presented by

Microsoft

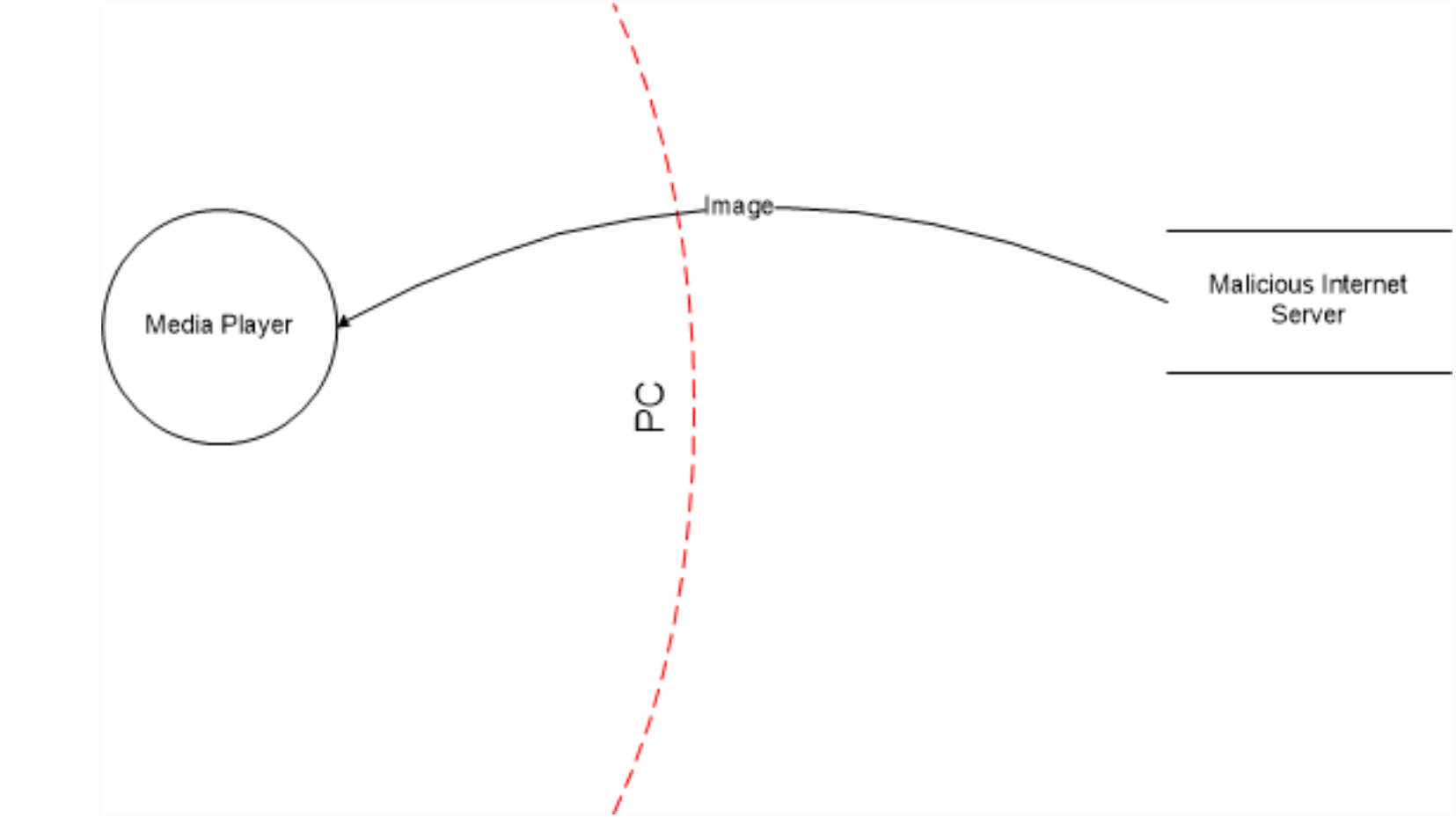
Windows

Hardening the UEFI Attack Surface

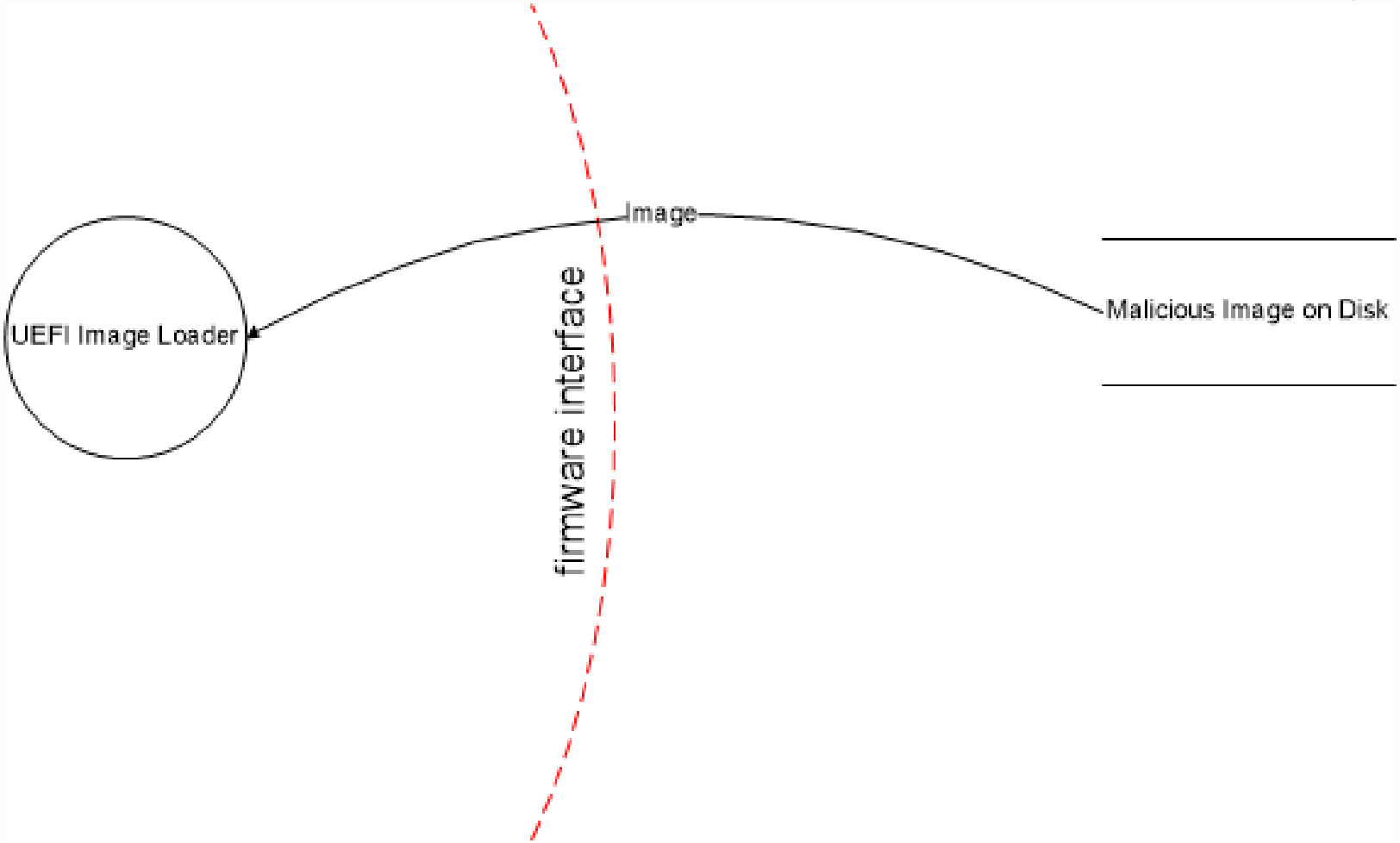
How to Harden an Attack Surface

- Threat Modeling
- Secure Coding
- Security Code Audits
- Fuzz Testing
- Software Security Defenses

Media Player Threat Model



UEFI Threat Model



Secure Coding (one aspect)

Validation of untrusted input!

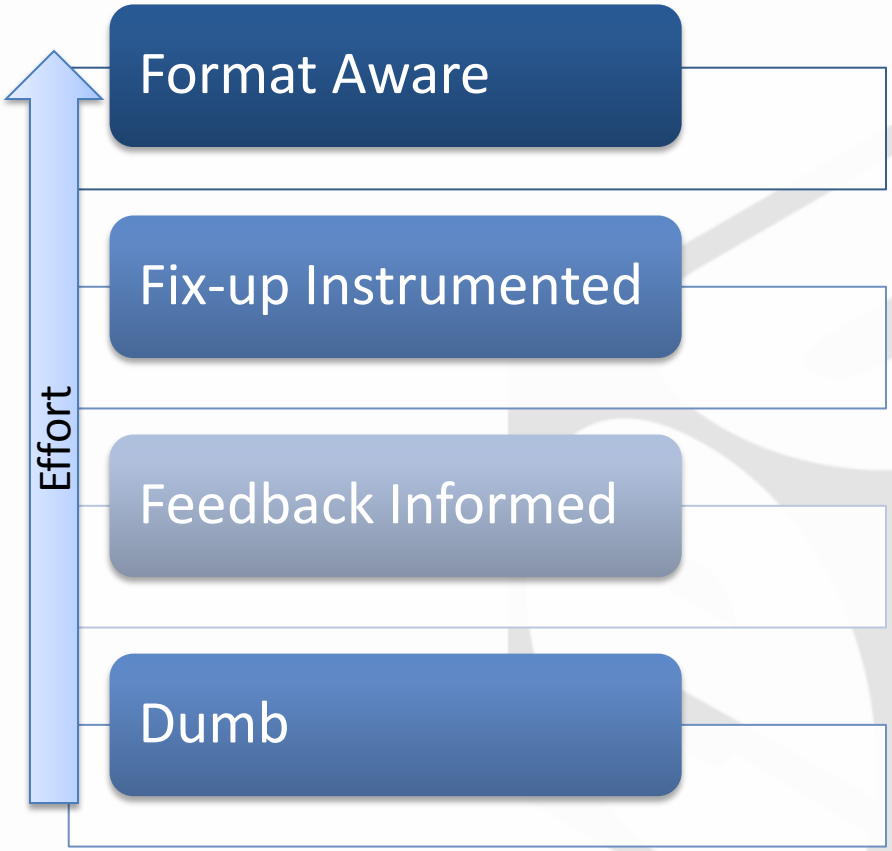
Poor validation of untrusted input may result in:

- Buffer overflows
- Integer and pointer corruption
- Memory overwrites
- …

Leading to:

- Compromised runtime integrity of authenticated components
- …

Fuzz Testing



Applying malformed data against the attack surface

Software Security Defenses

- Writing Secure Code
- Stack Buffer Overrun Detection (GS)
- Data Execution Prevention (DEP/NX)
- Address Space Layout Randomization (ASLR)
- Heap Corruption Detection
- Migration to Safer Functions

Tianocore Revisions of Interest

Revisions of interest EDK2 trunk between 2012/01/01 and 2012/04/15. It is important to review these changes and, if the revision is applicable to implementations, integrate them.

12927
13094
13095
13104
13109
13110
13120
13144
13156
13157
13158
13162
13185

How to Harden and Attack Surface

- **Secure Coding:** helps to avoid problems
  Guidelines for Writing Secure Code: http://msdn.microsoft.com/en-us/library/ms182020.aspx
  Writing Secure Code: http://msdn.microsoft.com/en-us/security/aa570401
  Safe Integer Arithmetic in C: http://blogs.msdn.com/b/michael_howard/archive/2006/02/02/523392.aspx
- **Threat Modeling**: helps to define trust boundaries and potentially malicious data input points
  http://www.microsoft.com/security/sdl/adopt/threatmodeling.aspx
- **Security Code Audits**: helps identify vulnerabilities through manual code inspection
  http://technet.microsoft.com/en-us/library/cc723542.aspx
  http://blogs.msdn.com/b/sdl/archive/2011/10/19/code-analysis-for-all.aspx
- **Fuzz Testing**: helps find input parsing and other vulnerabilities
  http://msdn.microsoft.com/en-us/testing/cc162782.aspx
- **Software Security Defenses**: helps provide blanket protection against some threats
  http://msdn.microsoft.com/en-us/library/bb430720.aspx