Plus

Plus tip:

Use these slides as a starting point for customizing your presentation.

Open the Plus add-on for more options.

ICSPatch: Vulnerability Localization and Patching for Industrial Control Systems

September 26, 2023

Agenda

- Introduction to Industrial Control Systems
- The Importance of Industrial Control Systems Security
- Objectives of the Study
- Methodology: Vulnerability Localization
- Recent Attacks on Critical Infrastructure
- Benchmarking Against Existing Approaches
- Discussion: ICSPatch Application
- Additional Features of ICSPatch
- Success Cases of ICSPatch
- Conclusion and Implications

Introduction to Industrial Control Systems

1

Critical infrastructure relies on Industrial Control Systems (ICS) for regulating physical processes in various sectors.

2

Attacks on critical infrastructure often exploit vulnerabilities in IT infrastructure to reach OT control systems.

3

ICS devices execute industrial logic and are confined to the industrial network.

Plus tip:

Highlight the importance of securing Industrial Control Systems in critical infrastructure and the need for vulnerability patching.

The Importance of Industrial Control Systems Security

Key Points

- Critical infrastructure relies on Industrial Control Systems (ICS) for regulating physical processes.
- Attacks on ICS can lead to devastating consequences.
- Increased cybersecurity budget indicates the growing concern for ICS security.

Challenges

- Vulnerability localization in control application binaries is crucial for patching.
- Remote connection to PLCs with admin privileges is a prevalent way to apply patches.
- Specialized tools like ICSFuzz enable the fuzzing of control application binaries.

Plus tip:

To customize this slide, provide specific examples of ICS attacks and highlight the importance of budget allocation for ICS security in your organization.

Objectives of the Study

Patch the vulnerability in the control application

Apply the patch remotely with admin privileges

Localize the vulnerability in the control binary

Plus tip:

To achieve the objectives of the study, focus on developing a methodology for automated vulnerability localization for control application binaries and control binary hotpatching that can be performed remotely with admin privileges.

Methodology: Vulnerability Localization

Assuming access to exploit input

The process begins with assuming access to an exploit input that can crash the control application executing on the development PLC.

Using specialized tools

Specialized tools such as ICSFuzz enable the fuzzing of control application binaries, providing the exploit input if available.

Extracting runtime process memory

ICSPatch extracts hexdumps of the runtime process memory space, the MainTask thread executing the control application, and any other required shared libraries.

Plus tip:

To customize this slide, you can provide specific examples of exploit inputs or mention any other tools used in the vulnerability localization process.

Recent Attacks on Critical Infrastructure

Examples of Recent Attacks

- Saudi Aramco: A self-replicating virus on the computer network of Saudi Aramco shut down 5.7 million barrels of output per day, impacting over 5% of the global oil supply.
- Other Attacks: There have been numerous attacks on critical infrastructure, exploiting vulnerabilities in IT infrastructure to reach control systems and causing devastating consequences.
- Example 1: [Insert example of recent attack on critical infrastructure]
- Example 2: [Insert example of recen
infrastructure]

Plus tip:

Include specific examples of recent attacks relevant to your audience to highlight the importance of cybersecurity measures.

Benchmarking Against Existing Approaches

96.9%

DeepVL Accuracy

70.1%

DeepVL Precision

80.24%

Devign Accuracy

Plus tip:

When benchmarking ICSPatch against existing approaches, consider accuracy and precision as key metrics for evaluation.

Discussion: ICSPatch Application

Patch Implementation

ICSPatch requires a kernel-level component (LKM, in our case, or a dedicated patch driver) for patching the control applications running on Linux operating systems.

Device Support

ICSPatch provides a JTAG-based patcher out-of-the-box to support devices like BeagleBone Black (BBB).

Function Extension

In most cases, extending ICSPatch to support oth
appropriate node to the DDG for automated vulne

Plus tip:

When implementing ICSPatch, make sure to have a kernel-level component for patching control applications, consider using the JTAG-based patcher for device support, and add the necessary nodes to the DDG for supporting additional functions.

Additional Features of ICSPatch

Memory-related functions

- ICSPatch includes eight different memory-related functions in its dataset.
- It successfully patches the vulnerable control binaries using ICSPatch.
- The patches implement a bound check and can be applied to all relevant examples with minor modifications to the live memory addresses.

Support for other functions

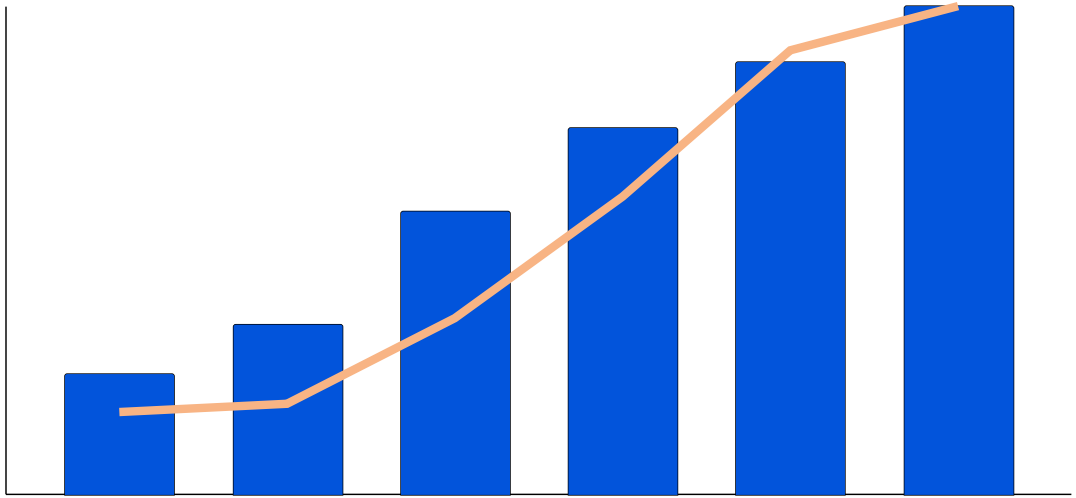
- ICSPatch can be extended to support other functions by adding the appropriate node to the data dependence graph (DDG) for automated vulnerability localization.
- This enables the detection and patching of vulnerabilities in a wider range of control applications.
- Example: Adding support for input validation function.

Plus tip:

Customize the content of this slide by providing specific examples of memory-related functions and the process of extending ICSPatch to support other functions.

Success Cases of ICSPatch

ICSPatch Success Cases



This chart is a placeholder. Customize it here.

Vulnerabilities Patched

- Out-of-bounds write/read
- OS command injection
- Invalid input validation

Plus tip:

Highlight the specific vulnerabilities that ICSPatch successfully patched in real-world scenarios.

Conclusion and Implications

1. ICSPatch is a valuable tool for automated vulnerability identification and patching in control applications running on Industrial Control Systems (ICS).

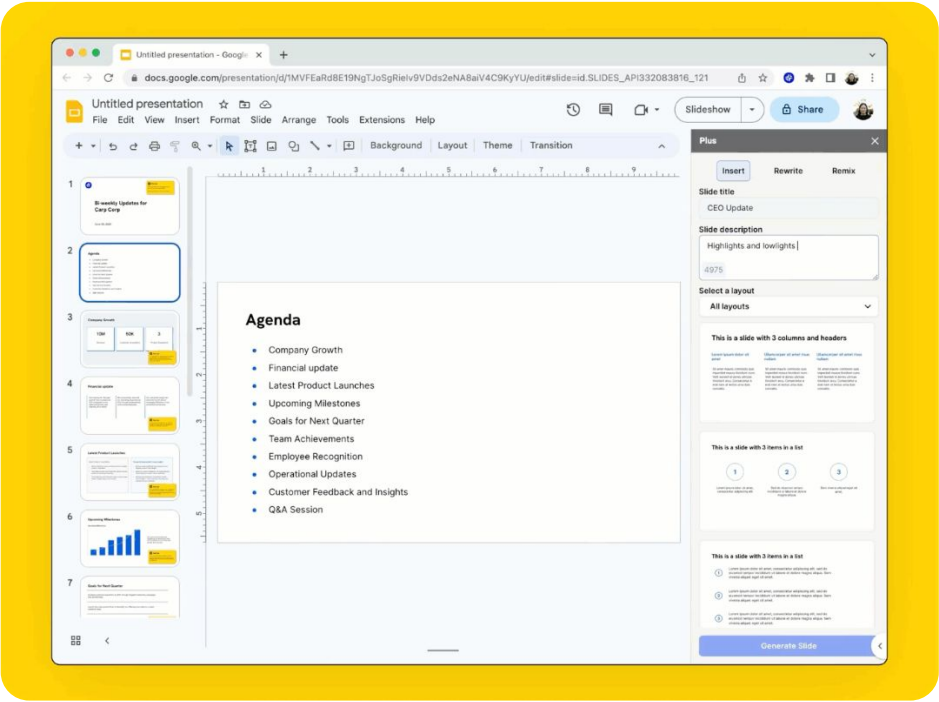
2. The implementation of ICSPatch on the Codesys platform has been proven effective in patching vulnerabilities on over 400 known ICS devices from 80 industrial device vendors.

3. ICSPatch can successfully patch various vulnerabilities in c
application binaries with minimal execution and memory ov

Plus tip:

Consider using ICSPatch to enhance the security of control applications in critical infrastructure and industrial systems.

Time to put the finishing touches on your Plus AI presentation ✨



Just created your first Plus AI deck? Here's what to try next:

- **Insert** - Choose a layout and create one slide at a time
- **Rewrite** - Shorten, lengthen, or spice up existing slide content
- **Remix** - Transform your slide into a new layout
- **Design** - Customize your slide colors, fonts, and add a logo

Need help? 👉guide.plusdocs.com