Published on *Telsoc* (https://telsoc.org)

Shall we hook up the old stuff?

Andreas Dannert [1]

ISACA Melbourne Chapter

AJTDE - Vol 3, No 4 - November 2015 [2]

[3]

☆ 9 [4]

Abstract

Computer systems, technologies and applications that do not meet current standards, known as legacy systems, are increasingly connected to the Internet for various reasons. Connecting them to an environment that they were never intended for can potentially have serious operational security risk implications. This article discusses some of the reasons.

Introduction

Connecting legacy systems (Wikipedia 2015a [5]) to the Internet can have serious implications for these systems and the environments they run in. These systems are typically designed to safely run in an intended, targeted environment, and not connected to the Internet.

The environments in which these systems can operate are described by a number of attributes with implicit requirements. These environmental attributes could be physical conditions, such as temperature range, humidity or pressure. For example, some computer systems need to run in harsh conditions like the extreme temperature ranges found in space while others may be deployed in the desert, the Arctic Circle or underwater.

Products like computer systems are typically optimised and built to meet the conditions of a particular environment. While theoretically a system could be built to function under any conditions, it is usually cost prohibitive to develop and deploy.

A set of requirements covering environmental suitability, security and usability is usually defined prior to a system being built. These requirements help to ensure that all parties involved in designing, building, commissioning and using a system get a better understanding of what can and cannot be expected. For critical systems, independent parties will also verify whether the set of requirements ? matching environmental conditions for example ? are in line with defined standards and practices. In these cases, meeting a particular standard might become a requirement in itself. Examples of these standards include the National Electrical Installation Standard (NEIS) (NEIS 2015 [6]) in the United States; DIN V 66304 (DIN 2015 [7]), a standard for industrial automation by the German Institute for Standardisation; or SAS 45, the Australian Standard for Safety (Standards Australia 2015 [8]).

Assuming that developers of legacy systems did not intend these systems to be connected to the Internet, these systems will not be designed to protect against the threats usually found in such a networked environment. An

example of a typical threat is a Denial of Service attack (Wikipedia 2015b [9]). Depending on the legacy system involved and its original requirements, this attack may have wider security implications. However, if the intended functionality of the system is not compromised by being connected to the Internet, then one should be able to conclude that it be done safely. On the contrary, if existing functionality is negatively impacted, the impact needs to be analysed and the risks mitigated by either changing the legacy system or introducing mitigating controls.

Some real world scenarios

Imagine a system running on the 23-year-old Windows 3.1 used to link air traffic control at one of France?s biggest airports with the country?s main weather bureau. (Whittaker 2015 [10]) What would be the implications of connecting it to the Internet? While one might question why the system runs on a Windows version that has been out of support for a while, we can assume that within a closed environment it might be cheaper and completely acceptable to run the system as it is as far as threats of being hacked are concerned. Of course the system owners and operators are running the risk that the skills required to support the system may become scarce.

The important question is: What are the implications of connecting this system to the Internet? Obviously the operating environment of the system would change, and connectivity to the Internet would introduce risks to a previously closed system. Suddenly the very dated operating system would become a liability that it might not have been before. Security patching of the system would be almost impossible, since the operating system has been out of support for a long time. The system will now not only have to be protected against physical attacks, but also against attacks over the network with the new connectivity in place (Jackson 2015 [11]).

There are many scenarios that would have to be considered that were previously irrelevant because limited connectivity made it impossible to reach the system via the Internet. Given the linkage of the system to other air traffic control systems, the newly-introduced connectivity could compromise their security. Assuming that the system itself cannot be changed, other controls would have to be implemented to protect it against the traffic from the Internet and to mitigate the risk of malicious cyber-attacks.

Another example of a legacy system being connected to the Internet with fewer far-reaching security implications is a government database already available to a limited number of users (Wells 1994 [12]). Now the government wants to make the database available to a larger user base by connecting the system to the Internet. Under the assumption that the system had already been built for an environment that needed to be secured against malicious activity, it is likely that no or minimal changes are required to safely connect this government database to the Internet. The biggest threat in this scenario comes from newly discovered attack vectors that emerge from changes in technology rather than changes in requirements.

Conclusion

The mere fact that a system can be classified as a legacy product does not pose a risk when it is connected to the Internet. It is the system?s original intended use, and the fact security was never considered in its initial requirements, that create the risk. While any set of requirements for computer systems and applications should include security, these requirements differ between closed systems and systems connected to the Internet. Finally, anyone considering connecting legacy systems to the Internet should be able to answer the following questions prior to establishing connectivity:

1. Is there a good reason, for example a business requirement, to connect the legacy system to the Internet? In other words, what are the benefits versus the risks when connecting a legacy system to the Internet?
2. How does Internet connectivity impact the risk profile of the legacy system and its original intended functionality?
3. Can negative impacts such as increased security risks be mitigated when connecting a legacy system to the Internet?

Once these questions have been answered to everyone?s satisfaction and the implications are understood, the decision to connect a legacy system to the Internet may be changed, or the connection made with a clearer

understanding of the implications, including the risks, and the mitigations required to address these risks.

References

German Institute for Standardisation (DIN). 2015. Accessed 1 December 2015 at http://www.din.de/en [13]

Jackson, K. 2015. ?Microsoft Windows 10: Three Security Features to Know About?, Dark Reading, 1 June 2015, Accessed on 1 December 2015 at http://www.darkreading.com/cloud/microsoft-windows-10-three-security-features-to-know-about/d/d-id/1320650 [14]

National Electrical Installation Standards (NEIS). 2015. Accessed 1 December 2015 at http://www.neca-neis.org/ [15]

Standards Australia. 2015. Accessed 1 December 2015 at http://www.standards.org.au [16]

Wells, R. 1994. ?Government Data on Corporations Now Available on Internet: Information: Experimental linkup with the SEC's 'Edgar' database increases public access, but critics say it could impede wider marketing efforts?, LA Times, 19 July 1994, Accessed on 1 December 2015 at http://articles.latimes.com/1994-07-19/business/fi-17364_1_public-access [17]

Whittaker, Z. 2015. ?A 23-year-old Windows 3.1 system failure crashed Paris airport?, ZDNet, 16 November 2015, Accessed online 1 December 2016 at http://www.zdnet.com/article/a-23-year-old-windows-3-1-system-failure-crashed-paris-airport/ [18]

Wikipedia. 2015a. ?Legacy System?, Accessed 1 December 2015 at https://en.wikipedia.org/wiki/Legacy_system [19]

Wikipedia. 2015b. ?Denial-of-service attack?, Accessed on 1 December 2015 at https://en.wikipedia.org/wiki/Denial-of-service_attack [20]

Cite this article as:

Andreas Dannert. 2015. *Shall we hook up the old stuff?*. ajtde, Vol 3, No 4, Article 34. http://doi.org/10.18080/ajtde.v3n4.34 [22]. Published by Telecommunications Association Inc. ABN 34 732 327 053. https://telsoc.org [23]

Legacy systems [24]

Legacy systems [24]

Industry case study [25]

---

[7] https://telsoc.org/journal/ajtde-v3-n4/a34#DIN_2015
[8] https://telsoc.org/journal/ajtde-v3-n4/a34#SA_2015
[9] https://telsoc.org/journal/ajtde-v3-n4/a34#Wikipedia_2015b
[10] https://telsoc.org/journal/ajtde-v3-n4/a34#Whittaker_2015
[11] https://telsoc.org/journal/ajtde-v3-n4/a34#Jackson_2015
[12] https://telsoc.org/journal/ajtde-v3-n4/a34#Wells_1994
[13] http://www.din.de/en
[14] http://www.darkreading.com/cloud/microsoft-windows-10-three-security-features-to-know-about/d/d-id/1320650
[15] http://www.neca-neis.org/
[16] http://www.standards.org.au/
[17] http://articles.latimes.com/1994-07-19/business/fi-17364_1_public-access
[18] http://www.zdnet.com/article/a-23-year-old-windows-3-1-system-failure-crashed-paris-airport/
[19] https://en.wikipedia.org/wiki/Legacy_system
[20] https://en.wikipedia.org/wiki/Denial-of-service_attack
[21] https://telsoc.org/copyright
[22] http://doi.org/10.18080/ajtde.v3n4.34
[23] https://telsoc.org
[24] https://telsoc.org/topics/legacy-systems
[25] https://telsoc.org/topics/industry-case-study