

Sandboxing .NET Assemblies for fun, profit and, of course Security!

Niels Tanis

NDC { Sydney }



Cover Slide Option w/
title/intro line, main
cover title, subhead
date, please delete
subhead, title, etc.
not needed, please le
justify all text



Slide with larger header
when there is not a need
for text heavy.

The content text slide
bullets as preview, so
you do not need to
bullets. Text is present
Trebuchet size 14,
bullets may be removed
not needed.

Who am I?

- Niels Tanis
- Principal Security Researcher @ Veracode
 - Background .NET Development, Pentesting/ethical hacking, and software security consultancy
 - ISC² CSSLP
 - Research on static analysis for .NET apps



NDC { Sydney }

@nielstanis



Slide with larger header
when there is not a need
for text heavy.

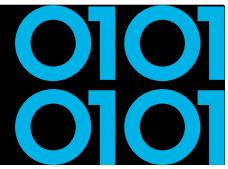
The content text slide
bullets as preview, so
you do not need to
bullets. Text is present
Trebuchet size 14,
bullets may be removed
not needed.

Agenda

- Introduction
- The security risks of third party libraries
- Sandboxing techniques
- Let's create a sandbox!
- Conclusion
- QA

NDC { Sydney }

@nielstanis



Slide with larger header
when there is not a need
for text heavy.

The content text slide
bullets as preview, however
you do not need to
bullets. Text is present
Trebuchet size 14,
bullets may be removed
not needed.

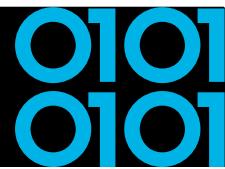
Third Party Libraries

- Big chunk (80%+) of our apps consists of 3rd party libraries
- Efficient in time, why reinvent the wheel?
- How actively is it maintained?
- What do they do for security?

NDC { Sydney }

@nielstanis

State Of Software Security v11 2021



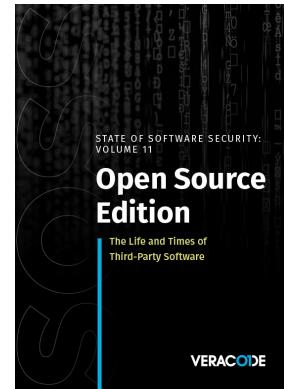
Slide with larger header
when there is not a need
for text heavy.

The content text slide
bullets as preview, so
you do not need to
bullets. Text is present
Trebuchet size 14,
bullets may be removed
not needed.

*"Despite this dynamic landscape,
79 percent of the time, developers
never update third-party libraries after
including them in a codebase."*

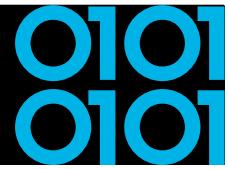


NDC { Sydney }



@nielstanis

<https://info.veracode.com/fy22-state-of-software-security-v11-open-source-edition.html>



Slide with larger heading when there is not a need for heavy text.

The content text slide bullets as preview, however you do not need to bullet. Text is present in Trebuchet size 14, bullets may be removed if not needed.

Vulnerabilities in libraries

A screenshot of a GitHub issue page for the repository "dotnet/announcements". The issue is titled "Microsoft Security Advisory CVE-2022-24512 | .NET Remote Code Execution Vulnerability #213". The issue was opened by "dcwhittaker" on March 8, 2022, with 0 comments. The issue has 186 issues and 3k pull requests. The "Issues" tab is selected. The issue content includes an "Executive summary" section which states: "Microsoft is releasing this security advisory to provide information about a vulnerability in .NET 6.0, .NET 5.0, and .NET Core 3.1. This advisory also provides guidance on what developers can do to update their applications to remove this vulnerability. A Remote Code Execution vulnerability exists in .NET 6.0, .NET 5.0, and .NET Core 3.1 where a stack buffer overrun occurs in .NET Double Parse routine." Below the summary is a "Discussion" section with a link to "dotnet/runtime#66348". The right sidebar shows the following details: Assignees (No one assigned), Labels (Monthly-Update, .NET Core 3.1, .NET 6.0, Patch-Tuesday, Security), Projects (None yet), and Milestone (No milestone). The URL of the issue is https://github.com/dotnet/announcements/issues/213.

@nielstanis

<https://github.com/dotnet/announcements/issues/213>



Slide with larger header when there is not a need for heavy text.

The content text slide bullets as preview, however you do not need to bullet. Text is present in Trebuchet size 14, bullets may be removed if not needed.

Vulnerabilities in libraries



Alerts and Tips Resources Industrial Control Systems

National Cyber Awareness System > Current Activity > Malware Discovered in Popular NPM Package, ua-parser-js

Malware Discovered in Popular NPM Package, ua-parser-js

Original release date: October 22, 2021

[Print](#) [Tweet](#) [Send](#) [Share](#)

Versions of a popular NPM package named [ua-parser-js](#) was found to contain malicious code. ua-parser-js is used in apps and websites to discover the type of device or browser a person is using from User-Agent data. A computer or device with the affected software installed or running could allow a remote attacker to obtain sensitive information or take control of the system.

CISA urges users and administrators using compromised ua-parser-js versions 0.7.29, 0.8.0, and 1.0.0 to update to the respective patched versions: 0.7.30, 0.8.1, 1.0.1

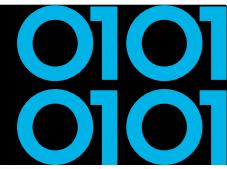
For more information, see [Embedded malware in ua-parser-js](#).

NDC { Sydney }

@nielstanis

<https://us-cert.cisa.gov/ncas/current-activity/2021/10/22/malware-discovered-popular-npm-package-ua-parser-js>

<https://portswigger.net/daily-swig/popular-npm-package-ua-parser-js-poisoned-with-cryptomining-password-stealing-malware>



Slide with larger header when there is not a need for text heavy.

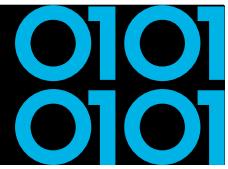
The content text slide bullets as preview, however you do not need to bullet. Text is present in Trebuchet size 14, bullets may be removed if not needed.

Vulnerabilities in libraries

The image shows two side-by-side screenshots of GitHub blog posts. The left screenshot is titled "GitHub's commitment to npm ecosystem security" and features a cartoon illustration of a person working on a large puzzle piece. The right screenshot is titled "Enrolling all npm publishers in enhanced login verification and next steps for two-factor authentication enforcement" and features the npm logo. Both posts are categorized under "Open Source" and "Security". The bottom left of the image has the text "NDC { Sydney }" and the bottom right has the text "@nielstanis".

<https://github.blog/2021-11-15-githubs-commitment-to-npm-ecosystem-security/>

<https://github.blog/2021-12-07-enrolling-npm-publishers-enhanced-login-verification-two-factor-authentication-enforcement/>



Slide with larger header when there is not a need for heavy text.

The content text slide bullets as preview, however you do not need to bullet. Text is present in Trebuchet size 14, bullets may be removed if not needed.

Vulnerabilities in libraries

Third-party code comes with some baggage



Recognizing risks introduced by statically linked third-party libraries

Introduction

Developing software solutions is a complex task requiring a lot of time and resources. In order to accelerate time to market and reduce the cost, software developers create smaller pieces of functional code which can be reused across

@nielstanis

NDC { Sydney }

<https://blog.secure.software/third-party-code-comes-with-some-baggage>

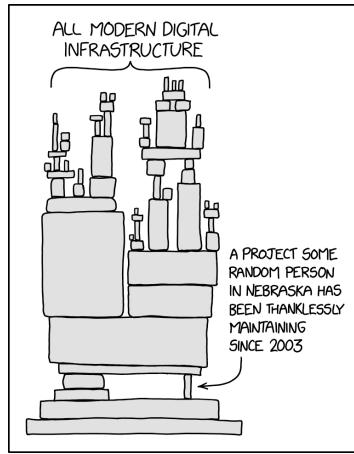
0101
0101

Slide with larger header when there is not a need for text heavy.

The content text slide bullets as preview, however you do not need to bullet. Text is present in Trebuchet size 14, bullets may be removed if not needed.

XKDC - Dependency

NDC { Sydney }



<https://xkcd.com/2347/> @nielstanis



Sandboxing .NET Assemblies

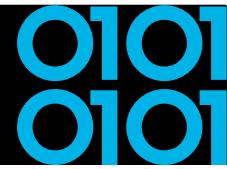
Slide with larger header
when there is not a need
for heavy text.

The content text slide
bullets as preview, so
you do not need to
bullets. Text is present
Trebuchet size 14,
bullets may be removed
not needed.

- Is there a way we can do a better job?
- A way for us to reduce the security risks?
- Keep in mind it's not a matter of how it's more when!

NDC { Sydney }

@nielstanis



Sandboxing .NET Assemblies

Slide with larger header
when there is not a need
for text heavy.

The content text slide
bullets as preview, so
you do not need to
bullets. Text is present
Trebuchet size 14,
bullets may be removed
not needed.

- We want to use the library without modification
- Can we maybe create a controlled (restricted) sandbox?
- A sandbox with limited capabilities?

NDC { Sydney }

@nielstanis

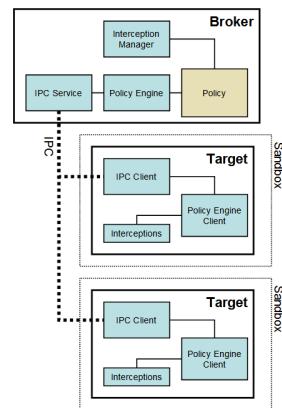


Slide with larger header when there is not a need for heavy text.

The content text slide bullets as preview, however you do not need to bullet. Text is present in Trebuchet size 14, bullets may be removed if not needed.

Browser Sandbox

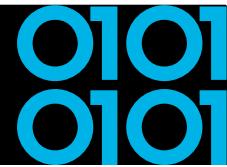
- Chromium Sandbox
- No direct system access
- Each OS related call is done via IPC
- FireFox Sandbox
 - Containers & Site Isolation
 - RLBox



@nielstanis

NDC { Sydney }

<https://chromium.googlesource.com/chromium/src/+/refs/heads/main/docs/design/sandbox.md>
<https://hacks.mozilla.org/2021/05/introducing-firefox-new-site-isolation-security-architecture/>



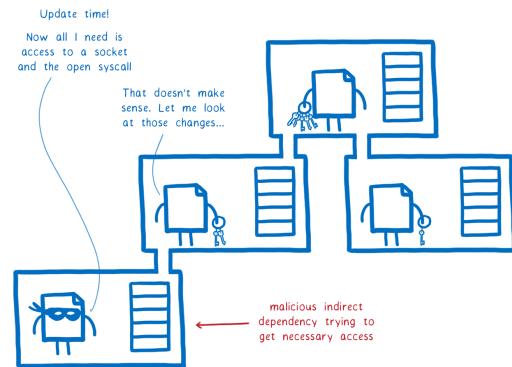
Slide with larger heading when there is not a need for heavy text.

The content text slide bullets as preview, however you do not need to bullet. Text is present in Trebuchet size 14, bullets may be removed if not needed.

WebAssembly Nanoprocess

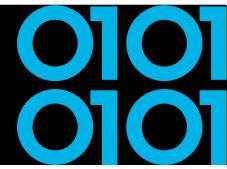
- Linear memory model
- WASM module isolation
- Declarative permissions
- Interface types
- WASI for BCL calls

NDC { Sydney }



@nielstanis

<https://hacks.mozilla.org/2019/11/announcing-the-bytecode-alliance/>

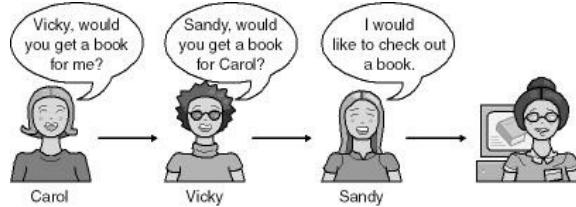


Slide with larger header when there is not a need for heavy text.

The content text slide bullets as preview, however you do not need to bullets. Text is presented in Trebuchet size 14, bullets may be removed if not needed.

Code Access Security

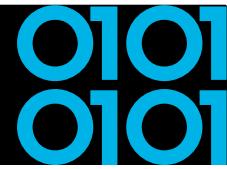
- Evidence based model
- Code from different origins have different sets of rights
- Stack-walks that protect against luring attacks



NDC { Sydney }

@nielstanis

Figure 18-1; Writing Secure Code 2nd Edition

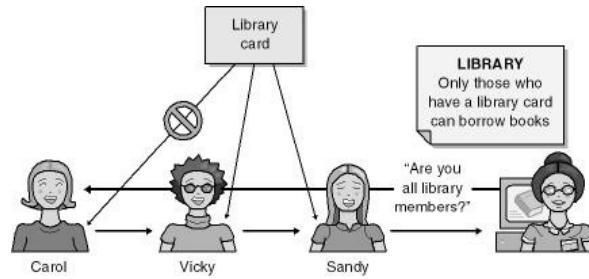


Slide with larger header when there is not a need for heavy text.

The content text slide bullets as preview, however you do not need to bullet. Text is present in Trebuchet size 14, bullets may be removed if not needed.

Code Access Security

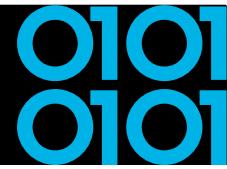
- Evidence library card
- Policy → Librarian only allows members



NDC { Sydney }

@nielstanis

Figure 18-2; Writing Secure Code 2nd Edition



Slide with larger header when there is not a need for text heavy.

The content text slide bullets as preview, however you do not need to bullet. Text is present in Trebuchet size 14, bullets may be removed if not needed.

Code Access Security

- Stack walk

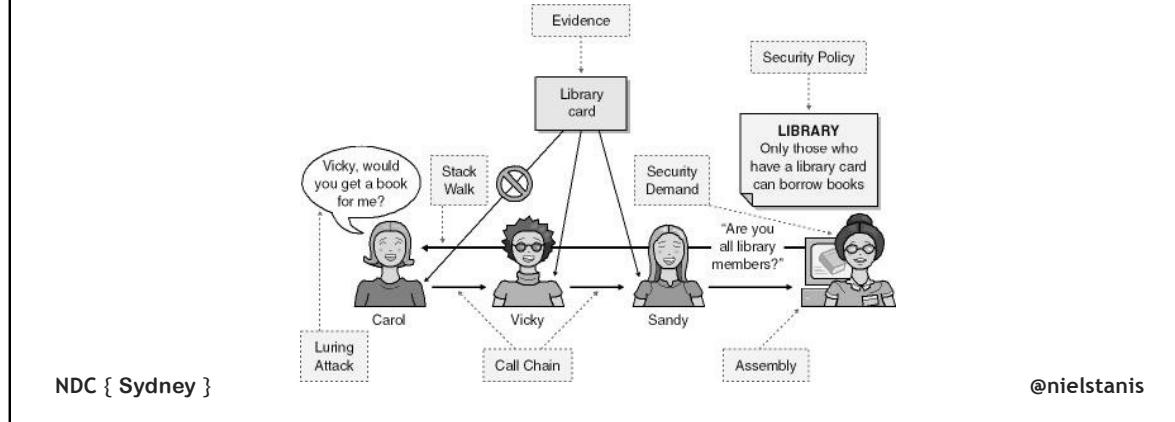
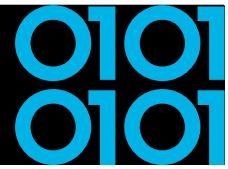


Figure 18-2; Writing Secure Code 2nd Edition



Slide with larger header
when there is not a need
for text heavy.

The content text slide
bullets as preview, so
you do not need to
bullets. Text is present
Trebuchet size 14,
bullets may be removed
not needed.

Code Access Security

- Most practical example, ASP.NET Medium Trust
- CAS is deprecated since .NET Framework 4
- Too complex in administering and use?
- Too early?

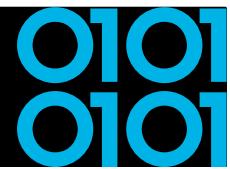
NDC { Sydney }

@nielstanis

<https://docs.microsoft.com/en-us/previous-versions/dotnet/framework/code-access-security/code-access-security-basics>

<https://docs.microsoft.com/en-us/previous-versions/dotnet/framework/code-access-security/code-access-security-policy-compatibility-and-migration>

Demo time!



Slide with larger header when there is not a need for text heavy.

The content text slide bullets as preview, however you do not need to bullets. Text is presented in Trebuchet size 14, bullets may be removed if not needed.



NDC { Sydney }

@nielstanis

Image: C# logo <https://docs.microsoft.com/en-us/dotnet/csharp/>



Slide with larger header
when there is not a need
for text heavy.

The content text slide
bullets as preview, however
you do not need to
bullets. Text is presented
Trebuchet size 14,
bullets may be removed
not needed.

DocumentProcessor Package

- Use package as is!
- Disclaimer: always comply with library license!
- Not allowed to reverse engineer/decompile
- We do want to change behaviour:
 - Opening documents directly from URL - SSRF
 - Writing files to any arbitrary directory - Path Traversal
- There are *several* ways to fix this!

NDC { Sydney }

@nielstanis



Slide with larger header
when there is not a need
for text heavy.

The content text slide
bullets as preview, so
you do not need to
bullets. Text is present
Trebuchet size 14,
bullets may be removed
not needed.

AssemblyLoadContext

- Only single AppDomain in .NET Core.
- AssemblyLoadContext replaces the isolation mechanisms provided by multiple AppDomain instances in .NET Framework.
- Conceptually, a load context creates a scope for loading, resolving, and potentially unloading a set of assemblies.

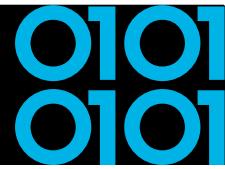
NDC { Sydney }

@nielstanis

[https://docs.microsoft.com/en-](https://docs.microsoft.com/en-us/dotnet/api/system.runtime.loader.assemblyloadcontext?view=net-5.0)

[us/dotnet/api/system.runtime.loader.assemblyloadcontext?view=net-5.0](https://docs.microsoft.com/en-us/dotnet/api/system.runtime.loader.assemblyloadcontext?view=net-5.0)

<https://docs.microsoft.com/en-us/dotnet/core/dependency-loading/understanding-assemblyloadcontext>



Slide with larger header
when there is not a need
for heavy text.

The content text slide
bullets as preview, however
you do not need to
use bullets. Text is present
Trebuchet size 14,
bullets may be removed
not needed.

AssemblyLoadContext

- It allows multiple versions of the same assembly to be loaded within a single process.
- It does not provide any security features. All code has full permissions of the process.
- But it does allow us to control what gets loaded!

NDC { Sydney }

@nielstanis

[https://docs.microsoft.com/en-](https://docs.microsoft.com/en-us/dotnet/api/system.runtime.loader.assemblyloadcontext?view=net-5.0)

[us/dotnet/api/system.runtime.loader.assemblyloadcontext?view=net-5.0](https://docs.microsoft.com/en-us/dotnet/api/system.runtime.loader.assemblyloadcontext?view=net-5.0)

<https://docs.microsoft.com/en-us/dotnet/core/dependency-loading/understanding-assemblyloadcontext>



Slide with larger header
when there is not a need
for heavy text.

The content text slide
bullets as preview, so
you do not need to
bullets. Text is present
Trebuchet size 14,
bullets may be removed
not needed.

AssemblyLoadContext

- Interface project used as shared contract
- Remove DocumentProcessor package from ConsoleApp
 - Add reference to interface project
- Create Library that implements interface
 - Reference interface project and DocumentProcessor Package
 - Self-contained deployment to folder that has all to be loaded by our sandboxed loadcontext

NDC { Sydney }

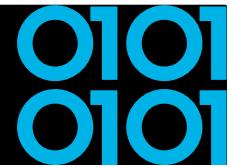
@nielstanis

[https://docs.microsoft.com/en-](https://docs.microsoft.com/en-us/dotnet/api/system.runtime.loader.assemblyloadcontext?view=net-5.0)

[us/dotnet/api/system.runtime.loader.assemblyloadcontext?view=net-5.0](https://docs.microsoft.com/en-us/dotnet/api/system.runtime.loader.assemblyloadcontext?view=net-5.0)

<https://docs.microsoft.com/en-us/dotnet/core/dependency-loading/understanding-assemblyloadcontext>

Sandboxing DocumentProcessor



Slide with larger heading when there is not a need for text heavy.

The content text slide bullets as preview, however you do not need to bullet. Text is presented in Trebuchet size 14, bullets may be removed if not needed.



NDC { Sydney }

@nielstanis

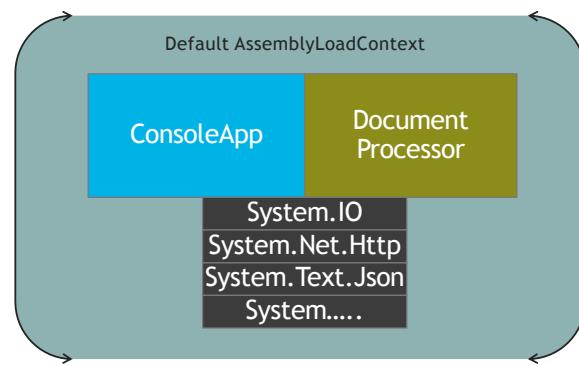
Image: C# logo <https://docs.microsoft.com/en-us/dotnet/csharp/>



Slide with larger header when there is not a need for heavy text.

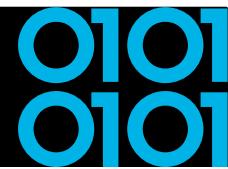
The content text slide bullets as preview, however you do not need to bullets. Text is present in Trebuchet size 14, bullets may be removed if not needed.

ConsoleApp Start



NDC { Sydney }

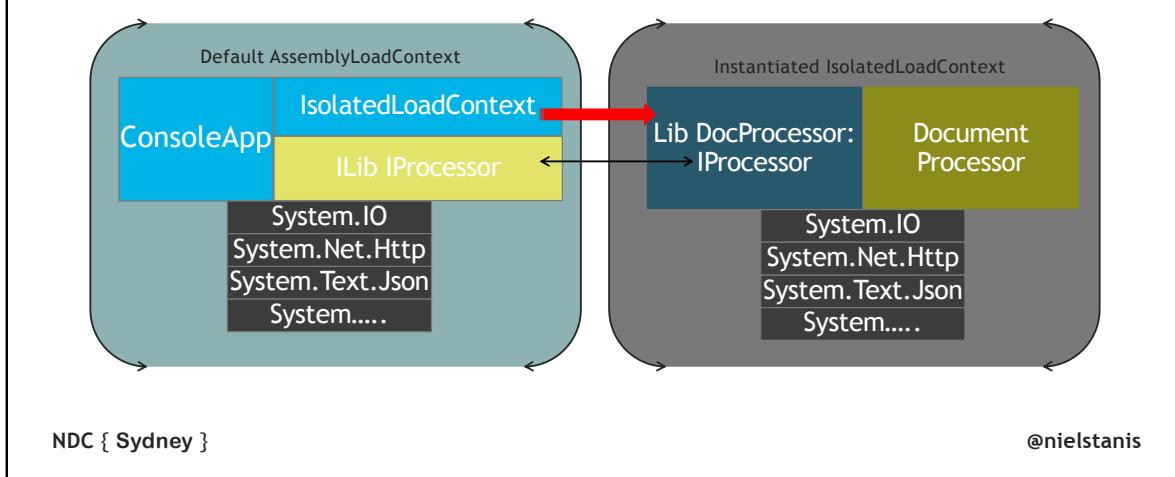
@nielstanis

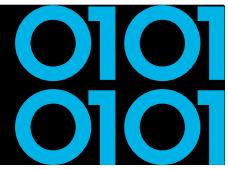


Slide with larger header when there is not a need for text heavy.

The content text slide bullets as preview, however you do not need to bullets. Text is present in Trebuchet size 14, bullets may be removed if not needed.

ConsoleApp & Sandboxed Library





Slide with larger header
when there is not a need
for text heavy.

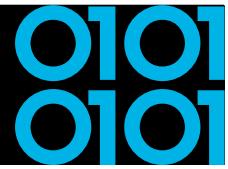
The content text slide
uses bullet points as preview,
however you do not need to
use bullet points. Text is present
in Trebuchet size 14,
bullet points may be removed
if not needed.

Removing Types?

- Self contained set of assemblies, could we not remove types?
- What about trimming that got introduced with .NET 5?
- Maybe we need something more rigorous?

NDC { Sydney }

@nielstanis



Slide with larger header
when there is not a need
for text heavy.

The content text slide
bullets as preview, however
you do not need to
bullets. Text is present
Trebuchet size 14,
bullets may be removed
not needed.

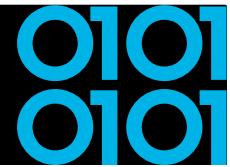
Patching with Harmony2

- A library for patching, replacing and decorating .NET and Mono methods during runtime.
 - Patch at runtime (pre- and postfix)
 - Transpile at compile time (rewrite IL)
- Harmony v2
 - Lib.Harmony on NuGet
 - <https://github.com/pardeike/Harmony>

NDC { Sydney }

@nielstanis

Sandbox & Patching with Harmony2



Slide with larger heading when there is not a need for heavy text.

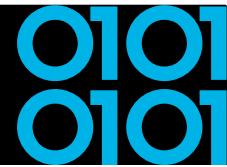
The content text slide bullets as preview, however you do not need to use them. Text is presented in Trebuchet size 14, bullets may be removed if not needed.



NDC { Sydney }

@nielstanis

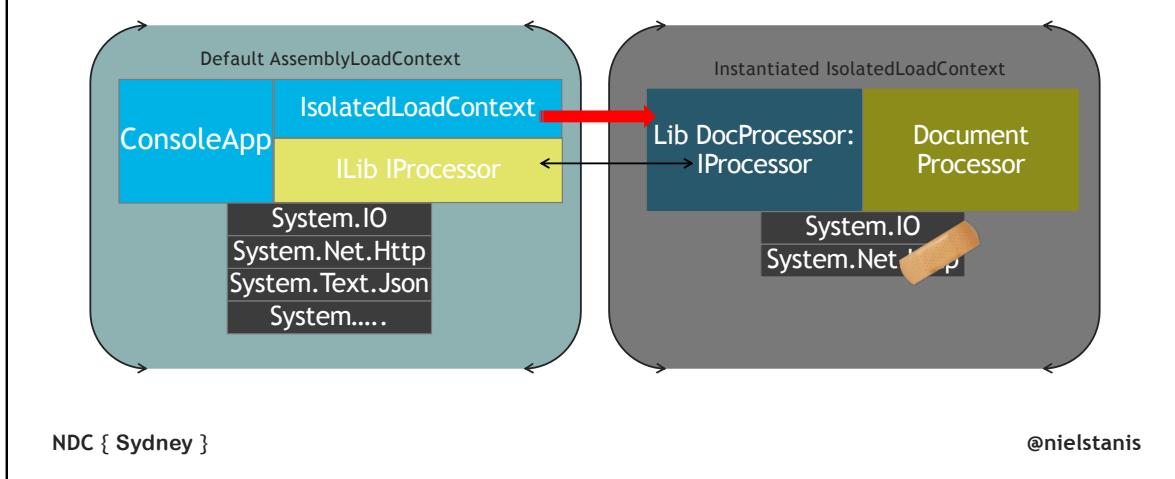
Image: C# logo <https://docs.microsoft.com/en-us/dotnet/csharp/>

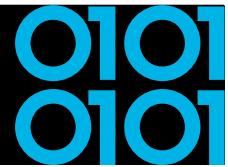


Slide with larger header when there is not a need for heavy text.

The content text slide bullets as preview, however you do not need to bullets. Text is present in Trebuchet size 14, bullets may be removed if not needed.

ConsoleApp & Sandboxed Library





Slide with larger header
when there is not a need
for text heavy.

The content text slide
bullets as preview, however
you do not need to
bullets. Text is present
Trebuchet size 14,
bullets may be removed
not needed.

Conclusion

- Update libraries; security problems get fixed
- Integrate security into your development lifecycle
- Know what libraries are used, where and what's inside
and most important what you'd expect from it.

NDC { Sydney }

@nielstanis



Slide with larger header
when there is not a need
for heavy text.

The content text slide
bullets as preview, so
you do not need to
bullets. Text is present
Trebuchet size 14,
bullets may be removed
not needed.

Conclusion

- **Futures of this Sandbox Concept**
 - Easier developer integration (e.g. source generator)
 - Package + good guidance on how this can be used in different application contexts like ASP.NET Core.
 - Basic patches/policy that can be applied on libraries

NDC { Sydney }

@nielstanis

010101010101010101010101010101
01 VERACODE 0101010101010101010101
0101010101010101010101010101010101

Thanks! Questions?

<https://github.com/nielstanis/ndcsydney2022>
ntanis at veracode.com
@nielstanis on Twitter

