Humans - the weakest and strongest link in securing systems

Scott Cadzow[1], Alexander Cadzow[2]

Abstract: Humans design, operate and are the net beneficiaries of most systems. However humans are fallible and make mistakes. At the same time humans are adaptable and resourceful in both designing systems and correcting them when they go wrong. These characteristics mean that humans can be both the strongest and the weakest link in system security. The aim of this paper is to look at how industrial control systems can use their human actors to build secure systems even noting the fallibility of the underlying machine.

Keywords: Security, Privacy, Standardisation, Human Factors.

1 Introduction

Humans design, operate and are the net beneficiaries of most systems. However humans are fallible and make mistakes. At the same time humans are adaptable and resourceful in both designing systems and correcting them when they go wrong. These characteristics mean that humans can be both the strongest and the weakest link in system security.

The set of Critical Security Controls (CSC) published by the SANS [SANS] Institute (see list below) are proposed as key to understanding the provision of security to systems. Misapplication of the controls by human error, malicious or accidental, will lead to system vulnerabilities. The importance of such controls has been widely recognised and they can be found, either duplicated or adopted and adapted for sector specific spaces, in ETSI, ISO and in a number of industry best practice guides.

- CSC 1: Inventory of Authorized and Unauthorized Devices
- CSC 2: Inventory of Authorized and Unauthorized Software
- CSC 3: Secure Configurations for Hardware and Software on Mobile Device Laptops, Workstations, and Servers
- CSC 4: Continuous Vulnerability Assessment and Remediation
- CSC 5: Controlled Use of Administrative Privileges

[1] Cadzow Communications Consulting Ltd (C3L). 10, CM21 9NP UK, scott@cadzow.com
[2] Bournemouth University and C3L, 10, CM21 9NP UK, alex@cadzow.com

- CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs
- CSC 7: Email and Web Browser Protections
- CSC 8: Malware Defenses
- CSC 9: Limitation and Control of Network Ports, Protocols, and Services
- CSC 10: Data Recovery Capability
- CSC 11: Secure Configurations for Network Devices such as Firewall Routers, and Switches
- CSC 12: Boundary Defense
- CSC 13: Data Protection
- CSC 14: Controlled Access Based on the Need to Know
- CSC 15: Wireless Access Control
- CSC 16: Account Monitoring and Control
- CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps
- CSC 18: Application Software Security
- CSC 19: Incident Response and Management
- CSC 20: Penetration Tests and Red Team Exercises

In recognising that it is the human factor that generally identifies risk and maps out the functionality of a system - its goal in other words - it is clear that this strength can be undermined by fallibility. The question we need to ask is how do we optimise the strengths of the human element and minimise the risk they present to the system?

2 Discovery protocols in Industrial IoT for IACS

When a device is introduced to a system is a factor in the risk it introduces to the system. Specifying components, both software and hardware, during the design and initial deployment is critical in determining the security of the final deployment and the first few moments of runtime.

What needs to be asked of a system that has been designed with attributes of "Secure by default" and "Private by default" and with due attention to give assurance of the security attributes, is "is the system operating as expected?" This is where the capabilities of the controls under CSC-4, CSC-6 and CSC-19 in particular apply. However how does this

work in practice? It is essential to be able to know that what is in the system has a right to be in the system and here is where discovery protocols start to come to the fore. All that a discovery protocol does is allow a device to identify itself and its capability to other devices. This means that a well constructed discovery protocol can build an accurate contextual and system map. Furthermore when a discovery protocol is tied to a means of identifying and reporting system errors or faults the human operator is able to react. A final (perhaps), attribute of a discovery protocol is that misbehaviour, or unexpected behaviour of a discoverable element can be isolated and treated.

Discovery protocols are essential for semi- and fully-autonomous networks and systems. It is not proposed that IACS and I-IoT move towards full autonomy but it is proposed that a secure discovery protocol tied into the concepts underlying the CSCs of knowledge of what a system does and is doing through design, implementation, operation and disposal, will lend a system the ability to give benefit to the users and allow the human element to be supported in managing the system.

3 Summary and Recommendations

On the basis that humans are the net beneficiaries of IACS, and I-IoT, and that they are infallible every effort has to be expended in making it simpler to design systems that are secure by default, and that furthermore give assurance of the security offered. Assurance is needed at design time and the various assurance programs of Common Criteria and similar offer this, but we also need to give assurance of security at runtime (operational assurance) and on shutdown through disposal - lifetime assurance.

Thus the strong recommendation of this paper is to drive industrial technology towards life time assurance that supports the human user to both minimise the vulnerabilities introduced by human fallibility and to maximise the information given to the human user to resolve incidents.

References

[SANS] SANS institute, Critical Security Controls, https://www.sans.org/critical-security-controls/