Foundations of Computer Security

Lecture 2: Why Security is Hard

Dr. Bill Young
Department of Computer Sciences
University of Texas at Austin

Is Cyber Security Particularly Hard?

Question: Why would security be any more difficult than most technological problems?

Answer 1: Most technology-related efforts are concerned with ensuring that something good happens. Security is all about ensuring that *bad things never happen*.

In security, not only do you have to find "bugs" that make the system behave differently than expected, you have to identify any features of the system that are susceptible to misuse and abuse, *even if your programs behave exactly as you expect them to.*

What Bad Things?

Answer 2: If security is all about ensuring that *bad things never happen*, that means we have to know what those bad things are.

The hardest thing about security is convincing yourself that you've thought of all possible attack scenarios, before the attacker thinks of them.

"A good attack is one that the engineers never thought of."
–Bruce Schneier

Programming Satan's Computer

Answer 3: Unlike most technology problems, you have to defeat one or more actively malicious adversaries.

Ross Anderson characterizes this as *"Programming Satan's Computer."* The environment in which your program is deployed works with malice and intelligence to defeat your every effort.

The defender has to find and eliminate *all* exploitable vulnerabilities; the attacker only needs to find *one*!

Easiest Penetration

Answer 4: Information management systems are a complex, "target-rich" environment comprising: hardware, software, storage media, peripheral devices, data, people.

Principle of Easiest Penetration: an intruder will use any available means to subvert the security of a system.

"If one overlooks the basement windows while assessing the risks to one's house, it does not matter how many alarms are put on the doors and upstairs windows." –Melissa Danforth

Security Isn't the Point

Answer 5: Security is often an afterthought. No-one builds a digital system for the purpose of being secure. They build digital systems to do something useful.

Security mechanisms may be viewed as a nuisance to be subverted, bypassed, or disabled.

Upshot: Perfect Security Ain't Happening

Perfect security is probably impossible in any useful system.

"The three golden rules to ensure computer security are: do not own a computer; do not power it on; and do not use it." –Robert H. Morris, former Chief Scientist of the National Computer Security Center (early 1980's)

"Unfortunately the only way to really protect [your computer] right now is to turn it off, disconnect it from the Internet, encase it in cement and bury it 100 feet below the ground." –Prof. Fred Chang, former director of research at NSA (2009)

If Security Gets in the Way

Security is meant to prevent bad things from happening; one side-effect is often to prevent useful things from happening.

Typically, a tradeoff is necessary between security and other important project goals: functionality, usability, efficiency, time-to-market, and simplicity.

Some Lessons

He who defends everything defends nothing. –old military adage

- Security is difficult for several reasons.
- Since you can never achieve perfect security, there is always a tradeoff between security and other system goals.

Next lecture: Security as Risk Management