Measuring Software Security

Defining Security Metrics

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

Last updated: May 1, 2015 at 08:15

Why Is CyberSecurity Hard?

Why is cybersecurity any harder than any other technological problem? *Or is it?*

Partial answer: Most technological problems are concerned with ensuring that something good happens. Security is all about ensuring that *bad things never happen*.

What Bad Things?

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

Cyber Defense is Asymmetric

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

In cybersecurity, you have to defeat an *actively malicious adversary*.

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

You Can't Defend Everything

Modern information management systems are a complex, "target-rich" environment comprising: hardware, software, storage media, peripheral devices, data, and people.

He who defends everything defends nothing. –old military adage

Security Isn't the Point

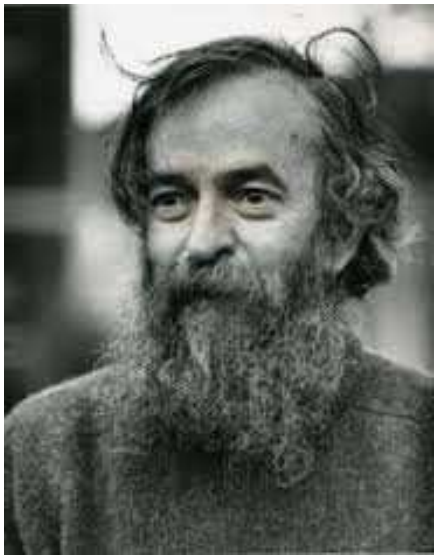
Security is often treated as an afterthought. *No-one builds a digital system for the purpose of being secure.* They build digital systems to do something useful.

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

It's often hard to convince management to allocate extra resources to prevent attacks that may never occur.

The More Things Change ...

"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 (mid 1980's), former chief scientist of the National Computer Security Center



"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 (2009), former director of research at NSA

Perfect Security: It Ain't Happening

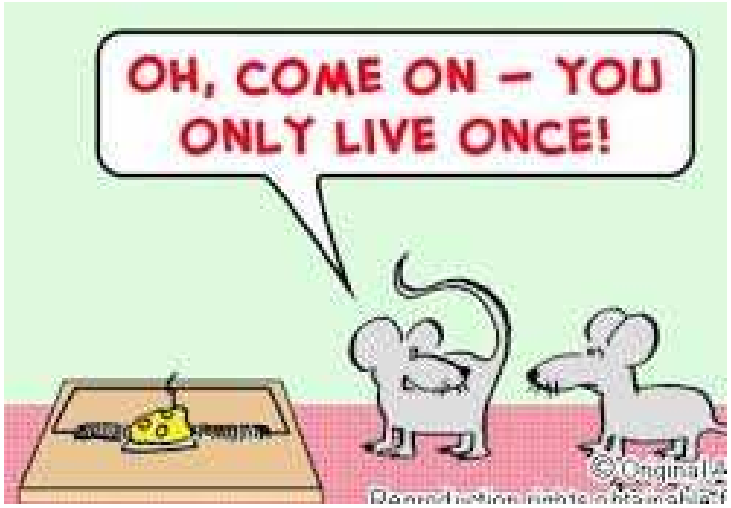
Perfect security is unachievable in any useful system.

We trade-off security with other important goals: functionality, usability, efficiency, time-to-market, and simplicity.

Security is Risk Management

Viega and McGraw, *Building Secure Software* assert that software and system security 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 is a process for an organization to identify and address the risks in their environment.

Current IT Security Metrics

"If you can't measure something, you can't understand it. If you can't understand it, you can't control it. If you can't control it, you can't improve it." H. James Harrington

Some Popular IT Security Metrics:

- Security risk assessment matrices
- Security vulnerabilities and incident statistics
- Annualized loss expectancy (ALE)
- Return on investment (ROI)
- Total cost of ownership (TCO)

Current Metrics are Flawed

Typical Security Risk Assessment:

		Likelihood of Event		
		High	Medium	Low
Severity of Impact	High	"We're Doomed!"	Bad	Outlier
	Medium	Bad	Not Good	Error
	Low	Annoyance	Typical	"Whatever..."

Problem: This doesn't measure security risk; it measures human judgments about risk. *That can be useful, assuming you understand what you're getting.*

Counting Vulnerabilities or Incidents

The number of vulnerabilities discovered or security-related "incidents" are often used as general indicators of the level of security.

But these depend critically on:

- How thorough are your scans?
- How many systems are scanned?
- What severity is assigned to what vulnerabilities/incidents?
- How many applications are deployed?
- How does your number compare with peers?

Annualized Loss Expectancy

ALE is a common tool for risk assessment. Given potential threats, where do you put your security dollars?

Risks in a large bank:

Loss type	**Amount**	**Incidence**	**ALE**
SWIFT fraud	$50,000,000	0.005	$250,000
ATM fraud (large)	$250,000	0.2	$100,000
ATM fraud (small)	$20,000	0.5	$10,000
Teller theft	$3,240	200.0	$648,000

But this is really nothing more than expected value! Is that the right way to compute risk?

Is ALE the Right Model?

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.

The expected values are exactly the same, but the risks seem quite different.

Often ALE deals in opinions and expectations because IT security does not have data to define actual probabilities.

ROI and TCO

Return on Investment (ROI) attempts to calculate how much benefit will be gained from an investment.

- How do current security expenditures affect future losses? This is very hard to estimate.
- Traditionally, ROI (in a financial setting) involves profit or rate of return. These don't apply well for a security investment.

Total Cost of Ownership (TCO) seeks to quantify the cost over the entire lifecycle of the investment.

- Only really applies to security purchases, not to measurement of the IT security process.
- Data for adequate comparison is lacking.

Lessons from Other Industries

We typically don't have very good data for estimating IT security risk!

Other industries—insurance, manufacturing, design—have a long history of dealing with risk.

Some lessons:

1. Metrics and process will improve as the ability to collect, analyze and understand data improves.
2. *Security is a business process.* You must measure the business process to measure security.
3. *Security results from human activities.* You must understand people as well as technology.

Choosing Good Metrics

One approach: The Goal-Question-Metric (GQM) method borrowed from software engineering.

Goal: *What do I need to accomplish in my security program?* Goals should be specific, limited, meaningful, contextual, well-documented.

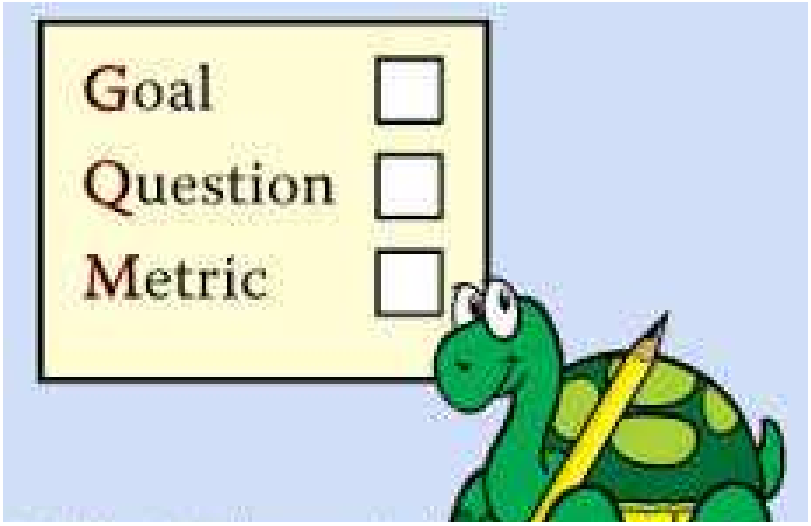
Questions: *What specifically must I learn for that goal to be realized?*

Metrics: *What data must I collect to answer the questions raised by the goals?*

GQM provides a structured process for thinking about security, translating thoughts into requirements, and developing the data to meet those requirements.

Example: GQM for Security-Related Downtime

Goal Statement: *Understand security impact on system availability by reviewing security-related downtime as a percentage of total downtime.*



Question 1: How often is the system down due to failure?

Metrics: Time between failures
Failure duration
Mean system availability

Example: GQM for Security-Related Downtime

Question 2: How often is the system down due to maintenance?

Metrics: Time between maintenance events
Maintenance duration
Mean system availability

Question 3: How often is downtime the result of a security event?

Metrics: Number of security events in time period
Duration of event remediation

Are Goals Appropriate? Cisco Example:

The security goals must align with the mission of the enterprise.

Operating System Count & Urgent Vulnerabilities

	# Hosts	# Vuln.	# Hosts w/ Vuln.	% Hosts w/ Vuln.
Windows	4212	593	347	8.2
Linux	8026	62	41	< 1
Solaris	2733	216	143	5.2
Cisco	4626	6	6	< 1

Presented with these findings, Cisco management responded that since Linux and Cisco OS teams "had less than 1 percent of their hosts with high severity vulnerabilities, those teams must be spending too much time, effort and resources patching their hosts." (Hayden, *IT Security Metrics*, p. 84)

Conclusions

- Cyber security is important, but hard.
- Perfect security is impossible, so treat it as risk management.
- Must measure security to improve security.
- Some popular metrics are weak, largely because the underlying data is weak.
- Systematic approaches exist to build successful IT security metrics programs.
- Treat security as another business process.