Is the Scanning of Computer Networks Dangerous?
The talk is about...

- The need of network scanning, its main principles and related problems
- A freely available network scanning tool, which can be used in practice, and its design – Angry IP Scanner
Scanning of computer networks

- Examining a single network address
- Searching for addresses with specific properties
- IP Scanning involves
  - Pinging
  - Port scanning
  - Gathering of other information
Typical gathered information

- Alive/dead status
- Average packet roundtrip time
- TTL – distance (in number of routers)
- Host and domain names
- Open and filtered TCP and UDP ports
- Running services and their versions
- OS type and version
- Much more info can be obtained indirectly
Scanning purposes

- **Offensive**
  (Attacks)

- **Defensive**
  (Preventive defense)

- **Maintenance**
  (Monitoring and inventory)
Legal issues

- Most countries' laws forbid
  - getting illegal access to data,
  - destroying, spoiling, modifying it,
  - or reducing its usefulness or value in any other way

- Scanning results provide
  - mostly publicly available and freely available information
  - therefore it is legal
  - with the probable exception of some 'more advanced' scanning techniques
Safety

- How safe is it to perform scanning nowadays?
  - legal, but may cause problems

- Are such tools dangerous for the humanity?
  - best tools for maintaining security are the same ones that can be used in preparation for attacks
State of Internet security

- Foundation protocols are old
  - there have been more trust before
- Present-day Internet is insecure
  - too much anonymity
  - weak authentication (passwords)
  - vulnerable routing and DNS
  - low-quality software
  - human factor (social engineering, mistakes, lack of knowledge and skills)
Angry IP Scanner

- Open source
- GPL
- Cross-platform
- User-friendly
- Extensible
- (Nice name)
Technological choices

Java
- modern and popular, now open-source
- productive
- portable, cross-platform
- JNI (Java Native Interface)

SWT
- open source
- good performance
- native look and feel on all platforms
Modularity and Extensibility

- Modular design
- Possibility of plugins
  - Feeders
    generate addresses for scanning
  - Pingers
    check the alive status
  - Fetchers
    retrieve info about each address
  - Exporters
    store the scanning results
  - Openers
    open addresses in other software
Increasing performance

- Parallelizing
- Adapted timeouts
- Thread pooling
- Speed-accuracy compromise
- SYN-ACK-RST scanning
Simplified state diagram

Begin

Idle

start scanning

all threads finished

Terminating

Scanning

Start a Thread

threads available

maxThreads reached

next

Wait

no more IPs

terminate

Waiting for active Threads

abort scanning
Platform support

- **Linux**
  - primary development platform
  - best choice for scanning

- **Mac OS X**
  - based on FreeBSD kernel
  - lots of conceptual differences

- **Windows**
  - support due to popularity
  - inferior to anything else out there
Deployment

- One-file executable (jar)
- Separate for each platform
  - Linux: rpm & deb
  - Mac: application bundle
  - Windows: exe
- Automatically extracts native libraries (.dll and .so)
- Size < 1 Mb
Comparison with other tools

- **Nmap**
  - Probably the most popular scanner
  - Has some 'more advanced' tricks
  - Windows support is fairly new
  - Harder to use
  - Requires proper installation

- **Angry IP Scanner**
  - No installation necessary
  - Runnable from USB drives
  - GUI by design – ease of use
  - Superior extensibility via plugins

- **No other comparable general-purpose, open-source and cross-platform scanners**
Problems (1)

- Many low-quality clones
  - Angry IP Scanner was the first general-purpose GUI scanner

- Anti-virus software
  - nowadays AV vendors tend to enlarge their databases at any price
  - they take users' freedom away (even more than Microsoft does)
Problems (2)

- Windows >= XP SP2
  - Used by ~70% of users (unfortunately)
  - Removed raw socket support
    - hard to do more exotic things
  - TCP connection rate limiting
    - max 10 simultaneous connection attempts
      (max 2 in some Vista editions)
    - very slow scanning performance
## Results (1)

### Working software

![IP Range - Angry IP Scanner](image)

*Working software is the primary measure of success.*

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Ping</th>
<th>Hostname</th>
<th>Web Detect</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>194.204.33.16</td>
<td>14 ms</td>
<td>[n/a]</td>
<td>[n/a]</td>
<td>[n/a]</td>
</tr>
<tr>
<td>194.204.33.17</td>
<td>17 ms</td>
<td>vanaisa.hansanet.ee</td>
<td>Apache/1.3.37 (Unix) [n/a]</td>
<td></td>
</tr>
<tr>
<td>194.204.33.18</td>
<td>[n/a]</td>
<td>[n/s]</td>
<td>[n/s]</td>
<td></td>
</tr>
<tr>
<td>194.204.33.22</td>
<td>[n/a]</td>
<td>[n/s]</td>
<td>[n/s]</td>
<td></td>
</tr>
<tr>
<td>194.204.33.23</td>
<td>34 ms</td>
<td>server1.bma.ee</td>
<td>Apache</td>
<td>21,22</td>
</tr>
<tr>
<td>194.204.33.24</td>
<td>38 ms</td>
<td>server2.bma.ee</td>
<td>Apache</td>
<td>21,22</td>
</tr>
<tr>
<td>194.204.33.25</td>
<td>[n/a]</td>
<td>[n/s]</td>
<td>[n/s]</td>
<td></td>
</tr>
<tr>
<td>194.204.33.26</td>
<td>37 ms</td>
<td>gepard.balticcrew.ee</td>
<td>Apache</td>
<td>21,22</td>
</tr>
<tr>
<td>194.204.33.27</td>
<td>50 ms</td>
<td>gepard2.balticcrew.ee</td>
<td>Apache</td>
<td>21,22</td>
</tr>
<tr>
<td>194.204.33.28</td>
<td>57 ms</td>
<td>ns2.alfanet.ee</td>
<td>Apache/1.3.37 (Unix) 21,22</td>
<td></td>
</tr>
<tr>
<td>194.204.33.29</td>
<td>89 ms</td>
<td>[n/a]</td>
<td>Apache/1.3.33 (Debi. 9,13,21)</td>
<td></td>
</tr>
<tr>
<td>194.204.33.30</td>
<td>[n/a]</td>
<td>[n/s]</td>
<td>[n/s]</td>
<td></td>
</tr>
</tbody>
</table>

---

Baltic DB&IS 2008
Anton Keks
Results (2)

- Official homepage: [http://www.azib.net/ipscan/](http://www.azib.net/ipscan/)
  - 10000 page views /day
  - 3000 downloads /day
  - The first ‘ip scanner’ in Google!
  - Subversion: version control
  - Bug and feature tracking
  - Forums
Results (3)

Download history of Angry IP Scanner *

Last 12 months

Increasing trend
(June stats are incomplete)

Last 2 months

Less downloads during weekends - people use it at work

* These stats reflect only downloads from sourceforge servers, but the application is widely mirrored on many 3rd-party software download sites

Baltic DB&IS 2008
Anton Keks
Now & Future

- Continue the development
  - more functionality
    (OS fingerprinting, version detection, stealth scanning, etc)
- bugfixing
- Involve more people
  - better documentation
  - wiki-based homepage
  - more example plugins
Scanning of computer networks

Live demo & Questions!