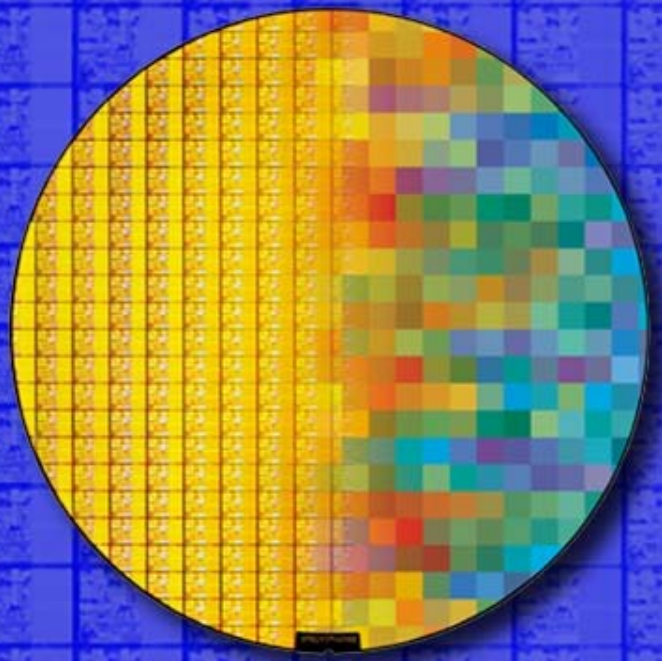


Digital Office Network Access Control Technology and Standards

Ned M. Smith

Security Architect,
Desktop Platforms Group

intel

Intel Developer FORUM

- INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY RELATING TO SALE AND/OR USE OF INTEL PRODUCTS, INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT, OR OTHER INTELLECTUAL PROPERTY RIGHT.

- Intel may make changes to specifications, product descriptions, and plans at any time, without notice.

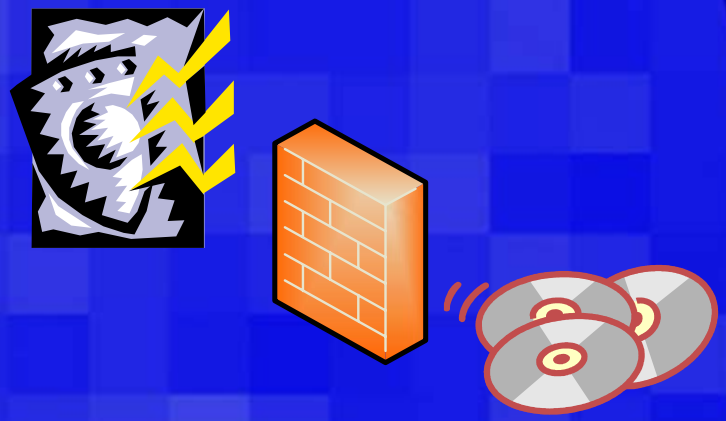
- All dates provided are subject to change without notice.

Agenda

- Overview of Network Access Control
- Is NAC Trustworthy?
- Improvements Through Standards
- Improvements Through Intel *Ts
  - Intel® Active Management Technology (Intel® AMT) and NAC
  - Intel LaGrande Technology (LT)
- Standards Update

What is Network Access Control? (NAC)

- Controlling access to the network based on platform configuration state
  - Anti-virus
  - Firewall configuration
  - Approved applications
  - Etc…



- Authenticating platform or user or both

NAC Performs Several Operations



Collection



Reporting



Decision Making



Enforcement

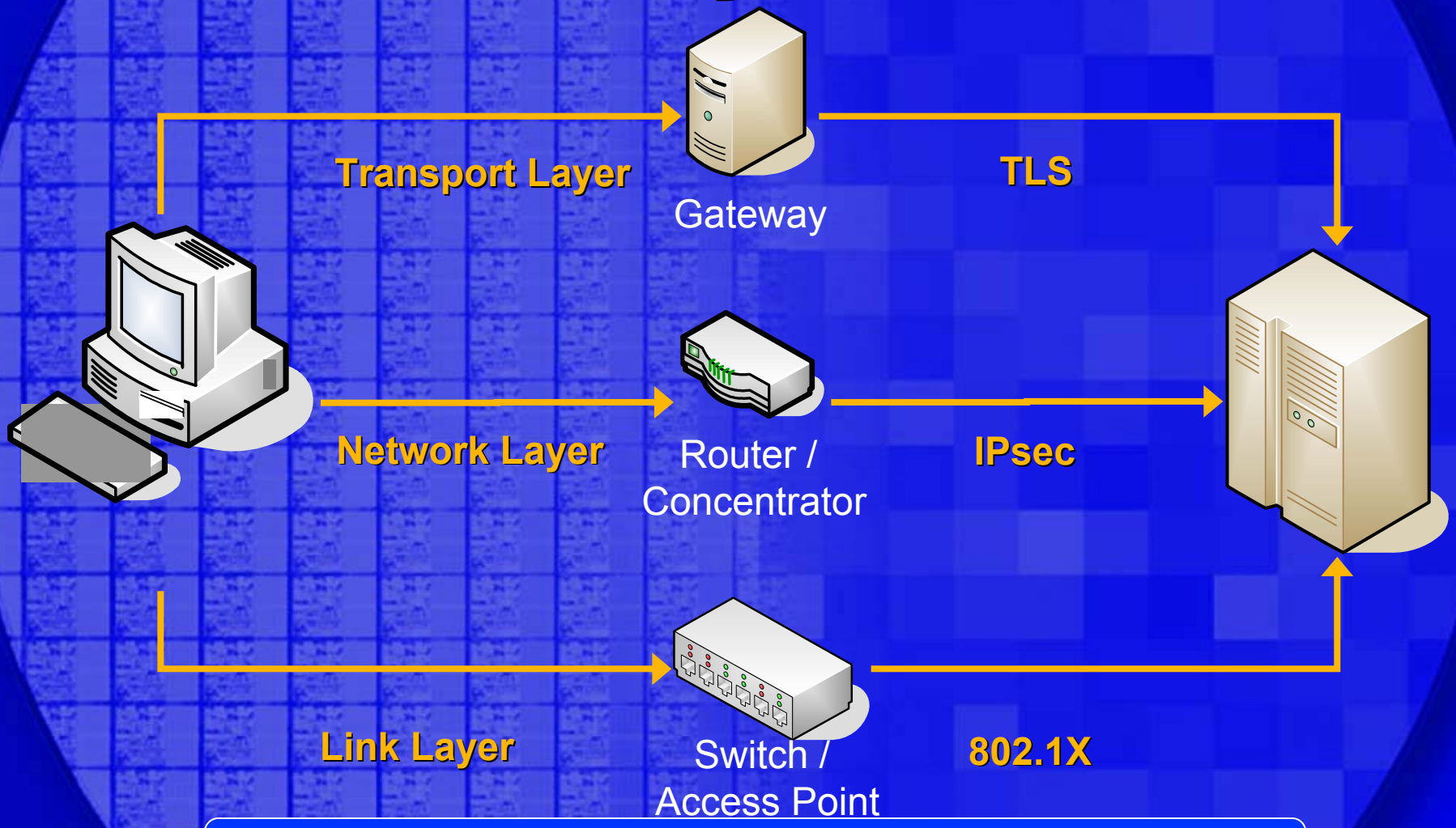


Remediation

- Find out the condition of the platform
- Communicate platform state when connecting
- Decide what level of access is acceptable
- Restrict the environment in accordance with access rights
- Remediation may be required to reconcile denied access

See IDF session DGOS007 for additional detail about NAC usage models

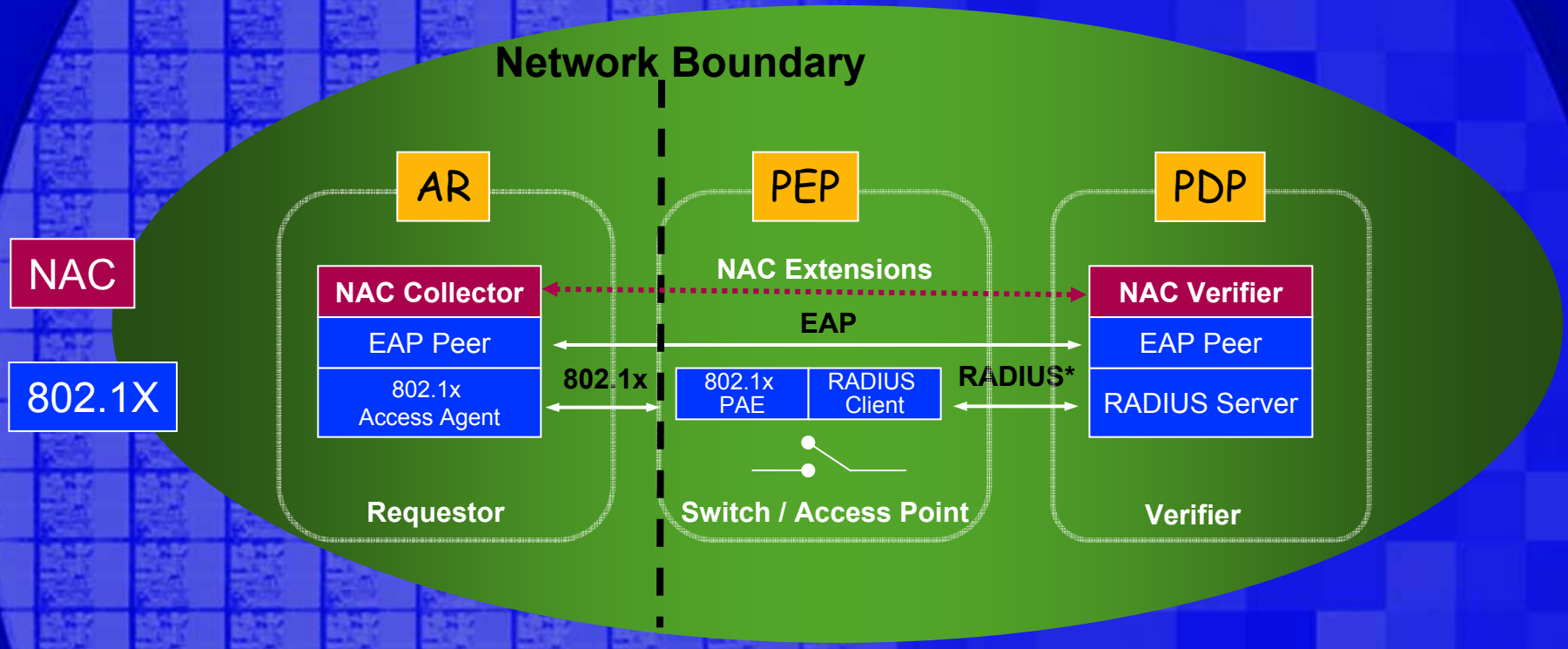
NAC can be Applied at Different Network Layers



NAC decisions should be enforced consistently even if NAC is implemented at a different layer

*Third party marks and brands are the property of their respective owners

NAC with 802.1X at Link Layer



NAC Verifier decides access based on posture information provided by the **NAC Collector** during port connect to switch or access point

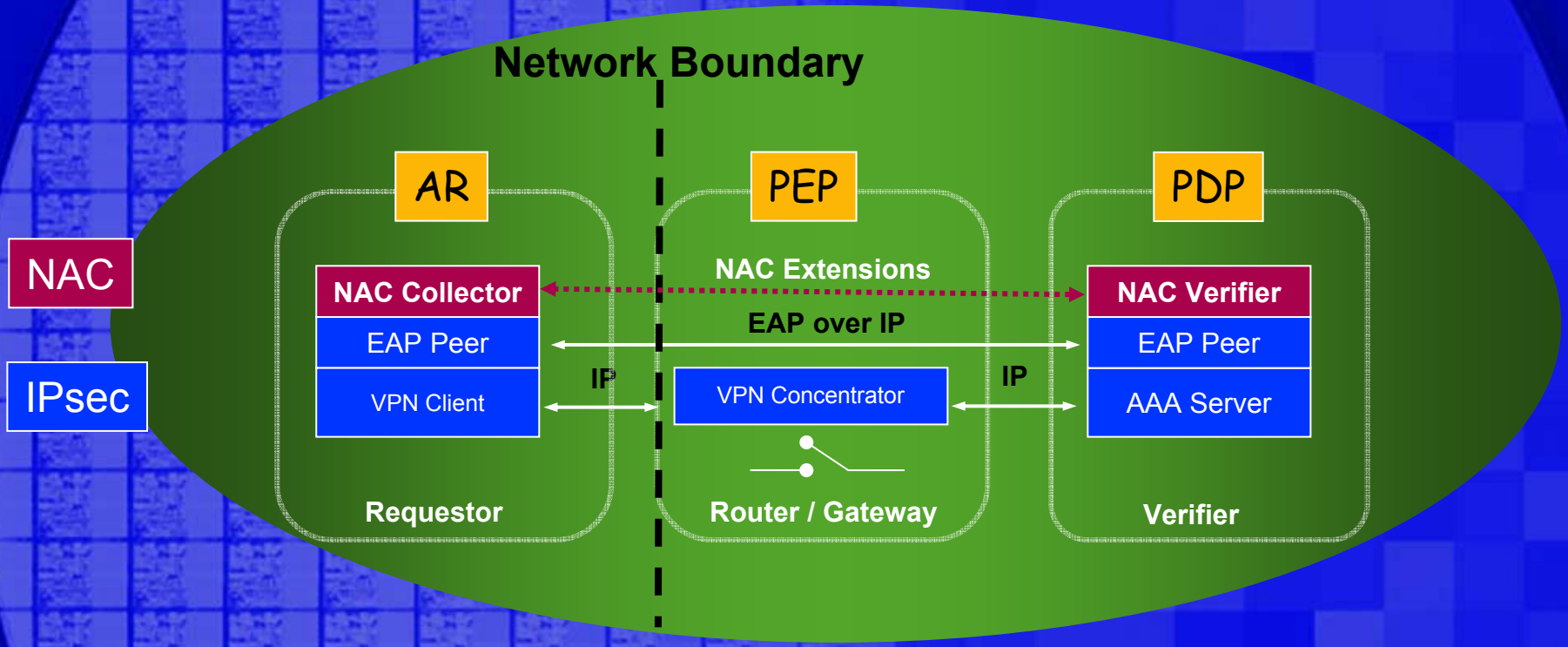
AR – Access Requester
AVP – Attribute Value Pair
EAP – Extensible Authentication Protocol
PAE – Port Access Entity

PDP – Policy Decision Point
PEP – Policy Enforcement Point
NAC – Network Access Control
TLV – Tag Length Value

*Third party marks and brands are the property of their respective owners

Intel Developer FORUM

NAC with IPsec at Network Layer

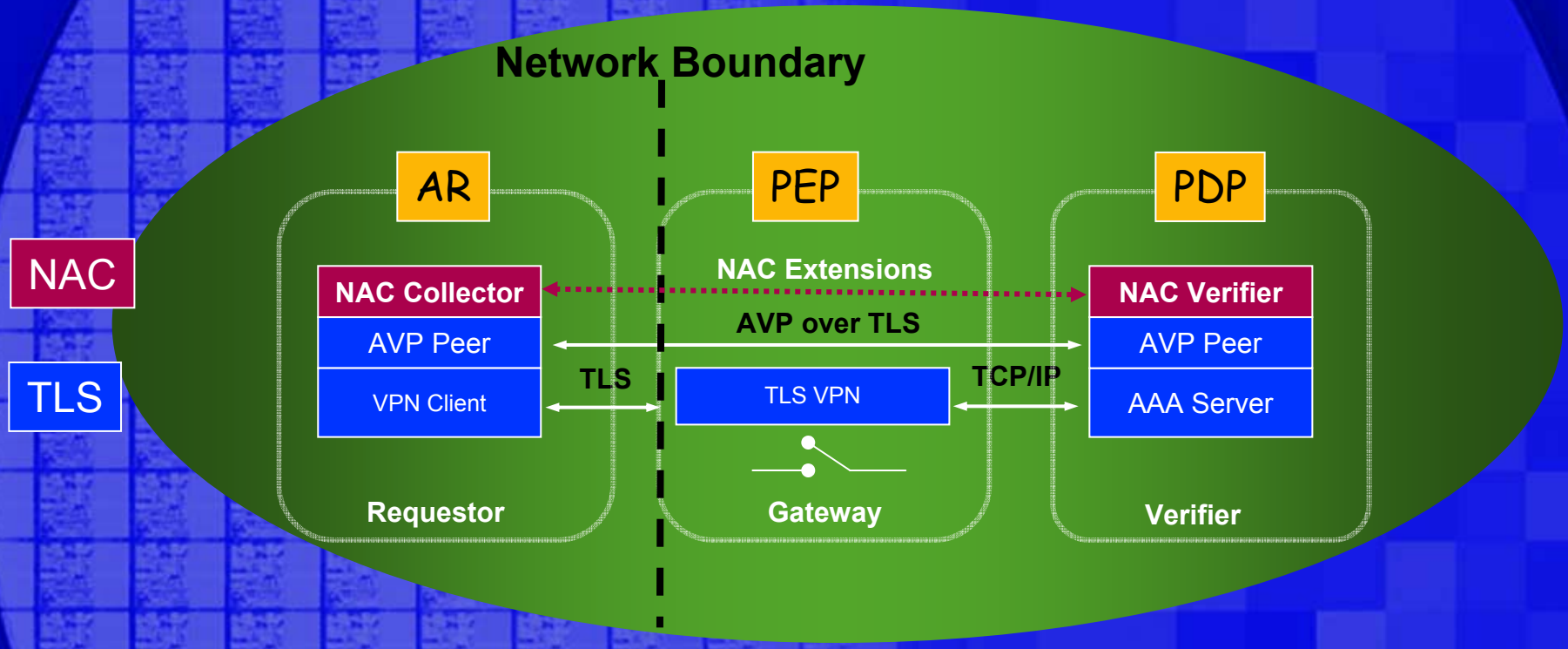


NAC Verifier decides access based on posture information provided by the **NAC Collector** during VPN handshake to VPN concentrator

AAA – Authentication, Authorization, Audit
AR – Access Requester
EAP – Extensible Authentication Protocol
IP – Internet Protocol
IPsec – IP security
PDP – Policy Decision Point
PEP – Policy Enforcement Point
VPN – Virtual Private Network

*Third party marks and brands are the property of their respective owners

NAC with TLS at Transport Layer



NAC Verifier decides access based on posture information provided by the **NAC Collector** during TLS handshake to TLS gateway

AAA – Authentication, Authorization, Audit
AR – Access Requester
AVP – Attribute Value Pair
TLS – Transport Layer Security
PDP – Policy Decision Point
PEP – Policy Enforcement Point
VPN – Virtual Private Network

*Third party marks and brands are the property of their respective owners

Intel Developer FORUM

Who is Building NAC Solutions Today

- TCG Trusted Network Connect (TNC)
  - A consortium of companies
- Microsoft* Network Access Protection
- Cisco* Network Admission Control

*Third party marks and brands are the property of their respective owners

Standards Related to NAC

- TCG Trusted Network Connect (TNC)
  - Client and Server NAC Interfaces
    - more on this later…
- Internet Engineering Task Force (IETF)
  - TLS Inner-Application extensions (TLS/IA)
  - EAP-TTLS
  - EAP over IPv6
  - RADIUS & DIAMETER
- IEEE
  - 802.1X / EAP

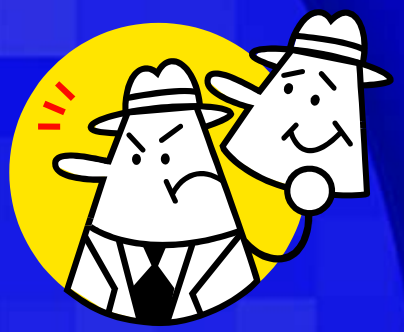


*Third party marks and brands are the property of their respective owners

Agenda

- Overview of Network Access Control
- Is NAC Trustworthy?
- Improvements Through Standards
- Improvements Through Intel *Ts
  - Intel® AMT and NAC
  - Intel LT
- Standards Update

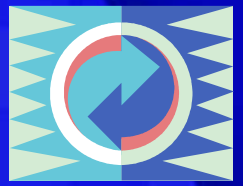
Security Threats Faced by NAC



- Compromised endpoint
  - Collector spoofing
    - A “good” status reported (when it isn’t)
  - Tunnel redirection
    - An authenticated tunnel passes unauthenticated status
  - Ambiguity
    - Insufficient / inconclusive status information returned
- Compromised network
  - Worm propagation
    - From network to endpoint
  - Denial-of-service
    - Can’t access network resources



NAC Trust Model Assumptions



- Assumption 1: Client is not trusted
  - Implication: Need to collect client status
- Assumption 2: Collected status is valid
  - Implication: Its OK to grant privileges
- Assumption 3: Client did not lie about assumption #2



- But what if client lies?

NAC needs trustworthy collection and reporting mechanisms

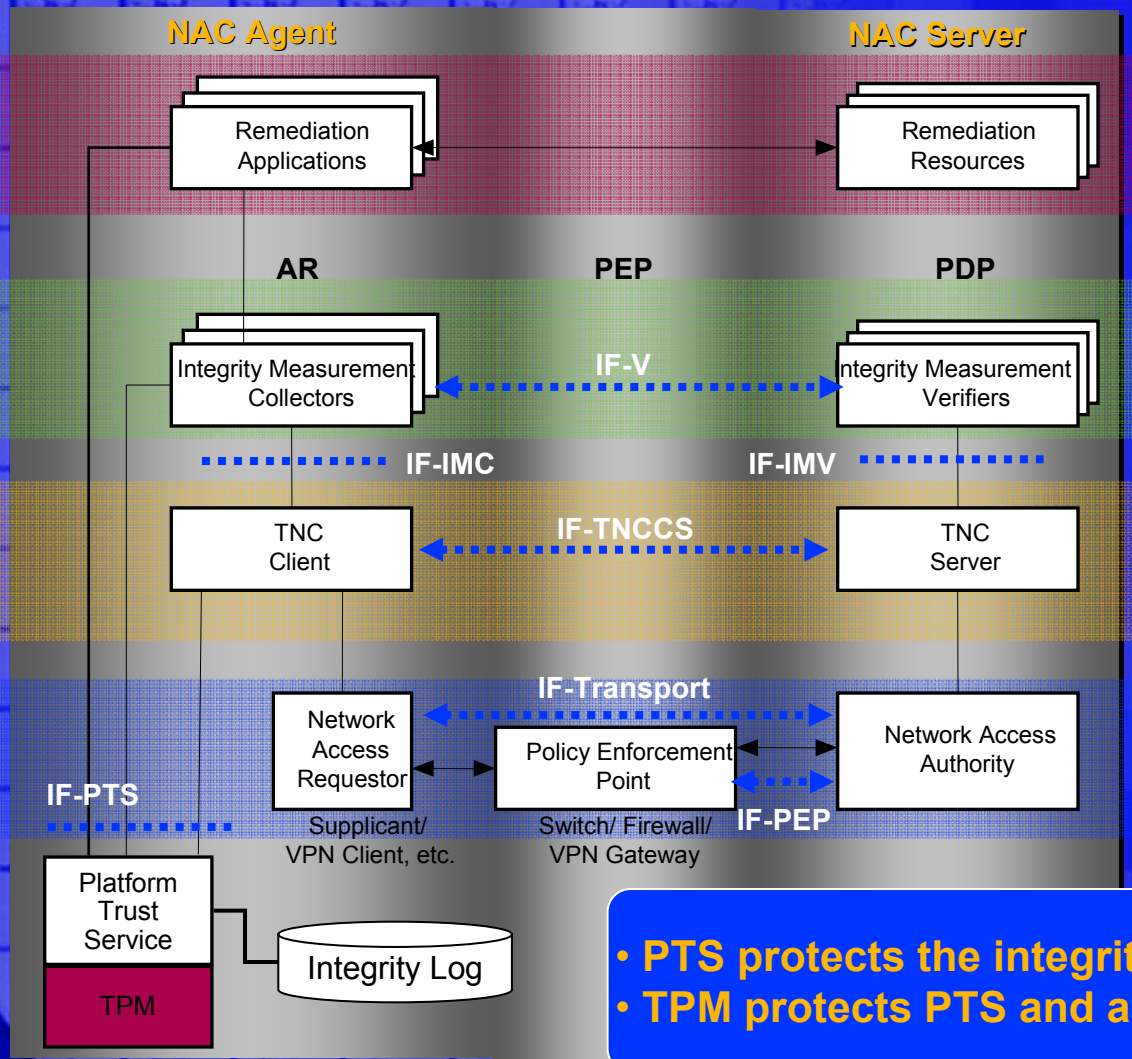
Possible Countermeasures

- Integrity checks applied to NAC collection and reporting mechanisms
- Authenticate integrity reports along with authenticating the channel
- Isolate NAC collection and reporting mechanisms from host tampering
- Protect keying material used for authentication
- Protect integrity logs and previously collected integrity state

Agenda

- Overview of Network Access Control
- Is NAC Trustworthy?
- Improvements Through Standards
- Improvements Through Intel *Ts
  - Intel® AMT and NAC
  - Intel LaGrande Technology
- Standards Update

TCG Trusted Network Connect



- Automated response and provisioning
- Collection of integrity information
- Authoring of rules
- Reporting and transfer of integrity information
- Access decision making
- Enforcement mechanisms
- Control of network boundary

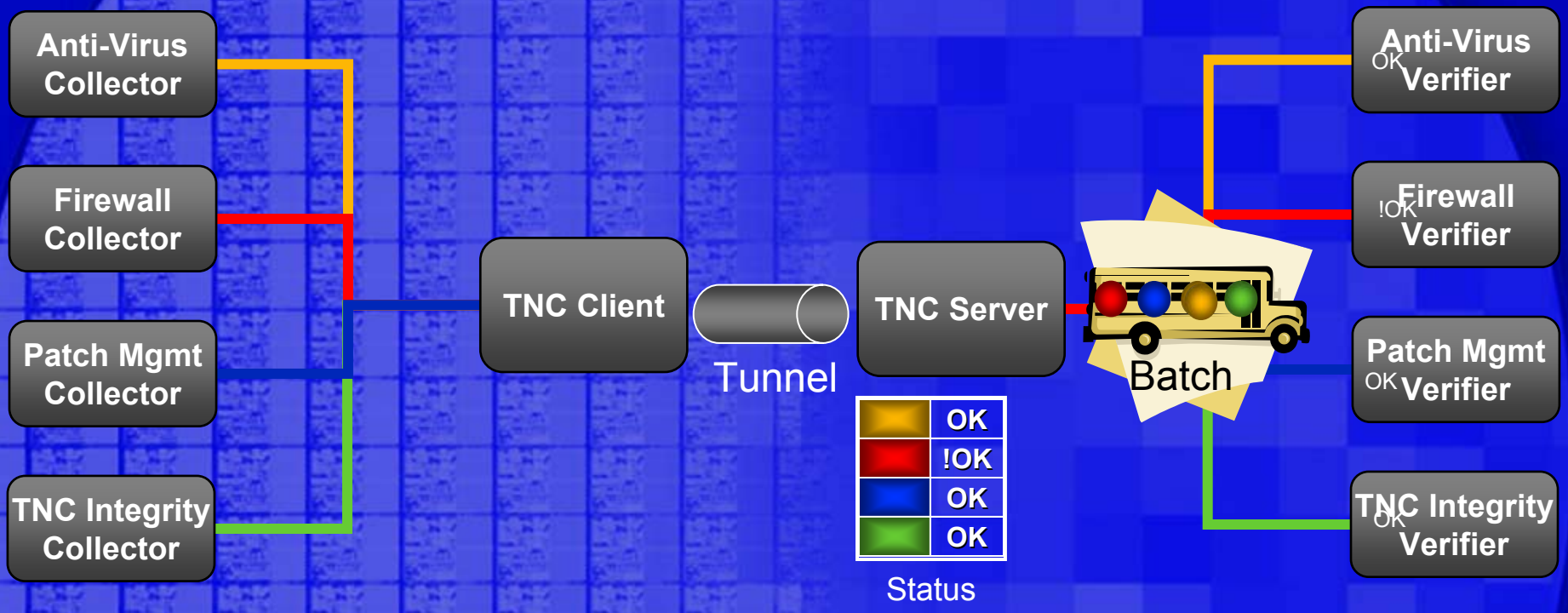
- **PTS protects the integrity of NAC components**
- **TPM protects PTS and authentication keys**

TNC specifications

Optional in TNC

*Third party marks and brands are the property of their respective owners

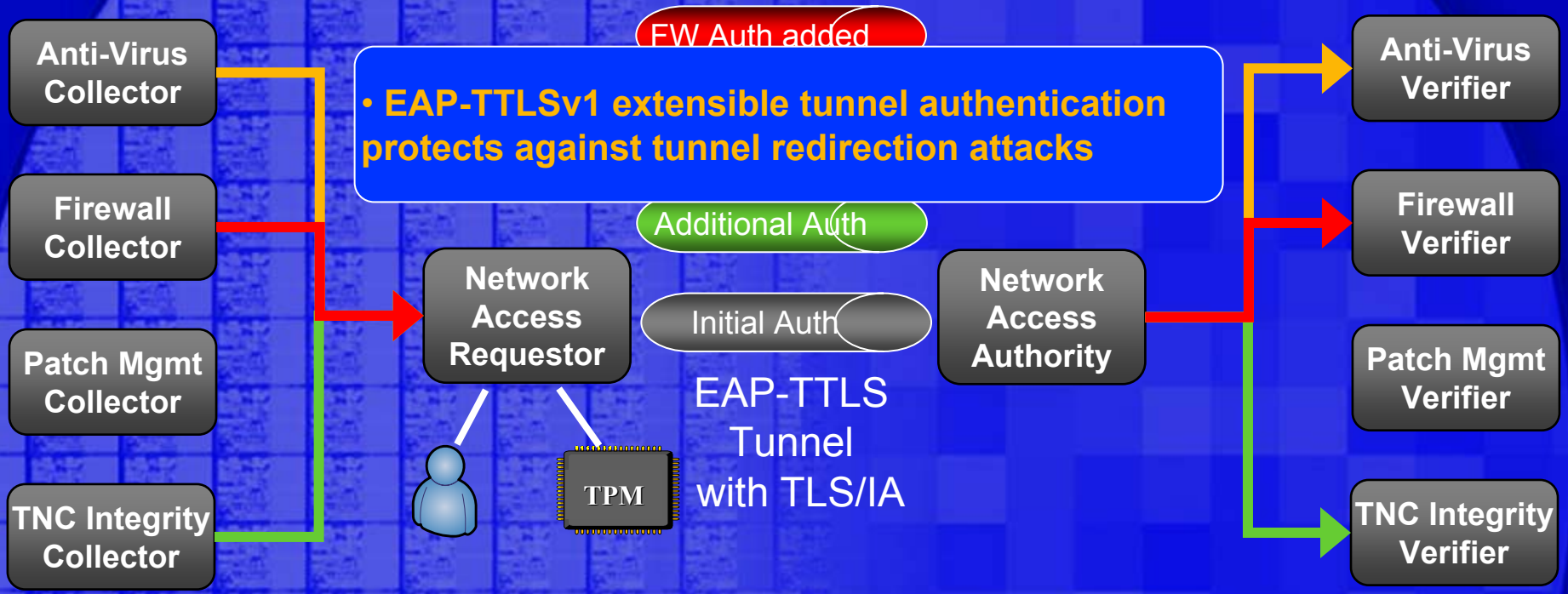
TCG Trusted Network Connect IF-IMC & IF-IMV



- IF-IMC & IF-IMV exchange messages
  - Messages are batched for delivery by TNCC / TNCS
  - Either side may start a batched exchange
  - IMCs and IMVs may subscribe to multiple message types
  - Follow-on exchanges may continue indefinitely
    - Gated by the underlying transport

*Third party marks and brands are the property of their respective owners

IETF EAP-TTLSv1

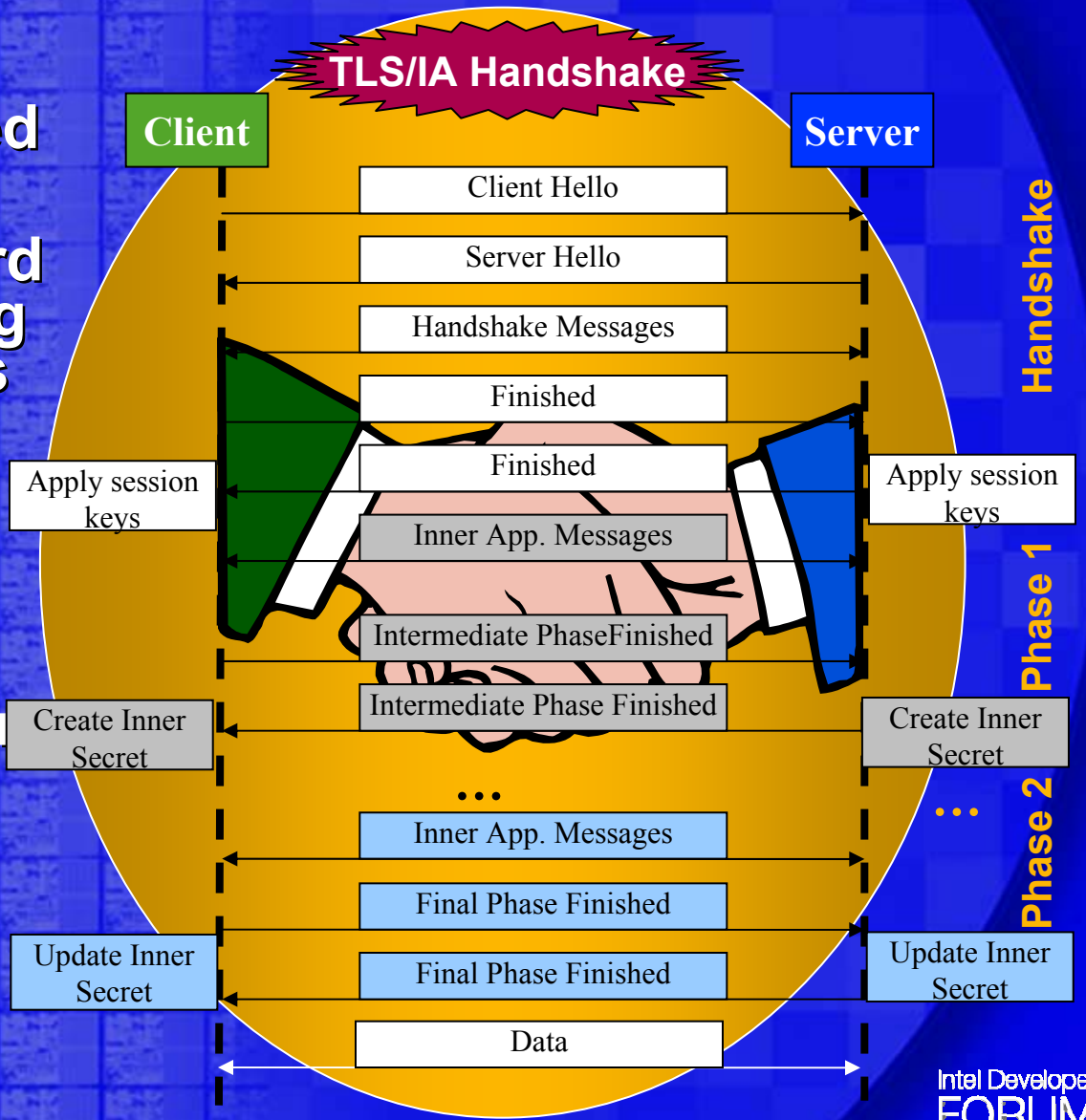


- EAP-TTLS establishes a tunnel between NAC endpoints
  - Tunnel provides protection from network-based attacks
  - Tunnel endpoints may be anonymous
- User and platform authentication
  - Links tunnel to cryptographic keys
  - Does not protect against platform-based MITM attacks
- TNC Integrity Collector further identifies the endpoint
- Authentication granularity can be added to the tunnel

*Third party marks and brands are the property of their respective owners

IETF TLS/IA - Inner Application Extension

- What is TLS/IA?
  - TLS extension based on RFC3546
  - Defines a new record layer for exchanging attribute value pairs (AVP)
- TLS/IA Value
  - Authentication of collected values
  - Protection from tunnel redirection
  - Flexible messaging model
  - Broad applicability

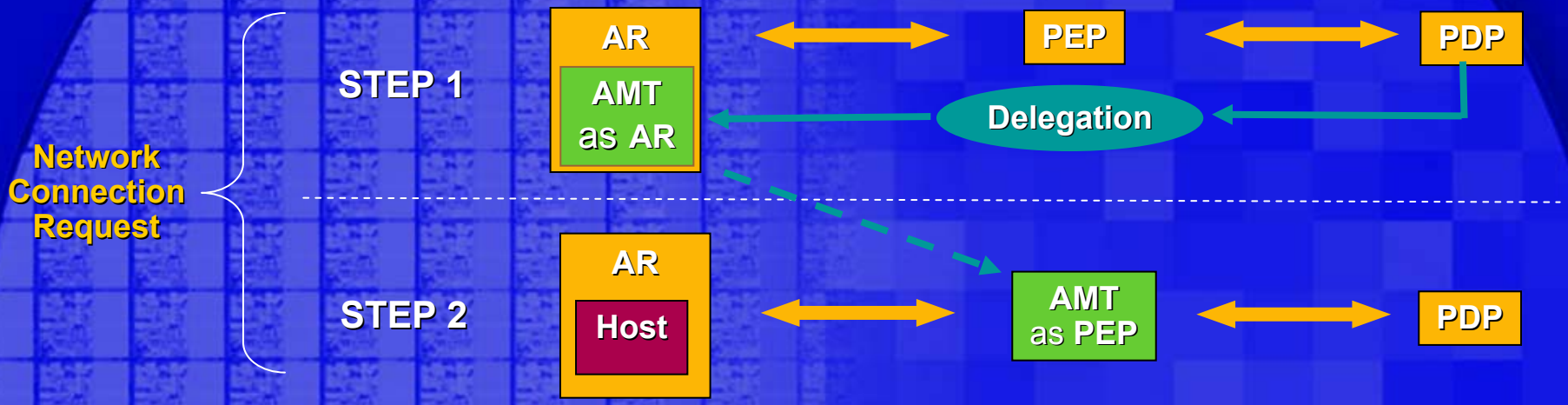


*Third party marks and brands are the property of their respective owners

Agenda

- Overview of Network Access Control
- Is NAC Trustworthy?
- Improvements Through Standards
- Improvements Through Intel *Ts
  - Intel® AMT
  - Intel LaGrande Technology
- Standards Update

Role of Intel® AMT in NAC



- Network connection with Intel® AMT
  - Two step process
- Intel® AMT adjustable network boundary
  - Platform level access control
  - Outbreak containment control
  - Defense in depth
- Intel® AMT enforcement
  - Protection of collection and reporting capability
  - Protection of protocol endpoint

*Third party marks and brands are the property of their respective owners

LaGrande Technology and NAC

- LaGrande Technology provides isolation of NAC processes
  - Increased assurance that the NAC mechanism has not been compromised
- LaGrande Technology provides additional platform measurements
  - Secure VMM launch
- LT measurements are collected, reported and evaluated via NAC infrastructure
- NAC and LaGrande Technology are synergistic
  - They can function independently but provide greater value when combined

Agenda

- Overview of Network Access Control
- Is NAC Trustworthy?
- Improvements Through Standards
- Improvements Through Intel *Ts
  - Intel® AMT
  - Intel LaGrande Technology
- Standards Update

Standards Update

- TCG
  - Trusted Network Connect
    - IF-IMC – Defines messaging between IMC and TNC-Client
    - IF-IMV – Defines messaging between IMV and TNC-Server
      - Specifications are complete and undergoing technical and IP review
    - IF-PTS – Establishes integrity of TNC components
    - IF-TNCCS – Defines interoperable message formats
    - IF-PEP – Defines conventions for PDP to PEP communication
    - IF-Transport –Profiles for TNC-Client use of access methods
      - Specifications are underway
- IETF
  - TLS/IA draft submitted as individual RFC
    - http://www.ietf.org/internet-drafts/draft-funk-tls-inner-application-extension-01.txt
  - EAP-TTLSv1 submitted as individual RFC
    - http://www.ietf.org/internet-drafts/draft-funk-eap-ttls-v1-00.txt
  - EAP over IP
    - http://www.ietf.org/internet-drafts/draft-eronen-ipsec-ikev2-eap-auth-02.txt>

Key Points

- Intel is driving industry NAC standards to make NAC broadly available
- Intel technology improves NAC
  - Intel® AMT provides control and enforcement of network boundary
  - Virtualization Technology and LaGrande technology improve isolation of NAC mechanisms
  - LT improves believability and trust
  - TPM provides protected storage for keys and PCRs
  - PTS extends transitive trust to NAC components

See IDF session DGOS007 for detail on Intel's NAC implementation Code named "Prineville"

*Third party marks and brands are the property of their respective owners

Please fill out the Session Evaluation Form

*Completed Session Evaluation forms will be entered into a daily drawing for prizes**

Thank You!

To download the presentation PDF, please go to:
http://www.cplan.com/idfsp05/USA/CCC
User name: idf
password: spring05

*See info sheet available at entrance to room, or Program Guide for details about the daily drawing.

*Third party marks and brands are the property of their respective owners