Computer Security

Lessons Learned:

What to Do to Try to Minimize the Dangers of Intrusion and Attack.

Our Current Predicament

- Why are we in our current predicament:
  - Software vendors focus on shipping products on time, to the exclusion of proper testing and security issues. Often, released code is barely alpha level, and as a result may have significant security vulnerabilities.
  - Security is often done only as an afterthought, sometimes using merely lip service ("Yes, we have that, too!")
  - Many networks are run by inexperienced and overworked system / network administrators, who may not know how to secure their systems, nor even how to discover whether an intrusion has occurred.
  - The number of users of computer systems is rapidly increasing, and virtually all of them are unaware of the dangers, are easily duped into doing unwise things, and are typically focused on getting their jobs done rather than worrying about "theoretical security threats".
  - Attackers seem to be in plentiful supply, are extremely inventive and resourceful, and are becoming more and more sophisticated.

What Can We Do?

- There's not much we can do about:
  - Fixing software vendors' poor habits
    - Short of giving strong feedback and/or refusing to buy their products!
  - Improving the abilities of system / network administrations
    - Short of ensuring that your company looks for the right kinds of people – assuming that they are available in the first place!
  - Reducing the demand for end users.
    - Companies are claiming high levels of productivity, but all this means is that fewer people are doing more work. Guess what those fewer people have less time to focus on?
    - Outsourcing isn't going to fix this; it just changes where the users are!
  - Dissuading attackers from attacking us.

What Can We Do?

- We can do the following, however:
  - Ensure that our system / network administrators and end users are as educated as possible about the problems.
  - Ensure that, at least for the systems we control, they are designed from the start with strong security in mind.
    - Harden systems to prevent malicious software from finding its way onto them.
    - Design applications to use only those features that they absolutely need, and to make them less susceptible to attackers' attempts to subvert them.
- In short, every organization needs a ***Security Policy***
  - Not merely a document that pays lip service to security requirements
  - An applied, constantly reviewed, policy that includes
    - Practical, day-by-day, active operations
    - Education of all the organization's users to increase awareness and show need.

What Does the Future Hold?

- ***The optimists***:
  - Eventually, software vendors, governments, companies, etc., will devote more resources to ensure system security.
  - Security will be designed into operating systems and applications from the ground up
  - Computing platforms and software will enforce strong security
  - Software products will be thoroughly tested before entering production
  - Systems will have vulnerabilities discovered very quickly, and patches developed and installed in almost real time
  - System features which introduce security risks will be disabled by default, and only turned on by users after examination of all the risk implications

Will this happen before Hell freezes over?

What Does the Future Hold?

- ***The pessimists:***
  - Attackers will continue to discover significant vulnerabilities in our systems.
  - Organizations will continue to fall victim to attacks
  - Attacks are likely to become more sophisticated and damaging.
  - Our society is becoming more and more dependent on computers for our daily operations – banking, medical, transportation, education, even PDAs, cell phones, cars (perhaps even toasters, and refrigerators!) – and so is more and more susceptible to such attacks.

Does this sound more realistic?

How Do I Keep Abreast of the Threats?

- There are a number of Web Sites which provide useful updates on the latest attacks, threats, and techniques:
  - **Packet Storm Security**
    - packetstormsecurity.nl & www.packetstormsecurity.org
  - **Security Focus**
    - www.securityfocus.com
    - Hosts the Bugtraq mailing list and archives, plus other mailing lists
  - **Global Information Assurance Certification (GIAC)**
    - www.giac.org
    - Founded by the SANS (System Administration, Networking, and Security) Institute
    - Certifies information security professionals

How Do I Keep Abreast of the Threats?

  - **Phrack Electronic Magazine**
    - www.phrack.org
    - Free, online magazine
  - **The Honeypot Project**
    - http://project.honeynet.org/
    - Installs systems on the Internet which simply wait for attacks.
  - **Mega Security**
    - www.megasecurity.org
    - Large collection of Trojan Horses, backdoors, RootKits, etc., showing screen shots, author's name, origination country, etc.
  - **Infosec Writers**
    - www.infosecwriters.com
    - Includes Hitchhiker's World, an online magazine about security

How Do I Keep Abreast of the Threats?

- **Counterhack**
  - www.counterhack.net
  - Ed Skoudis' Web site (same name as his Counter Hack book)
- **Security Portal**
  - The Web site www.securityportal.com now simply redirects to www.redsiren.com, which appears to be a commercial security company.
  - Skoudis, in his Counter Hack book, describes "Kurt's Closet" articles especially an "Ask Buffy" ("Buffy Overflow") feature. Both seem to be hard to find, now:
    - http://www.postfix.org/securityportal.199909/closet19990915.html
    - http://linuxtoday.com/search.php3?author=Buffy:Overflow

How Do I Keep Abreast of the Threats?

- **2600 / Hacker Quarterly**
  - http://www.2600.com/
- **White Hats**
  - http://www.whitehats.com/
- **Attrition.org**
  - http://www.attrition.org/
  - Virtual museum of hacked Web pages
- **Information Security Magazine**
  - http://www.infosecuritymag.com/
  - Corporate view

Security-Related Mailing Lists

- Each of these mailing lists requires you to subscribe by sending an email, and then responding to the response email:
  - Bugtraq
    - http://www.securityfocus.com/archive/1
  - NT Bugtraq
    - http://www.ntbugtraq.com/
  - CERT (Computer Emergency Response Team) Coordination Center at Carnegie Mellon University has a CERT Advisory mailing list
    - http://www.cert.org/
  - Crypto-Gram
    - http://www.counterpane.com/crypto-gram.html
    - Bruce Schneier's monthly email newsletter

Security-Related Conferences

- **DefCon**
  - http://www.defcon.org/
- **Black Hat Briefings**
  - http://www.blackhat.com/
- **SANS (System Administration, Networking, and Security)**
  - http://www.sans.org/