Wireless Intrusion Detection Systems (WIDS)

Dragan Pleskonjic

CONWEX
Dragan_Pleskonjic@conwex.net
dragan@empowerproduction.com

Motivation & idea

- Wireless networks are forecasted to expand rapidly (Wi-Fi IEEE 802.11a/b/g…)
- WLANs offer area coverage and access unlimited by wires, but this implicates openness to various attacks
- It is possible that we will have wireless Access Points everywhere, even in computer chipsets
- Inherent lack of security and experience
- WEP was broken pretty quickly

Wireless vs. wired intrusions

- Wired – physically attached: intruder / attacker needs to plug directly into the network
- Wireless – intruder can stay anywhere and intrude unseen
- No exact “border” between internal and external network => losing exact classification to insider and outsider attacks

Wireless vs. wired intrusions (continued)

- Sometimes people assume that:
  - Host based systems – prevent insider attacks
  - Network based systems – outsider tasks
- We may not agree with this in practice, but as soon as you add a Wi-Fi signal, the border of defense becomes unclear and not sharply defined.

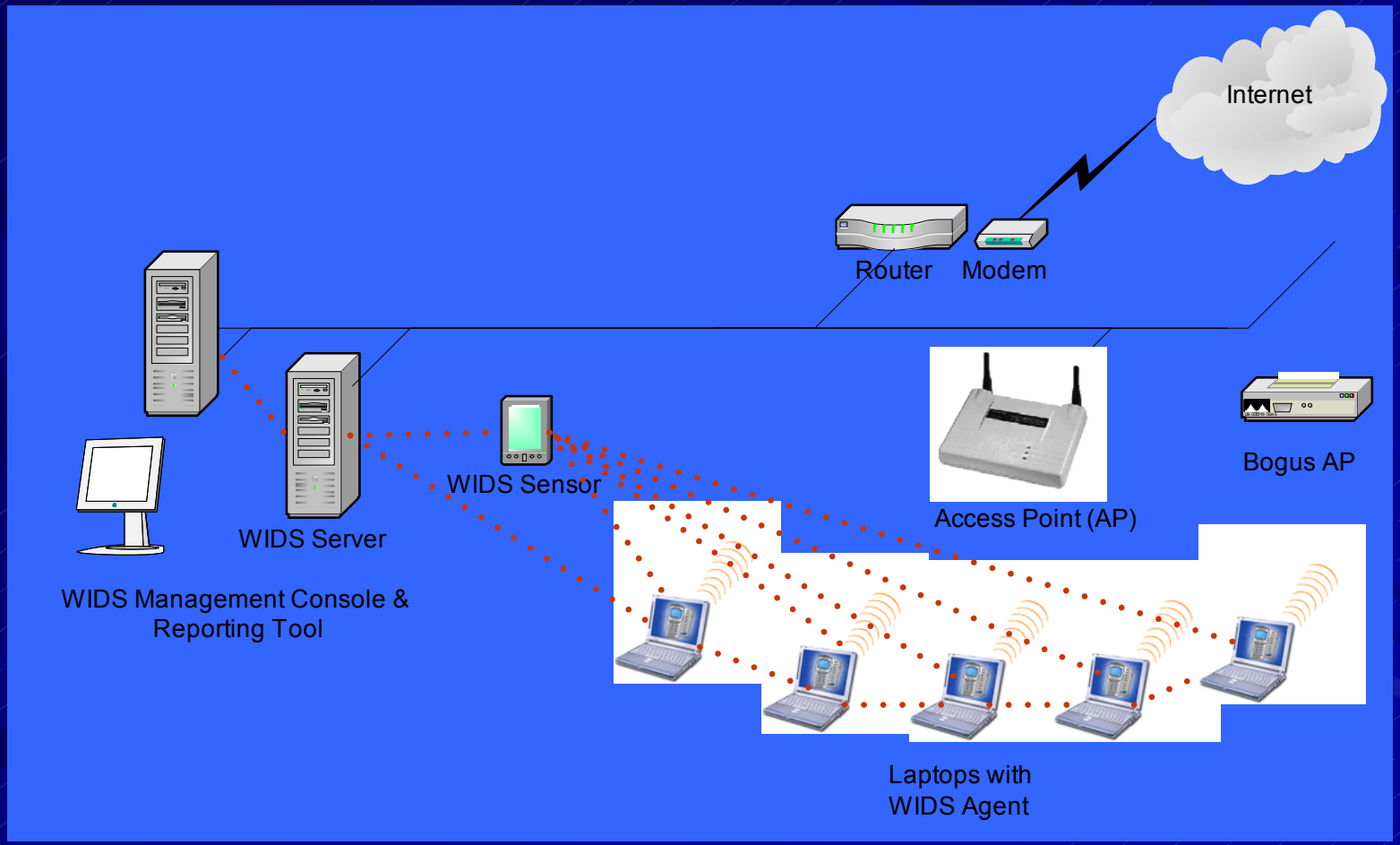
Some wireless specific attacks

- Unauthorized APs - Bogus APs that designed to steal the association and login Credentials
- War Driving - Probe requests which don't have the ESSID field set in the probe
- Flooding - Attempts to flood the AP with associations.
- MAC address spoofing
- To detect:
  - Rogue APs
  - Monkey/Hacker JACKS
  - Null probes
  - Null Associations
  - Bad MAC controlled by a MAC black list
  - bad SSIDs controlled by a ESSID black list
  - floods etc.

Components and Products

- WIDS consists of:
  - Agent
  - Sensor
  - Server
  - Console & Management, Reporting Tools
- These components should contribute to achieve intrusion detection and protection goal

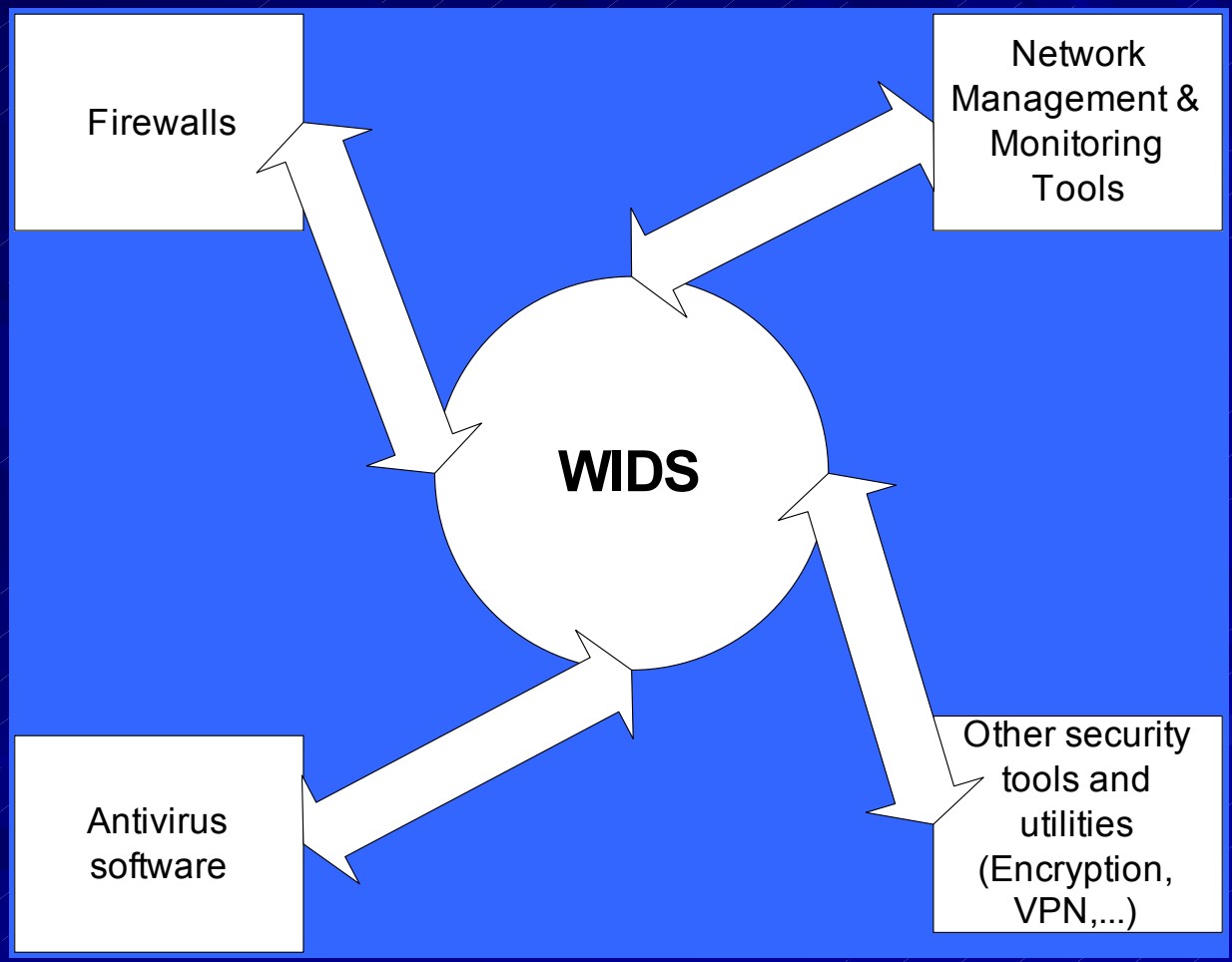
System Components Relationship



Related to:

- Firewall software and devices
- Antivirus software
- Network Management Tools
- Other security tools

Schema


Firewalls
Network Management & Monitoring Tools
WIDS
Antivirus software
Other security tools and utilities (Encryption, VPN,...)

Goal

- To make an efficient system to defend the wireless network
- Define attack and intrusion “axioms scope”
- Define conclusions mechanisms (“theorems”)
- Self learning system and anticipation – even if we fail to make a fully intelligent system we can accept some weaker decision points to get the system functional
- Implement attack recognition
- Launch response to defend system or network

Structure

- Neural networks and fuzzy logic
- Self learning system (AI - artificial intelligence, neural networks, fuzzy logic…)
- Automatic answer to intrusions
- Defend against new intrusion types (previously unknown or similar but different)
- Local and global answer on attack (intrusion)
- Wireless specific attacks detection

Approach

- Recognize more attacks
- Autonomy and cooperation of components
- Multidimensional system
- Level of autonomous decision and self defense
- Resistance and denial of new kinds of intrusions
- Providing two kinds of response: Local and global
- Elements of intelligent behavior etc.

Status

- Currently under development
- Completed steps:
  - Elements for multidimensional concept and axioms scope
  - Partially developed components and elements of system
  - Product family definition and implementation

Conclusions and future

- Further work to be done:
  - To define remaining part of system
  - To make proof of concept implementation
  - To test single components and system overall
  - To gain understanding of the need and solution.
  - Example: WIDS Agent as part of Operating System (as personal firewall or antivirus tool)

Questions?

e-mail: dragan@conwex.net

Abstract

- *Today's wireless networks are vulnerable in many ways (eavesdropping, illegal use, unauthorized access, denial of service attacks, so called warchalking etc). These problems and concerns are one of main obstacles for wider usage of wireless networks. People are worried to unknowingly "expose" their computers to illegally access through air from undefined location. On wired networks intruder can access by wire, but in wireless he has possibility to access to your computer from anywhere in neighborhood.*
- *In this paper solution to overcome this obstacle is presented. Here is proposed WIDS (Wireless Intrusion Detection System) based on client based IDS agents, their cooperation and capabilities such as: self learning, autonomy and decision, self-decision and self defense including alerting. This is multidimensional system in development which is intended to cover most of wireless networks specific vulnerabilities on intrusion. It should work in real-time and defend user i.e. his computer or system against majority of intrusions nevertheless of fact if they are already known or new kind of attacks. System is integrated in clients and performs local data collection and filtering, works as local detection engine cooperating with neighboring IDS agents (cooperative detection engine). It provides local response and/or global response against intrusion.*
- *This system can be coupled together with authentication systems and air encryption systems proposed by 802.11i (including AES encryption) and 802.1x (EAP and its implementations) for better security.*
- *At present time there are IDS but mostly wired networks based and rules/signs based. These systems can't answer on demanding environments and every day practice where we can see new and new types of attacks uncovered by current "signs" present in IDS, so its efficiency is dependent on frequency of signs / rules discovering and updates.*
- *WIDS system, as described here, will require existence of next components WIDS Agent, Sensor, Server and Management & Reporting Tool and these components are object of analyze.*

Additional description

- People are worried about unknowingly exposing their computers to illegal access through the air, from an undefined location. On wired networks the intruder can access by wire, but in wireless environments the intruder can access the network from anywhere in the neighborhood.
- In this paper, solutions to overcome this obstacle are presented. …. This is a multidimensional system, currently in development, ….It should work in real-time and defend the user's computer or system against the majority of intrusions, whether they are already known or represent a new kind of attack. The System is integrated with the client performing local data collection and filtering and working as a local detection engine cooperating with other servers and agents on the network. The client provides local and/or global response to intrusions.
- …At the present time there are IDS's but mostly deployed on wired networks, and based on known rules. These systems can't answer the demand in environments where new intrusions are occurring every day. They are limited by current known signatures of intrusions.
- WIDS system, as described here, will require Agents, Sensors, Servers, and Management and Reporting tools, and these components are the object of the analysis.