8.2 IoT and CVD

Next we turn our attention to the implications that the Internet of Things brings to the CVD discussion. "Smart things" are expected to outnumber traditional computers in the near future and will likely surpass mobile phones not long thereafter. IoT will have implications to the protection of privacy, opportunities for fraud and abuse, and ensuring safety. Every vulnerable thing becomes a potential point of leverage for an attacker to persist or maneuver laterally through a network. Immature security on IoT devices can leak information that could allow an attacker to gain a foothold.

Because many such systems and devices are expected to remain operationally useful for years or even decades with minimal intervention, it is especially important that their security be thoroughly understood prior to deployment. This section collects a number of issues we observed in the course of recent work done by the CERT Vulnerability Analysis team, and is adapted from a CERT/CC blog post by Householder [1].

Black Boxes

We identified issues such as the inclusion of networked appliances in a larger system where the appliances provided networked services based on sensor data. Enterprise security policy treated the device as a black box rather than a general-purpose computer with regard to patch levels, included software, and so forth. The attack vector posed by the sensor data interface had not been considered either.

Unrecognized Subcomponents

In a number of projects, we observed that while many systems were composed of highly specified off-the-shelf and custom components, the vendors providing those systems often could not identify the third-party subcomponents present in the delivered codebase. The problem can be as simple as not identifying statically linked libraries or as complicated as dealing with complex supply chains for code components.

Long-Lived and Hard-to-Patch

We observed various devices with wireless data capabilities embedded within a larger system yet little or no ability to patch the fielded systems except within very sparse service windows. Instances where physical contact with the device is required in order to update it can be especially problematic once vulnerabilities are discovered (See Dan Geer's talk at the Security of Things Forum for more on the "long-lived and not reachable" problem [2]).

New Interfaces Bring New Threats

We also encountered smart grid devices built out of a traditional electrical component coupled to an embedded Linux system to provide networked services. In a deployment context, the device was treated as an appliance. However, the impact of potential vulnerabilities in the general-purpose operating system embedded in the device had not been fully addressed.

Summarizing the IoT's Impact on CVD

We anticipate that many of the current gaps in security analysis tools and knowledge will begin to close over the next few years. However, it may be some time before we can fully understand how the systems already available today, let alone tomorrow, will impact the security of the networks onto which they are placed. The scope of the problem does not appear to contract any time soon.

We already live in a world where mobile devices outnumber traditional computers, and IoT stand to dwarf mobile computing in terms of the sheer number of devices within the next few years. As vulnerability discovery tools and techniques evolve into this space, so must our tools and processes for coordination and disclosure. Assumptions built into the CVD process about disclosure timing, coordination channels, development cycles, scanning, patching, and so on, will need to be reevaluated in the light of hardware-based systems that are likely to dominate the future internet.

< 8.1 Vulnerability IDs and DBs | 9. Conclusion >

References

1. A. Householder, "Vulnerability Discovery for Emerging Networked Systems," 20 November 2014. [Online]. Available: https://insights.sei.cmu.edu/cert/2014/11/-vulnerability-discovery-for-emerging-networked-systems.html. [Accessed 16 May 2017].
2. D. Geer, "Security of Things," 14 May 2014. [Online]. Available: http://geer.tinho.net/geer.secot.7v14.txt. [Accessed 16 May 2017].