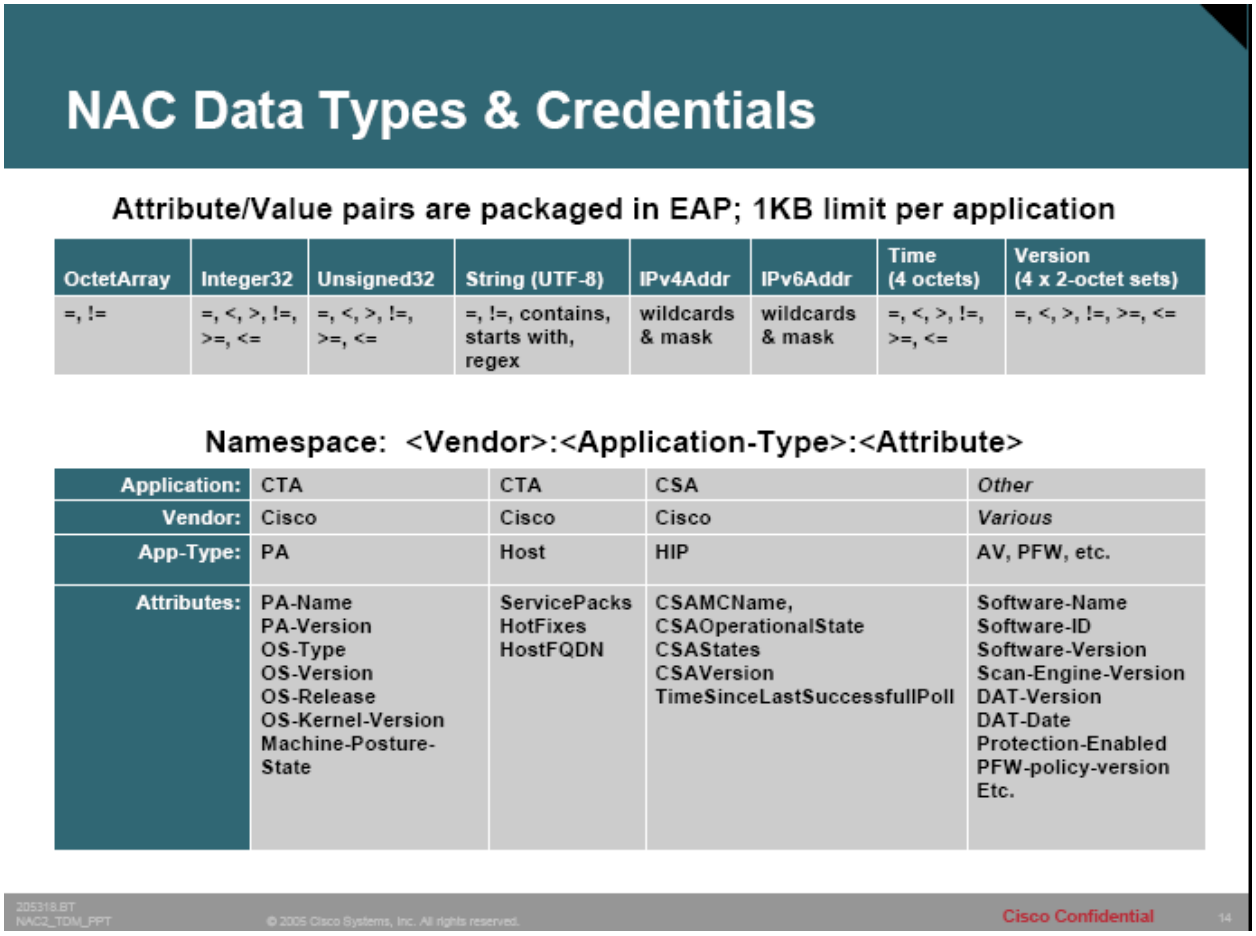
- **From CISCO:**



NAC Data Types & Credentials

Attribute/Value pairs are packaged in EAP; 1KB limit per application

OctetArray	Integer32	Unsigned32	String (UTF-8)	IPv4Addr	IPv6Addr	Time (4 octets)	Version (4 x 2-octet sets)
=, !=	=, <, >, !=, >=, <=	=, <, >, !=, >=, <=	=, !=, contains, starts with, regex	wildcards & mask	wildcards & mask	=, <, >, !=, >=, <=	=, <, >, !=, >=, <=

Namespace: <Vendor>:<Application-Type>:<Attribute>

Application:	CTA	CTA	CSA	*Other*
Vendor:	Cisco	Cisco	Cisco	*Various*
App-Type:	PA	Host	HIP	AV, PFW, etc.
Attributes:	PA-Name PA-Version OS-Type OS-Version OS-Release OS-Kernel-Version Machine-Posture-State	ServicePacks HotFixes HostFQDN	CSAMCName, CSAOperationalState CSAStates CSAVersion TimeSinceLastSuccessfullPoll	Software-Name Software-ID Software-Version Scan-Engine-Version DAT-Version DAT-Date Protection-Enabled PFW-policy-version Etc.

- **From TNC:**

What are some attributes of TNC?
TNC is based on the twin concepts of integrity and identity. *Integrity* is used in this case to describe the desired state of an endpoint's "health" or configuration, as defined by IT policies. Examples might be to check if the system adheres to pre-determined policies and determine the system is not engaged in unusual or malicious behavior. *Identity* ensures that systems are authenticated for authorized users only.

The TNC specifications will also define interoperability interfaces to allow for the exchange of new types of attributes in the context of network access control solutions. Those attributes will include endpoint compliance information, software state attestation, as well as information pertaining to the Platform-Authentication exchange [2].

Here, the TNC Architecture seeks to provide a richer set of security attributes for use in authorization policies. Thus, a Requestor can be given or denied network access based on a set

of finer grain rules that peer deeper into the Requestor's system state. In this way, a AAA Server can provide authorization to a Client not only on the basis of the Client's network-related attributes (e.g. IP address, domain) and user-related attributes (e.g. user password, user certificate), but also on the Client platform integrity state (e.g. hardware configuration, BIOS, Kernel versions, OS patch level, Anti-Virus signatures, etc).

With the growing popularity of EAP as a way to allow various authentication methods to be used between the AR (i.e. client, EAP-Peer or Supplicant) and PDP (Authentication Server), extensions have thus been defined in RFC3579 for RADIUS itself to support EAP. The aim of the extensions is to use RADIUS to shuttle RADIUS-encapsulated EAP packets between the AR (or PEP in the TNC Architecture) and the PDP Two new attributes that were introduced into RADIUS in RFC3579 to achieve this are the EAP-Message and Message-Authenticator attributes.

- **From Encyclopedia:**

Attributes of a secure network

Network security starts from authenticating any user, most likely an username and a password. Once authenticated, firewall enforces access policies such as what services are allowed to be accessed by the network users.[1] Though effective to prevent unauthorized access, this component fails to check potentially harmful contents such as computer worms being transmitted over the network. An intrusion prevention system (IPS)[2] helps detect and prevent such malware. IPS also monitors for suspicious network traffic for contents, volume and anomalies to protect the network from attacks such as denial of service. Communication between two hosts using the network could be encrypted to maintain privacy. Individual events occurring on the network could be tracked for audit purposes and for a later high level analysis.

Honeypots, essentially decoy network-accessible resources, could be deployed in a network as surveillance and early-warning tools. Techniques used by the attackers that attempt to compromise these decoy resources are studied during and after an attack to keep an eye on new exploitation techniques. Such analysis could be used to further tighten security of the actual network being protected by the honeypot.[3]

- **From Sun-**

Trusted Network Security Attributes

Network administration in Trusted Extensions is based on security templates. A security template describes a set of hosts that have common protocols and identical security attributes.

Security attributes are administratively assigned to systems, both hosts and routers, by means of templates. The security administrator administers templates and assigns them to systems. If a system does not have an assigned template, no communications are allowed with that system.

Every template is named, and includes the following:

- A host type of either Unlabeled or CIPSO. The protocol that is used for network communications is determined by the host type of the template.

  The host type is used to determine whether to use CIPSO options and affects MAC. See Host Type and Template Name in Security Templates.

- A set of security attributes that are applied to each host type.