Kerberos in Intel® vPro™

Ned Smith
Principal Engineer
Intel Business Client Platform Division

Legal Disclaimer

Intel Software Secrets

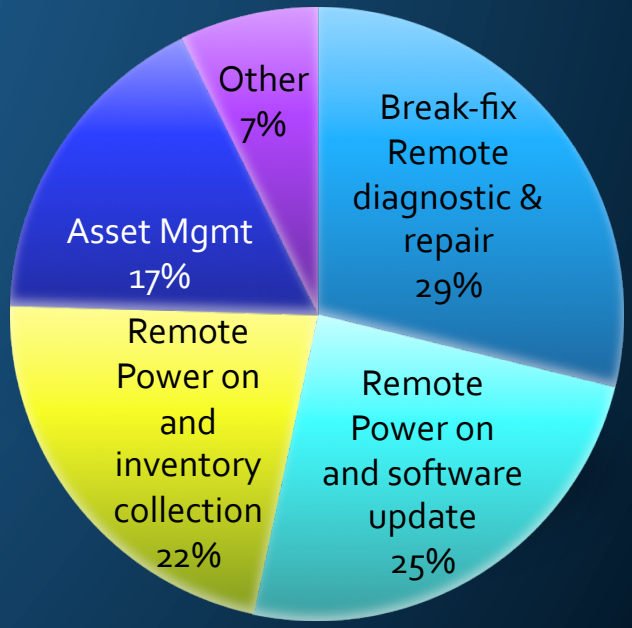
- If Intel Software were an independent software company, we'd be the 6th largest in the world
- Intel Software has the 3rd largest developer program, after MSDN and IBM
- Intel is the 3rd largest Linux institutional contributor, after Red Hat and IBM
- Intel contributed specifications to seed creation of UEFI 2.0
- Intel developed a Kerberos client for UEFI 2.0
- Intel developed a Kerberos server in vPro™ platforms

vPro™ Manageability Use Cases

Immediate Response

- Break-fix / remote KVM
- Remote platform disable
- Network outbreak containment
- Asset management / tracking
- Audit-log maintenance
- Software update
- Inventory collection

Delayed Response

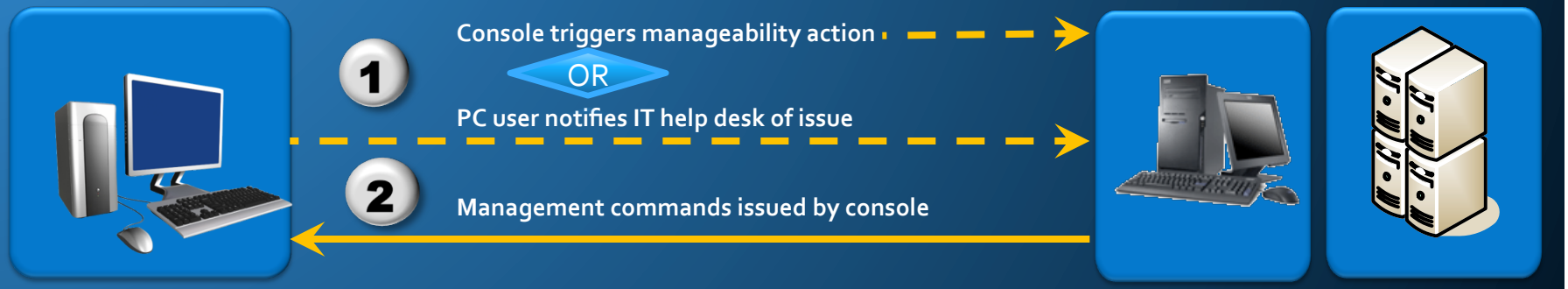


Mix of vPro usages by end customers

Platform can be powered down or in sleep states

Typical vPro™ Use Case Flow

Console-Initiated Use Model

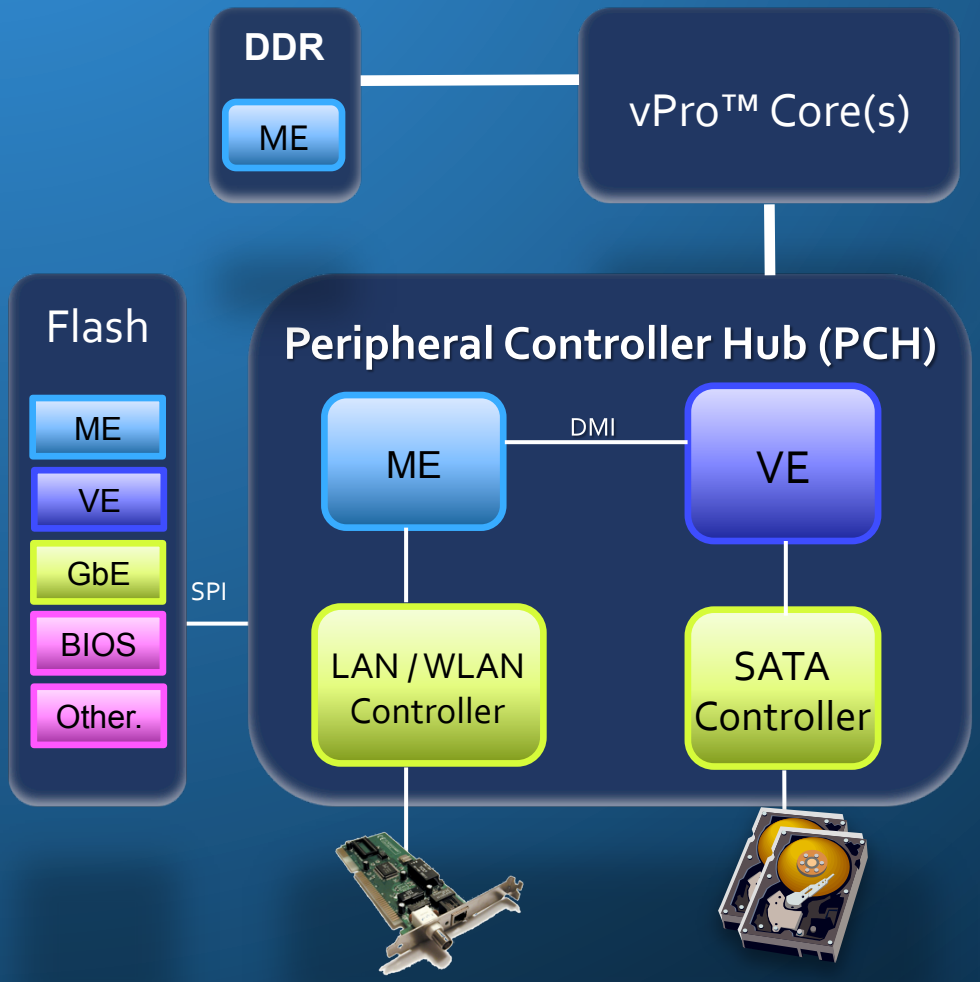


How Kerberos is used:

- MC obtains a Svc Ticket to access vPro platform
- Svc Ticket may contain AD PAC structure authorizing ME actions
- Svc Ticket used with WS-Man to establish a connection
- MC may wake platforms that are powered down
- ME maps PAC to ME-realms (more on ME realms later)
- Manageability action is performed using ME commands

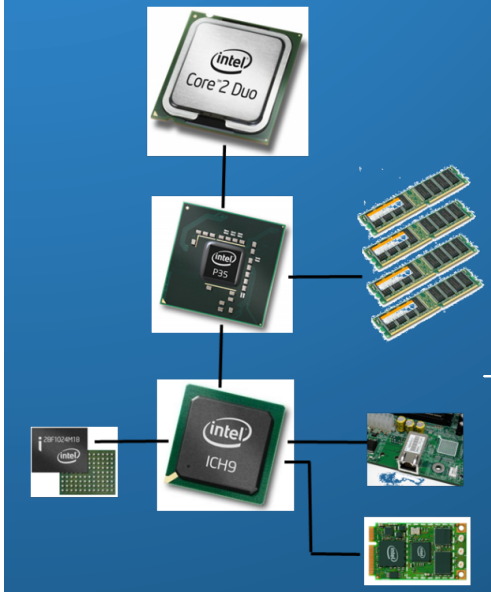
Source: *"Making Security Practical in the Enterprise with Client Technologies"*, Ned Smith, IDC2007

vPro™ Hardware Architecture



- Management Engine (ME)
  - ARC4 micro-controller
  - Direct access to LAN / WLAN
- SPI Flash
  - ME code and data storage
- DDR Memory
  - ME partition hidden from CPU
- Virtualization Engine (VE)
  - ME signaling traffic

vPro™ Embedded Software Architecture



PCIe Device Inteface

Intel® Active Management Technology (AMT)

Intel® Anti-Theft Technology

Future Capability

ME Common Services

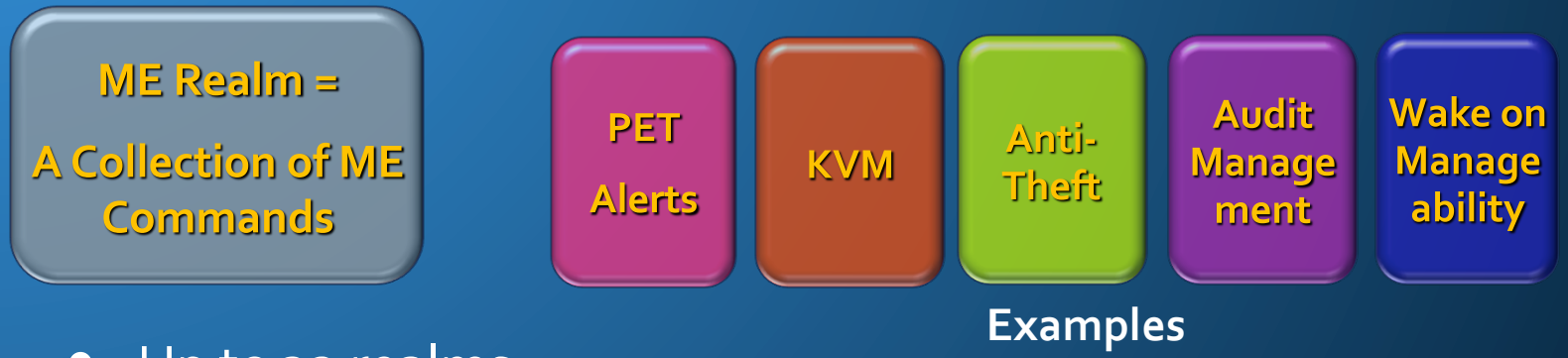
Networking Services
TCP/IP, TLS, HTTP
SOAP, WSMAN
N/W interface to Host

Security Services
Authentication
(HTTP Digest, Kerberos),
authorization, secure time,
Secure Audit Logging

Provisioning Services
Pre-shared Key based,
Certificate based
(Zero Touch, One Touch)

ME Kernel
(Thread X)

ME Realms



- Up to 32 realms
- May contain any / all ME commands
- Realm definition performed at time of manufacture
- 3 types of user authentication are supported
  - Local (password), HTTP-digest or Kerberos

Allowing dynamic Realm definition has been considered

Challenges

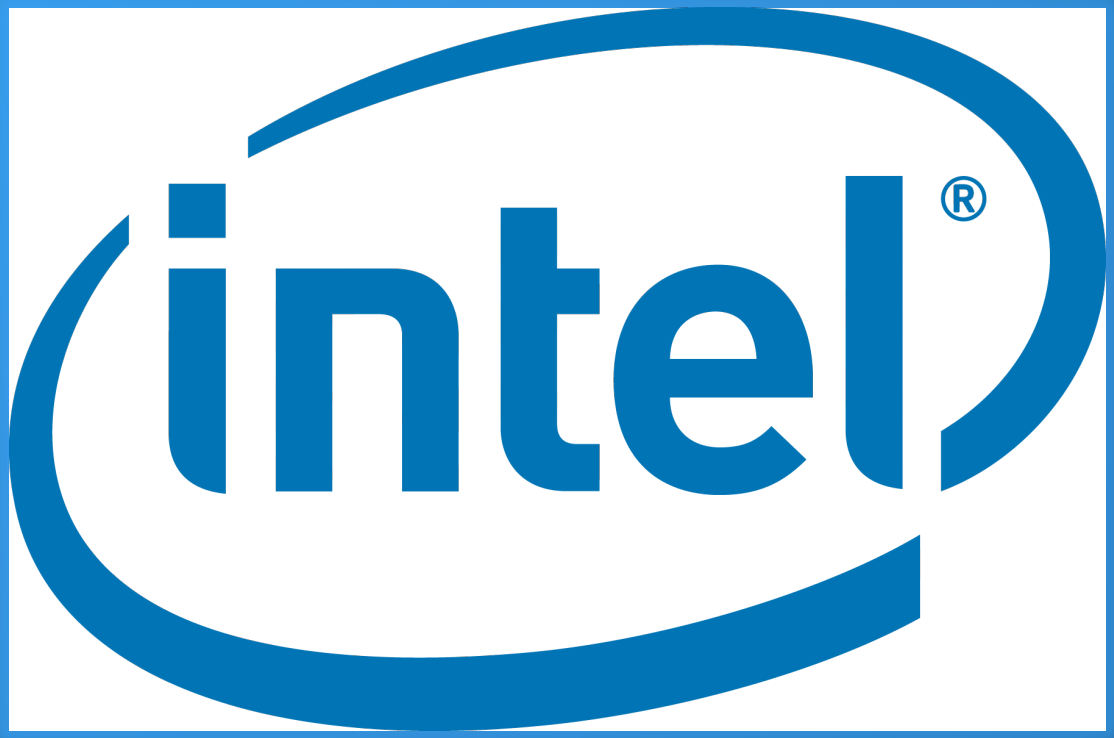
- Authorization
  - Large PAC structure parsing can "run out of gas"
  - ME Realms must span different identity systems (e.g. HTTP-digest, local, AD etc…)
- Roaming / Remote Access
  - vPro™ server platform can roam where IP address changes frequently.
  - DNS updates don't propagate in real-time.
    - >45 min delay typical for large enterprise
    - Active Directory DNS update adds additional latency
  - VPN / firewall traversal solutions often don't support "inside-out" connections
- Client Authentication
  - vPro use cases also require user authentication (e.g. KVM, Anti-theft, and others)
  - Multi-factor integration (e.g. smartcards, biometrics, OTP and NFC)
  - Strength of function for authentication factors

Possible Solutions

- Authorization
  - SAML assertions - Can it be implemented in constrained environments?
- DNS / Roaming kerberized servers
  - SIP – Will it work for Service Principal Names?
- Authentication
  - PKINIT – Will it work for OTP, NFC, and biometrics?

Conclusion

- Intel® vPro™ technology includes a Kerberos server
- Manageability usages appear to be compelling,
- But….
  - Heavy use of authorization / PAC can overwhelm "small" servers
  - DNS doesn't scale appropriately for roaming servers
  - VPN and firewall traversal for "inside-out" connectivity is not easy
  - Authentication strength of function for human-computer interaction is missing

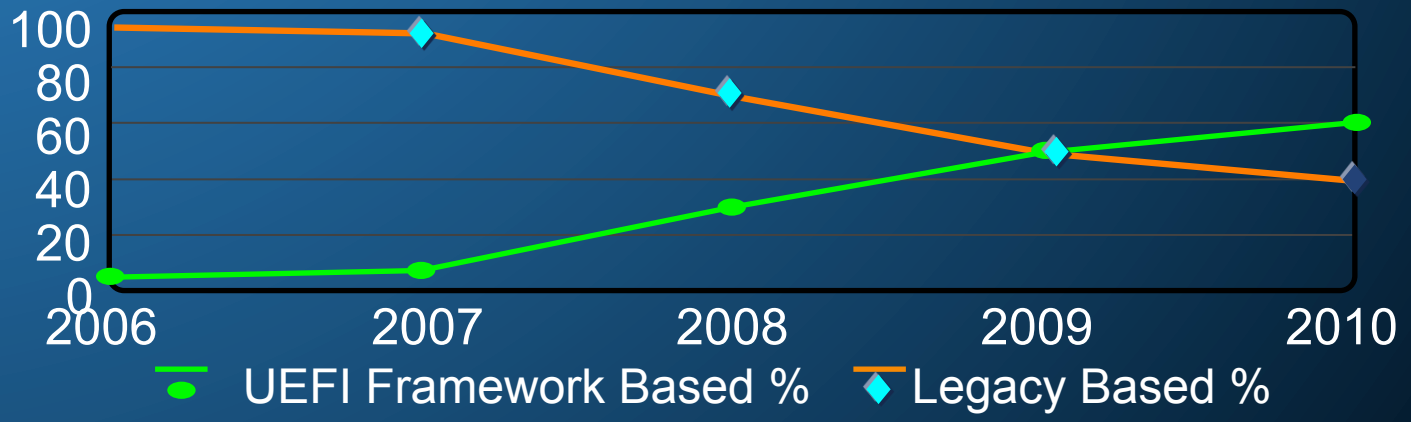

intel

Pros and Cons

- SIP
  - Pros: Standards-based, scalable
  - Cons: SIP designed to track people not platforms – will it work
    - Not yet ubiquitous
    - Security concerns
- PKINIT
  - Pros: Allows multi-factor auth
  - Cons: Lacks proof of assurance
    - VPN / firewall traversal lacking

Interfaces like the Intel® Framework for EIF spur innovation

- Intel® Platform Innovation Framework is Intel's implementation of EFI
- Unified EFI forum promotes and manages specs (www.uefi.org) and brings standards to the system firmware
  - Dell, HP, IBM, Lenovo, AMI, Insyde, Phoenix; Intel, AMD, Apple, Microsoft
- Intel contributed specifications to seed creation of UEFI 2.0 and Platform Initialization 1.0



Source: Various – IDC Sep'07 worldwide vendor market share; Intel customer platform adoption projection