

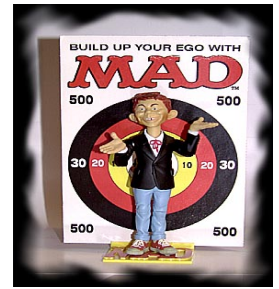
# IQware Architecture

What We Do Differently  
(The Right Technology at the Right Time)



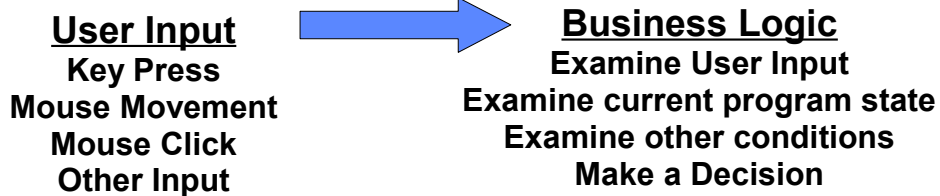
Dr. Steve G. Belovich  
([www.iqware.us](http://www.iqware.us), [www.iqmtm.com](http://www.iqmtm.com))  
June 10, 2010

# Software Application Structure



What, Me Worry?

## PC or PC Server



- **Malware can observe this process**
- **Malware can interfere with this process**
- **Malware can steal data stored in RAM**

**“Idle Time”**  
Wait for next user input  
Wait for external event

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

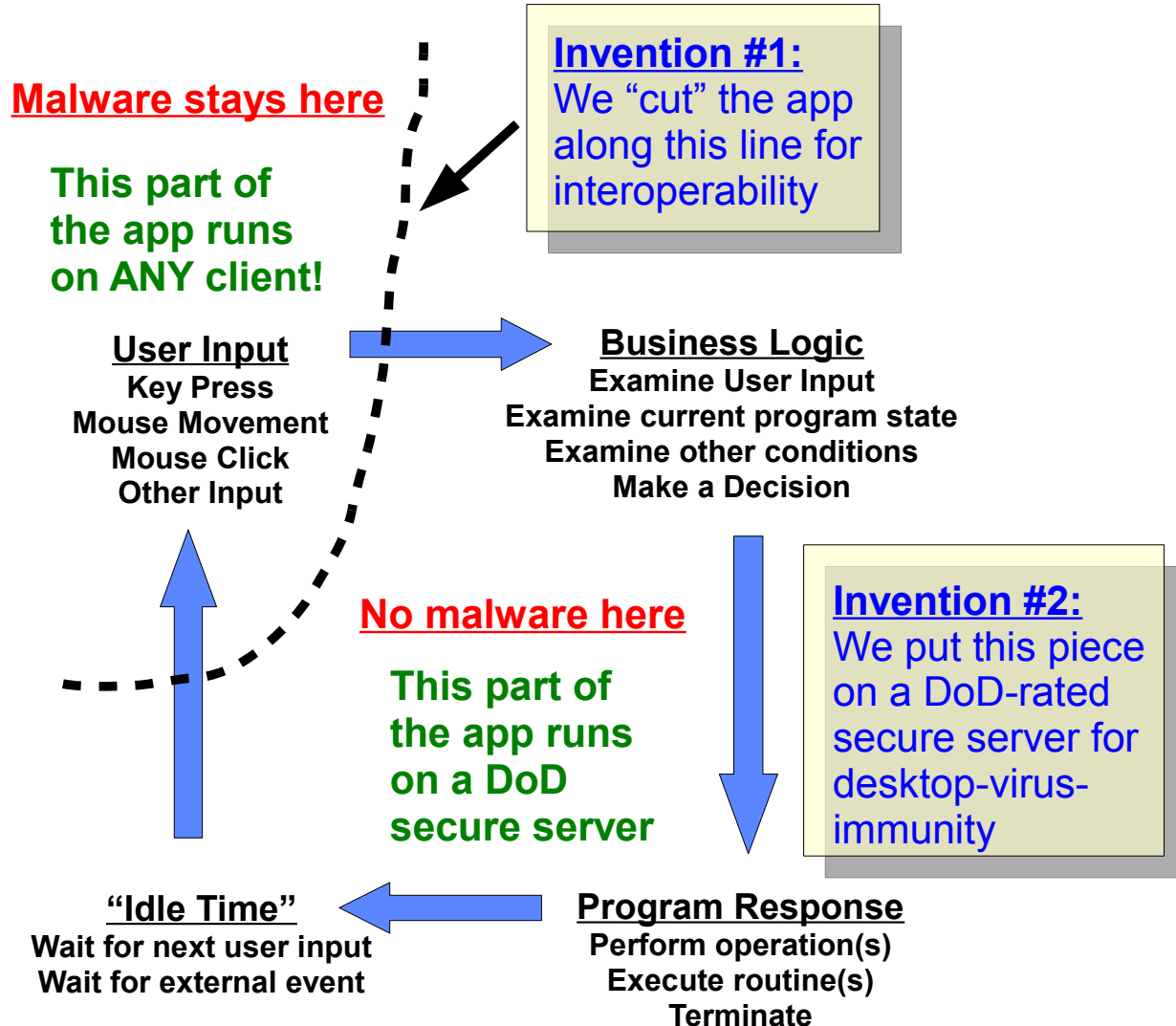
- Applications receive user inputs and make one or more decisions.
- Applications perform one or more operations in response to the decision.
- Applications then wait for the next user input and event.
- All this processing occurs on the desktop or laptop machine.
- Encrypted data is still decrypted on the PC and stored as 'plaintext' in RAM – where it's vulnerable to “spyware”.
- “Spyware” and “malware” can observe and interfere with this process because it all occurs on the desktop or laptop.
- Malware can observe and 'steal' critical data.

# IQware's New Approach

(Patented US #7,322,028)



No Worries, Mate!



- We separate the “user input piece” from the rest of the application so “malware” cannot “infect” the critical business logic and program operation.
- We use a TCB (Trusted Computing Base) that is DoD rated B2/C2 for the secure server.
- We can use any kind of laptop / desktop for the “user input piece” (Windows, Linux, Apple, PDAs, etc.).
- The client piece is very thin and is available as open source freeware (XLIB).
- The secure server handles all program logic, decision making and operation execution.
- All communication to/from client is encrypted.

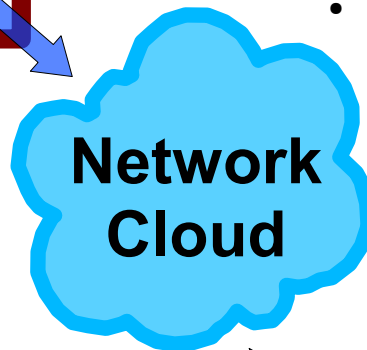
# IQware's Secure Architecture

## PC or PC Server

- **Malware remains here**
- **Only this machine is vulnerable.**

User Input  
Key Press  
Mouse Movement  
Mouse Click  
Other Input

- User events are encrypted and sent to the secure server.
- No sensitive data (e.g., UID or PWD strings) is in PC's RAM.
- Malware within PC cannot “infect” secure server.
- PC client is “thin” and uses XLIB which is available as open source freeware.
- Any PC may be used: Windows, Linux, Apple, UNIX-based, PDAs.



- Secure server controls all business logic and makes all application decisions.
- Secure server performs all application operations.
- Malware cannot affect secure server (non-Intel CPU ISA, DoD rated B2/C2).
- Optional CAPTCHA images can be used so that text strings (E.g., SSNs, UIDs, PWDs, etc.) are never sent to the virus-prone PC client.

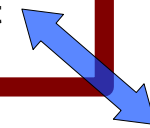
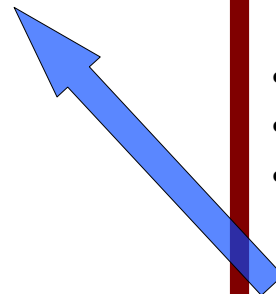
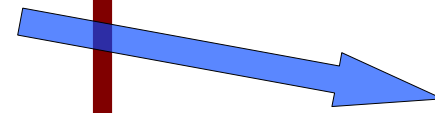
## IQware Secure Server

- **No malware**
- **No interference**
- **No data theft**

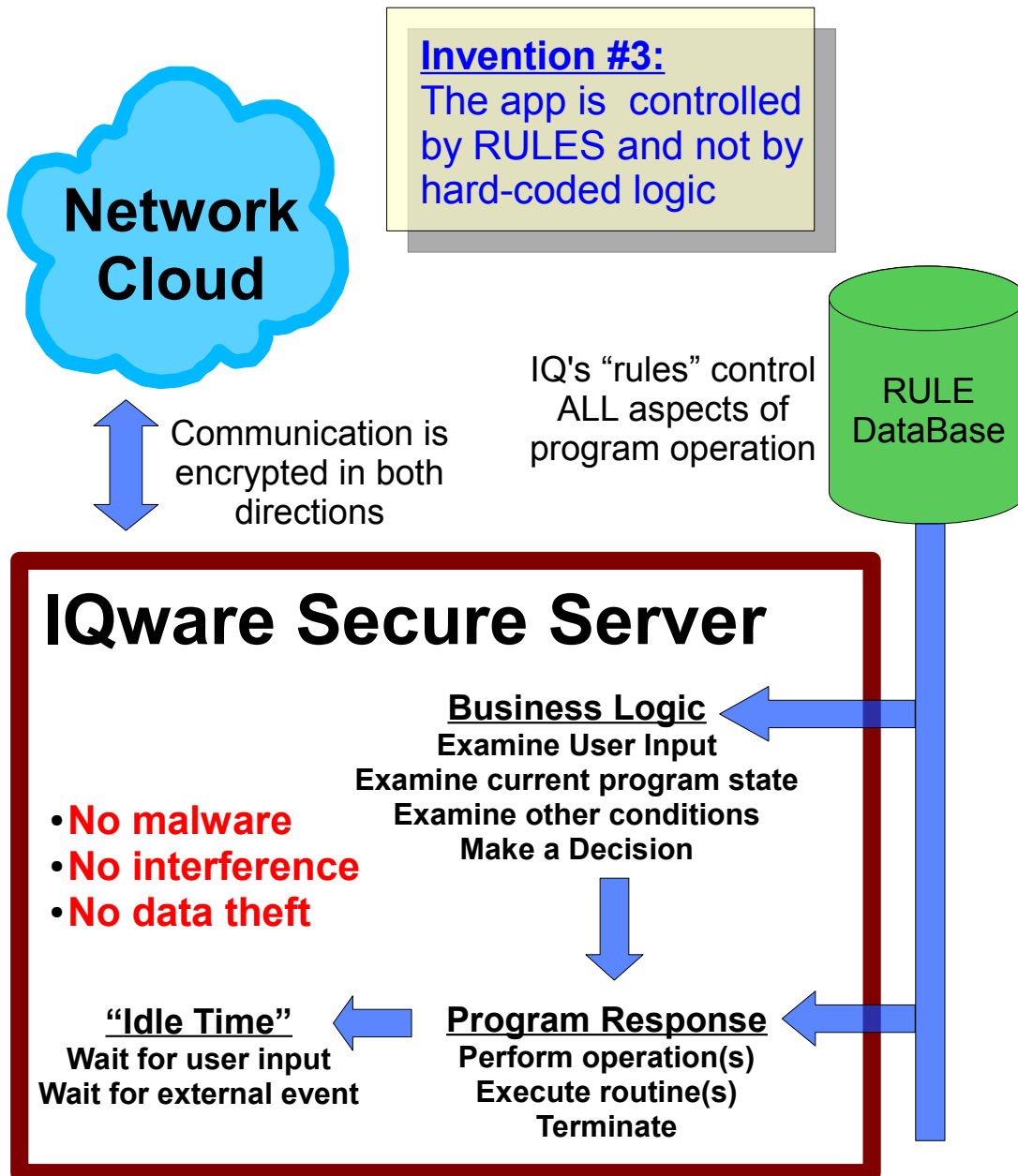
Business Logic  
Examine User Input  
Examine current program state  
Examine other conditions  
Make a Decision

“Idle Time”  
Wait for user input  
Wait for external event

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

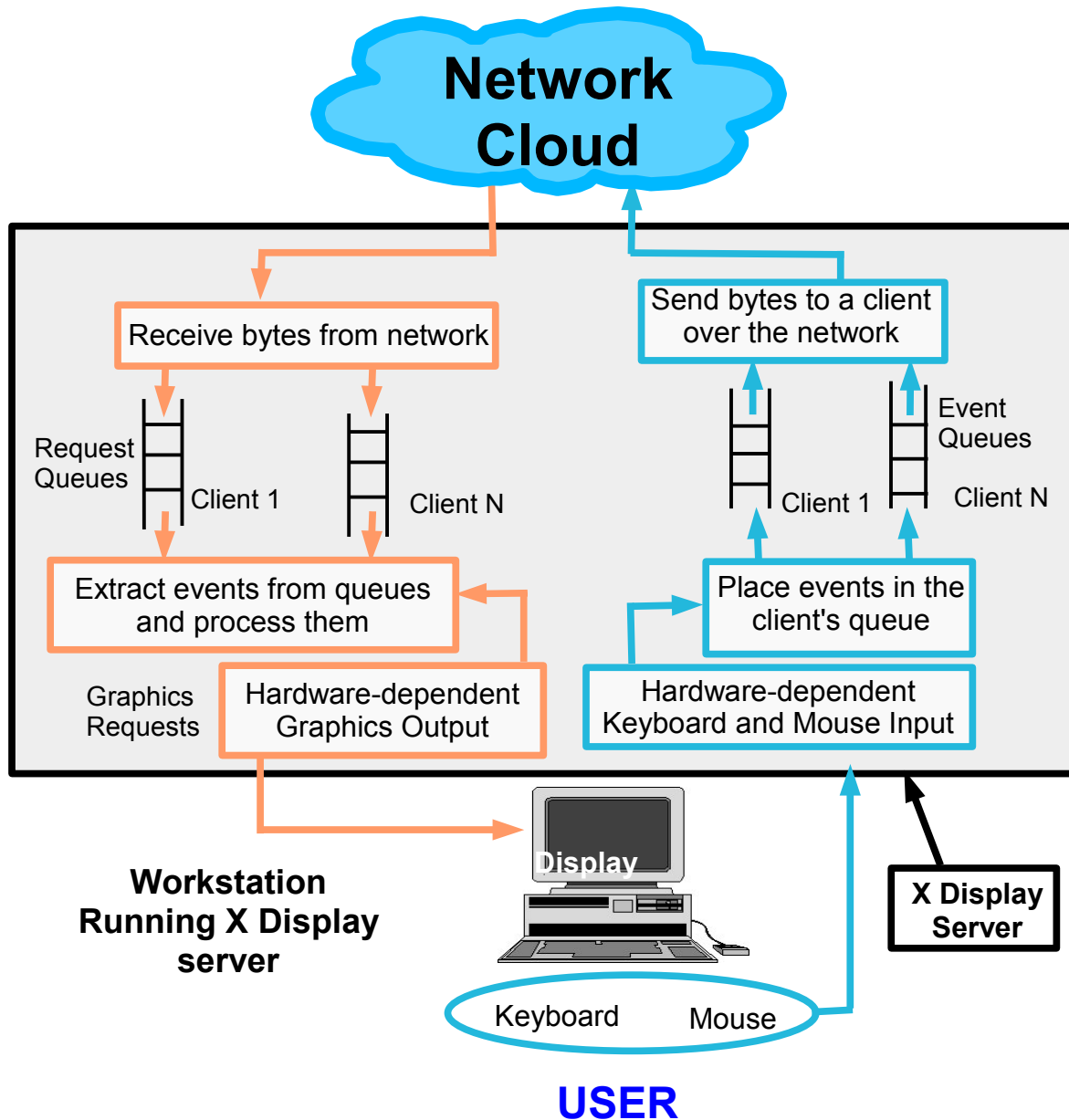


# IQware's Rule-Based Invention



- IQware converted the application into a "Rule Processor" that executes rules.
- Rules control the business logic, program state, other conditions.
- Rules control screen appearance, menus, toolbars, other visual aspects of the application.
- Rules control all program decisions and operations.
- Rules control all database access, data formatting, data presentation and data display.
- 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!

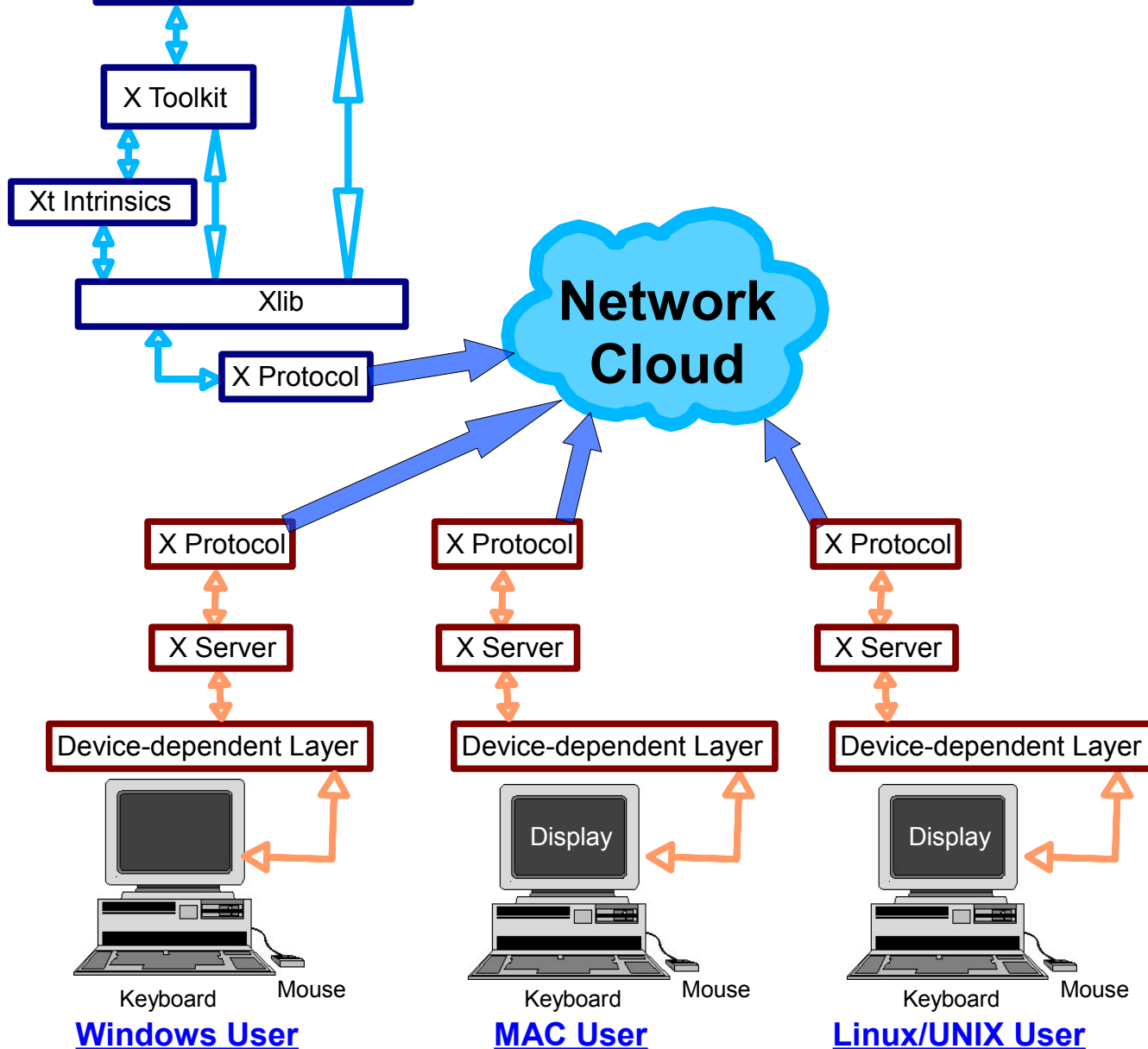
# Client Side of IQware (X-Server)



- The X-Server actually runs on the client machine.
- The X-server is VERY thin – **much** smaller than a web browser and all of its "plug-ins".
- The X-server runs on all client machines, including Windows, Apple MACs, Linux (all varieties), Sun UNIX, PDAs, etc.
- X-servers are available as open-source freeware.



# IQ Deployment Architecture



- IQware works with any client
- All network communication is encrypted
- Client side is open source freeware
- Client side is ultra-thin
- Rules can be changed at any time