Hardening The Attack Surface

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

Douglas MacIver
Principal Test Engineer, Microsoft Corp.
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

UEFI Image Loader → Image → firmware interface → Malicious Image on Disk
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
  – ...

UEFI Plugfest – February 2012
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

- Customer wants/needs
- Design
  - Good design
    - Good impl
  - Bad design
    - Bad impl
- Implementation
  - Bad design
    - Bad impl
- Sadness
- Lucky

- Design: a cupcake.
- Implementation: a red explosion symbol.
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
How to Harden and Attack Surface

- **Secure Coding:** helps to avoid problems

- **Threat Modeling:** helps to define trust boundaries and potentially malicious data input points

- **Security Code Audits:** helps identify vulnerabilities through manual code inspection

- **Fuzz Testing:** helps find input parsing and other vulnerabilities

- **Software Security Defenses:** helps provide blanket protection against some threats
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