Four Grand Challenges in Trustworthy Computing

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

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 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 CCR-0335324, which is gratefully acknowledged.

Trustworthy Computing?

- Identified as important in first Grand Challenges conference
- Clear and increasing public needs
- Poses significant research challenges
- Synergistic with current industry and government initiatives
  - e.g., NSF Cyber Trust

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 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

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

The Grand Challenges:

1) Eliminate epidemic-style attacks within 10 years
   - Viruses and worms
   - SPAM
   - Denial of Service attacks (DOS)

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

The Grand Challenges:

3) Within 10 years, quantitative information-systems risk management is at least as good as quantitative financial risk management.
4) For the dynamic, pervasive computing environments of the future, give end-users security they can understand and privacy they can control.

Challenge #1

What is the Challenge?

Elimination of epidemic-style attacks by 2014

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

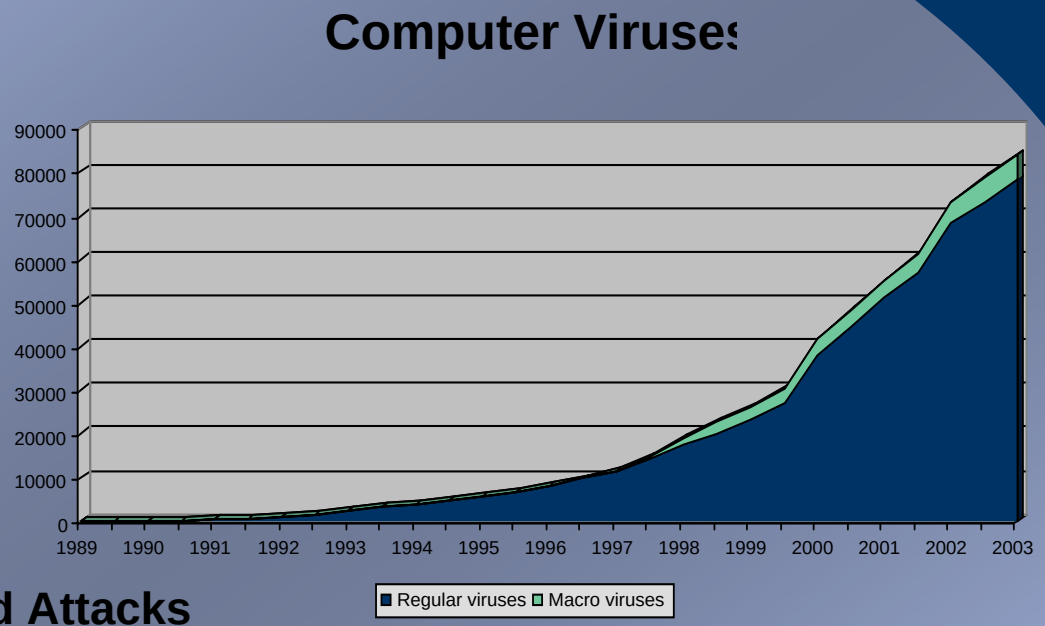
Why is this a Grand Challenge?

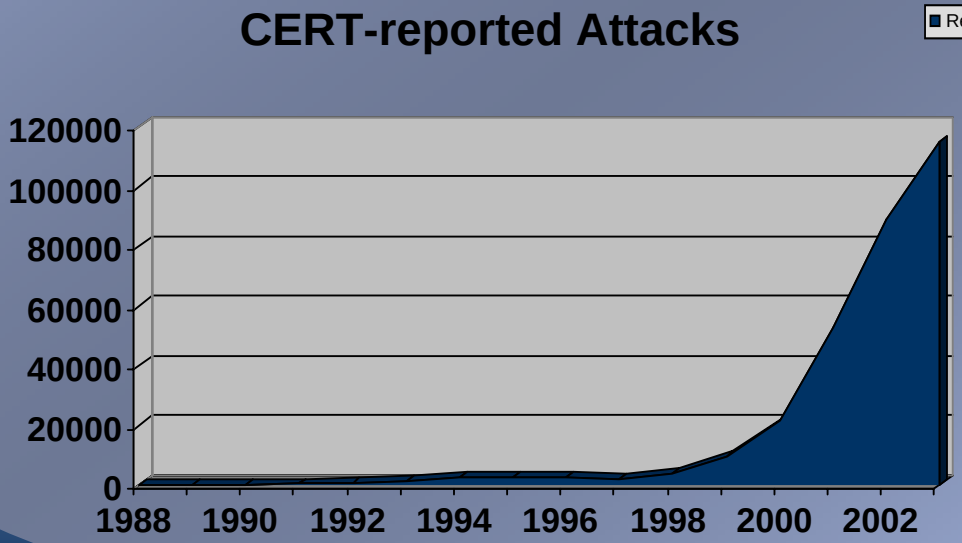
- Epidemic-style attacks can be fast
  - Slammer worm infected 90% of vulnerable hosts in less than 30 minutes
  - Attacks exploit Internet's connectivity and massive parallelism
- Price of entry is low for adversaries
  - Very easy for "uneducated" to launch the attack
- Unpredictable attack techniques 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)
  - 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





Why is Progress Possible?

- All stakeholders now recognize this as a significant, growing problem
- We have built some systems with limited functionality that are not susceptible to attacks
- We can envision solutions that should work if they were further developed and deployed

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

How can Success be Demonstrated?

- No more:
  - Internet Worms
  - Internet-wide Service Interruptions
  - Massive spam attacks against ISPs, Email Providers, and businesses
- Internet protection:
  - Supplied standard on all new computers, routers, large & small appliances
  - A mitigation strategy is available for existing infrastructure

What Else Might be Enabled?

- Reduction in “noise” enabling better identification of other cyber crimes
- Redirection of significant capital (human, financial, and technical) to other, constructive needs
- Increased confidence in computing infrastructure

Who Will Be Involved in the Solution?

- Short Term:
  - Researchers
  - Software developers
  - Network operators
  - Businesses
  - End-users
- Long term:
  - Researchers
  - Educators
  - Media
  - Regulators & law makers
  - International law enforcement

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

- 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
- 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!

Why is Progress Possible?

- Recent paradigm shift from perimeter defense to intrusion and failure tolerance and recovery
  - Survivable systems look promising
- Encryption technologies have been proven trustworthy
- Moore's Law
  - Amazing growth in computing, communication, and storage resources
  - May allow trustworthiness to be a 1st class property along with functionality, performance, and cost

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

How Can Success be Demonstrated?

- Create online medical databases that survive severe disasters and attacks without human intervention
  - Confidentiality: no unauthorized disclosure of records
  - Integrity: no unauthorized alteration of records
  - Auditability: record all attempts to access online info
  - Availability: maximum downtime less than 2 minutes per day, and an average of less than 5 minutes per month
  - Accessible globally

Who Will be Involved in the Solution?

- Researchers
- Software & product developers
- Network operators
- Businesses
- Service providers (e.g., medical professionals)
- End-users
- Regulators & government
- Media

Challenge #3

What is The Challenge?

Within 10 years, 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**

Why is Progress Possible?

- We are already collecting data
- Security is now on the minds of senior management
  - But, we don't yet speak their language
- There exist things to steal
- But we have even yet to try concepts from portfolio management, public health, accelerated failure time testing, quality control, insurance

Barriers to Overcome?

- It's hard – 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"

How Can Success be Demonstrated?

- We will be able to predict outcomes
- We will be able to titrate – we can choose our point on the cost vs. risk curve
- Our businesses and governments can take more risk and gain more reward
- We can communicate across the boundaries of shareholders, suppliers, regulators, the market, and others
- Risk transfer for information security can achieve liquidity

Who Will be Involved in the Solution?

- People in the other disciplines already doing similar things
  - Public health, quality control, portfolio management, insurance, fault tolerance
- People who worry about fault tolerance
- Researchers
- Businesses

Challenge #4

What is The Challenge?

For the dynamic, pervasive computing environments of the future, give computing 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!

Why is Progress Possible?

- Widespread concern in many segments of society
- New awareness that trust and cyber security require a broader view of needs
- Some existing efforts are laying groundwork to respond to this challenge

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

How Can Success be Demonstrated?

- Societal acceptance
  - Does the user feel in control of this world she now lives in?
  - Has the user in fact lost control of his information, his privacy, his …
- Emergence of a ubiquitous world of computing and communication that is:
  - Simple and easy to use
  - Dependable, reliable
  - Trustworthy
  - Not overly intrusive

Who Will be Involved in the Solution?

- Researchers
- Regulators
- Policymakers
- Software and hardware vendors
- Telecommunications
- Educators
- Many “average” users from around the world


COMPUTING RESEARCH ASSOCIATION
CRA

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