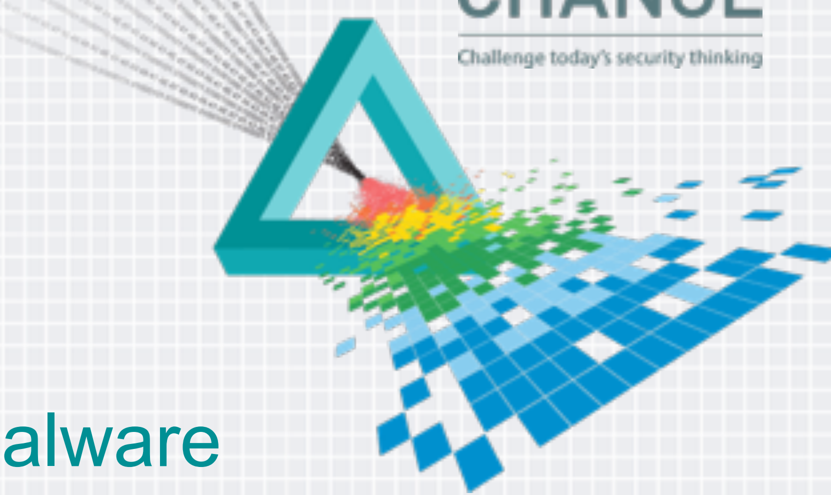
RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking



SESSION ID: BR-W03

Watt, Me Worry?
Analyzing AC Power to Find Malware

VirtaLabs

Ben Ransford, Ph.D.

Chief Technical Officer
Virta Laboratories, Inc.
@virtalabs

Denis Foo Kune, Ph.D.

Chief Executive Officer
Virta Laboratories, Inc.
@virtalabs

Your Speakers

- Ben Ransford, Ph.D., CTO Virta Labs
  - Medical device attacks & “zero-power” defenses
  - Power analysis attacks and defenses
- Denis Foo Kune, Ph.D., CEO Virta Labs
  - EMI injection attacks on medical devices
  - Privacy attacks on GSM phones

- Co-founded **Virta Labs** in 2013 to find malware via the power line

#question

- How can we monitor machines that we can't modify *at all*?

Image: nihonkohden.com, madmonkeyhostels.com

Legacy Systems Challenges

- Systems stay in service long past operating system EoL
- Often performing critical roles
- Hard or impossible or forbidden to upgrade/patch
- Clear high-ROI entry point for attackers!

Legacy Systems Challenges

- Systems stay in service long past operating system EoL
- Often performing critical roles
- Hard or impossible or forbidden to upgrade/patch
- Clear high-ROI entry point for attackers!

- Are we doomed to repeat the same problems with IoT?

Legacy Systems Challenges

- Systems stay in service long past operatin
- Often performing critical roles
- Hard or impossible or forbidden to upgrad
- Clear high-ROI entry point for attackers!

- Are we doomed to repeat the same proble

Today: Analyzing AC Power to Find Malware

- Side channels 101
- AC power side channels
  - Demo!
  - Using side channels to attack privacy
- Demo!

What are Side Channels?

- Information flows in channels by design
  - e.g., video signals
  - e.g., encrypted Wi-Fi frames

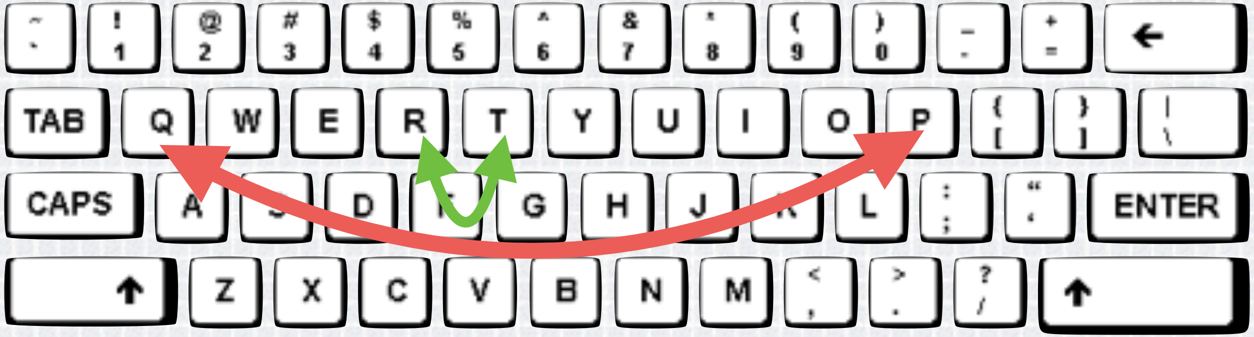
- Side channels are **accidental** channels of information flow
  - Example: timing differences that reveal plaintext

Side Channels in Context

- Adversary can observer side channels to compromise security
  - Generally a passive adversary, e.g., eavesdropper
- Long history of side-channel attacks. Examples:
  - WWI: signals intelligence on buried TX lines
  - Differential power analysis (Kocher et al., CRYPTO ’99)
  - Tromer lab’s work with acoustic (Tel Aviv)

Timing Side Channels in SSH

- SSHv1 sent a packet every time you pressed a key…



- Eavesdropper can infer typed text from inter-keystroke timings!
- "Timing Analysis of Keystrokes and SSH Timing Attacks," USENIX Security 2001

Optical Eavesdropping

- Raster scan of a CRT’s electron beam = time-varying light intensity

OH
HELLO
THERE
OH
HELLO
THERE

(artist's rendition)

- “Optical Time-Domain Eavesdropping Risks of CRT Displays,” IEEE S&P 2002

TEMPEST

- NSA program since '60s (?)
- Super-sensitive RX gear
- Electromagnetic emanations betray plaintext!
- Remediations: shielding, spacing, separation
  - $$$$$

Image: atomictoasters.net

TEMPEST Shielding

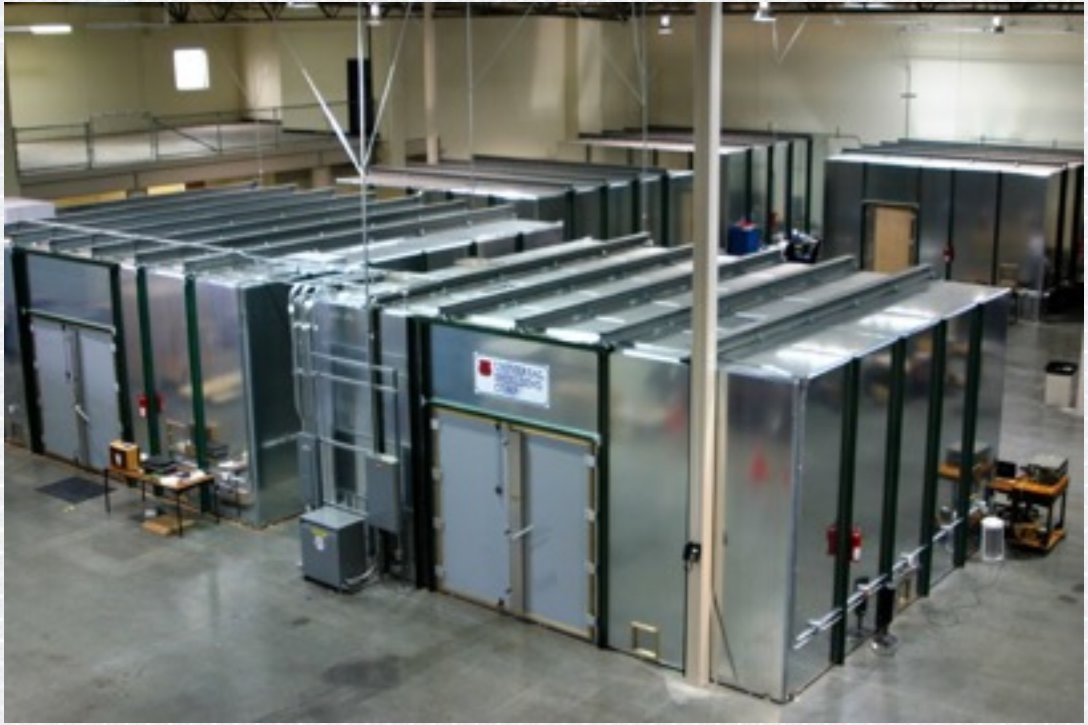


Image: ramayes.com

TEMPEST Shielding

- E.g.: KG-13 crypto machine (1960s)
- AC power filter to prevent secrets leaking onto power lines!

Image: jproc.ca

AC Power Side Channels

- Main idea: power consumption contains information
  - Which computer is this?
  - What is the computer doing?

- What makes AC power analysis **possible**?
- What makes AC power analysis **challenging**?
- What makes AC power analysis **work in practice**?

Side Channel Analyst's Toolbox

- Physical side channels: scope, scope, scope, store!

Oscilloscope

Data Acquisition Unit (DAQ)

- Sensors that output voltage proportional to signal
  - Sense resistor: voltage ∝ current through the sensor
  - Measure voltage across the sense resistor to measure current (V=IR)

Image: BK Precision

Side Channel Measurement Points

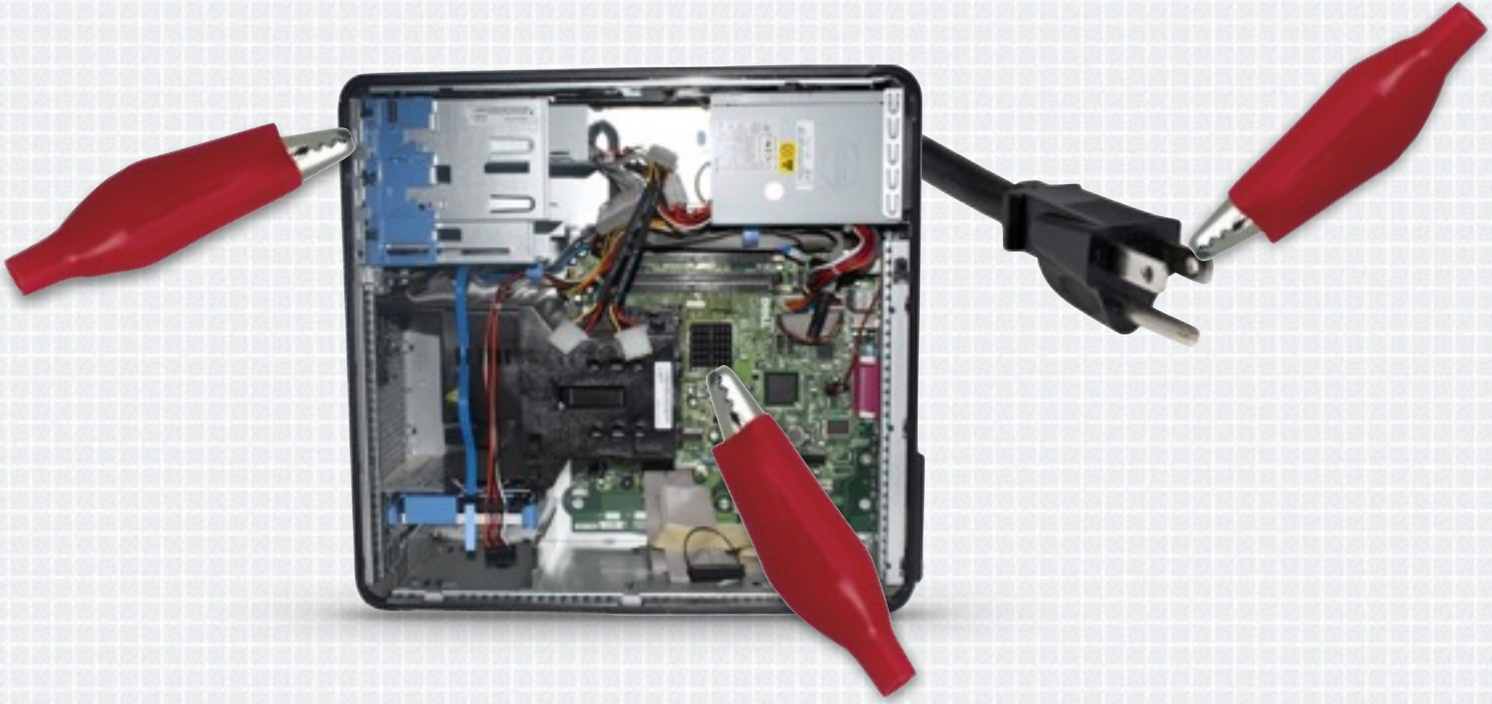


Image: refurbished-pc.com; sterenshopusa.com

Side Channel Measurement Points

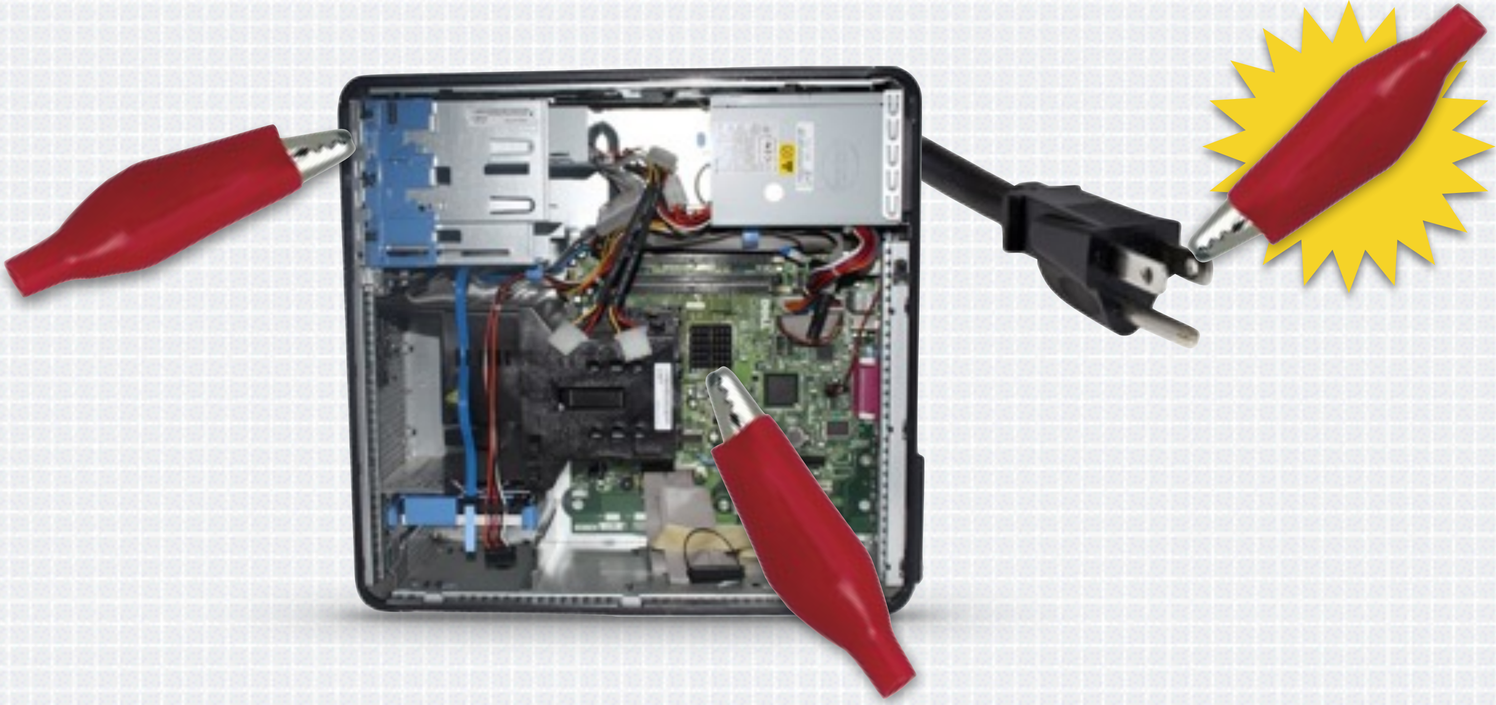
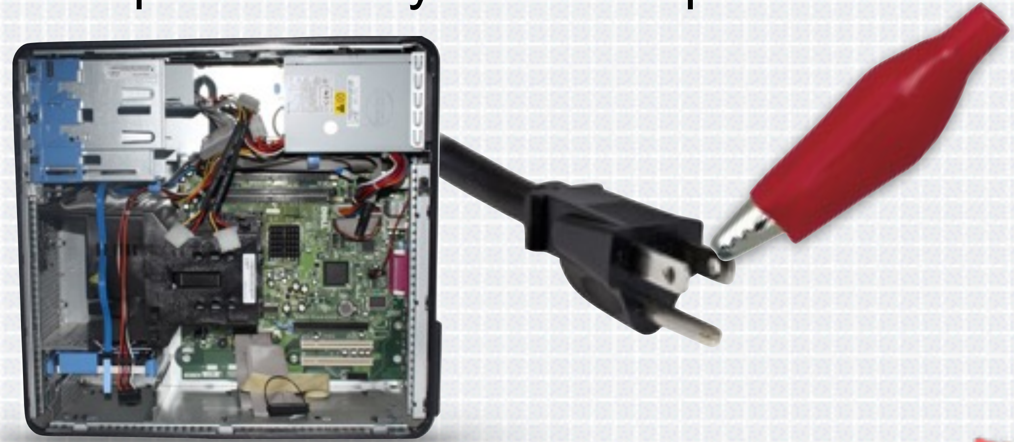


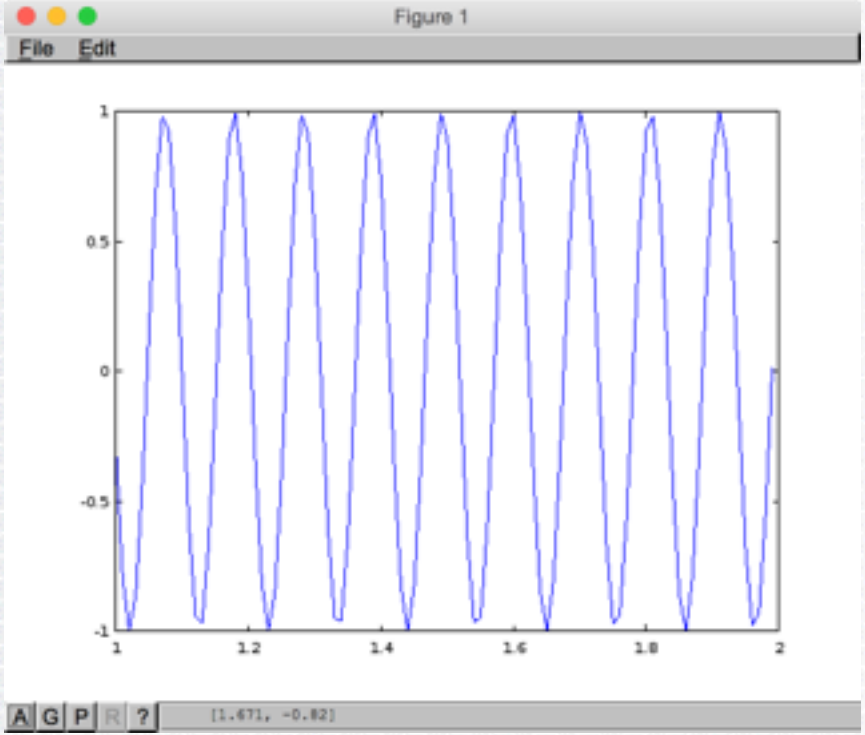
Image: refurbished-pc.com; sterenshopusa.com

AC Power Analysis: Enabling Factors

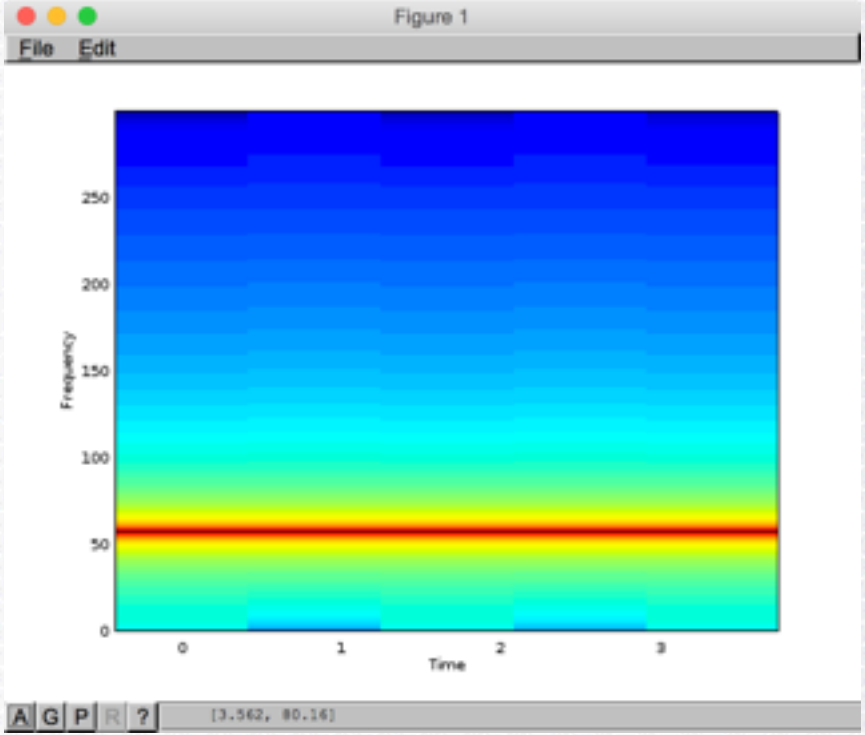
- Probe points are easily accessible (hot, neutral, ground)
  - No need to open the box!
  - No need to hunt for signal wires!
- Changes in DC current consumption readily visible to probes
- **What do we see on the wire?**



Signals on the Wire

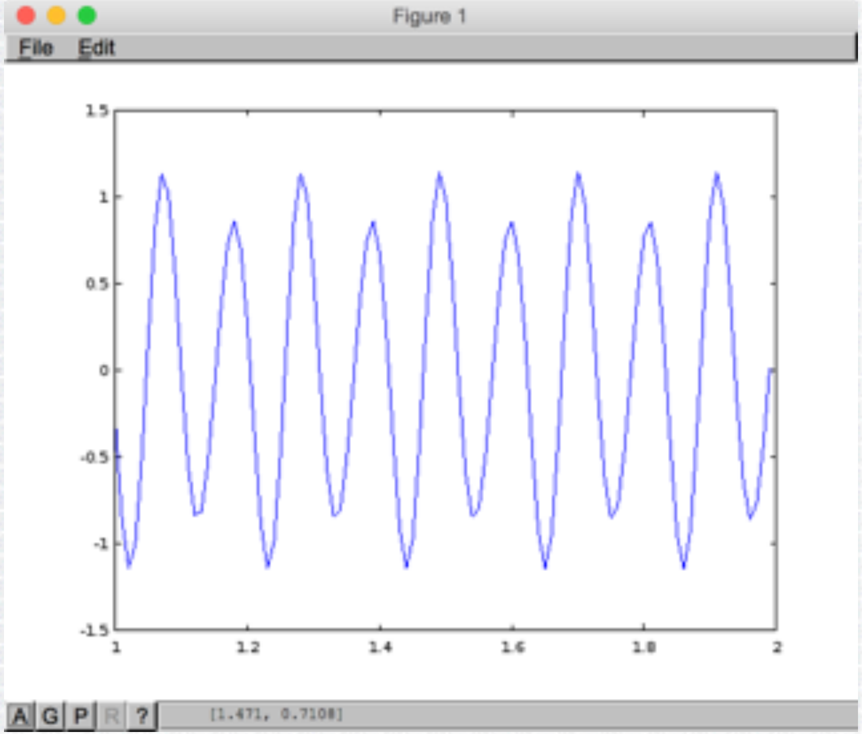


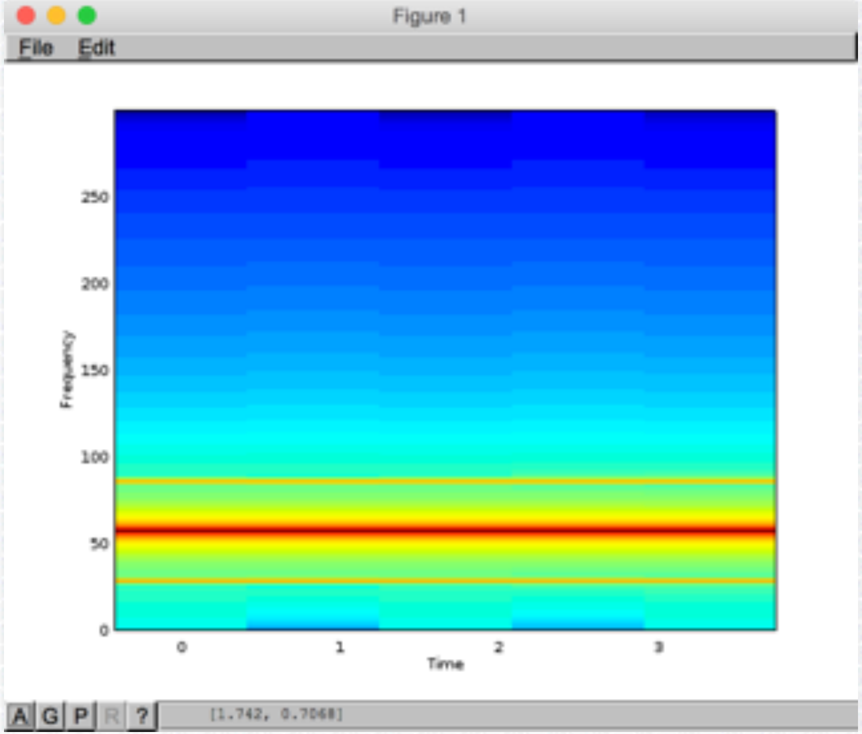
[1.671, -0.82]



[3.562, 80.16]

Signals on the Wire

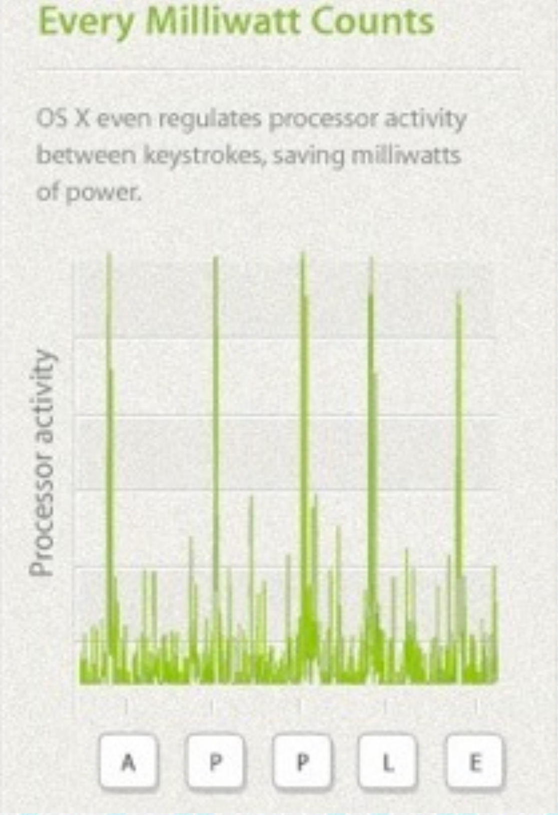




Current Consumption Varies

- Today’s CPUs and software are careful to use power management!
  - Modern systems exhibit *high dynamic range*

- Workloads ➞ patterns of high/low
  - CPU busy ➞ more current
  - Peripherals busy ➞ more current
  - Idle time ➞ less current



Every Milliwatt Counts

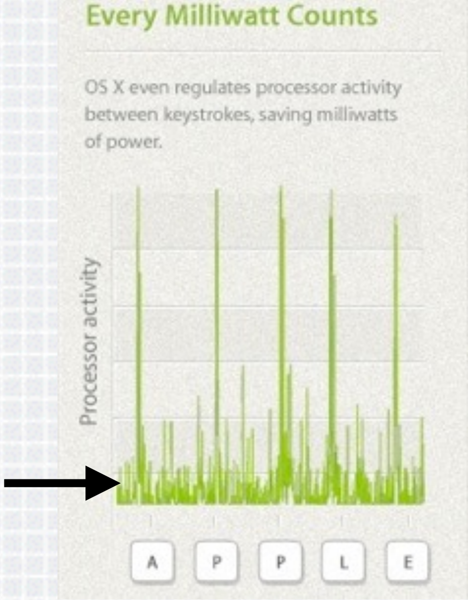
OS X even regulates processor activity between keystrokes, saving milliwatts of power.

Image: Apple

AC Power Analysis: Challenges

- Signals to analyze are noisy; where's the information?
- Power supply aggregates signals
  - CPU's power consumption +
  - Hard drive's power consumption +
  - Memory's power consumption + …
- Difficult to disentangle signals
  - Our approach: **machine learning**

What's all this? →



Every Milliwatt Counts

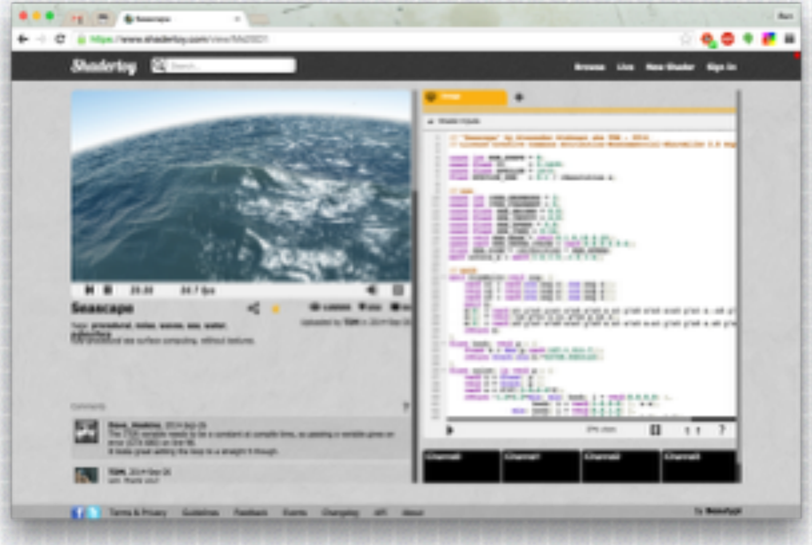
OS X even regulates processor activity between keystrokes, saving milliwatts of power.

AC Power Analysis Example: Private Browsing

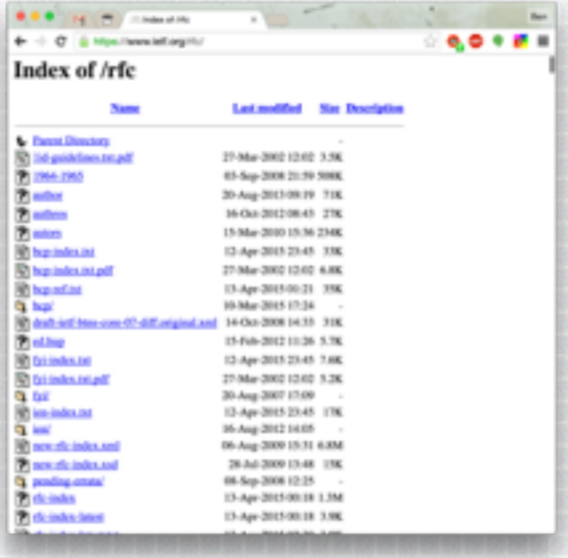
- Threat model: you can access my AC outlet
  - ~15 seconds to swap a faceplate…
- **Q: Which webpage am I visiting?**
- Analyze power during webpage loading
  - Train a **classifier** to recognize webpages' power-line signatures
  - Test new signals against the trained classifier

Task: Webpage Identification

- Intuition: pages exercise computing resources differently



vs.



Index of /rfc

Name	Last modified	Size	Description
Parent Directory		-	
1id-guidelines.txt.pdf	27-Mar-2002 12:02	3.5K	
1964-1965	03-Sep-2008 21:59	508K	
author	20-Aug-2013 09:19	71K	
authors	16-Oct-2012 08:43	27K	
autors	15-Mar-2010 15:36	234K	
bcp-index.txt	12-Apr-2015 23:45	33K	
bcp-index.txt.pdf	27-Mar-2002 12:02	6.8K	
bcp-ref.txt	13-Apr-2015 00:21	35K	
bcp/	10-Mar-2015 17:24	-	
draft-ietf-btns-core-07-diff.original.xml	14-Oct-2008 14:35	31K	
ed.bcp	15-Feb-2012 11:26	5.7K	
fyi-index.txt	12-Apr-2015 23:45	7.6K	
fyi-index.txt.pdf	27-Mar-2002 12:02	5.2K	
fyi/	20-Aug-2007 17:09	-	
ien-index.txt	12-Apr-2015 23:45	17K	
ien/	16-Aug-2012 16:05	-	
new-rfc-index.xml	06-Aug-2009 15:31	6.8M	
new-rfc-index.xsd	28-Jul-2009 13:48	15K	
pending-errata/	08-Sep-2008 12:25	-	
rfc-index	13-Apr-2015 00:18	1.3M	
rfc-index-latest	13-Apr-2015 00:18	3.9K	

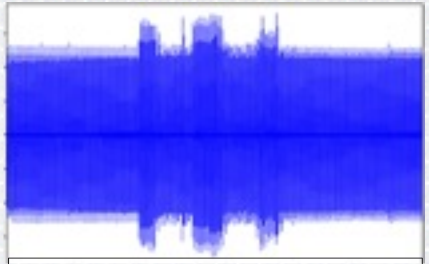
RSAConference2015

San Francisco | April 20-24 | Moscone Center

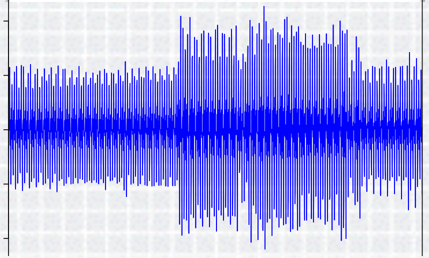
Demo: Page Loads on the Wire

Page Loads on the Wire

UMASSCS

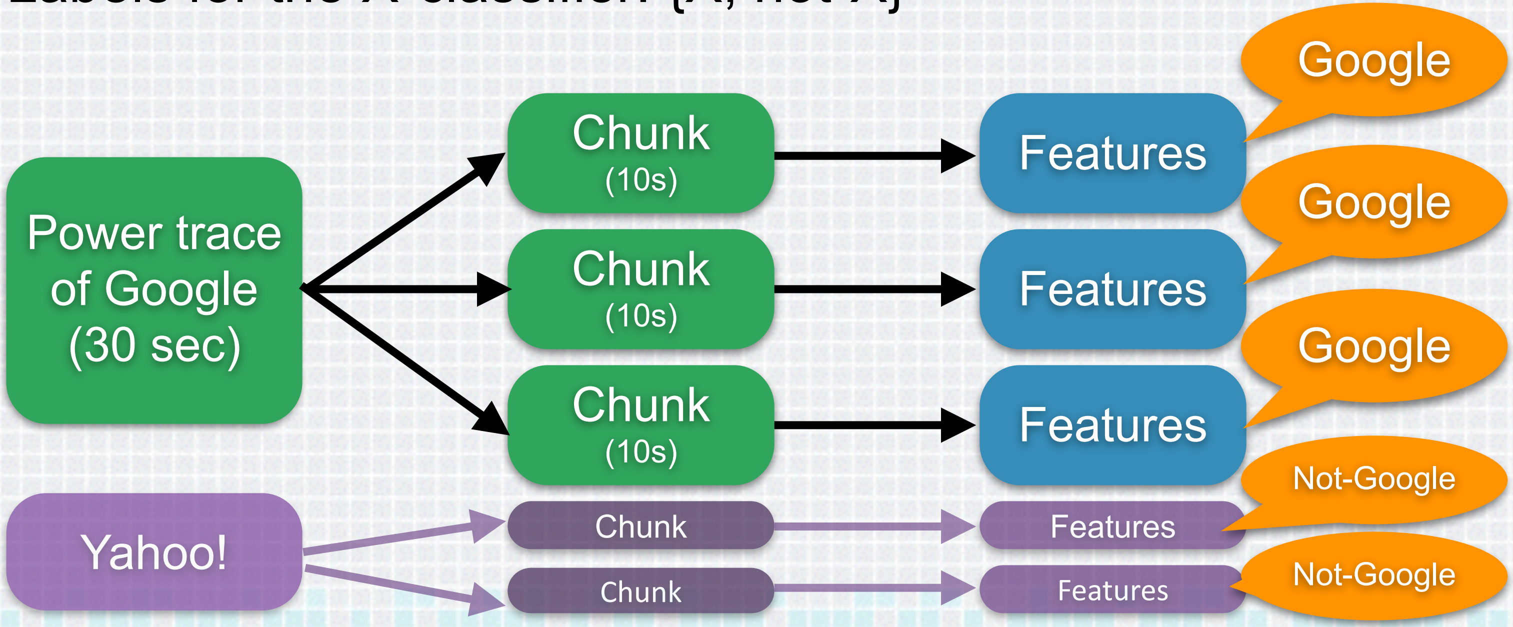


Google

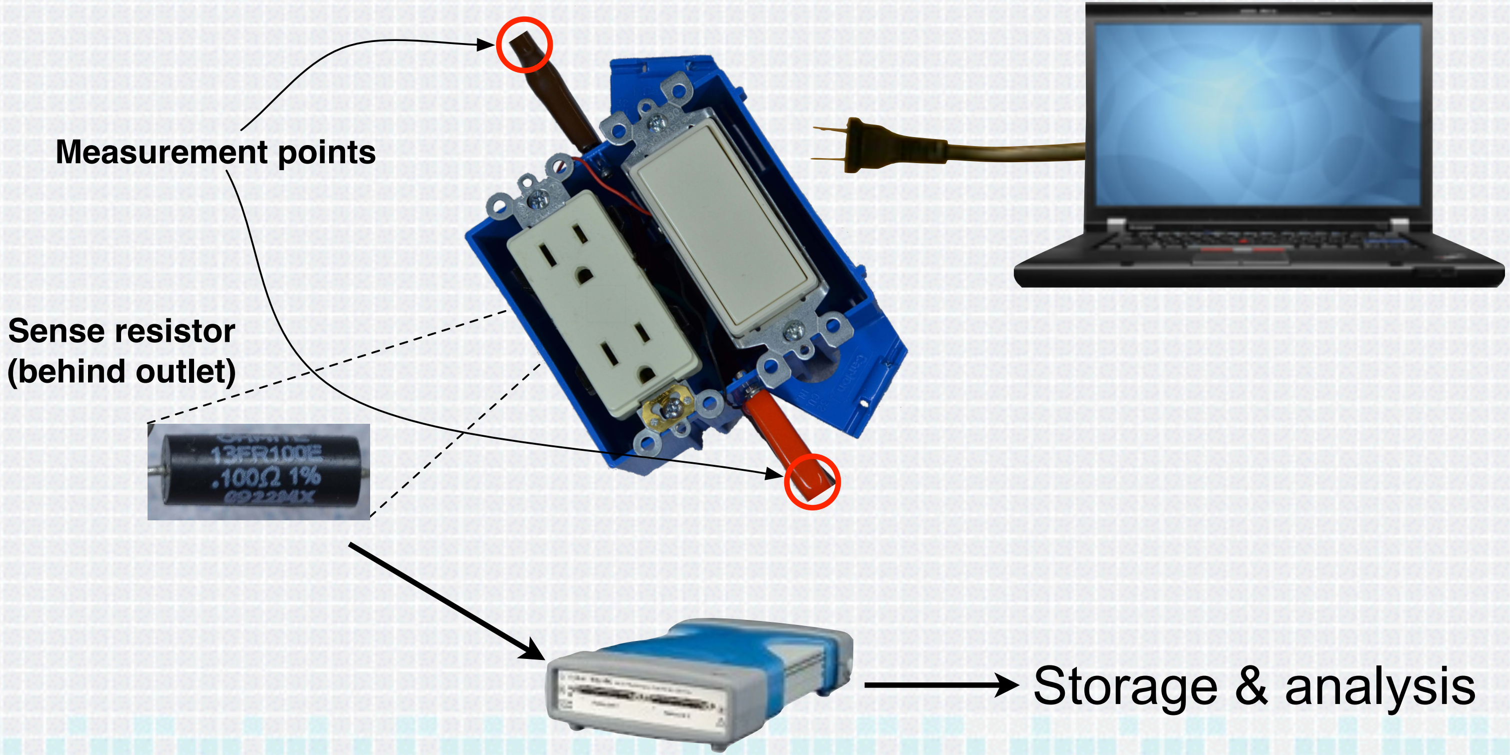


Training a Binary Classifier

- Supervised learning: assemble and label a training set
- Labels for the X-classifier: {X, not-X}



Instrumenting an Outlet



Measurement points

Sense resistor
(behind outlet)

Storage & analysis

Building a Training Set

- Instrumented outlet
- Scripted page loads + power traces
- 9,240 traces (~72 hours of traces)

Webpage Classification Results

- > 99% accuracy, 99% precision, 99% recall
  - > 98% accuracy excluding samples of 441 unknown webpages

- More details: *Current Events: Identifying Webpages by Tapping the Electrical Outlet*, ESORICS ’13

Robustness of Classification To Changes In…

- 🟩 Virtual private network encryption
- 🟩 Browser cache
- 🟩 Network interface
- 🟩 Background activities
- 🟩 Passage of time
- 🟨 Content distribution network
- 🟨 Physical location
- 🟥 Operating system
- 🟥 Hardware
- 🟥 Tor
- 🟥 Browser

🟩 Classifier still works

🟨 Classifier sort of works

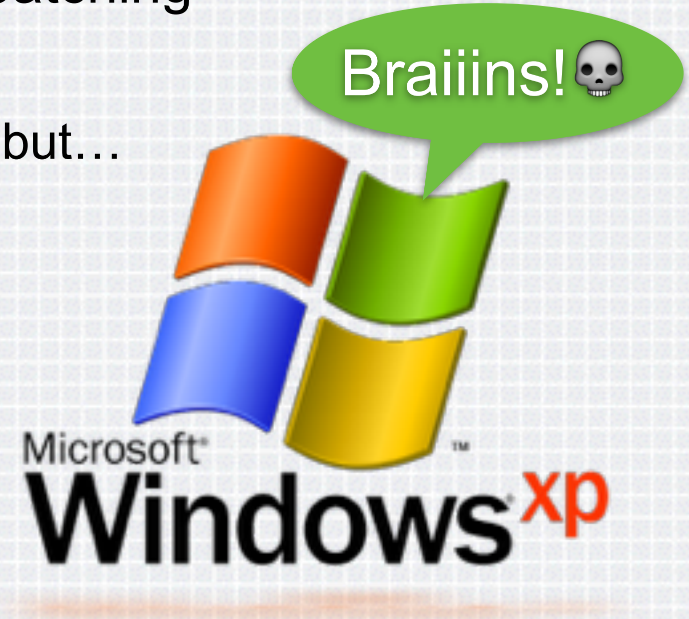
🟥 Classifier doesn’t work

AC Power Analysis for Other Domains

- Webpage identification is an **attack**
  - Spy on **people** by watching web traffic
- Defensive applications!
  - Turning traditional side channel analysis on its head
  - Spy on **malware** instead

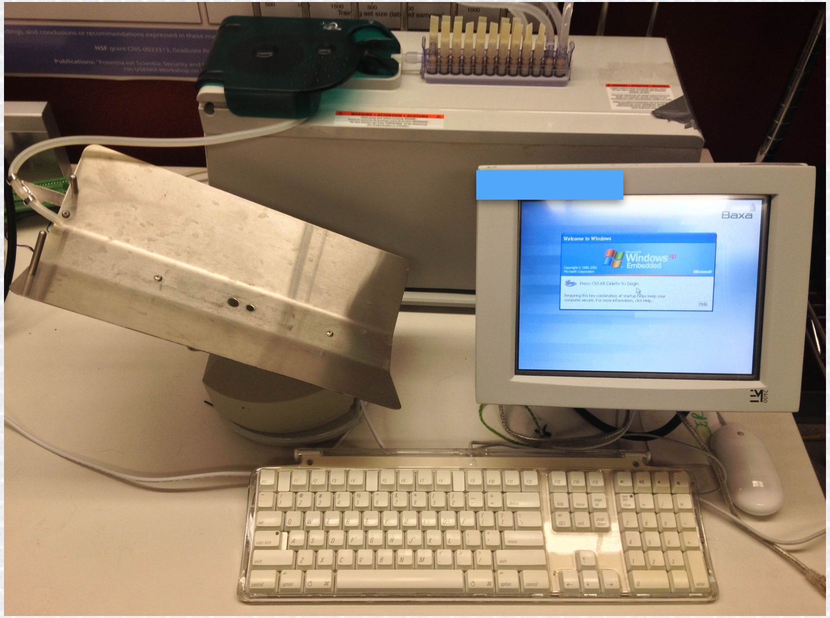
AC Power Analysis to Find Malware

- Motivation: Legacy devices without AV or patching
- Root causes:
  - COTS OS means short development cycle, but…
  - Many manufacturers lack upgrade path!
  - Zombie pseudo-embedded machines!
- Often can’t get inside the box
  - … or install software



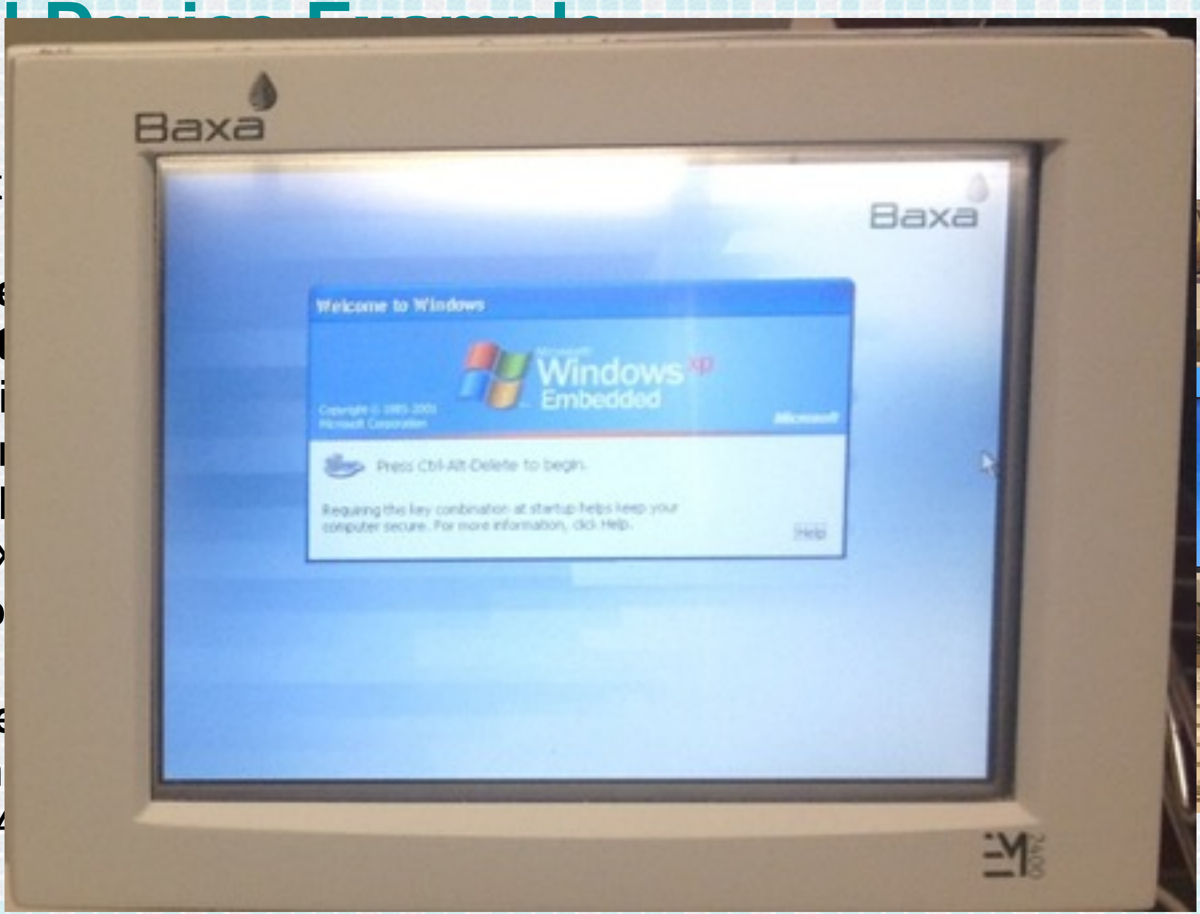
Medical Device Example

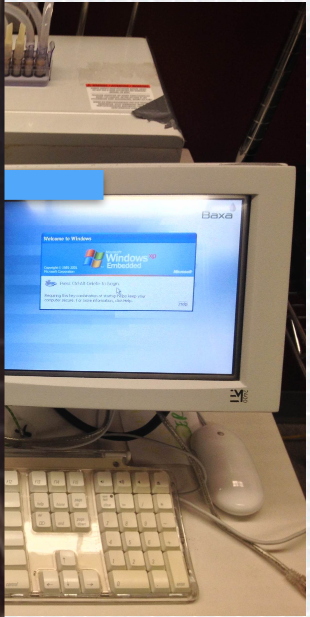
- “information systems department together with the pharmacy has **requested that [X] provide a microsoft security patch** to prevent this infection from occurring again. [X] is **unwilling to allow these patches** to be applied to the [X] [compounder]. Instead [X] has recommend that we place a router with the functionality for a **firewall between the compounder and the network** (b) (4) as protection.”
  —*FDA MAUDE report #*1621627



Medical Device Example

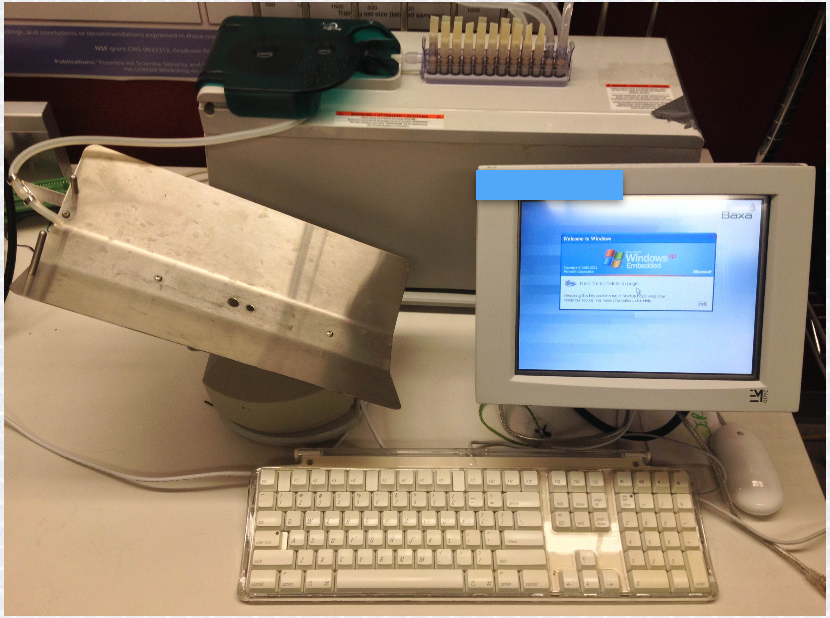
- “informat
together
requeste
microsoft
this infecti
is **unwilli**
to be appl
Instead [X
place a ro
a **firewall**
and the
protection
—*FDA MA*


Baxa
Baxa
Welcome to Windows
Microsoft Windows XP Embedded
Copyright © 1985-2001 Microsoft Corporation
Microsoft
Press Ctrl-Alt-Delete to begin.
Requiring this key combination at startup helps keep your computer secure. For more information, click Help.
Help
EM 2400



Medical Device Example

- "information systems department together with the pharmacy has **requested that [X] provide a microsoft security patch** to prevent this infection from occurring again. [X] is **unwilling to allow these patches** to be applied to the [X] [compounder]. Instead [X] has recommend that we place a router with the functionality for a **firewall between the compounder and the network** (b) (4) as protection."
  —*FDA MAUDE report #*1621627



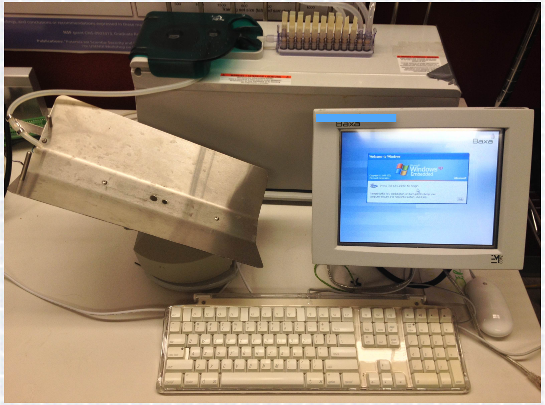
Other High-Assurance Examples

- Medical: infusion pumps, bedside monitors, fetal monitors…
- Industrial: SCADA systems
- Point-of-sale terminals
  - RAM scrapers steal payment card data! TARGET
- ATMs

- Common element: lagging software, difficult change management!

Image: APRO, Mongolia Tourism

IT Administrators’ Crucial Dilemma



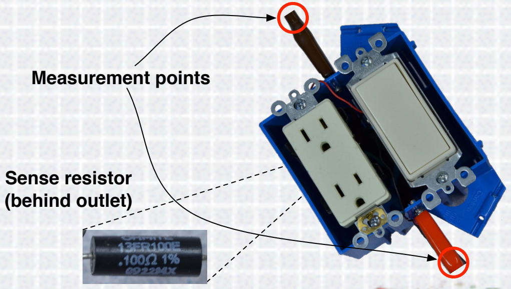
- Cannot patch or install AV
- Device serves a critical role
- **Take device offline** or **leave it unprotected**?

- Partial solution #1: NIDS for network traffic
  - Won’t find malware that doesn’t use network
- **Partial solution #2: Power analysis to find malware**

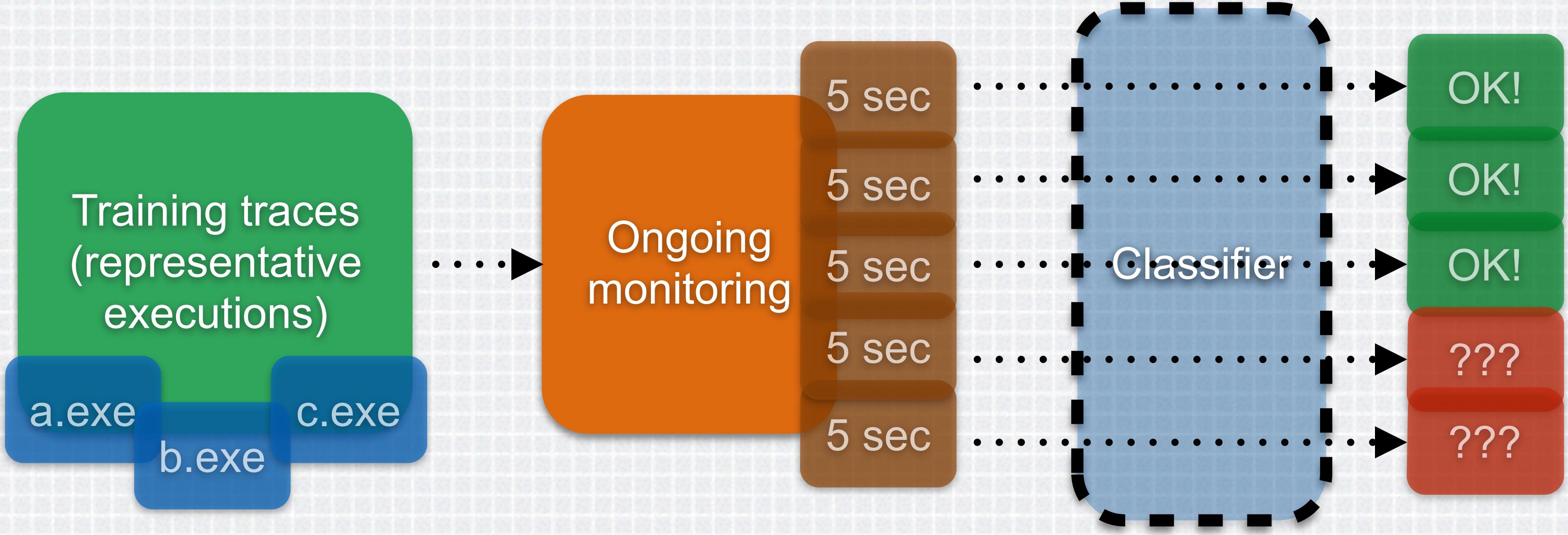
Power Analysis to Find Malware

- Like webpages, many software operations induce distinct power-consumption patterns
- Learn normal activity for a given machine
- Learn patterns of malware execution
- **Spy on execution** to look for unusual or alarming patterns suggesting malware

- Good visibility into *patterns* of operations
- Limited visibility into *individual* operations



Power Analysis Workflow: Anomaly Detection



Training traces (representative executions)

a.exe

b.exe

c.exe

Ongoing monitoring

5 sec

5 sec

5 sec

5 sec

5 sec

Classifier

OK!

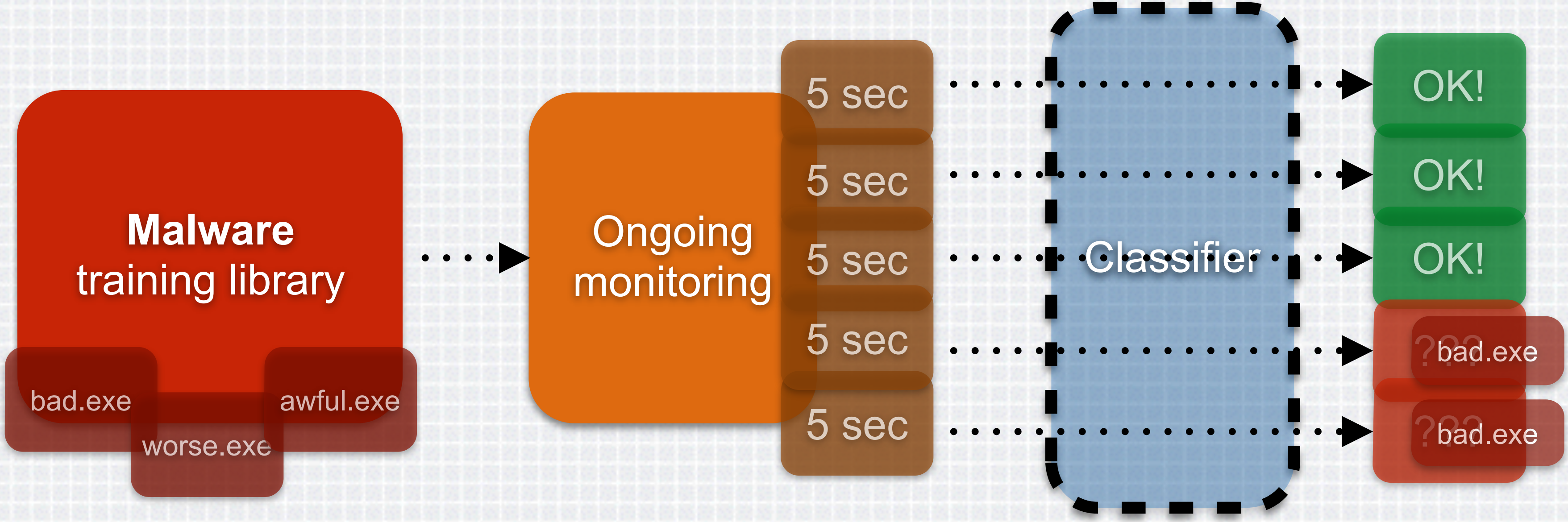
OK!

OK!

???

???

Power Analysis Workflow: Malware Detection



- On a pharmaceutical compounder:
  - 88.5% accuracy; **93.5% precision**; 92.1% recall

- On a SCADA substation computer (XP):
  - 84.9% accuracy; **98.3% precision**; 80.8% recall

- Simple technique already compares well to state-of-the-art malware detection (behavioral & signature-based)
- More: *WattsUpDoc: Power Side Channels to Nonintrusively Discover Untargeted Malware on Embedded Medical Devices*, HealthTech '13

RSAConference2015

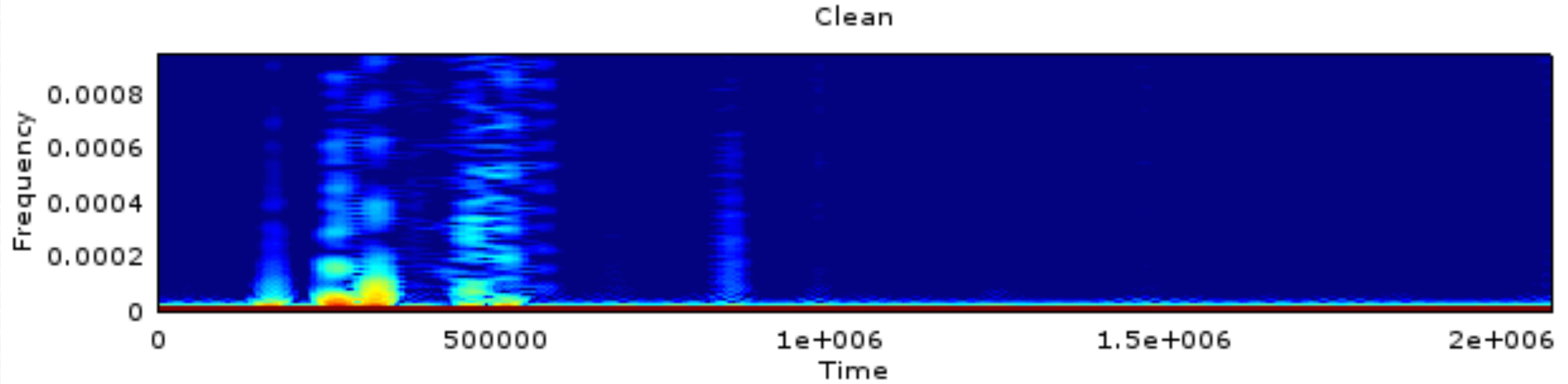
San Francisco | April 20-24 | Moscone Center

Demo: Detecting Malware on the Wire

#RSAC

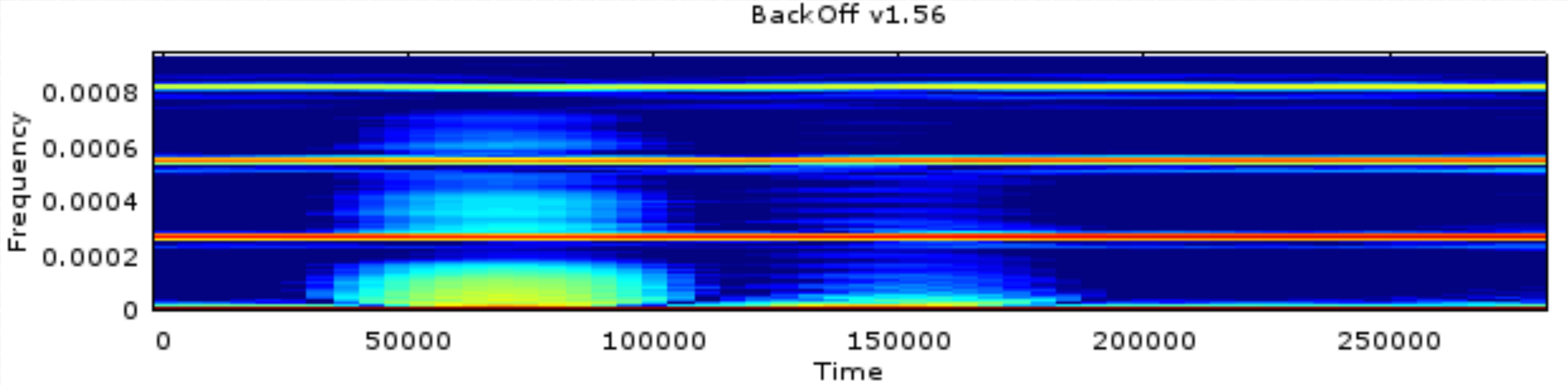
Example: RAM Scrapers

- This is what a clean system looks like
- Normal software activity shown on left side



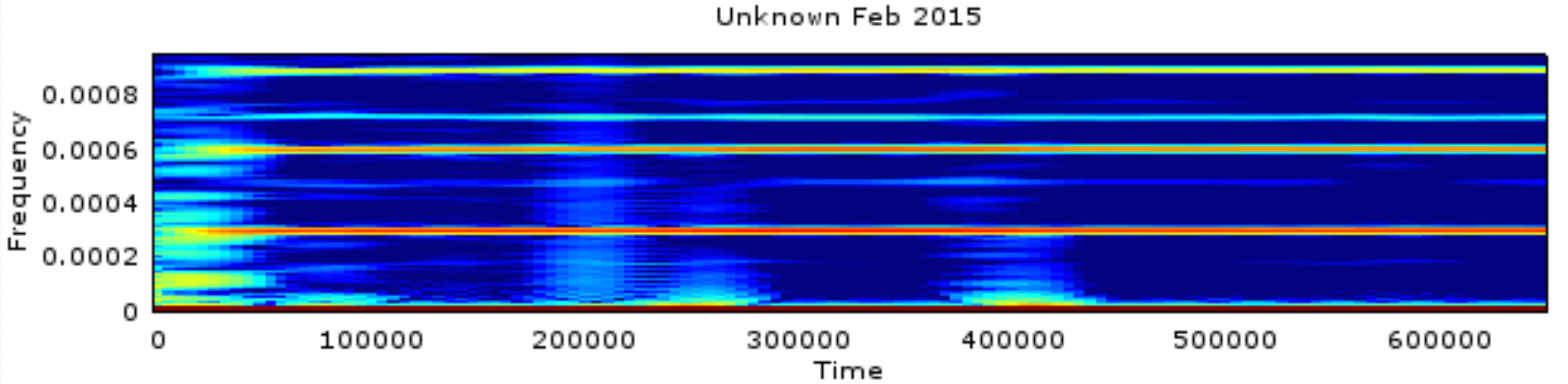
Example: RAM Scrapers

- This is the same system infected with BackOff v1.56
- Check out these horizontal lines

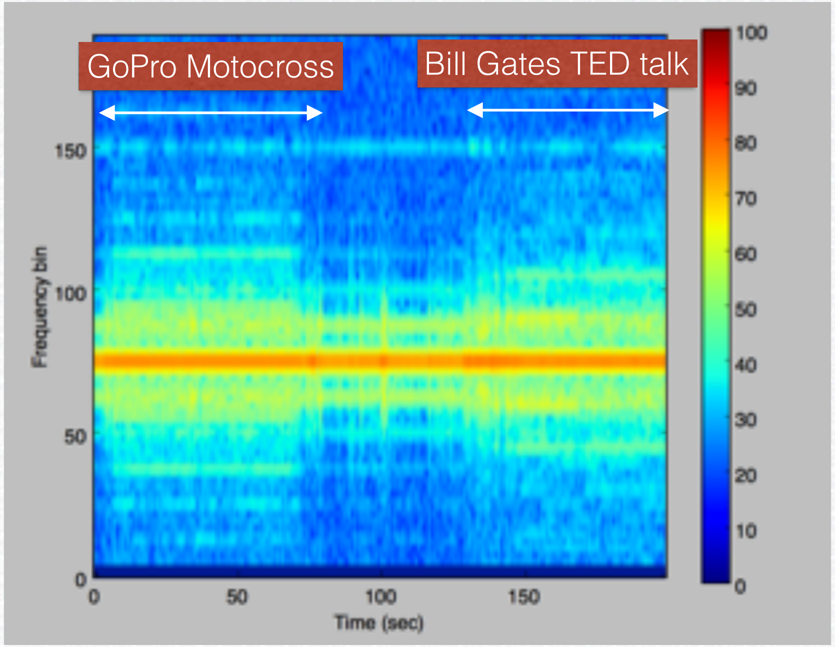


Example: RAM Scrapers

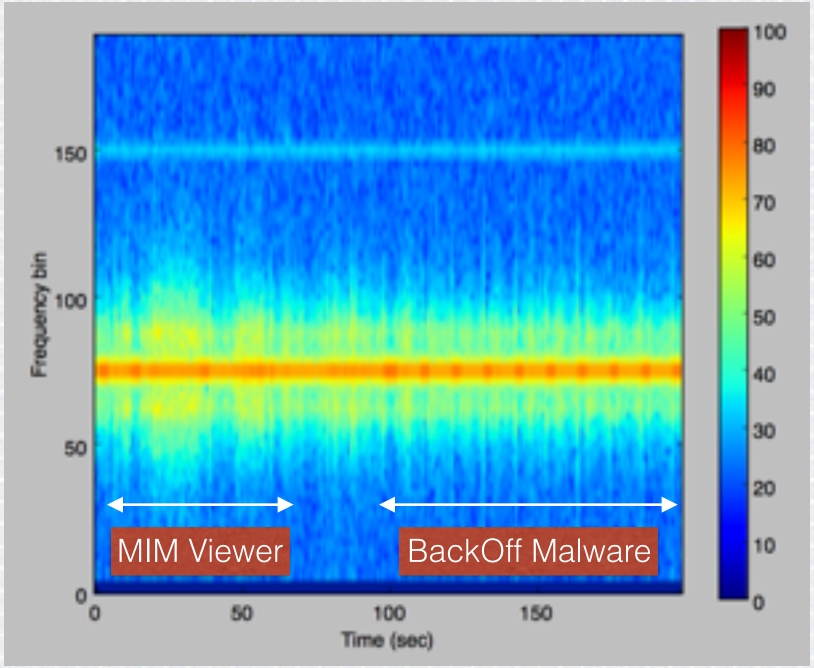
- This is the same system with 0-day variant of BackOff
- The features are recognizable!



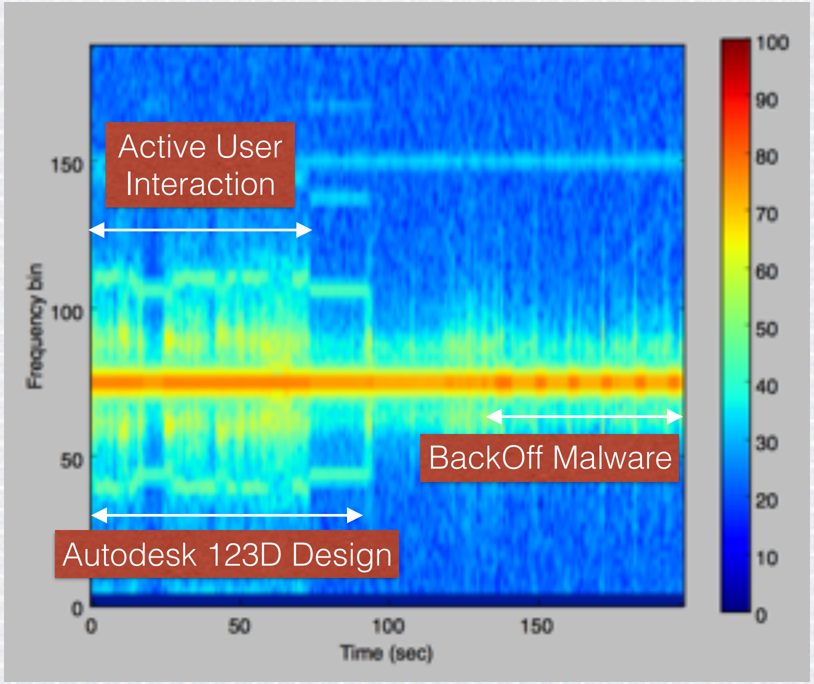
GoPro Motocross vs Bill Gates



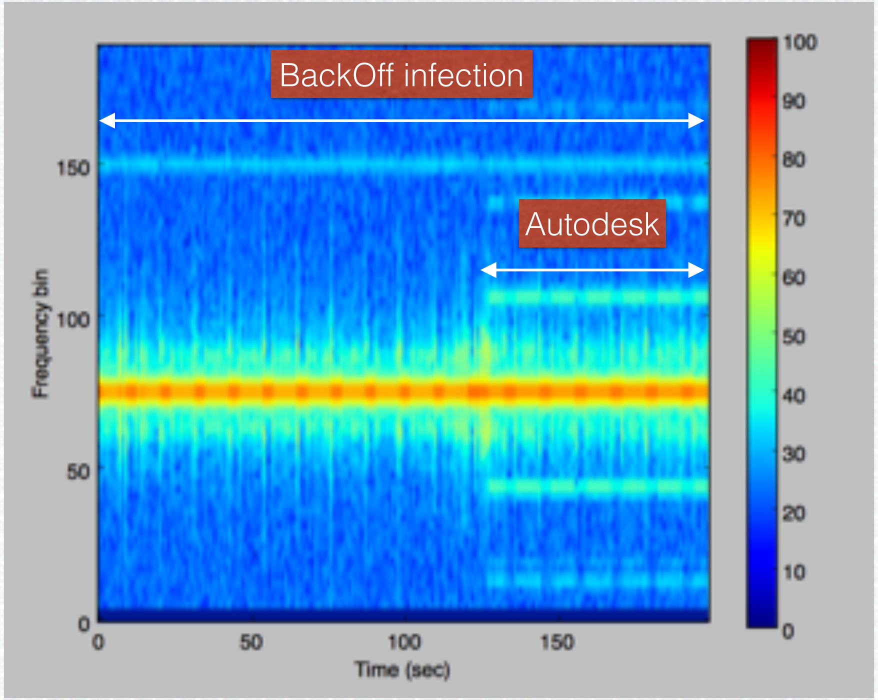
MIM vs BackOff



Autodesk vs BackOff



BackOff on top of Autodesk



Conclusion

- We need to think **outside the box** for endpoint security
  - Legacy devices: no good solutions for visibility/monitoring
  - Side channels can tell us information
  - Sometimes that information is useful
  - Sometimes it's just argyle

Apply: Find Unpatchable Systems

- High-assurance systems that don’t go out of service
- Systems that have undergone extensive regulatory testing
- Systems that are simply old

- *If you work in a medical environment: get MDS2 forms and keep bothering manufacturers!*

Image: Crashspotting

RSAConference2015

San Francisco | April 20-24 | Moscone Center

#RSAC

{ben, denis}@virtalabs.com

https://www.virtalabs.com/