Scientific Best-Practices for Recurring Problems in Computer Security R & D

Daniel Bilar
Director of Research, Siege Technologies
Manchester, New Hampshire, USA
dbilar@acm.org
@daniel_bilar

SyScan 2014
Singapore
April 3rd, 2014
Outline of Talk

• Dynamic SyScan update: Car CAN R & D
• Signals/ Side Channels
• Side Channels & Methods
  – Detection
  – Representation
  – Analysis
• Case studies
  – ROPe, Bochspwn, Cyber Mission Planning
• Epilogue/Blueprint

Thanks for help/ inspiration and appreciation to

Thomas Dullien
Ero Carrera
Alex Sotirov
Travis Goodspeed
Anna Shubina
Sergey Bratus
Rebecca Shapiro
Jason Geffner
Jon Stuart
Georg Wicherski
Mateusz Jurczyk
Gynvael Coldwind
+ many more
Addendum: Car CAN bus hacking

• Did a subset of what Chris and Charlie did in March 2013, presented at RECon June 2013
• “Hot-Wiring of the Future”
  – Lots of tips, (free, $) tools, workflow/methodology, Costs: $6k (2 cars)
• Sponsored 3 undergraduate students (knew nothing at all about RE) who learned how to reverse, hook up boards, use goodThopter and denial of view/manipulation of CAN dashboard in 3 months

http://tinyurl.com/CarCAN2013
A Case Study – ID 513

<table>
<thead>
<tr>
<th>ArbID</th>
<th>Fuzzing Response</th>
<th>Refined Inferences</th>
</tr>
</thead>
<tbody>
<tr>
<td>513</td>
<td>Dashboard components change</td>
<td>Bytes 0, 1 = RPM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Byte 4 = Speedometer</td>
</tr>
</tbody>
</table>
Higher Level Protocol: ID 513

![Graph showing the relationship between Data Byte 4 Value and Speedometer Reading (MPH).]
Higher Level Protocol: ID 1056

1056

DLC = 8

Arbitration ID

Control Field

Data Field

SOF

EOF

Engine Temp

Odometer

Battery Charge

Engine Clock

Dashboard Warnings

Check Fuel Cap

Unused

Counter
Signals: Side Channel

- Side channels = observables that are emitted by active systems
- On a computer system, these can be observed time, power, OS events, EM radiation, characteristic acoustic spectral signature and more
- 2014: Mark Stoettinger’s NTU group is doing cutting edge punctuated hardware magnetic field side channel analysis (SCA)

Figure 2. Intel i7 memory hierarchy plus clock latency for the relevant stages

Graph from [Hund2013]. Generic timing side channel attack against MMU system to infer information about the privileged address space layout

Some innovative attacks: data structures (2007 timing attacks against databases), protocols and underlying algorithms (2007 QoS attacks against balancing algorithms, MMU (cache) and more
Side Channels as Consilient Evidence

• Generalize: Use side channel evidence to reason about system/sub-system (internal states)
• Whewell’s “Consilience of Induction”
  – Concept of aggregate evidence
  – Convergence of several, ideally independent hypotheses serves to strengthen conclusion
• Question: What side channels are available, easy to access, analyze, expressive, type I/II error etc
Three Questions on Signals

• Want actionable handling of higher dimensional signal dynamics as they occur in live computer systems as side channels
  – Actionable is to be understood as useful in practice
  – Higher dimensional refers to six or more data dimensions
  – Dynamics emphasizes the signal’s unfolding in temporal and feature space

• We’ll discuss
  – How to represent such signals
  – How to detect signals with various characteristics
  – How to prevent or mitigate the leaking of such signals
# Signal Representation: Visuals

<table>
<thead>
<tr>
<th>Property</th>
<th>Elaboration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Well-boundedness</td>
<td>Do changes in the representation express changes in the data, and not particular algorithmic artifacts?</td>
</tr>
<tr>
<td>Actionability</td>
<td>Does the representation support formulating hypotheses and subsequently testing them?</td>
</tr>
<tr>
<td>Specificity</td>
<td>Does the representation fit the nature of the domain whence the data sprung? Is it amenable to revealing the essence of the underlying process?</td>
</tr>
<tr>
<td>Parsimony</td>
<td>Does the representation uses the absolute minimum number of attributes necessary for specificity?</td>
</tr>
<tr>
<td>High-Dimensionality</td>
<td>Does the data representation support enough dimensions to facilitate comprehension of the underlying process?</td>
</tr>
<tr>
<td>Scalability</td>
<td>Can large orders-of-magnitude rescaling with concomitant drill down/zoom out be intelligibly accommodated?</td>
</tr>
<tr>
<td>Perspective</td>
<td>Can dependent and independent dimensions be changed to enable different process view of the data?</td>
</tr>
</tbody>
</table>

Table 1: Representation Evaluation Criteria
Signal Representation: Visuals & more

- Fundamental cognitive limits for visuals very hard to overcome for high dimensional representation

Rich gamut of human senses remain neglected
- Aural (hearing), haptic (touch), vestibular (balance and acceleration), kinesthetic, thermoception (temperature), etc
Signal Detection: MINE Statistics

Maximal Information-based Nonparametric Exploration (MINE) statistics

- General: Captures wide range of associations between pairs of variables (linear, exponential, periodic, non-functions)
- Equitable: Assigns similar scores to equally noisy relationships of different types [Reshef2011sup]

<table>
<thead>
<tr>
<th>Data</th>
<th>MIC</th>
<th>MAS</th>
<th>MEV</th>
<th>MCN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.00</td>
<td>0.00</td>
<td>1.00</td>
<td>2.00</td>
<td></td>
</tr>
<tr>
<td>1.00</td>
<td>0.74</td>
<td>1.00</td>
<td>3.00</td>
<td></td>
</tr>
<tr>
<td>1.00</td>
<td>0.89</td>
<td>1.00</td>
<td>4.00</td>
<td></td>
</tr>
<tr>
<td>1.00</td>
<td>0.69</td>
<td>1.00</td>
<td>2.56</td>
<td></td>
</tr>
<tr>
<td>0.79</td>
<td>0.16</td>
<td>0.70</td>
<td>6.91</td>
<td></td>
</tr>
<tr>
<td>0.71</td>
<td>0.03</td>
<td>0.32</td>
<td>6.87</td>
<td></td>
</tr>
<tr>
<td>0.46</td>
<td>0.19</td>
<td>0.22</td>
<td>6.98</td>
<td></td>
</tr>
</tbody>
</table>

MIC captures general relationship strength
MIC-r^2 captures non-linearity (Not shown)
MCN captures complexity
MAS captures departure from monotonicity
MEV captures closeness to being a function
Signal Detection: Association ‘Types’

Graphs from [Reshef2011sup]
Signal Prevention: Side Channel Leaks

- **Possible to control rate but not eliminate side channels**
- Recently, Goldwasser (MIT/Technion) and Rothblum offer a practical way forward
- Resisting leakage at *design time* and offers progress towards *formulation of automatic approaches* that generate “leakage-resilience” programs for a wide range of side channel attacks
- Proved that for any computationally unbounded $A$ observing the results of computationally unbounded leakage functions, will learn no more from its observations than it could given blackbox access only to the input-output behavior of $P$
- Result is *unconditional* and does not rely on any secure hardware components
Cyber Mission Planning

• Cyber-operations have potential to be more pinpointed than kinetic counterpart
  – Minimize collateral damage by ‘crisp’ targeted operations

• However, unlike kinetic planning (centuries of well-understood natural laws), cyber-planning lacks foundational corpus of predictive laws

“Natural Laws for/of/in Virtual Reality”
Thread / Process/ Cache Execution

- Behavior arises as a complex interaction of timing of memory requests (program behavior), cache coherence protocol (dependent on MA), or thread pre-emption (depending on OS) [Alistarh2014]
- Modern operating systems (OS) and microarchitectures (MA) = dynamic complex feedback system that tries to continuously minimize CPI (cycles per instruction)
  - Memory latency is bottleneck, hence memory hierarchies from ns to s
- OS and MA continuously solve a time-space optimization problem to ‘flatten’ (parallelize) sequential processing
Signal Detection: MINE/MIC

Maximal Information-based Nonparametric Exploration (MINE) statistics

Intuition: (Simple) asset ‘signals’ are reflected in convex/concave parabola-type curves in time

Identify signals that are less periodic (lower MAS), less linear (MIC-$r^2$), but still a function (higher MEV)

“not a heartbeat, not a shooting star, but still a function”

MIC captures general relationship strength
MIC-$r^2$ captures non-linearity (Not shown)
MCN captures complexity
MAS captures departure from monotonicity
MEV captures closeness to being a function
Issue: Experimental Factors

- Free NIST tools: Automated Combinatorial Testing for Software (ACTS) and Coverage Measurement (CCM)
- Cut down combinatorial explosion: 2-way, 3-way, n-way testing
Asset-Target Matching

- Say asset tested on configuration A and it has 18 categories (e.g. language, OS/patch, service running, workload, etc) @ dozen of values
- How similar is the unknown configuration B to A?
- Question of distance
  - Easy enough for ratio data (like Kelvin), much harder for categorical data (like OS type)
- Table shows 14 categorical distance (similarity) measures
- Differ primarily how they weigh matches and mismatches between categories

‘Success’ functions are not smooth but stepped
- Can shove 10cm^3 (~elastic) object through 9.8cm^3 hole — > smooth success degradation
- Difference between patch1 and patch2 is difference between works/doesn’t work -> step/catastrophic success degradation

Table from [Boriah2013]
Case study: ROPe

- **ROPe**: Detection of kernel-level ROP through branch return mispredictions
- **16 (N)** entry shadow stack of call-sites / return addresses
  - 0x89 – BR_MISP_EXEC.*: mispredicted executed branches
  - 0x800 – .RETURN_NEAR: normal, near ret
  - 0x8000 – .TAKEN: unconditional branch
- **PMC interrupts after certain number of mispredictions (N/2 = 8)**
  - Upon interrupt, handler checks MSR Last Branch Recording (LBR) whether targets of the previously executed instructions are preceded by an instruction
  - If not -> likely ROP (chain) induced

Graph from G. Wicherski, SysCan 2013

Started telling Travis Goodspeed at RECon 2013 about this and after less than 8 seconds he exclaims and I quote: *Holy cow! That’s a $^&* brilliant idea once you understand it!* 😊
Suggestions for ROPe

- Generalize ROP/0x8889 insight: Side channel ‘spectral signature’ for variety of interesting attacks
  - JOP, ‘weird machine’-inducers, hardware-based attacks, ...
  - Additional OS/MA vents

Workplan (high-level):

- Identify signals of interest
  - Scope with MINE [Reshef2011]
- Signal periodicity analysis
  - DSP, System Identification tools
- Scientifically valid experiment setup
  - Use procedures [Mont2012]

PMC measurements over time for programs in SPEC benchmark suite. Graph from [Demme2013]. Good results with 4-dim spectral signature from x86 MA events
0x0440 -- L1D_CACHE_LD.E_STATE
0x0324 -- L2_RQSTS.LOAD
0x03b1 -- UOPS_EXECUTED.PORT (1 or 2)
0x7f88 -- BR_INST_EXEC.ANY
Case study: Bowspwn

- Study of Double fetch operations
  - Two virtual address reads from kernel mode thread close in time
  - Virtual address concurrently writable by ring-3 threads
- Assumption of value consistency over time gives rise to race condition
  - User address space is shared across ring0 / ring3
  - User-mode memory regions can be modified at any time by concurrent ring3 thread
- Bochspwn idea: Extend time window between value Check and value Use to give ring3 attack thread opportunity to modify value
  - How? Bleed time by slow cache line and page boundaries, non-cacheability, TLB flushing (2500x slowdown achieved)
- 69 (!) LaTex pages at SyScan 2013
  - Fundamental applied security paper, vital for safer concurrent programming [JC2013a]
  - Refinements: Flip interval dependence on value (binary, arithmetic) types, logistic S-curve discussion [JC2013b]
Suggestions for Bochspwn

12 high level computation language patterns mined from seven general application areas (green & blue rare) [Asan2009]

Practical: Find low level assembly pattern translation and investigate susceptibility to double fetch and resulting ‘distortions’/ error

Theory: Investigate multi-core control systems (system scheduler, Paging) and ‘bring out’ assumptions
Epilogue: Methods ‘Blueprint’

• Signal Selection
  – Construct model of system
  – Identify side channel observables (OS/MA events & others)
  – Scope SCO’s MINE properties
  – Use MIC/MINE statistics [Reshef2011]

• Signal Representation & Analysis
  – Octave (free but not powerful enough), MATLAB (best choice)
    • Boxplots, Probability Plots
    • Toolboxes: Statistics, DSP, System Identification
  – Machine Learning
    • Internalize [Dom2012]
    • Select ML procedures from [Murph2012] appropriate for and educed from a system model and the signals’ macro-properties
    • [PMTK3] for Bayesian reasoning/modeling

• Scientific Experiments [Mont2012]

• Specialized tools:
  – Signal Analysis: Eureka [Lipson2009]
  – Signal Representation: Viewpoints [Gazis2010]
Pro-Tip ML

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Prior</th>
<th>Name</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gaussian</td>
<td>Uniform</td>
<td>Least squares</td>
<td>7.3</td>
</tr>
<tr>
<td>Gaussian</td>
<td>Gaussian</td>
<td>Ridge</td>
<td>7.5</td>
</tr>
<tr>
<td>Gaussian</td>
<td>Laplace</td>
<td>Lasso</td>
<td>13.3</td>
</tr>
<tr>
<td>Laplace</td>
<td>Uniform</td>
<td>Robust regression</td>
<td>7.4</td>
</tr>
<tr>
<td>Student</td>
<td>Uniform</td>
<td>Robust regression</td>
<td>Exercise 11.12</td>
</tr>
</tbody>
</table>

Table 7.1 Summary of various likelihoods and priors used for linear regression. The likelihood refers to the distributional form of $p(y|x, w, \sigma^2)$, and the prior refers to the distributional form of $p(w)$. MAP estimation with a uniform distribution corresponds to MLE.

- Know what features your favourite ML algo selects and weighs
- Many blind spots possible
- Study Domingos (2013)!
Current/upcoming R & D topics

• Added to the talk is a short WP with a selection of R & D issues
  – Concurrency Attacks
  – Compositional Security
  – Systemic Computer Security

• All these in my humble opinion benefit from SCA
Concurrency Attacks

- Even though we increasingly rely on concurrent execution, such programs are much more difficult to write, test, debug.
  - Potential for serious concurrency errors in many widespread concurrent programs, enabling feasible concurrency attacks
- Many ‘sequential’ defense techniques, if unaware of concurrent programming, are ineffective
- Careful study of Bowspwn and ROPe will yield insights

<table>
<thead>
<tr>
<th>Findings</th>
<th>Implications</th>
</tr>
</thead>
<tbody>
<tr>
<td>A majority (24 out of 46) of the concurrency attacks corrupt pointer data.</td>
<td>Existing memory safety tools, once made aware of concurrency, may be able to prevent concurrency attacks that corrupt pointer data.</td>
</tr>
<tr>
<td>9 concurrency attacks directly corrupt scalar data, such as user identifiers, without compromising memory safety.</td>
<td>Few existing defenses handle attacks that directly corrupt scalar data.</td>
</tr>
<tr>
<td>Many existing defenses become unsafe in the face of concurrency errors</td>
<td>These defenses must consider concurrent execution.</td>
</tr>
<tr>
<td>The exploitability of a concurrency error highly depends on the duration of its vulnerable window (i.e., the timing window within which the concurrency error may occur).</td>
<td>New defense techniques may reduce the exploitability of concurrency errors by reducing the duration of the vulnerable window.</td>
</tr>
</tbody>
</table>
Compositional Security

Secure Composition Problem

**Composition** What can you say about composition of modules A and B?

Parsers, Language Classes & Power

**Formal Input Verification** Input to parser constitutes valid expression in input-handler’s protocol

**Secure Composition** Prove computational equivalence of input-handling routines, i.e. do two grammars produce exactly the same language? (if not, in extremis birth of ‘weird machines’)

**Requirement** Equivalence *undecidable* for complex protocols - starting from language classes that require Non-Deterministic PDA to recognize input language

Way Forward: Minimum Power Principle to Reduce Insecurity of Composition

1. Parser must *not provide more than the minimal computational strength necessary to interpret the protocol* it is intended to parse

2. Protocols should be *designed to require the computationally weakest parser necessary to achieve the intended operation*

**DECIDABLE** For regular + deterministic context-free grammars

Systemic Computer Security

- Motivation: Flash Crash (May 2010) – see my IEEE SP article
  - phenomenological ‘signatures’ of interacting autonomous computer agents in real-world dynamic (trading) system
  - All-machine time regime characterized by frequent ‘black swan’ events with ultrafast durations (<650ms for crashes, <950ms for spikes
- Aggregate behavior of simple agents is unpredictable in principle; no useful security guarantees anent dynamics possible

HFT Nanex 2010
Systemic Computer Security II

• Aggregate behavior of simple agents is unpredictable; no useful security guarantees anent dynamics possible [Joh13] [Bil14]

• Analysis of (side channel) event signatures in phase space; design of circuit breakers, graceful degradation, rectifiers

• Relevance to Singapore ‘Smart Cities’ (see good/bad example Songdo, Portland)
Thank you

How Scientists Relax
• Infrared spectroscopy on a vexing problem of our times:
  Truly comparing apples and oranges

Thank you for your time and the consideration of ideas.

I appreciate being at SyScan and to finally visit Singapore 😊

A spectrographic analysis of ground, desiccated samples of a Granny Smith apple and a Sunkist navel orange. Picture from [San95]
References I


References II


[Wich2013] G. Wicherski "Taming the ROPe on Sandy Bridge", SyScan, April 2013 http://www.syscan.org/index.php/download/get/3c6891f2e90e661ea23224cd8f419262/SyScan2013_DAY1_SPEAKER05_Georg_WIcherski_Taming_ROP_ON_SANDY_BRIDGE_syscan.zip
References III


