Future Directions in Malware Detection on Mobile Handsets

Leaving the as-is state for the better?

André Egners, RWTH Aachen

ASMONIA

- Funded by German government
- Industry, Research, Telco, Government

- *Attack Analysis and Security Concepts for MObile Network Infrastructures supported by collaborative Information Exchange*
  - Network infrastructure
    - HeNB, eNB, SAE-GW, …
  - User equipment
    - Phones, dongles, Smartphones (this talk)

- What’s my task in ASMONIA?
  - Security mechanisms on Smartphones
  - (New) infection vectors
  - Malware detection on UE and NE

Disclaimer

This talk is not “the solution” but rather to raise awareness and inspire ideas

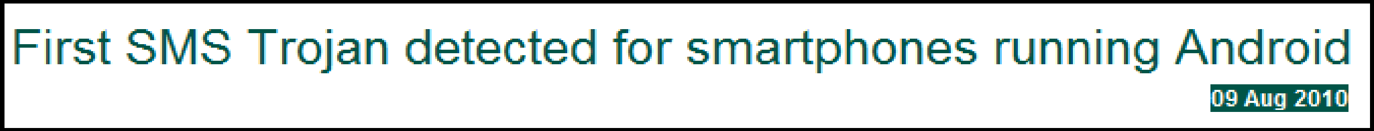
Outline

- Introduction
- Motivation
- The Problems
- Alternative mechanisms
- Deployment ideas
- Open problems

Smartphones

- Multi-purpose
- Mobile internet
- GPS, WLAN, …
- 3rd party apps
- More computer than phone
- “Unmanaged mess” (Enno)

Tales from the “Smartphone Hell”



First SMS Trojan detected for smartphones running Android

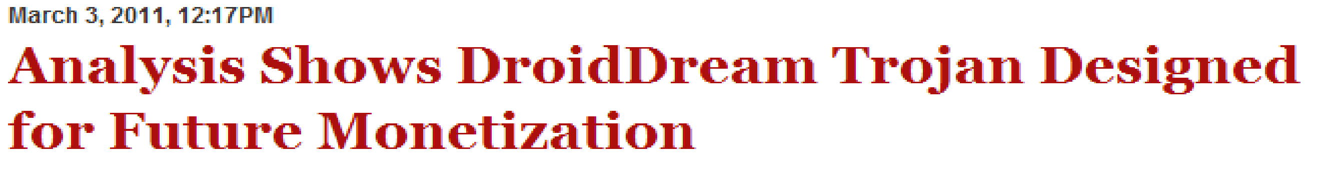
09 Aug 2010

August 19, 2010, 11:35AM

iPhones, BlackBerrys, Droids Becoming a Moveable Feast for Attackers

March 2, 2011, 3:19PM

DroidDream Attack Underscores Weaknesses of App Stores



March 3, 2011, 12:17PM

Analysis Shows DroidDream Trojan Designed for Future Monetization

More Hellish Tales

The General Problems

- Malware, Trojans, (viruses)
- Issues with current detection from classical IT
  - Signature-based
  - Aftercare
  - External experts
  - Computation and storage overhead
- May not be suited for Smartphones
  - Still significantly slower
  - Frequent scanning is energy intensive

Smartphone Induced Challenges

- Many different OSs
- Many different software distribution paths
- Many different communication interfaces
  - 2/3/4G, Wi-Fi, BT, (NFC)
- Many different hardware vendors
  - ACER, Samsung, HTC, LG, Motorola, …
  - Different OS image
  - Different update cycle
- Even OS distributors may stop updating older devices
- Android: Inflationary usage of permissions

Attacks

- Privacy leakage
- Battery depletion
- Send SMS messages
- Infect files
- Spread to PC
- Block functionality
- Change user settings
- Demand money and delete incoming and outgoing SMS
- Disable / fake AV products
- Monitor user
- Damage user data
- Cause damage to xG network (Botnets)

Alternative Detection Methods

- Monitor behavior
  - Of user
  - Of app
  - Of Phone
  - …
- Compare monitored traces to model
  - Resembles benign behavior
  - May point out unknown/suspicious incidents
  - Iterative learning
- Profit from data mining research
- Allows partial matching wrt. known good behavior

Roadmap

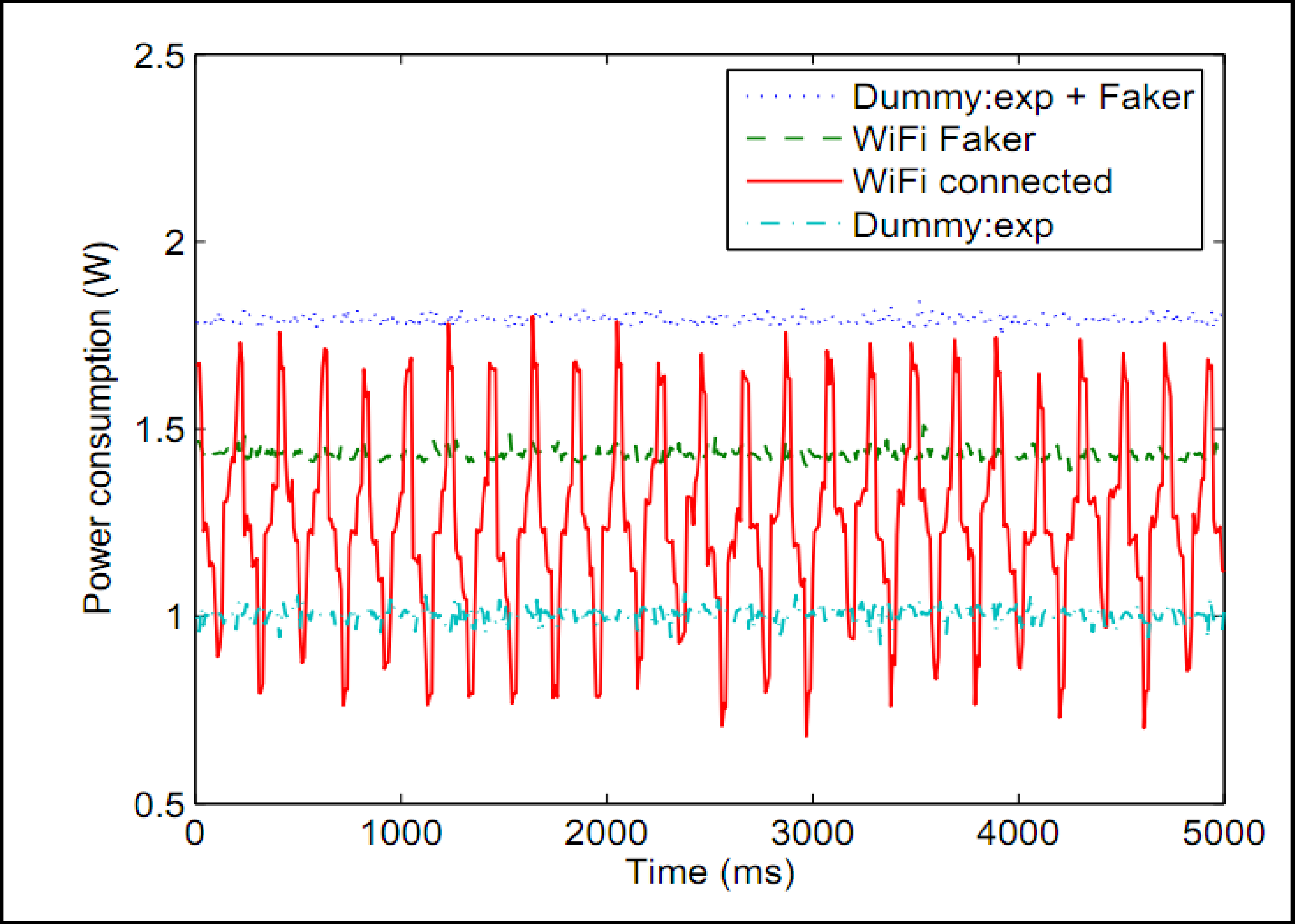
- Energy-greedy malware (2008)
- Symbian OS monitoring (2008)
- SMS-Watchdog (2009)
- User & App correlation (2010)
- General machine learning (2010)

Energy Greedy Malware [KSK08]

- Initial motivation:

  Improve effectiveness to detect new outbreaks
- Focus on energy depletion threats
- Power monitor
  - Collects power samples and builds history
  - Based on available CE .Net API
- Data analyzer
  - Power signature generation & matching
  - Local or remote processing
- Experiments on HP iPAQ (WM5)

Energy Greedy Malware [KSK08]



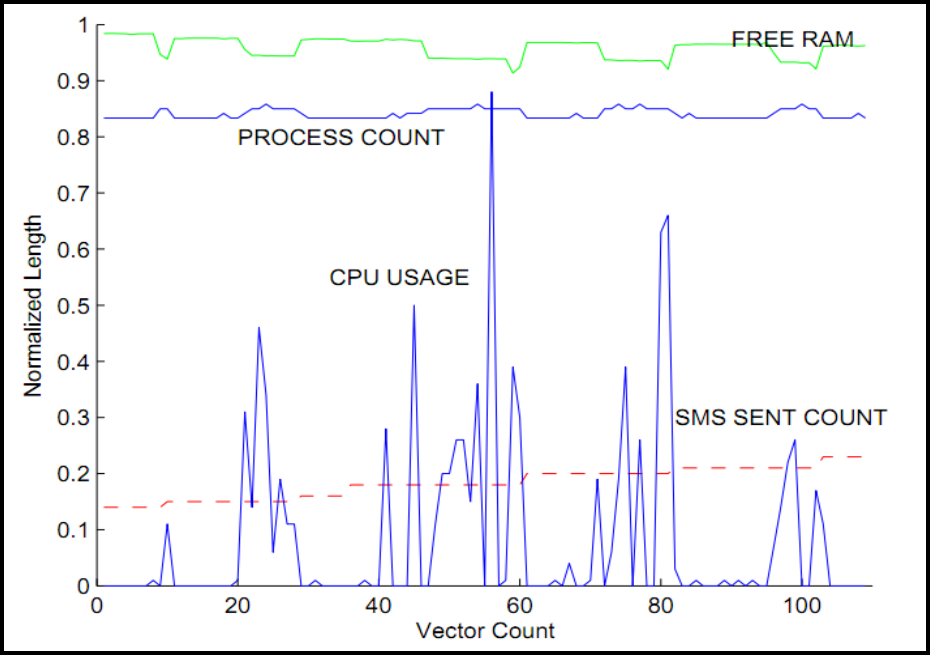
Energy Greedy Malware [KSK08]

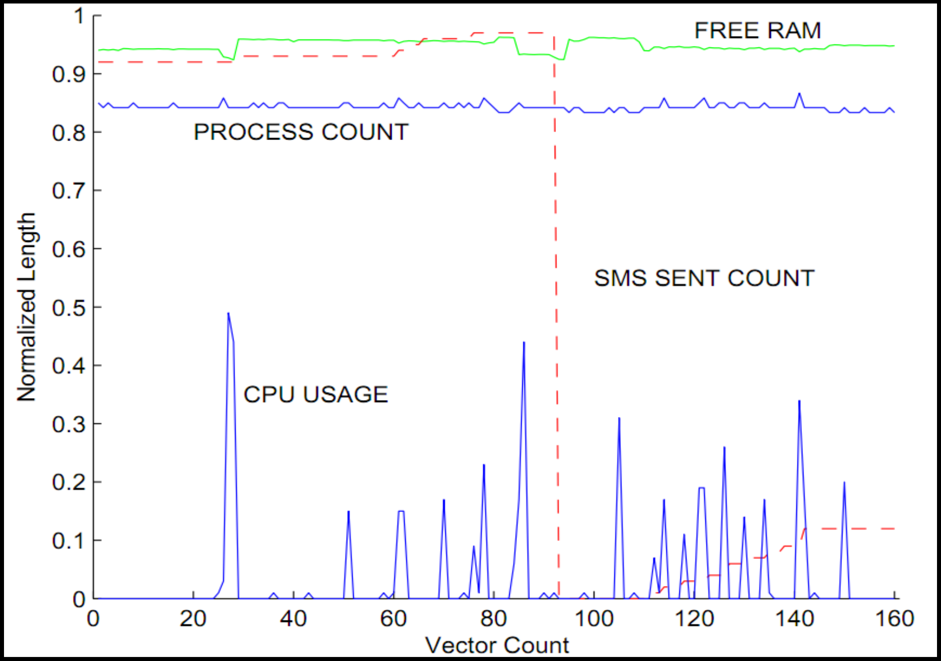
- Is energy really scarce?
  - How many mini-/micro USB cables do you have on you right now?
  - Free USB power outlets in airports
- Kind of outdated
  - Assumes one running app
- It’s not really the business model of (Botnet) malware to make a host go offline

Monitoring Smartphones … [SPAL08]

- Symbian-based monitoring
- Move processing to remote system (newspeak: cloud)
  - Less processing power on phone
  - Less storage on phone
  - Secure always-on connection
- Fingerprinting the app
  - RAM FREE
  - USER INACTIVITY
  - PROCESS COUNT
  - CPU USAGE
  - SMS SENT COUNT

Monitoring Smartphones … [SPAL08]





SMS Sending vs. SMS-Malware

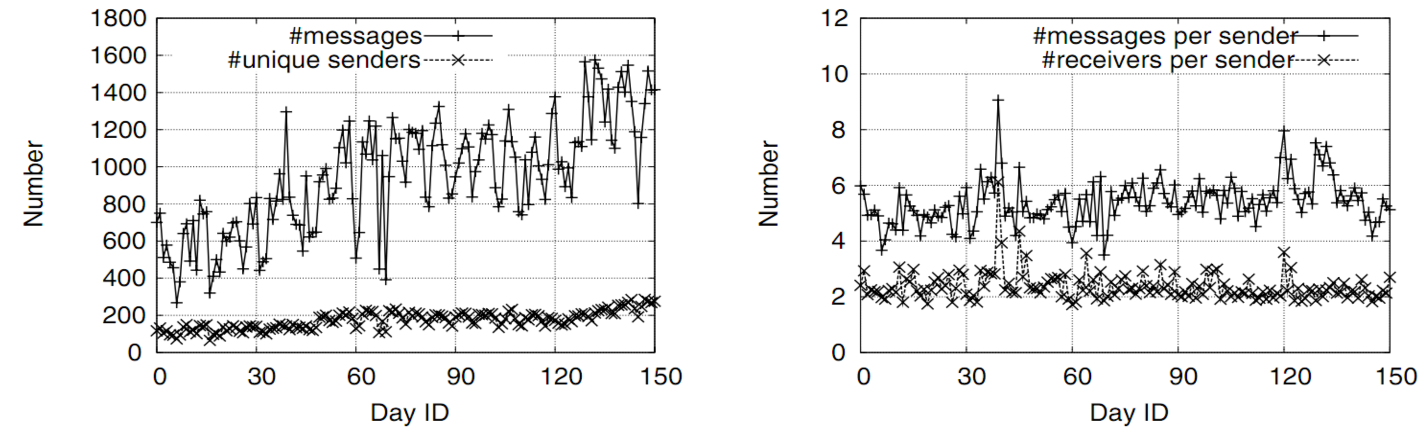
Monitoring Smartphones … [SPAL08]

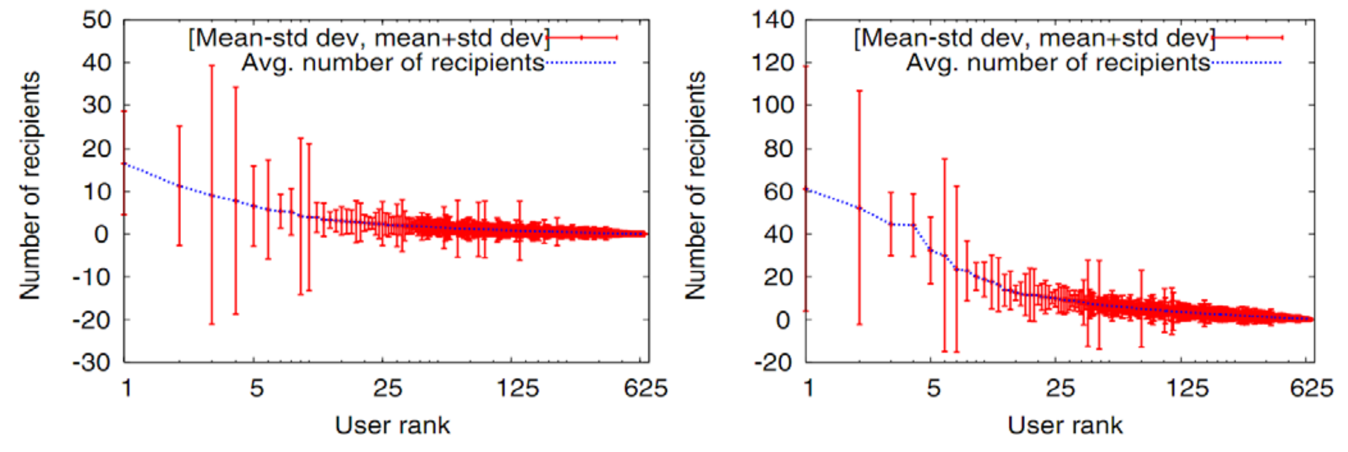
- Demonstration of “app fingerprinting”
  - Apps affect features in distinct ways
- Verification by “Button-2-pressed-Send-SMS”-malware
- Remote processing may cause additional risks
- How well does it work across different phones?

SMS-Watchdog [YEG09]

- Focus on SMS-based attacks and spreading
  - SPAM (unwanted, costly, increased netload)
  - Spoofing (of senders, potentially useful for phishing)
  - Flooding (increased netload)
  - Faking (mimicking SMSC behavior)
- Collect SMS traces of users
- System is deployed on SMSC (NE)
- Detect deviation from known behavior profile
  1. Monitor user for some time
  2. Anomaly detection at intervals
  3. Inform user about possible malware

SMS-Watchdog [YEG09]





(1) Daily (2) Weekly

SMS-Watchdog [YEG09]

- High variation unsuited for detection model
- Improvement by computing similarities between monitor windows
- Min # SMS required to make model work
- Unclear how to obtain the “normal”-trace
- Model needs extensive training per user
- Are there legal implications?

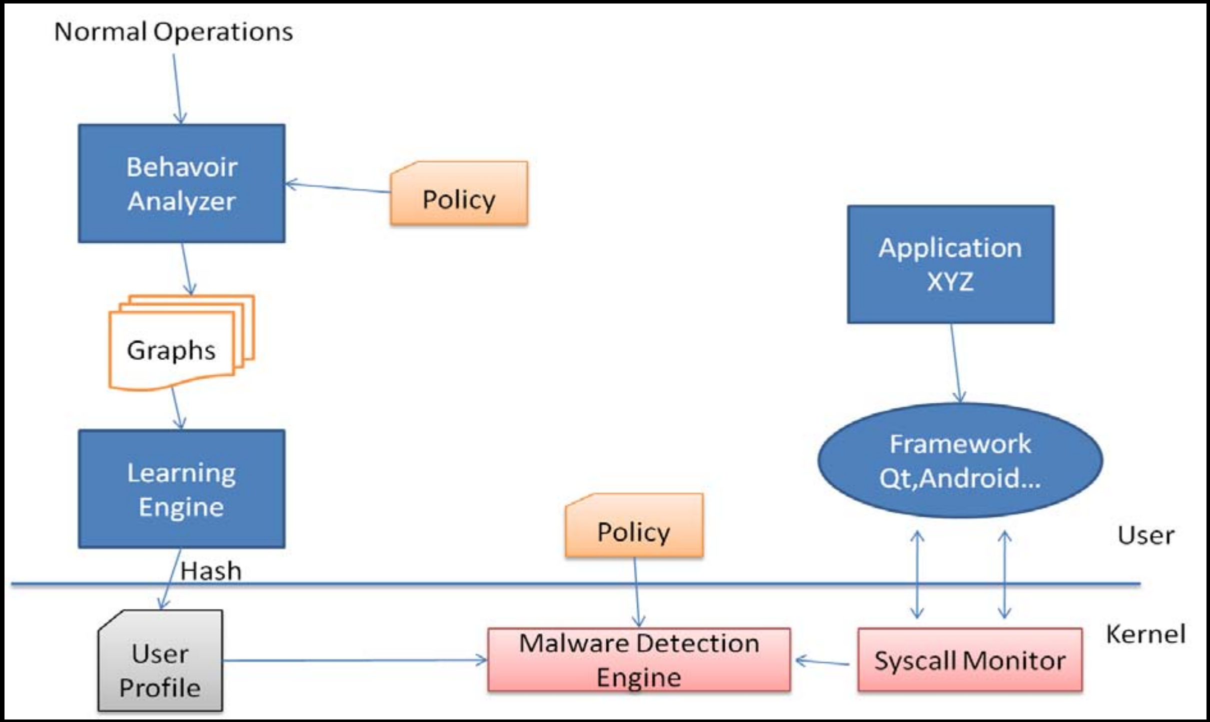
pBMDS [XSZZ10]

- Behavioral differences between:

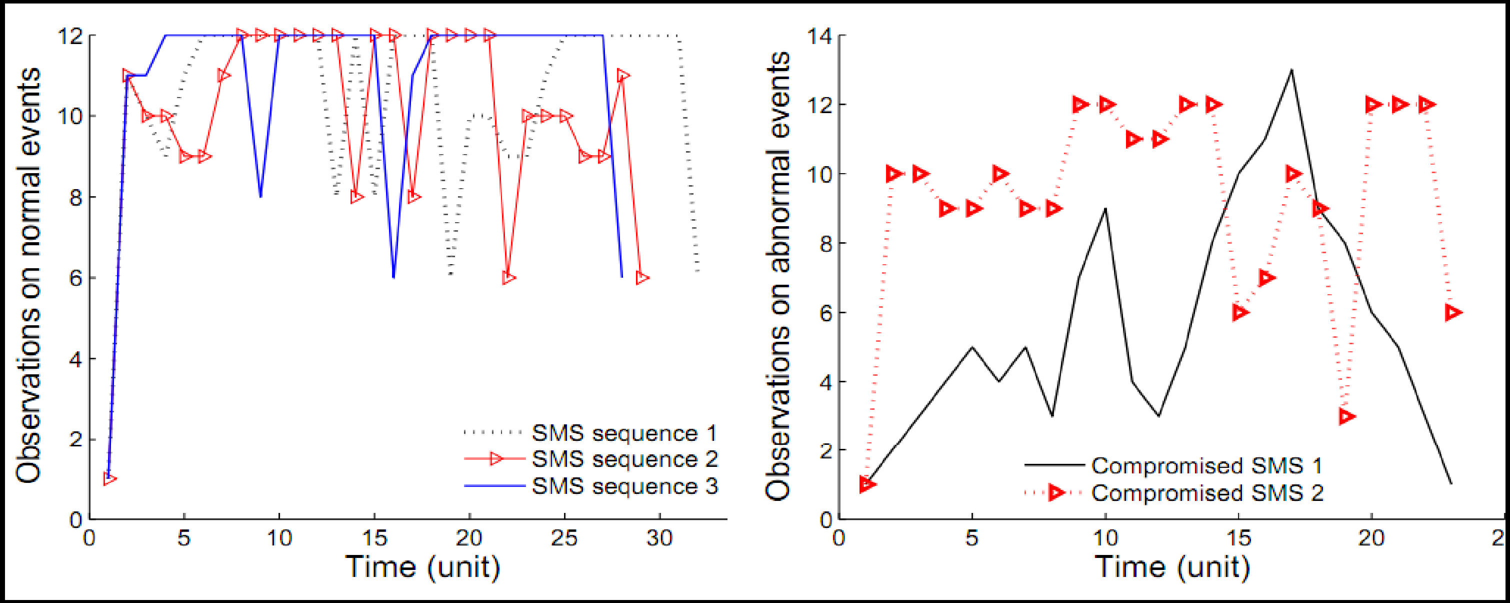
  malware and users
- Correlating user input and syscalls
  - Process state transitions
  - User operational patterns
- Scope:
  - Real phone evaluation
  - MMS & BT spreading
  - Application level attacks

pBMDS [XSZZ10]

- User action => series of syscalls unique to action
  - Deviation from regular behavior
  - Predictability of actions



pBMDS [XSZZ10]

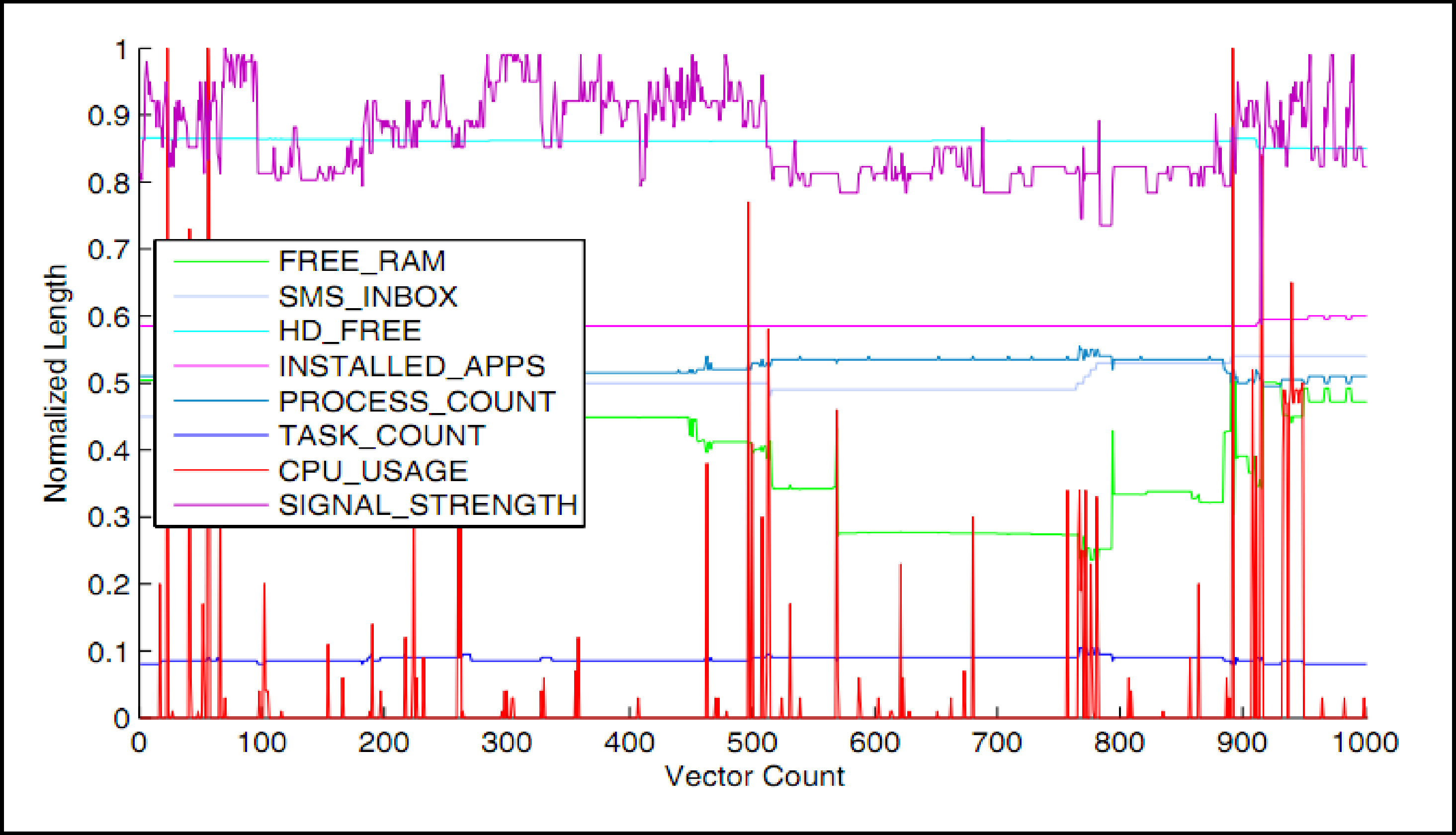


- Input events can be simulated by (smart) malware
- SMS sequenced behavior is biased
- Turing test deals with false positives
- Intrusive mechanism (kernel hooks)

Anomaly Detection … [ABS10]

- General model
- Based on device usage patterns
- “Observable features” mapped to vector
- Experimenting with similarity measures
  - ECD (6-dim & 40-dim)
  - Mahalanobis distance (6-dim)
  - Self-organizing maps (6-dim)
  - Kullback-Leibler divergence (6-dim)

Anomaly Detection … [ABS10]



1000 sample normal usage pattern

IT | SEC

Anomaly Detection … [ABS10]

- Remote processing
- Training data is highly biased
  - Public MIT volunteer data set
  - Calls, SMS, and data communication logs
- Verification by “Button-2-pressed-Send-SMS”-malware
- Challenge of non-stationary usage behavior
  - E.g., new apps

Methods Summary

- Basically feature extraction is done on
  - User behavior
  - System behavior
  - Application behavior
- Communication monitoring
  - SMS, Bluetooth, WLAN, etc.
- Application of classification and clustering methods
  - Support vector machines: Good/Bad behavior classes
  - Probabilistic learning
- General fine tuning of matching methods

Hmmm…

so now what needs to be done to put these mechanisms to work?

Deployment Ideas

- Think telco
  - Large user base
  - Monitoring is possible
  - Use branding as a basis?
- Think app store
  - Large user base
  - Initial good behavior could be supplied along with app
    - How to trust this?
  - Feedback loop from user behavior
- Think OS
  - Why not push security updates as in Linux distributions

Open Issues

- Signature-based detection rarely has false alarms
- Is the user feedback loop useless?
  - The “ok, leave me alone”-hazard
- Sanity check of detector by asking user
  - “Do you think this is suspicious?”
- Which inputs are “good”?
  - Fight the bias
- Where to monitor?
  - Local vs. in network
- Where to process?
  - Local vs. remote
- Risks of monitoring?
  - Trust, Privacy?

Open Issues (2)

- Statistical methods lack semantic capabilities and contextual information
  - Challenge to distinguish rare behavior from malware
- Can we use in-place security mechanisms as sensors?
  - Permissions
  - Integrity checks
  - Trusted boot
  - …
- How to keep up with the progress

To-do

- Experimentation and practical validation is needed
- Research across platforms
- Consider new input for monitoring
    - overwriting and accessing specific files
    - Voice, Data, downloading from suspicious sources
    - …
- App profiling
- Keep up with the progress on Smartphones ;)

IT | SECURITY
RESEARCH GROUP

Thanks for the attention

André Egners
egners@umic.rwth-aachen.de

References

[ABS10] Alpcan et al., *A Probabilistic Diffusion Scheme for Anomaly Detection on Smartphones,* WISTP 2010

[KSS08] Kim et al., *Detecting Energy-Greedy Anomalies and Mobile Malware Variants*, MobiSys 2008

[SPAL08] Schmidt et al., *Monitoring Smartphones for Anomaly Detection*, Mobilware 2008

[XSZZ10] Xie et al., *pBMDS: A Behavior-based Malware Detection System for Cell Phone Devices*, WiSec 2010

[YEG09] Yan et al., *SMS-Watchdog: Profiling Behaviors of SMS Users for Anomaly Detection*, RAID 2009

Me

- Obviously IT-Security interested
- CS Diploma from Aachen with (anonymity) networking background
- Now PhD studies @ ITSec Research Group
- Field of research: Security in wireless networks
  - Key Management
  - Security Bootstrapping
  - IDS / Monitoring
  - 4G networks and phones (ASMONIA)