vulnerabilities prevail
• Impact Assessment Disputes
• Demo Exploits
• Patch Quality & Deployment Challenges
  • Lack of Code Quality Improvement
• Partial (Code) Coverage
• Partial Coverage
• Coincidental Discoveries
• Lack of “Standards”
• Reverse Engineering
• Economics
• National Security
• Geopolitics
• Complex Communication Networks
• Colorful Terminology
• Various Actors and Interests

TECHNOLOGY

POLITICS

PROCESS

problems?
bugs
<table>
<thead>
<tr>
<th>OUSPG META LEVEL 4</th>
<th>?</th>
</tr>
</thead>
<tbody>
<tr>
<td>OUSPG META LEVEL 3</td>
<td>Single scheme in multiple protocols / protocol families</td>
</tr>
<tr>
<td>OUSPG META LEVEL 2</td>
<td>Single protocol embedded in multiple protocol families</td>
</tr>
<tr>
<td>OUSPG META LEVEL 1</td>
<td>Single protocol, multiple implementations by multiple vendors</td>
</tr>
<tr>
<td>TRADITIONAL APPROACH</td>
<td>Single vendor, single implementation, single vulnerability</td>
</tr>
</tbody>
</table>
understanding ASN.1
Protocol specifications

- IETF
- ITU-T
- ATM Forum
- Other standardisation organisations

Problems:
- Information gathering is laborious
- Seeing hidden dependencies
Prototype information gathering methods

Prototype ad hoc - visuals

visualisation
protos testing methodology

- protocol structure description
- generating test material to break implementations
- C-07
- C-08
- C-09
- release
protos testing methodology bottlenecks

RFC
specs

XYZ complete
book

experts

--------------

{ manual work ...

model
fuzzing

testing material
protos-genome testing methodology
Problem: analyse with traditional analysers
problem: read the specifications?
TOOL SETUP

TOOL VIEW

EXPERTISE LEVEL

network operator

frontline support

administrators / developers

the cure: visualisation
Pick your strategy

Public
Vendor
Reporter
Government
Shareholder

BE

Fooled
Cooperated with
Informed
Damned

strategy?
THE END

http://www.ee.oulu.fi/research/ouspg/