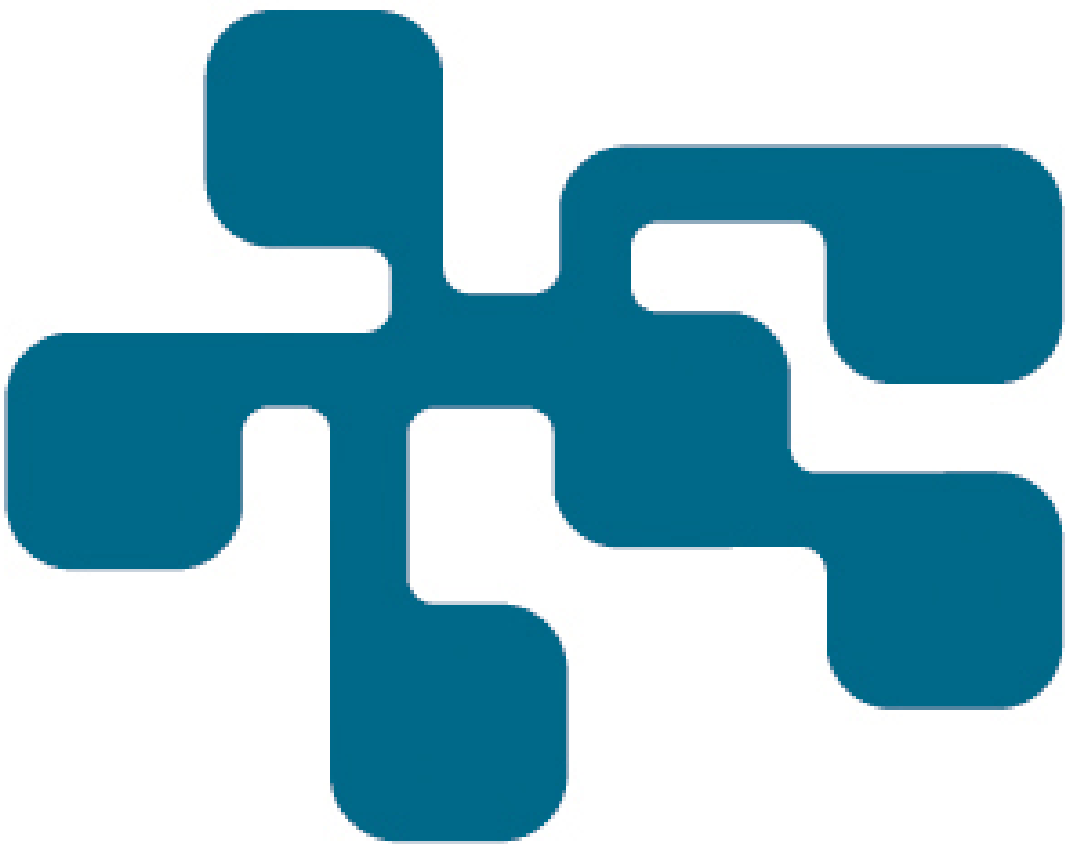
NCS3 - Reactive networks

A possible protection against pivot attacks on ICS equipment

TOMMY GUSTAFSSON, FREDRIK MÖRNESTEDT

FOI
MSB



FOI-R--4051--SE
MSB 2014-1131
ISSN 1650-1942

December 2014

Tommy Gustafsson, Fredrik Mörnestedt

NCS3 – Reactive networks

A possible protection against pivot attacks on ICS equipment

Titel	NCS3 – Reaktiva nätverk
Title	NCS3 – Reactive networks
Rapportnr/Report no	FOI-R--4051--SE
Månad/Month	December
Utgivningsår/Year	2014
Antal sidor/Pages	23
ISSN	1650-1942
Kund/Customer	MSB
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	
Projektnr/Project no	E3239608
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Information and Aeronautical Systems

Sammanfattning

Den här rapporten beskriver hur tekniken för reaktiva nät kan användas för att förbättra skyddet för industriella kontrollsystem (ICS). Reaktiva nät utnyttjar nätverkskomponenter såsom nätverksswitchar för att skapa en isolerad kommunikation mellan en användare och en server. Under tiden som den isolerade vägen är aktiv tillåts ingen annan trafik, exempelvis ut på internet.

Syftet med reaktiva nät är att försvåra för en angripare som sitter utanför aktuellt nätverk att aktivt kunna kontrollera angripna datorer inne på nätverket.

Nyckelord: Säkra system, separation av tjänster, nätverkssäkerhet, ICS.

Summary

This report describes how the technology of reactive networking can be used to improve the protection of industrial control systems (ICS). In reactive networking, network components such as network switches are utilized to create an isolated path from a user to a service or server. As long as the isolated path is active, other traffic, such as Internet access, is blocked.

The purpose with reactive networking is to make it more difficult for an antagonist outside of the network in question to actively control compromised computers on the inside.

Keywords: Secure systems, separation of services, network security, ICS.

Table of contents

1 Introduction

This report describes a concept called reactive networking and how it may be used to prevent pivot attacks against a network with industrial control systems. Reactive networking is a concept developed by the Swedish Defence Research Agency (FOI) in 2012 that makes it possible to change the security posture of a network. This is achieved by restricting access to some network functionality, while allowing other, based on the sensitivity of the information or system that is currently being accessed (Gustafsson, Almroth & Mörnestedt 2012).

In 2012, the concept was developed with the purpose to keep information confidential. The technology worked as projected but information leakage could still occur once normal network access was restored. Therefore, the reactive networking had to be combined with technologies such as Storage capsules (Borders, Weele, Lau & Prakash 2009).

In the end of 2013, a need to protect industrial control systems (ICS) from pivot attacks from the Internet was identified within the National Centre for increased security in industrial control systems (NCS3)[1]. The concept of reactive networking was thought of as a possible solution and therefore it was reinvestigated during 2014. The activities performed in 2014 were:

- Investigate reactive networking as a mean to prevent access rather than keep information confidential.
- Investigate how the implementation of reactive networking could be simplified to facilitate future use and improve resilience.
- To implement reactive networking as a component in CRATE, a Cyber Range and training environment at FOI in Linköping.

In addition to a description of the 2014 version of reactive networking, this report will also give the reader a short introduction into information security in relation to industrial control systems and of the 2012 version of reactive networking.

1.1 Industrial control system

An industrial control system is a general term used to describe computerized systems that control or monitor a physical process such as a production line or a water purification plant. Simplified, an ICS installation consists of local control units, a centralized monitor and control system and storage for historic process data. The local control units are rudimentary and robust mini-computers that convert analogue and digital signals and conduct logical operations. Examples of

[1] In Swedish: *Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet* (NCS3).

local control units are PLCs (Programmable Logic Controllers) or RTUs (Remote Terminal Units). The PLCs and RTUs are often connected to a central monitor and control system such as SCADA (Supervisory Control And Data Acquisition). Typically, there is also some form of storage for processed data. This is basically a database, also called a Historian, which stores relevant historic data from the operation. The historic data is often exported to IT-systems such as business systems or financial systems.

ICS is a technology that encourages system interconnection since it makes it possible to tightly control and/or monitor several processes from a distance, ensuring cost-effective operations. Once the ICS is interconnected, another gain is the ability to get remote support which increases system availability and decreases costs even further. Interconnection also makes it possible to export production data and import production instructions on a near real-time basis.

Historically, the interconnections were mainly in-house on physically separated networks but today many ICS networks are operated in an Internet-connected environment, either directly or via a connected network. There are many examples of ICS equipment that are directly accessible from the Internet (Radvanovsky 2013).

The problem with these interconnections is that the ICS equipment often has rudimentary cybersecurity mechanisms due to design and poor implementation. One issue is that historically, security was not a concern when the ICS component was developed and, as a consequence, the technologies used are often insecure by design. Also, the few security mechanisms that were available were seldom utilized. For instance, using default passwords are common practice in ICS installations as it makes maintenance easier when several technicians are involved. Another design issue is the incorporation of COTS-based[2] IT-components, such as operating systems, web servers or Java engines. These IT-components are often designed for a relatively short life span of 3–5 years, during which they may also be updated or upgraded several times.

The issues mentioned above become a problem due to the operational life span of a typical ICS installation which is measured in decades rather than years. There is probably ICS equipment that was designed in the pre–Internet world still operational. The long life span of ICS installations also means that it will take a very long time before security mechanisms developed and implemented today will provide full protection for a system.

Poor security mechanisms combined with operating ICS equipment in Internet-near networks makes the ICS equipment exposed to both intentional and unintentional IT-based attacks and incidents.

[2] COTS – Commercial off the shelf – products that are sold or licensed on the open market.

Due to the financial and operational gains with interconnected ICS equipment, the obvious solution to fall back on isolated systems is not feasible. Therefore, new cybersecurity solutions that utilize currently available technology are highly desirable.

1.2 The pivot attack

A pivot attack is an attack vector where another computer system than the targeted system is used as a stepping stone to gain access to the target system. The point of pivot may be a computer with an internet connection, as depicted in Figure 1, or it may be a vulnerable system connected on the same network segment as the targeted system.

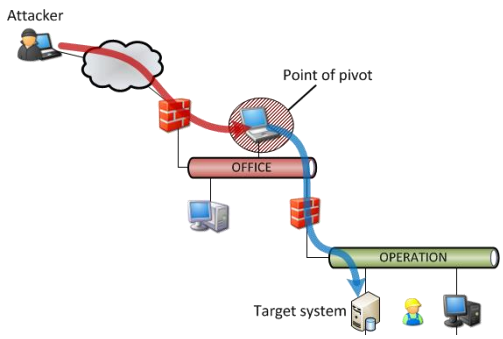


Figure 1: In the pivot attack, the attacker utilizes a computer system as a stepping stone to reach further into an attacked network.

The pivot attack vector utilizes the combination of two frequently used system designs:

1. That some computer systems (such as web servers) have services that are exposed to less protected networks than the targeted system.
2. That the exposed systems have greater access to the targeted system than the attacker does from the less protected network.

In the example with the ICS environment in Figure 1, the point of pivot may for instance be the Historian or the computer of the process engineer used to connect to the ICS equipment via a terminal server.

1.3 Reactive networking 2012

In 2012, FOI successfully demonstrated the concept of reactive networking for increased security. The basic idea was to use security features currently available in most modern networking equipment to dynamically create a

temporary logical network segment, as pictured in Figure 2. Once implemented, the security policy prevented the user from having simultaneous connections to the protected systems and the Internet.

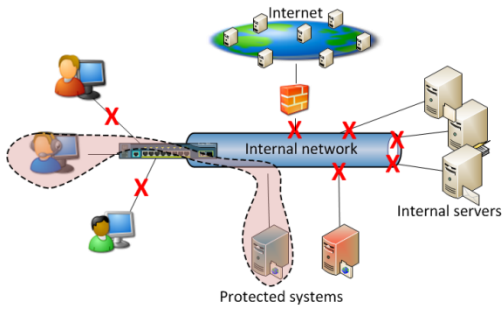


Figure 2: The basic principal of reactive networking is to use commonly available switch technologies to temporarily change the security posture of the network.

The first version of reactive networking utilized 802.1X (Institute of Electrical and Electronics Engineers (IEEE) 2013) and the RADIUS protocol, to identify where a user connected to the network. Once triggered, a control server utilized SSH, a wide-spread method to control everyday switch configuration, to reconfigure the switch. FOI developed the control server in-house and used a web application to trigger the change in the network security posture. The first version of reactive networking operated as depicted in Figure 3 and the steps are further described below.

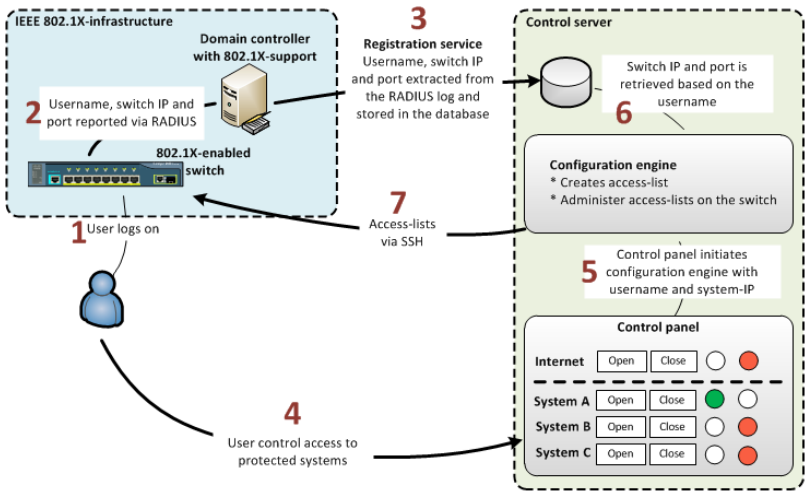


Figure 3: The operation of the first generation reactive networking. The numbers indicate each action in the operation, further described below.

1. The user connects to an 802.1X-enabled port on a switch and logs on the domain.
2. A RADIUS server verifies the logon at the network level.
3. A registration service (developed by FOI) extracts the user's username, the switch IP address and switch port from the RADIUS log file and stores it in a database for future use. This action is performed pre-emptively to shorten system delay.
4. When a user wants access to a protected system, a web-based control panel is used to manually trigger the change of network security posture.
5. The control panel initiates a configuration engine with the user's username and the IP address of the protected system.
6. The configuration engine extracts the switch IP address and the switch port of the user from the database and creates an access list that explicitly allows the access to the protected systems.
7. The configuration engine utilizes SSH to apply the access list to the switch port of the user.

Once the user has finished the interaction with the protected system, actions 4 through 7 are repeated in order to restore the security posture the system had before the access.

1.4 Delimitations and assumptions

This report investigates the concept of using reactive networking in an ICS environment. The following aspects have been delimited or assumed in the scope of the report:

- Implementing reactive network technology on an ICS environment is no silver bullet that handles every type of plausible attack vector against the systems. For instance, it will not prevent an attack that can be performed in offline mode. It can however be assumed that concepts such as reactive networking would make an attack harder to succeed.
- Investigation is required on how large a threat the pivot attack constitutes for an operational internet-near ICS network. Based on general knowledge of cyber security and of ICS installations it can be assumed that the pivot attack is a plausible way to attack critical installations.
- The methods of writing powerful access control lists to protect ICS equipment connected to an IT environment are not covered here. The focus of reactive networking is to change the security posture of the

network in a live context and the specific access lists will have to be designed with a case-by-case approach.

- The possibility to use ARP or IP spoofing to circumvent the security policy of the network is a risk not discussed here. There are technologies that can handle such attacks and these can be implemented as described by each hardware manufacturer.
- The second version of reactive networking does not identify the user in the same manner as the first version did. If authentication is sought, there are technologies already available on the market that can be used.
- Private virtual LANs (VLANs) are a security feature available on some switches that may be utilized to achieve a similar effect on security in a network infrastructure. This is however not included since it is not as commonly available as the technologies utilized in reactive networking.

1.5 About NCS3

The National Centre for increased security in industrial control systems (NCS3) is a centre of excellence focused at building and disseminating awareness, knowledge and experience about cyber security aspects on ICS. The Centre is a cooperation between the Swedish Defence Research Agency (FOI) and the Swedish Civil Contingencies Agency (MSB). The activities of the centre are aimed at actors that own and/or operate critical infrastructure where ICS are a part.

2 Reactive networking 2.0

As described in the introduction, there has been a previous reactive networking design (Gustafsson et al. 2012), hereafter referred to as RN_v1. Besides the shift in security focus, a couple of design enhancements were identified before beginning work on the second version, RN_v2. These were:

- To simplify the process of identifying where the user connects to the network to eliminate the need of 802.1X.
- RN_v1 only used one-directional security policies. RN_v2 is designed to implement bi-directional security policies.

The design changes between RN_v1 and RN_v2 are further described below in section 2.1 System design.

2.1 System design

Reactive networking is designed to protect valuable assets on the network, using basic switch functionality that is already present in many networks. The basic design and operation of RN_v2 can be viewed in Figure 4.

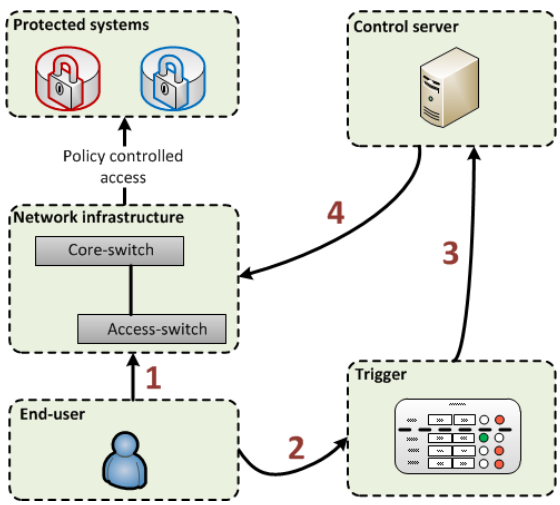


Figure 4: The basic design and operation of RN_v2. Each component is explained further in the text.

During normal operations a security policy in the core switch prevents access to the protected systems via the network. The end-user connects to a port on the

access switch in (1). To gain access to the protected systems, there has to be some kind of trigger action invoked by the end-user (2). In (3), the trigger instructs the control server to change the security posture in (4).

2.2 Testbed

In order to develop and verify the functionality of RN_v2, a testbed was created. The configuration of the testbed can be viewed in Figure 5. The network infrastructure of the testbed was set up using two Cisco switches, one C3560G as core switch (1) and one C2960G as access switch (2). The switches were configured with four VLANs and the core switch acted as router. There were no other configurations applied to the switches.

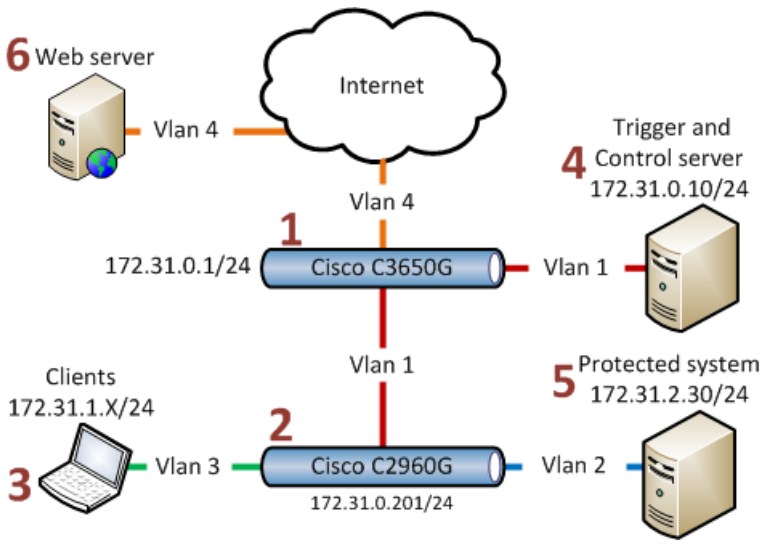


Figure 5: The testbed used to develop and verify RN_v2 consisted of two switches and a series of virtualized computer systems.

The VLANs were then distributed as outlined in Figure 5. The clients and servers of the testbed were virtualized using Oracle VirtualBox. There were two end-user clients (3) installed with a standard Windows 7 operating system. Besides setting a static IP, there were no changes made to the network configuration on the clients. In the testbed, the web server of the triggering system and the application of the control server resided on a single Windows 2008 server in (4). Functionality-wise though, the two services in (4) communicated as if they were on different servers, so this would have no principal effect on how the testbed worked. To complete the testbed, web servers were added to simulate a protected system in (5) and to simulate the Internet in (6).

2.3 Operations

Due to the elimination of 802.1X to identify the user and to the incorporation of bi-directional security policies, RN_v2 operates a bit differently than RN_v1. The operations can be viewed in Figure 6 and are further described in the text.

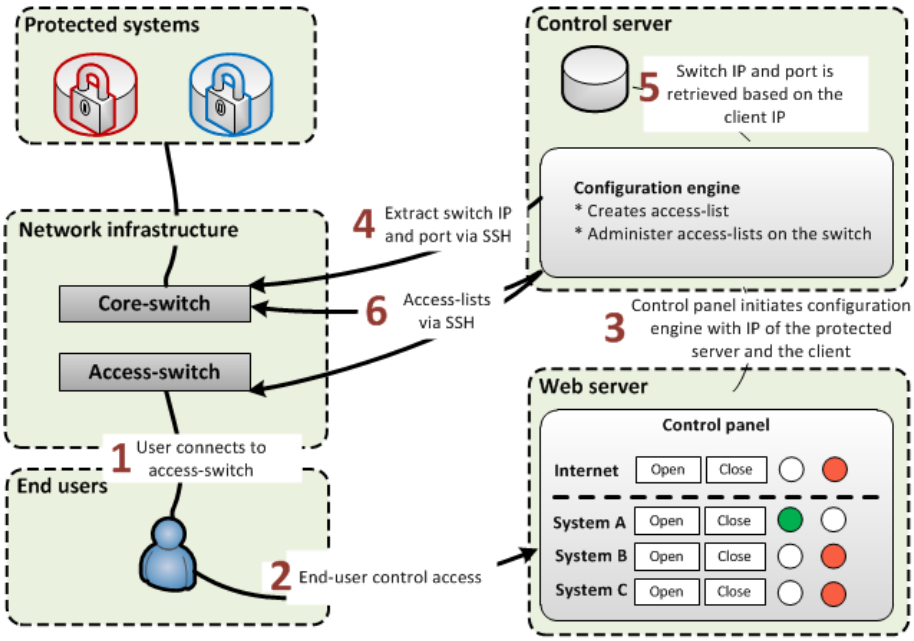


Figure 6: Operations of RN_v2. One major difference between RN_v1 and RN_v2 is that RN_v2 has no need to operate until the user actually requests access to a protected system.

The operations of RN_v2 include the following steps:

1. The user connects to a switch port and logs on to the domain. This actually does not trigger any action from the reactive networking.
2. The end-user uses the control panel to manually trigger a change in network security posture.
3. The control panel application initiates the requested change by sending a request to the control server.
4. The configuration engine extracts the end-user access switch IP address and physical connection port.
5. The control server creates access lists.

6. The control server connects to the core switch and the end-user's access switch and configures the access lists. It then returns the status to the control panel.

Once the user has finished the interaction with the protected system, actions 2 through 6 are repeated and normal restricted network access is restored. Each step is further described in the chapters below.

2.3.1 Identify where the user connects (1)

During the design of RN_v1, the first approach was to use RADIUS to apply the access lists to the switch port and thereby 802.1X was chosen to identify where the user connected. However, RADIUS-controlled access lists proved too slow and could not be used to guarantee the security. As a result, SSH was instead utilized to control the access lists but 802.1X was kept to identify where the user connected.

The problem with keeping 802.1X was that it results in a quite complicated setup requiring both a RADIUS server, configuration on the switch and changes on each client. This would make it more expensive and time-consuming to implement reactive networking and an easier solution was sought. Also, the only way to identify the connection point of the user without causing delay is to do it when the user initially logs in and to then store this information, making RN_v1 less resilient.

The solution was to initiate an interaction with the routing switch in the network architecture and to run a command that would trace the connection point of the end-user's client (4). The routing switch would then reply with the IP address of the access switch and the connection port of the end-user.

2.3.2 Triggering change in the security posture (2 & 3)

In reactive networking, it is basically the end-user that initiates the reconfiguration of the security posture of the network. It is however important to remember two basic design features:

1. Before an end-user can gain access to the protected systems, a security policy that allows the access must at first be configured into the system. Otherwise the end-user has no way to change the security posture.
2. The end-user never interacts directly with the control server or the network infrastructure, ensuring the integrity of the reactive network.

The change in the security posture is triggered by an event initiated by the end-user. In RN_v2, this is done via a web application where the end-user simply presses a button to trigger the change. The web application then sends a request

containing the IP addresses of the end-user client and of the protected system to the control server.

A web application is however only an example of how to trigger a change in security posture. In an ICS environment a terminal server is often used as a gateway between two network segments and it is plausible that the trigger function can be executed as part of the connection process with the terminal server. This would create a reactive network that would be automatic and completely transparent to the end-user.

2.3.3 Configuration engine (5)

The configuration engine resides on the control server and is the component that changes the security posture in the network. It has been developed by FOI. In RN_v2, the following actions are taken when a user triggers an access request:

a) The user opens the web application used as a trigger in RN_v2 and requests access to a protected system.

b) The web application extracts the client IP address and sends it along with the IP address of the protected system to the configuration engine.

c) The configuration engine connects to the core switch and uses the ARP table to get the client MAC address, and then uses this to run a MAC-traceroute command. This operation will return the IP address of the access switch along with switch port where the end-user client is connected. This information is stored on the configuration server.

d) The configuration engine uses the retrieved information to create an access list to be placed on the core switch and on the access switch.

e) The configuration engine uses SSH to apply the access lists in accordance with the request.

f) As a final step, the configuration engine reports back to the web application which in turn changes the connection status indicator in the control panel.

When the user has finished working with the protected system, the normal security posture will be restored in much the same manner. The only difference is that the configuration engine utilizes the position data stored earlier.

2.3.4 Switch interaction (4 & 6)

A central functionality in reactive networking is to interact with, and reconfigure the switches in the network. This is achieved by utilizing SSH between the switches and the control server (4 & 6). SSH is a wide-spread method to handle

every-day switch configuration and having the control server using SSH should not introduce any new vulnerabilities.

2.3.5 Bi-directional security policies

RN_v1 used a port-based access list on the user's switch port to set the security posture of the network. One problem with this configuration is that switches from several major suppliers, for instance Cisco and HP, only filter traffic entering the port and not on the exit, something which was a potential vulnerability. Also, RN_v1 never dynamically handled the security policy that would protect the protected systems.

One of the first actions carried out when designing RN_v2 was to investigate how to use the access list features of the switches to create a bi-directional security policy. It turned out that it was no easy task to configure a bi-directional access list close enough to the end-user client (1). One alternative was to place a port-based access list on the uplink port to prevent access to the client, but this would not stop access from computers on the same VLAN and switch. Another alternative was to place the clients that needed access to protected systems on separate VLANs and to configure the VLAN-based access lists on the core switch.

In RN_v2, the port-based access list was kept to reduce complexity. This leaves a small vulnerability but an attacker would have to perform the attack offline, since there would be no traffic received from the targeted system.

To handle the security of protected systems, there was also a need of an additional security policy that was not implemented in RN_v1. After some consideration, it was decided to place the protected system on a separate VLAN and to apply an access list to the VLAN in the core switch. Thus, RN_v2 changes the security policy by two separate access lists in two separate switches.

2.4 Development

The development of RN_v2 was carried out in three steps. First, the basic functionality was established where 802.1X was removed as a design component. In this step the security policy in the network infrastructure utilized static access lists. Second, the access lists where made dynamic but it was still a single-client system. The third step was to implement the support for simultaneous access by several independent clients and protected systems.

During the second and the third development phases it turned out that it was possible to solve both the dynamic functionality and the multi-user system all at once. This was achieved by dynamically creating a generic access list on the

access switch, and by adding or deleting entries in the access list on the core switch.

2.5 Verifying functionality

Reactive networking relies on well-known and basic technologies such as SSH and switch-based access lists. These technologies have been used publicly for a long time and can be regarded as reliable. Therefore, verification of functionality has been performed through monitoring the switch configurations, and tests of access to the protected system have been performed in the testbed. The concept has been tested with simultaneous multi-user access by utilizing the two clients in the testbed. RN_v2 has performed as expected and the changes in security posture of the network infrastructure can be triggered by the end-user.

The next (and important) step in the verification process is to verify whether or not reactive networking can work as a security mechanism preventing pivot attacks in real-world ICS environments. However, as this cannot be done at an operational site, the testbed will be fully integrated into the Cyber Range and Training Environment (CRATE). This will make it possible to test the concept in realistic antagonistic scenarios against highly competent personnel.

3 Discussion

With reactive network, FOI has investigated a way of combining basic technologies already available in many switches to mitigate internet-based pivot attack as a potential threat against ICS environments. The concept has proved to be rather simple to develop and implement in a testbed environment. The core component in RN_v2, the configuration engine placed on the control server, constitutes of about 250 lines of source code.

3.1 Secure by design

RN_v2 is secure by design since the only component that needs to be accessible to the end user is the trigger mechanism. The control server is the only component allowed to interact with the network infrastructure, thus there is no interaction between the end-user and the control server. In the event that the trigger or the control server becomes unreachable the only effect on the system would be that the end-user cannot gain access to the protected systems.

3.2 Usability

Several network vendors, such as Cisco and HP, offer different solutions to dynamically changing the security posture of a network. However, these solutions are user-oriented rather than system-oriented, meaning that the access policies are configured for each user or user-group. This makes the configuration process very time consuming. These solutions also generally use RADIUS to apply the security policies, a technology that Gustafsson et al. (2012) proved to be less reliable due to the delays introduced.

With reactive networking, the only policy that needs to be configured is the access policy of the protected system. In RN_v2, this can simply be done by adding a button to the web application since the configuration engine creates the access lists. This would make it less time consuming to configure than traditional solutions using dynamic access lists.

Another usability aspect is that reactive networking can be completely transparent to the end-user if the trigger is a part of the connection process, for instance when connecting to a terminal server.

3.3 Flexibility

RN_v2 is developed on a Cisco testbed and of course implement Cisco commands. But by using SSH to configure the switches, it would be entirely possible to adjust the concept to run on networks containing switches from other

vendors. It would also be possible to develop the SSH engine to function in a heterogeneous network environment by extracting the switch vendor and product name along with the access switch IP address.

In the testbed, the security policy only handles access to the protected system. But this is only limited by the access lists in the switches and could easily be adjusted to suit other security policies.

3.4 Mitigating the pivot attack

So, the main question – would reactive networking mitigate a pivot attack? Yes, it would prevent simultaneous access and thereby mitigate the internet-based pivot attack. However, as assumed in the beginning, reactive networking is no silver bullet and there are still ways to attack the protected systems. But it would require a more advanced attacker since it requires more sophisticated attack vectors.

References

Borders, K., Weele, E.V., Lau, B. & Prakash, A. (2009). Protecting Confidential Data on Personal Computers with Storage Capsules. In *SSYM'09, Proceedings of the 18th conference on USENIX security symposium*. Montreal, Canada 10-14 August 2009, pp. 367-382.

Gustafsson, T., Almroth, J. & Mörnestedt, F. (2012). *Reaktiva nät* (FOI-R--3560--SE). Linköping: Totalförsvarets forskningsinstitut.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (2013). *Alert (ICS-ALERT-12-046-01A) Increasing Threat to Industrial Control Systems (Update A)*. 8 May. https://ics-cert.us-cert.gov/alerts/ICS-ALERT-12-046-01A [2014-12-15]

Institute of Electrical and Electronics Engineers (IEEE) (2013). *Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Part 1X: Port-based network access* (ISO/IEC/IEEE 8802-1X:2013). IEEE: New York, USA.

Radvanovsky, B. (2013). Project SHINE: 1,000,000 Internet-Connected SCADA and ICS Systems and Counting. *Tofino Security*, 19 September. https://www.tofinosecurity.com/blog/project-shine-1000000-internet-connected-scada-and-ics-systems-and-counting [2014-12-15]

Security in Industrial Control Systems

Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) är ett kompetenscentrum med uppdraget att bygga upp och sprida medvetenhet, kunskap och erfarenhet om cybersäkerhetsasspekter inom industriella informations- och styrsystem. Centrumets är ett samarbete mellan de svenska myndigheterna FOI och MSB och dess verksamhet fokuserar på aktörer som äger och/eller driver samhällsviktig verksamhet där industriella informations- och styrsystem ingår.

The National Centre for increased security in industrial control systems is a centre of excellence focused at building and disseminating awareness, knowledge and experience about cyber security aspects in ICS. The Centre is a cooperation between the Swedish Defence Research Agency and the Swedish Civil Contingencies Agency and the activities is focused on actors that owns and/or operates critical infrastructure where ICS are a part.

FOI
Swedish Defence Research Agency
SE-164 90 Stockholm

Phone +46 8 555 030 00
Fax +46 8 555 031 00

www.foi.se

Swedish Civil Contingencies Agency
SE-651 81 Karlstad

Phone: +46 (0) 771-240 240
Fax: +46 (0) 10-240 56 00

www.msb.se