presented by

Microsoft

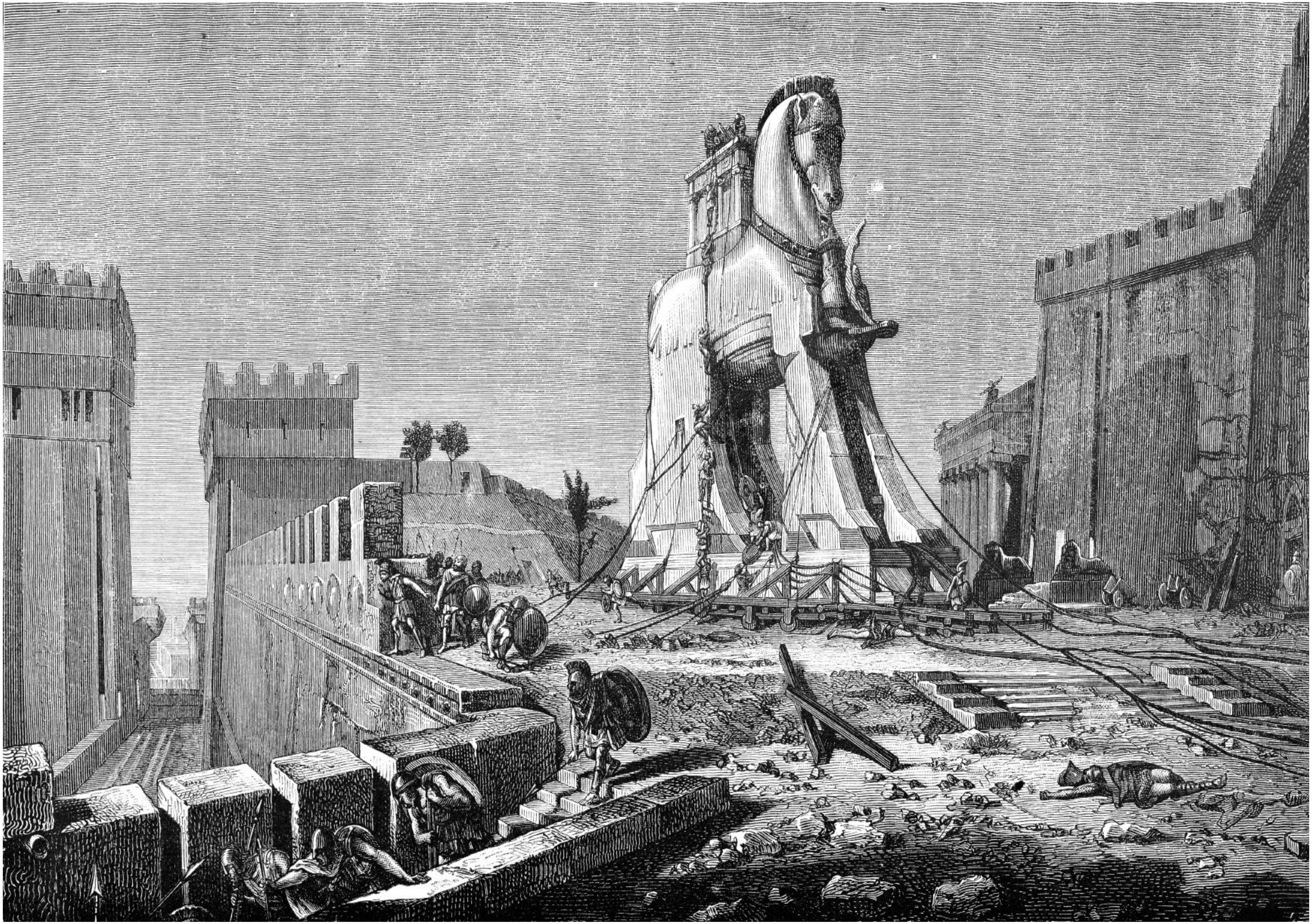
Windows

Hardening The Attack Surface

UEFI Winter Plugfest – February 21-23, 2012
Presented by

Douglas MacIver

Principal Test Engineer, Microsoft Corp.

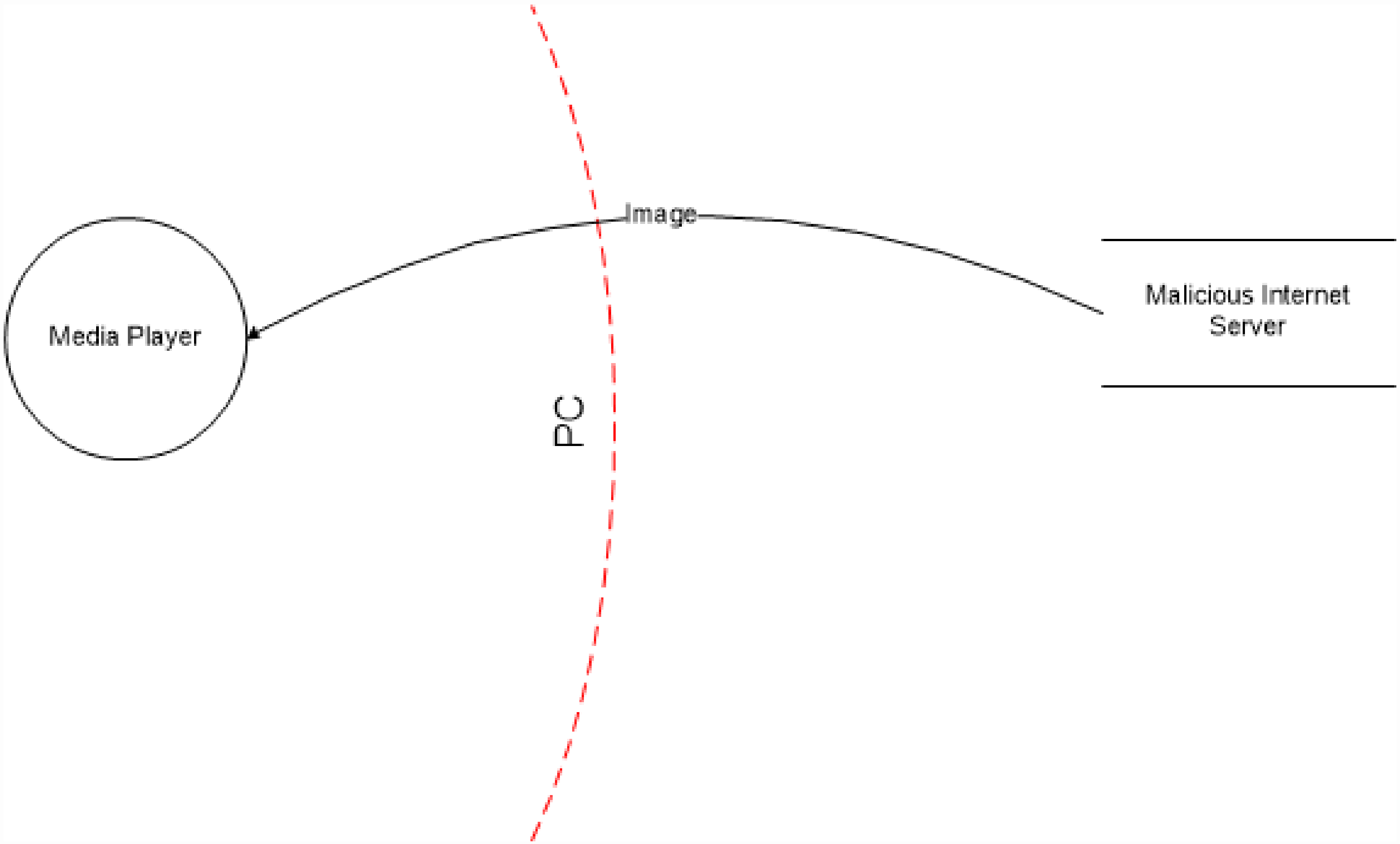


Harden Attack Surface

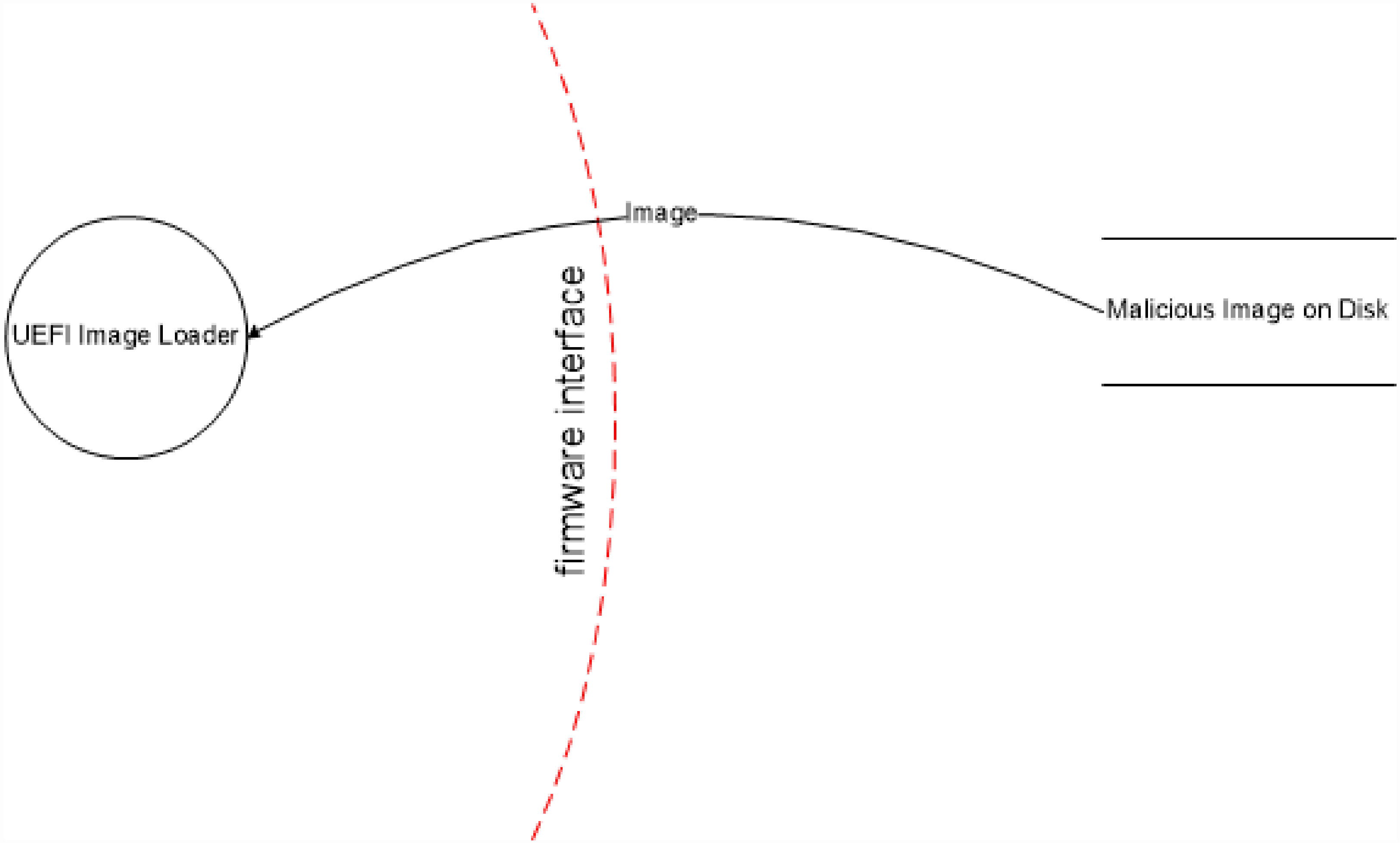
How to Harden an Attack Surface

- 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
- …

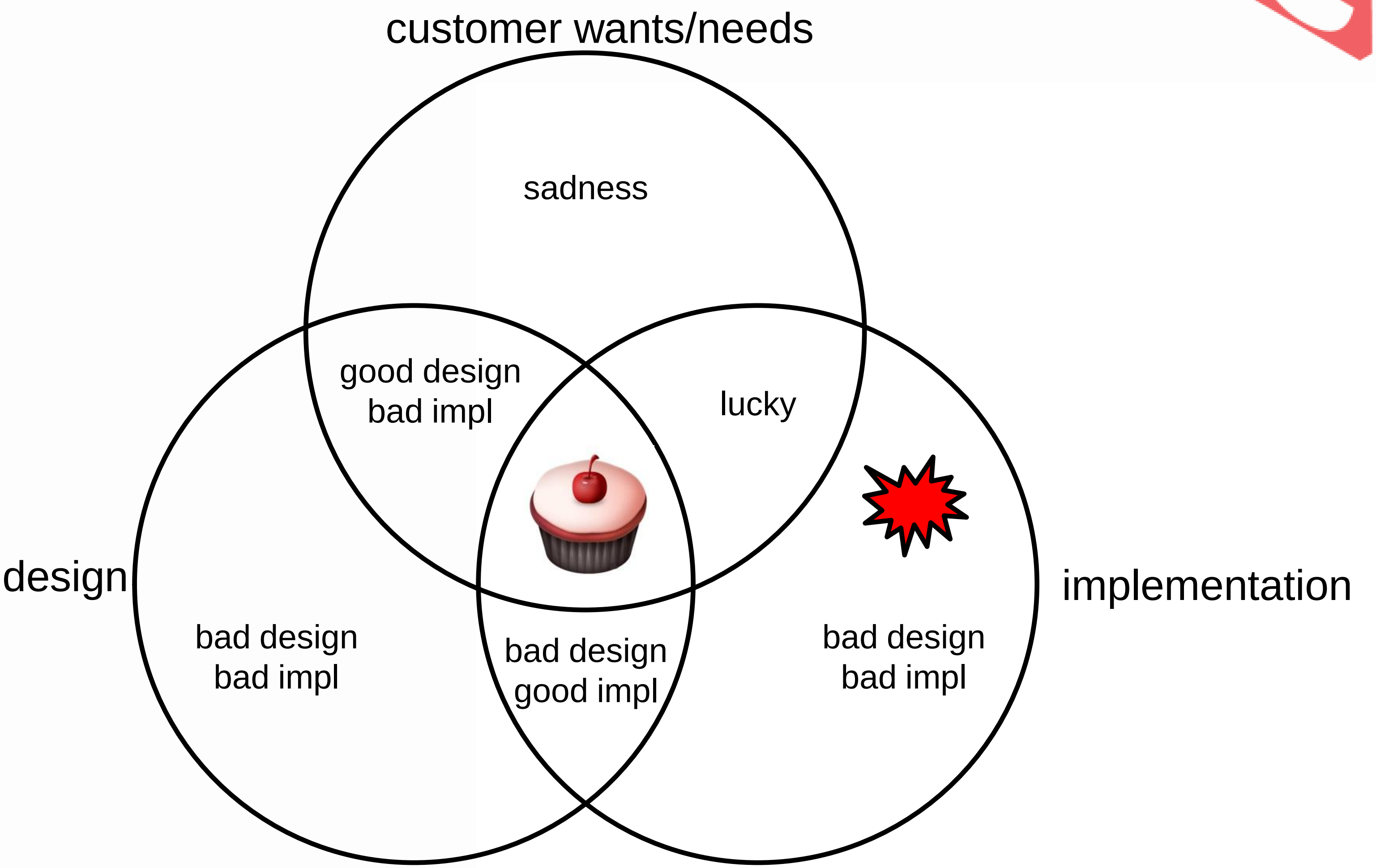
Security Code Audits

```
UINT32 FindJamInBlob(BLOB* Blob, size_t BlobSize)
{
      UINT32 JamOffset;

      JamOffset = Blob->Start + Blob->Hdr.Size;

      return JamOffset;
}
```

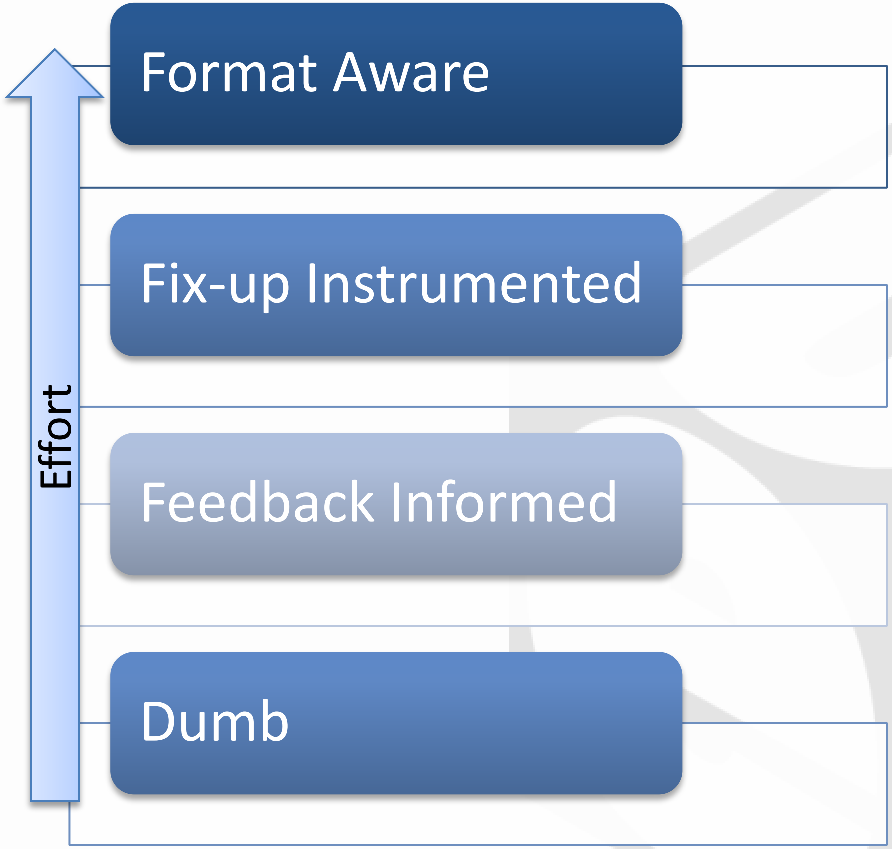
First, ask questions

Second, identify vulnerabilities

Venn and the Art of Security Testing



Fuzz Testing


Effort

Format Aware

Fix-up Instrumented

Feedback Informed

Dumb

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

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

Harden Attack Surface

Thanks for attending the UEFI Winter Plugfest 2012

For more information on the Unified EFI Forum and UEFI Specifications, visit http://www.uefi.org

presented by

Microsoft

Windows