Ten Years Past
and
Ten Years from Now

Matt Bishop
Department of Computer Science
University of California at Davis

Introduction

- Before 2000
  - Ware report (1970), Anderson report (1972)
  - Formal models: Bell-LaPadula (1973-1976)
    - Described a Multics implementation, with proofs
  - Saltzer and Schroeder (1975)
  - Program Analysis, RISOS (1976-1978)

Vulnerabilities in Systems

- PA, RISOS funded to study them
  - Focus was on detection
  - RISOS focus shifted to helping managers
  - Both gave classification schemes
- As computers became popular, systems grew
  - Still had security holes
- . . . And so did the consequences of those holes

Vulnerabilities Then and Now

- Then: buffer overflows, race conditions, failure to check input, malware including Trojan horses
- Beginning of decade: same ideas, different realization
  - Phishing
  - Command (SQL) injection
- Refined over the decades
  - Spearphishing
  - Cross-site scripting

And Still . . .

- Old vulnerabilities *not* solved
  - Often combined with new technology, so may be obscured
  - Not always; Mathematica flaw earlier this year
    - Race condition with /tmp file
- Many flaws due to improper configuration
  - Complex interaction of components
  - Confusing user interfaces
  - Patches not installed (or installed!)

Prominence of Security

- Initially, physical
  - Access to systems guarded
  - Network end points secured
- Not considered too important before 1988
- Grew slowly in importance since then, until 2000

Changes in Computer Use

- How has our use of computers changed?
- How will it change?

Previous Decade: 2001–2010

- Increase in connectivity led to security problems
  - Interconnected networks grew in size, number
  - Security policies conflicted
  - More data available to all

Government Computer Use

- Advanced, sophisticated in some areas
  - Sensor networks
  - Remote controlled vehicles
- Security issues
  - Video transmissions not encrypted
- Assurance Issues
  - NASA probe to Mars

Standards: Common Criteria

- Protection Profiles for functionality
- Evaluated Assurance Level (EAL) for assurance
- Certification
  - Independent testing laboratories certified by government agency
  - Multilateral recognition agreements
- Read *any* certification claim carefully!

Other Government Computers

- Used primarily internally
  - Typically developed long before 2000
- Developing plans, mechanisms to upgrade
  - Internally, to provide better information for decisions
  - Externally, to provide better access to public
- Requirements often constrained by laws, regulations

Compliance

- Demonstrate that systems meet these requirements
  - Paperwork: evaluators examine the paper descriptions of systems, procedures, policies
  - Examination: evaluators access system, examine it directly
  - Testing: evaluators try to compromise the system
- Mandate a specific configuration
  - Does not assure it won't be changed once deployed!

Connectivity

- Increased dramatically
  - Networks connected to provide wider access to devices and information
  - Also provided access for the nasty people!
- Risks for industry
  - Bad publicity
  - Financial liability

Convergence

- Ability to deliver same services over many varied devices and networks
  - VoIP-enabled cell phones that switch to get best coverage
  - Messages, phone calls go to device in user's possession, wherever he or she is
- Lots of security implications . . .

Security Implications

- Information flows over devices, networks that organization has no control over
  - Indeed, the organization may not know about them!
- Data may be available to intermediate organizations or people
  - Especially if not properly protected . . .

Data Aggregation

- Lots of personal information out there
- What happens when people find it and assemble it?
  - Make correct inferences about you, your life, etc.
  - Make *incorrect* inferences about you, your life, etc.
- Especially revealing with data on social networks
  - Often *very* personal

Non-Computer Folks

- Use of computers among average people grew dramatically
  - Don't want to learn how to secure their system
  - Just want to get their task done
- May not know what "security" means
  - Exact definition may vary . . .
- Vendors providing the security
  - Like centralized security configurations of organizations mentioned above

Problems

- Home, small business use much more varied
  - Microsoft Windows XP SP2 locked system down
  - It also broke third-party software
- Environments also more varied
  - User interface security: abbreviations can be deceptive
  - Automatic updating: what fixes one system may break another

Summary

- Lots of improvements in understanding, practicing security
- Growth of computer use, Internet introduced problems of scale and connectivity
- “Security as a service” began to aid those who could not secure their own systems
- Data aggregation became a problem as well as a benefit

Next Decade: 2011–2020

- Convergence accelerates
  - Interconnection of technology increases availability of data
  - Merging of computer security domains (the composition problem)
  - Collaboration involving different, possibly contradictory, laws and customs

Data Aggregation

- Better techniques, tools for building profiles of people, events
  - Spot trends, interpret events as they occur
  - Reveal private information
  - Derive inaccurate profile of subject or target
- Better techniques, tools for evading this
  - Try to minimize information exposure
  - Deception: give false informtion

Compliance

- Shift from paper-based validation to combination of paper, examination, testing
  - Move away from checklist evaluations
- Standardized configurations common
  - Centralize security administration
  - Vendors will do this, too
- For home, small business, this will evolve to opt-in
  - Allows vendor to configure patches properly

Communication with Users

- Asking writer to construct security policy won't work
  - Skilled with words, ideas, expression
  - Usually not technologically knowledgeable
- Area of study: how to construct, implement security policies, mechanisms that protect such users
  - Notification of problems in *their* language, not ours!

Paradigm Shift

- Human-oriented, not technology-oriented
- Beginnings: social networking
  - Trust models based on properties of social networks
  - Will enhance quality of life for users
  - Also increases exposure of personal information
- People accept loss of privacy . . . Or "privacy" redefined to reflect new needs, new world

Computer Infrastructure

- Infrastructure: a collective term for the subordinate parts of an undertaking: substructure, foundation
- Infrastructure is:
  - Internet and interconnected networks
  - Human resources to support computers

Previous Decade: 2001–2010

- Trust in the infrastructure
  - Foundational protocols (TCP, IPv4, UCP, etc.) designed for different security model
  - Security protocols layered on top (SSL, TLS, etc.)
  - Designed for specific purposes
    - Getting packets to destination reliably
    - Providing confidentiality, integrity between two endpoints

Public Key Infrastructures

- Certificate-based PKIs under design since 1980s
- Hierarchical, business-oriented
  - What standards does Certification Authority use?
  - How do you cross-certify (or do you?)
- Web of trust
  - How do you know what terms “untrusted”, . . . , “ultimate trust” mean?
  - How is this enforced (or is it?)

DNS and IP

- Domain Name Service
  - Foundation of how many network protocols, structures work
  - Currently vulnerable to many types of attacks
- DNSSEC
  - Allows digitally signed DNS records
- IPSec, IPv6
  - Add authentication, integrity to IP layer
- Neither is widely used

Forensics

- Tracing packets, attacks back to origin is of increasing importance
  - What is “origin”?
- Infrastructure does not support this analysis
  - Can get some information
- Do you want it for technical purposes, legal purposes, or both?
  - Rules for gathering, preserving data vary

Attribution

- Ability to identify origin of packets and data
  - At all layers
  - Again, what is “origin”?
- Entities involved in this:
  - End points (users, systems, organizations, etc.)
  - Infrastructure (routers, resolvers, transited networks, governments, etc.)
- Types: sender-receiver, one only, none, deniable, incorrect

SCADA Networks

- Not usually thought of as infrastructure
- Now, as SCADA networks being connected to other networks, they are
- Much easier to reach and maintain (good)
- Much easier to reach and disrupt (bad)
  - Involve basic community services like power, water
  - Disruption much more disastrous than compromising Internet!

Testing

- How do we test effects of changes, attacks, defensive policies and mechanisms on large infrastructures?
  - Implement, see what happens (really bad idea)
  - Simulation (often not effective)
  - Build large testbeds
- DETER/EMIST, Planetlab
- Beginnings of GENI

Research in Computer Security

- Becoming more scientifically rigorous
- 2000: McHugh's critique of Lincoln Labs IDS testing
  - Pointed out need for proper testing procedures, proper framing of hypotheses
- Currently, data for experiments rarely shared
  - Often, data not usefully characterized
  - This makes interpretation of results hard

Summary

- Assurance of infrastructure not suitable for highly secure computations, applications
- New security technology needs support old infrastructure often cannot supply
- Need to protect end points as well as connections
- Need more science in this field!

Next Decade: 2011–2020

- Some great things simply won't work
  - Universal PKI
- Need to consider social impacts of security policies, procedures, mechanisms
- Complexity of management increases
- Rise of infrastructure-oriented virtualization

Universal PKI

- Non-technical barriers block it
  - Would People's Republic of China accept as authoritative the root CA of the Republic of China?
  - A forest of certification hierarchies, cross-certified
- Web of Trust
  - Similar to social networks, as meaning of trust levels are personal, not standardized
  - Thus, create confusion until you know what "untrusted" . . . "ultimate trust" mean *to the signer*
  - Enables anonymity easily

Attribution: Double Edged Sword

- Great for governments
  - Track down malefactors
  - Observe spies, other people visiting government systems
- Bad for governments
  - Others can use it too, against government
  - Example: in U.S., intelligence agents visit Al Queida web site . . . With complete attribution, Al Queida *knows* what these folks are looking for

Societal Impacts

- Law evolves slowly
  - Specialized requirements to meet evidentiary constraints
  - What is traditional is held to work (usually)
- Technology evolves rapidly
  - Often implications not clearly understood
  - Interpretation of technical information difficult for non-specialists, depending on education, research

Secure Technologies

- More numerous
- These will spread throughout the network
  - Slowly at first
  - Then very rapidly
- Why? Security is not their driver . . . Yet
  - Cost of implementation, deployment
  - "If it ain't broke, don't fix it" attitude

Security Management

- Current view: a necessary evil
  - If it interferes with work, ignore it
- Changing to symbiotic relationship supporting the proper functioning of the organization
  - Institutional imperative
- Need for better management tools
  - These will be unified
  - User interface will be complex initially

Virtual Infrastructure

- Apply notion of "virtual system" to infrastructure
- "Slices" provide illusion of an infrastructure
  - Many slices per infrastructure system (routers, etc.)
  - Slices can be isolated, so attack on one can't affect another
- GENI using something like this for experimentation

Conclusions

- Practitioners at the forefront of security
  - Talk to people to find out what they really need
  - Educate people is what can *and cannot* be done
  - Set up defenses
  - Gather *real* data, test ideas out
- Academics provide needed support
  - New ways to approach problems
  - Lay foundation for validating, improving practice
  - Teach what we have learned
- **Academics, practitioners *must* work together**

More Conclusions

- Some conflicts simply cannot be resolved, so we must accept that and learn to live with them
- Security must be flexible, not rigid, because of the unexpected

- Ultimately, it's all about people!

Author Information

Matt Bishop
Department of Computer Science
University of California at Davis
1 Shields Ave.
Davis, CA 95616-8562
USA

phone: +1 (530) 752-8060 *fax*: +1 (530) 752-4767
email: bishop@cs.ucdavis.edu
www: http://seclab.cs.ucdavis.edu/~bishop