advenica

ICCP/TASE.2
Secure filter & validation

The risk of attacks against ICCP servers is high and can have severe implications. Protecting the ICCP server mitigates the attacker's possibility to propagate the attack over the network and special solutions are needed to do so.

The Inter-Control Center Communications Protocol (ICCP) as defined in IEC 60870-6 (TASE.2/ICCP) has been specified to provide data exchange between electrical power control centres. Tying together systems for generation, transmission and distribution of electrical power allows real-time and historical data exchange between regional, national and even international utility entities. The coordination needed in current and future energy markets depend on safe and reliable information exchange. These interconnected control centres form a network, that sometimes covers large geographical areas with millions of habitants. A breach that spreads across such networks could therefore affect a large number of people and organisations. The ICCP protocol suite consists of protocols representing a transport layer, a session layer, a presentation layer, and an application layer of the OSI network model. As systems and control centres become interconnected, they also become exposed to network-based attacks. There are today a limited number of implementations of the ICCP protocol suite and therefore vendors of ICCP servers use the same implementation. Hence, a previously unknown vulnerability in any of the ICCP protocol layers could have major effects on the power-grid.

Challenge

Few protocol implementations and unhardened server machines

Different attack scenarios are plausible against ICCP servers, each with a different level of impact:

- Eavesdropping or tampering with process control data.
- Denial-of-service attacks, or remote code execution in the ICCP server application. By exploiting vulnerabilities in the implementation, and consequently disrupting the availability and/or integrity of the server.
- Arbitrary code execution on the ICCP server machine. By exploiting vulnerabilities in the implementation of the ICCP application, or in any other services running in the machine, arbitrary code is executed, privileges are escalated, and consequently the machine is taken over. New attacks can thereafter be launched against either the local SCADA/ICS systems or against other ICCP servers.

Limited number of implementations

Security vulnerabilities have been reported on implementations of ICCP, but given the limited use of ICCP, this has not been getting much attention from security researchers or penetration testers. One can therefore assume that there are flaws yet to be discovered in the implementations.

Significant impact

A zero-day vulnerability would, due to the small number of providers of ICCP stacks, potentially allow the attacker to cause a significant impact on the services provided by ICCP. Also, the attacker would only need to develop one single exploit to carry out the attack.

It would require a fair amount of resources to find a vulnerability, implement an exploit, and carry out the attack. Threat agents in the form of state sponsored agents or well-funded cyber terrorists could however most likely easily mobilise that amount and type of resources and given the severity of the impact – such a scenario should not be disqualified as implausible.

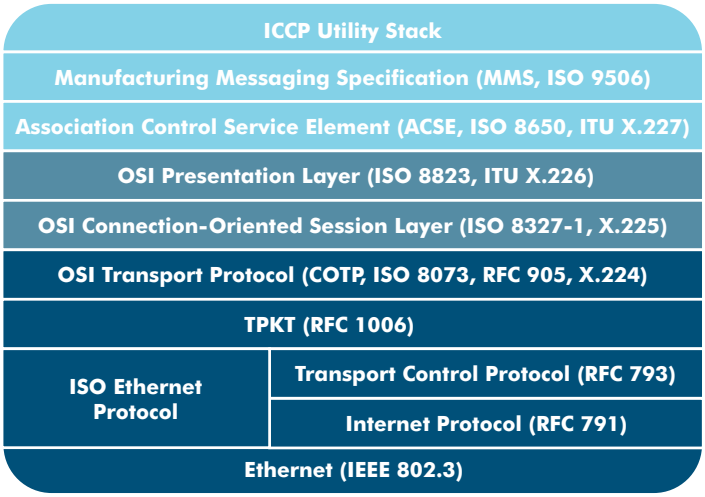

Figure 1. ICCP Utility protocol stack consists of a relatively large number of sparsely used protocol layers.

Lack of proper boundary protection

ICCP is typically exchanged between organisations on dedicated networks (i.e. not over public networks such as the internet). Firewalls should be deployed in the traffic flow, but due to the narrow use and complexity these have limited support for the ICCP protocols and therefore cannot properly inspect or validate the correctness of the traffic and drop or reject malformed ICCP packets. Also, the fact that these networks are "private" increases the risk of not having a proper boundary protection at all between the organisations.

Lack of security functions

The ICCP stack has very few security functions for mitigating different types of threats. Secure ICCP, that is sometimes brought up as the cure, boils down to sending all ICCP traffic through a TLS tunnel. This will prevent anyone from eavesdropping or connecting to the ICCP server before establishing a secure TLS session with the server. However, if anyone would get access to any of the servers the attack could nevertheless be carried out within the encrypted tunnels and still spread uncontrollably over the network. The ICCP stack must, despite having secure ICCP in place, be correctly implemented with respect to security.

Unhardened ICCP server machines

The operating system, services, processes, and applications residing on the ICCP server machine are often vulnerable to attacks. Unpatched and unhardened Windows machines are too commonly used by attackers to gain access to systems, including ICS/SCADA.

Solution

Protect the ICCP server process and machine with Advenica's ZoneGuard

The ICCP server process implementation and the ICCP server machine can be protected using Advenica's ZoneGuard, a stand-alone device developed from the ground up as a security device with a hardened high assurance security platform.

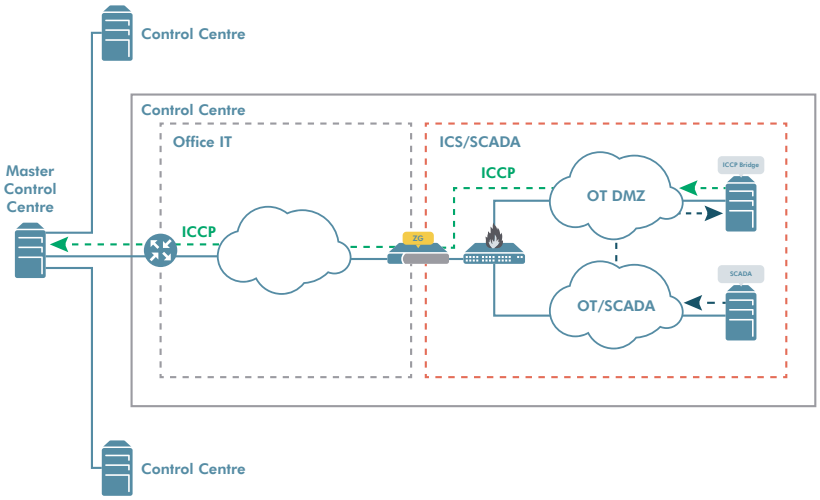

Figure 2. ZoneGuard with the ICCP/TASE.2 protocol validation service validates the ICCP/TASE.2 traffic flow between the local ICCP server/bridge and the control centre.

The ICCP implementation in the ZoneGuard has no relations to any of the commercially available protocol stacks and it is therefore unlikely that a vulnerability in one of the available implementations also exist in ZoneGuard. From a defence-in-depth strategy point of view, we get another level of protection the attacker must penetrate to reach the ICCP server. Protecting the ICCP server mitigates the attacker's possibility to propagate the attack over the network and the ZoneGuard built-in intrusion detection functionality will most likely be triggered before the attack has reached the server. ZoneGuard's hardened ICCP implementation in combination with its internal security architecture makes it very difficult for an attacker to get to the ICCP server without being detected.

Advantages

Defence-in-depth using Advenica's ZoneGuard technology

Protecting the ICCP server using ZoneGuard technology mitigates attacks against vulnerable ICCP protocol stack implementations and ICCP servers. Attacks that could cause catastrophic consequences if spread to the ICS/SCADA environments.

Any solution using unhardened standard ICCP stack implementations expose potential vulnerabilities that could allow an attacker to take over systems and to propagate the attack over the network. Also, policy-based filtering can be applied to the content of ICCP messages, assuring that only valid ICCP data is exchanged between the control centres. This reduces the threat vector, i.e. possible paths or means an attacker can use to gain access to the ICCP server.

advenica

Advenica provides expertise and world-class high assurance cybersecurity solutions for critical data in motion up to Top Secret classification. We enable countries, authorities and companies to raise information security and digitalise responsibly. Founded in 1993, we are EU approved to the highest level of security. Our unique products are designed, developed and manufactured in Sweden.

Read more at advenica.com

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED