Next Generation Secure Computing Base Nexus Fundamentals

Stephen Heil
Security Business Unit
Microsoft Corporation

Microsoft

Intel Developer Forum

Safer Computing Track – Fall IDF

Tuesday

- LT Overview
  SCMS-16
- TCG & TPM v1.2
  SCMS-17
- LT Architecture
  SCMS-18
- Tech Showcase
  Every Day
  Birds of a Feather Lunches
  Tuesday & Wednesday

Wednesday

- Privacy Method for Assuring Trust
  SCMS-19
- Opt-In Strategy
  SCMS-156
- Trusted Mobile KB Controller
  SCMS-24
- Software for LT
  SCMS-20
- Fundamentals for NGSCB
  SCMS-21
- Migrating Apps to NGSCB
  SCMS-22

Thursday

- TPM Recovery
  SCMS-25
- TCG Credentials
  SCMS-157
- TPM Mfg & Testing
  SCMS-180

= Overview
= Medium Technical
= Highly Technical

Microsoft

Intel Developer Forum

Agenda

- Basic NGSCB Environment
- Standard-Mode/Left Hand Side (LHS)
- Nexus-Mode/Right Hand Side (RHS)
- Derivative Works
- Agent Samples
- Summary
- Q&A

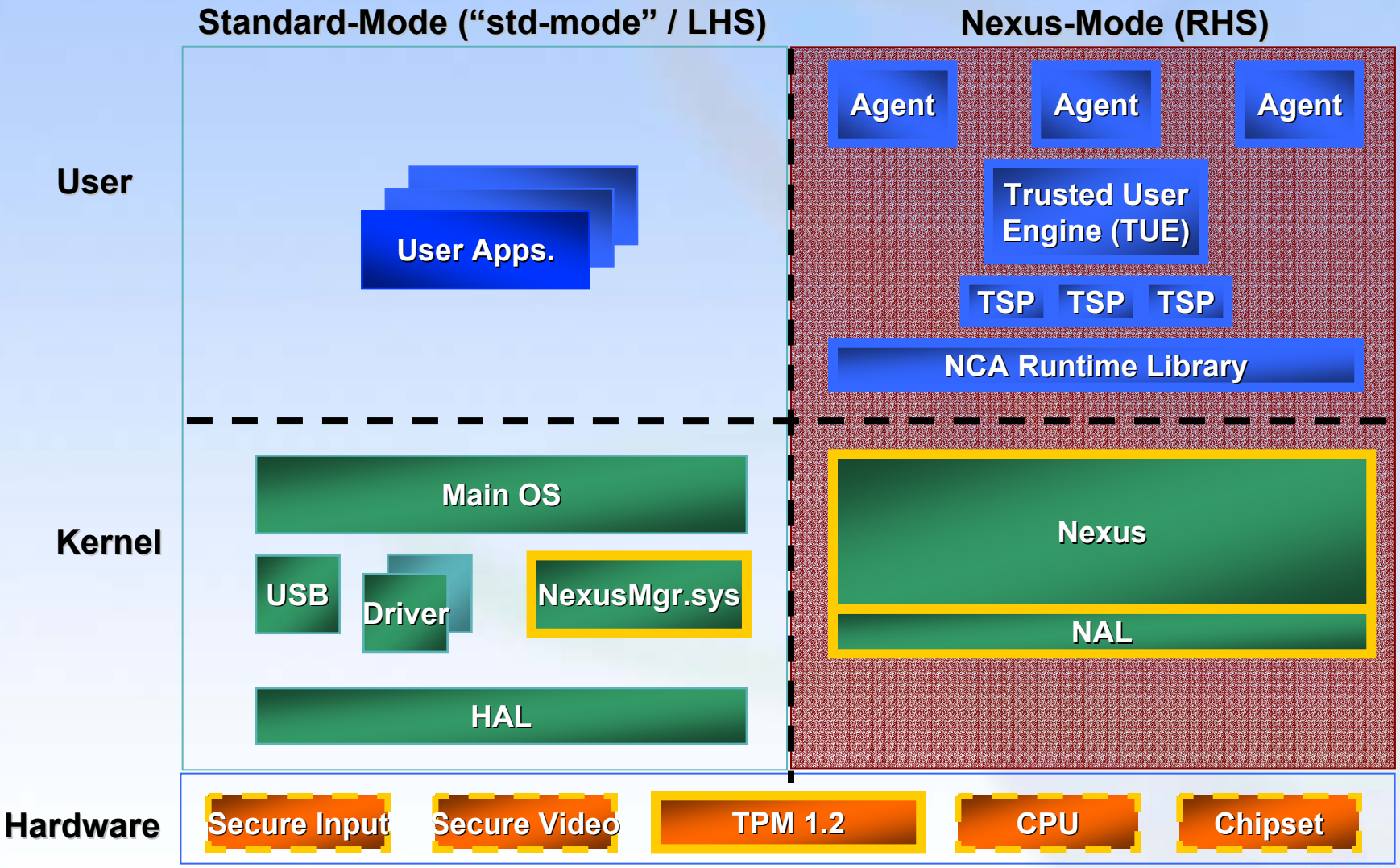
Next Generation Secure Computing Base Defined

- Microsoft's Next-Generation Secure Computing Base (NGSCB) is a new security technology for the Microsoft Windows platform
  - Uses a unique hardware and software design
  - Gives people new kinds of security and privacy protections in an interconnected world

Microsoft

Intel Developer Forum

NGSCB Quadrants



A Basic Environment

- Basic Operating System Functions
  - Process and Thread Loader/Manager
  - Memory Manager
  - I/O Manager
  - Security Reference Monitor
  - Interrupt handing/Hardware abstraction
- But not a complete Operating System
  - No File System
  - No Networking
  - No Kernel Mode/Privileged Device Drivers
  - No Direct X
  - No Scheduling
  - No…
- Kernel mode has no pluggables
  - All of the kernel loaded at boot and in the PCR

A Basic Environment

- Virtualization of hardware fundamentals for Agents
  - Sealed storage, attestation, etc.
- Minimal Services
  - Trusted UI Engine
    - XML Based Graphical Services for UI
    - Input Routing/Focus Management
    - Minimum Fonts (inc. Multiple Languages…)
    - Windows Manager
  - Inter-Process Communications (IPC)
  - TSPs (Trusted Service Provider)
    - Run in User Mode RHS
    - Provide Services
    - Are “Drivers” for Trusted Input/Video

Device Drivers

- NGSCB doesn't change the device driver model
- NGSCB needs very minimal access to real hardware
- Secure reuse of Left Hand Side (LHS) driver stacks wherever possible
  - Right Hand Side (RHS) encrypted channel through LHS unprotected conduit
- Every line of privileged code is a potential security risk
  - No third-party code on the RHS
  - No kernel-mode plug-ins

Partitioned System

- RHS = Security
  - In the presence of adversarial LHS code the system must not leak secrets
    - → The RHS must NOT rely on the LHS for security
- LHS = Richness and Compatibility
  - In the absence of LHS cooperation NGSCB doesn't run
    - → The RHS MUST rely on the LHS for stability and services

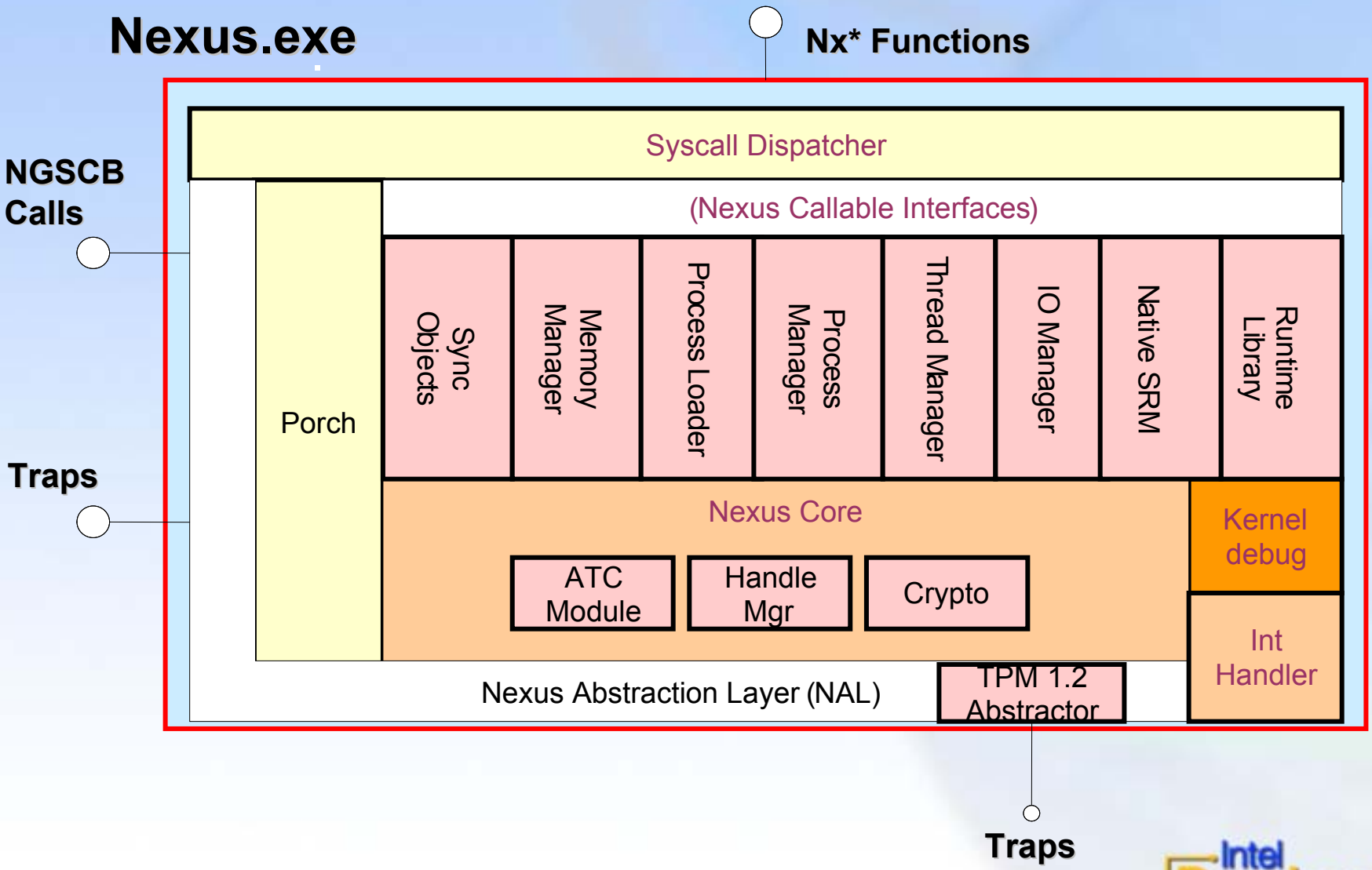
What Runs On The LHS

- Applications and Drivers still run
- Viruses too
- Windows as you know it today
- Any software with minor exceptions
  - The new hardware (HW) memory controller won't allow certain "bad" behaviors, e.g., code which
    - Copies all of memory from one location to the next
    - Puts the CPU into real mode

What NGSCB Needs From The LHS

- Device Driver work for Trusted Input / Video
- Memory Management additions to allow nexus to participate in memory pressure and paging decisions
- User mode debugger additions to allow debugging of agents (explained later)
- Window Manager coordination
- Nexus Manager Device driver (nexusmgr.sys)
- NGSCB management software and services

Close-Up Of The Lower RHS



I Think, Therefore I Am

Descartes Problem

- Challenge for attestation must always come from outside the machine
  - Local (the user with a superkey)
  - Remote (some server)
- No nexus can directly determine if it is running in the secured environment
- No Agent can directly determine if it is running in the secured environment
- Must use Remote Attestation or Sealed Storage to cache credentials or secrets to prove the system is sound

Microsoft

Intel Developer Forum

Nexus Derivative Works

- The user can run any nexus, or write his own and run it, on the hardware
- That nexus can only report the attestation provided by the Trusted Platform Module (TPM 1.2)
  - The TPM won't lie
  - The nexus cannot pretend to be another nexus
- Other systems will need to decide if they trust the new derived nexus
- Nexus writers need to prove to others that their derivative is legitimate

Microsoft

Intel Developer Forum

Agent Derivative Works

- The user can run any agent, or write his own and run it, on the nexus
- That agent can report the attestation provided by the nexus
  - The nexus won't lie
  - The agent cannot pretend to be another agent
- Other systems will need to decide if they trust the new derived agent
- Agent writers need to prove to others that their derivative is legitimate

Machine Policy Controlled By The Owner Of The Machine

- NGSCB enforces machine policy but does not set the policy
- The hardware will load any nexus
  - But only one at a time
  - Each nexus gets the same core platform services
  - The hardware keeps nexus secrets separate
  - Nothing about this architecture prevents any nexus from running; however, the owner can control which nexuses are allowed to run
- Proposed software (nexus) policies
  - The Microsoft nexus will run any agent
    - The platform owner can set policy that limits this
    - User gets to pick some other delegated evaluator (e.g., my union) if they choose

Microsoft

Intel Developer Forum

Policy Notes

- Policy is a way for users and machine owners to make general, abstract statements, about what software runs
  - "Run any agent I click"
  - "Run only agents whose source code I've examined/trust"
  - "Run agents that a third party I trust, trusts"
- The point of policy is to enable the users to control what runs on their machines

Agent Environment

- Sealed Storage
- Quote
- XML dialog engine
- IPC to LHS and other Agents
- Expo API for LHS services
- System Services
- Standard Crypto Libs

Agent Samples 1

- The following code displays the UI to the user and returns a Dialog Handle:
  - XML describes the initial layout of the dialog
  - The agent uses the Dialog Handle to manipulate the UI once it's displayed

```
DocumentHandle document_handle =
                TRendDisplayXML(String XML);
```

- Register an event:

```
TRendUtilRegisterEvent( document_handle,
                        "mybutton",
                        "click",
                        mybutton_OnClick() );
```

Agent Samples 2

- **Set up a while loop to catch events:**

```
while (TRendUtilGetEvent(document_handle, event) {
        TRendUntilDispatchEvent(Document_handle, event);
}
```

- **An event method to process the event:**

```
Mybutton_OnClick(document_handle, sender) {
        // sender would be “mybutton”
        // do what you need to do when the button is clicked
        // use TRendUtilGetProperty and TRendUtilSetProperty to
        // change UI as necessary
}
```

Agent Samples 3

- When finished with the dialog, destroy it:

```
TRendDestroy (document_handle);
```

Management Services

- Installation
- Controlled upgrade of the nexus and of agents
- Secure managed migration of application and nexus secrets
  - Migration
  - Backup and Restore
- Machine Policy and Configuration UIs

Shadow Process And Threads

- The nexus has no scheduler
- LHS threads to call the right to load and run a RHS thread
- These LHS threads are part of the Agent's LHS shadow process
- Not getting scheduled again does not leak a secret
- Safe RHS synchronization primitives

Summary

- NGSCB is a combination of
  - New hardware which creates secure space for…
  - …A new kernel, called the nexus, which…
  - …Will run applications in a secure memory partition, and which…
  - …Will provide these apps with security services so that they can…
  - …Provide users with trustworthy computing

Microsoft

Intel Developer Forum

Summary – Remember That

- When the nexus is turned off, literally everything runs just like before
- When the nexus is on, the LHS runs very close to everything that ever ran
- The nexus makes no claims about what runs on the LHS
- The hardware should run any nexus, and give full function to any nexus, with at most an admin step by the user
- The nexus will run any software the user tells it to

Microsoft

Intel Developer Forum

Next Steps

- Study the code
- Come to the next session
  - SCMS-22 Migrating Applications to NGSCB
- Come to Microsoft Professional Developers Conference (PDC)
  - Developer Preview SDK and Tools
  - October 26-30, 2003 in Los Angeles
  - http://msdn.microsoft.com/events/pdc/
- Ask your vendors what NGSCB-enabled components they will provide
- Read the available white papers and specs

Microsoft

Intel Developer Forum

Resources

- Visit our site
  - http://www.microsoft.com/ngscb
- Q&A
  - ngscb_qa@microsoft.com
- E-Mail updates
  - Subscribe to the WTPI information newsletter for ongoing updates; send blank e-mail to
  - wtpiinfo-subscribe@pens.tm500.com

Microsoft

Intel Developer Forum

Thank you for attending.

Please fill out the Session Evaluation Form.

Microsoft

Intel Developer Forum