

Is Trusted Computing An Achievable Objective?

David C Blight

dcblight@marzenka.com

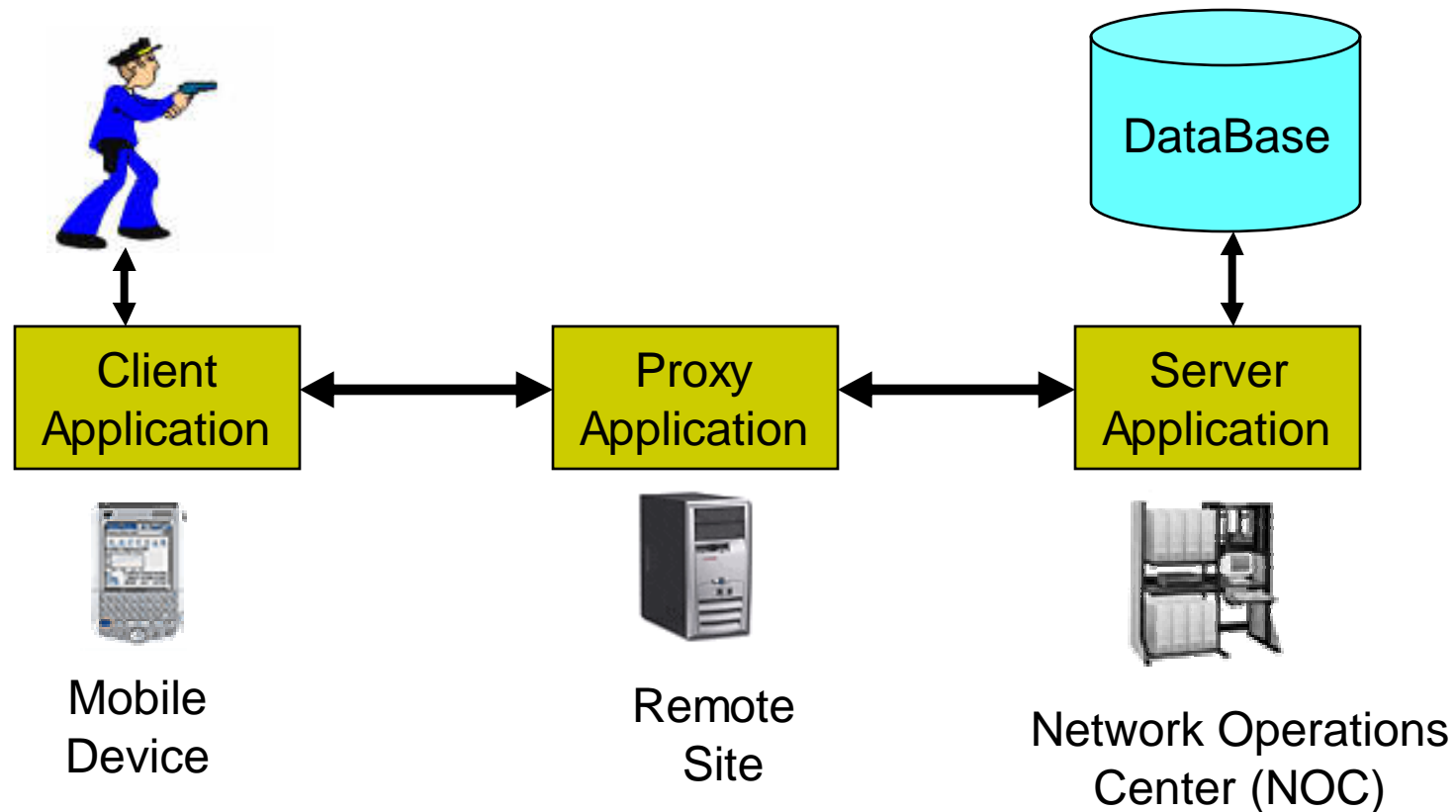
Can you trust your computer?

- *By [Richard Stallman](#)*
- <http://www.newsforge.com/article.pl?sid=02/10/21/1449250>
- Who should your computer take its orders from?
- Treacherous computing
 - the plan is designed to make sure your computer will systematically disobey you.
 - In fact, it is designed to stop your computer from functioning as a general-purpose computer. Every operation may require explicit permission.

Can your computer trust you?

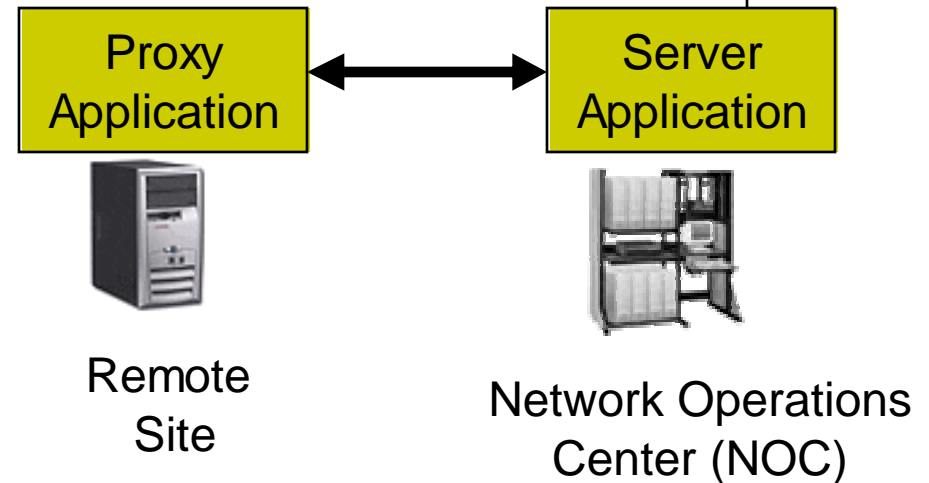
- Establish Trust in a remote computing environment
 - Users, hardware, and software
- The ultimate goal is to be able to bind data to applications, users, and/or computers.

Example Problem (Real)



Example Problem (Real)

How to secure the inter application link?



- Encryption is possible without stored secrets
 - Diffie-Hellman
- Authentication requires stored secrets on both systems
 - Store secrets are a vulnerability
 - Applications



Why is this difficult

- Secrets must be stored in persistent storage
- Where is secret stored
 - In Application
 - Applications may be reversed engineered
 - In file system / database
 - Non secure
 - At best protected by encryption, but where is the key stored
 - Obfuscated
 - Non secure



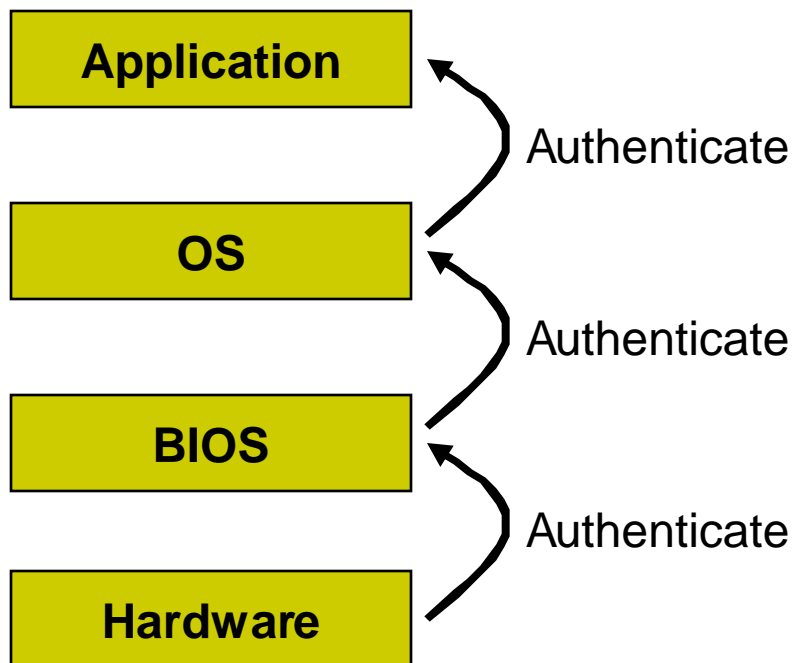
Securing Information

- What is needed
 - Ability to store a secret on a computer such that
 - Application can get the secret
 - No other application can get the secret
 - Secret must be secure within the application
 - No other application can retrieve the secret from the application
- Can not be a software only solution
- Data (secret) needs to be bound to an application.

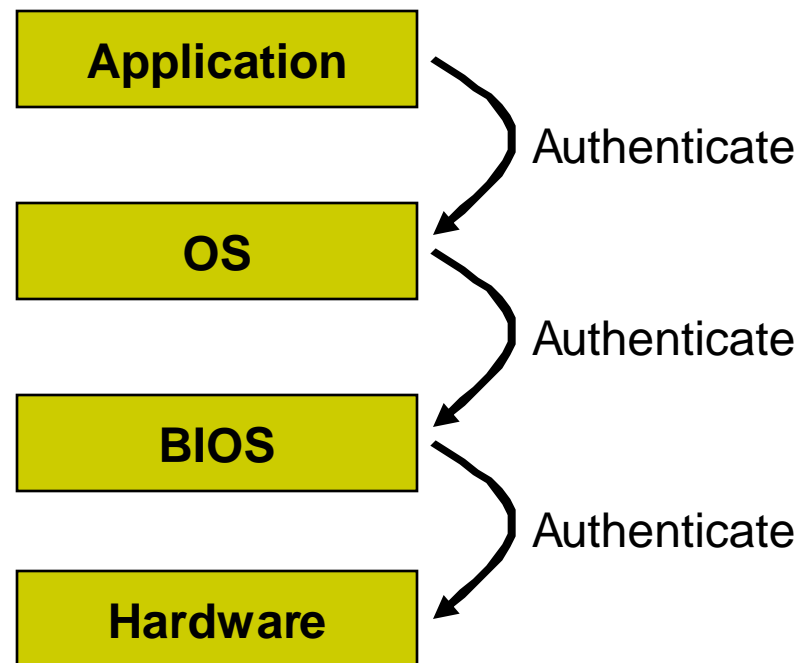
Hardware Security



Forward Security Chaining



Reverse Security Chaining



Xbox Security



- What is needed for Xbox security
 - Need to ensure Xbox integrity
 - Correct BIOS
 - BIOS will only load intended OS
 - Correct OS
 - Will only load signed Applications (Games)
 - Correct Applications
 - Games must not open security holes



Xbox Security



- Xbox security was broken by people eating to run Linux on Xbox
- Security model is backwards
 - Each stage verifies the next
 - If the next stage is verified
 - It is executed
 - Each stage should verify all previous stages



Windows Media Player



- Windows Media Player and DRM
 - Displays files
 - Honors DRM restrictions encoded in formats
- Its just software application
 - It can be reverse engineered
 - And has been
 - Encryption keys, algorithms, and protocols have been extracted
 - New application can be constructed which does not honor DRM restrictions in content
- Server only



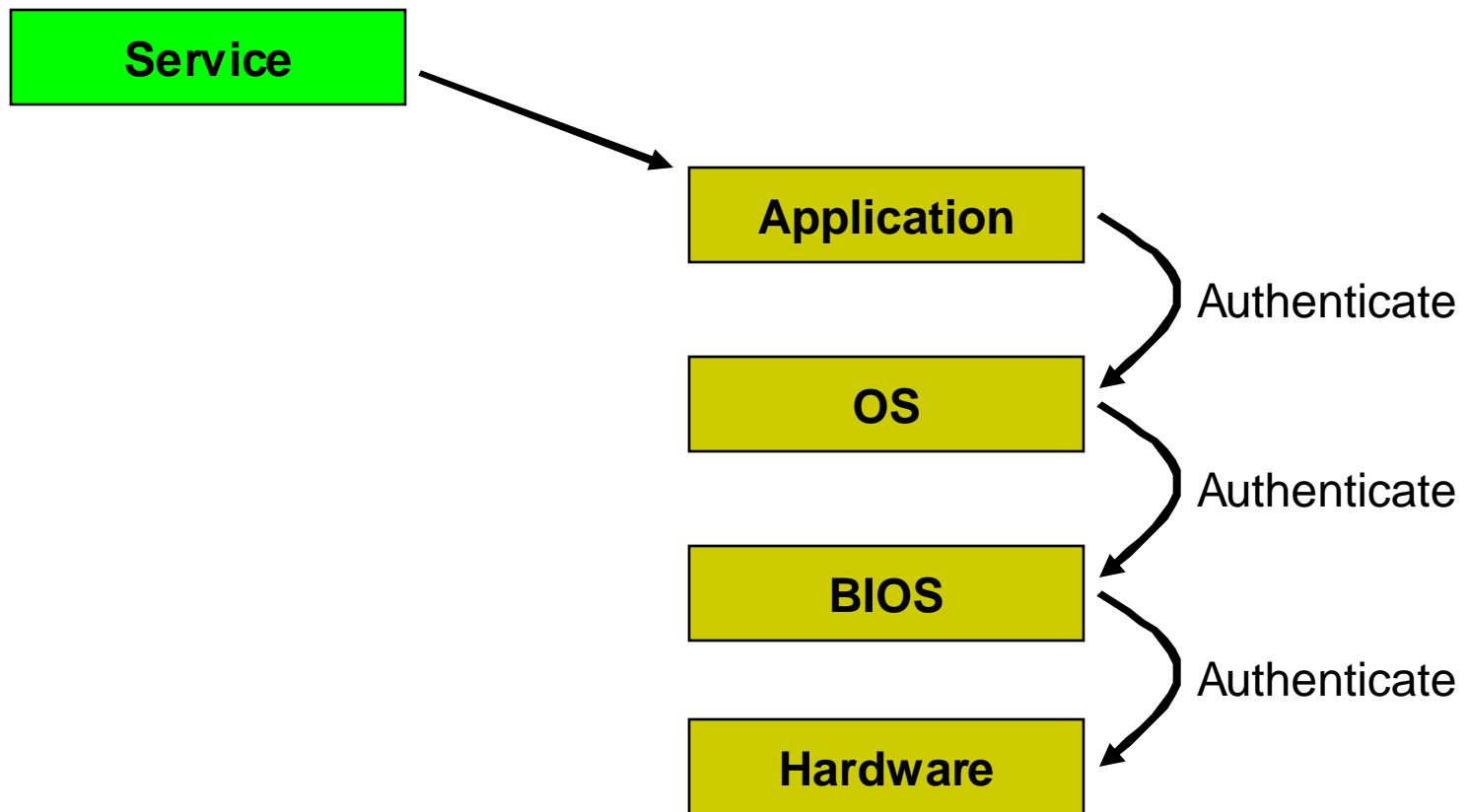
Windows Media Player



- What is required
 - Media Server needs to be sure that data is not going to imposter applications
 - Server needs to verify the application it is sending content to
 - Content needs to be bound to
 - Application
 - Application Environment
 - Software and hardware



Attestation Model



Security Initiatives



**Applications
Operating System**

**Microsoft
Next Generation Secure
Computing Base**

PC Chipsets

**Intel
LaGrande
Technology**

**AMD
SEM**

BIOS

**Graphic
IO
Proc.**

**Secure
Hardware**

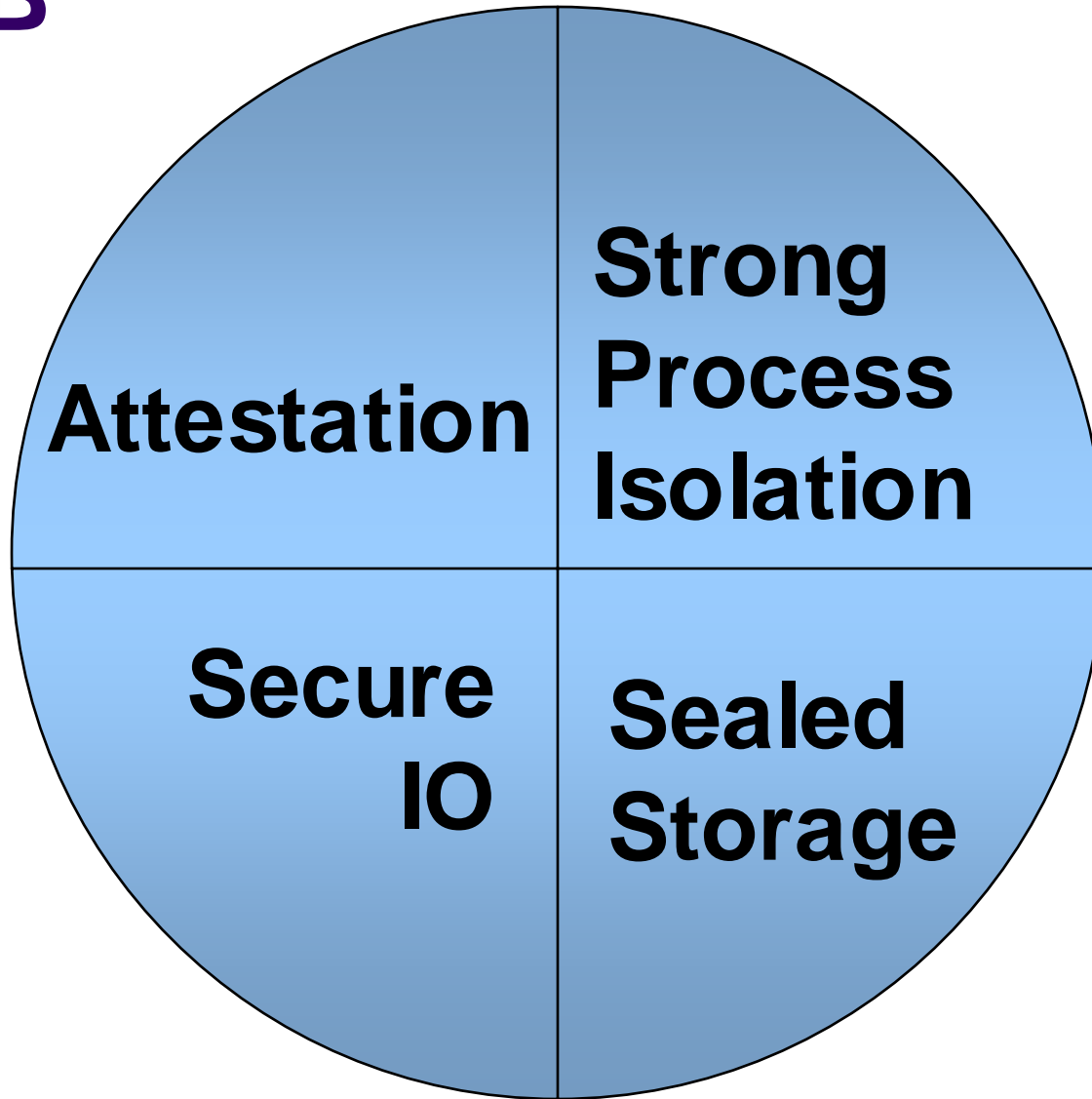
**TCPA
TPM**

Next Generation Secure Computing Base (NGSCB)



- Formerly called Palladium
- Windows can not be made completely secure
 - Kernel is too big
 - Will always have bugs/security holes
 - Applications and services
 - Offer many potential holes to external attackers to get to kernel.
- Secure applications should run outside of Windows
 - Still have access to windows services

NGSCB

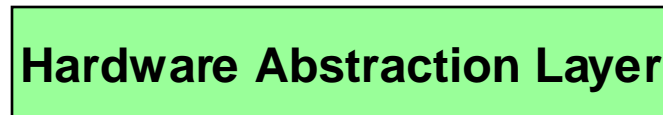
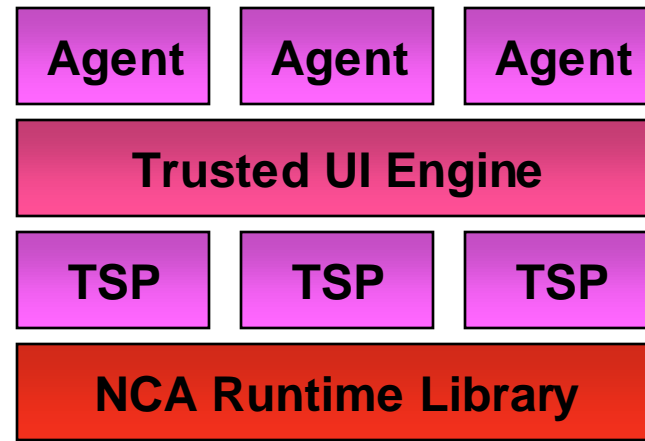


NGSCB

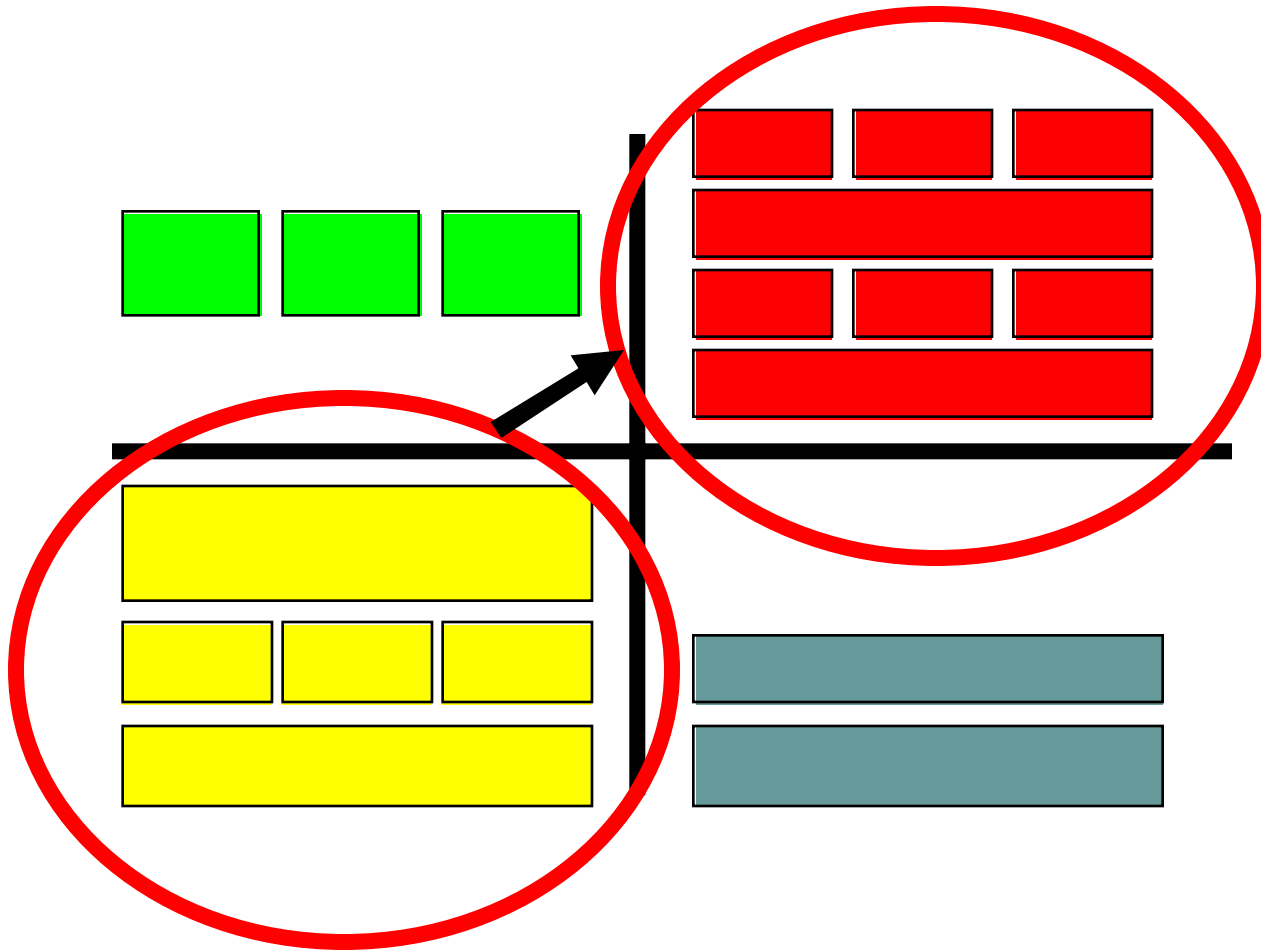


- Attestation
 - Ability to verify the operating environment
 - Remote verification
- Strong Process Isolation
 - Memory isolation (curtained memory)
- Sealed Storage
 - Data bound to operating environment
 - Application, OS, drivers, CPU, hardware, TPM,...
- Secure Path to IO
 - No keyboard sniffing
 - No framebuffer reading/writing

NGSCB



NGSCB Complexity



NGSCB



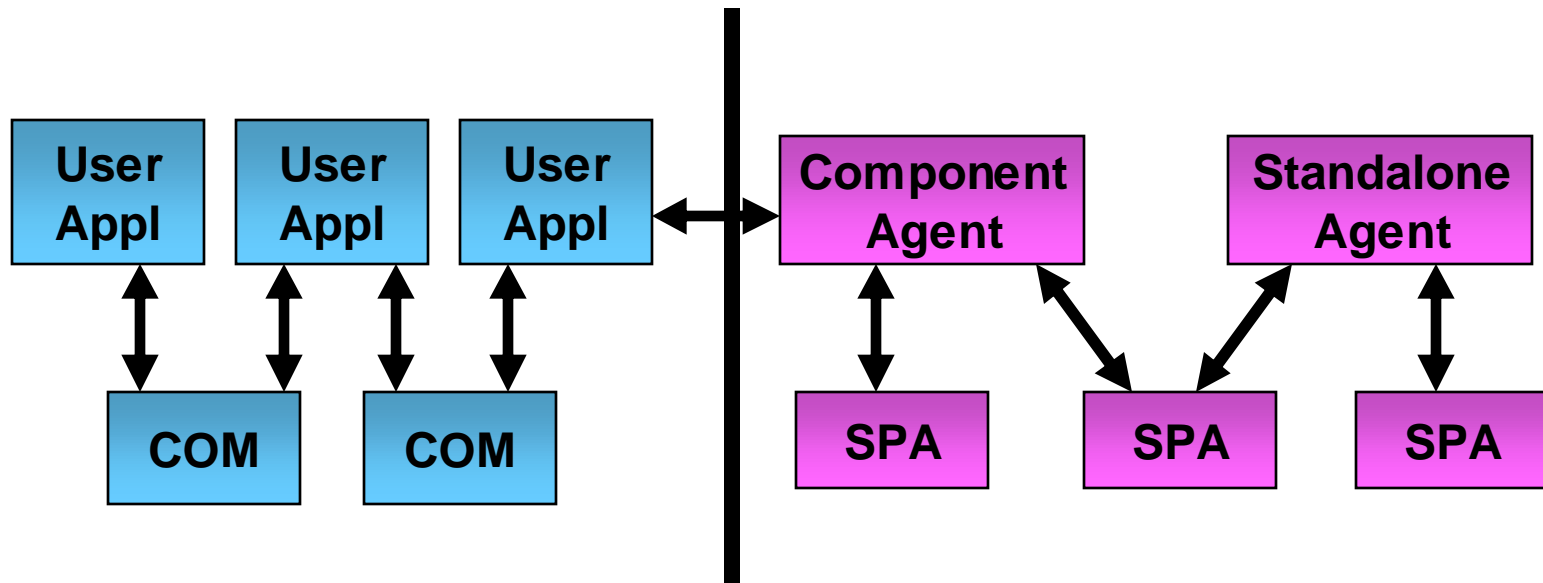
- Isolation of Nexus from Windows is done at hardware level
 - No windows bug will affect nexus applications
- Nexus
 - Only one nexus at a time
 - Not a complete Operating System
 - Implements
 - Process, thread, memory, and IO manager
 - Does not implement
 - File System, networking, device drivers, plugins, nor directX



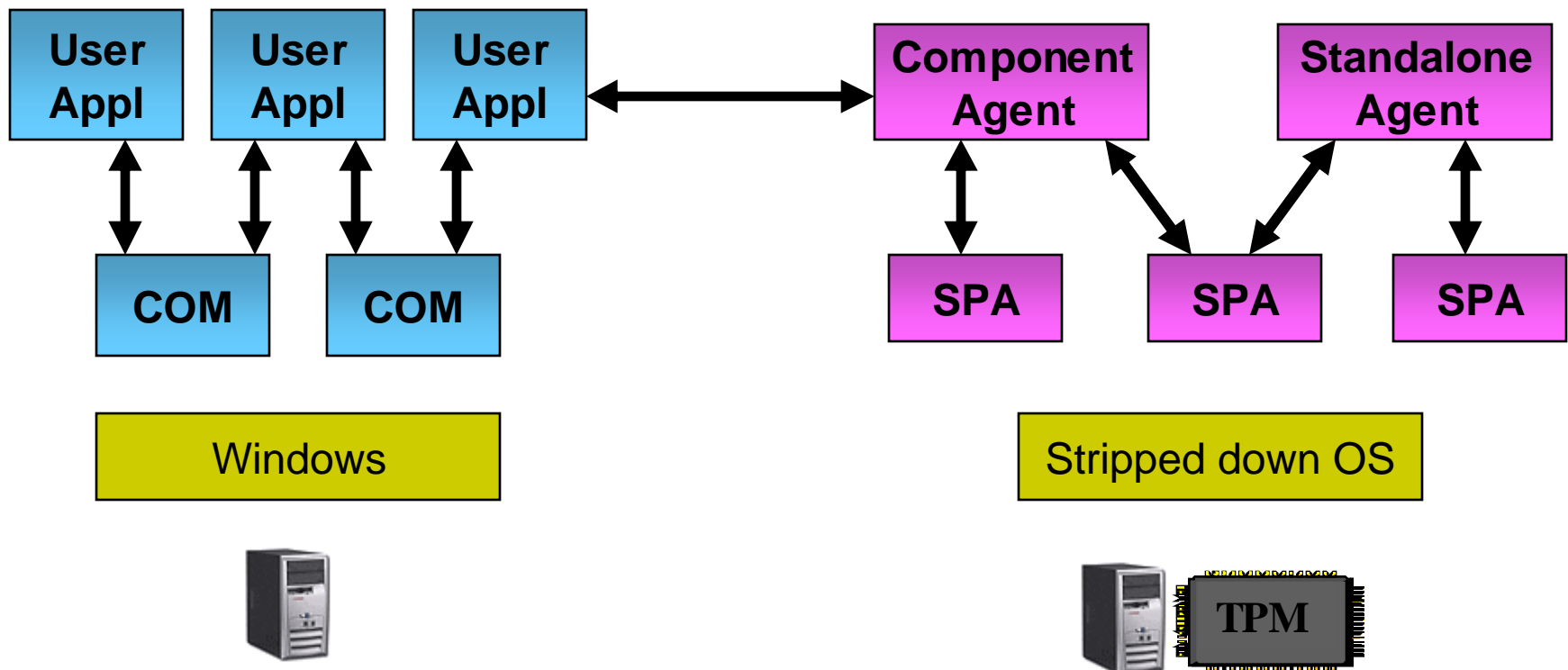
Nexus Applications

- Application Agents
 - Standalone program which runs in Nexus space
- Component Agents
 - Agents appear as external Com object or managed object
 - Windows proxy translate COM to IPC
- Service Provider Agents (SPA)
 - Agents provide services to other agents
 - IPC facility exists for agents to communicate

NGSCB



NGSCB (logical Equivalent)





Trusted UI Engine

- Nexus agents need to be able to securely put graphics on the display
 - Windows robust graphics systems are not available to nexus agents
 - Potential security hole
 - Nexus windows must not be hidden by windows applications
- Lightweight graphic system
 - XML based
 - Processed by graphics card

Attestation



- Attestation challenges must come from other computers
 - ?????
 - Nexus and agents can not directly determine if they are running in secure mode
 - It is up to others to determine if they trust the nexus or the agents.



Manifests

- Each agent has a signed manifest
 - Extension of manifests to appear in Longhorn
- XML description of agent
 - Agent components and properties
 - Agent policy requests (non binding, controlled by owner)
 - System Requirements
 - Descriptive Properties
 - Secret migration
- For example
 - A flag indicates if the agent is debuggable



Debugging

- Nexus agents are debuggable
 - Debugging occurs in Windows
 - Debugger communicates with agent
 - A debuggable agent generates a different digest than a non debuggable agent
 - A remote entity can attest that the agent is not in debug mode when it interacts
- The nexus itself is debuggable
 - Special version of nexus



NGSCB Policies

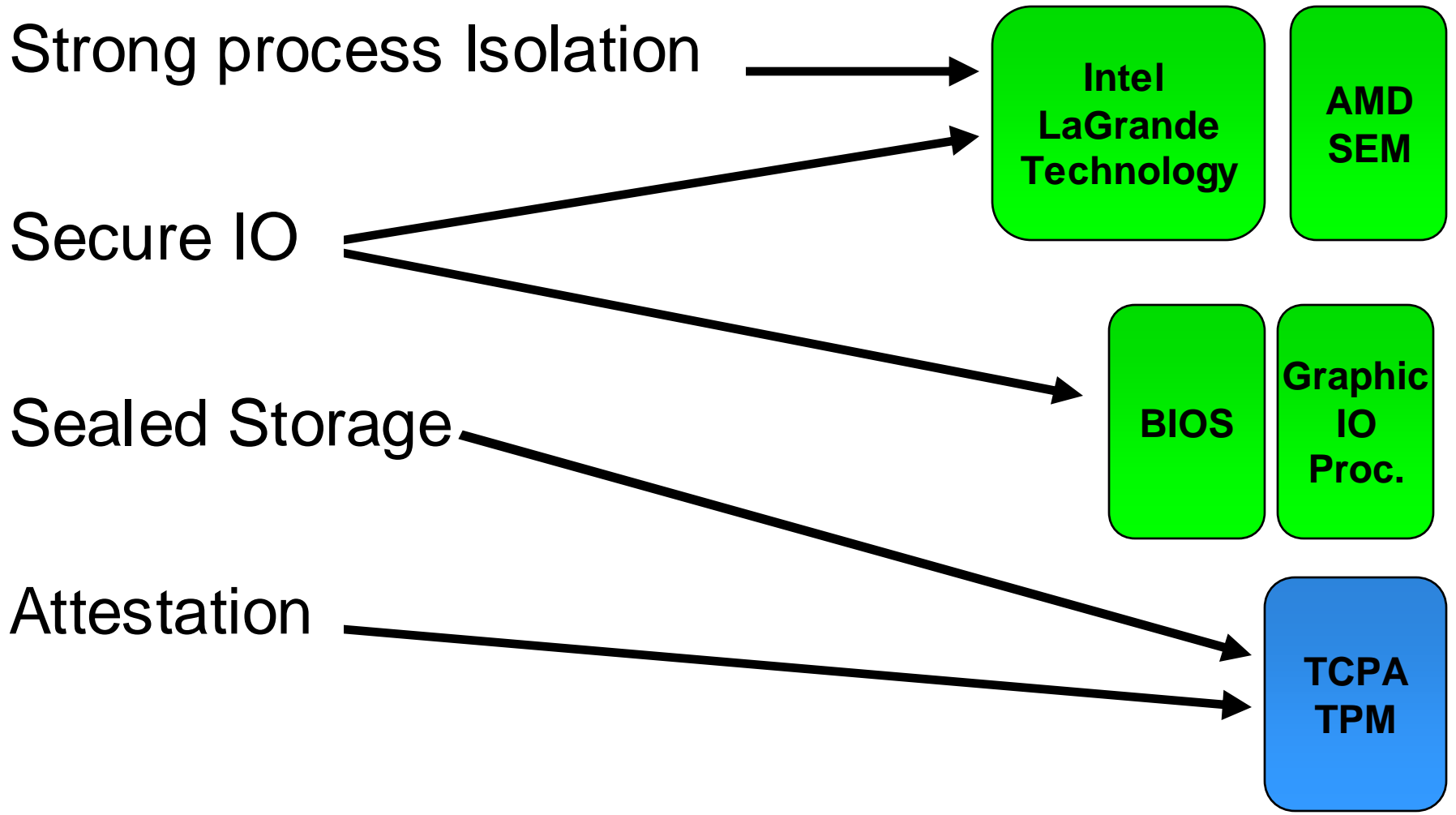
- Microsoft promises policies to control the operation and resources of nexus and agents
 - Running agents
 - Accessing secrets
 - Seal Storage
 - Networks and file systems
- Policies are a mixed blessing
 - Implies there is lots to manage



NGSCB Caveats

- Nexus does not mitigate bad/insecure software design
 - Onus is still on designer
 - Must carefully use windows services
- What protects nexus agents from each other
 - Nexus
 - Kept open(?) and simple

NGSCB Hardware Requirments

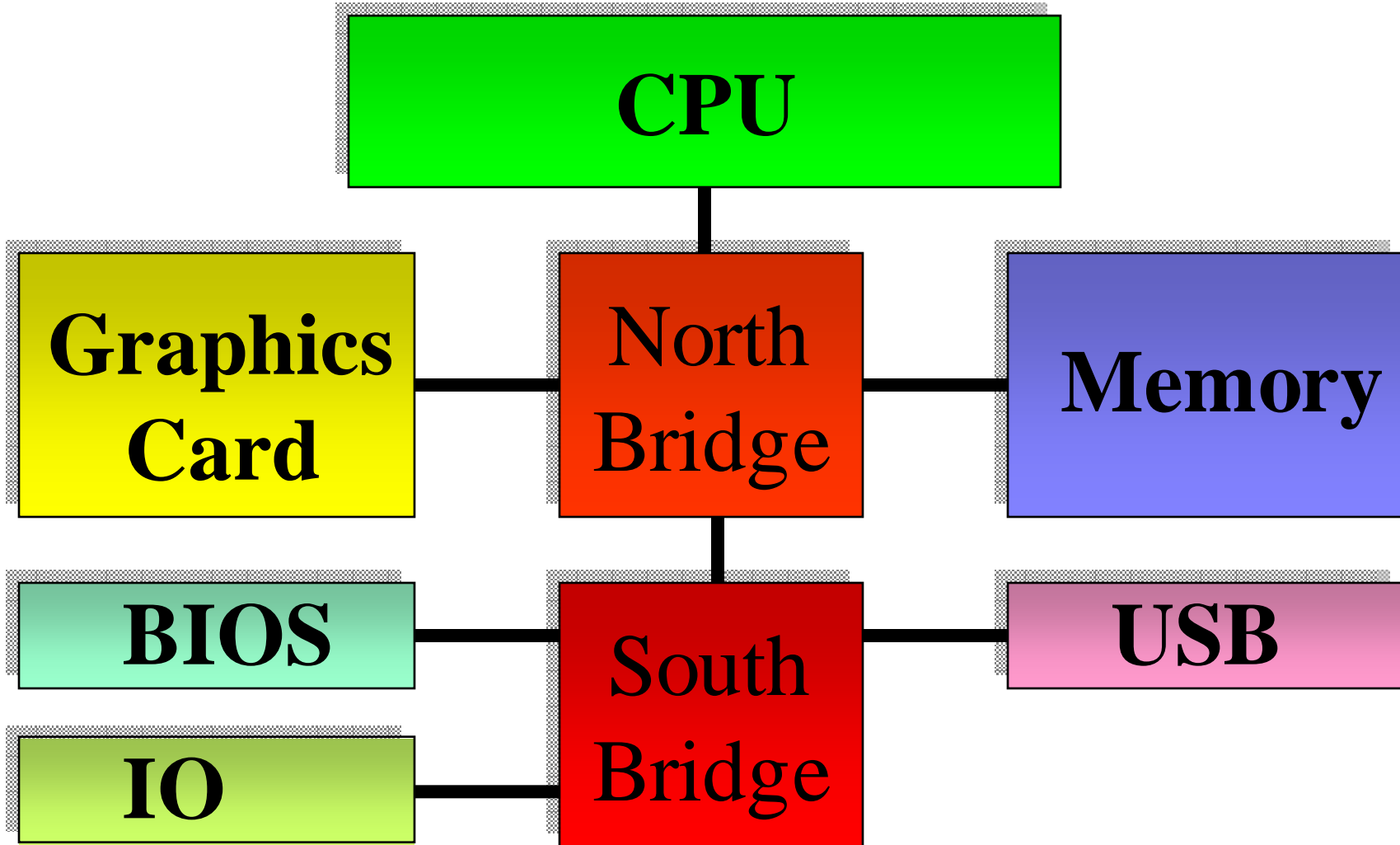




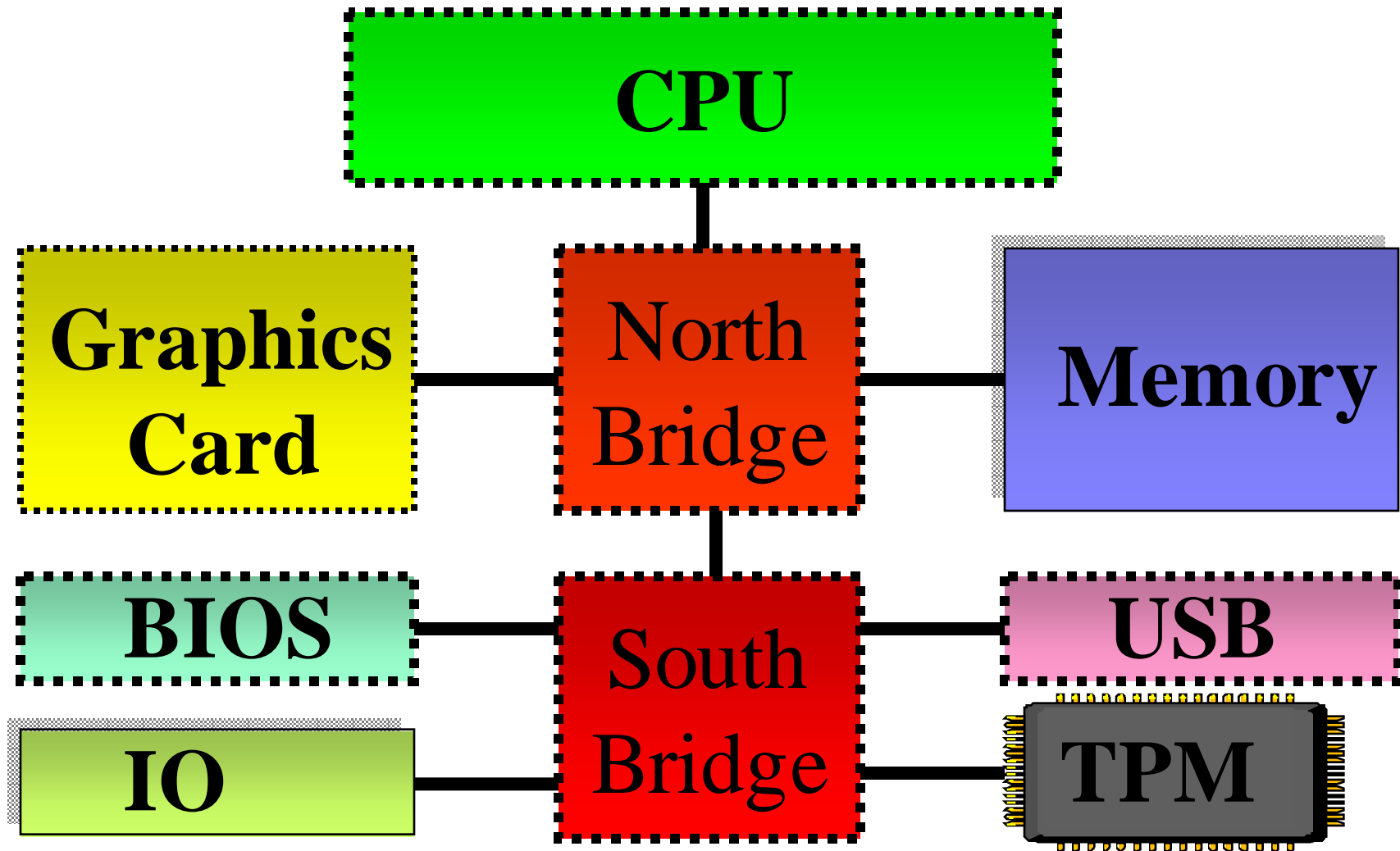
NGSCB Real Challenges

- Keep things from getting too complex
 - Putting IE in a nexus agent will not make it secure
- Manage Sealed Storage
 - Lots of potential to lose data with hardware/software failures
 - How to backup data in sealed storage
 - Hardware management as part of data management

PC Architecture



Trusted Computing PC Architecture



Intel LaGrande Technologies



- Strong Processor Isolation
- Secure path to IO

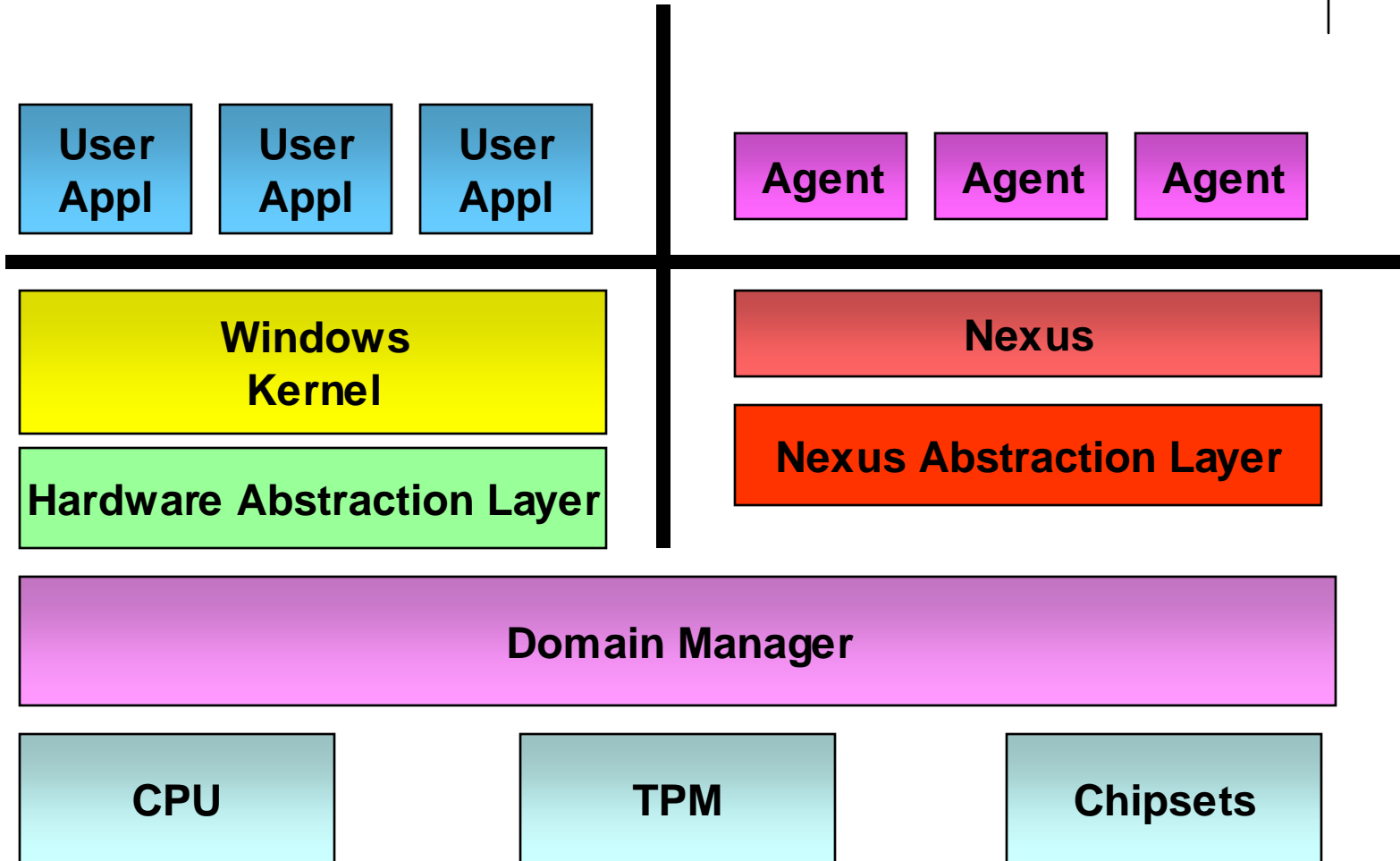


Secure Path

- Goal: to protect data within the PC
 - No keyboard sniffers
 - No reading/writing framebuffer
 - Input and output is secured to Agent
 - USB to nexus
 - Graphics card
 - Keyboard/pointer (for notebooks)



LaGrande Protection Model





Memory Isolation

- Protecting memory is critical
 - Northbridge usually contains memory manager
 - Memory curtaining prohibits DMA from protected areas
- Devil in the details
 - Lots of things that need to be controlled
 - Memory during system resets
 - Memory during system sleeps
 - Initial trust ?????

TCPA / TPM

- Trusted Computing Platform Alliance (TCPA)
 - <http://www.trustedcomputing.org>
- Trusted Computing Group
 - <https://www.trustedcomputinggroup.org/home>
 - Successor to TCPA
 - Same initiative
- Trusted Platform Module (TPM)
 - One component of TCPA



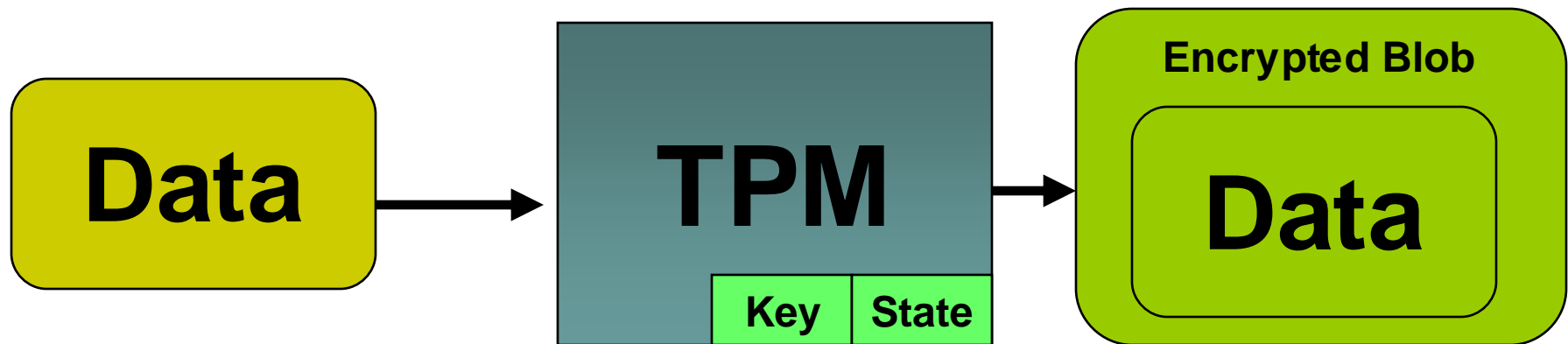


Anti-TCPA

- <http://www.againsttcpa.com/>
- The informational self-determination isn't existing anymore, it's not possible to save, copy, create, program, ..., the data like you want. This applies for privates as for companies
- The free access to the IT/Software market is completely prevented for anyone except the big companies, the market as we know it today will get completely destroyed
- Restrictions in the usage of owned hardware would apply
- The liberty of opinion and the free speech on the internet would finally be eliminated
- The own rights while using IT-technologies are history.
- The national self-determination of the der particular countries would be fully in the hands of the USA
- Probably the world would break into two digital parts (Countries that express against TCPA)

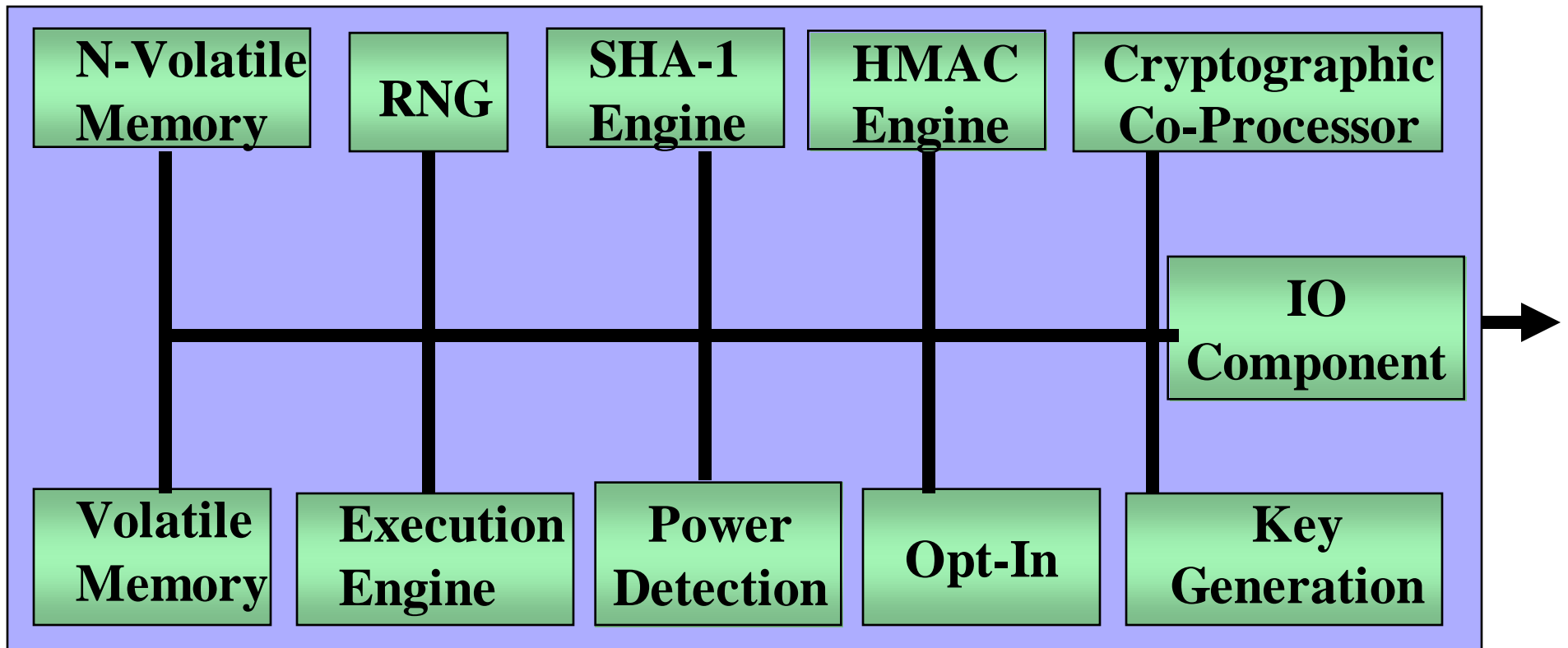


TPM Sealed Storage



- Keys never leave TPM
- Data can only be unsealed
 - When system in is specified state
 - Authorized command

TPM Architecture



Trusted Computing

Constraining

Or

Opportunity?



Back to Original Problems

- Secure communications between servers
 - All authentication secrets stored in sealed storage
 - Only a security hole in application can reveal secrets
 - System is not dependent upon OS security
- Xbox
 - NGSCB/TPM is only partial solution
 - OS and application self attest (TPM allows)
 - Still need to prohibit certain apps
 - Stronger version of what is currently done



Back to Original Problems

- Windows Media Player
 - Server attests client
 - Server sends content to client (securely)
 - Encrypted with unique key for application/device
 - Keys stored in sealed storage
 - Bound to application/device
 - Some additional info stored with keys
 - Number of time played (to prevent copy/play/restore)

Is this Safe Technology



Yes