# Attack surface

John Slankas
jbslanka@ncsu.edu

Design Flaw #9: Understand how external components change your attack surface

Slides adopted from Laurie Williams

Computer Science
NC STATE UNIVERSITY

# What is an Attack Surface?

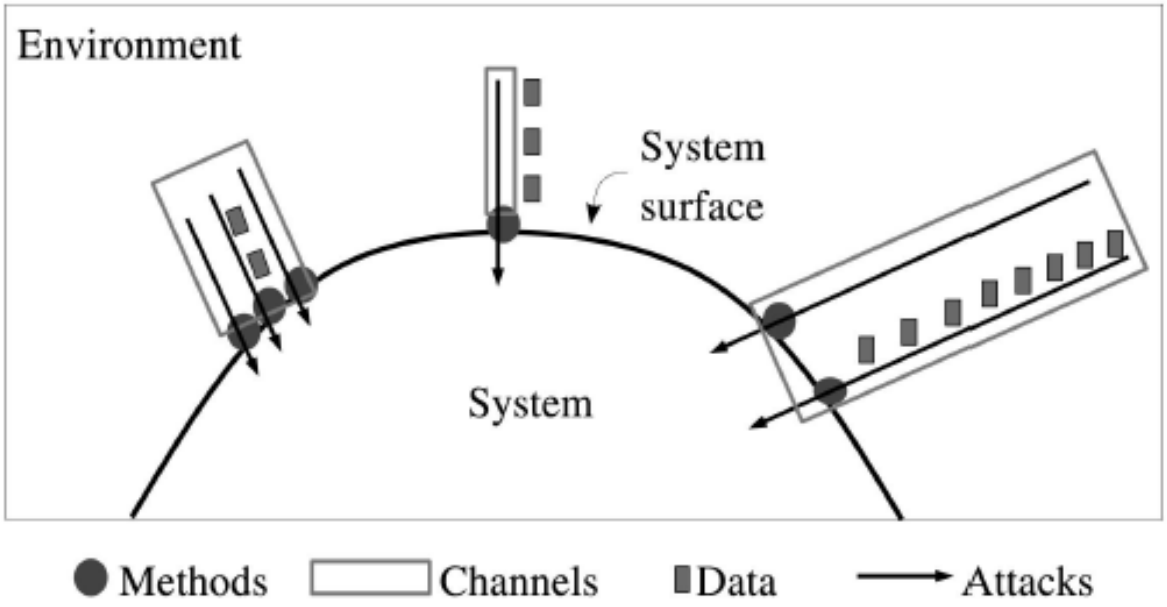



Fig. 2. A system's attack surface is the subset of the system's resources (methods, channels, and data) potentially used in attacks on the system.

Entry and exit points of a program/system

P. K. Manadhata and J. M. Wing, "An Attack Surface Metric," *IEEE Transactions of Software Engineering*, vol. 27, no. 3, pp. 371-386, May/June 2011.

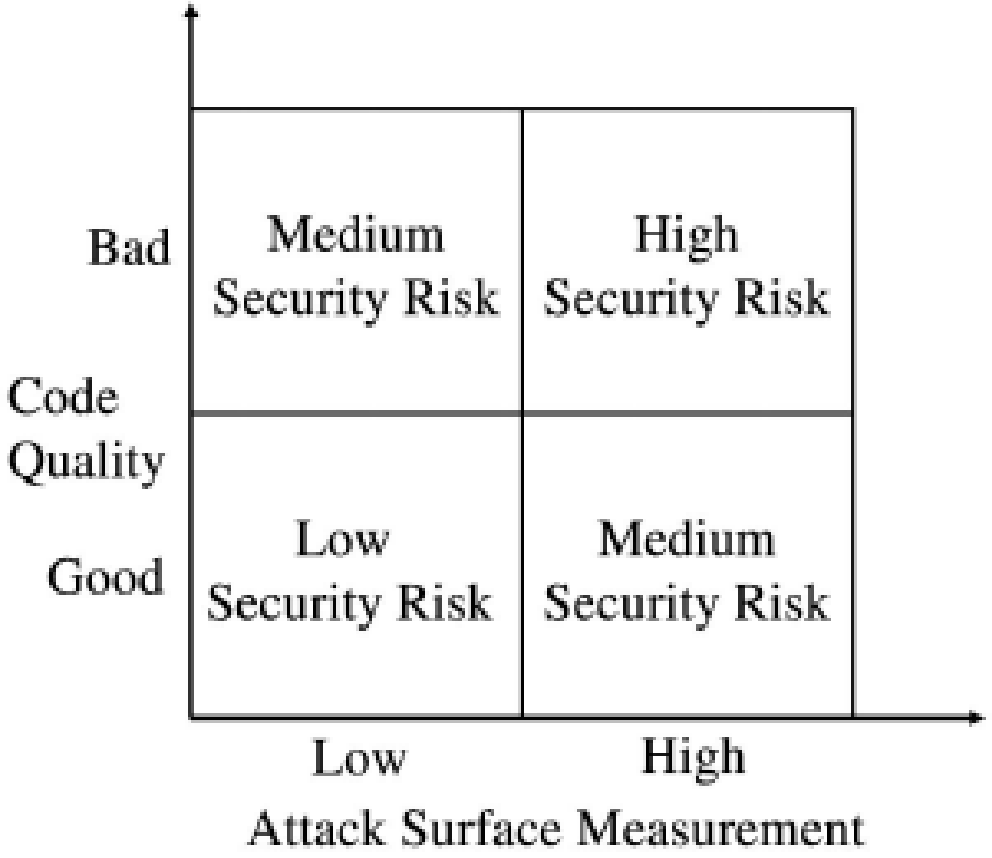
# Considering the attack surface

- the sum of all paths for data/commands into and out of the application;
  - the code that protects these paths (including resource connection and authentication, authorization, activity logging, data validation and encoding);
- all valuable data used in the application, including secrets and keys, intellectual property, critical business data, personal data and personally identifiable information (PII); and
  - the code that protects these data (including encryption and checksums, access auditing, and data integrity and operational security controls)

# Attack surface analysis

- To understand and manage application security risks as applications and operating systems are designed and changed in a software system. The goal is to close all but required entry and exit points leading to and from system assets and to constrain others with access rights, monitoring, and response

# Security Risk




Protecting from exploitation of future vulnerabilities

P. K. Manadhata and J. M. Wing, "An Attack Surface Metric," *IEEE Transactions of Software Engineering*, vol. 27, no. 3, pp. 371-386, May/June 2011.

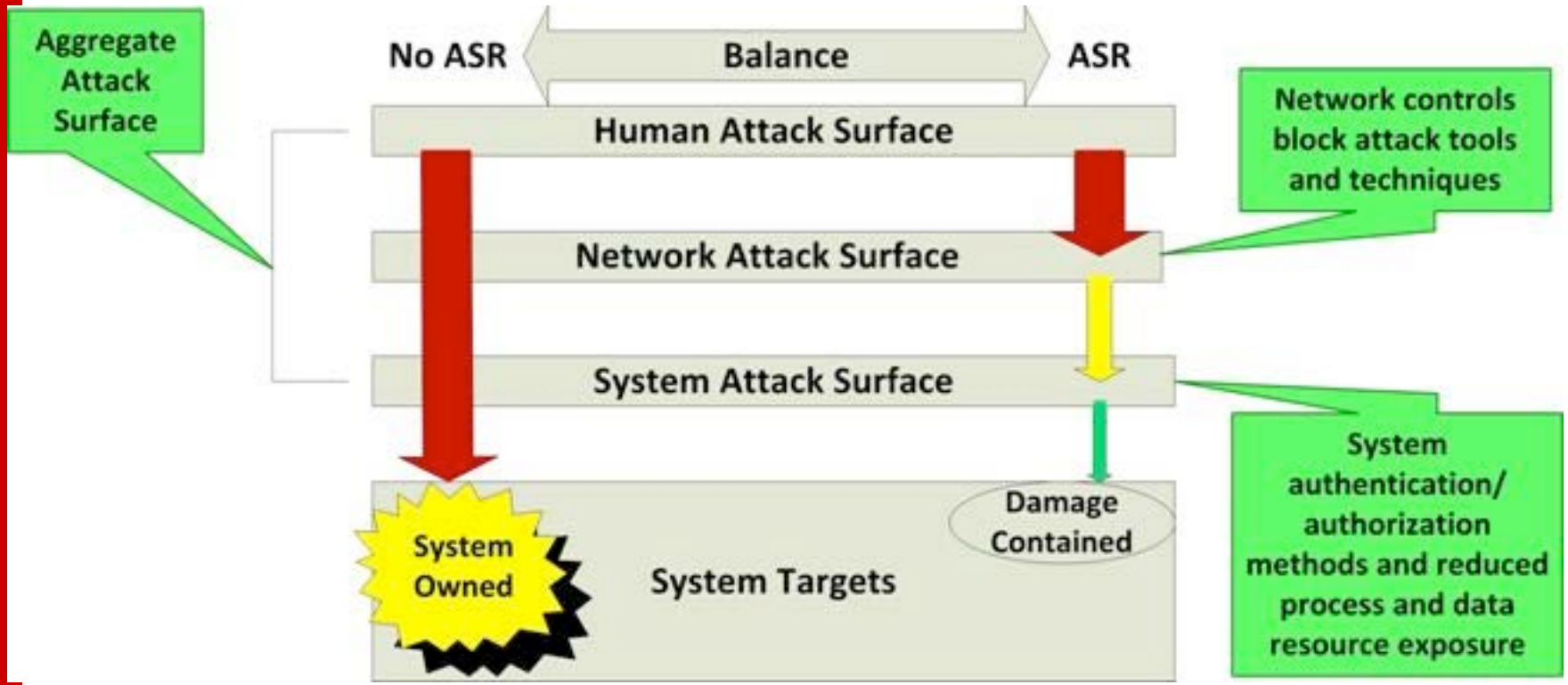
# How to reduce the attack surface

- Keep entry and exit points to a minimum and allow users to enable functionality as needed.
  - Number of open sockets (TCP and UDP)
  - Number of open named pipes
  - Number of open remote procedure call (RPC) endpoints
  - Number of services
  - Number of services running by default
  - Number of services running in elevated privileges
  - Number of dynamic content Web pages
  - Number of account you add to administrator's group
  - Number of files, directories, and registry keys with weak access control lists

# Attack Surface Comparison

| High Attack Surface | Low Attack Surface |
|---|---|
| Features running by default | Feature off by default |
| Open network connections | Closed all unnecessary connections |
| System always on | System intermittently on, as needed |
| Anonymous access | Authenticated access |
| Code running will full admin privileges | Code running under “least-privilege” account |
| Uniform defaults | User-chosen settings, secure by default |
| Larger code | Smaller code |
| Weak Access Control Lists (ACLs) | Strong Access Control Lists (ACLs) |

# Defense in depth and the attack surface




http://resources.infosecinstitute.com/attack-surface-reduction/

# Components Change the Attack Surface

- OTS components, platform, applications
- Third party open source or proprietary libraries
- Widgets and gadgets loaded at runtime as part of a web project
- Software developed by a different team
- Software your team developed at a different point in time

… as binaries, source code, API …

# What to do …

- Isolate components as much as possible
- Configure to only open functionality you will use
- If the component cannot be configured to comply with your security policy, don't use it
- Look at vulnerability history in CVE database
- Maintain up-to-date components
- Maintain a healthy distrust
- Authenticate dataflow
- Consider data coming in untrusted

# Document / Inventory

# Example

From: Steve

Date: 9/22/2015 4:59PM

To: John

Subject: DataVerse and Curation

John,

One of the goals for the Metrology CCT is to inventory data at LAS.

We'd like to get an instance of Dataverse up to allow us to evaluate it for our use.

Is that something y'all can help with?

Thanks,

Steve

# References


- M. Howard, "Mitigate Security Risks by Minimizing the Code You Expose to Untrusted Users," MSDN Magazine, November 2004, http://msdn.microsoft.com/en-us/magazine/cc163882.aspx.
- M. Howard, "Threat Models Improve Your Security Process," MSDN Magazine, November 2008, http://msdn.microsoft.com/en-us/magazine/dd148644.aspx - id0080033.
- M. Howard, J. Pincus, and J. Wing, "Measuring Relative Attack Surfaces," in *Computer Security in the 21st Century*: Springer, 2005, pp. 109-137.
- P. K. Manadhata and J. M. Wing, "An Attack Surface Metric," *IEEE Transactions of Software Engineering*, vol. 27, no. 3, pp. 371-386, May/June 2011.


- ADD DESIGN FLAWs