Foundations of Computer Security

Lecture 3: Security as Risk Management

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

Security as Risk Management

If perfect security is not possible, what can be done.

Viega and McGraw (*Building Secure Software*) assert that software and system security really is "all about managing risk."

Risk is the possibility that a particular threat will adversely impact an information system by exploiting a particular vulnerability.

The assessment of risk must take into account the consequences of an exploit.

Risk Management Framework

Risk management is a process for an organization to identify and address the risks in their environment.

One particular risk management procedure (from Viega and McGraw) consists of six steps:

1. Assess assets
2. Assess threats
3. Assess vulnerabilities
4. Assess risks
5. Prioritize countermeasure options
6. Make risk management decisions

Coping with Risk

Once the risk has been identified and assessed, managing the risk may involve:

Risk acceptance: risks are tolerated by the organization. e.g. sometimes the cost of insurance is greater than the potential loss.

Risk avoidance: not performing an activity that would incur risk. e.g. disallow remote login.

Risk mitigation: taking actions to reduce the losses due to a risk; most technical countermeasures fall into this category.

Risk transfer: shift the risk to someone else. e.g. most insurance contracts, home security systems.

Annualized Loss Expectancy

One common tool for risk assessment is *annualized loss expectancy* (ALE), which is a table of possible losses, their likelihood, and potential cost for an average year.

Example: consider a bank with the following ALE. Where should the bank spend scarce security dollars?

Loss type	Amount	Incidence	ALE
SWIFT* fraud	$50,000,000	.005	$250,000
ATM fraud (large)	$250,000	.2	$50,000
ATM fraud (small)	$20,000	.5	$10,000
Teller theft	$3,240	200	$648,000

* large scale transfer of funds.

Is ALE the Right Model?

Annualized Loss Expectancy effectively computes the “expected value” of any security expenditure.

Consider the following two scenarios:

1. I give you a dollar.
2. We flip a coin. Heads: I give you $1000. Tails: you give me $998.

Note that *the expected values are the same in both cases* ($1), but the risks seem quite different.

Lessons

- Because perfect security is impossible, realistic security is really about managing risk.
- Systematic techniques are available for assessing risk.
- Assessing risk is important, but difficult and depends on a number of factors (technical, economic, psychological, etc.)

Next lecture: Aspects of Security