Security Awareness

- Goals
  - Educate attendees on the importance of security in our organization.
  - Provide a security framework that can be implemented for a low- to medium-risk site.

Why Security?

- NIST and DOC requirements
  - OMB Circular A-130, Appendix III
  - NIST Security Policy and Procedures
  - DOC and government-wide initiatives
- Our reliance on information technology
- Confidentiality, Availability, and Integrity[1]
- Cost of incident response and disaster recovery
- Protecting each otherCommon Misconceptions

[1] Basically we're talking about the creditibility of an organization. If you don't have a basic level of confidentiality of data, availability of resources, and integrity for your IT services, why should anyone trust what you say?

Common Misconceptions

- “We’ve never had an incident...”
- “My data isn’t that important”
- “We have an open campus anyway, what’s the use”

Threats

- Use/abuse of resources[1]
- Corruption of data
- Denial of Service (DOS)
- Deletion of Data
- Disclosure of Data
- Component Failure

[1] An attacker using your system/resources to attack other systems (maybe your systems or maybe those of another organization).

Methods of Attack

- network scanning, hacker toolkits
- stolen laptops
- social engineering
- guessed, cracked passwords
- stale accounts
- known security vulnerabilities in software, denial of service, viruses
- capturing information transferred insecurely (e-mail, ftp, telnet)

Threats	Methods of Attack	Risks	Examples[a]
Usage of Data/ Services	• All methods	• Loss of credibility[b]	Kevin Mitnick
Corruption of Data	• All methods	• Loss of credibility[c] • May never know extent of corruption	• http://www.2600.com/hacked_pages/index.html • http://www.2600.com/hacked_pages/old_archives.html
Denial of Service	• Automated tools • Known vulnerabilties	• Loss of services to audience • Loss of credibility[d]	Yahoo, eBay, Amazon, CNN, February 2000 DDOS attacks.
Deletion of Data	• All methods	• Downtime • Loss of credibility[e]	ILOVEYOU virus and variants

[a] Realize that most organizations do not make break-ins public due to the possible loss of credibility to the organization. Sanitized statistics may be found at www.cert.org but not all incidents are reported to CERT so we can only guess at how many examples exist in the world today.

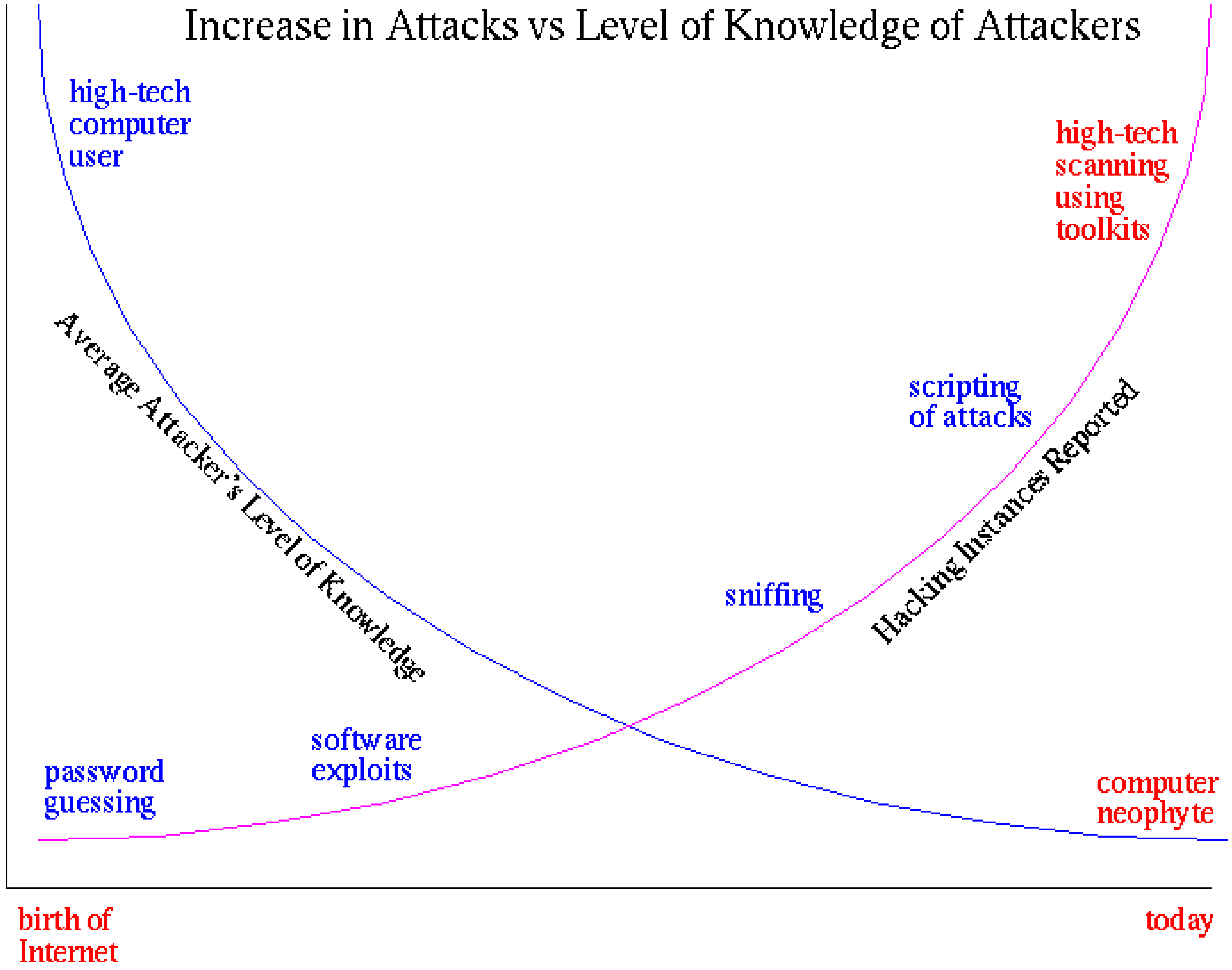
[b] Our resources used to break into other sites, other sites go public with our involvement, we lose credibility.

[c] Our organization releases a report/spreadsheet/whitepaper or runs tests with corrupted data, errors are found, we lose credibility with industry.

[d] Customers attempt to use our our service are denied access, Our reputation is tarnished if downtime or service lapse is lengthy or reasons for lapse are discovered. Who would want to trust data that comes from a site with poor security?

[e] Downtime cauases a denial of service or loss of productivity. Deliverables slide, we lose credibility with industry.

Increase in Attacks vs Level of Knowledge of Attackers



Our Security Issues

- Sharing and writing down passwords
- Guessable, less-secure passwords
- Cleartext passwords and other sensitive data (i.e. telnet, e-mail, POP)
- Remote computers (i.e. laptops, home computers)
- Training system administration staff
- Awareness training for all staff
- Stale/unused network accounts
- No clear policy/procedures

Solution

- Standardize Security Infrastructure
- Computer Security Policy and Procedures[1]
- Awareness training for all staff
- Management support (i.e. allocate budget & time)
- Technical solutions (i.e. Firewall, IDS)
- All parts work together

[1] Based on our accepted level of risk. Policy defines how we protect our organization. Procedures assist with implementation of policy.

How do we get there

- Acknowledge importance of security
- Balance security with our mission
- Follow security policy and procedures
- All staff assist in education process
- Be an example to other staff

Summary

- Each person has a responsibility to every other person
- All IT services are at risk when there is an incident
- Policy is just one part of the Security Infrastructure

Security Web Sites

- {Our organization’s security site}
- NIST Security Clearinghouse: http://csrc.nist.gov
- White hats: www.cert.org
- Grey hats: www.l0pht.com (that’s a zero in the name)
- Black hats: www.2600.com
- Timely articles:
- www.securityfocus.com

The 7 Top Management Errors that Lead to Computer Security Vulnerabilities

Number Seven:
Pretend the problem will go away if they ignore it.

Number Six:
Authorize reactive, short-term fixes so problems re-emerge rapidly

Number Five:
Fail to realize how much money their information and organizational reputations are worth.

Number Four:
Rely primarily on a firewall.

Number Three:
Fail to deal with the operational aspects of security: make a few fixes and then not allow the follow through necessary to ensure the problems stay fixed

Number Two:
Fail to understand the relationship of information security to the business problem -- they understand physical security but
do not see the consequences of poor information security.

Number One:
Assign untrained people to maintain security and provide neither the training nor the time to make it possible to do the job.

As determined by the 1,850 computer security experts and managers meeting at the SANS99 and Federal Computer Security Conferences held in Baltimore May 7-14, 1999. http://www.sans.org/newlook/resources/errors.htm

Social Engineering Example

Social Engineering Threats (from http://www.ernst.ns.ca/networks/english/social.htm)

With the many security features of your computers, the worst security breach is most always your users because they hold a key to the door to your system with their accounts.

First and foremost, social engineering is about convincing people to do what you want by either playing on their assumptions or by misrepresentation and lying. If the intruder uses this method, he has realized that people, in general, want to be helpful. If given the opportunity they will usually try to help out as much as they possibly can. For example, a simple phone call following the dialog below is a method intruders often
use:

Mr. Smith:

Hello?

Caller:

Hello, Mr. Smith. This is Fred Jones in tech support. Due to some disk space constraints, we're going to be moving some user's home directories to another disk at 8:00 this evening. Your account will be part of this move, and will be unavailable temporarily.

Mr. Smith:

Uh, okay. I'll be home by then, anyway.

Caller:

Good. Be sure to log off before you leave. I just need to check a couple of things. What was your username again, smith?

Mr. Smith:

Yes. It's smith. None of my files will be lost in the move, will they?

Caller:

No sir. But I'll check your account just to make sure. What was the password on that account, so I can get in to check your files?

Mr. Smith:

My password is tuesday, in lower case letters.

Caller:

Okay, Mr. Smith, thank you for your help. I'll make sure to check you account and verify all the files are there.

Mr. Smith:

Thank you. Bye.

The reality of this situation, is that in the morning when Mr. Smith calls technical support he will probably find out that there is nobody by the name of Fred Jones who works there. The only way to prevent situations like these from happening, is to educate the users on a system. They should never give out a password over the phone to a caller, or leave one in their email or voice mail. Intruders use social engineering by convincing users to give them what they want without even having to try to break in.