Temasek Defence Systems Institute

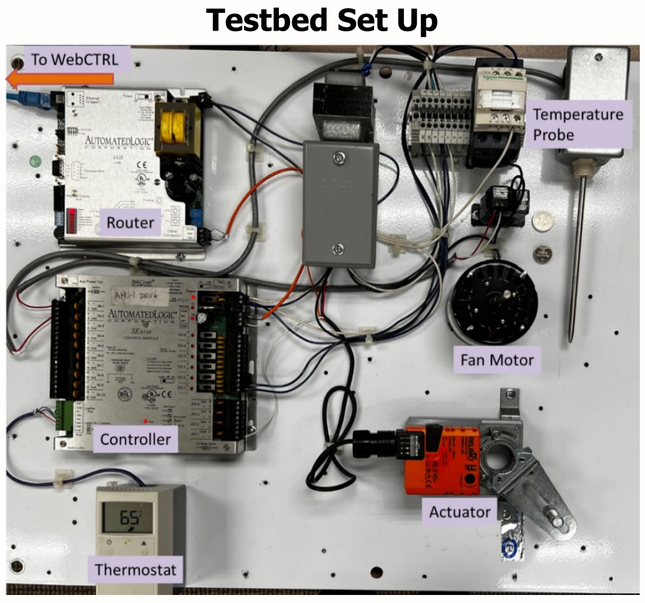
# SECURITY ANALYSIS OF A BACNET CONTROLLER IN BUILDING AUTOMATION ENVIRONMENTS

Author: ME5 Lee Wei Zhi Jonathan
Thesis advisor: Prof Thuy Nguyen, Prof Neil C. Rowe

**Abstract**

Heating, ventilation, and air conditioning (HVAC) systems are industrial control systems that form the backbone of the working environment within modern buildings. They have historically been designed more for operational needs rather than with security in mind. As such, HVAC systems are vulnerable to cyberattacks which can cause significant damage, considering the massive and powerful structures that these systems often control. This research analyzed the vulnerabilities in a fan-coil unit (FCU) that used the industrial BACnet protocol used in many HVAC networks around the world. Additionally, it assessed vulnerabilities in the BACnet protocol and studied how it was implemented in one commercial building automation management product. Proof-of-concept exploits of discovered vulnerabilities were developed to demonstrate potential attacks, and findings from the experiments can help inform patching efforts and risk mitigation of building automation systems in the U.S. Department of Defense and Singapore Ministry of Defence.

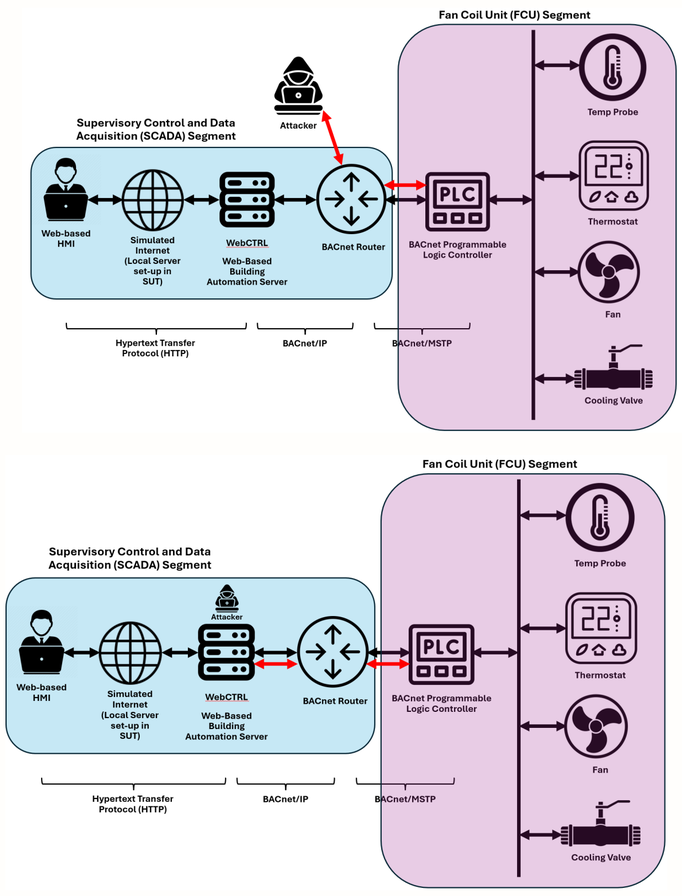
## Testbed Set Up




## Tools Used

1. Wireshark with BACnet packet dissector – Packet sniffing and inspection
2. Notepad++ with Compare plugin – Reverse engineering of proprietary BACnet protocol used by WebCTRL.
3. BACpypes – Open source Python library for crafting spoofed BACnet packets. Used for command insertion.
4. PyDivert – Open source Python library implementation of WinDivert, which is a driver used for Man-In-The-Middle (MITM) packet interception and modification attacks.

## Attack Scenarios







## Exploits Tested

*Objective 1: Achieve manual control over a target*

1. Gain manual control over the fan (on-off)
2. Gain manual control over the actuator (open-close at 0 to 100%)
3. Gain manual control over the thermostat (temperature reported to SCADA server)

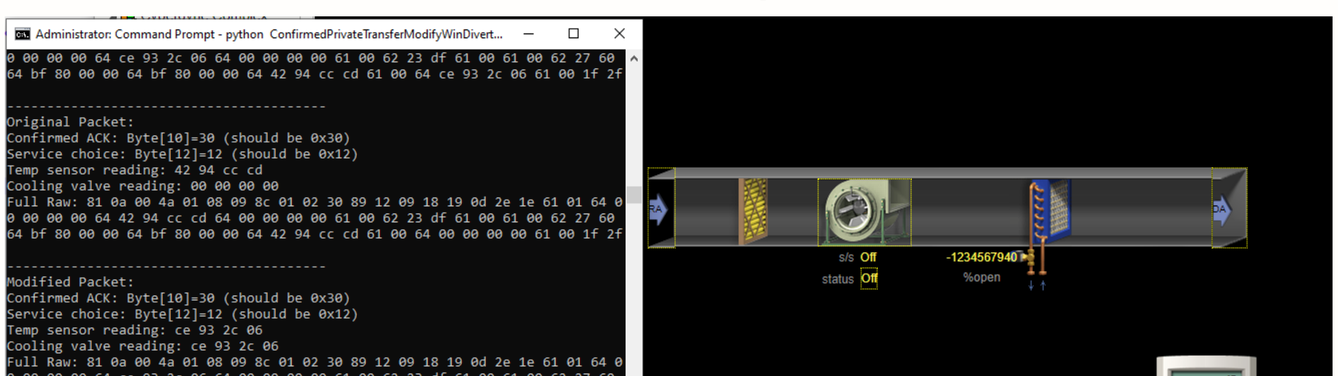
Exploit code was written using BACpypes open source Python library. 10 out of 10 test conditions succeeded.

*Objective 2: Remove signs of attack on the graphical display for stealth*

1. Control the SCADA user display of the fan state (on-off)
2. Control the SCADA user display of the actuator state (open-close at 0 to 100%)
3. Control the SCADA user display of the thermostat state (temperature reported to SCADA server)
4. Prevent any SCADA alarms from sounding due to unexpected system behavior or malicious attack.

Exploit code was written using PyDivert open source Python library. 10 out of 10 test conditions succeeded.

## Demonstration of Exploit




## Vulnerabilities Discovered

*CWE-605 Multiple Binds to the Same Port*

This vulnerability allowed an attacker to connect to the same port that the legitimate SCADA server was connected to, which enables the attacker to spoof commands that would look like they are coming from the server.

*CWE-290 Authentication Bypass by Spoofing*

This vulnerability allowed the attacker to send arbitrary commands to the PLC and gain full control over it and all devices connected to it, without requiring any sort of authentication.

*CWE-311 Missing Encryption of Sensitive Data*

This vulnerability allowed the attacker to reverse engineer proprietary formats and sensitive operational data which allowed them to craft malicious packets and conduct spoofing attacks.

## Conclusion

We discovered several weaknesses present in the BACnet protocol and how it was implemented within WebCTRL concerning (1) a port reuse, (2) lack of source authentication, and (3) lack of encryption of sensitive data. Exploiting the first weakness allows malicious code to run on the same machine as WebCTRL, making malicious packets seem legitimate. Exploiting the second weakness allowed attackers to send malicious service commands to the PLC devices, resulting in physical control over those devices. Finally, exploiting the third weakness allows reverse-engineering the proprietary protocols used by WebCTRL in managing the PLC. This enables intercepting and modifying packets, resulting in loss of control over the information displayed on the user interface and subsequent mishandling of the real devices. This could increase the time to discover an attacker on the network, as the attacker could prevent alarms from triggering or make the display appear as though everything was operating normally.

## Future Work

- More research should be done to investigate the feasibility of spoofing other values on the WebCTRL interface display. Future work could manipulate information on other pages on WebCTRL, such as the second and third-layer information displayed on the Properties page.
- Improve the existing PoC exploits to be more stealthy, by suppressing alarms and log records, and to eliminate any traces of their actions being displayed on the interface.
- Do experiments on a simple FCU testbed with three devices connected to a single router and PLC. Different configurations and different numbers of devices could result in different protocol structures within ConfirmedPrivateTransfer. A more generalized approach can be developed to handle them.
- Reverse engineering of other OT protocols could discover other vulnerabilities and generate exploit code.

NUS National University of Singapore