Developing secure software
A practical approach

Juan Marcelo da Cruz Pinto

Security Architect

Argentina Software Development Center

Legal notice

Intel® Active Management Technology requires the computer system to have an Intel(R) AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications of implementation of new business processes. With regard to notebooks, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off.

BunnyPeople, Celeron, Celeron Inside, Centrino, Centrino Inside, Core Inside, i960, Intel, the Intel logo, Intel AppUp, Intel Atom, Intel Atom Inside, Intel Core, Intel Inside, the Intel Inside logo, Intel NetBurst, Intel NetMerge, Intel NetStructure, Intel SingleDriver, Intel SpeedStep, Intel Sponsors of Tomorrow., the Intel Sponsors of Tomorrow. logo, Intel StrataFlash, Intel Viiv, Intel vPro, Intel XScale, InTru, the InTru logo, InTru soundmark, Itanium, Itanium Inside, MCS, MMX, Moblin, Pentium, Pentium Inside, skoool, the skoool logo, Sound Mark, The Journey Inside, vPro Inside, VTune, Xeon, and Xeon Inside are trademarks of Intel Corporation in the U.S. and other countries.

*Other names and brands may be claimed as the property of others.

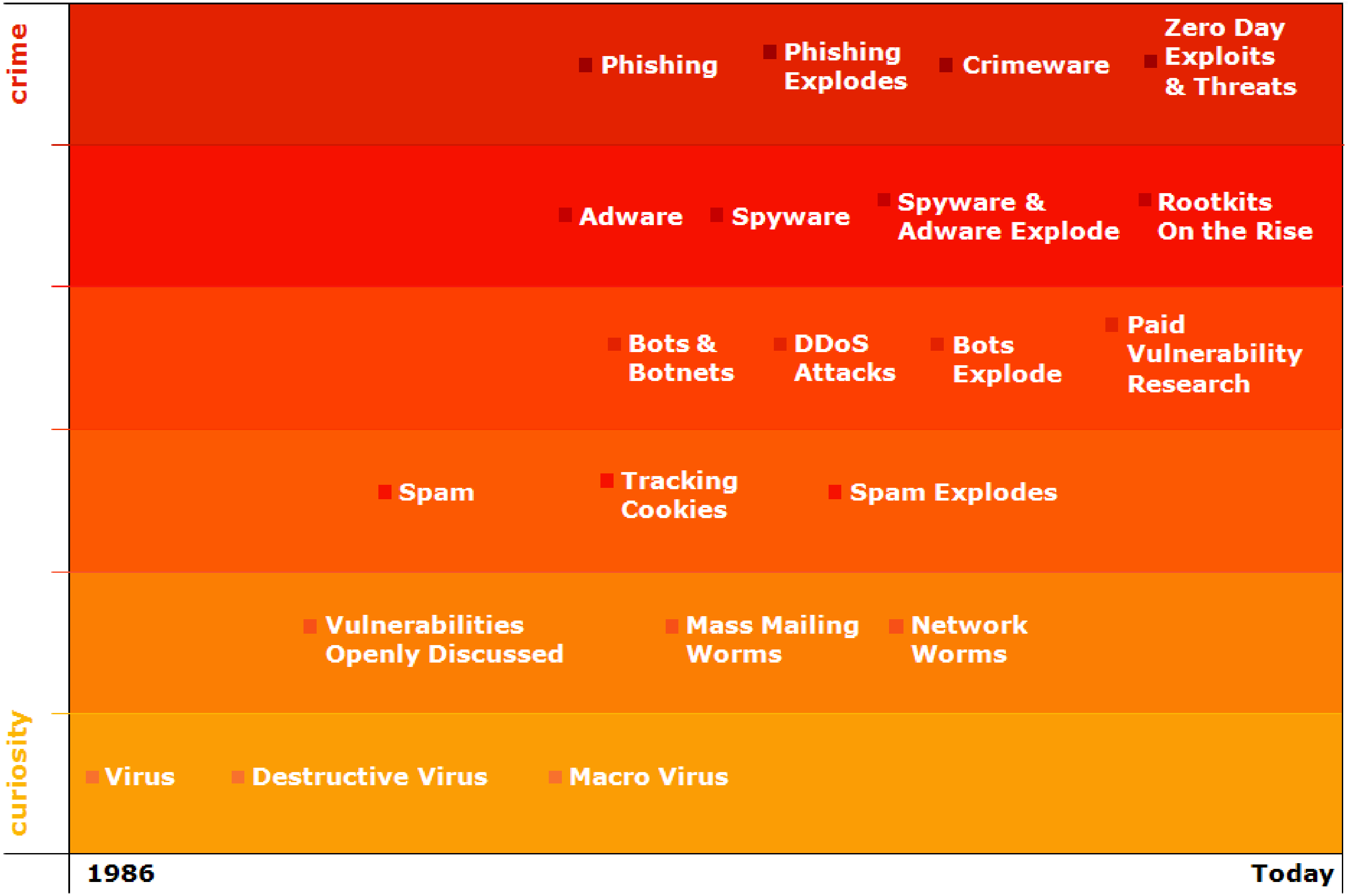
Goals & Expectations

- Evangelize secure software development
- This is not a talk about how to use technology “X” to make software more secure
  - You can apply this in every platform/system
  - You can apply this in every programming language
- By the end of this talk (hopefully ☺), you will:
  - Have a better understanding of the threats that we (software/firmware/hardware developers) face today
  - Understand the processes that support secure software development in a company such as Intel
  - Have a set of “seeds” (tools, guidelines, links) you can use to improve the quality of code
  - Become an secure software development evangelizer yourselves

BTW, What is “Secure Software”?

Source: Symantec JWIS 2007*

The evolution of computer threats



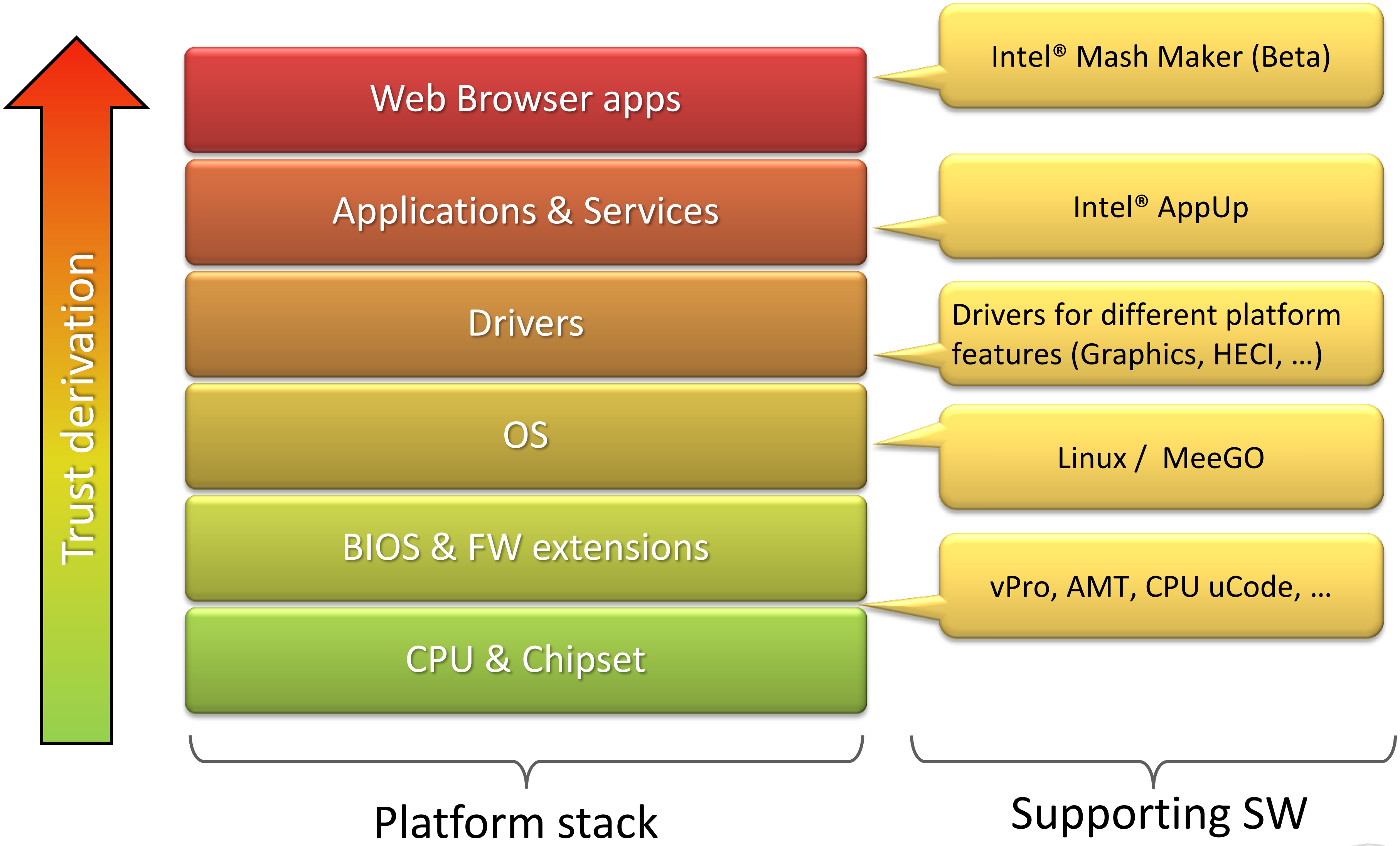
Huge explosion in the number and type of attacks

The evolution of computer threats (cont.)

- Software depends on hardware to provide protection: Rings, Intel® TXT (root of trust), vPro™ (manageability), VT (virtualization), …
- With hardened OS, savvy attackers move down stack
- Detection and patching can be difficult or impossible
- Intel has large, global deployment footprint

Intel develops both <u>hardware</u> and <u>software</u>

The Hardware/Software stack



Trust derivation

Web Browser apps

Applications & Services

Drivers

OS

BIOS & FW extensions

CPU & Chipset

Intel® Mash Maker (Beta)

Intel® AppUp

Drivers for different platform features (Graphics, HECI, …)

Linux / MeeGO

vPro, AMT, CPU uCode, …

Platform stack

Supporting SW

Hardware hacks in the news…

Security research community in action

- “TPM chips used for encryption hacked” (February 2010)
  - Presented at Black Hat 2010 (http://www.blackhat.com/presentatio 10/Tarnovsky_Chris/BlackHat-DC-2010-Tarnovsky-DASP-slides.pdf)
  - Using acid to remove plastic protection, removing silicon substrate and using a *electron microscope* to analyze circuitry and advanced protection

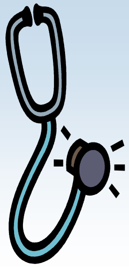
Source: http://www.flylogic.net/blog/

- “GoodFET for Wireless Keyboard Sniffing” (Black Hat 2011, TBP)
  - To be presented at Black Hat 2011 (Travis Goodspeed, https://www.blackhat.com/html/bh-us-11/bh-us-11-arsenal.html#Goodspeed)
  - Sniffing wireless keyboards

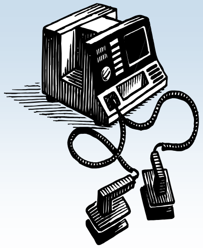
Source: http://travisgoodspeed.blogspot.com/ - http://goodfet.sourceforge.net

Intel Security Assurance Framework

Prevent ▶ Prevent security and privacy issues from being created



Detect ▶ Detect security & privacy issues prior to release



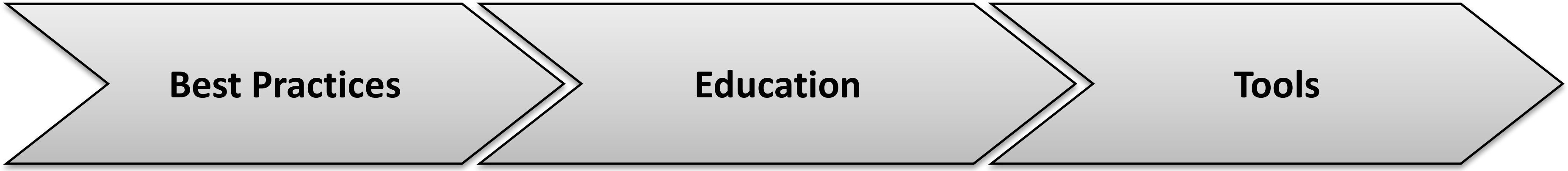
Survive ▶ Survive security & privacy issues after release

Intel Security Center of Excellence

(SeCoE)

Design for Security (DFS)

Definition: Application of security best practices by knowledgeable teams throughout the development lifecycle to continuously improve product security



Security Development Lifecycle

- Concept
- Architecture
- Design
- Implementation
- Support

Security Policy / Guidance

- Product Development
- Cryptography
- Incident handling
- Many others

Security Training

- Requirements
- Architecture
- SW Coding
- Evaluation
- HW Security

Security Newsletter

- Learn from issues
- Trends in security
- Sharing best practices

Architecture

- Threat modeling

Implementation

- Klocwork K7
- Threat Analysis Automation

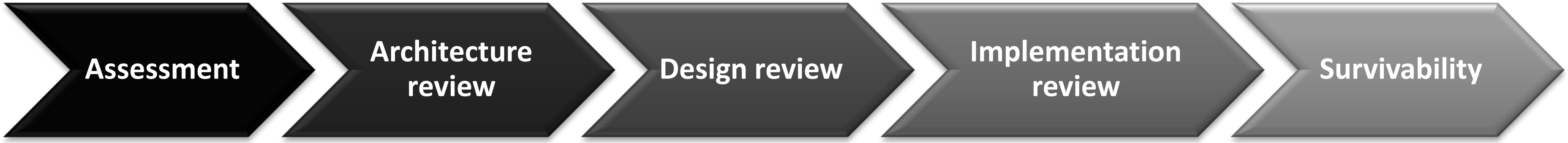
Evaluation

- Open source attack tools
- Fuzzing frameworks

Enable Teams to Engineer More Secure Products

Intel Security Development Lifecycle (SDL)

- Tailored version of Microsoft* SDL (http://www.microsoft.com/security/sdl/default.aspx)
  - Adds the hardware/firmware twist to the mix
- What it provides?
  - Guidelines and development process modifications for including periodic security checkpoints
  - Guidance in all of the development stages (from requirements to release)
  - Ensures that products meet the stated and assumed security and privacy requirements



Assessment

Architecture review

Design review

Implementation review

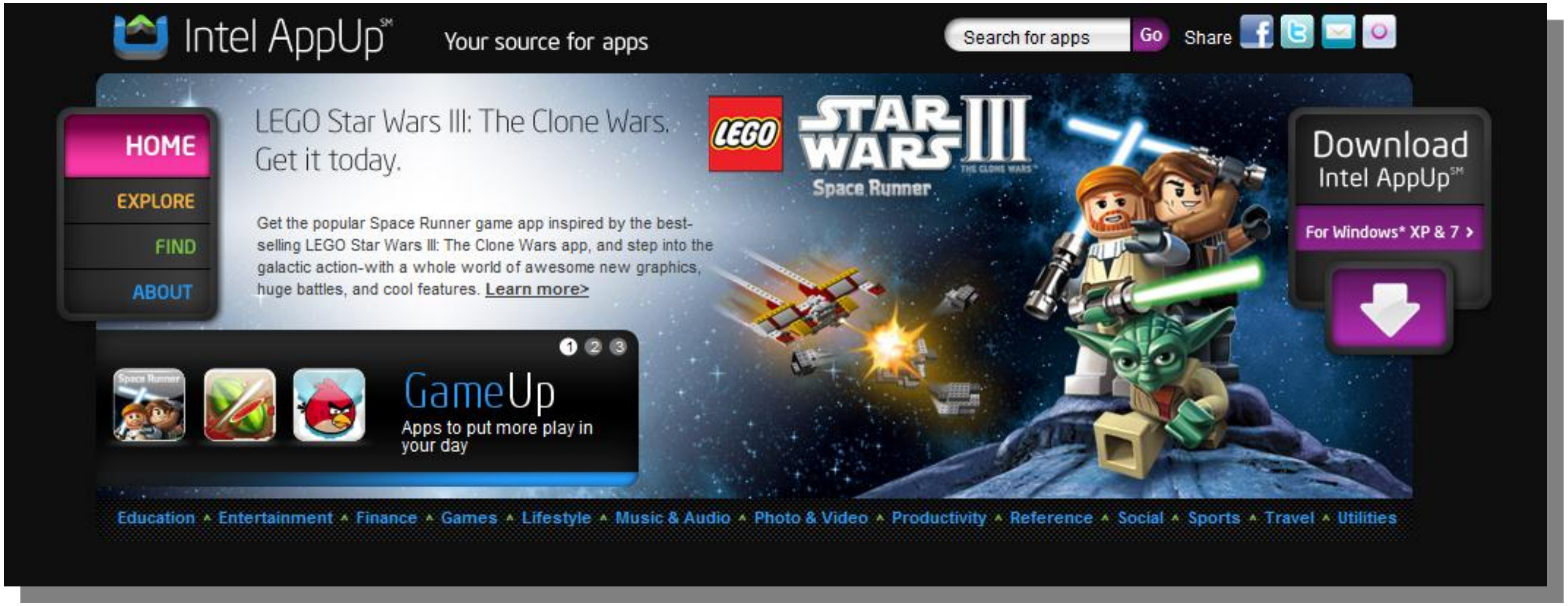
Survivability

SDL can also be agile

A case study: The Intel® AppUp(SM)

Source: http://www.appup.com/ (July 2011)

Con sabor a peperina ☺



Intel AppUp℠ Your source for apps

Search for apps Go Share

HOME

EXPLORE

FIND

ABOUT

LEGO Star Wars III: The Clone Wars. Get it today.

Get the popular Space Runner game app inspired by the best-selling LEGO Star Wars III: The Clone Wars app, and step into the galactic action-with a whole world of awesome new graphics, huge battles, and cool features. Learn more>

GameUp Apps to put more play in your day

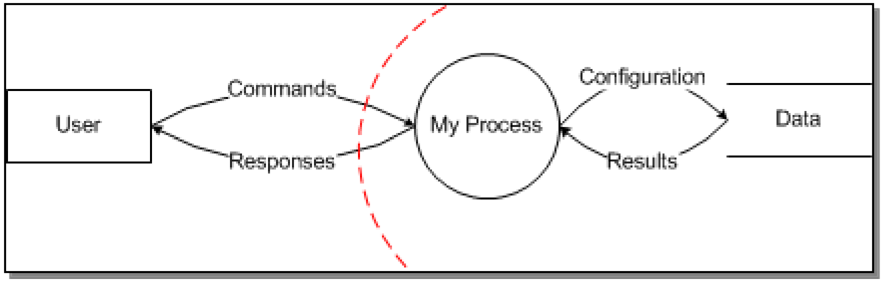
Download Intel AppUp℠ For Windows* XP & 7 >

Education · Entertainment · Finance · Games · Lifestyle · Music & Audio · Photo & Video · Productivity · Reference · Social · Sports · Travel · Utilities

Developed in ASDC

Architecture/Design review

- Requires clear security objectives
  - What does the customer expect from the product/technology?
  - Matching the business objectives: This is the tricky part



*Source: Microsoft SDL Threat Modeling Tool **

- Strong focus on threat modeling
  - Analyze use cases, identify risks, specify requirements
  - Methodologies: STRIDE, Attack Trees, CIA

- **Outcome**: List of security requirements to be built into the architecture

Key: Threat modeling

Architecture/Design review

Tools & Assets

- Tools
  - Microsoft* SDL Threat Modeling Tool: http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=2955#Overview
  - Microsoft* Threat Analysis & Modeling Tool: http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=14719
  - SeaMonster*: http://sourceforge.net/projects/seamonster/
- Guides
  - OWASP*: https://www.owasp.org/index.php/Threat_Risk_Modeling

Implementation review

- Requires tools for static source code analysis
  - Integration of static analysis tools and the build environment
  - Keeping track of vulnerabilities in the code

- Strong focus on static analysis and code reviews
  - Fixing static analysis vulnerabilities is a high impact / low cost activity

```
// source: http://www.linuxjournal.com/article/6701

void function (char *str) {
   char buffer[16];
   strcpy (buffer, str);
}
int main () {
  char *str = "I am greater than 16 bytes"; // length of str = 27 bytes
  function (str);
}
```

- **<u>Outcome</u>**: Static analysis reports and finding documentation

Key: Static analysis, Code review & Penetration testing

Implementation review

Tools & Assets

- **CWE/SANS Top 25 Most Dangerous Software Errors (2011)**
  - SQL Injection
  - OS Command Injection
  - Buffer Overflow
  - Cross-Site Scripting (XSS)
  - Missing Authentication / Authorization
  - Hard-coded credentials
  - Missing encryption for sensitive data
  - Lack of input validation
  - Execution with unnecessary privileges
  - Cross-Site Request Forgery
  - Download of Code Without Integrity Check
  - …

Implementation review

Tools & Assets (cont.)

- Source Code Analysis
  - Klocwork*
  - FxCop*
  - CAT.NET*
- Binary Analysis
  - Valgrind*
  - BinScope*
- Fuzz Testing
  - Peach* framework: http://peachfuzzer.com/

Ship review

- Requires the product release criteria to include a metric for security findings
  - Understand the impact of unaddressed vulnerabilities

- Strong focus on building a survivability plan
  - What to do in case of an incident?
  - How to report vulnerabilities?
  - How to patch system's software once in the field?

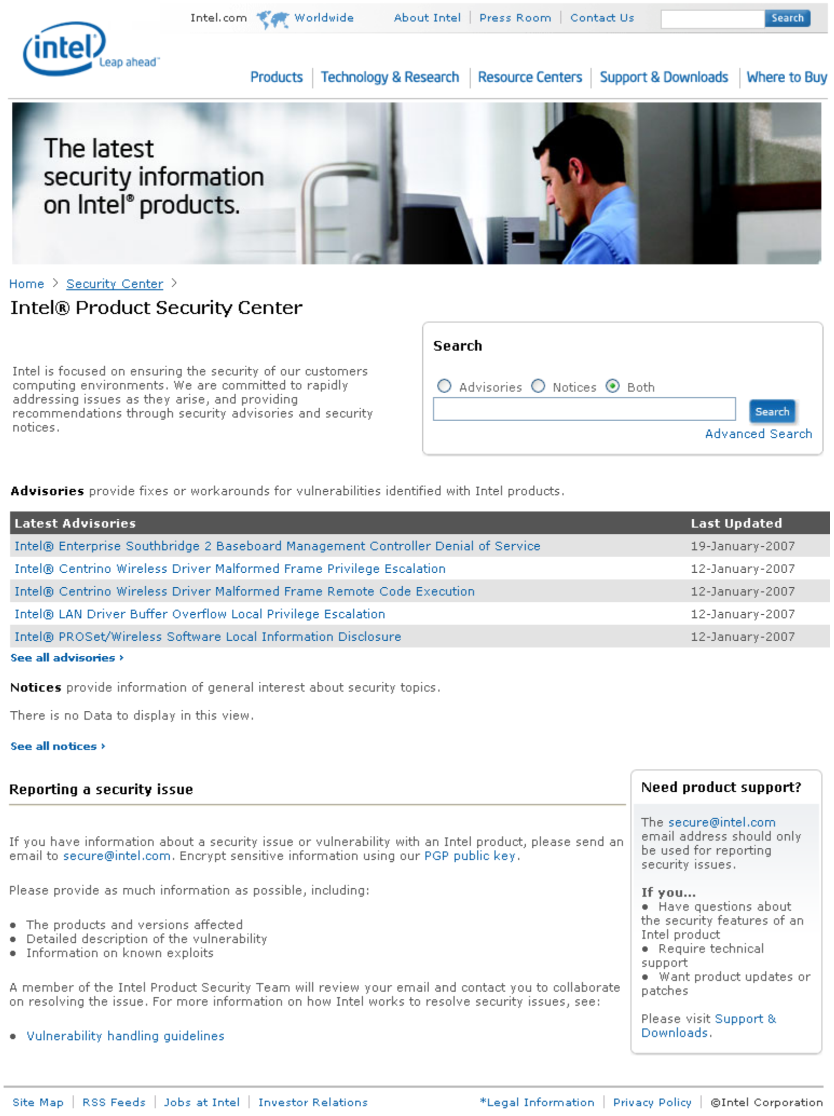
- **<u>Outcome</u>**: Survivability and incident response plan

Key: Survivability plan

Intel’s PSIRT

www.intel.com/security:

- **Engage security community**
  - Standard reporting process
  - Working with researchers
  - Open & active engagement
- **Address security vulnerabilities**
  - Internally identified and externally reported
  - BKMs for impact assessment through resolution
- **Avenue to disseminate security information**
  - Publication of Security Advisories and Notices


Intel.com
Worldwide
About Intel | Press Room | Contact Us
Search
intel Leap ahead™
Products | Technology & Research | Resource Centers | Support & Downloads | Where to Buy
The latest security information on Intel® products.
Home > Security Center >
Search
○ Advisories ○ Notices ● Both
Search
Advanced Search
Site Map | RSS Feeds | Jobs at Intel | Investor Relations
*Legal Information | Privacy Policy | ©Intel Corporation

Intel® Product Security Center

Intel is focused on ensuring the security of our customers computing environments. We are committed to rapidly addressing issues as they arise, and providing recommendations through security advisories and security notices.

Advisories provide fixes or workarounds for vulnerabilities identified with Intel products.

Latest Advisories	Last Updated
Intel® Enterprise Southbridge 2 Baseboard Management Controller Denial of Service	19-January-2007
Intel® Centrino Wireless Driver Malformed Frame Privilege Escalation	12-January-2007
Intel® Centrino Wireless Driver Malformed Frame Remote Code Execution	12-January-2007
Intel® LAN Driver Buffer Overflow Local Privilege Escalation	12-January-2007
Intel® PROSet/Wireless Software Local Information Disclosure	12-January-2007

See all advisories ›

Notices provide information of general interest about security topics.

There is no Data to display in this view.

See all notices ›

Reporting a security issue

If you have information about a security issue or vulnerability with an Intel product, please send an email to secure@intel.com. Encrypt sensitive information using our PGP public key.

Please provide as much information as possible, including:

- The products and versions affected
- Detailed description of the vulnerability
- Information on known exploits

A member of the Intel Product Security Team will review your email and contact you to collaborate on resolving the issue. For more information on how Intel works to resolve security issues, see:

- Vulnerability handling guidelines

Need product support?

The secure@intel.com email address should only be used for reporting security issues.

If you...

- Have questions about the security features of an Intel product
- Require technical support
- Want product updates or patches

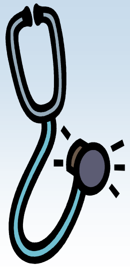
Please visit Support & Downloads.

Wrapping up

Prevent

Prevent security and privacy issues from being created

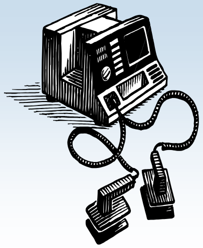
Architecture review: Threat modeling



Detect

Detect security & privacy issues prior to release

Impl. review: Static analysis and pen test



Survive

Survive security & privacy issues after release

Ship review: survivability plan

Intel Security Center of Excellence

(SeCoE)

Training & continuous improvement (DFS)

Summary / Q&A

- Threats are evolving, and secure software development processes need to evolve and adapt as well
- Following a secure development process provides a set of milestones focused on reducing the risk of the product and identifying risks earlier in the lifecycle
- Team up with the security research community: they will always be one step ahead

Back
up

More resources

- OWASP: https://www.owasp.org/
- CWE/SANS: http://cwe.mitre.org/
  - Top 25 most dangerous software errors: http://cwe.mitre.org/top25/
  - Monster mitigations: http://cwe.mitre.org/top25/mitigations.html
- Threat modeling
  - SeaMonster*: http://sourceforge.net/projects/seamonster/
  - Microsoft* SDL Threat Modeling Tool: http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=2955#Overview
  - Microsoft* Threat Analysis & Modeling Tool: http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=14719