Exploring Grand Challenges in Trustworthy Computing

Eugene H. Spafford
Executive Director, Purdue University CERIAS
-and-
CRA Board of Directors

Computing Research Association (CRA)

200+ computing research departments, industrial and government labs

- Six affiliated societies
- Mission:
  - strengthen research and education in the computing fields
  - expand opportunities for women and minorities
  - improve public and policymaker understanding of the importance of computing and computing research in our society

The State of Cybersecurity

- 4000+ security flaws reported in 2003
  - 3/4 were simple design flaws
- Over 100,000 known viruses & worms
  - New ones reported at a rate of 200 per week
- Large-scale attacks doubling per year
- Damages “hidden” but mounting
  - Viruses alone projected at $55B per year
  - Spam is 60% of email

Current research

- Mostly focused on fixing the past or on abstract theory
  - Fixes for Windows, Linux, TCP/IP v4 ...

Viruses, worms, DDOS, buffer overflow, authentication, forensics, firewalls, MLS design, intrusion detection and prevention, covert channels, crypto, digital cash, datamining, cyber terrorism, patch application, residues, root kits, trojan horses, sniffers, DRM, ...

Need Focus on Long-Term Research

- Immediacy of threat has led to too much focus on near-term needs
  - Patch rather than innovate
- Policy lags innovation
- Focus, and thus progress, is often episodic
- Problems go beyond national defense
- Need to grow the talent pool

We need more of this:

Why Grand Challenges?

- Inspire creative thinking
  - Encourage thinking beyond the incremental
- Some important problems require multiple approaches over long periods of time
- Big advances require big visions
  - Small, evolutionary steps won't take us everywhere we need to go

The Conference*

- Held 16 Nov 03 – 19 Nov 03
- 50+ invitees from around the world
  - Invitations based on 220 submitted abstracts
  - Students to retirees, novices to legends
  - Industry, academia, government
- Series of debates and writing exercises, guided by a program committee

* Supported, in part, by NSF grant EIA-0137943, which is gratefully acknowledged.

Computing in the Future

- Smaller, cheaper, embedded computing
- Pervasive networking and mobility
- Global reach and global participation
- Growing volumes of data
- Growing population of user-centric services
  - Internet commerce
  - E-government
  - On-demand services
  - Telecommuting
  - Individualized entertainment

Two Alternate Futures

- Overwhelming unsolicited junk
- Rampant ID theft
- Frequent network outages
- Frequent manual intervention
- Largely unchecked abuses of laws and rights

- No spam or viruses
- User-controlled privacy
- Uninterrupted communications
- "Hassle-free" computing
- Balanced regulation and law-enforcement

Overarching Vision

- Intuitive, controllable computing
- Reliable and predictable
- Supports a range of reasonable policies
- Adapts to changing environment
- Enables rather than constrains
- Supports personal privacy choices
- Security not as an afterthought, but as an integral property

The Role of Security

Security is like adding brakes to cars. The underlying purpose of brakes is not to stop you: it's to enable you to go fast! Brakes help avoid accidents caused by mechanical failures in other cars, rude drivers, and road hazards.

Better security is an enabler for greater freedom and confidence in the Cyber world.

Why is it Difficult?

- Adversaries with a variety of motives and backgrounds
- Increasing complexity
- Increasing value of targets
- Reduced cost of entry
  - Low-cost connectivity
  - “Point and shoot” attacks
- Increasing leverage from asymmetric threats

Challenge #1

What is the Challenge?

Elimination of epidemic-style attacks

- Viruses and worms
- SPAM
- Denial of Service attacks (DOS)

Why is this a Grand Challenge?

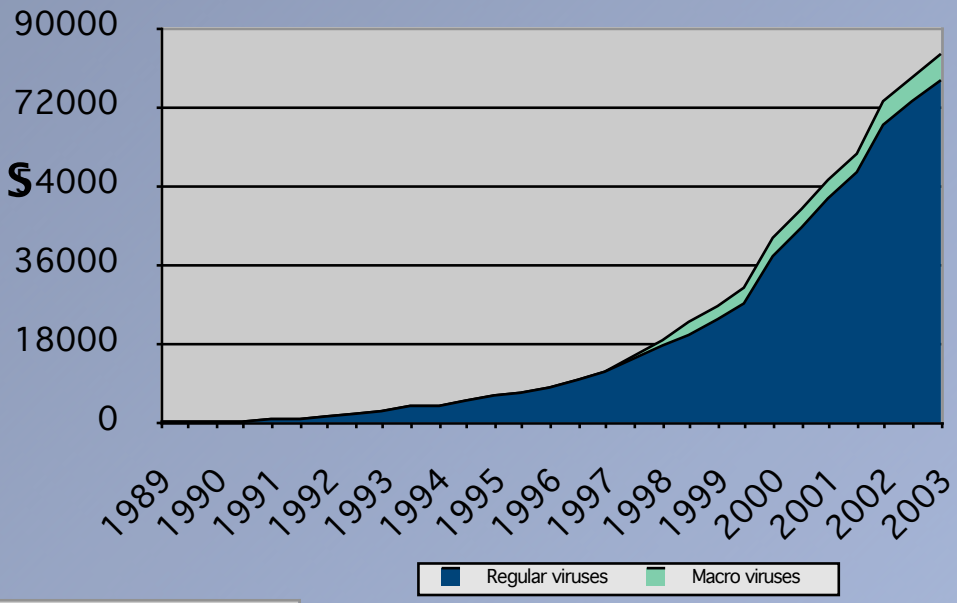
- Epidemic-style attacks can be fast
  - Slammer worm infected 90% of vulnerable hosts in less than 30 minutes
  - Attacks exploit Internet's connectivity and massive parallelism
- Price of entry is low for adversaries
  - Very easy for "uneducated" to launch the attack
- Unpredictable attack techniques and sources
  - Polymorphic worms and viruses
  - Anonymous attackers
- No organized active defense
  - Poor visibility into global Internet operations
  - No emergency global control

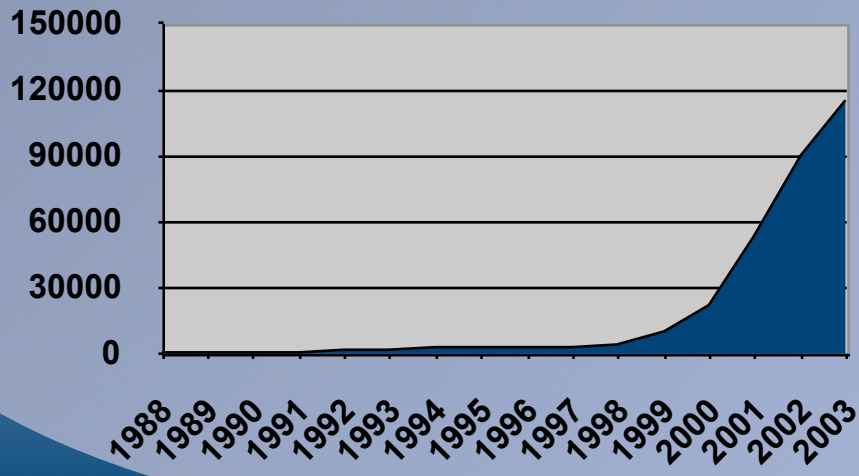
Why Does it Matter?

- Cost of attacks are tremendous (tens of billions of $$ annually; $55 billion in 2003!)
  - Costs to enterprise operations
  - Decreased productivity
  - Loss of confidence in information infrastructure
- Internet is being used today for critical infrastructure
  - Hospitals, ATM networks, utilities, air traffic control
- Eliminating malware will:
  - Support emerging classes of applications (e.g., telemedicine)
  - Increase trust and confidence

Current Trends

Reported Viruses





Attacks Reported by CERT

Barriers to Overcome?

- Nobody owns the problem
  - Finger-pointing among developers, network operators, system administrators, and users
- Lack of Internet-scale data
- Lack of Internet-sized testbeds
- May need legislative support
- Conflicting economic interests

Challenge #2

What is The Challenge?

Develop tools and principles that allow construction of large-scale systems for important societal applications that are highly trustworthy despite being attractive targets.

- e.g., patient medical record databases
- e.g., electronic voting systems
- e.g., law enforcement databases

Why is This a Grand Challenge?

- Worldwide, computing technology is being adopted to support critical applications
- We do not know, in general, how to build systems that resist failures and repel attacks with high confidence
- We do not understand how to compose systems into networks of trustworthy systems

Why Does it Matter?

- Computing and networking are becoming pervasive in all aspects of society
- Systems are being built and deployed now that may not be fully trustworthy, and whose failures will have major negative impacts.
- Critical applications must be trustworthy!

Why Does it Matter? Examples

- If medical databases are trustworthy and doctors have access to full patient results
  - There are fewer mistakes due to online checking, fewer defensive medical tests, fewer unnecessary medical procedures, lower medical costs, and fewer patient deaths, saving more than $100B / year in the US alone!
- Ensuring that e-voting is trustworthy
  - Helps preserve faith in democracy for all parties around the world
  - May eventually help reduce fraud and mistakes in elections worldwide

Barriers to Overcome?

- Reconciling various legal regimes with technological capabilities
- Provision with acceptable cost
- Achieving balance of privacy with security in record-keeping
- Integration/replacement of legacy applications having lesser (or no) protections

Challenge #3

What is The Challenge?

For the dynamic, pervasive computing environments of the future, give end-users security they can understand and privacy they can control

- Technology can easily outrun comprehensibility. Security implementation must not make this worse
- Must not lose control of my information, my privacy, my location

Why is This a Grand Challenge?

- The looming future
  - Instant access to information
    - First responder, medical records, parents
  - Exploiting the benefits of IT everywhere
  - Convenience, safety, empowerment
- Why a challenge for this community?
  - Avoid the high pain of leaving these concerns for later
- Product-makers should not be the only stakeholders in the design process
  - Threats to privacy are a critical concern
- Multicultural issues

Why Does it Matter?

- It's important to get in at the beginning
  - Experience teaches us that these concerns are hard to add after the fact
- The Internet experience informs us:
  - It is also a social system, not simply a technology
- Once we give up privacy or security, we may not be able to regain it
- Important to assert a leadership role while we can!

Barriers to Overcome?

- User needs are much broader than traditional security models
  - Bridge the gap from user to mechanism
  - Privacy doesn't always fit in traditional security models
- Dynamic environments are challenging
- Device heterogeneity is challenging
- Multiple competing stakeholders
- It's difficult, in general, to make things usable
- Real-life user security requirements and policies are hard to express in terms of current mechanisms

Challenge #4

What is The Challenge?

Develop quantitative information-systems risk management that is at least as good as quantitative financial risk management.

Why is This a Grand Challenge?

- We do not understand the full nature of what causes IT risk
- We do not understand emergent behavior of some vulnerabilities and systems
- Failures in networked systems are not independent

Why Does it Matter?

- We cannot manage if we cannot measure: If you don't have a measure you will either under-protect or over-spend
- What you measure is what you get
  - Measuring the wrong thing is as bad or worse than not measuring anything at all
  - The measures ultimately need to be consistent, unbiased, and unambiguous

Why Does it Matter?

Lord Kelvin (William Thompson) wrote:

> "When you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is a meagre and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely, in your thoughts, advanced to the stage of science."

Why Does it Matter?

- Questions the CIO cannot answer
  - How much risk am I carrying?
  - Am I better off now than I was this time last year?
  - Am I spending the right amount of money on the right things?
  - How do I compare to my peers?
  - What risk transfer options do I have?
- For that matter, they have no corresponding ability to match their efforts to warning levels such as **Yellow**, **Orange**, **Red**

Barriers to Overcome?

- It's difficult – getting the model right, picking the right measures, gathering the right data
- No one wants to be first to disclose information
- This requires data sharing and common terminology
- There are legal, cultural, business, and scientific issues here
- The "I don't want to know" mentality
  - "This will remove plausible deniability"
  - "I might have to do something about it or tell somebody"

The future does not need to look like the past!

"Legacy" should be a base, not an anchor.

Quote to start

- "A program that has not been specified cannot be incorrect; it can only be surprising ."
  Proving a Computer System Secure,
  W. D. Young, W.E. Boebert and R.Y. Kain, The Scientific Honeyweller (July, 1985), vol. 6, no. 2, pp. 18-27.

Quote #2

- "…From a practical standpoint the security problem will remain as long as manufacturers remain committed to current system architectures, produced without a firm requirement for security. **As long as there is support for ad hoc fixes and security packages for these inadequate designs and as long as the illusory results of penetration teams are accepted as demonstrations of a computer system security, proper security will not be a reality.**"

Preliminary Notes on the Design of Secure Military Computer Systems, Roger Schell, USAF, 1/1/73

Spaf's Top 10 #1

- Composable policy
  - Dynamic coalitions
  - Reuse of policy
  - Expressed in
    - human language
    - computer-readable format
  - Captures existing models

TOP 10 #2

- Useful security metrics
  - Comparison metrics
  - Economic metrics
  - Incident metrics
  - Analytical models
- Answer the questions:
  - Is system A more secure than B?
  - Have I spent enough on security?

Top 10 #3

- Useful (new) models of security
  - do away with MLS!
  - replace C-I-A
  - take into account
    - mobility
    - anonymity
    - processing power
  - need to support coalitions
  - support change

Top 10 #4

- Securable architectures
  - minimized and/or partitioned
  - heterogeneity
  - distributed
    - location
    - control
    - production
  - appropriate reuse
  - verified?

Top 10 #5

- Forensic technologies based on science
  - network traceback
  - causality analysis
  - attribution
  - chain of custody, evidentiary issues
- Attribution and root cause analysis are forensic issues

Spaf's Top 10 #6

- Data pedigree technologies
  - correctness
  - temporal trail
  - combination/processing retention
  - "interval" processing
  - usable audit
  - entity tracing

Top 10 #7

- Usable HCI for infosec/privacy control
  - standard ontology
  - requires metrics
  - usable by novices
  - understandable feedback
  - “what-if” controls
  - expert system advice

Top 10 #8

- Science-based privacy
  - what is privacy?
  - cultural basis
  - understanding trade-offs
  - transitive controls
  - effect containment

Top 10 #9

- Effective identity management
  - include authorization without identification
  - support for pseudonyms
  - group identities
  - single-use identities
  - integration with social and psychological models

Top 10 #10

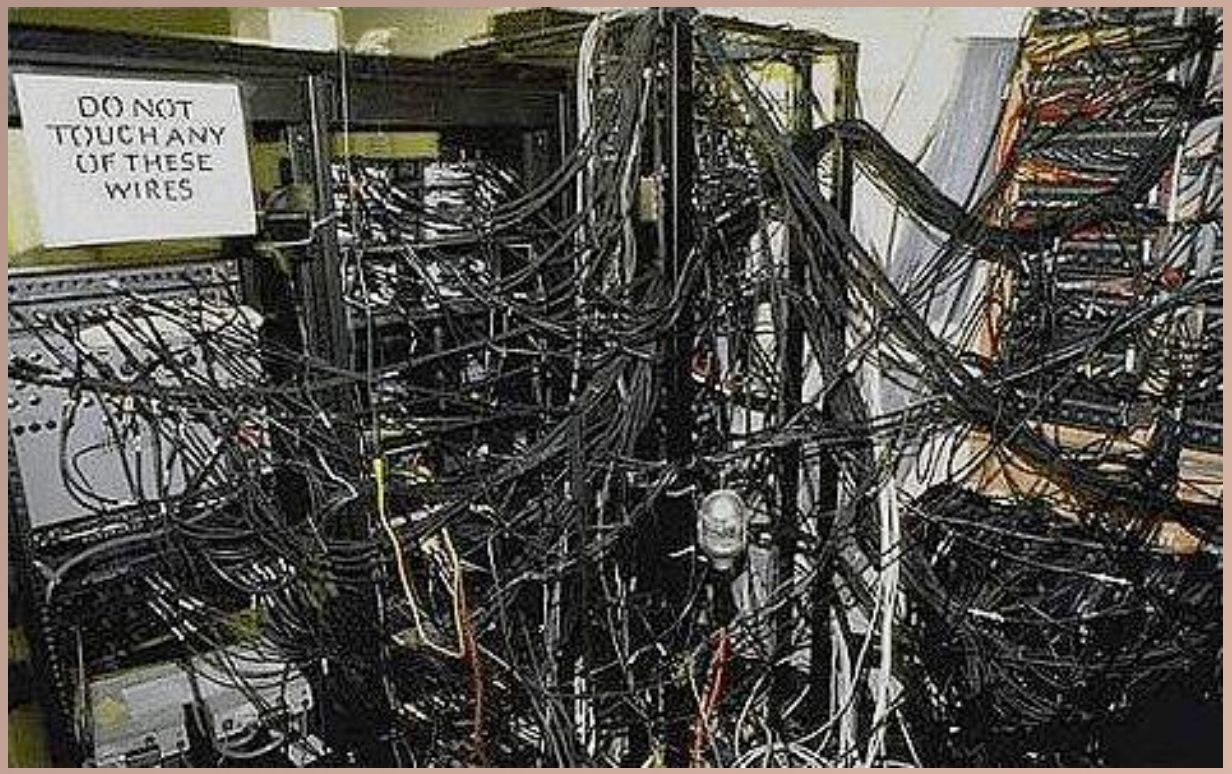
- Science-based QoS control
  - formal definition of QoS/availability
  - graceful degradation design
  - attack tolerance
  - capacity switching
  - reactive capacity

And not strictly security...

- Rigorous software development
  - Full design
  - Full requirements capture
  - Emergent property consideration
  - Safe(r) programming languages
  - Self-test and recovery
  - Strong V&V methods
- Strong configuration management

Keep in mind

Emergent behavior is important in the real world



For More Information

Visit the CRA Grand Challenges WWW page:

http://www.cra.org/Activities/grand.challenges/

http://www.cra.org/Activities/grand.challenges/security/home.html

CERIAS

http://www.cerias.purdue.edu/