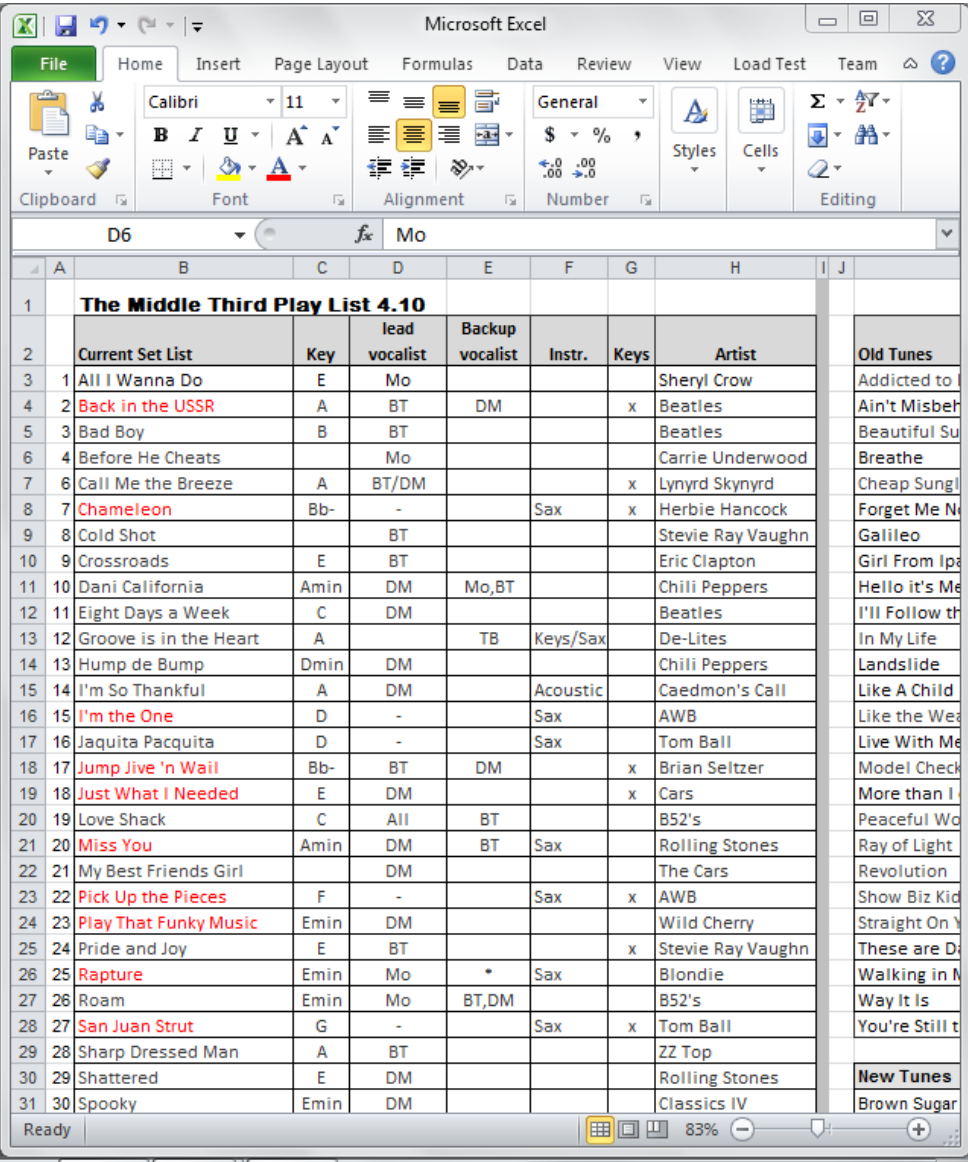


Figure 1. The Field environment.

Connectedness via COM, 1993

"The Component Object Model (COM) grew out of Microsoft's efforts to make the various parts of its Office productivity suite *work together*."
http://www.polberger.se/components/read/com.html


Document1 - Microsoft Word
File Home Insert Page Layout References Mailings Review View Add-Ins Design Layout
Times New Roman 10
Paste Clipboard Font Paragraph Quick Styles Change Styles Editing
My band's song list
The Middle Third Play List 4.10
Current Set List
1 All I Wanna Do
2 Back in the USSR
3 Bad Boy
4 Before He Cheats
6 Call Me the Breeze
7 Chameleon
8 Cold Shot
9 Crossroads
10 Dani California
11 Eight Days a Week
12 Groove is in the Heart
13 Hump de Bump
14 I'm So Thankful
15 I'm the One
16 Jaquita Pacquita
17 Jump Jive 'n Wail
18 Just What I Needed
19 Love Shack
20 Miss You
21 My Best Friends Girl
22 Pick Up the Pieces
23 Play That Funky Music
Page: 1 of 1 Words: 126 100%


Microsoft Excel
File Home Insert Page Layout Formulas Data Review View Load Test Team
Calibri 11 General
Paste Clipboard Font Alignment Number Styles Cells Editing
D6 Mo
The Middle Third Play List 4.10
Current Set List | Key | lead vocalist | Backup vocalist | Instr. | Keys | Artist | Old Tunes
1 All I Wanna Do | E | Mo | | | | Sheryl Crow | Addicted to
2 Back in the USSR | A | BT | DM | | x | Beatles | Ain't Misbeh
3 Bad Boy | B | BT | | | | Beatles | Beautiful Su
4 Before He Cheats | | Mo | | | | Carrie Underwood | Breathe
6 Call Me the Breeze | A | BT/DM | | | x | Lynyrd Skynyrd | Cheap Sungl
7 Chameleon | Bb- | - | | Sax | x | Herbie Hancock | Forget Me N
8 Cold Shot | | BT | | | | Stevie Ray Vaughn | Galileo
9 Crossroads | E | BT | | | | Eric Clapton | Girl From Ipa
10 Dani California | Amin | DM | Mo,BT | | | Chili Peppers | Hello it's Me
11 Eight Days a Week | C | DM | | | | Beatles | I'll Follow th
12 Groove is in the Heart | A | | TB | Keys/Sax | | De-Lites | In My Life
13 Hump de Bump | Dmin | DM | | | | Chili Peppers | Landslide
14 I'm So Thankful | A | DM | | Acoustic | | Caedmon's Call | Like A Child
15 I'm the One | D | - | | Sax | | AWB | Like the Wea
16 Jaquita Pacquita | D | - | | Sax | | Tom Ball | Live With Me
17 Jump Jive 'n Wail | Bb- | BT | DM | | x | Brian Seltzer | Model Check
18 Just What I Needed | E | DM | | | x | Cars | More than I
19 Love Shack | C | All | BT | | | B52's | Peaceful Wo
20 Miss You | Amin | DM | BT | Sax | | Rolling Stones | Ray of Light
21 My Best Friends Girl | | DM | | | | The Cars | Revolution
22 Pick Up the Pieces | F | - | | Sax | x | AWB | Show Biz Kid
23 Play That Funky Music | Emin | DM | | | | Wild Cherry | Straight On
24 Pride and Joy | E | BT | | | x | Stevie Ray Vaughn | These are D
25 Rapture | Emin | Mo | * | Sax | | Blondie | Walking in M
26 Roam | Emin | Mo | BT,DM | | | B52's | Way It Is
27 San Juan Strut | G | - | | Sax | x | Tom Ball | You're Still t
28 Sharp Dressed Man | A | BT | | | | ZZ Top
29 Shattered | E | DM | | | | Rolling Stones | New Tunes
30 Spooky | Emin | DM | | | | Classics IV | Brown Sugar
Ready 83%


11:43 AM
5/25/2011

Key Ideas of COM

- **Binary standard** for components, classes, and interfaces
- **Memory layout** follows pure virtual C++ classes
- **Interface definition language**
- **Type libraries (metadata)**
- **Automation**: the ability for one program, typically a script, to access and control another

1990s: Connectedness (Web 1.0)

- 1991: World Wide Web
- 1993: Mosaic
- 1995: Java applets
- 1996: JavaScript, “DOM Level 0”
- 1996: Microsoft’s ActiveX
- 1998: “DOM Level 1” recommended by W3C

2000s: Buffer Overflow and Security Exploits

- Connectedness of code with many buffer overflows (lack of isolation) leads to a security crisis at Microsoft
- Security Definition Lifecycle
- Static tools for buffer overflows (SAL, PREfast)
- SAGE white box file fuzzing
- IE 8-9 security improvements

2000s: Connectedness (Web 2.0)

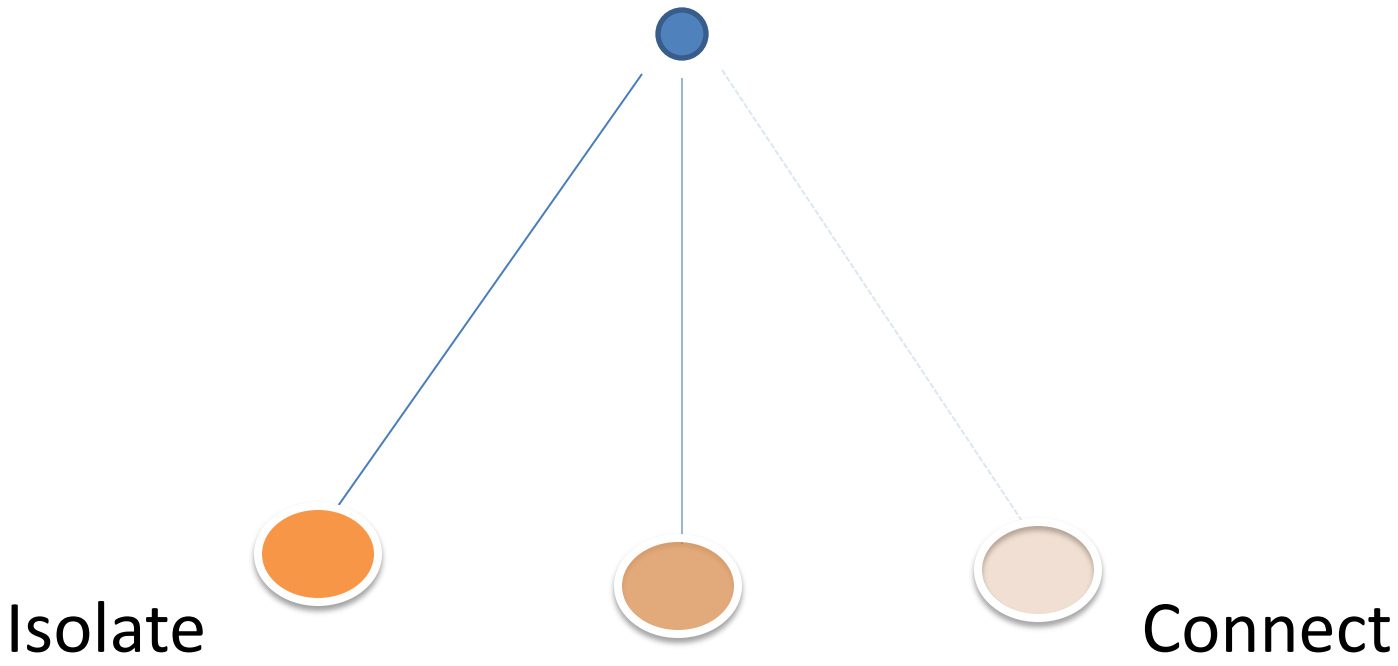
- Search and advertising (Google)
  - Connect consumers to producers via search and auction of ad terms
  - Plug-ins for site-targeted advertising
- Facebook
  - “Open graph” connects individuals, pages, groups, pictures, etc. in a huge graph
  - Plug-ins (apps) require access to your information to run

2011:
Humans Plugged Into the Web

Clickjacking

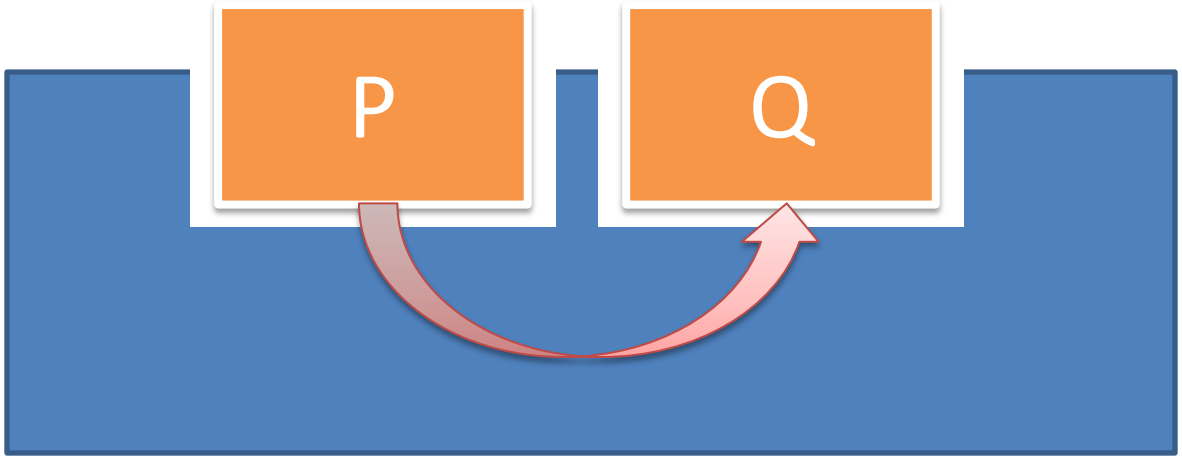
- Fooling users into “liking” a page
- **Connect**: “Clickjacks succeed because people tend to trust information given to them on social networking sites, especially if it appears to have won the approval of several friends.”
- **Isolate**: “Preventing clickjacking attacks requires users trust no one.”

The Pendulum Keeps Swinging



Security, Reliability, Availability, …

Dependences



Unix Package Management

- Package Manager
  - The Unix system administrators best friend
  - Leading edge in SunOS -> Solaris (early 1990s)
  - Also in A/IX, HP/UX, even Windows from the early days

- http://en.wikipedia.org/wiki/Package_manager
  - Ian Murdock has commented that package management is "the single biggest advancement Linux has brought to the industry", that it blurs the boundaries between operating system and applications, and that it makes it "easier to push new innovations into the marketplace and evolve the OS".

Managing Dependences with SAT

Feature A requires
(Feature B1 and ... and Feature Bn)
or ... or
(Feature Z1 and ... and Feature Zm)

Feature X modeled by boolean variable **F_X**

Requirements(A) =
F_A =>
((F_B1 /\ ... /\ F_Bn)
\/ ... \/
(F_Z1 /\ ... /\ F_Zm))

Feature Conflicts

Features A and B are incompatible

FeatureConflict(A,B) :

$!F\_A \vee !F\_B$

Can We Combine Features A, B, and C?

Is the following formula satisfiable?

F_A /\ F_B /\ F_C

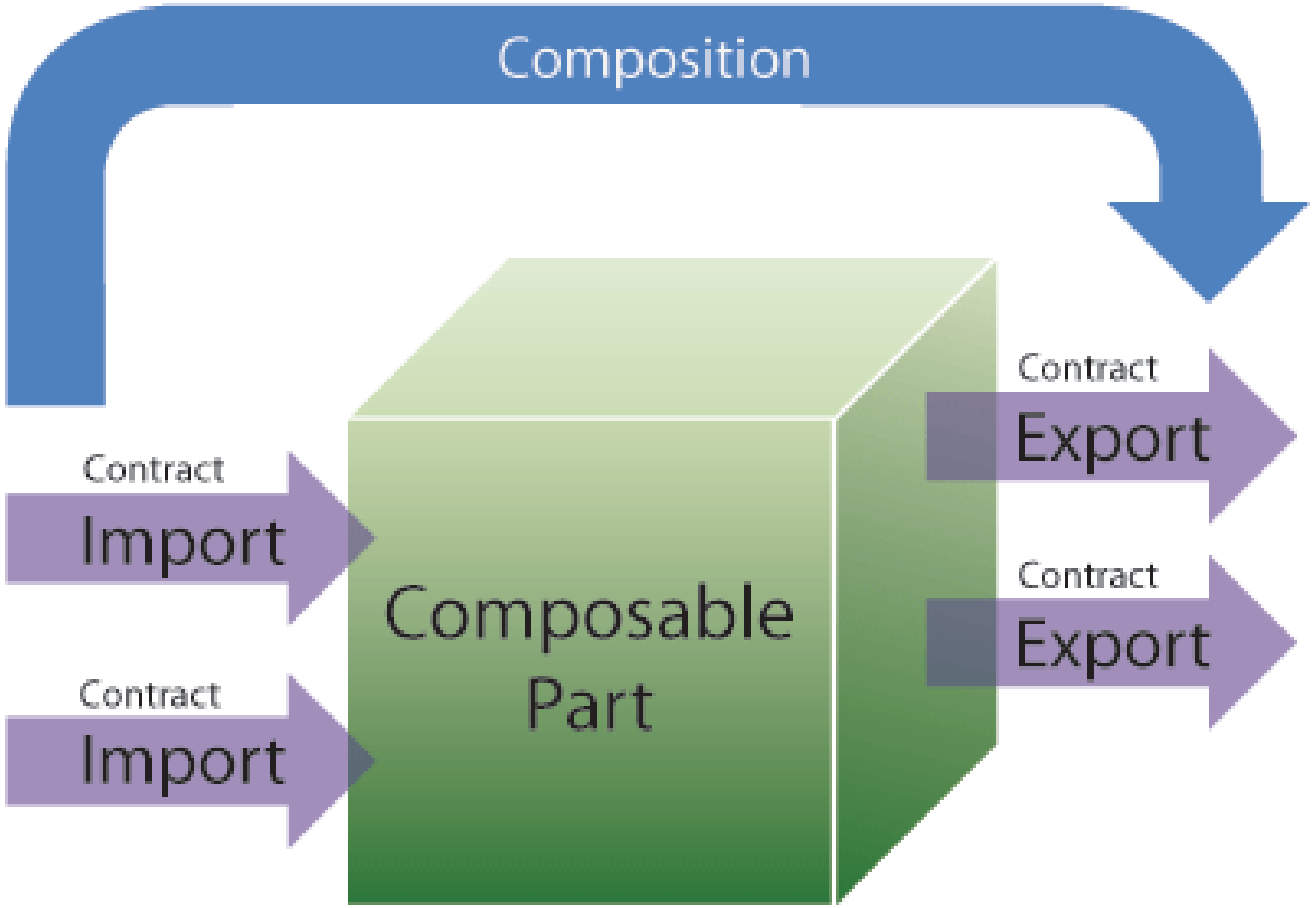
/\

Requirements(A) /\ Requirements(B) /\ Requirements(C)

/\

FeatureConflicts

Managed Extensibility Framework (.NET 4)



Managed Extensibility Framework

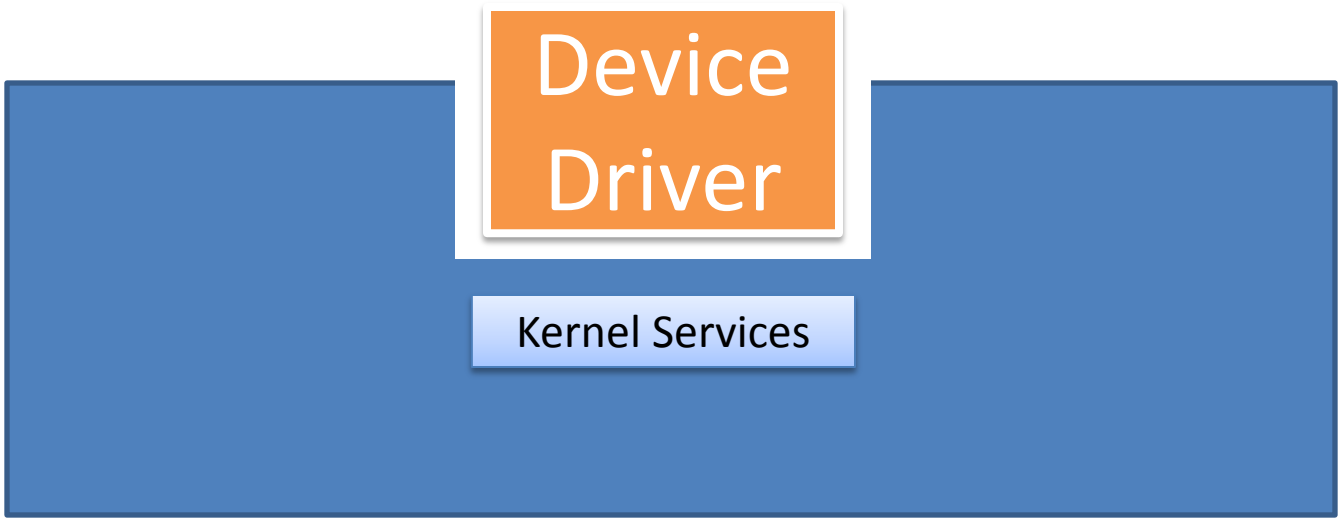
- MEF presents a solution for the runtime extensibility problem.
- MEF provides a standard way for a host to expose and consume extensions
  - Extensions can be reused amongst different applications.
  - Extensions themselves can depend on one another
  - MEF will make sure extensions are wired together in the correct order

Comparison

MEF is to Visual Studio as Equinox is to Eclipse

Sort of …

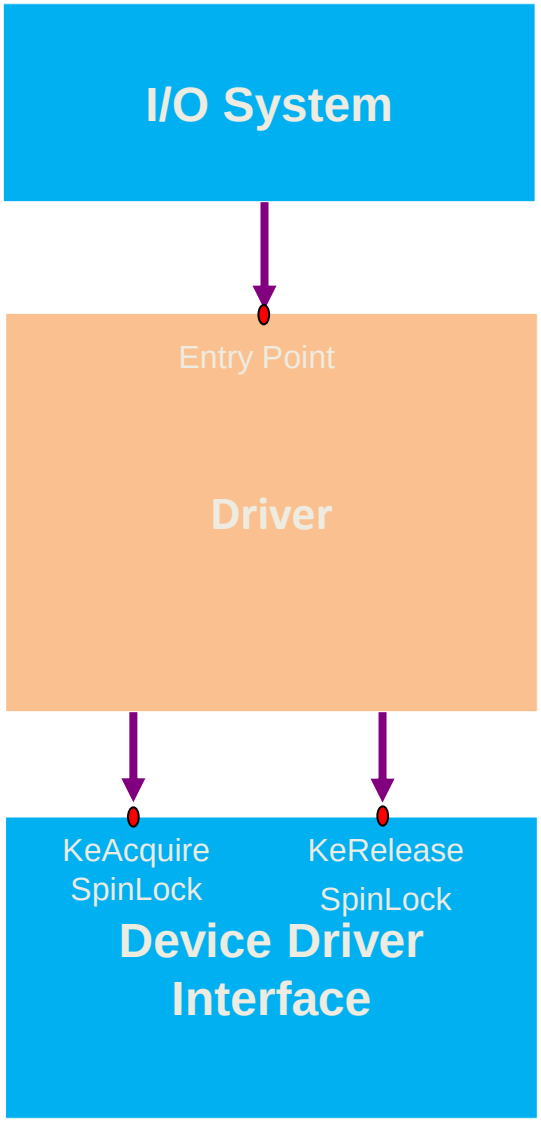
Protocols (Rules)



What are Rules? A Fact of Life!

- Proper temporal sequencing of calls to APIs
  - "Never call **IoCompleteRequest** while holding a spin lock. Attempting to complete an IRP while holding a spin lock can cause deadlocks." http://msdn.microsoft.com/en-us/library/ff548343(VS.85).aspx
- Typestate: A Programming Language Concept for Enhancing Software Reliability, Strom, Yemini, 1986
- Message Sequence Charts

SpinLock Rule



KeReleaseSpinLock - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Microsoft.com Home | Site Map

Comments

This call is a reciprocal to **KeAcquireSpinLock**. The input *NewIrql* value must be the *OldIrql* returned by **KeAcquireSpinLock**.

For more information about spin locks, see Spin Locks.

Callers of this routine are running at IRQL = DISPATCH_LEVEL. On return from **KeReleaseSpinLock**, IRQL is restored to the *NewIrql* value.

Parameters

SpinLock
Pointer to a spin lock for which the caller provides the storage.

NewIrql
Specifies the IRQL value saved from the preceding call to **KeAcquireSpinLock**.

Return Value

None

Headers

Declared in *wdm.h* and *ntddk.h*. Include *wdm.h* or *ntddk.h*.

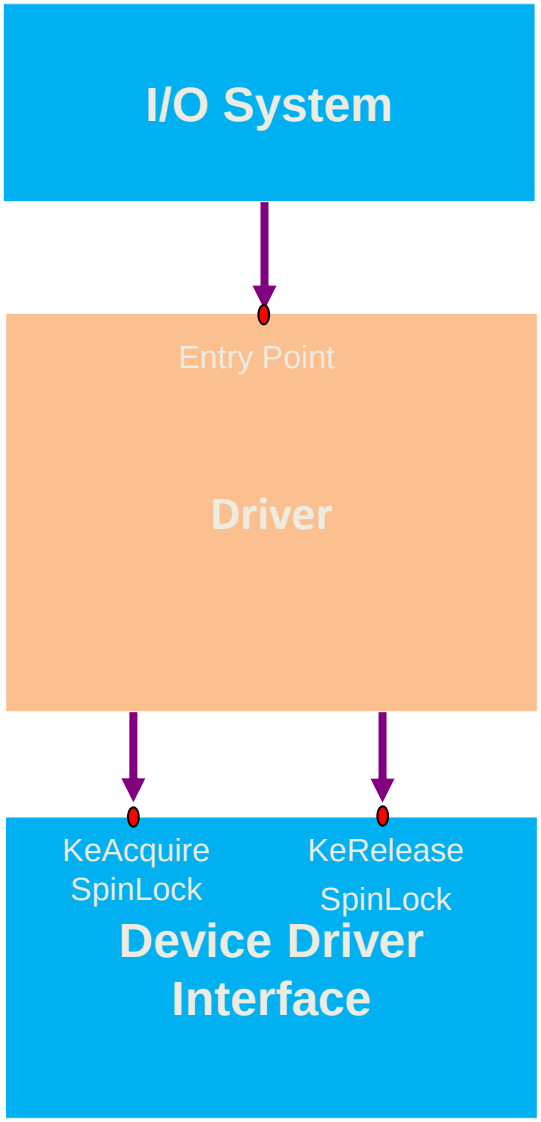
Comments

This call is a reciprocal to **KeAcquireSpinLock**. The input *NewIrql* value must be the *OldIrql* returned by **KeAcquireSpinLock**.

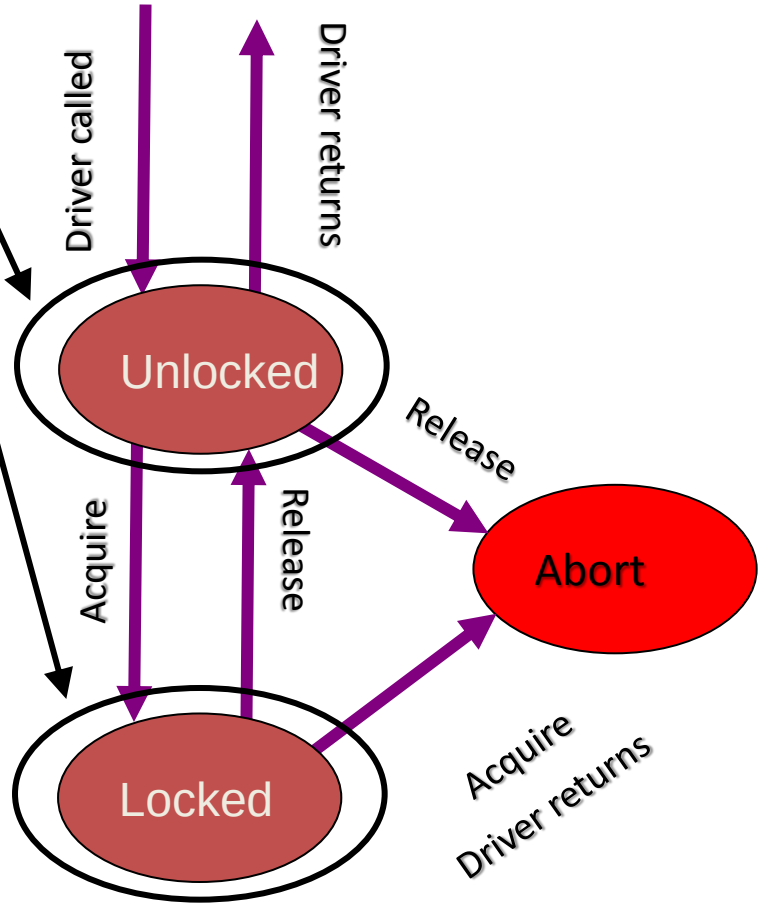
For more information about spin locks, see Spin Locks.

Callers of this routine are running at IRQL = DISPATCH_LEVEL. On return from **KeReleaseSpinLock**, IRQL is restored to the *NewIrql* value.

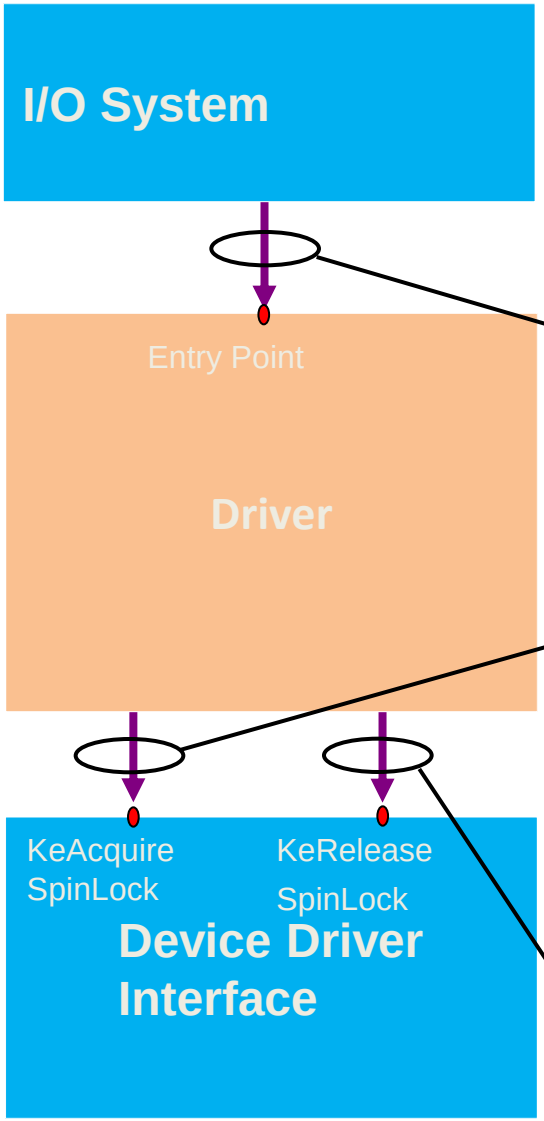
SpinLock Rule as State Machine




```
state {
  enum {unlocked, locked} s = unlocked;
}
```



SpinLock Rule (in SLIC language)

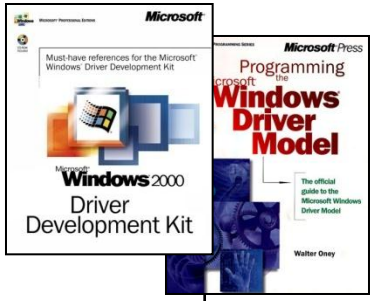



```
state {
  enum {unlocked, locked} s = unlocked;
}
```

```
RunDispatchFunction.exit
{
  if (s != unlocked) abort;
}
```

```
KeAcquireSpinLock.entry
{
  if (s != unlocked) abort;
  else s = locked;
}
```

```
KeReleaseSpinLock.entry
{
  if (s != locked) abort;
  else s = unlocked;
}
```



Rules

Development

Testing

Static Analysis

Read for understanding

Automate testing

API Usage Rules

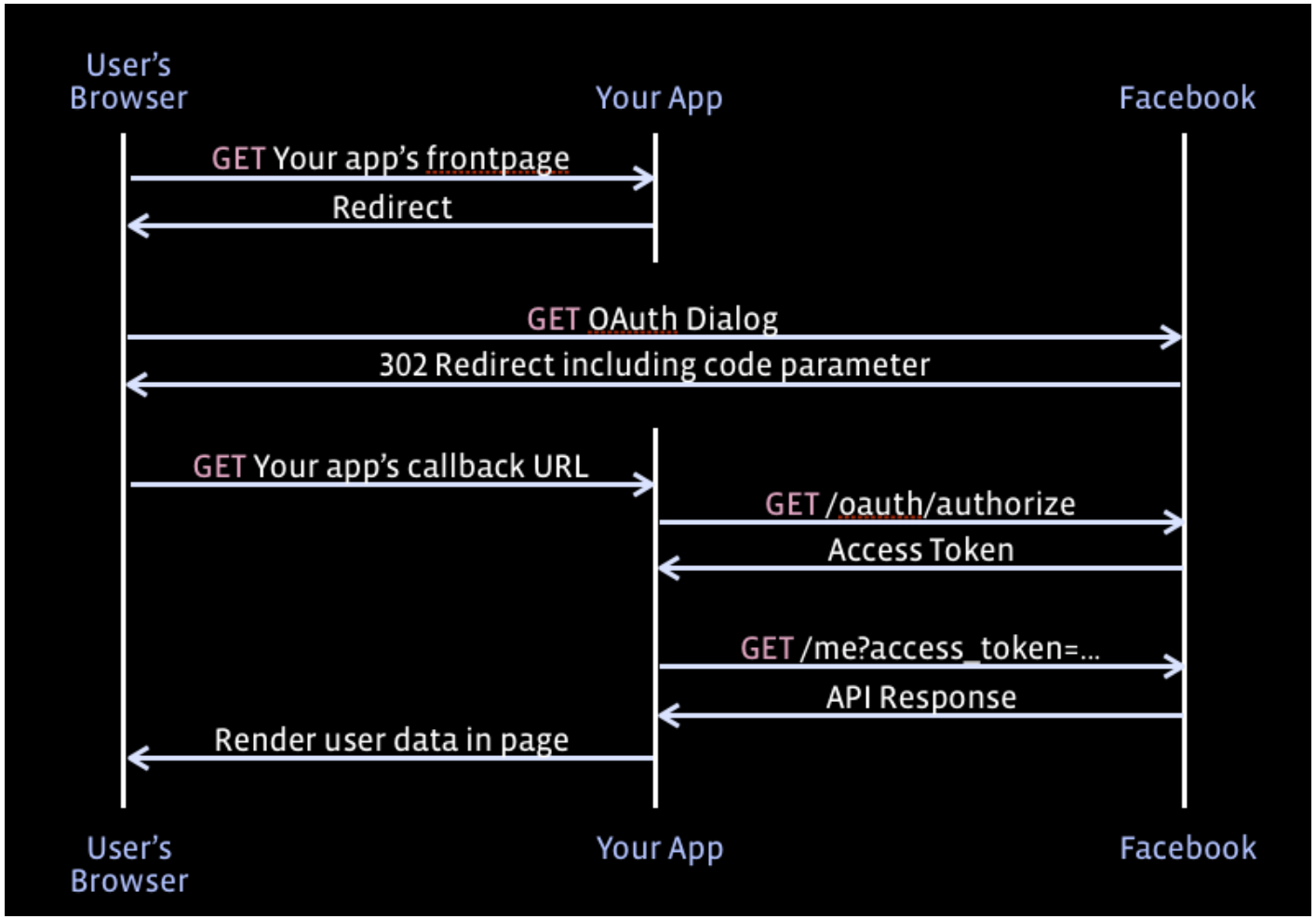
Verification Engine

Defects

100% path coverage

Source Code

Facebook Protocols

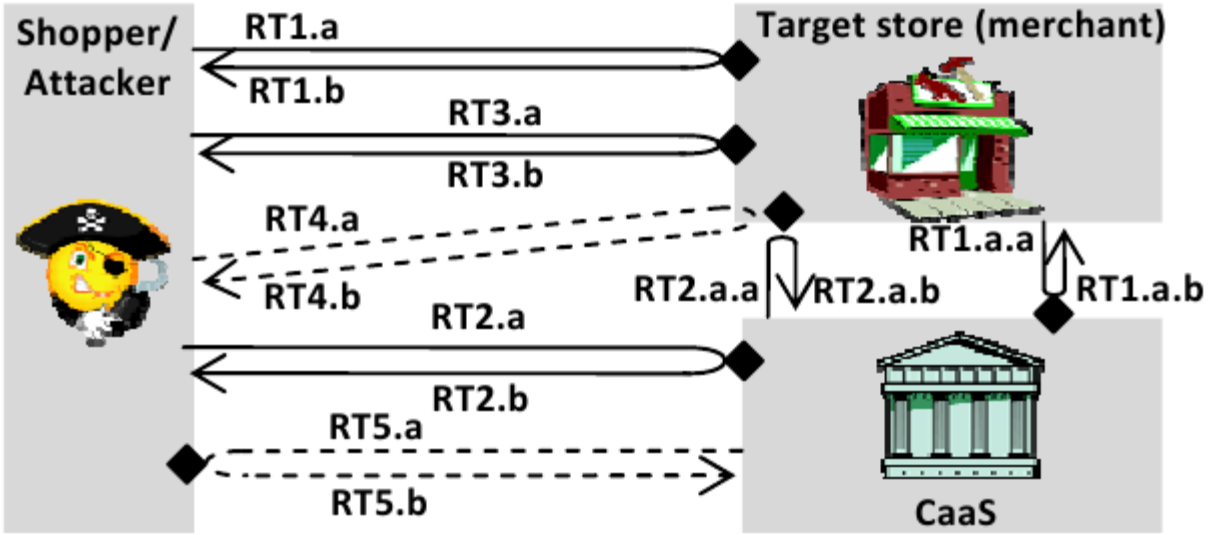


How to Shop for Free Online

Security Analysis of Cashier-as-a-Service Based Web Stores

Rui Wang[1], Shuo Chen[2], XiaoFeng Wang[1], Shaz Qadeer[2]

[1] Indiana University Bloomington [2] Microsoft Research



Feature Interaction

Feature Interaction (Zave)

- In a software system, a feature is an increment of functionality, usually with a coherent purpose
- If a system description is organized by features, then it probably takes the form B + F1 + F2 + F3 . . .
  - B is a base description,
  - each Fi is a feature module, and
  - “+” denotes some feature-composition operation
- Consider B=Integrated Development Environment

Eclipse JDT Extension Points

- org.eclipse.jdt.core.manipulation.changeMethodSignatureParticipants
- org.eclipse.jdt.debug.breakpointListeners
- org.eclipse.jdt.debug.javaLogicalStructures
- org.eclipse.jdt.junit.testRunListeners
- org.eclipse.jdt.ui.cleanUps
- org.eclipse.jdt.ui.foldingStructureProviders
- org.eclipse.jdt.ui.javaCompletionProposalComputer
- org.eclipse.jdt.ui.javaCompletionProposalSorters
- org.eclipse.jdt.ui.javaEditorTextHovers
- …

Feature Interaction: org.eclipse.jdt.debug.breakpointListeners

Description:

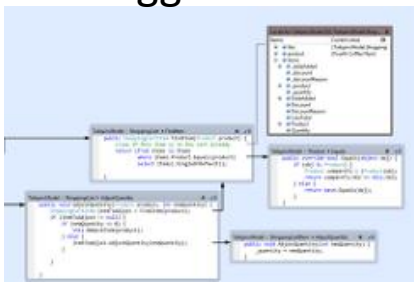
Allow clients to contribute listeners for Java breakpoint notifications. For example, listeners are called when a breakpoint is hit and about to suspend execution. *The listener can vote to resume or suspend the debug session*. …

Some Visual Studio Extensions From MSR

Editor
MSIL Rewriting

CLR Profiler

Debugger Canvas



VS Debugger

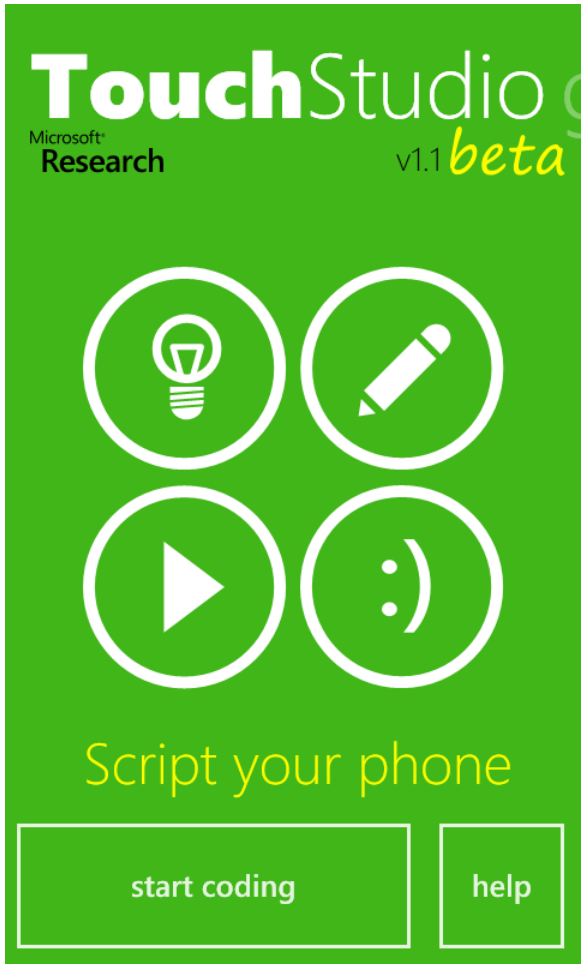
Extension Points

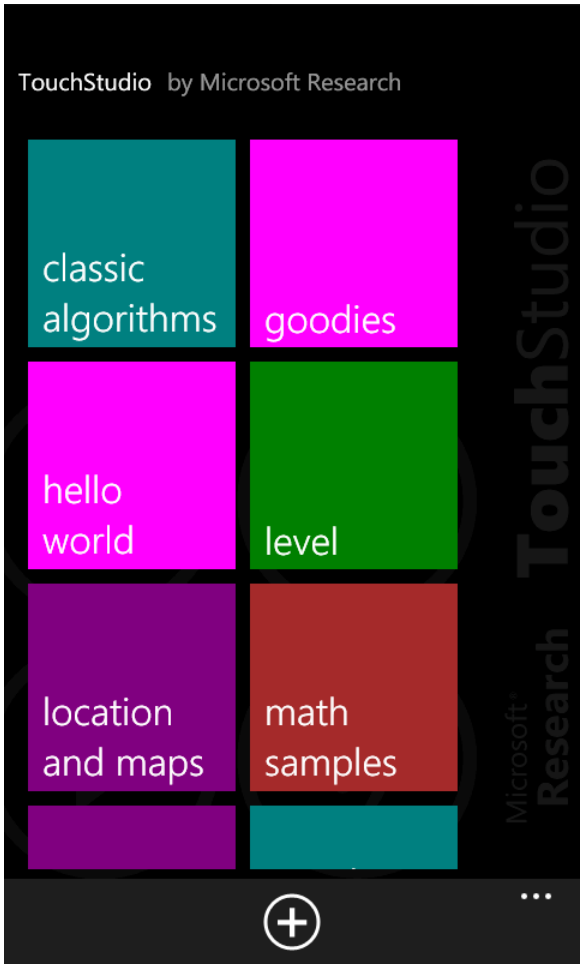
Smart Phones

Apps

- Installation requires users to permit app access to phone sensors
- Isolate, isolate, isolate
- Connectedness via copy/paste

TouchStudio: Script the Phone, On The Phone





Cloud Computing and Plug-ins

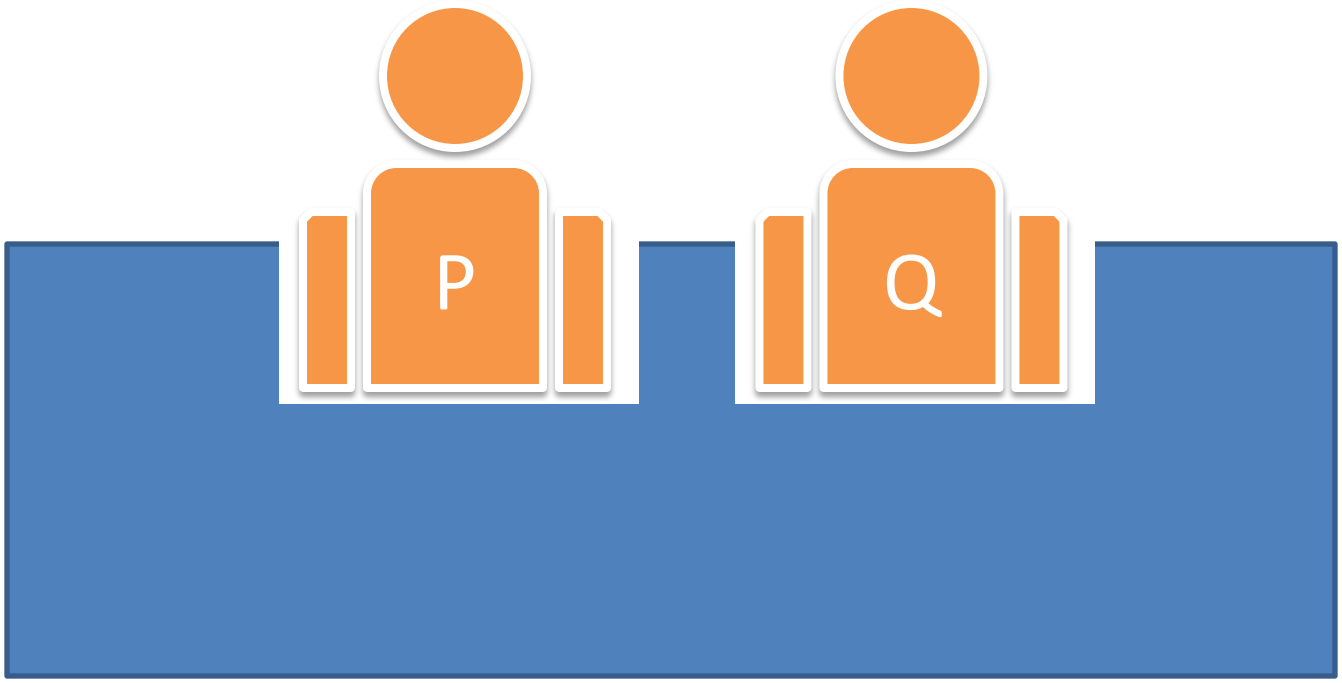
Cloud Computing = Complete Control

Programming the Salesforce Platform

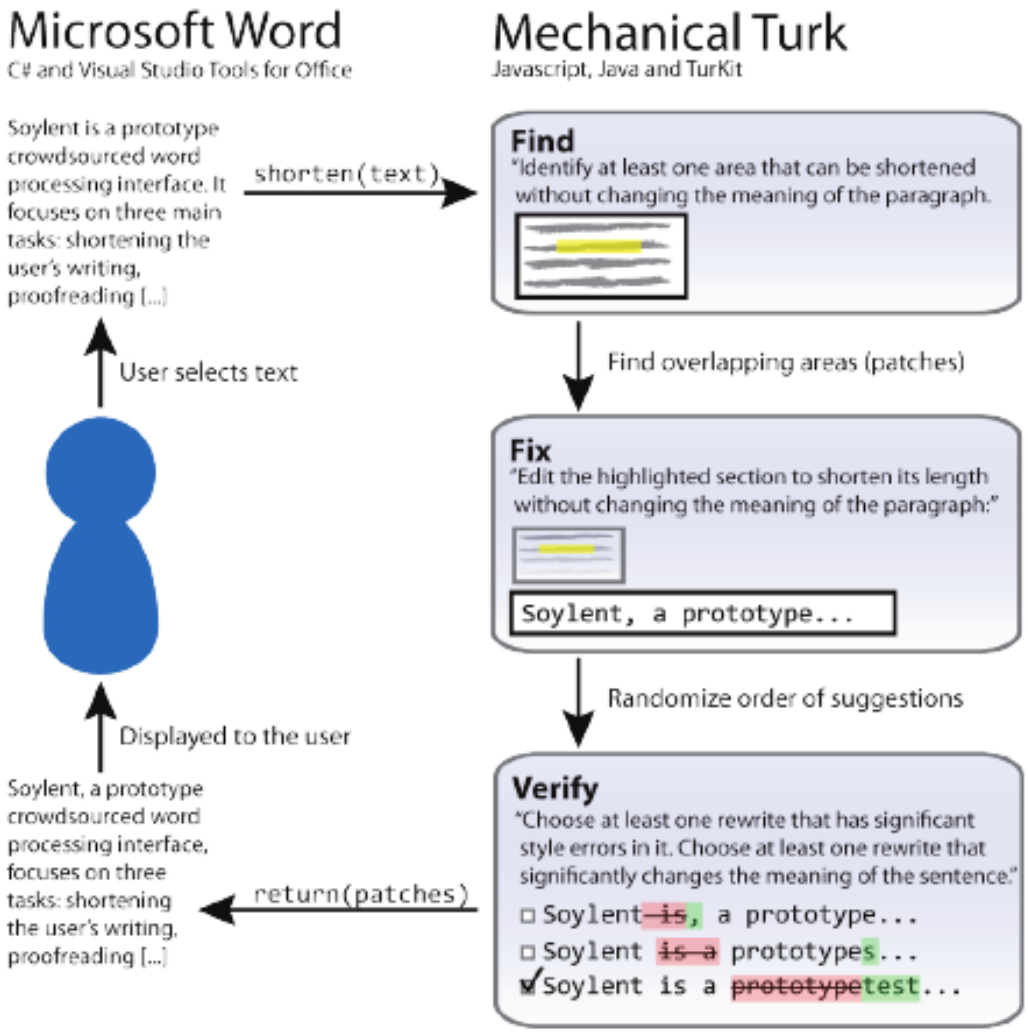
- Developers can also use the Web services API to issue data manipulation commands … Because the controlling logic for these client-side programs is not located on Force.com platform servers, they are restricted by:
  - The performance costs of making multiple round-trips to the salesforce.com site to accomplish common business transactions
  - The cost and complexity of hosting server code, such as Java or .NET, in a secure and robust environment

- To address these issues, and to revolutionize the way that developers create on-demand applications, salesforce.com introduces Force.com ***Apex code, the first multitenant, on-demand programming language*** for developers interested in building the next generation of business applications.

Human-based Computation



Example from MIT
Soylent: A Word Processor with a Crowd Inside



Bernstein, M., Little, G., Miller, R.C., Hartmann, B., Ackerman, M., Karger, D.R., Crowell, D., and Panovich, K. Soylent: A Word Processor with a Crowd Inside. In Proc. UIST 2010. ACM Press

An IDE with a Crowd Inside?