A Paradigm Shift

Software Innovation
for
Security & Flexibility

V1.3

(Patented US #7,322,028, #8,924,928, others pending)

Cyber Security = “Trust”

- **"Trust"** means that the **entire IT system** will do the following:
  - Operate ONLY on behalf of authorized personnel
  - Never operate on behalf of unauthorized personnel
  - Do exactly what is it supposed to do
  - Never do anything it's not supposed to do
- **Net-centric cyber defense techniques fail** because the TCP/IP network protocol permits “challenge-and-response” without authentication. Therefore, it cannot be trusted.
- **Data encryption techniques fail** because the software process that implements those techniques is built on a platform that cannot be trusted. Anything built on top of an untrusted platform cannot be trusted. (Note: encryption processes built on a trusted platform CAN be trusted)

Basic Concepts 1

Asking Basic Questions

- Can I protect my network 100%?

  No. TCP/IP protocol security flaws prevent this

- Can I make existing software systems “secure”?

  No. “Prophylactic software” cannot improve a bad design

How much time and money
have been wasted
attempting the impossible?

Basic Concepts 2

Common Security Questions & Models

- Can I put my data in a “vault” and protect it that way?

  Yes - but the data is then unusable! The “vault” model is inaccurate. Data is not a “physical thing” that can be guarded like a bank vault. Also, transfer of data to/from a “vault” requires a software process which by itself creates exposure.

- Can I “add on” security via some “appliance”?

  No. Security must be built-in to the O/S, and ALL software above it. Additionally, the data objects must have “marking” to indicate allowed access. The USAF's “Reference Monitor” can then enforce the security policy, using the “object marking”. Data object “marking” must be “built-in” to the object so that it is indelible. It cannot just be “added on”.

Basic Concepts 3

Software Models

- Why is software so difficult when it comes to security?

Software is the implementation of an algorithm. An algorithm is a step-by-step process for doing something.

The goal of software is to do what you want it to do - on behalf of only authorized people.

The goal of the hacker is to alter that algorithm so that it does what the hacker wants it to do – while “faking you out” so that it still does what you want it to do (mostly).

Security means protecting the “process” or “algorithm” - not just the “data”!

Basic Concepts 4

How IQware is Really Different

- What Makes IQware Fundamentally Different?

Everyone else tries to protect the network and/or the data. Both cannot be done with 100% success because they require a secure software process to do that. If you cannot "trust" the software process, then you can't "trust" anything that it does or touches – including your data!

IQware's patented architecture provides a ***secure software process*** that provides any desired SaaS functionality, governed by rules. You get functionality, flexibility and security in one software system. We are the first organization to do that.

That's the "IQ" difference!

Basic Concepts 5

- What you're doing now doesn't work
- There's no way to “make it work”
- Must rethink the ENTIRE thing

Need a clean sheet of paper!

Secure Design – 6

Basic Concepts 6

(The Hardest Part: Making Room for New Ideas)

New Ideas

Old ones don't work

Gotta create new possibilities

Three Kinds of Ideas

1st Kind: Ideas that solve problems (nice)

2nd Kind: Ideas the prevent problems (nicer)

3rd Kind: Ideas that create new possibilities (best!)

IQware

(A Category 3 Idea!)

Why Software Stinks

Too Expensive

Too Long to Create

Customer Hates It

What Is Innovation?

Creating New Possibilities
& Markets Using Invention

Innovation isn't understood
and it's ignored

What Is Cyber Security?

Only Authorized People Can
Use Your “Stuff”

Always Guarantee Correct
System Operation

Here Is Your “Box”:

You're Doing Exactly What Grandpa Did!

(Nothin' New)

Get Out of the Box!

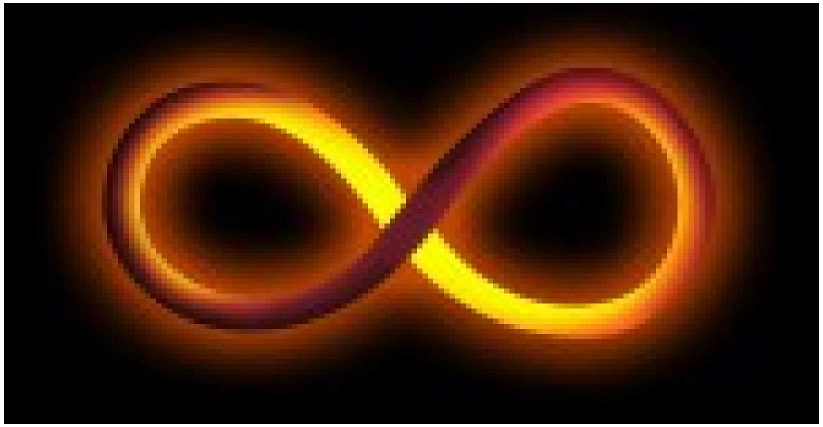
Question ALL Assumptions

Are Programmers Really Needed?

Useful Ideas (From Diverse Fields)

Language, DNA, Numbers
Use Finite Set of Symbols

They Can Form Infinite
Combinations

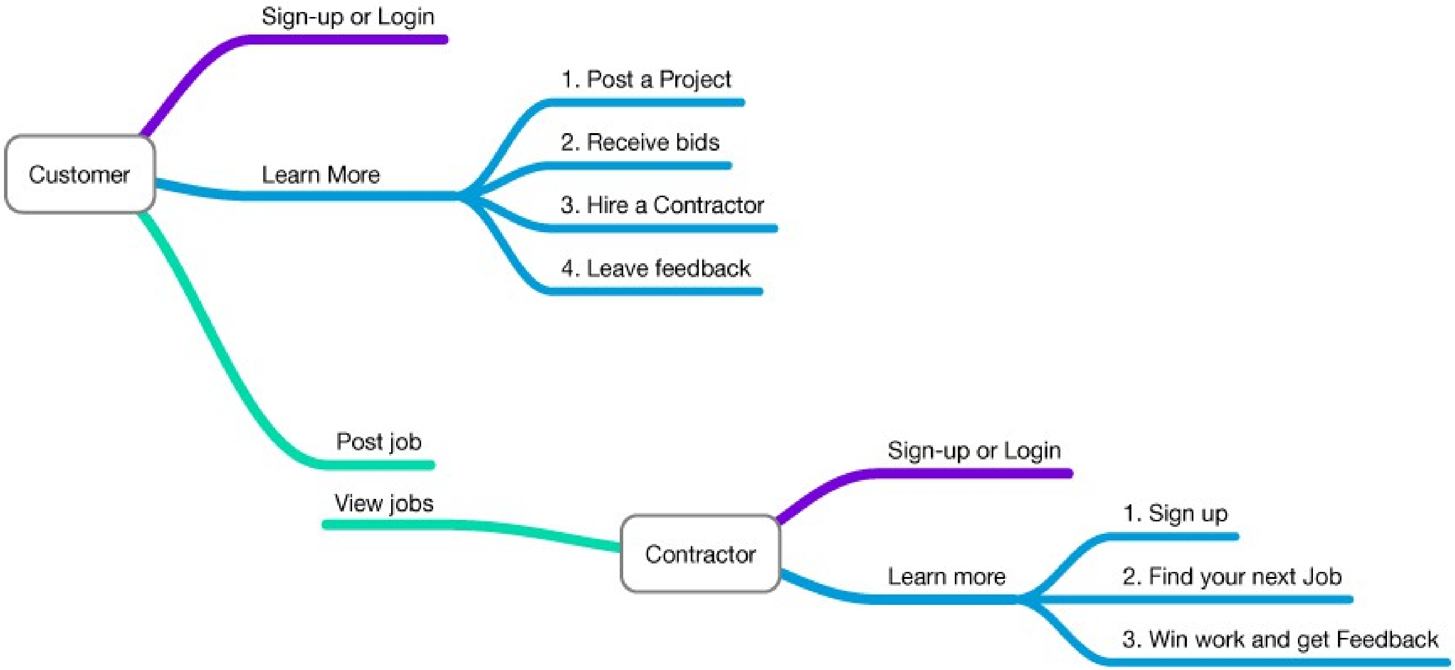


Software Apps – What's Needed?

Workflow

Dataflow

UX (User Experience)



Software Creation Idea

Stop Writing Code!

Create New Symbol Set

Graphically Configure To Implement App

Summary

Use Symbol Set – Not Code

Use Secure O/S (USAF)

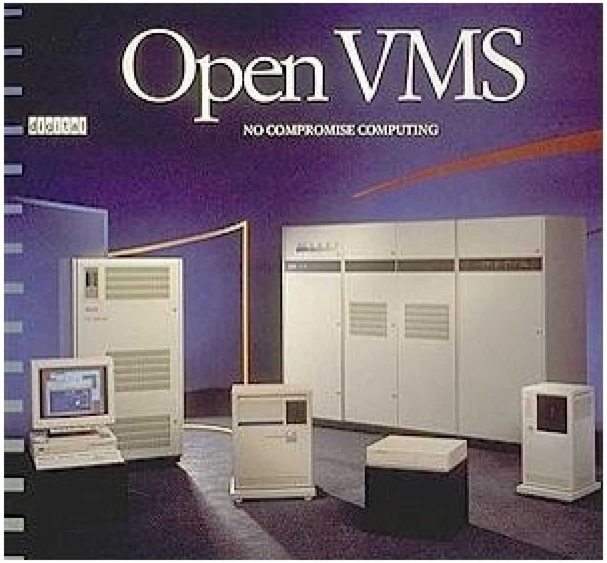
Configuration + Symbols + Secure O/S = App

What We Know Now – Dirty Little Secret 1

The “Dirty Little Secret”

(We Know How to Solve The Security Problem)

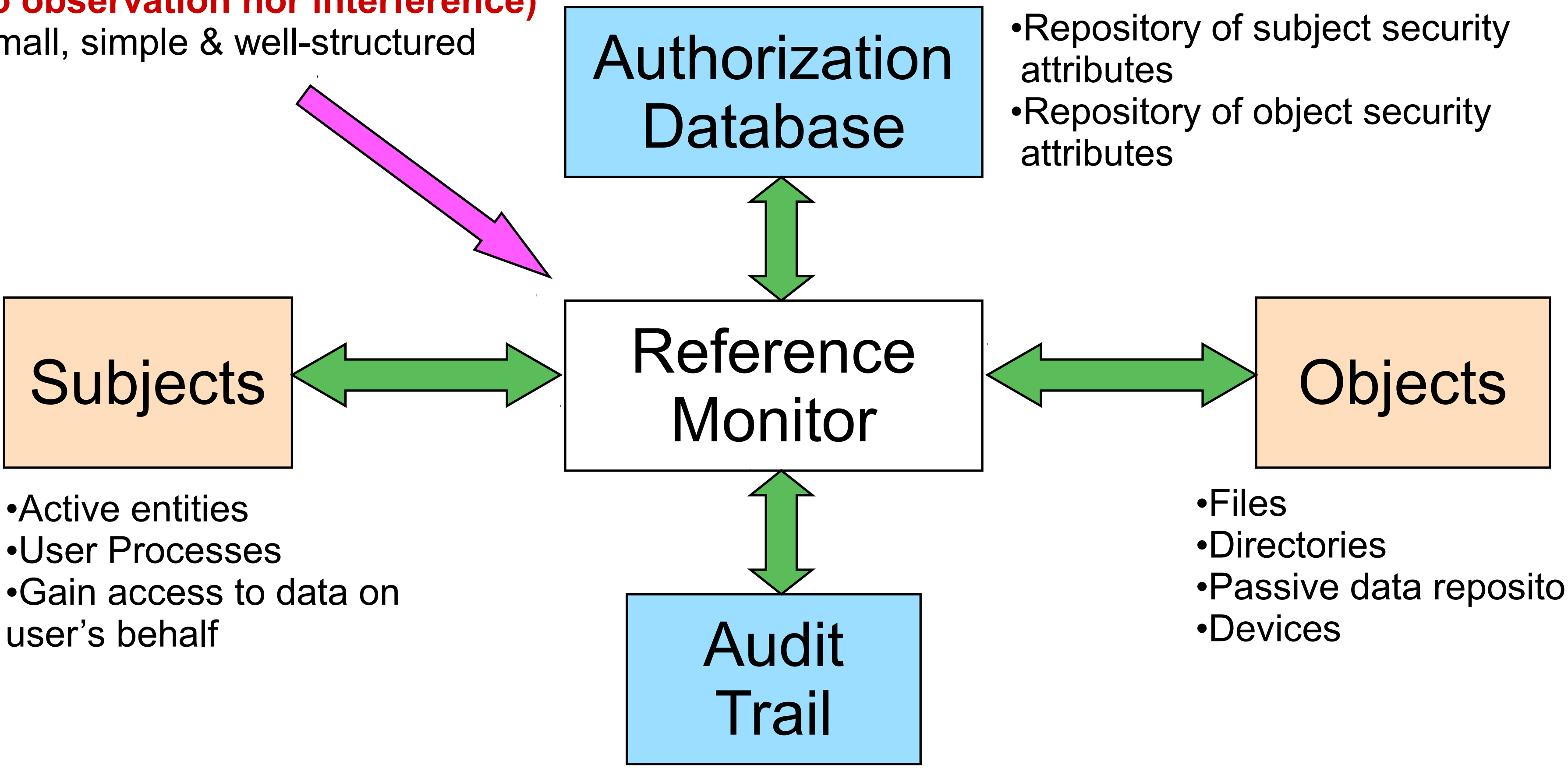
- October 1972 – USAF produces “Computer Security Technology Planning Study” (ESD-TR-73-51 Vol.II, produced per contract with James P. Anderson & Co.) – they invent the “Reference Monitor”, a secure system architecture.
- April 1974 – Barry Schrager @IBM headed up the RACF (data security stuff) project. They implement what they can but the economics of the installed base prevents wide adoption of a fundamentally new O/S architecture.
- Mid 1970s - DEC was transitioning from the 16-bit PDP-11 to the new 32-bit VAX architecture so a new O/S was warranted. They included most of the “Reference Monitor” in the design of their VMS O/S.
- Mid 1980s – Business apps start migrating to PCs because they are perceived to be cheap - no real plan for scale-up nor security.
- Mid 1990s – Deployment of critical business apps and government apps to desktops continues, networking is ubiquitous, security issues becoming important.
- 1998 - Compaq buys DEC
- 2001 - HP buys Compaq.
- 2011 – The only transaction-based, real-time O/S that has not been successfully hacked (when configured properly) is OVMS (c.f., DEFCON 9 in 2001, Kevin Mitnick's testimony).
- August 2014 – HP sells OVMS to VMS Software, a well-financed startup which has rehired the “old DEC guys” who designed it.



The Reference Monitor

(A Secure System Architecture USAF, October 1972)

- Enforces security policy
- Mediates all attempts by subjects to access objects
- Tamperproof database & audit trail **(no observation nor interference)**
- Small, simple & well-structured

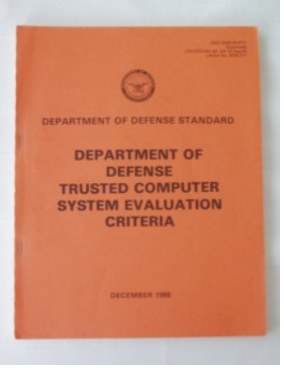


- Repository of subject security attributes
- Repository of object security attributes

- Active entities
- User Processes
- Gain access to data on user's behalf

- Files
- Directories
- Passive data repositories
- Devices

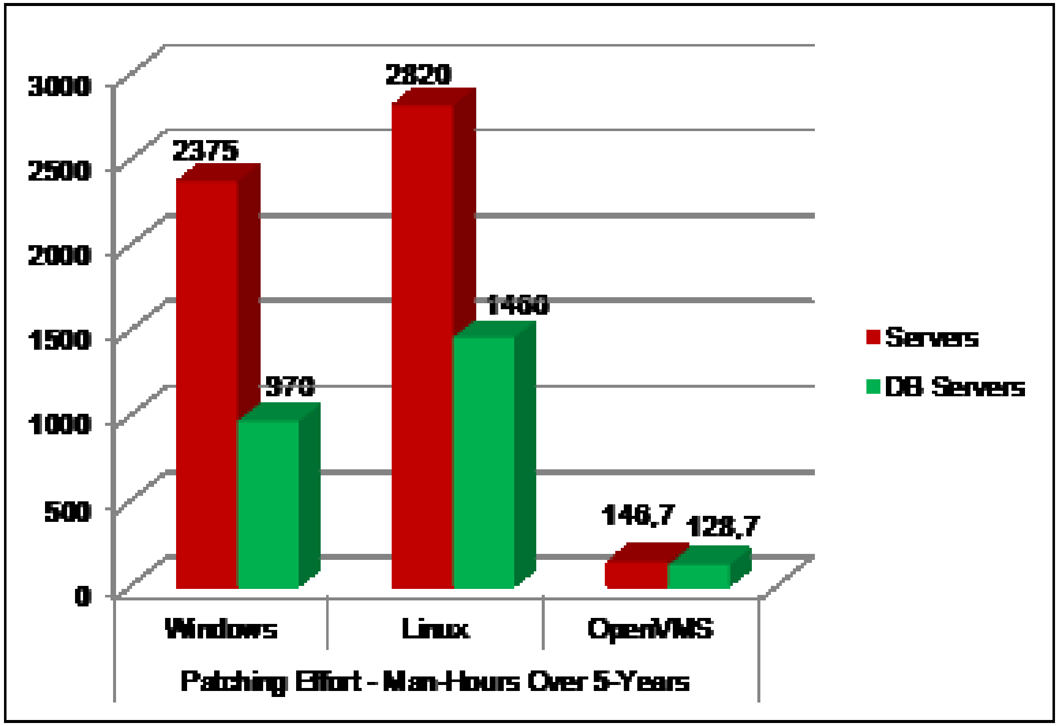
- Record of all security-related events


DEPARTMENT OF DEFENSE STANDARD
DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA
DECEMBER 1985

Secure Design 1

Basic Guidelines

- Don't assign mission critical operations to a non-secure platform. If you have already done so, then migrate away from that ASAP.
- Re-architect your data sources' IT connections to control the valuable (& vulnerable) data pathways.
- Use a secure platform (DoD B2/C2 per DoD 5200.28 minimum) for any SaaS deployment or any centralized data handling.
    - Note: The Orange Book or DoDD 5200.28-STD was canceled by DoDD 8500.1 on October 24, 2002. DoDD 8500.1 reissued as DoDD 8500.02 on March 14, 2014.
- Use a platform with a true real-time kernel and that qualifies as a TCB per DoD specifications.
- Use a platform that does NOT have a “back door”.
- Spend the dollars to do it right the first time – it's a LOT cheaper that way.
- Be open to new ideas and paradigm shifts.



Secure Design 2

Paradigm Shift: A new Way To Create & Deliver IT Functionality

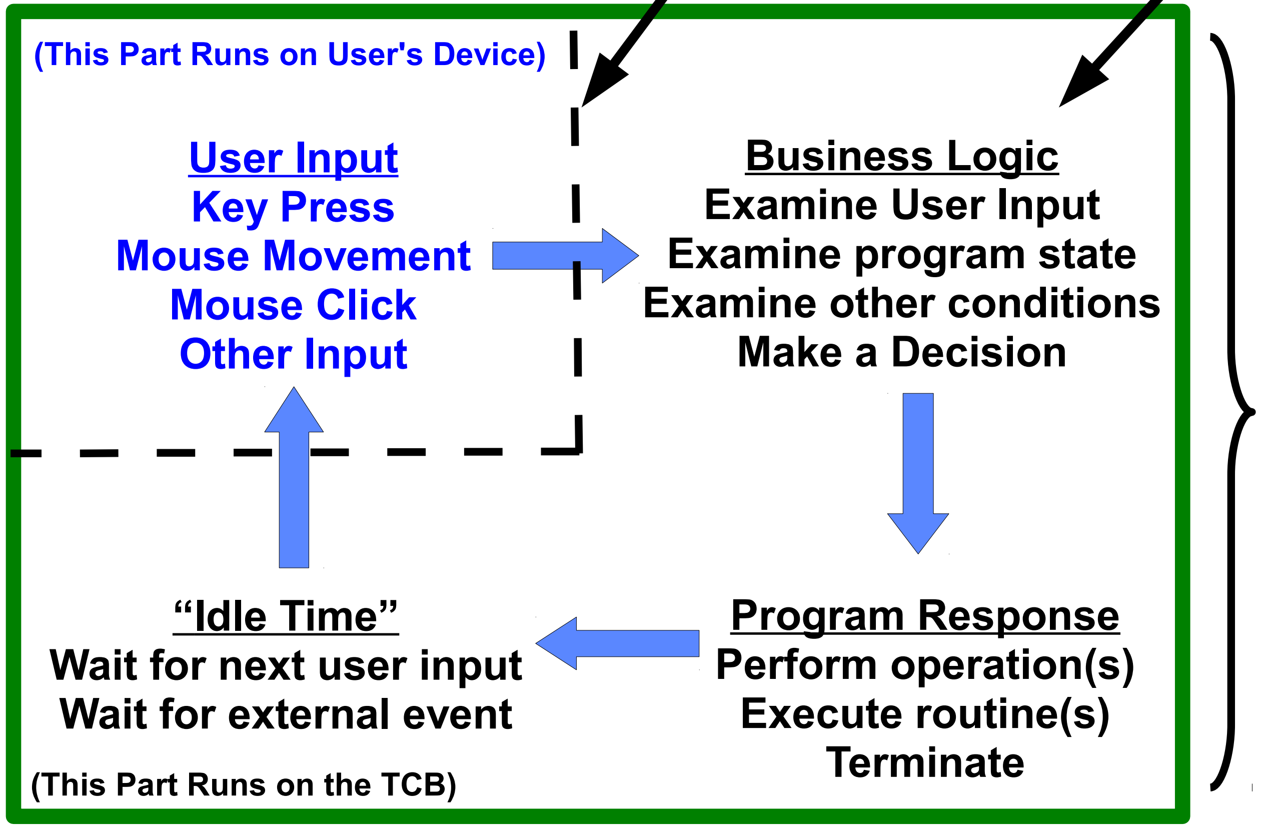
This part of the app runs on ANY client!
Malware stays here

This part of the app runs on a DoD secure server
No malware here

Typical App Flowchart

Invention #1:
We "cut" the app along this line for SaaS deployment and user device interoperability

Invention #2:
We put this piece on a DoD rated secure server for virus-immunity



(This Part Runs on User's Device)

User Input
Key Press
Mouse Movement
Mouse Click
Other Input

Business Logic
Examine User Input
Examine program state
Examine other conditions
Make a Decision

"Idle Time"
Wait for next user input
Wait for external event

Program Response
Perform operation(s)
Execute routine(s)
Terminate

(This Part Runs on the TCB)

Invention #3:
This part is 100% controlled by RULES and not by hard-coded logic

(Patented US #7,322,028, #8,924,928, others pending)

Secure Design 3

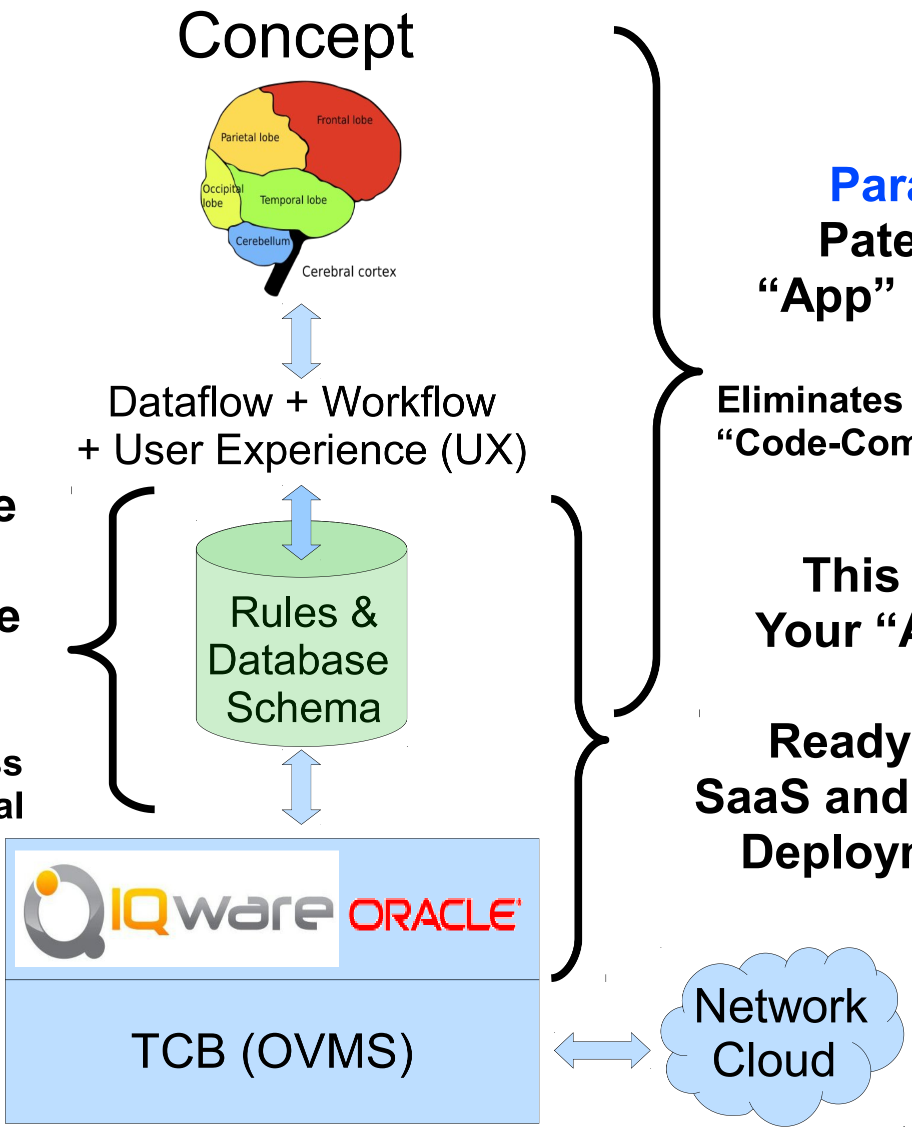
Paradigm Shift: A New “Full-Function” Rule Structure

- IQware uses “Rules” to implement the desired “App”
- Rules control all business logic, program state determination, other miscellaneous conditions
- Rules control all program decisions and responses
- Rules control all visual aspects of the App, including screen appearance, menus, toolbars, etc.
- Rules control all database access, data formatting, data presentation and data display
- Rules define and control a “superset” to SQL so that all rule-operations can be used to create SQL strings for database operations “on-the-fly” at run-time via “special directives” (Patented, US #8,924,928)
- Rules consist of event(s) action(s), data sources (DS), data destinations (DD), data transformations (DT), auditing parameters, O/S permissions and other miscellaneous control parameters
- Rules can operate on themselves and are fully extensible
- Rules can send commands, files, etc. to foreign platforms and foreign systems for easy integration with existing software installations and IT systems
- Rules are configured graphically without any programming
- Rules can be changed “on-the-fly” so new functionality can be added while the application is running

(Patented US #7,322,028, #8,924,928, others pending)

Secure Design 4

Game Changer: A New Software Development Process & Structure



Paradigm Shift: **Patented IQware "App" Design Process**

Eliminates the costly, error-prone "Code-Compile-Test-Debug" loop

Paradigm Shift: **Patented IQware Rule "Event-Action" Structure**

It's Part of the Development Process AND Part of the "Final App"

This is Your "App"

Ready for SaaS and Mobile Deployment!

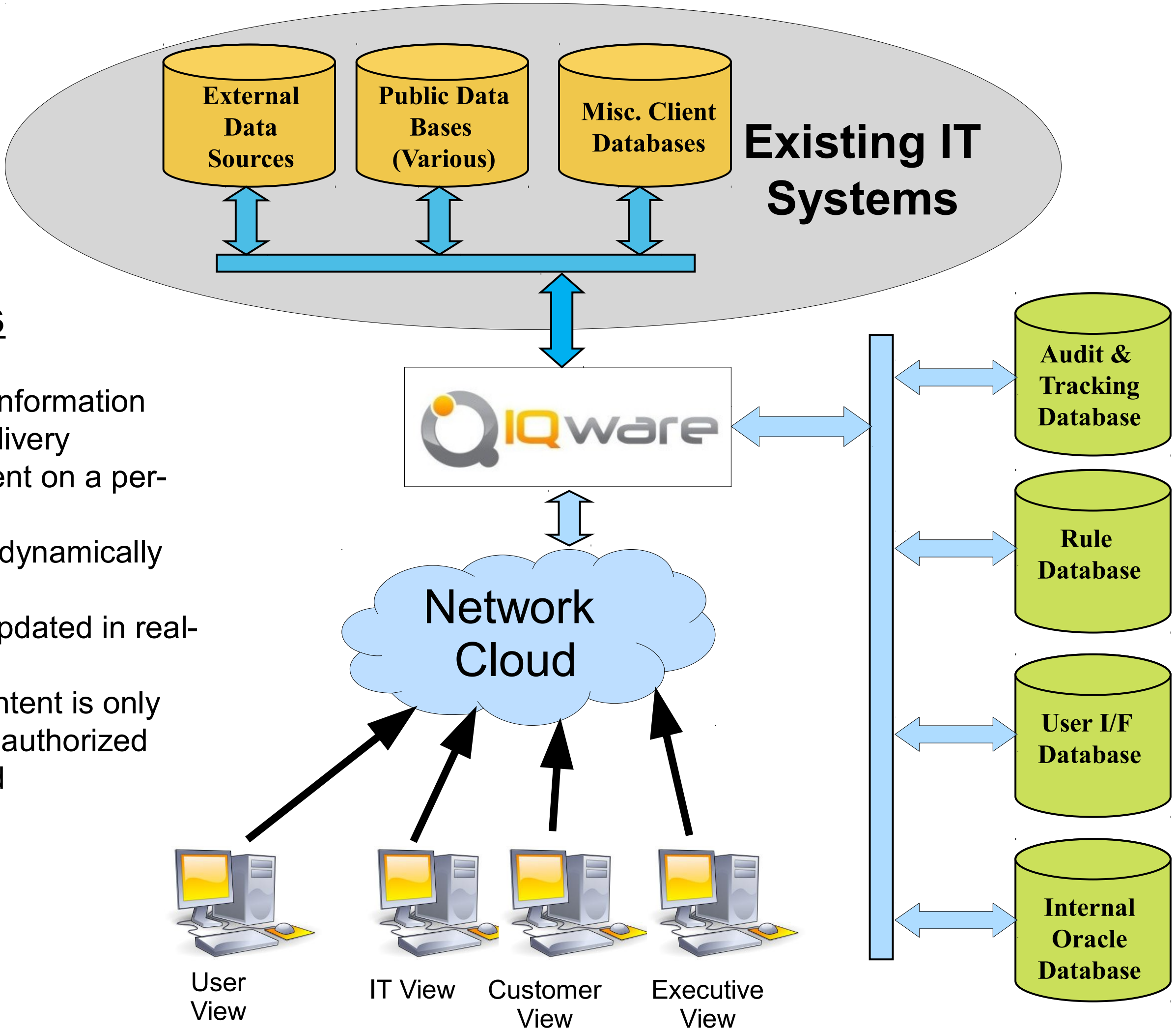
Paradigm Shift: **Patented IQware "App" Structure and Deployment**

Easy integration with new desktop and mobile technologies

(Patented US #7,322,028, #8,924,928, others pending)

Secure Design 5

Game Changer: A New SaaS Deployment Model



Key Advantages

1) Secure via the TCB
2) Can track and control information access and content delivery
3) Supports tailored content on a per-requestor basis
4) Content's appearance dynamically alterable
5) Functionality may be updated in real-time.
6) Physically secure – content is only displayed when/where authorized and properly requested

Key Attributes

1) Hacker-Proof & Secure.
2) Secure audit trail for all data access and edits.
3) Interoperable – use any mobile or desktop client.
4) Can work with existing IT systems.

Reports (Outputs)

1) To Administrators
2) To Users
3) To Accounting
4) To Regulatory Authorities

Other Inputs

1) Manual data entry.
2) Existing IT Systems
3) Existing legacy processing systems.

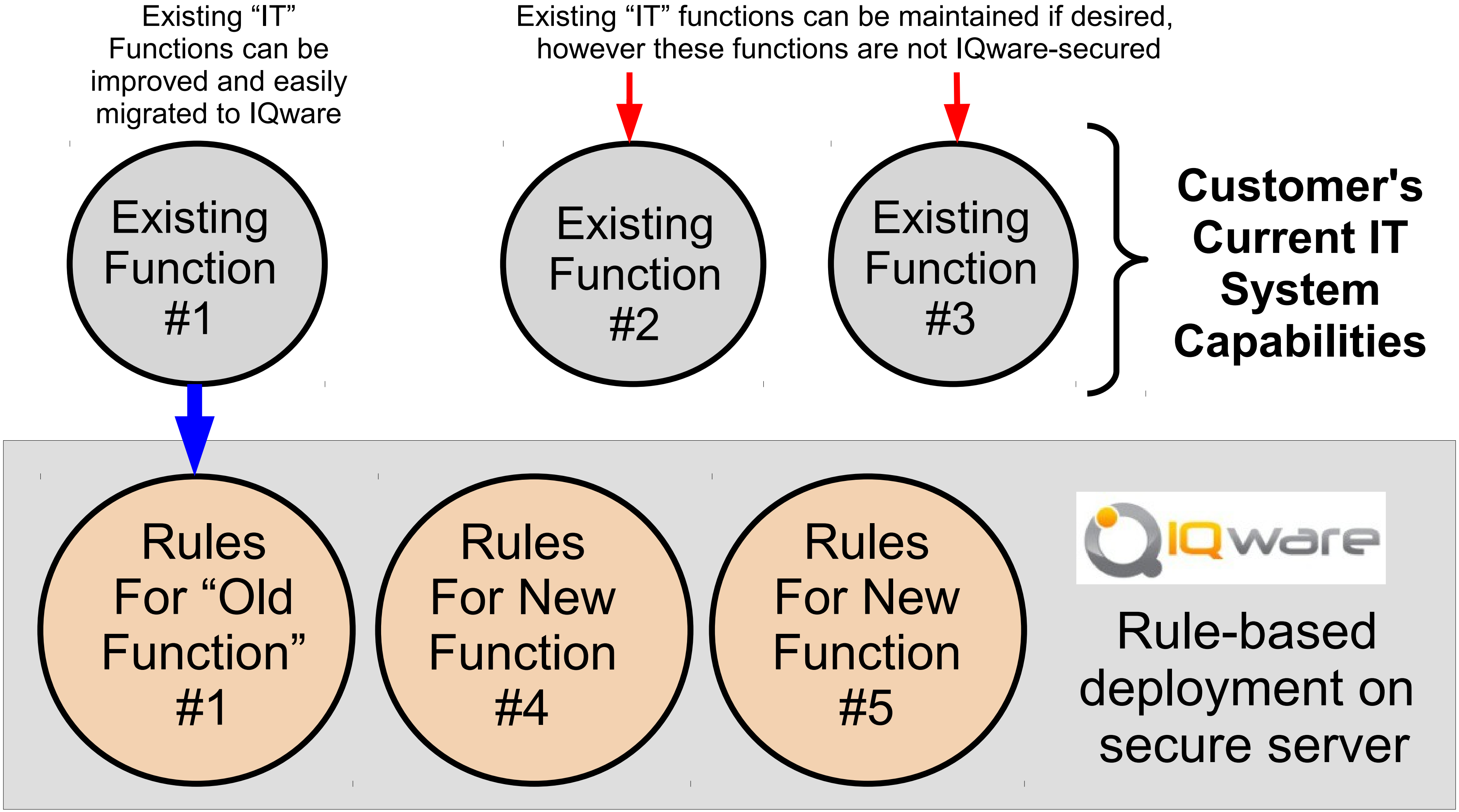
Authorized Users

1) User-specific views based upon login credentials
2) Content control, audit & reporting based upon approved roles

(Patented US #7,322,028, #8,924,928, others pending)

Secure Design 6

Game Changer: A New Systems Integration (SI) Model


Existing "IT"
Functions can be
improved and easily
migrated to IQware
Existing "IT" functions can be maintained if desired,
however these functions are not IQware-secured
Existing Function #1
Existing Function #2
Existing Function #3
Customer's Current IT System Capabilities
Rules For "Old Function" #1
Rules For New Function #4
Rules For New Function #5
IQware
Rule-based deployment on secure server

IQware delivers NEW functionality ... in a SECURE environment

(Patented US #7,322,028, #8,924,928, others pending)

The IQware Difference

(US #7,322,028, 8,924,928, others pending)

- We are built on a trusted platform (c.f. “Computer Security Technology Planning Study”, ESD-TR-73-51 which contains the “Reference Monitor” design, DoDD 5200.28, DoDD 8500.1, DoDD 8500.02, etc.)
- We do not deploy any key functionality on an untrusted platform
- We do not deploy any key software pieces on an untrusted platform
- We do not distribute critical data to an untrusted platform
- We provide a trusted software process that delivers whatever functionality is required for the "App"

Summary - 1

Game Changer: Transformational Value

Securing & Preserving IT Investment with IQware

- IQware invented a new way of describing an idea to the computer
- IQware skips costly “traditional programming”
- IQware avoids error-prone “module-based” software design
- IQware delivers functionality to the customer by a simple formula:

IQware + Rules + Oracle + (TCB) = Secure App

Put YOUR software functionality here!

(preserve your investment)

(Patented US #7,322,028, #8,924,928, others pending)

Summary - 2

Game Changer: Transformational Value

Securing & Preserving IT Investment with IQware

- Software functionality is delivered for 1/5th the cost
- Software functionality is delivered in 1/4th the time
- Software functionality is secure because TCB implements all of the dataflow, workflow and UX (user experience) via IQware's patented rule processor
- The user's “device” (e.g., smartphone, laptop, tablet, etc.) is turned into a “dumb terminal” via the ultra-thin “XLIB” client and is thus is not handling the “work” of the app – that's all done on the TCB.
- Can use the latest mobile technologies without worrying about the myriad security issues that other “traditionally developed” apps have.
- Can use the SaaS deployment model, which allows the very profitable “tax the transaction” revenue model.
- Can customize revenue model as needed per customer for maximum revenue generation.

(Patented US #7,322,028, #8,924,928, others pending)

Why Use IQware ?

- Traditional Software:
  - Costs too much
  - Takes too long
  - Customers hate it
  - Inflexible
  - Not secure

I NEED A COST ESTIMATE ON YOUR PROJECT.
E-mail: SCOTTADAMS@AOL.COM
I HAVE NO IDEA. I HAVEN'T EVEN GATHERED THE USER REQUIREMENTS.
DON'T WORRY. I WON'T HOLD YOU TO THE ESTIMATE.
© 2007 Scott Adams, Inc./Dist. by UFS, Inc.
YES YOU WILL. YOU WILL PUT IT IN THE PLAN, FORGET WE HAD THIS CONVERSATION, AND FIRE ME WHEN I GO OVER BUDGET.
GIVE ME A NUMBER OR I'LL FIRE YOU RIGHT NOW.
OKAY, IT WILL COST TEN MILLION DOLLARS.
THAT'S TOO HIGH.
IF YOU ALREADY KNOW THE COST, WHY ARE YOU ASKING ME?
www.dilbert.com
SO YOU'LL FEEL LIKE YOU HAD INPUT.
IS INPUT SUPPOSED TO FEEL THIS BAD?

© Scott Adams, Inc./Dist. by UFS, Inc.

The IQware Paradigm Shift

Cut costs by 5x
Reduce time by 4x
Secure & Flexible
Cloud-ready

It's Time to Think Differently!