Plus

ICSPatch: Automating Control Logic Vulnerability Localization and Patching

September 25, 2023

Plus tip:

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

Open the Plus add-on for more options.

Agenda

- Challenges in OT and IT Intercommunication
- Need for In-memory Vulnerability Patching
- Reliance on OT Vendors
- Introduction to ICSPatch
- ICSPatch: Methodology and Application
- Impacts on Critical Infrastructure
- Divergence from Previous Research
- ICSPatch: Limitations and Capabilities
- ICSPatch Performance and Evaluation
- Conclusion and Future Directions

Challenges in OT and IT Intercommunication

Removal of air gapping increases vulnerabilities in OT devices

Conventional patching involving device reboot is not feasible for OT devices controlling critical processes

Reliance on OT vendors for rapid vulnerability discovery and patch development

Plus tip:

Consider highlighting the need for alternative patching methods and the importance of collaboration with OT vendors.

Need for In-memory Vulnerability Patching

Challenges of Conventional Patching

Conventional patching involves device reboot and downtime.

OT devices controlling critical processes cannot afford downtime.

In-house proprietary compilers hinder the patching process.

Reliance on OT vendors for vulnerability discovery and patch development.

Introduction to ICSPatch

ICSPatch is a framework for automating control logic vulnerability localization.

ICSPatch uses Data Dependence Graphs (DDGs) to pinpoint vulnerabilities in control applications.

ICSPatch can non-intrusively hotpatch vulnerabilities in the main memory of Programmable Logic Controllers (PLCs).

ICSPatch ensures reliable continuous operation while applying patc

Plus tip:

To address the challenges of conventional patching, consider implementing ICSPatch for in-memory vulnerability patching in control applications of OT devices.

Reliance on OT Vendors

OT devices controlling critical processes require in-memory vulnerability patching due to downtime constraints.

Control binaries are often compiled by in-house proprietary compilers, making patch development challenging.

OT vendors play a crucial role in discovering vulnerabilities and developing patches for control applications.

Plus tip:

When relying on OT vendors for vulnerability discovery and patch development, it's important to establish effective communication and collaboration to ensure timely and effective patching of control applications.

Introduction to ICSPatch

ICSPatch: Framework for Vulnerability Localization and Control Binary Hotpatching

- Enables vulnerability localization and hotpatching in control applications
- Designed for Industrial Control Systems (ICS)
- Focuses on control applications rather than firmware
- Does not assume availability of trusted source patches

Plus tip:

To customize this slide, you can replace the Codesys platform with the relevant platform used in your organization and highlight any additional features or benefits of ICSPatch.

ICSPatch: Methodology and Application

Methodology

ICSPatch uses Data Dependence Graphs (DDGs) to automate control logic vulnerability localization. It identifies and patches vulnerabilities in control applications.

Application

ICSPatch is designed for the Codesys platform. It localizes and patches vulnerabilities in control application binaries, focusing on hotpatching control applications.

Limitations

ICSPatch is Codesys-specific and patches tl
vulnerability. User input is needed for memo
OS command injection patching is automate

Plus tip:

Customize this slide by providing specific examples of vulnerabilities that ICSPatch can localize and patch in control applications.

Impacts on Critical Infrastructure

225,000	Customers without electricity
50	Water supply disruptions
3	Transportation system failures
2	Communication network outages

Plus tip:
Customize the metrics on this slide based on the specific impacts on critical infrastructure relevant to your audience.

Divergence from Previous Research

1

ICSPatch focuses on hotpatching control applications rather than firmware and does not assume the availability of trusted source patches.

2

ICSPatch is a Codesys-specific implementation that identifies vulnerabilities, localizes them, and applies patches.

3

Orthogonal control logic modification protection solutions, such as checksums, digital signatures, control logic comparison, and formal verification, are needed for scenarios like these.

Plus tip:

Highlight the unique features of ICSPatch compared to previous research and emphasize its Codesys-specific implementation.

ICSPatch: Limitations and Capabilities

Limitations

- ICSPatch is a Codesys-specific implementation.
- It currently only patches the first instance of a vulnerability.
- User input is required for memory-related vulnerabilities.
- A more elaborate mechanism is needed for multicore cases.

Capabilities

- ICSPatch is a Codesys-specific implementation.
- It currently only patches the first instance of a vulnerability.
- User input is required for memory-related vulnerabilities.
- A more elaborate mechanism is needed for multicore cases.

Plus tip:

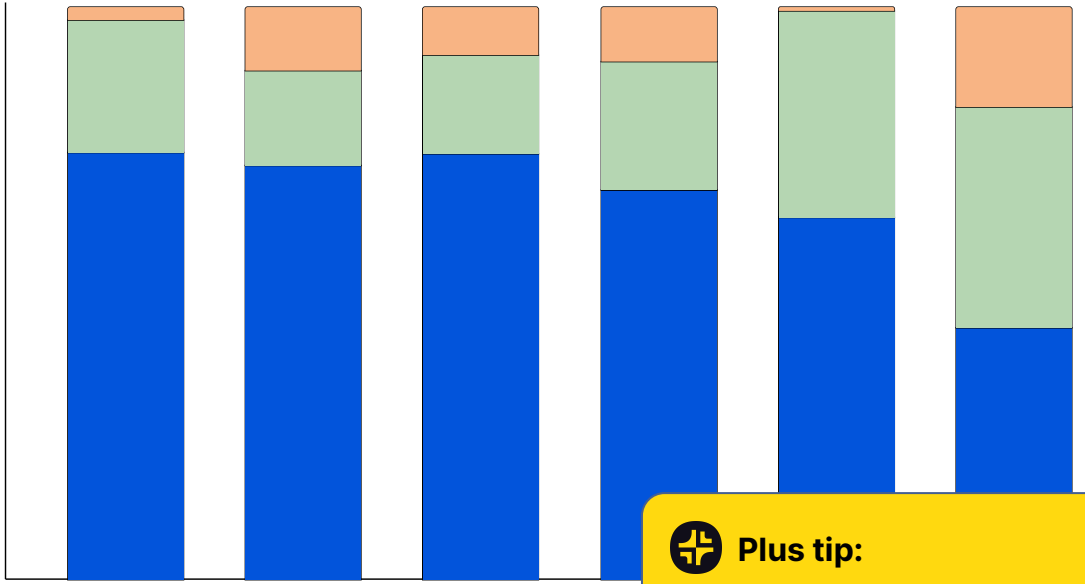
Consider customizing the capabilities and limitations based on the specific needs of the audience.

ICSPatch Performance and Evaluation

This chart is a placeholder. Customize it here.

ICSPatch Performance

ICSPatch successfully localized all vulnerabilities and applied patches with negligible latency increase.



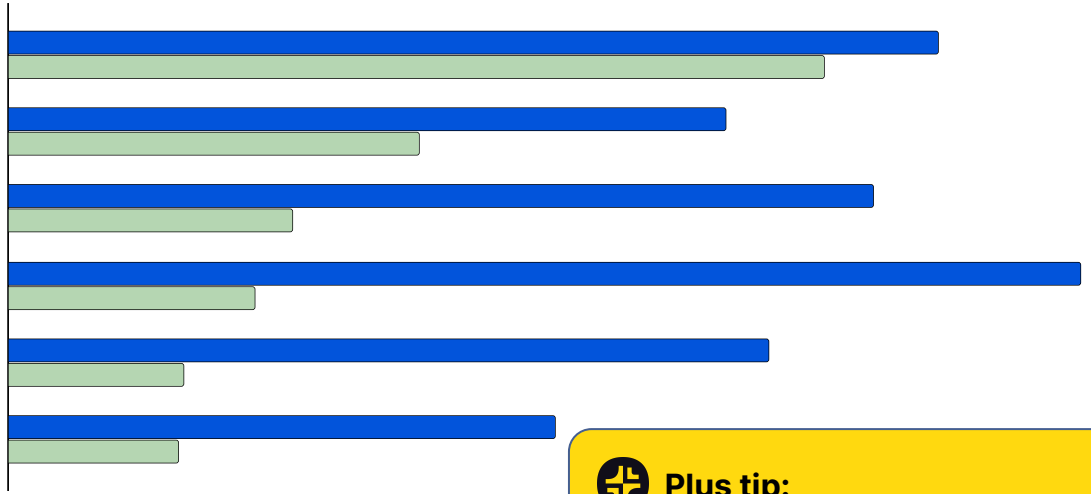
Plus tip:

Highlight the successful localization of vulnerabilities and the minimal impact on latency to demonstrate the effectiveness of ICSPatch.

Conclusion and Future Directions

Summary of Findings:

- ICSPatch successfully localizes vulnerabilities in control application binaries.
- The framework can non-intrusively hotpatch vulnerabilities in the main memory of Programmable Logic Controllers.
- Patching control applications does not cause significant latency increase and maintains correctness and protection against vulnerabilities.

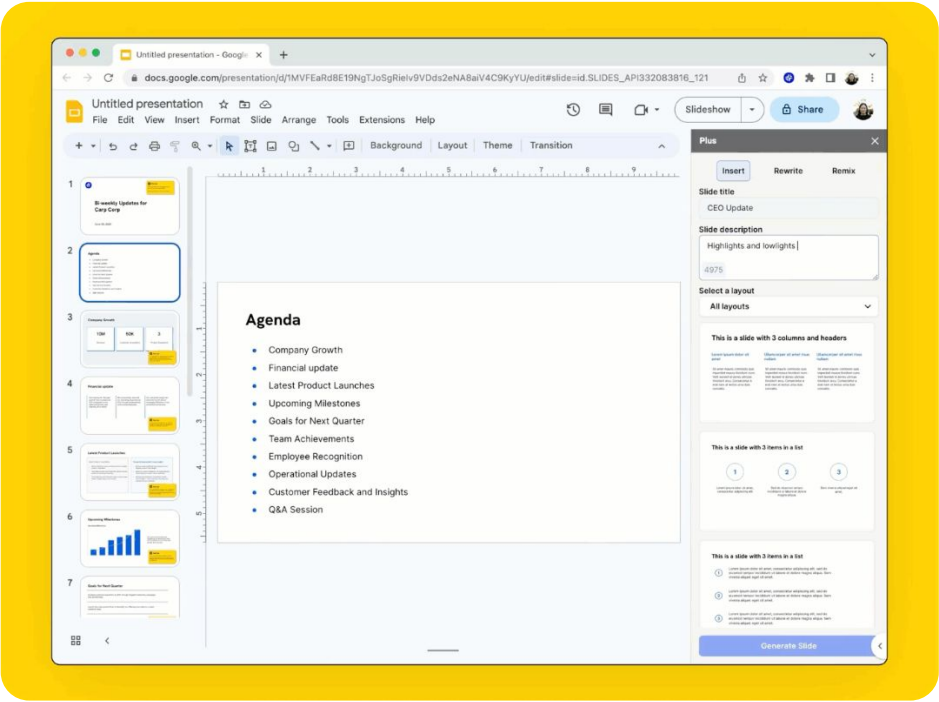


This chart is a placeholder. Customize it here.

Plus tip:

Consider highlighting the key achievements of ICSPatch in localizing and patching vulnerabilities, and emphasize the importance of maintaining continuous operation and protection against vulnerabilities in control applications.

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

Highlights

1

We have developed a methodology for automated vulnerability localization for non-executable control application binaries using custom-built data dependence graphs.

2

Our methodology has been successfully applied to patch out-of-bounds write/read, OS command injection, and invalid input validation vulnerabilities in a dataset of 24 synthetic control application binaries with minimal execution and memory overheads.

3

In addition, we have developed a methodology for control binary hotpatching that can be performed with only remote

Plus tip:

Customize the bullet points to highlight specific vulnerabilities and applications relevant to your organization. Use visuals and examples to support your findings.

Motivation

Increasing Attacks on Critical Infrastructure

In recent years, attacks on critical infrastructure have become more frequent and sophisticated. These attacks target vulnerabilities in the IT infrastructure to gain access to the Operational Technology (OT) control systems, resulting in severe consequences.

Budget Allocation for Cybersecurity

According to a survey conducted by SANS, 42% of the respondents confirmed an increase in the cybersecurity budget for their organization. This indicates a growing recognition of the importance of securing control systems and preventing cyber threats.

Importance of Localizing Vulnerabilities

To effectively address security risks in control applications, it is crucial to patch the vulnerabilities within the control binary itself, rather than relying solely on imported functions. This approach ensures a more co
se

Plus tip:

Customize the content on this slide by providing specific examples of recent attacks on critical infrastructure and their impact. Emphasize the importance of allocating resources for cybersecurity and the need to prioritize vulnerability localization.

Findings

1

A self-replicating virus on the computer network of Saudi Aramco shut down 5.7 million barrels of output per day, impacting more than 5% of the global oil supply.

2

The approach Devign reached an accuracy of 80.24%.

3

The machine learning-based approach DeepVL achieved an accuracy of 96.9% but had a low precision of 70.1%.

Plus tip:

To customize this slide, you can provide specific examples of other self-replicating viruses and their impact on computer networks. Additionally, you can discuss the limitations and potential improvements of the DeepVL and Devign approaches.

Findings

1. Such scenarios require orthogonal control logic modification protection solutions, for instance, using checksums, digital signatures, control logic comparison while uploading, and formal verification employing behavior, state, specification verification.

2. To test the accuracy of ICSPatch, we utilize our synthetic application binary dataset with 24 binaries and the 20 vulnerable binaries from the ICSFuzz dataset.

3. ICSPatch targets hotpatching of control applications in the firmware, so we cannot assume the existence of patc a trusted source.

Plus tip:

Customize the findings to highlight the specific results and implications for your audience.

Comparative Analysis

1. Orthogonal control logic modification protection solutions include checksums and digital signatures.

2. Formal verification methods like behavior and specification verification can also be used.

3. Control logic comparison while uploading is another pro solution.

Plus tip:

To customize this slide, you can add specific examples of how each protection solution is implemented in real-world scenarios.