Mitigating ICS Vulnerabilities Through IDS/IPS Signatures

May 8, 2012

Nate Kube
Founder and CTO
Wurldtech

Alexander Damisch
Director Industrial
Wind River

Mike Ahmadi
VP Operations
GraniteKey

wurldtech

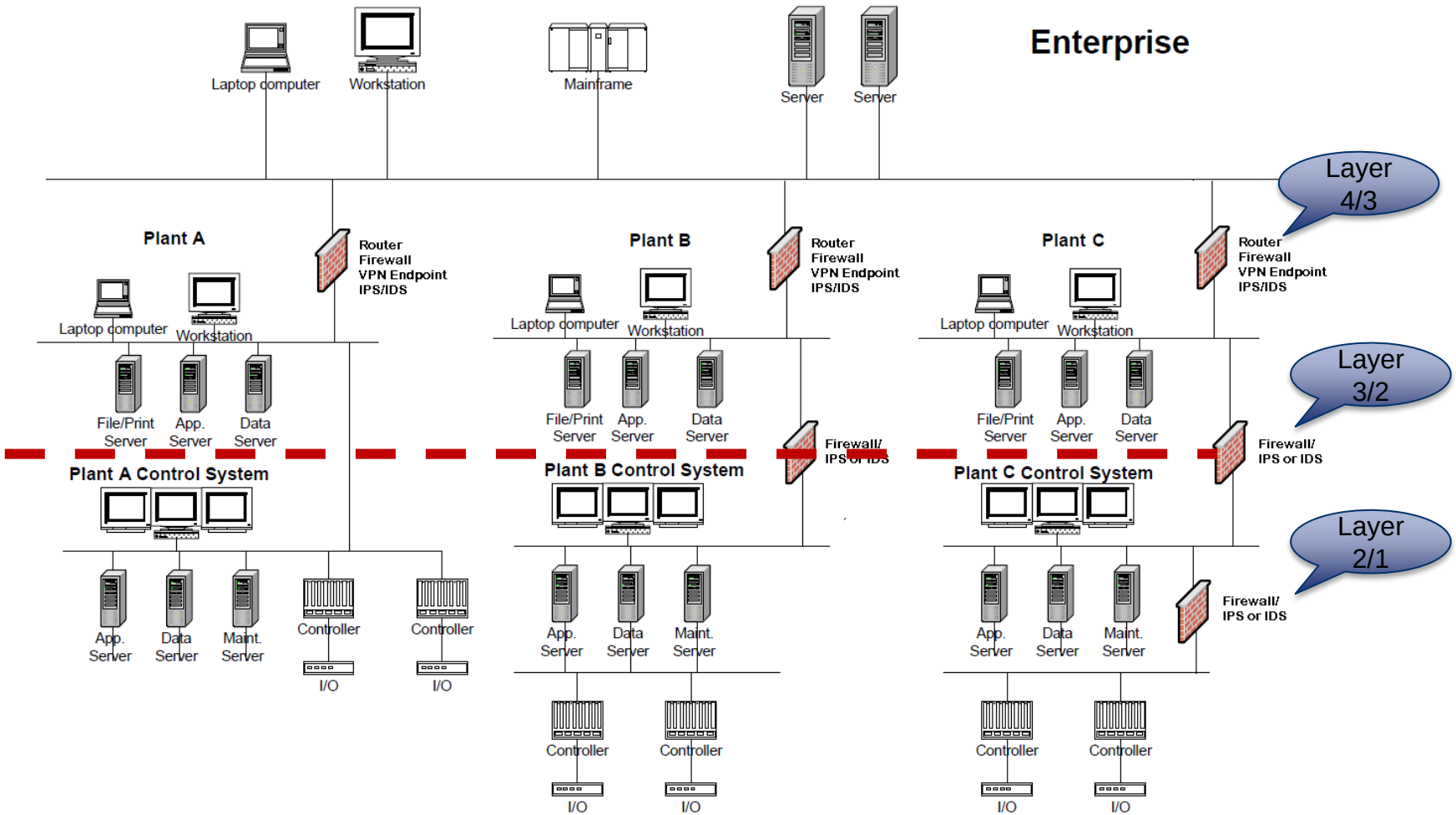
WIND RIVER

Problem Statement

- Operators of Critical Infrastructure Need:
  - Protection against zero day vulnerabilities within hours of the Zero-Day becoming known
  - Protection without the need to patch firmware or shut down operations

- Results:
  - Maximize uptime, throughput, revenue.
  - Ensure correct and safe operation.
  - Protect the IT System from threats from connected Industrial Control system.
  - Reduce corporate risks (for public company - SOX).

Device Protection - RTOS



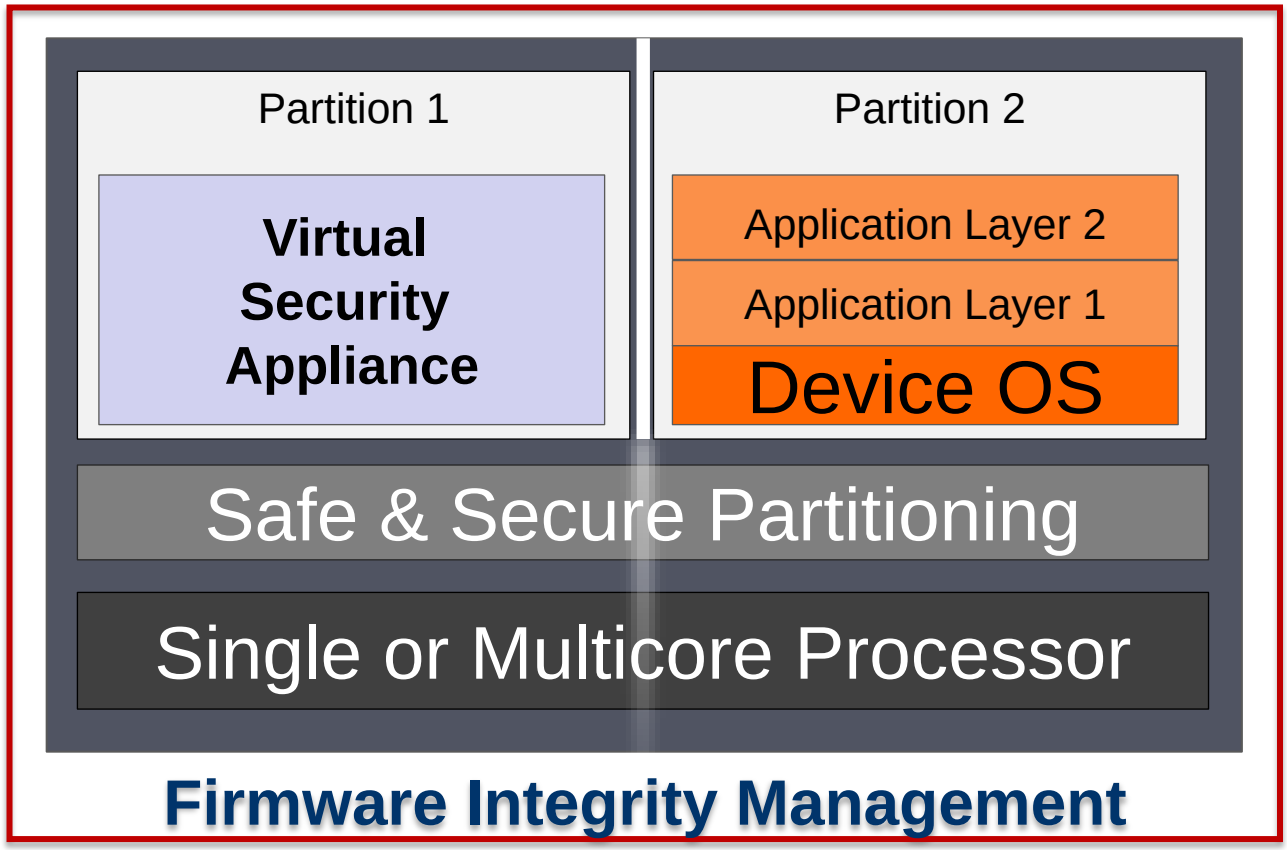
IT Technology versus Industrial Control Systems

Security Control	Information Technology	Control System
Anti-virus	• Very common • Easily deployed	• To high impact • Difficult to deploy
Asset Classification	• State of practice • Result driven investment	• Only if compliance need • Critical asset protection depending on budget
Change Management	• Regular, scheduled	• Non-trivial and expensive • Can be impossible
Incident Response & Forensic	• State of practice • Part of the system	• Non existing, apart from logging
Patch Management	• Enterprise, remote, automated	• Very device/install specific • Very high risk and cost
Security Perimeter	• None (Office) to perfect (Server/CIP)	• Good to very good • Educated insider problem
Secure Design Process	• Yes, took a long time to establish	• Only Functional Safety • Evolving for security
Security Testing & Audit	• Yes	• Evolving
Technology Support Lifetime	• Up to 3 years	• 10 – 30 years

Security Improvement Approach

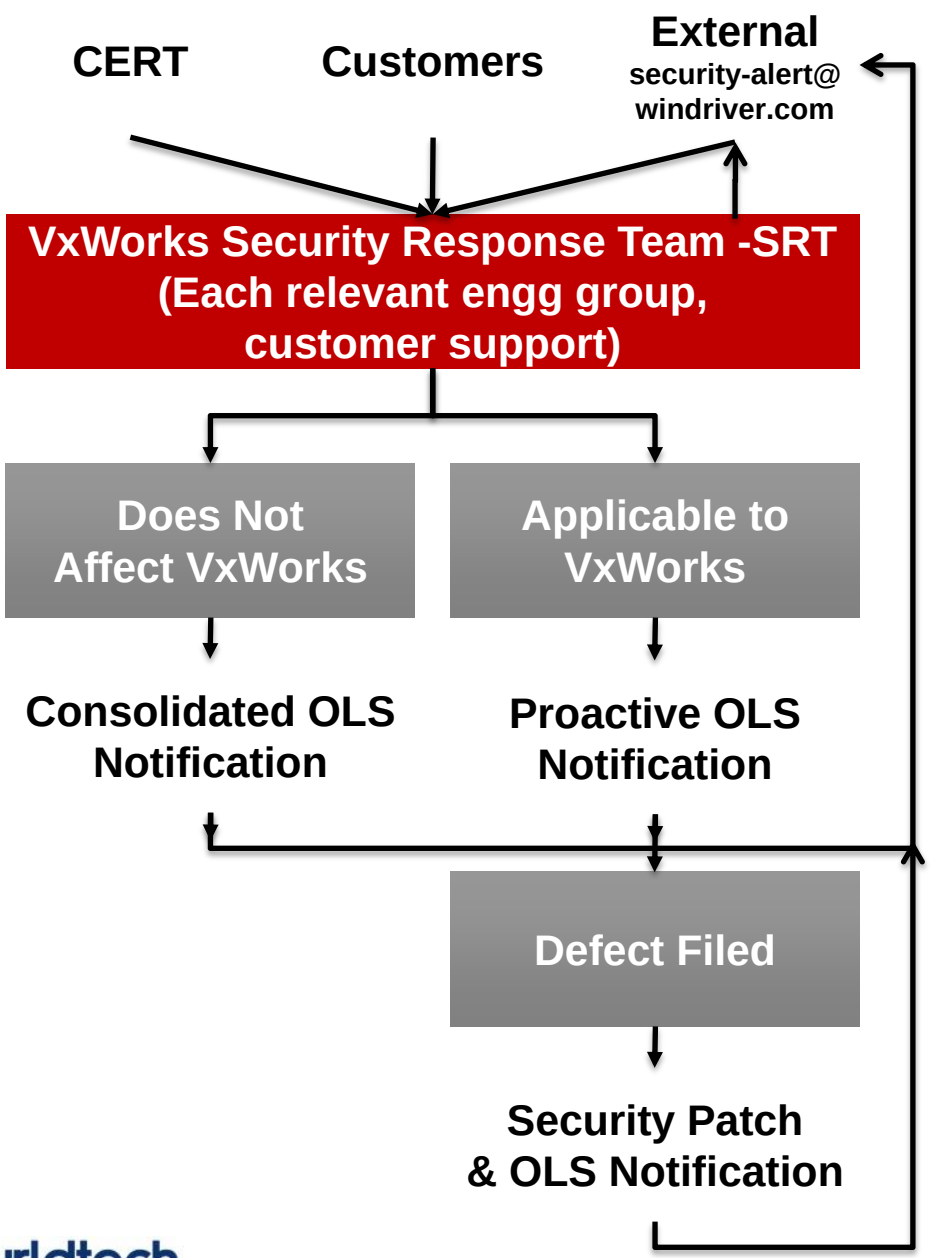
Security Optimized Design: OS Agnostic Partitioning

Separation



Timely response against security incidents

Standard Process for Security Life Cycle

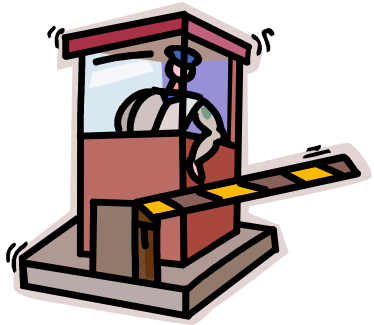


Monitoring

- Wind River actively monitors key lists for vulnerabilities applicable to supported products

Assessment / Prioritization

- Assess, prioritize vulnerabilities and responds with an initial acknowledgement within 1 day of receipt (for External source)
- Prioritization
  - High
  - Medium
  - Low
  - Not Susceptible



Notification

- Proactive notifications for VxWorks vulnerabilities that DO apply at OLS and external party (if applicable)
- Regular consolidated alerts for vulnerabilities that DO NOT affect VxWorks at OLS and external party (if applicable)
- Certain public disclosure restrictions apply to some vulnerabilities (e.g. CERT)

Remediation

- Posting & notification of patch / resolution on OLS and external party (if applicable)

Embedded Vulnerability Management

No firmware patching, but signature loaded by EVM agent

- Data based signature update
- Non intrusive to the running device
- Limiting risk of side effects
- Zero impact after removal

Limit exposure to validated vulnerabilities of specific devices

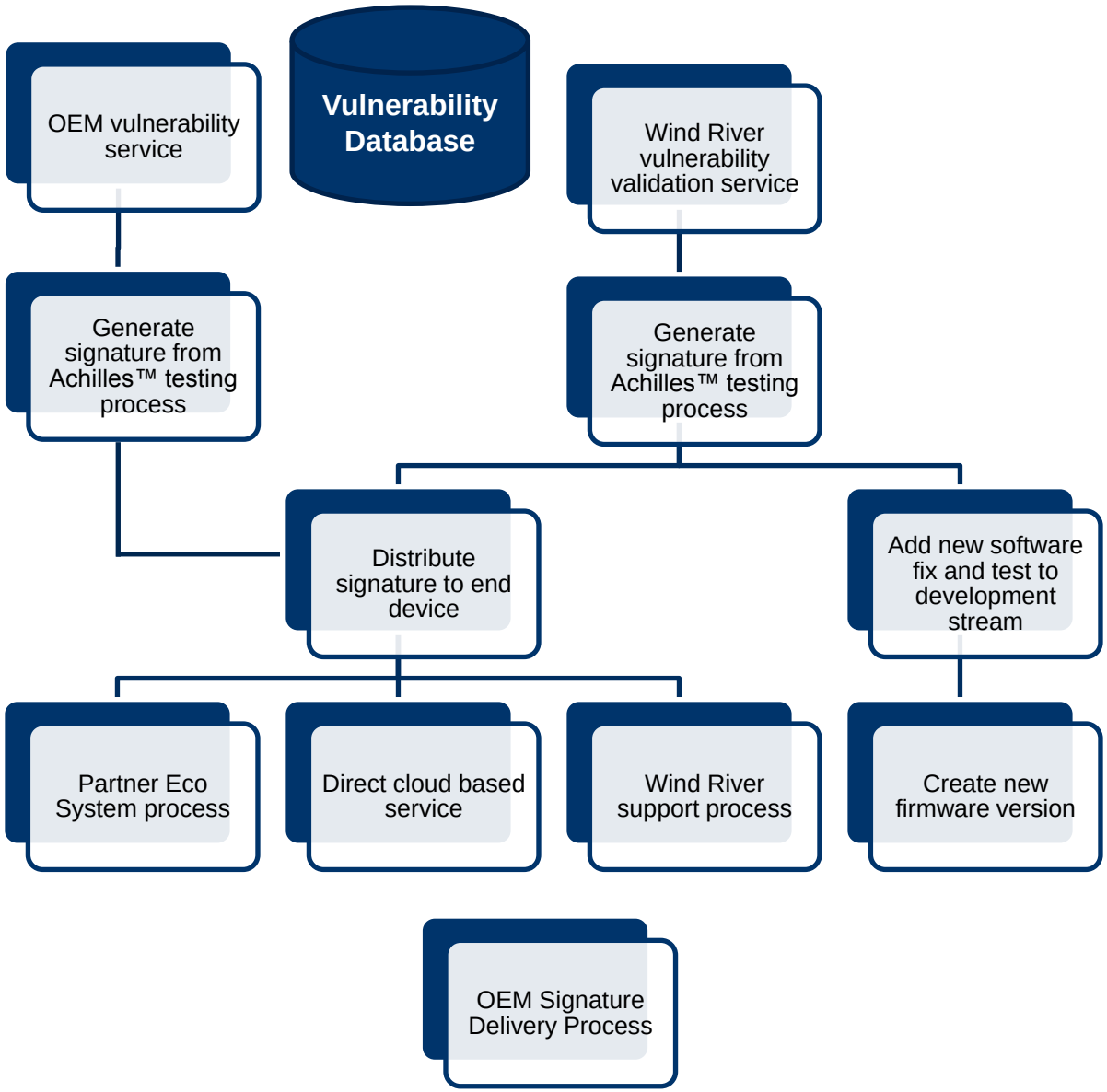
- Validation with OEM device
- Signature directly for specific device
- Liability coverage with minimum effort

Timely Response Service

- Testing of devices
- Generation of signatures
- Alert of customer
- Software fix Service optional
- Response ahead of time

Handle Regulatory Impact

- State of Practice can be claimed
- Easy to reproduce and document
- Change Management friendly (IEC 61508, FDA)



So what is it for?

- critical devices, that can’t be “patched”
- deeply embedded devices
- consolidated embedded devices
- devices with very high uptime
- CIP devices, regulated/liability
- devices with a very long life cycle

Vulnerability Root Cause Analysis

- "Grey-Box" process of identifying the vulnerable code path and mechanism, utilizing advanced dynamic and static binary analysis techniques **without** access to source code
- Determines the **critical input parameters** to exploit the vulnerable code path, and what **attacker-controlled fields** in a PDU contribute to conditions necessary for exploitation
- Process is crucial to developing signatures for the "vulnerability" as opposed to the "exploit"
- Provides
  - Complete understanding of the vulnerabilities in the products and systems submitted for analysis
  - Information and background to support outreach to customers, regulatory organizations, and the public
  - Conclusive findings that are not debatable

Work Flow

Discovery

- Input: Controller firmware, workstation binaries, or device running said code
- Activites: Reverse engineering, Achilles plug-in development, fault injection and fault monitoring via the Achilles plug-in
- Output: Anomaly notifications

Analysis

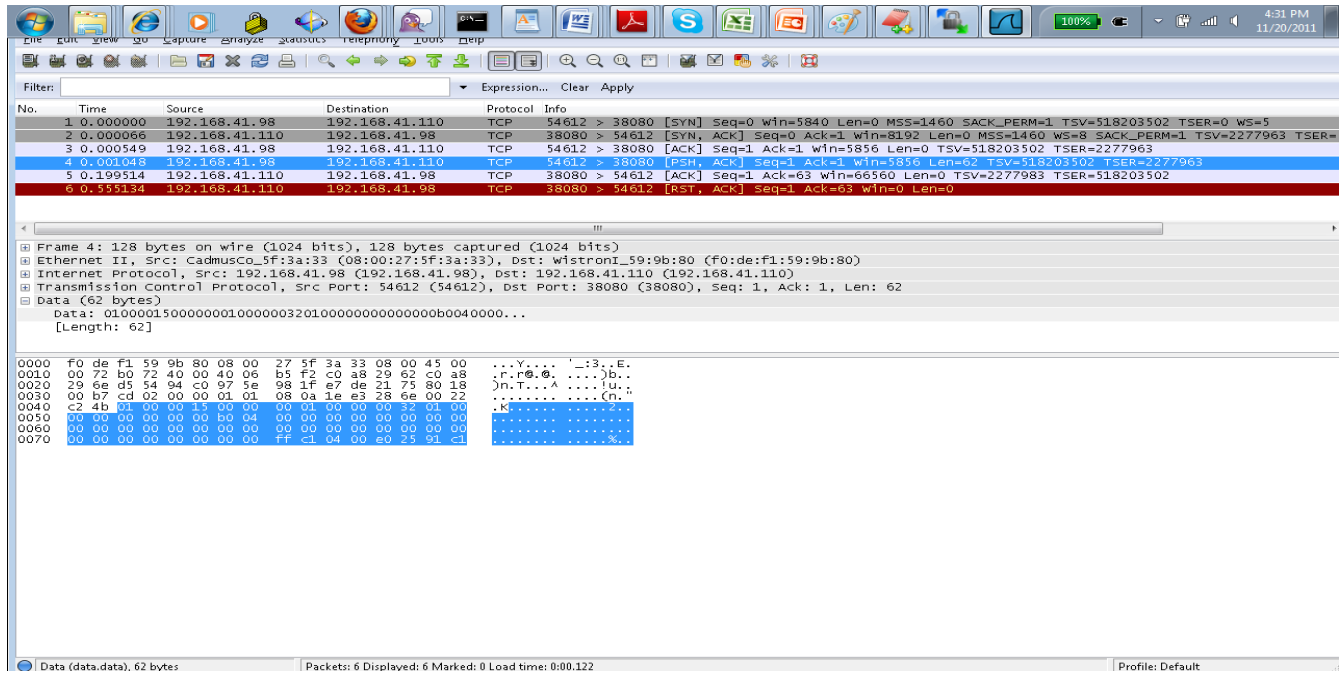
- Input: Anomaly notifications
- Activites: Work environment setup, code auditing, code execution tracing, code instrumentation, reverse engineering, documentation
- Output: Root cause report along with patching advisory and exploit code

Mitigation

- Input: Root cause report
- Activities: Generation of functional exploit module for demonstration and testing and creation of IPS/IDS signature and associated validation
- Output: Achilles Test Module demonstrating exploit behavior and V&V'd IPS/IDS signiture for target platform (Cisco, Nitro, etc)

Case Study

- Let's consider an example: ICS−ALERT-11-080-02 Iconics GENESIS32/64 Double-Free Memory Corruption
- Original Disclosure: http://aluigi.altervista.org/adv/genesis_1-adv.txt
- Includes a Proof-of-Concept code that demonstrates remote code execution:



Exploit Detecting Signature

- Signatures must include information to unique identify attempts to exploit an application vulnerability
- **Pedestrian Approach**: Detect the Exploit Payload
  - alert tcp any any -> $HOME_NET 38080 (msg:“********** Iconics Genesis SCADA Freeing of Unitialized Memory Trigger Option 1"; flow:to_server,established; dsize:62;content**:"|b0 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff 0f 00 00 ff 0f 00 00|";** classtype:attempted-user; reference:url,aluigi.org/adv/genesis_1-adv.txt; sid:2801834; rev:4;)
- **Why?**
  - Trivially evadable because only some parts of the payload contribute to accessing the vulnerable code path.
  - Any change to non-essential fields to allow the exploit to by-pass this signature.

Detailed Root Cause Analysis

```
IDA
File Edit Jump Search View Debugger Options Windows Help
Windbg debugger
IDA View-EIP, General registers, Hex View-1, Stack view | Structures | Enums

IDA View-EIP
GenBroker.exe:004446CF db  3Bh ; ;
GenBroker.exe:004446D0 db 0C5h ; +
GenBroker.exe:004446D1 db  76h ; v
GenBroker.exe:004446D2 db  14h
GenBroker.exe:004446D3 ; ---------------------------------------------------------------------------
GenBroker.exe:004446D3
GenBroker.exe:004446D3 loc_4446D3:                     ; CODE XREF: GenBroker.exe:004446E5↓j
EIP GenBroker.exe:004446D3 mov     ecx, [esi+2Ch]
GenBroker.exe:004446D6 mov     edx, [ecx+edi*4]
GenBroker.exe:004446D9 push    edx
GenBroker.exe:004446DA call    ebx
GenBroker.exe:004446DC mov     eax, [esi+28h]
GenBroker.exe:004446DF add     esp, 4
GenBroker.exe:004446E2 inc     edi
GenBroker.exe:004446E3 cmp     edi, eax
GenBroker.exe:004446E5 jb      short loc_4446D3
GenBroker.exe:004446E7 mov     eax, [esi+2Ch]
GenBroker.exe:004446EA push    eax
GenBroker.exe:004446EB call    near ptr unk_4A7356
GenBroker.exe:004446F0 mov     eax, [esi+30h]
GenBroker.exe:004446F3 add     esp, 4
GenBroker.exe:004446F6 xor     edi, edi
GenBroker.exe:004446F8 cmp     eax, ebp
UNKNOWN 004446E5: GenBroker.exe:004446E5

General registers
EAX 01020304 ↳ debug277:01020304
EBX 7C36355A ↳ MSVCR71:msvcr71_free
ECX 7C363598 ↳ MSVCR71:msvcr71_free+3E
EDX 00000005 ↳
ESI 00F68568 ↳ debug071:00F68568
EDI 00000000 ↳
EBP 00000000 ↳
ESP 022AFD8C ↳ debug286:022AFD8C
EIP 004446D3 ↳ GenBroker.exe:loc_4446D3
EFL 00000202
OF 0 DF 0 IF 1 TF 0 SF 0 ZF 0 AF 0 PF 0 CF 0

Hex View-1
7FFEFFF0 ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ????????????????
UNKNOWN 7FFEFFF0: debug276:7FFEFFF0

Stack view
022AFD8C 00F68568 debug071:00F68568
022AFD90 00F68568 debug071:00F68568
022AFD94 022AFE20 debug286:022AFE20
UNKNOWN 022AFD8C: debug286:022AFD8C

Output window
IDA is analysing the input file...
You may start to explore the input file right now.
---------------------------------------------------------------------------
Python 2.6.5 (r265:79096, Mar 19 2010, 21:48:26) [MSC v.1500 32 bit (Intel)]
IDAPython v1.5.0 final (serial 0) (c) The IDAPython Team <idapython@googlegroups.com>
---------------------------------------------------------------------------
The initial autoanalysis has been finished.
Debugger: thread 5440 has exited (code 0)
77EA6679: thread has started (tid=5912)
437180: thread has started (tid=5580)
75F9B9BC: 75F9B9BC: unknown exception code E06D7363 (exc.code e06d7363, tid 5580)
Sorting 'Breakpoints'... ok
WINDBG
AU: idle  Down  Disk: 344GB
100%  1:58 PM 17/11/2011
```

Analysis Results

- Vulnerable application uses proprietary binary network protocol
- “Free()” loop is controlled by a 4-byte value found in the packet at “field _16”
- Values of “field_4” that are less than or equal to 0x00000032 cause the raising of a software exception, whose handler code invokes the free() standard library function a number of times that is controlled by “field_16”. This allows the attacker to invoke the free function upon malicious data, creating a code-execution scenario .
- No other values in the packet payload contribute to the vulnerability.
- Remote code execution is possible with this vulnerability
- CVSS score is 10.

VRCA Facilitates A Better Signature

- Correct Signature:
  - alert tcp any any -> any 38080 (msg:“Iconics Genesis Freeing of Uninitialized Memory“; dsize: >58; byte_test:4, <, 0x33, 8; content: "|b0 04 00 00|"; offset: 20; depth: 4; sid: 60001;)
- Does not depend on fields not involved in accessing the vulnerable code path
- Does not have to be updated for new exploits utilizing the vulnerable with different parameters, significantly reduces false negatives
- Limits unexpected impacts to application logic
- Does not require directionality to reduce false positives

Ask Your Vendor, How Are Their Signatures Developed?

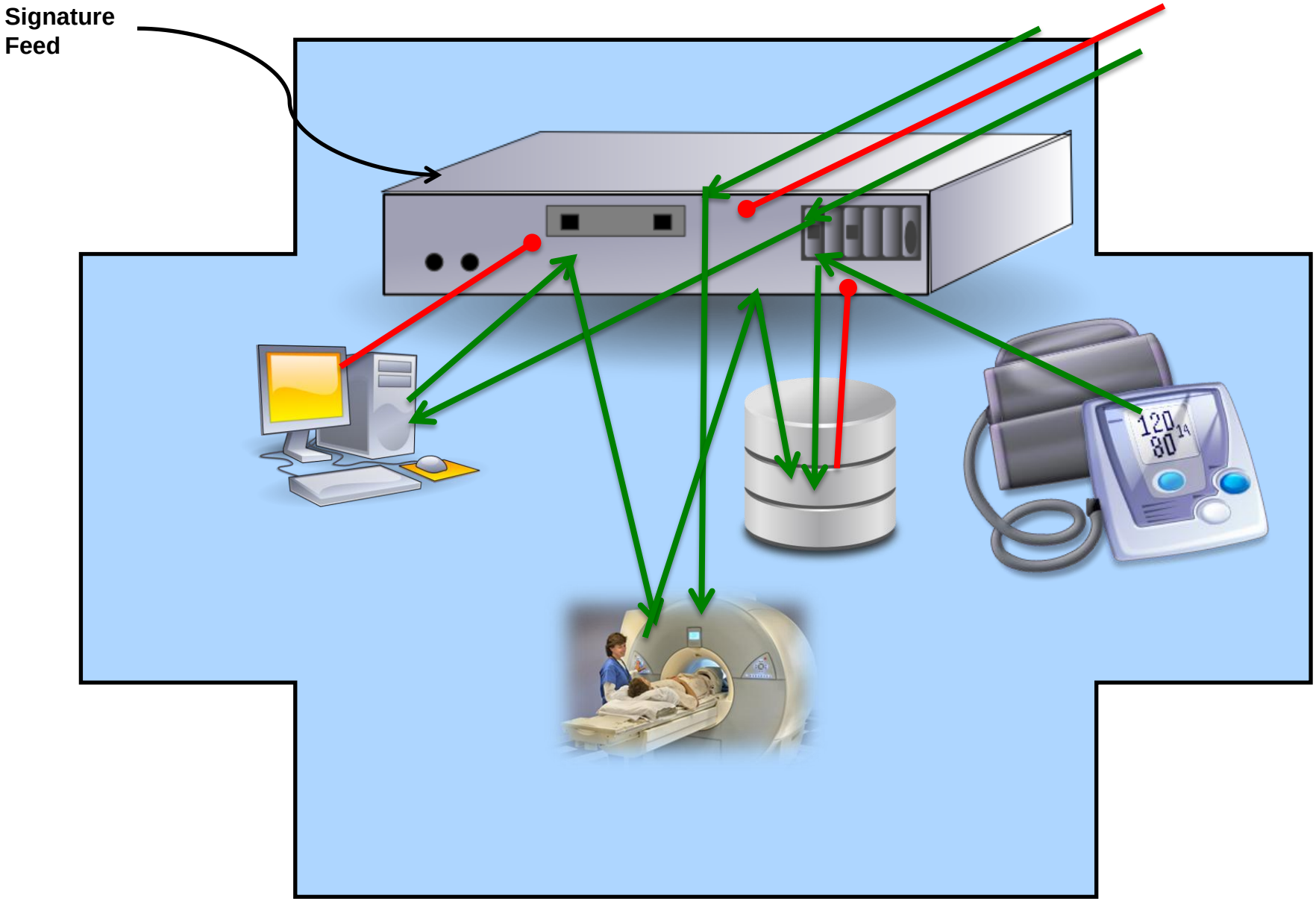
Benefits of Vulnerability Root Cause Analysis

- Protect your customers, your profitability, and your brand.
- Minimize (across your organization) unexpected and un-budgeted reactionary time, effort, and costs due to vulnerability disclosure
- Advisories for patching vulnerabilities identified in the tested components, and security suggestions for future revisions based on existing and emerging regulations and standards.
- Coordinated public relations effort, including outreach to bloggers, thought leaders, etc., to counter rhetoric as needed.

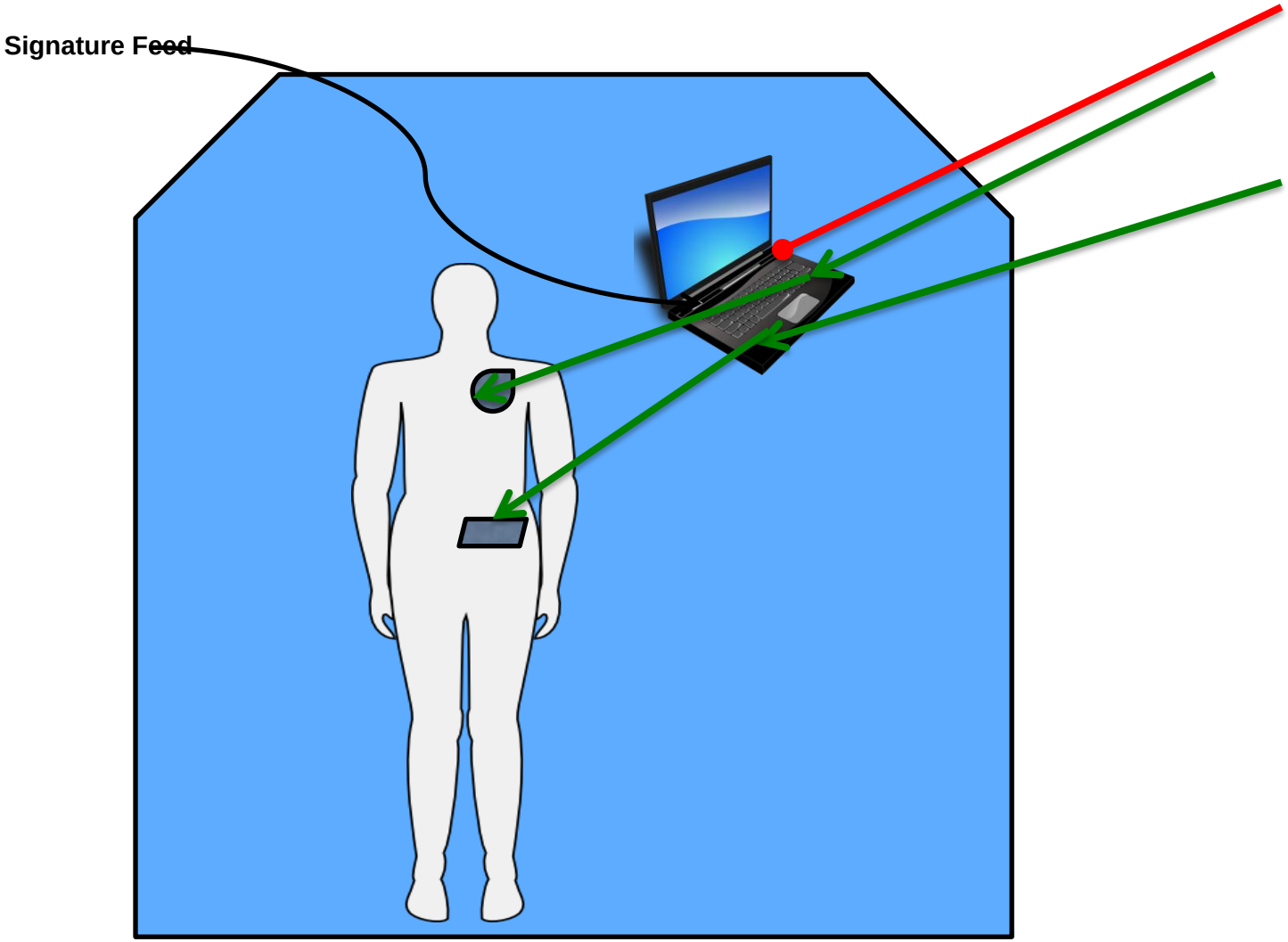
Health Care

- Health Care systems are part of Critical Infrastructure
- Impact of security breaches can be extremely high
- Discovery of Zero-Day vulnerabilities:
  - Consequences of disclosure can be quite serious (panic, increased patient danger)
  - Firmware changes must go through a long approval process (both internally and through the FDA)
- Primary objective must always be safe and consistent continuation of patient therapy

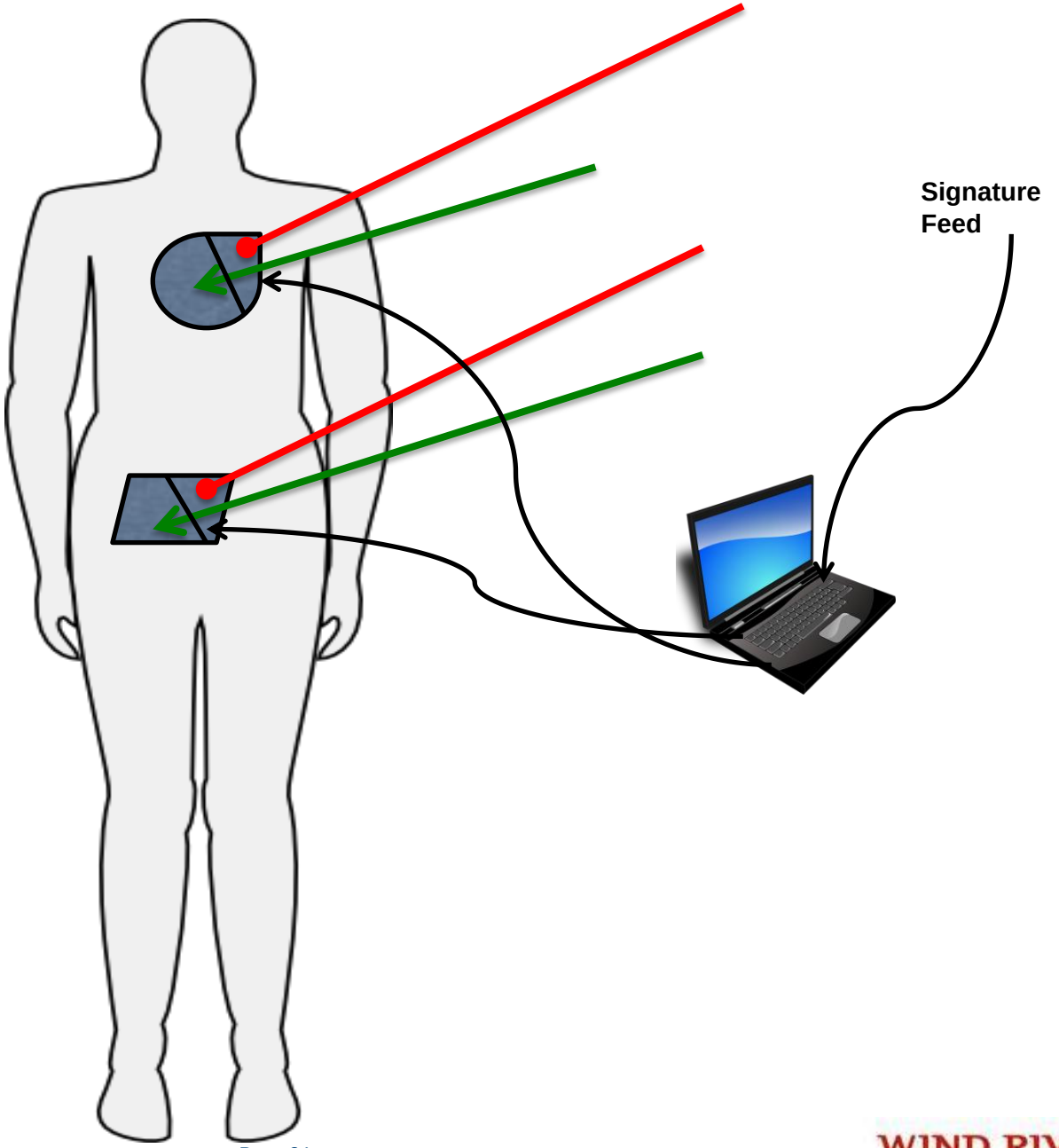
Network Perimeter Protection - Hospital



Network Perimeter Protection – Home Care System



Perimeter Protection – Device Level



Thank You

Nate Kube
Founder and CTO
Wurldtech

Alexander Damisch
Director Industrial
Wind River

Mike Ahmadi
VP Operations
GraniteKey

wurldtech

WIND RIVER