TRUSTED NETWORK COMMUNICATIONS ARCHITECTURE

Security Standards for Intelligent, Responsive, Coordinated Defense

TCG's Trusted Network Communications (TNC) network security architecture and open standards enable intelligent policy decisions, dynamic security enforcement, and communication between security systems. TNC standards provide network and endpoint visibility, helping network managers know who and what is on their network, and whether devices are compliant and secure. TNC standards also enable network-based access control enforcement — granting or blocking access based on authentication, device compliance, and user behavior — and security automation.

The need for IT security standards innovation

The constant innovation that makes technology so appealing—and so essential—also makes digital security a moving target. The explosive growth of mobile devices, our increasing reliance on wireless networks, and the Internet of Things—the interconnection of physical objects through the Internet that promises more personalized experiences and deeper integration of technology in our lives—brings with it an ongoing wave of new security threats which require new and innovative ways of dealing with them.

IT security standards play an ever-increasing role in striking a balance between consistent personalized experiences on a variety of devices and environments on the one hand, and the need to contain cost and minimize barriers to commerce on the other. IT security standards need to innovate and evolve in order to address:

- Managing risk across a wide range of computing devices in cost effective efficient ways
- Growing risks of endpoint compromise and data loss in an ever-increasing connected cyber world
- Increasing need to share security information and threat protections with others
- Automated cyber-attacks that necessitate the need for automated cyber defenses

TNC – security standards for intelligent, responsive, coordinated defense

TNC standards integrate security components across the endpoint, network, and servers into an intelligent, responsive, coordinated defense. The Trusted Computing Group (TCG), an international not-for-profit organization that develops, defines, and promotes open, vendor-neutral specifications for interoperable trusted computing platforms include business and technical specialists from the world's leading silicon makers, device manufacturers, and software and solution providers. Working collaboratively with industry experts, government officials, and academic researchers, TCG has been advancing trusted computing technology worldwide for more than a decade.

In response to the global need for a more secure computing environment, TCG has developed and published Trusted Network Communications (TNC) standards since 2005 as an open architecture originally intended as a network access control standard with a goal of multi-vendor endpoint policy enforcement. In 2009 TCG announced expanded Specifications which extended the specifications to systems outside of the enterprise network. Additional uses for TNC which have been reported include Industrial Control System (ICS), SCADA security, and physical security.

Solutions offered by TNC

TNC addresses four main classes of problems. ***Network visibility*** asks who is on the network, and what they are trying to access. ***Endpoint compliance*** asks whether devices on the network are secure, and whether user/device behavior is appropriate. ***Network enforcement*** gives the ability to block unauthorized users, devices, and/or behaviors, and to grant appropriate levels of access to authorized devices. ***Security system integration*** supports sharing real time information about the environment without giving out sensitive, private, or protected data; and asks how to benefit from threat intelligence generated across the spectrum, both internally to the environment and externally from other sources.

Capabilities enabled by the TNC architecture:

TNC offers three primary capabilities, which can be used individually or in combination to permit authorized access and prevent, detect and respond to unauthorized access and network attacks.

TNC Compliance Capability

The compliance capability enables endpoint compliance self-reporting and external scanning of the endpoint. Values received, either from the compliance report of from the results of a scan, can be compared to a policy housed on the compliance capability. Administrators can automate as much or as little of this process as they wish.

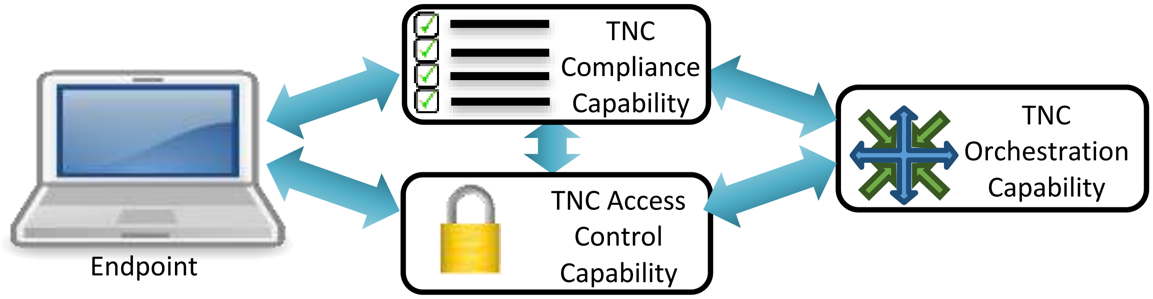
TNC Access Control Capability

The Access Control Capability can make decisions about whether to allow an endpoint to join the network, or to allow a currently connected endpoint to stay on the network. The Access Control Capability can gather information about the endpoint (i.e., whether the firewall is on, or whether the antivirus signatures are up-to-date) and compare the results to network policy. Based on the policy, the Access Control Capability may allow the endpoint to connect to the network, send it to a quarantine or remediation VLAN, or block the endpoint's access all together.

TNC Orchestration Capability

The Orchestration Capability offers a notification service and unified, extensible data model, enabling network and security devices to benefit from context they obtain from the capability to better perform their functions, and to share context with the capability to enable other components to better perform their functions. For example, a log reporting component can share information about activity on the network, enabling a policy server to make more informed decisions about an endpoint; the policy server can share information about the characteristics or state of an endpoint, enabling the SIEM to apply device-specific analytics.

Each of these capabilities can operate independently, which allows organizations to implement the features their network security plan requires. These capabilities can also act in concert, which provides abundant data for analyzing the state of enterprise network security.


TNC Compliance Capability
TNC Orchestration Capability
TNC Access Control Capability
Endpoint

Benefits of TNC

- TNC standards have a proven track record of delivering interoperable solutions to address endpoint, network, and server security. Products based on TNC standards have been shipping since 2005. There are many open-source implementations as well.
- TNC standards are widely deployed in real production scenarios. A broad range of customers across many sectors (Government, Healthcare, Finance, Retail and Education, among others) are benefitting from interoperable security solutions based on TNC standards.
- TNC standards are completely vendor-neutral. TNC based solutions leverage existing network infrastructure in a production environment, adding value to the existing investment.
- TNC standards are flexible. They support a broad range of assessment options (identity, health, behavior, and location; hardware-based & software-based security; and pre-admission & post-admission evaluation and monitoring). TNC standards also accommodate rapid change and can adapt to the evolving security landscape.
- TNC standards can and do easily integrate with other standards both existing and emerging, e.g., SCAP and SWID Tags (ISO 19770-2).

TPM Integration

The Trusted Platform Module is a hardware-based "root of trust" which helps provide platform integrity, user security, and privacy. The TPM enables a "chain of trust" for a device's core components which are responsible for its boot process and ultimately the execution of the OS and applications. In the context of TNC architecture and solutions, if available, TPM represents one example of a hardware-based root of trust which helps create a chain of trust that can be extended to TNC components.

Conclusion and next steps

The TNC architecture enables intelligent policy decisions, dynamic security enforcement, and communication between security systems. These capabilities give administrators visibility into networks and endpoints to determine who and what is on the network and whether devices are compliant and secure. TNC facilitates context-based access control - granting or blocking access based on authentication, device compliance, and user behavior - and security automation, for orchestration of network and security systems. Implementers and deployers of TNC-enabled technology are encouraged to review the updated architecture, as well as explore open-source implementations such as strongSwan. More information is also available in the TNC FAQ.