A Cloudy Crystal Ball
--
Visions of the Future

David D. Clark

M.I.T. Laboratory for Computer Science

IETF, July 1992

Alternate title: Apocalypse Now

Guessing the future

Identify the major external forces.

Consider each separately: the future if each dominates.

Speculate on what happens when we mix the stories together.

Forces that shape us

New services:

- **Real time (video)**
- **Information access**

Commercial network offerings:

- **SMDS -> B-ISDN -> ubiquitous ATM access**
- **A new “kid” on the block?**

Cyber-terrorists:

- **“Security” gateways (Mail relays…)**

Us:

- **We have met the enemy and he is ...**

Video and Real-Time

Our best success was not computing, but hooking people together.

Video and related services might be even more powerful.

- **Do not use the phone analogy to speculate.**

Small technical problems:

- **Figure out how to do it. (MIT research here)**
- **Change all the routers.**
- **Charge for service.**
- **Make it affordable.**

Work-stations are “almost there”.

Computer mediated video interaction, a.k.a. games.

The network as an Information Mesh

An old goal, not yet achieved.

Recently, some neat stuff.

- **WAIS, W3, Archie, Gopher, Prospero, etc.**
- **IETF, IRTF activities.**

Does it require changes in the infrastructure?

- **Scale, not speed, is the issue.**
- **Infrastructure must know about information objects. (MIT research here)**
  - **Names**
  - **Types**

New services: charging for services, security (MIT research)

Video as an information interface.

Commercial network services

What are the issues?

Policy:

- **How do we charge?**
- **Is there a role for monopoly?**
- **Business vs. ubiquitous access?**

Technical:

- **Control of routing.**
- **Support for accounting.**
- **Security.**
- **…**

ATM -- A really big elephant

Myths from New Jersey:

- **"They" will supply the scalable address space.**
- **"They" will solve the routing problem.**
- **ATM will solve the problem of real-time and QOS.**
- **"They" will be here real soon.**

What are the real issues here?

- **The network designers with telephony background do not understand multi-application networks.**
- **The phone companies have no history or approach to rapid deployment.**
- **They do not know how to do QOS either.**

An example: why ATM LANs.

- **My personal research: Everyone -> Sun -> standard.**
- **WHEN will the standard come? Mismatch possible.**

The 90's -- the decade of the cyber-terrorist

What I hated about the Morris worm:

- **I found out about it on the Today show.**

A worked example of a painless act of terrorism.

- **The hacks of today are the commonplace of tomorrow. (True for the good stuff, why not bad stuff?)**

A digression: my Internet security talk.

SECURITY

Security is a CRITICAL problem.

Lack of security means the END OF LIFE AS WE KNOW IT!!

A time for ACTION!!!

(Can I be more explicit?)

WHAT'S THE PROBLEM?

Large networks and poor security don't mix.

Users will less and less tolerate the risk of being attacked from anywhere in the universe.

Look at the Internet worm.

- **Check out the level of publicity.**
- **Consider the potential for damage.**
- **Consider who else has noticed the above.**

Will this be the decade of the cyber-terrorist?

WHAT WILL HAPPEN?

Without better levels of protection, people will not be willing to attach to the Internet.

The "GREAT UNPLUGGING"?

- **Too dramatic…**

The decade of firewalls?

- **Already happening.**

MAIL RELAYS (Yuck!).

WHY ARE APPLICATION RELAYS SO BAD?

Application level relays have two problems:

- **They signal the end of flexible service introduction.**
- **They don't work very well (consider mail today).**

The end of the open road….

The fencing of the West….

The Italian telephone system….

WHY DO APPLICATION LEVEL RELAYS HELP?

Why do they help?

- **Most security bugs are not in the specification, but in an implementation of the specification.**
- **To penetrate a system protected behind an application level relay, it is necessary to break two implementations.**
- **Lower level attacks (tunneling attacks) cannot get past the relay.**
- **Insecure services can be blocked.**

WHAT CAN WE DO?

Option 1: Make system security better.

- **Not “our” problem.**
- **We must band together and make demands.**
- **Fix insecure services.**

Option 2: Accept the inevitable; make it work.

Why doesn’t it work well?

RELAYS ARE NOT CONSISTENT WITH THE BASIC ASPECTS OF THE PROTOCOL ARCHITECTURE!!

THE ARCHITECTURE AND THE RELAY

The protocol architecture assumes universal connectivity at the network layer.

Relays break that assumption. Things stop working.

Some examples:

- **Names, addresses, routes.**
- **Fault isolation.**

Recreation in *ad hoc* manner of the whole network functionality at application level.

- **Consider X.500 and X.400**

WHAT "WE" SHOULD DO

Lobby for better system security.

Fix insecure services.

- **PASSWORDS!!!**

Push for "open domains".

- **Better security = larger domains.**

Develop a new protocol reference model for application level relay networks. Make it work. Accept it.

Don't just sit there and think it does not matter.

- **Security is the problem we love to ignore.**

Some lessons

Bad things do not happen all at once.

- **AIDS, crime, routing collapse**

Things get worse slowly. People adjust.

The problem is assigning the correct degree of fear to distant elephants.

- **When should we (have) declared panic about:**
  - **Addressing, security**

Always ask: What will happen if I do nothing?

- **Use these rules.**

No security -> mail gateways.

- **No addressing -> ?? MAIL GATEWAYS and X.400.**

Walking among the wild elephants

Plan of today:

- **Fix addressing and routing.**
- **Leave security at end point. Pray.**
- **See if new services stamp out mail gateways.**

An alternative plan (just for fun!!!)

- **Build application-independent border crossing boxes.**
- **Ignore the addressing problem.**
- **Build a new network based on application, not IP connectivity. Routing and addressing at this level.**

The last force on us -- us

The standards elephant of yesterday -- OSI.

The standards elephant of today -- it's right here.

As the Internet and its community grows, how do we manage the process of change and growth?

- **Open process -- let all voices be heard.**
- **Closed process -- make progress.**
- **Quick process -- keep up with reality.**
- **Slow process -- leave time to think.**
- **Market driven process -- the future is commercial.**
- **Scaling driven process -- the future is the Internet.**

We reject: kings, presidents and voting.

We believe in: rough consensus and running code.

A look at us

What are we good at?

- **Responding to short term reality.**
- **Building stuff that works.**
- **Calling bad stuff bad.**

What are we bad at?

- **Growing our processes to match our size.**
- **Setting long-term direction.**

An example -- making standards.

What is the correct model?

- **I am trying to ask this in a constructive way, please.**

Today: IESG proposes, with IAB advice and consent.

- **Sort of like the House of Lords.**

IESG alone is enough?

- **I think some "checks and balances" are good.**

Supreme court model?

- **Life appointments!!! No…**
- **Arbitration? TANNSAAFL judging?**

What is the community (meta-) process that will create the acceptable process?

An example -- long term planning

Consider the addressing/routing situation.

Consider (just for fun) my security elephant.

How could we as a group decide what to do about security?

- **Can we converge on an assessment of the peril?**
- **Can we rank this with other perils?**
- **Can we direct the funds to do research?**
- **Can we hold a steady course in the storm?**

I offer these questions for deliberation?

- **Think positive thoughts.**
- **Remember: If we have a problem it is due to too much success.**