SHARKFEST '12

Wireshark Developer and User Conference

OpenWIPS-ng

A modular and Open source WIPS

Thomas d'Otreppe, Author of Aircrack-ng

Agenda

- What is OpenWIPS-ng?
- Origin
- Architecture
- Internal design
- Release plan
- Demo

~# whoami

- Author of Aircrack-ng and this tool
- Work at NEK Advanced Securities Group

OpenWIPS-ng, WTF is that?

- Let's split that word to explain it
  - Open: Open source
  - 'W': Wireless
  - IPS: Prevent intrusions on networks by reacting (active)
  - IDS: Detect intrusions on networks by notifying (passive)

- Basically, it is a free Wireless Intrusion Prevention System.

Where did the idea come from?

- A project I started almost 2 years ago.
  - Monitor all channels on 2.4Ghz


EDEN

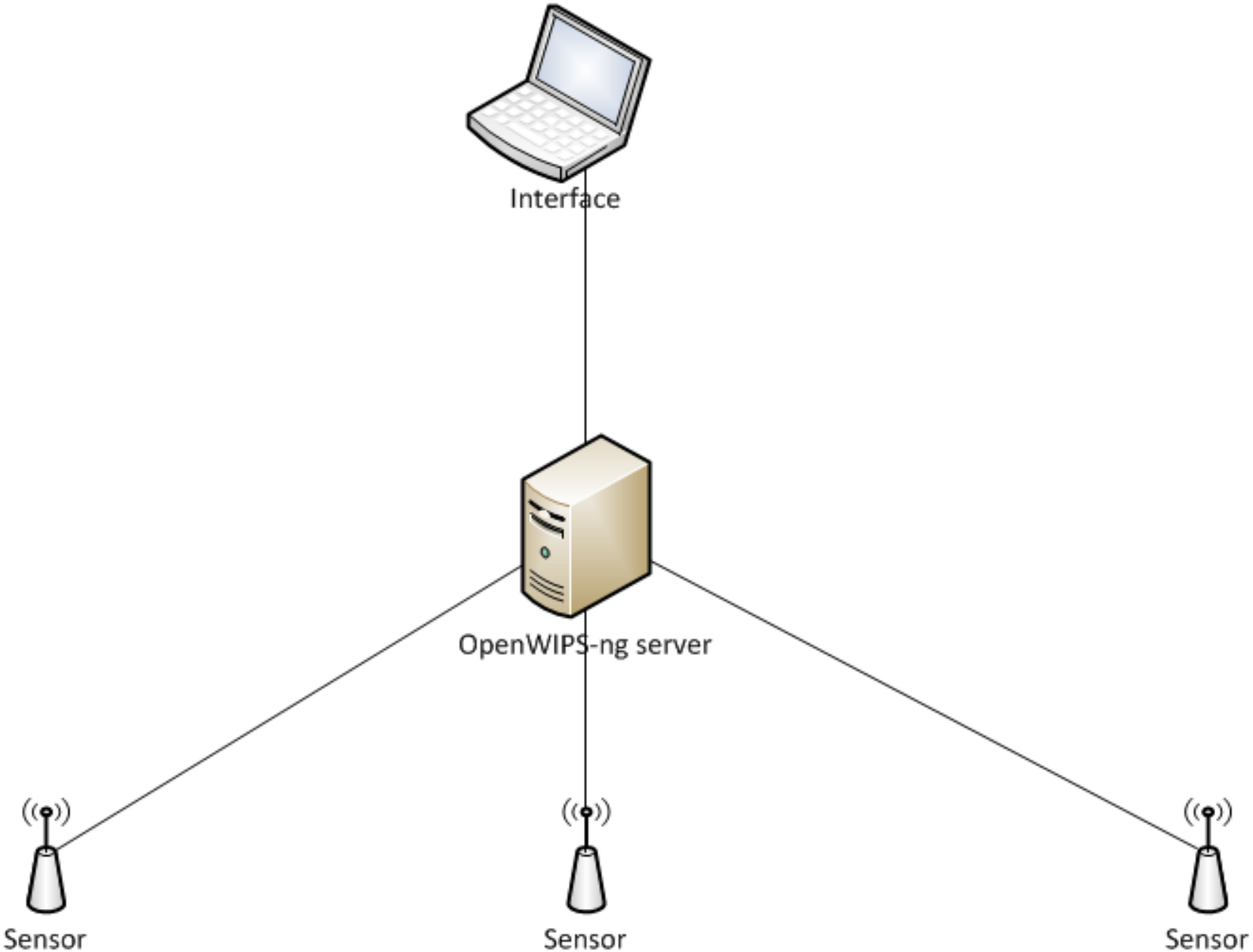
Pushing the idea further

- Wireless IPS are freakin' expensive
- No existing open source solution.
- Don’t want to spend $6-10K for a nice toy, so I applied the open source philosophy: “do it yourself”.

Architecture

- Three parts
  - Sensor(s)
  - Server
  - Interface

Architecture



You said modular?

- Most of its detection functions are plugins
  - Shared libraries (DLL or SO on linux)
  - Some basic checks needs to be always run and run before plugins
- Advantages:
  - No need to recompile the server
  - If you have proprietary code, no need to distribute it
    - DLL/SO can be given compiled.
    - No licensing issue
  - For developers, just a few functions to implement

Modularity

- Most plugins will run on the server
  - CPU/GPU/FPGA power
  - Where the packets are reassembled
- In some rare cases, it will run on the sensor
  - Need to react really quickly

Modularity – Plugin types

- Frame analysis (anomaly/attack detection/response)
- Logging
- Alert
- Database connection
- Script wrapper

Multiple sensors

- Yes, that can be a nightmare
  - Sensors may “overlap” => see same traffic
  - Sensors not always see the same traffic
  - Sensors have small CPU
- Server reassemble data
  - And remove duplicate traffic
  - Then process it
  - Intrusion prevention: Use sensor who see the most of the attack.

Intrusion prevention

- When attacked:
  - In most cases, deauthenticate attackers
  - Log it and alert the administrator
- If legitimate users are attacked: ban both from the network until the issue is solved or some time.
- Can prevent your users from connecting to other networks

And what about DoS

- Can detect Denial of Service
  - All you can do is wait for it to finish
  - Or make it stop
- An hardware add-on is capable to stop it.
  - Must have for any network admin
  - Cheap and widely available
  - Gets the job done quickly

BBRoS*

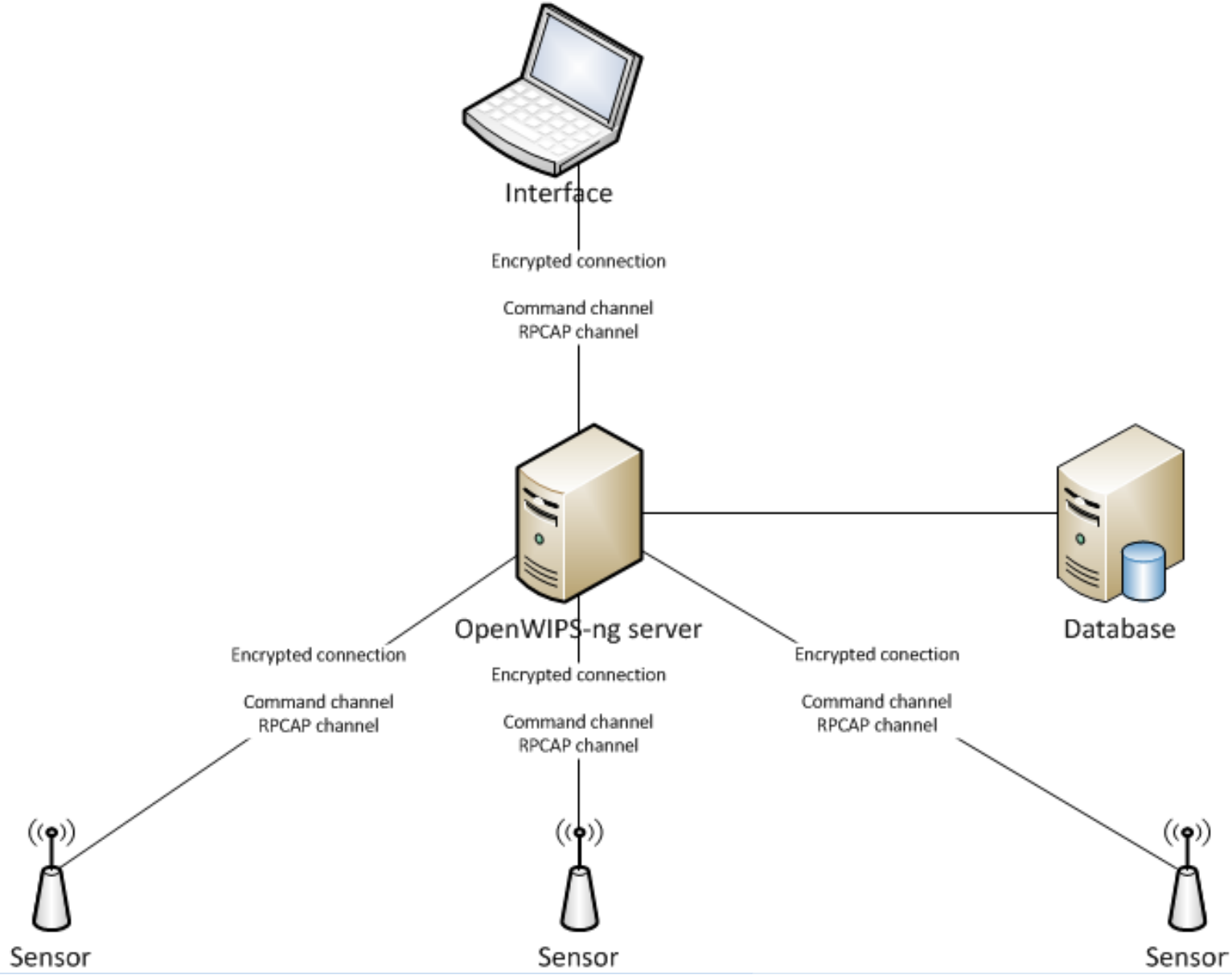
- Locate the attacker accurately
  - Guy who runs away (with a laptop) when you show up with the bat.
- $15-$30 on Amazon/Walmart
- Available in different sizes

*Baseball Bat Restoration of Service

Internal Design

- A bit more technical

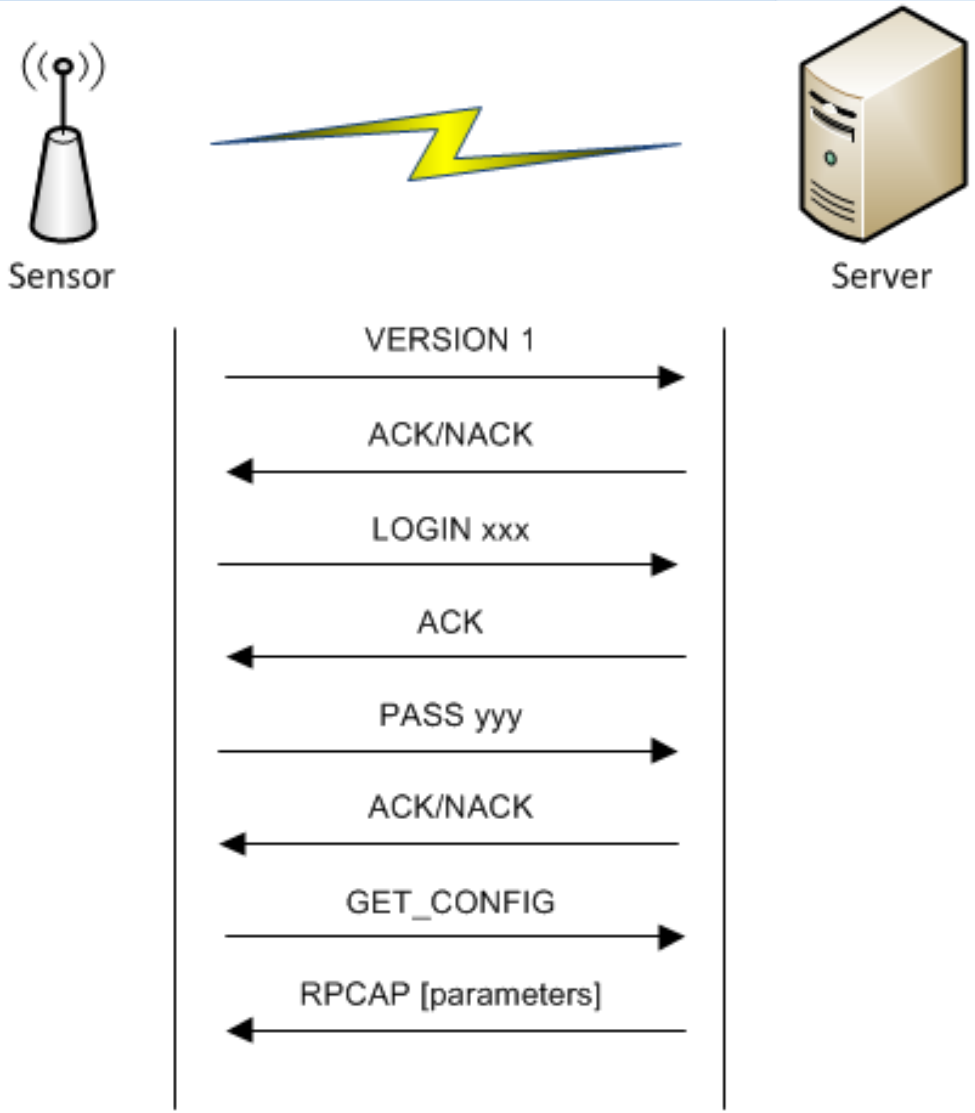
Internal Design - Architecture



Internal design - Communication

- Similar to FTP
  - Command channel
    - Sensor authenticate to server
    - Establish the remote PCAP link.
  - Data channel: Remote PCAP
    - Binary data
    - Same structure as a packet in a PCAP file (header, packet)
- Both channels encrypted by default

Internal design – Communication (2)



Internal design - Plugins

- Type of plugins
  - Frame analysis (attack detection/response)
  - Logging
  - Alert
  - Database connection
- Script Wrapper
  - Wrapper to use a scripting language
  - For any type of plugin

Internal design – Plugins (2)

- Very easy
- How?
  1. Implementation
     - Use any programming language that can create a shared object
     - Implement common functions to all plugins
     - Implement functions specific to the type of plugin
     - The server takes care of the packet list so no need to manage it
  2. Compile it
  3. Edit configuration file
  4. (Re)start OpenWIPS-ng server

Internal design – Plugins (3)

- Script Wrapper
  - For any type of plugin (Frame analysis, Logging, etc)
  - Wrapper to use a scripting language
    - Same function names to implement
  - Is a plugin itself but needs parameters
    - At least the path to the script and the language
    - Any parameter the script needs/accept

Internal design – Plugins (4)

- Let's see how a script is made
  - Functions to implement
  - Example implementation
  - Makefile
  - Installation

Internal design – Packet reassembly

- Data can come from several devices
- Those devices view different parts of the communication
  - Sometimes the same
  - Sometimes completely different parts

- How packet reassembly works:
  1. Gather packet from all the sources
  2. Discard duplicate
  3. Sometimes needs reordering

Releases

- 0.1 beta available (close to 0.1 stable)
- 0.1.1, 0.2 and 0.3: More modules, features

- 1.0:
  - Rewrite in C++
  - Graphical User Interface

v0.1

- Sensor
- Server
  - Single sensor support
  - Built-in logging (none/file/syslog)
  - Plugins available: Frame analysis
- Partially work on OSX Lion
- Documentation
  - Installation, configuration and usage
  - Plugin development

v0.1 – Plugins

- Anomaly check
  - FromDS/ToDS fields
  - Management frames IE
  - Frame type/subtype
- Attack detection
  - Fragmentation
  - Deauthentication
  - **Replay detection**

v0.1.1

- Server
  - Rewrite attack detection system
  - Parse prism and PPI headers (might happen sooner)
- Full Windows support (server/sensor)
  - Airpcap only

v0.2 – v0.3

- v0.2:
  - Sensor: channel hopping
  - Server
    - Multiple sensor support
    - Encrypted communications
- v0.3
  - Web interface

- More plugins
- Bug fixes (obviously)

v1.0

- Rewrite in C++
  - No change in how plugins work
- Real remote PCAP
- GUI

Following versions

- Detailed planning available on the website

~~Video~~ Demo

- Murphy's law: "A live demo always work as expected, nothing wrong ever happens."
  - Or maybe is it the other way around? ☺
- Especially with wireless traffic which is ~~un~~predictable
  - And nobody is ever going with mess with it.

- Let's see it in action.

I want it

- Subversion: http://svn.openwips-ng.org

- http://OpenWIPS-ng.org
- #openwips-ng on Freenode.net
- tdotreppe@openwips-ng.org

- Ideas? Features request? Email me


That's all Folks!

- http://OpenWIPS-ng.org
- #openwips-ng on Freenode.net

- tdotreppe@openwips-ng.org
  - We need your ideas/remark/suggestions.
  - If you want to help/join.