Cyber Security Research Priorities

Florida State University Information Security Summer School

Jim Davis
Chief Information Officer
Iowa State University

Overview

- In a more perfect world….
- PITAC Recommendations
- CRA identifies Grand Challenge problems in security
- Discussion – what do you think are the big near-term research issues?

In a perfect world

I want my computer to be secure! I want:

- My private information protected
- Software to be resistant from attacks so it doesn't fail
- Software updates that never break my computer
- Easy integration of new software and hardware that is compatible with my security schema

In a perfect world (2)

- Control over who can access my files
- Secure transmission of information to/from my computer
- Networks that can resist attacks so I'm not inconvenienced by toasted routers and hosts
- To feel confident about the validity of the identity of those I communicate with

In a perfect world (3)

- Clear and consistent laws covering information processing
- Shared consensus on ethical behavior in the cyber world
- All this security stuff has to be cheap, fast, effective, and easy to use

Am I asking for too much?

Break it down

- Authentication – effective, easy to use, preserves my privacy, scope may be extended beyond my enterprise network to encourage collaboration
- Software and systems designed to be secure, can be build piecewise incorporating components from unknown parties, and benchmarked against accepted metrics
- Secure network protocols adopted
- Sound technical basis for laws, supported by appropriate accountability mechanisms in systems

Challenges to security

We have (a billion?) systems deployed in which:

- Interoperability and ubiquity is more important than security
- Contain poorly designed or tested software
- Have incorrectly configured security controls
- Basic security “science” is not yet well developed
- Incomplete, inconsistent, or incompatible security policies
- Explosive growth of the Internet exacerbates these problems

Challenges to security

And we have (a billion?) users who have:

- Poor computing practices (sharing accounts, weak passwords, etc.)
- Lack of knowledge about *best practice* techniques
- No ownership for the security problem, nor a commitment to the solution

Challenges to security

And an environment where:

- The responsibility for building secure systems has shifted from the government to industry (COTS)
- Core research problems are under funded
- Few US Universities offer a robust education and research program in security like FSU does
- Many federal organizations are involved, without focused leadership and accountability

Focusing the community on important problems in security

- President's Information Technology Advisory Committee (PITAC) http://www.nitrd.gov/pitac/
- Computing Research Association (CRA)
  2003 Grand Challenge Workshop www.cra.org

President's Information Technology Advisory Committee

- President's Information Technology Advisory Committee (PITAC) http://www.nitrd.gov/pitac/
- Report released February 2005
- Major themes:
  - Fund more basic research in cybersecurity
  - Increase the number of researchers in cybersecurity
  - Focus on problem areas that need more research

PITAC Recommendations

1. Authentication Technologies

- Research on infrastructure protocols for large-scale key distribution and management
- Certificate and revocation management
- Integration with biometrics and physical tokens
- Decoupling authentication from identification to address privacy issues

PITAC Recommendations

2. Secure Fundamental [network] Protocols

- Tradeoffs between Security and performance
- Security of protocols even when parties are not trusted
- Areas: VoIP, everything wireless, VPN, Web services

PITAC Recommendations

3. Secure Software Engineering and Assurance

- Programming languages and systems that include security features
- Portable and reusable code
- Technologies that capture requirement definitions and design specifications
- Verification and validation techniques
- Ability to test against metrics
- Ability to verify that software does not contain undocumented exploitable features

PITAC Recommendations

4. Holistic System Security

- Build secure systems with trusted and untrusted components new and legacy components
- Address insider threats
- Modeling and analyzing emergent failures in complex systems
- “Human factors engineering”: easy to use interfaces that promote security
- Supporting privacy in conjunction with security

PITAC Recommendations

5. Monitoring and Detection

- Real-time and dynamic protection that can react when attacks are detected
- Global scale monitoring and IDS
- Monitoring systems to ensure they comply with security policies
- Tools that better characterize “normal” behavior
- Better user interfaces that help humans understand what is happening when an incident unfolds

PITAC Recommendations

6. Migration and Recovery Methodologies

- Rapid recovery from outages and attacks
- Increase automatic operation and self-recovery of systems to reduce the insider attack threat
- Fault tolerance and graceful degradation

PITAC Recommendations

7. Cyber Forensics

- Identifying the origin of cyber attacks, traceback
- Identifying attackers based on their behaviors
- Tracing stolen information, for example, as it is used in identity theft
- Forensic friendly systems that are more amenable to investigation after an incident

PITAC Recommendations

8. Modeling and Testbeds for New Technologies

- System simulation environments
- Validating simulations involving millions of nodes
- Gathering and synthesizing large amounts of data

PITAC Recommendations

9. Metrics, Benchmarks, and Best Practices

- Develop security benchmarks and metrics
- Risk assessment, objective measures of risk and cost of defense
- Automated tools to assess compliance and risk
- Tools (e.g., code scanning) to assess vulnerabilities
- Documenting best practices in, for example, auditing, configuration, and patch management

PITAC Recommendations

10. Non-Technology Issues

- Enhance the perceived value of security in products
- Enhance the perceived value of protecting privacy
- Examine how users interact with IT, focusing on ethics, culture, and behavior
- Examination of issues related to regulation and taxation
- Consideration of the impact of IT laws

Computing Research Association 2003 Grand Challenge Workshop

1. **Address epidemic style attacks**

   Spam, DoS, trojans, …, plague critical services

2. **Build trustworthy large-scale systems**

   Key societal applications moving to computers

3. **Quantitative information risk management**

   Enable decisions based on cost and benefit

4. **End user security and privacy**

   Give end users security they understand and privacy they control

Bottom Line…

Problems in security:

- Are very challenging, some approach the unsolvable
- Often more about people than technology
- Require a healthy dose of creativity mixed with methodical problem solving skills
- Are important (critical?) to society
- Are very rewarding to work on

You have chosen a wonderful discipline to work in!

Discussion

- What do you see as being important research problems?