Trend Micro Incorporated
Research Paper
2013

SCADA in the Cloud

A Security Conundrum?

By: Kyle Wilhoit

Contents

Introduction

Two of the hottest buzzwords circulating in the IT world today are "SCADA" and "cloud computing." Combining the two technologies has been discussed and is starting to gather more attention in connection with cost savings, system redundancy, and uptime benefits. The question then is: "Are the savings substantial enough to offset the security concerns that users may have if they migrate integral SCADA devices to the cloud?"

Why Migrate SCADA Devices to the Cloud?

The cloud has many uses for information technology (IT). In fact, companies like Apple and Google already offer integrated, robust cloud services, showing that cloud use is not just a passing fad.[1] Some of the typical reasons for cloud use include saving on costs, enjoying the benefits of embedded security, ensuring uptime, and guaranteeing system redundancy.

SCADA devices do not differ from critical systems in that these also require redundancy, security, reduced costs, and uptime. Migrating SCADA devices to the cloud can solve critical issues related to uptime and redundancy in industrial control systems (ICS) environments.

ICS environments have notoriously high uptime requirements, which cloud use can help resolve. In addition to the benefits cited above, cloud computing for SCADA devices permits access from any Internet-connected location, allowing easy access to data. Along with scalability, SCADA devices allow new services and servers to be spun up in a matter of minutes. Migrating critical devices and/or services to the cloud can help establish baselines for redundancy and uptime while lowering costs.

Redundancy and Flexibility Benefits

Over 65% of the respondents to a recent InformationWeek analytics study said the ability to rapidly meet business needs was very important.[2] Cloud use can help with the increased need for speed in access to information even for ICS and SCADA devices. The ability to quickly put infrastructure up makes redundancy an easy-to-fix problem with cloud utilization. In addition, the flexibility afforded by this method allows quicker device upgrades should these have low hard drive space or CPU cycle overuse.

1 http://www.apple.com/icloud/; https://cloud.google.com/
2 http://www.informationweek.com/cloud-computing/software/time-to-think-about-cloud-computing/211300562

Disaster Recovery and Automated Updates

According to an Aberdeen Group study, cloud service providers handled many of the issues surrounding disaster recovery (DR) efforts. Businesses that used the cloud were, for instance, able to resolve issues in 2.1 hours on average. But those that did not use the cloud did the same on an average of 8 hours.[3] This is likely attributed to troubleshooting possible issues related to hardware.

In addition to improving DR efforts, automated updates can be directly attributed to cloud use as well. Most cloud service providers are responsible for server maintenance, including security update rollouts. Cloud utilization frees up time and resources that IT administrators can use for other projects.

What Does Cloud Use for SCADA Devices Mean?

The cloud can be used for SCADA devices in many ways. But, for the purposes of this paper, only two will be discussed here.

The first option involves directly connecting SCADA applications to a control network with upstream processing occurring in the cloud. The second option allows SCADA applications to be entirely hosted in the cloud and pass instructions back to the control device inside a corporate network.

Application Partially Hosted in the Cloud

Cloud-based SCADA applications are most commonly deployed on-site. As such, the applications in this scenario are directly connected to the control network and data is pushed to the cloud for analytics and access purposes. This setup allows the "heavy lifting" for data analytics to be done using the infrastructure as a service (IaaS) model.[4]

3 http://research.aberdeen.com/1/ebooks/Proven-Benefits-of-Backing-Up-Data-to-the-Cloud.pdf
4 http://en.wikipedia.org/wiki/Cloud_computing

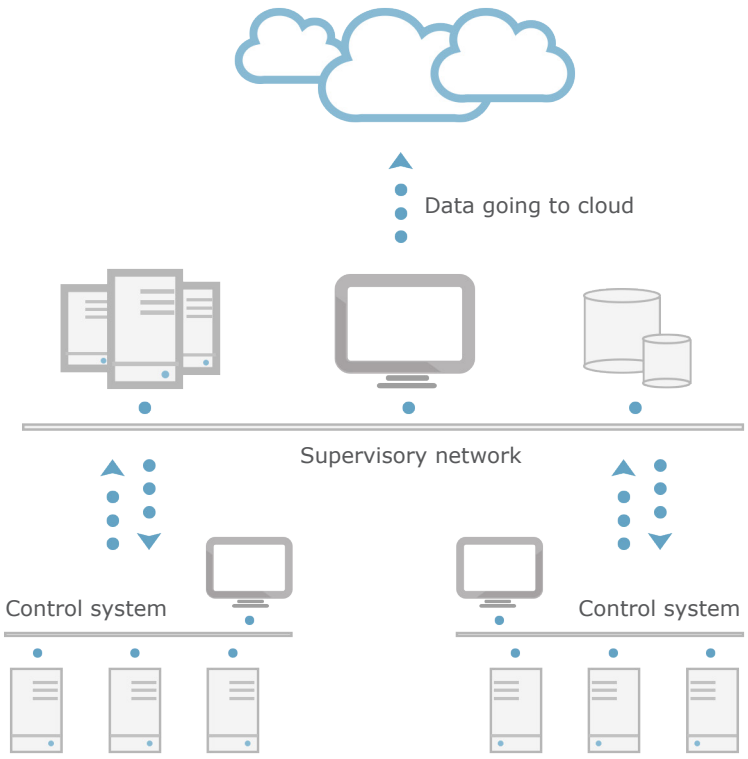

FIGURE 1: Sample internally hosted SCADA application where data is externally pushed

Entirely Cloud-Based SCADA Application

SCADA application architectures can also be entirely run in the cloud with remote connectivity to a control network. This architecture allows data to reside either on-site or in the cloud, depending on login requirements. Command-and-control (C&C) messages are downloaded to controllers then processed.

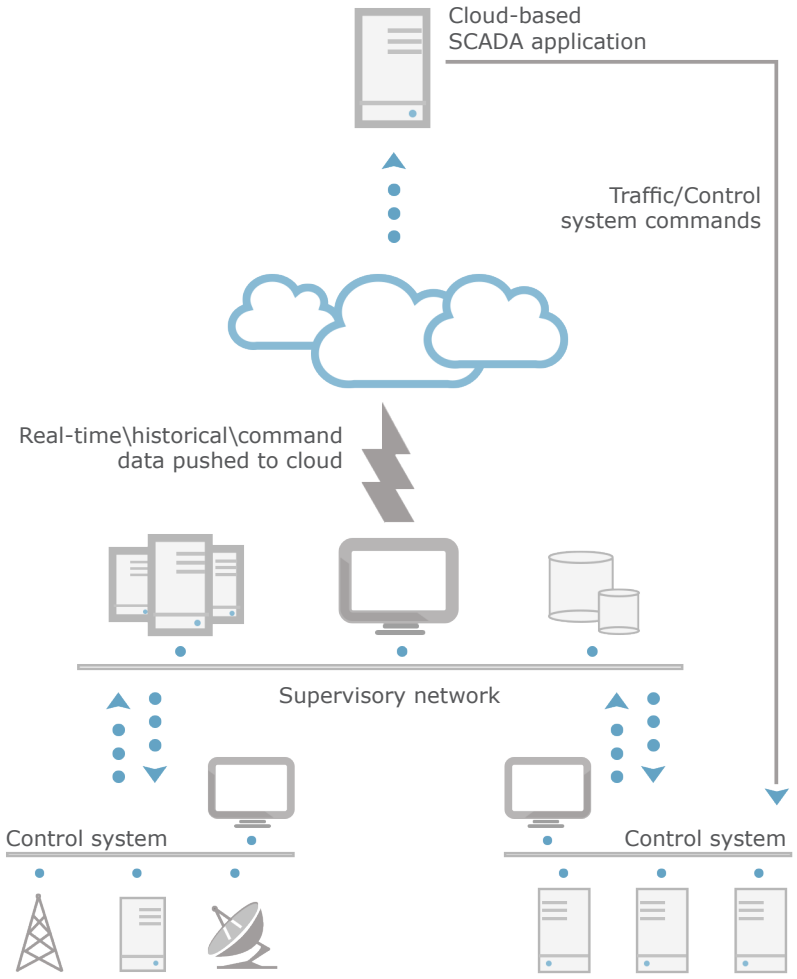

FIGURE 2: Sample SCADA application entirely hosted in the cloud

Differences Between the Two Types of SCADA in the Cloud Architectures

Significant differences exist between the aforementioned cloud architecture types. In the first example, the SCADA application is hosted on the client's hardware, typically on the control network. Data is then offloaded to the cloud for processing and storage. This allows data processing and retrieval to be performed in the cloud. The significant risk to this type of architecture is that confidential ICS and/or SCADA data is hosted and stored in the cloud.

The second example is an application that is entirely hosted in the cloud. The application generates C&C traffic and pushes it downstream to the controllers at the client's site. This architecture poses two significant security risks, namely:

- The real-time data and/or commands that travel from ICS or SCADA devices to the cloud, depending on an attacker's skill, can be sniffed, spoofed, denied, or modified in a litany of fashions.
- On the opposite end, pushing commands from a cloud-based application to the internal ICS or SCADA environment introduces internal connectivity that bypasses security devices like firewalls. This required connectivity opens a door to a secure internal network that is typically not allowed because it can let an attacker gain a foothold in that network.

Security Risks

The idea of migrating critical business functions to the cloud makes tremendous sense and is typically very secure. However, users of such services should consider several security concerns related to the nature of data, web application attacks, control, authentication, encryption, and logging.

Nature of Data

While virtually every cloud service provider touts the data stored on its servers is not publicly accessible, note that the data is still housed on a shared server with that of hundreds or possibly even thousands of other clients. As such, this data can either be intentionally or unintentionally shared with others. Breaches like the one Citigroup suffered in 2011, which involved the compromise of cloud-held data, should be taken into consideration when thinking of migrating SCADA devices to the cloud.[5]

The best question to ask when storing data in the cloud is: "Is it okay for the stored information to be shared with the public?"

Web Application Attacks

Web application attacks still lead the pack in terms of threats to cloud infrastructures.[6] SCADA devices are not immune to this attack vector either.

Web application attacks can target SCADA applications hosted in the cloud. This threat is, of course, also present when utilizing a local data center although an organization's footprint is increased when using a well-known cloud service provider. These attacks can be considered attacks of happenstance. This means an attacker scanning a known cloud service provider's IP space has a chance to find your SCADA application and begin attacking it. The attacker's familiarity with SCADA protocols and devices may be very limited but your attack footprint inherently increased because you used a well-known cloud service provider.

The best questions to ask yourself in this instance are: "Am I okay if my applications attract attacks of happenstance because of my increased presence? Is there anything I can do to reduce my exposure?"

Lack of Control

Migrating data to the cloud takes the ownership away from an organization and puts it in the hands of the cloud service provider. If the cloud service provider that hosts the data for the SCADA device, for instance, decides to integrate new connections to the back end of its infrastructure, which is connected to the SCADA application server, this can introduce connections the data owner is unaware of, creating risks that are unknown to the customer as well. A recent Bloomberg article illustrates just how private data can end up in the public eye.[7]

5 http://www.infoworld.com/d/security/citigroup-breach-exposed-data-210000-customers-664; http://blog.trendmicro.com/trendlabs-security-intelligence/no-excuses-when-it-comes-to-data-security/

6 http://www.alertlogic.com/resources/cloud-security-report/

7 http://www.bloomberg.com/news/2013-03-26/how-private-data-became-public-on-amazon-s-cloud.html

Ask this question when considering lack of control: "Is it okay to trust the cloud service provider who can introduce back-end infrastructure updates and third-party connections to the servers I purchase and has all of my data?"

Lack of Authentication

The two most common SCADA protocols—Modbus and DNP3—have fundamental flaws with regard to supporting authentication. Many SCADA protocols do not support or perform authentication.[8] As such, no "trust" checking between two parties interacting via DNP3 or Modbus occurs. A version of DNP3 called "Secure DNP3," however, allows for authentication though this is not supported on older control systems and remains limited in terms of use.

If part of a cloud-based SCADA architecture uses the said protocols, especially one that is hosted on a public cloud, an attacker can easily spoof not only IP addresses but also user names and traffic to get access to data they do not otherwise have.

The best question to ask yourself when thinking of this security problem is: "What risks would I face if an attacker gains access to my unauthenticated data?"

Lack of Encryption

Similar to the lack of authentication that SCADA protocols are inherently plagued with, many do not allow any form of encryption to protect information as well. Modbus and DNP3, in particular, do not inherently support any type of encryption, opening traffic to man-in-the-middle (MiTM) attacks and traffic sniffing.[9] These threats allow attackers to not only see data in transit but also redirect traffic to any field device with the desired changes in place.

When using cloud-based services for SCADA environments and the said protocols, regard the protocols' inherent lack of encryption support a major security flaw. It should be one additional concern when migrating SCADA devices to the cloud.

When considering this particular security issue, ask yourself: "Would it be okay if attackers saw my sensitive control system data?"

The Logging Conundrum

As with any service solution, logging is often a challenge. While performing localized logging is relatively easy to do, getting logs back across a wide area network (WAN) connection is somewhat more difficult to do and often unreliable for a centralized security information and event management (SIEM) solution.[10] In addition, having these logs go back to your corporate infrastructure requires firewall rules in place to allow this connectivity. This opens communication from an outside party to a secure trusted network, therefore increasing security risks.

Transmitting logs back to an internal logging infrastructure is often done in plaintext, which can easily be obtained via various MiTM techniques.

The question to ask yourself is: "If I lose access to my ICS and/or SCADA system logs, would that pose security risks?"

8 http://www.ida.liu.se/labs/rtslab/iisw04/camready/SCADA-Attack-Trees-Final.pdf
9 http://en.wikipedia.org/wiki/Man-in-the-middle_attack
10 http://en.wikipedia.org/wiki/Security_information_and_event_management

What Can You Do?

While using SCADA in the cloud this time poses security risks, your organization can do some things to harness the power of the cloud while keeping data safe. Note though that the following list is not inclusive of all solutions:

- **Use Internet Protocol Security (IPsec).** When available, utilize the advantages IPSec provides. IPsec supports both authentication and encryption, which can help ensure that attackers have a more difficult time sniffing, modifying, or spoofing traffic in cloud-based SCADA deployments.
- **Use secure protocols.** Using secure protocols, if available, will help offset some of concerns with regard to authentication and encryption. Using more secure protocols like Secure DNP3 will help.[11]
- **Encrypt data at rest.** While encrypting data at rest in an ICS or SCADA environment is not always applicable, doing so in a cloud environment has tangible benefits. If attackers, for instance, compromise data stored in a cloud service provider's server, it will be hard for them to unencrypt and read the information. Using encryption, if possible, is always advised in cases where data is stored off-site.
- **Enable thorough logging.** If possible, push all logs to a centralized logging solution. Build up redundancy in the logging solution. In addition, send as many logs to the SIEM as possible. Sending system, security, network, and application logs from Windows® workstations are, for instance, a good start.
- **Sign robust agreements.** Sign robust agreements with your cloud service provider to make sure erroneous third-party connections are not allowed on your servers. This may increase the premium for your cloud service but will help enhance your security profile in addition to giving you peace of mind.
- **Use virtual private networks (VPNs) or Secure Sockets Layer (SSL).** When available, use site-to-site VPNs, SSL VPNs, or SSL traffic. These ensure that communication is always done in a secure fashion from the source to the destination, which prevents sniffing and/or spoofing.
- **Use security solutions if available.** If security solutions are available, make sure to choose one that:
  - Prevents programs not specifically on an approved application list from running
  - Is easy to install and can be updated without stopping its components from running
  - Has a small footprint compared with other endpoint security solutions that rely on large pattern files, which require constant updating
  - Uses role-based administration that provides full control during installation and setup and allows simplified monitoring and maintenance after deployment
  - Has graphical and command line interfaces for ease of use and convenience

11 http://www.digitalbond.com/scadapedia/protocols/secure-dnp3/

- Is compatible with other security solutions used to ensure straightforward removal of threats that do make it onto the device

Conclusion

Like most IT companies, ICS and/or SCADA controllers can benefit from cloud use. SCADA devices do not differ from critical systems in that these also require redundancy, security, reduced costs, and uptime. That said, migrating SCADA devices to the cloud can solve issues with regard to uptime in ICS environments.

While cloud computing provides very tangible benefits for SCADA environments, it also presents opportunities for attackers to gain a foothold in trusted environments. Cloud service users should consider several security concerns with regard to the nature of data, web application attacks, control, authentication, encryption, and logging.

Until SCADA and ICS security improves, ICS and/or SCADA device owners and/or controllers should use the cloud with caution. If cloud use is indeed required, approach it with care. Implement basic security postures to ensure safety at the baseline.

References

- http://blog.trendmicro.com/trendlabs-security-intelligence/no-excuses-when-it-comes-to-data-security/
- http://en.wikipedia.org/wiki/Cloud_computing
- http://en.wikipedia.org/wiki/Man-in-the-middle_attack
- http://en.wikipedia.org/wiki/Security_information_and_event_management
- http://research.aberdeen.com/ebooks/Proven-Benefits-of-Backing-Up-Data-to-the-Cloud.pdf
- http://www.alertlogic.com/resources/cloud-security-report/
- http://www.apple.com/icloud/
- http://www.bloomberg.com/news/2013-03-26/how-private-data-became-public-on-amazon-s-cloud.html
- http://www.digitalbond.com/scadapedia/protocols/secure-dnp3/
- http://www.ida.liu.se/labs/rtslab/iisw04/camready/SCADA-Attack-Trees-Final.pdf
- http://www.informationweek.com/cloud-computing/software/time-to-think-about-cloud-computing/211300562
- http://www.infoworld.com/d/security/citigroup-breach-exposed-data-210000-customers-664
- https://cloud.google.com/

TREND MICRO INCORPORATED

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years' experience, we deliver top-ranked client, server and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge—from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.

TREND MICRO INCORPORATED

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003

www.trendmicro.com

TREND MICRO™

Securing Your Journey to the Cloud