

**A Long-term Internet Perspective
on Confidence:
Confidence building and future
challenges in the Internet tradition**

John C Klensin, Ph.D.

15 June 2008

A Confidence Question?

- Be sure we are focusing on the right question
 - “Confidence” means different things to different people
 - And from different perspectives
- Useful to
 - Understand history
 - Understand implications of the technology
 - Understand tradeoffs and make them intelligently
 - Continue to make (or let) a very adaptable network design adapt.

Design for Resiliency

- Examples...
 - Hourglass design (presentation this morning)
 - Resilient to changes in low-level media
 - Unaffected by new applications -- no disruption
 - No need to standardize and test network-wide first
 - Routing architecture can find alternate paths on packet basis, not just at call setup
 - Redundancy in network, not just in super-hardened devices
 - Network reliability, not device reliability

Resiliency and Confidence

- Local outages not Internet outages
- Response to a weak ISP...
 - More connections, not more investment in ISP
 - Several weak ISPs ... often more robust than one high-cost excellent one
 - One can follow the traditional model: endpoint choice, not an Internet decision
- Think about access plans in Internet ways

A Changing Network

- Internet technology had two decades to mature before most people were aware of it
 - Stopped being a basic technology experiment a long time ago
- Many transitions without visible disruption
- The hourglass and new transport technologies
 - No low-level transport in use in 1980 is in significant use today
 - Remember the WiFi transition? Compare to cell phones.

A Stable Network Supporting Innovation

- Because...
 - Network does not need to be changed to add applications
 - Applications do not need to be changed to add or change access-layer (below IP) media
- ... network remains stable as applications and connectivity change
- History of the Internet should inspire confidence about ability to respond to future changes and problems.

Terminology and Answers

- Choices of terminology can confuse us and lower confidence
- Evaluate in terms of needed basic functions
 - PSTN is optimized differently
 - Evaluating with PSTN language or regulations unfair to both.
- Think carefully about questions

Communications Networks, Innovation, and Bad Behavior

- In new communications networks throughout history,
 - Often the bad guys are the early innovators and adopters.
 - No one tried to rob an intercity train until there were intercity trains
- Criminal adaptation to technology
 - Does not make the technology bad
 - Should not lower basic confidence
- Must respond to, deter, and punish the behavior

Criminals and Technology

- Criminal behavior is a social/legal problem, not generally a technology one
- There are few, if any, new Internet crimes
 - Adaptations of old ones
 - E.g., identity theft and stock fraud via postal scams long before the Internet
- Technology
 - Should offer tools for responding to or preventing Internet-facilitated crimes
 - Cannot solve the problems
- Avoid technology “solutions” that reduce robustness, impair innovation, and reduce confidence

Challenges to Legal System and Law Enforcement

- Hard to keep Internet within National Boundaries
- Not completely a new problem – history of International Broadcasting
- Problem not amenable to technology-only solutions
- Will continue to need better cooperation models

Spam as an Example

- Actually an old problem – the Internet makes it more efficient but motivations unchanged
- Technology can provide some tools
 - Tradeoffs with legitimate privacy concerns and efficient, robust email
- Still not being taken seriously as antisocial behavior
 - Transition from “spam conditionally tolerated” to “spammers go to jail”
 - Like any other antisocial behavior

Assuring Confidence, Security, and Deployment

- Strong user and system authentication could provide a foundation for solving problems
- Technology available for decades
- Never really deployed – obstacles:
 - Tools
 - Liability
 - Regulations
 - Education
- Strong identifiers not always desirable
- Be thoughtful and sensible

Attacking the Medium, Not the Crimes

- Blaming the Internet for...
 - Poorly-designed user interfaces
 - Weak operating systems and careless users
 - Ordinary criminal behavior that now uses the Internet rather than, e.g., the Post.
 - Unattractive or illegal content
- Crippling the Internet to prevent these things
 - Bad strategy
 - May destroy potential for innovation
 - Also will not work

Protecting the User

- Things computers do well; things people do well
 - Important to figure out the difference
 - ...and then take advantage of it
 - Need to get lots better at how systems advise users
 - Mostly a local system problem, not an Internet one
- Fool-proof systems
 - May protect ordinary fools against their own follies and carelessness
 - But cannot protect complete and exceptional fools

User Confidence and User Behavior

- Security, privacy, application robustness, confidence
 - Depend on User-System-Internet partnership
 - All three required
 - More police cannot completely compensate for unlocked doors
- Some actions require informed user decisions about risks and consequences
- Technology can help inform, but should not be expected to decide

The Internet of the Future

- Ongoing evolution in access-level media
- Many more new applications
- Continuing threats and responses
 - but better sense of proportion
- User understanding and responsibility
 - Increase to match “normal” world
 - Better technology to inform and advise
- No return to telephone-style “intelligent” network unless
 - We want to suppress innovation or raise costs

Summary

- Internet is inherently robust against
 - Local failures
 - New applications (even bad ones)
 - Criminal behavior as a network disrupter
- We need to treat crimes as crimes... internationally
- Continued adaptation and evolution is a necessity, not an option
- History and experience should give us a sense of confidence