vulnerabilities prevail.
• Impact Assessment Disputes
• Demo Exploits
• Patch Quality & Deployment Challenges
• Lack of Code Quality Improvement
• Partial (Code) Coverage

• Liability
• DMCA

• Partial Coverage
• Coincidental Discoveries
• Lack of “Standards”

• Reverse Engineering
• Economics
• National Security
• Geopolitics
• Complex Communication Networks

• Colorful Terminology
• Various Actors and Interests

• Impact Assessment
• Demo Exploits
• Patch Quality & Deployment Challenges
• Lack of Code Quality Improvement
• Partial (Code) Coverage

• Liability
• DMCA

• Partial Coverage
• Coincidental Discoveries
• Lack of “Standards”

• Reverse Engineering
• Economics
• National Security
• Geopolitics
• Complex Communication Networks

• Colorful Terminology
• Various Actors and Interests
NEGATIVE REQUIREMENTS

POSITIVE REQUIREMENTS

IMPLEMENTATION

IN SPECIFICATION

UNDESIRED FUNCTIONALITY

DESIRED FUNCTIONALITY

ACQUIRED FUNCTIONALITY

PLANNED FEATURES

“CREATIVE FEATURES”

CONFORMANCE BUGS

b u g s
Government services and protocols:

- NTP
- RADIUS
- Kerberos
- LDAP
- NFS
- CIFS
- DCE-RPC
- CORBA/IIOP
- HTTP
- SIP
- H.323
- X.509
- H.225
- ISDN
- ATM
- JDBC
- X.25
- X.400
- IPv6
- IPv4
- ISAKMP
- L2TP
- PPTP
- PPP
- SMTP
- NNTP
- IRC
- OpenPGP
- MIME
- DIAMETER
- SSH
- GIF
- JPEG
- PNG
- WAP
- WML
- XML
- SOAP
- HTML
- RTF
- Jabber
- VCard
- DHCP
- DNS
- SunRPC
- SNMP
- X.509
- Finger
- Telnet
- XMODEM
- H.245
- Bluetooth

Chaos of protocols.
OUSPG bites the dust
## PROTOS

<table>
<thead>
<tr>
<th>TEST SUITE</th>
<th>TEST CASES</th>
<th>VENDORS</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP</td>
<td>29516/24100</td>
<td>140</td>
</tr>
<tr>
<td>SIP</td>
<td>4527</td>
<td>92</td>
</tr>
<tr>
<td>H.323</td>
<td>4497</td>
<td>34</td>
</tr>
</tbody>
</table>
can of worms
<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>
Meta level 1

Meta level 2

Meta level 3

A
A1
A2

B
B1
B2

C
C1
C2

I

II

impact
PUBLIC ATTENTION
- media, mailing lists

EXPERTS
- interviews
- communication strategy
- models of structuring information

PROTOCOL DEFINITIONS
- ITU-T
- ISO
- IETF

THE PREVALENCE OF PROTOCOL IMPLEMENTATIONS
- market situation
- historical data
- usage environments

points out, with respect to protocols
- dependencies
- relations
- structures
- problems relating to information security

and facilitates:
- strategic planning
- decision making
- communication
- coordination of information security research

VERSATILE MODEL
HTTP Server
- HTTP load balancing failover

HTTP “like” entity

HTTP Server

STORAGE

MDA
- mail delivery agent

MTA
- mail transfer agent
- media scaling
- virus scanners
- spam/pr0n/content filters

MUA
- mail user agents
- virus scanners
- spam/pr0n/content filters

NEWS readers
- desktop
- PDA/mobility
- digitv?

BROWSERS
- desktop
- PDA/mobile
- digitv?

STORAGE

(MIME)

tech/usage view (MIME)
protocol
description
structure
generating test material to break implementations

F

C-07
C-08
C-09

release

protos testing methodology
protos testing methodology bottlenecks

RFC specs

XYZ complete book

experts

manual work ...

M model F fuzzing testing material
protos-genome testing methodology

G → M → F → testing material

automatic structure inference → model → automatic fuzzing

feedback
OUSPG bites the dust
Problem: analyse with traditional analysators
the cure: instrumentation
problem: read the specifications?
the cure: visualisation
partners in crime

Cisco
Microsoft
TeliaSonera
Sun
Nokia
+over 100

PARTNERS

VENDORS

COORDINATORS

PRESENTATIONS

PUBLICATIONS

media

AUSCERT
CERT/CC
CERT-FI
NISCC

ISG, EE, OU, VTT, ...
MEDIATOR-CONTROL
[Coordinators]
- Free software vendor
- Sub-contractor
- Service Provider / Integrator
- Education
- Insurance body
- Media

DEVELOPER/PROVIDER
[Recipients]
- Retailer
- Shareholders

EVALUATOR
[Reporters]
- CERT
- VENDOR
- Non-affiliated evaluator
- Security Vendor

USER

security evaluation stakeholders
- image
- identity
- reputation

- Government EXECUTIVE body
- Government JURISDICTIONAL body
- Government POLITICAL/LEGISLATIVE body
- NGO (advocate / professional industry)
- Tiger-team
Pick your strategy

{ Public
Vendor
Reporter
Government
Shareholder }

BE

{ Fooled
Cooperated with
Informed
Damned }

strategy?
THE END

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