Surveillance of small-scale systems

Chamseddine Talhi

École de technologie supérieure (ÉTS)

Dép. Génie logiciel et des TI

Agenda

- Project Presentation
- Why surveillance of small-scale systems?
- Small-scale Systems of interest
- Host-Based surveillance: challenges & alternatives
- Ongoing activities
- Feedback?

Project Presentation

- New research thread to Advanced Host-Level Surveillance: since September 2013 ... 1 year project!

- Team:
  - 1 professor
  - 2 Master students
  - 1 research professional
  - Part-time students

- Objectives:
  - Surveillance of small-scale systems
  - Use of small-scale systems (possibly highly parallel) for the surveillance of other systems

Agenda

- Project Presentation
- **Why surveillance of small-scale systems?**
- Small-scale Systems of interest
- Host-Based surveillance: challenges & alternatives
- Ongoing activities
- Feedback?

Small-scale systems, why?

From Mobile Phones to general-purpose small devices

- « Cabir » 2004 : first mobile phone malware
- « CommWarrior » & « Doomboot » 2005 :
- And …

2 years of mobile malware evolution <=>

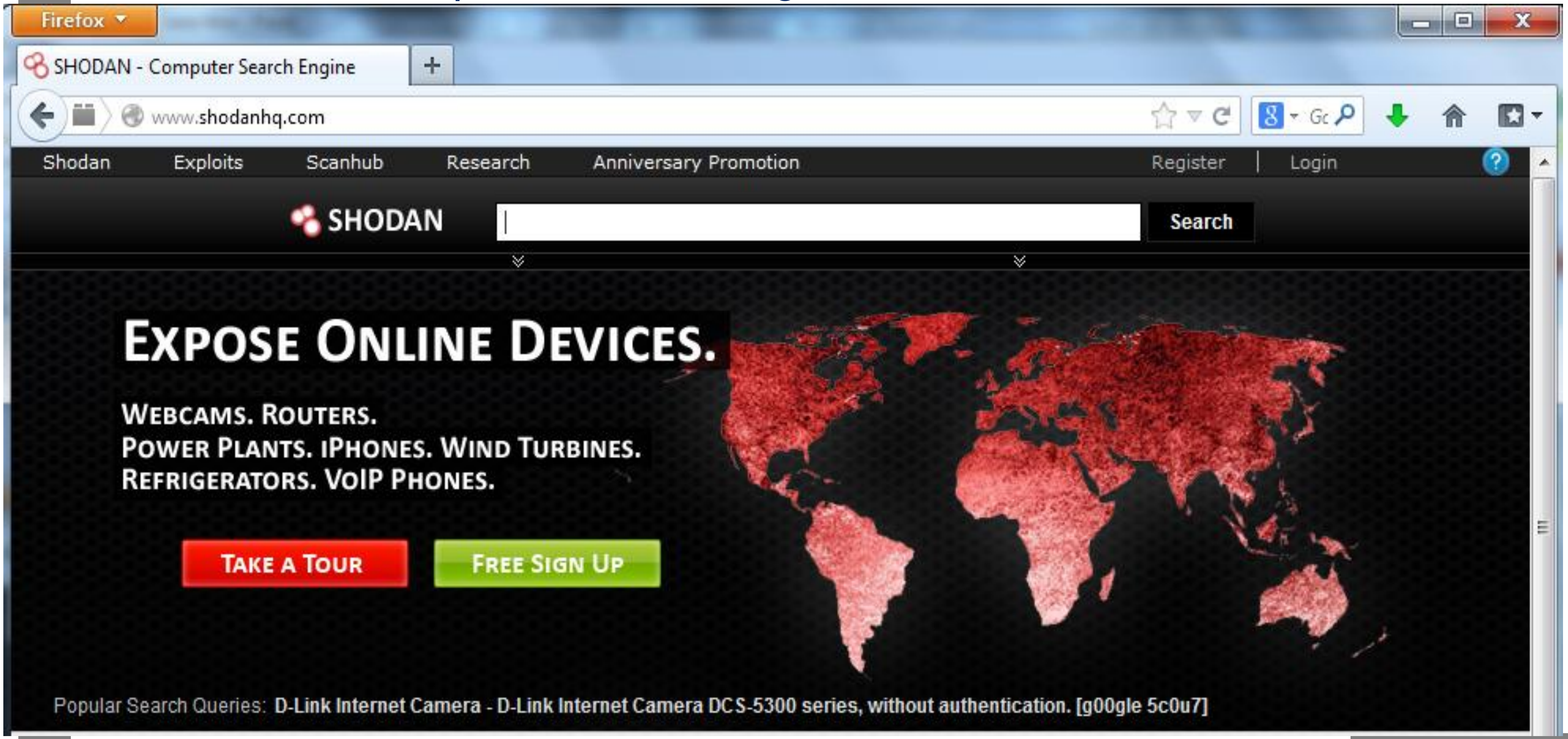
20 years of Computer malware evolution!!!

Name	Variant	Type of malware	Discovered	Actions	Infection vector	Encrypted	Distribution potential	Damage potential
Droid09	A	Full-Malware	Nov. 2009	Phishing targeted banks	Installing an APK file	No	Low	High
FakePlayer	A	Full-Malware	Aug. 2010	Sends SMS w/o user's knowledge to premium numbers	Installing an APK file	No	Low	High
	B	Full-Malware	Sept. 2010	Sends SMS w/o user's knowledge to premium numbers	Installing an APK file	No	Low	High
	C	Full-Malware	Oct. 2010	Sends SMS w/o user's knowledge to premium numbers	Installing an APK file	No	Low	High
Geinimi	A	Packaged-Malware	Jan. 2011	Sends information to the attacker Kills legitimate processes Performs web queries Changes wallpaper	Installing an APK file	No	Low	Low
ADRD	A	Packaged-Malware	Feb. 2011	Steals information	Installing an APK file	No	Medium	Low
PjApps	A	Packaged-Malware	Feb. 2011	Navigates to websites Sends SMS Installs packages Adds bookmarks	Installing an APK file	No	Medium	Medium
DroidDream	A	Packaged-Malware	Mar. 2011	Steals information Can root the device and install packages	Installing an APK file	No	Low	Medium
DroidKungFu	A	Packaged-Malware	May 2011	Steals information Communicates with Command & Control server Can root the device Gets access to files, install/ remove packages	Installing an APK file	Yes	Low	High
Basebridge	A	Packaged-Malware	May 2011	Installs applications with user's authorization Sends SMS w/o user's knowledge to premium numbers Make high cost phone calls	Installing an APK file	Yes	High	High
Denofow, aka Smspacem	A	Packaged-Malware	May 2011	Sends SMS w/o user's knowledge to contact list Steals information Changes wallpaper Executes commands from Internet/SMS	Installing an APK file	No	Low	Low
Raden, aka Zsone	A	Packaged-Malware	May 2011	Subscribes the user to premium number service w/o his knowledge	Installing an APK file	No	Medium	High
DroidDreamLight	A & B	Packaged-Malware	May 2011	Steals information Can root the device and install packages	Installing an APK file	No	Low	Medium
Plankton	A	Packaged-Malware	June 2011	Steals information Communicates with Command & Control server Downloads/updates .jar files from server	Installing an APK file	No	Low	Medium
GoldDream	A	Packaged-Malware	July 2011	Steals information Installs/executes/uninstalls packages Make phone calls w/o user's knowledge Sends SMS w/o user's knowledge	Installing an APK file	No	Low	Medium
Zeus	A	Full-Malware	July 2011	Attacks authentication mecanisms of banks' sites	Installing an APK file	No	Medium	High

Small-scale systems, why?

Small-scale systems are not limited to Smartphones!

- Linux/Android based devices.
- Shodan : Computer Search Engine

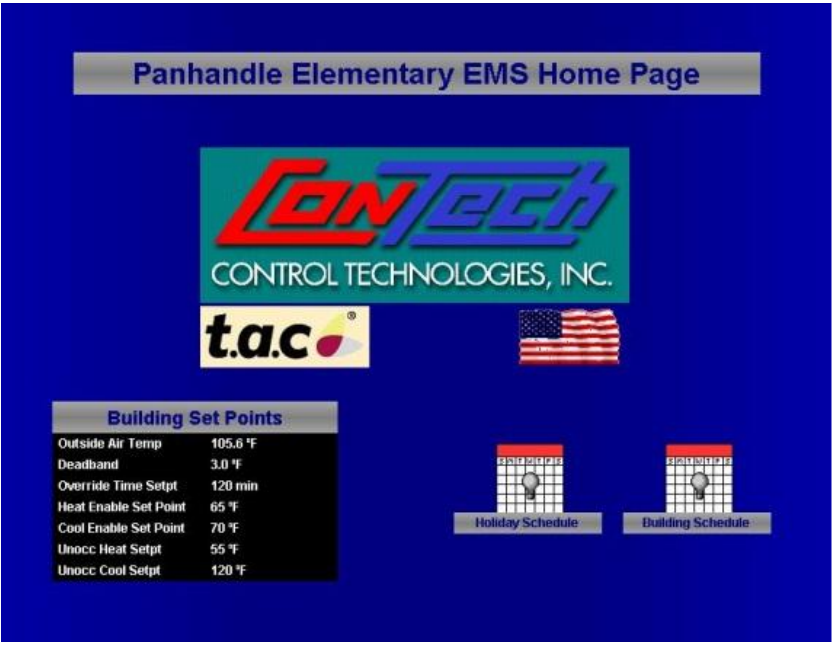


EXPOSE ONLINE DEVICES.

WEBCAMS. ROUTERS.
POWER PLANTS. IPHONES. WIND TURBINES.
REFRIGERATORS. VOIP PHONES.

Popular Search Queries: D-Link Internet Camera - D-Link Internet Camera DCS-5300 series, without authentication. [g00gle 5c0u7]

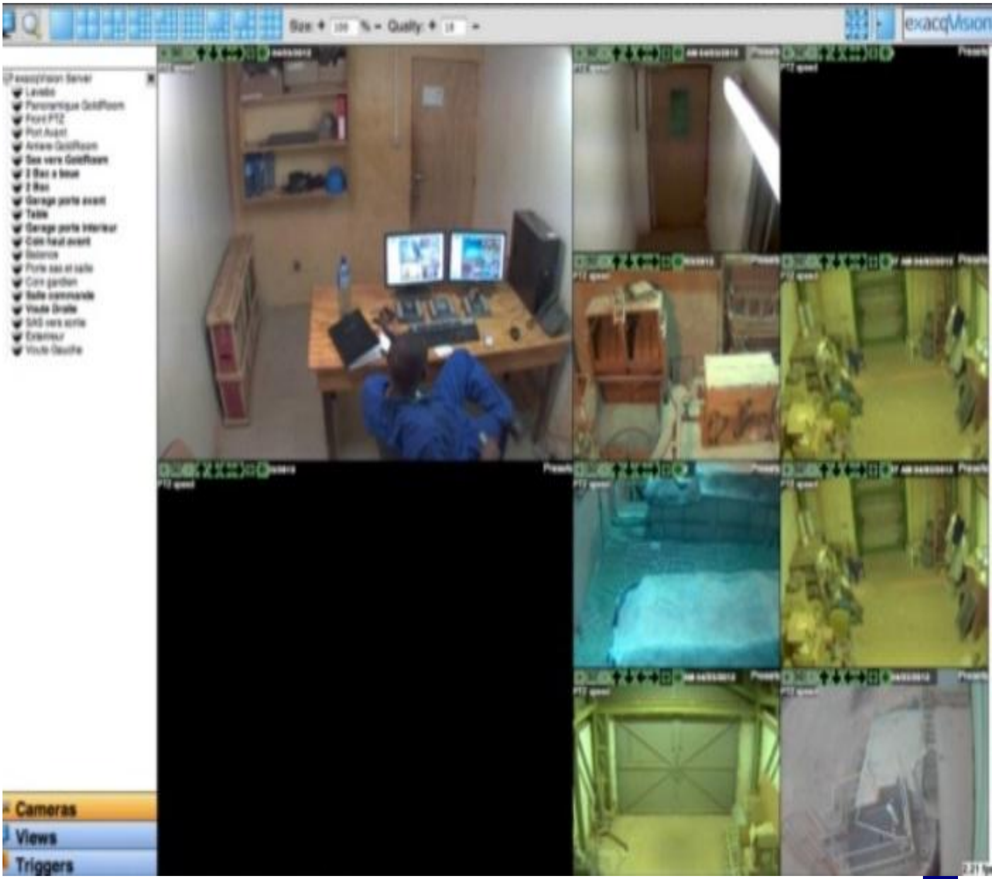
Small-scale systems, why?



Panhandle Elementary EMS Home Page

CONTROL TECHNOLOGIES, INC.

Building Set Points	
Outside Air Temp	105.6 °F
Deadband	3.0 °F
Override Time Setpt	120 min
Heat Enable Set Point	65 °F
Cool Enable Set Point	70 °F
Unocc Heat Setpt	55 °F
Unocc Cool Setpt	120 °F



Privacy? Security?

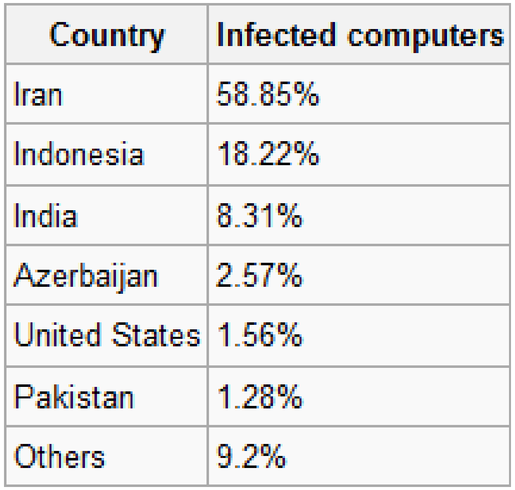
Small-scale systems, why?

- Malwares in Embedded Systems: next (r)evolution!

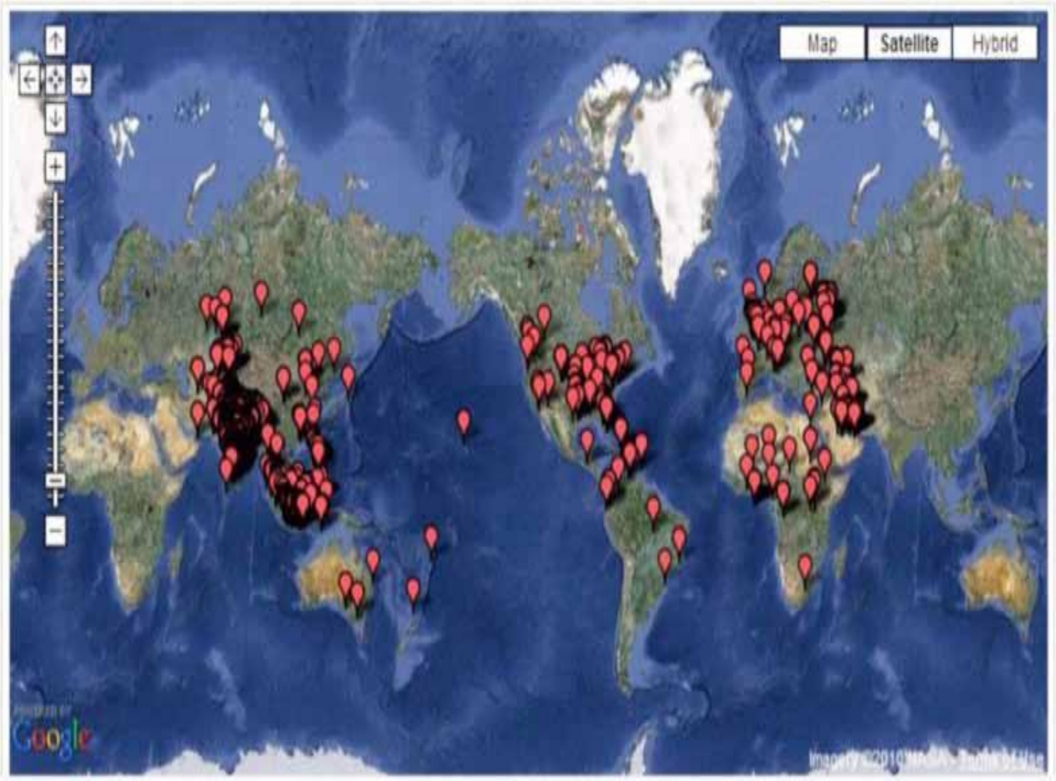
Year	Malware /attack	Target	Threats
2009	**psyb0t**	**Linux-based** routers and DSL modems	DDoS
2010	**Chuck Norris Botnet**	**Linux-based** routers, DLS modems	DDoS +DNS Spoofing
	Stuxnet	industrial control systems (ICS)	alter PLCs for supported facilities
2012	**DNSChanger**	computers and routers	DNS spoofing/poisoning
2013	**JUL: GPS attack**	GPS based systems	**total control of system**
	Sept: Linux/Flasher	wireless routers	login credentials captured and transferred to remote web servers.
	Nov 26 : Linux.Darlloz	**Linux-based** computers, industrial control servers, routers, **cameras, set-top boxes.**	generates IP @ randomly, accesses a specific path on the machine with well-known ID and passwords, and sends HTTP POST requests

Small-scale systems, why?

- Stuxnet Malware (2010)!



Country	Infected computers
Iran	58.85%
Indonesia	18.22%
India	8.31%
Azerbaijan	2.57%
United States	1.56%
Pakistan	1.28%
Others	9.2%

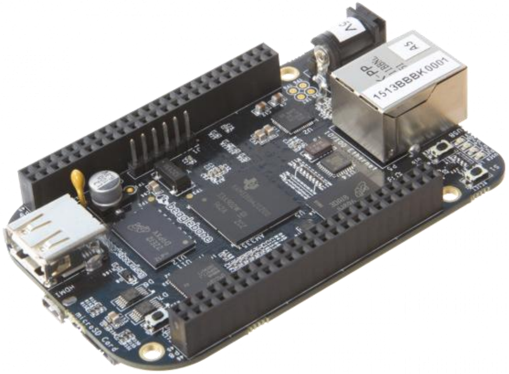


Agenda

- Project Presentation
- Why surveillance of small-scale systems?
- **Small-scale Systems of interest**
- Host-Based surveillance: challenges & alternatives
- Ongoing activities
- Feedback?

Small-scale Systems of Interest

Evaluation Boards



- PandaBoard, BeagleBoards

- Arndale Board, OMAP5432

Small-scale Systems of Interest

Evaluation Boards : Use cases

BeagleBone Black:

- Spectrum Analyzer http://www.youtube.com/watch?v=6YhrKMBrJ2g
- Motor Controller http://www.youtube.com/watch?v=34xJIR-mD4A
- Game console http://www.youtube.com/watch?v=U4P_s-7dDRQ
- Web server http://www.youtube.com/watch?v=CDhyVdpXuqQ

Beagleboard-XM:

- Robot Controller http://www.youtube.com/watch?v=FZKtQLj8NLE
- Motor controller http://www.youtube.com/watch?v=bahmjwWKWIo
- Domotic Control System http://www.youtube.com/watch?v=elAWYCFv0Rw

Pandaboard ES:

- Robot http://www.youtube.com/watch?v=ZWbZBBs9WSs

Small-scale Systems of Interest

OMAP SOC

	BeagleBone	Overo® FE COM (Gumstix)	Gumstix (DuoVero) Zephyr COM
Manuf.	BeagleBoard.org	Gumstix Inc	Gumstix Inc
CPU	AM335x, 720MHz ARM **Cortex-A8**	OMAP 3530, 600 MHz ARM **Cortex-A8**	OMAP4430, Dual-Core : 1 GHz, **Cotex-A9**
GPU	NEON (SIMD) 2D/3D graphics	OpenGL POWERVR SGX for 2D and 3D graphics acceleration	PowerVR SGX540 ™
Memory	256 MiB DDR2 4GB microSD, Cloud9 IDE on Node.JS	512 MB RAM 512 MB NAND microSD slot	RAM : 1GB microSD slot
Feature s	USB client and Host, **Ethernet**, 2x 46 pin headers, Power consumption 2w	Bluetooth and 802.11b/g, Performance up to 1,400 Dhrystone MIPS, Powered via expansion board (Overo series or custom) connected to dual 70-pin connector	**Ethernet** (10/100 Mbps) **Wifi**, Bluetooth, USB OTG Power: SmartReflex technologies
OS	**Android, Linux**	**Linux** distribution pre-installed. **Android**	**Linux, Android**
Size	76.2 ×76.2 ×16mm	58mm x 17mm x 4.2mm	58mm x 17mm x 4.2mm

Small-scale Systems of Interest

Military Smartphone/Platforms

	Nautiz X1	Sabre-Tooth	SCORPION H2
SOC	OMAP (TI)	MediaTek	Qualcomm
CPU	OMAP 4430, **dual core**, (1 GHz)	MT6515, **dual-core** (1 GHz)	Snapdragon S3, **dual core**(1.5GHz)
Memory	RAM : 512 MB, flash: 4 GB, MicroSD card slot	RAM : 512 MB MicroSD card slot (32GB)	RAM : 1MB, Flash : 16 GB, expandable to 32GB micro SD
Connectivity	GSM, CDMA, GPS, Bluetooth, 802.11 b/g/n WiFi	Wi-Fi: 802.11 b/g/n, 2G: GSM, Bluetooth	3g/4G compatible, Wi-Fi 802.11 and Bluetooth, GPS
Connectors	E-compass and G-Sensor, Extended battery, Vehicle cradle, 5-megapixel camera, LED flash	2x GSM, Micro SD Card Slot, Micro USB, Gravity and Linear Acceleration Sensor	tactical data radios, extended battery life
features	survive humidity, vibration, drops /extreme temperatures. waterproof and impervious to dust and sand. runs **Android 4.0**	Water Resistant, Shockproof, Dustproof, Battery Standby: 72 Hours, dimensions: 136x75x18mm , weight: 144g Runs **Android 2.3**	run/charge simultaneously via USB port, batteries, or vehicle power. vibration, shock, drop, humidity **Runs Android 4.0**

Agenda

- Project Presentation
- Why surveillance of small-scale systems?
- Small-scale Systems of interest
- **Host-Based surveillance: challenges & alternatives**
- Ongoing activities
- Feedback?

Challenges & alternatives

- Memory:
  - ***Size of traces*** : filtering, compressing, ...
  - ***Detection engine complexity***: optimizing data structures and algorithms
  - ***Device limitation***: Offloading to remote servers

- Battery:
  - ***Continuous surveillance activities***: periodic analysis
  - ***Large monitored surface***: reducing controlled functionalities
  - ***Overloaded Processor s***: adaptive live surveillance activities

Agenda

- Project Presentation
- Why surveillance of small-scale systems?
- Small-scale Systems of interest
- Host-Based surveillance: challenges & alternatives
- **Ongoing activities**
- Feedback?

Ongoing Activities

- Signature based detection:
  - Experimenting existing tools :
    - Antimalware for Smartphone
    - Antimalware for embedded systems
  - Optimized pattern matching algorithms

- Anomaly-based detection:
  - Features selection
  - Lightweight and optimized algorithms
  - Adaptive algorithms
  - Experimenting and adapting algorithms developed by collaborators: Concordia University

Time for
Feedback