Networked device security posture management

1. United States Patent: 12184646
2. Date of Patent: December 31, 2024
3. Inventors:
    a. Mannengal; Arun (Sammamish, WA)
    b. Surapaneni; Chandra Sekhar (Sammamish, WA)
    c. Kumaraswamy; Rajesh (Bothell, WA)
4. Assignee: Microsoft Technology Licensing, LLC (Redmond, WA)
5. Abstract: Networked device management is based on an ontology graph which includes device nodes, physical facility nodes, and edges. The ontology graph may go beyond network topology by also documenting: relationships between devices and facilities, facility attributes such as facility-specific security scores, and device characteristics such as whether a device is recognized, whether it is authorized, and its mission criticality. Medical devices, physical condition sensors, and other internet of things devices, including those embedded in vehicles, those located on a vehicle, those used for industrial control, or those which are intermittently air-gapped, are managed. Devices may be discovered by extraction of identifications and characteristics from telemetry data in a staged architecture. Security postures may be assessed, and security recommendations based on device context may be provided.
6. BACKGROUND
    a. (1) A wide variety of devices may be connected by a network. Some devices include computing hardware, which may be controlled by firmware or other software. Some devices include physical condition sensors, to sense temperature, humidity, acceleration, pressure, position, or other physical conditions. Some devices include a display screen, while others do not. Some devices can only transmit data over a network connection, while other devices can transmit data and also receive data. Some devices have a typical working life span of multiple years, while others cease to be reliable, or even to function at all, after a shorter time. Some devices are inexpensive, while others are not.
    b. (2) Efforts to manage networked devices also vary widely. Management may be directed at goals such as accuracy, convenience, coverage, economy, efficiency, flexibility, portability, reliability, or security, for example. Improvements in networked device management are possible with respect to various goals.
7. SUMMARY
    a. (3) Some embodiments described herein address technical challenges related to networked device management, such as how to formulate device-specific management recommendations, as opposed to more general recommendations that do not apply as well to the specific device and its circumstances. Some embodiments manage networked devices based on relationships between specific devices and specific physical facilities, e.g., based on facility-specific security scores.
    b. (4) Some embodiments construct, update, or utilize an ontology graph as a basis for networked device management. The ontology graph has device nodes, facility nodes, and edges. Each edge between a device node and a facility node represents

a relationship between a corresponding device and a physical facility. Each edge between two device nodes represents a network communication between the corresponding devices.

c. (5) Other technical activities and characteristics pertinent to teachings herein will also become apparent to those of skill in the art. The examples given are merely illustrative. This Summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used to limit the scope of the claimed subject matter. Rather, this Summary is provided to introduce—in a simplified form—some technical concepts that are further described below in the Detailed Description. The innovation is defined with claims as properly understood, and to the extent this Summary conflicts with the claims, the claims should prevail.