National Cyber Security Centre
a part of GCHQ

Practical Security Architecture Design

Security design principles and patterns from the NCSC

National Cyber Security Centre
a part of GCHQ

Agenda

- How NCSC approaches security architecture design
- The malware mitigation techniques that underpin our approach
- Our design principles
- Putting those things together

National Cyber Security Centre
a part of GCHQ

Security architecture

- It's technical architecture, focused on achieving security goals
- It's about ***designing*** systems to be secure (note: **building** and **operating** systems securely are equally important aspects)
- It's best when security architects have knowledge or experience of how hard it is to **find** and **exploit** vulnerabilities

National Cyber Security Centre
a part of GCHQ

Security architecture in practice

Architectural patterns

- Reference solutions for common security problems
- Hard to create, easy to use
- e.g. web applications, remote access solutions

Architectural principles

- For everything else
- e.g. Distributed identity verification – GOV.UK Verify
- e.g. The land registry – who owns which plot of land

National Cyber Security Centre
a part of GCHQ

Security principles prior art

National Cyber Security Centre
a part of GCHQ

Defense in depth

National Cyber Security Centre

a part of GCHQ

Least privilege

National Cyber Security Centre
a part of GCHQ

Attack surface minimisation

National Cyber Security Centre

a part of GCHQ

Howard & LeBlanc's Principles

Writing Secure Code, 2nd Edition, Howard & LeBlanc, 2001

National Cyber Security Centre
a part of GCHQ

Howard and LeBlanc's Principles

1. Learn from Mistakes
2. Minimize Your Attack Surface
3. Employ Secure Defaults
4. Use Defense in Depth
5. Use Least Privilege
6. Backward Compatibility Will Always Give You Grief
7. Assume External Systems Are Insecure
8. Plan on Failure
9. Fail to a Secure Mode
10. Remember That Security Features != Secure Features
11. Never Depend on Security Through Obscurity Alone
12. Don't Mix Code and Data
13. Fix Security Issues Correctly

National Cyber Security Centre
a part of GCHQ

Our turn

1. Things to get right first (to have a hope)
2. Security architecture design goals
3. Malware mitigation techniques
4. Security design principles

National Cyber Security Centre
a part of GCHQ

Things to get right first

Understand your service, the needs it meets, and the data you need to operate it

Have a clear, **end-to-end** understanding of your service and how it is accessed.

Don’t forget:

- End user devices
- Third party access or admin
- Those random network security appliances that might MITM your comms
- Copies of data

Understand the role your suppliers play in securing your service

National Cyber Security Centre
a part of GCHQ

Security architecture design goals

Make services hard to compromise

Reduce the impact of a compromise

Make compromises easy to detect

Make services hard to disrupt

National Cyber Security Centre
a part of GCHQ

Malware mitigation techniques

National Cyber Security Centre
a part of GCHQ

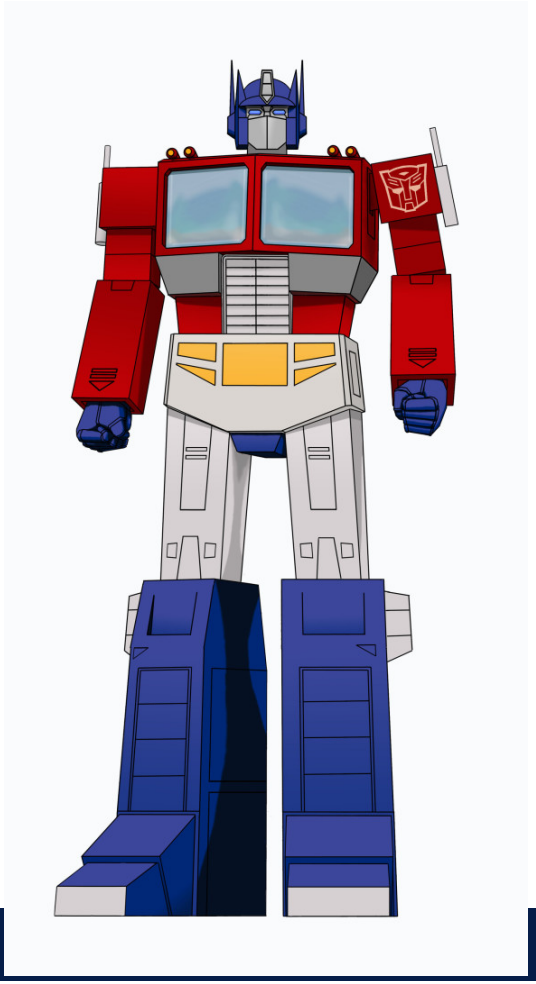
Identify

- Authenticate that messages are from a trusted source
- Example:
  - Check a signature to confirm the origin
  - Authenticate the channel over which the message is received

National Cyber Security Centre
a part of GCHQ

Transform

- Convert between formats with the intention that no original content remains
- Malware present shouldn't survive the transformation
- Example:
  - PDF->Series of Bitmaps



National Cyber Security Centre
a part of GCHQ

Verify

- Check validity of the format, structure and content of a message
- Not AV scanning!
- XML example:
  - Valid XML,
  - Message meets XML schema
  - Elements and attributes are within expected parameters

National Cyber Security Centre
a part of GCHQ

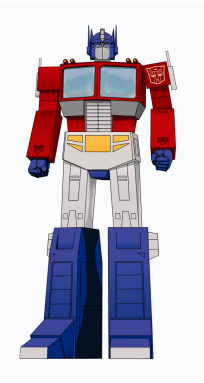
Render

- Handle untrusted content with care
- Parse it in a fume cupboard

National Cyber Security Centre
a part of GCHQ

Malware mitigation model

Identify → Transform → Verify → Render

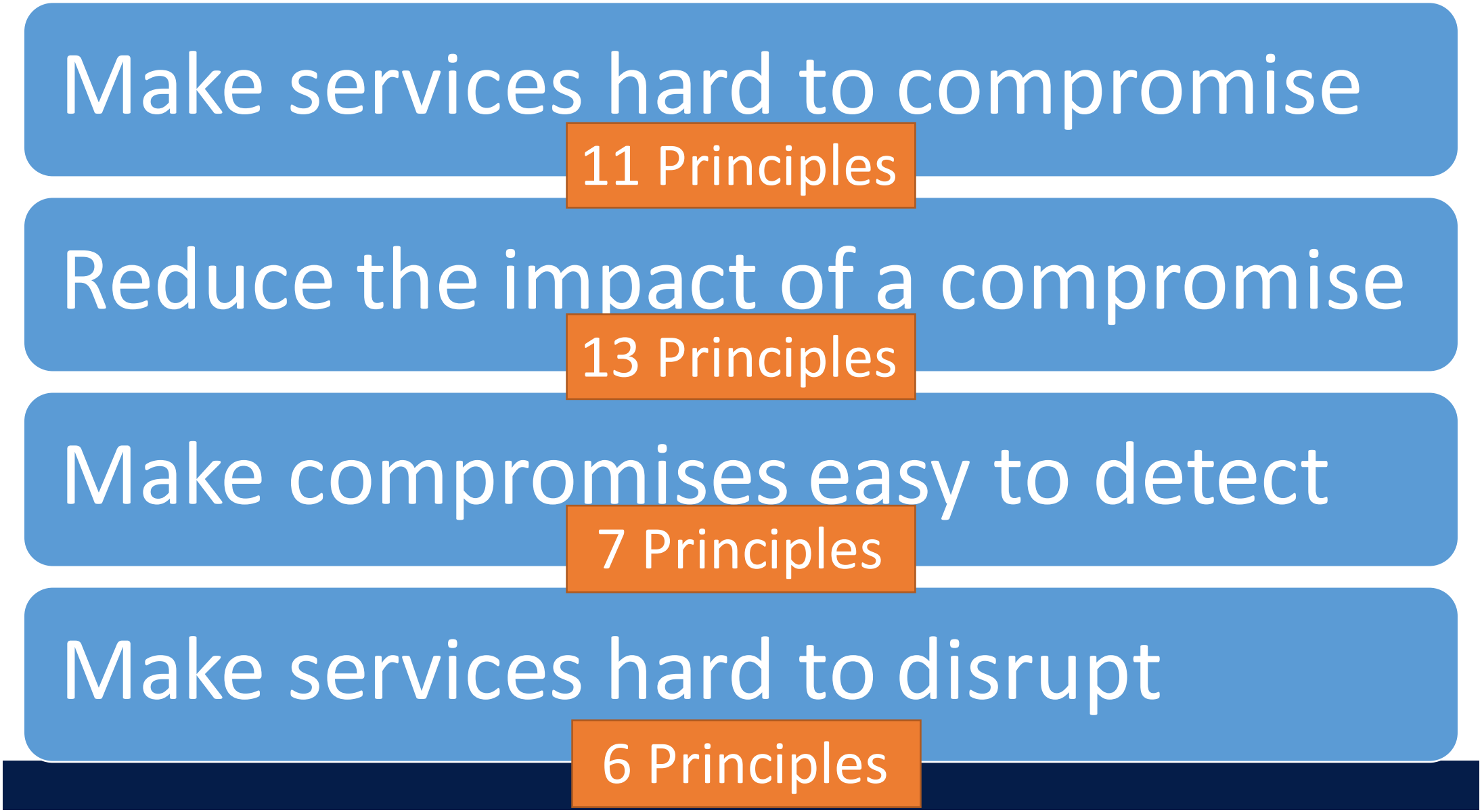


National Cyber Security Centre

a part of GCHQ

Security design principles

March 2016


Make services hard to compromise
11 Principles
Reduce the impact of a compromise
13 Principles
Make compromises easy to detect
7 Principles
Make services hard to disrupt
6 Principles

National Cyber Security Centre
a part of GCHQ

Some favourites

National Cyber Security Centre

a part of GCHQ

Making systems hard to compromise

Validate or transform all external input before processing it.

National Cyber Security Centre

a part of GCHQ

Making systems hard to compromise

Design for easy maintenance.

National Cyber Security Centre
a part of GCHQ

Making compromises easy to detect

Protect management/operations environments from spear-phishing and watering-hole attacks.

National Cyber Security Centre
a part of GCHQ

Reducing the impact of a compromise

Build your service using a segmented approach.

National Cyber Security Centre
a part of GCHQ

Reducing the impact of a compromise

Anonymise data when it's exported to reporting tools.

National Cyber Security Centre
a part of GCHQ

Reducing the impact of a compromise

Regularly rebuild components that would have considerable access to data over a long period of time.

National Cyber Security Centre
a part of GCHQ

Reducing the impact of a compromise

Make it easy to recover following a compromise.

National Cyber Security Centre
a part of GCHQ

Making compromises easy to detect

Design simple communication flows between your components.

National Cyber Security Centre
a part of GCHQ

Putting that together

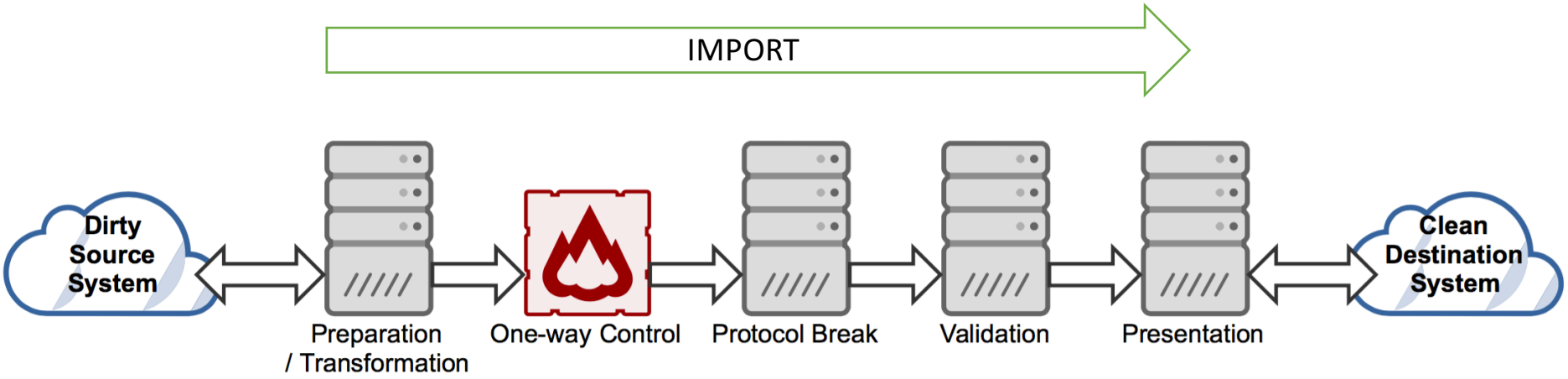
National Cyber Security Centre
a part of GCHQ

How do you safely import data import into a critical system?

Example

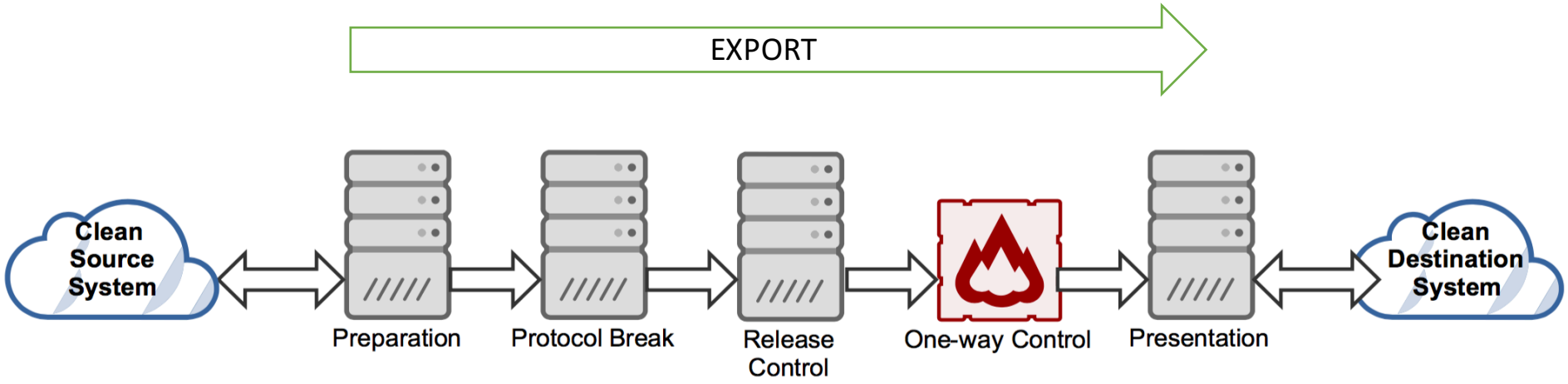
National Cyber Security Centre
a part of GCHQ

Importing data safely



National Cyber Security Centre
a part of GCHQ

Exporting (just the data you want to)



National Cyber Security Centre
a part of GCHQ

Thanks!

Our design principles: https://www.ncsc.gov.uk/designprinciples