Systems Thinking + Web Security

Michael Stone <*mistone@akamai.com*>

Introductions

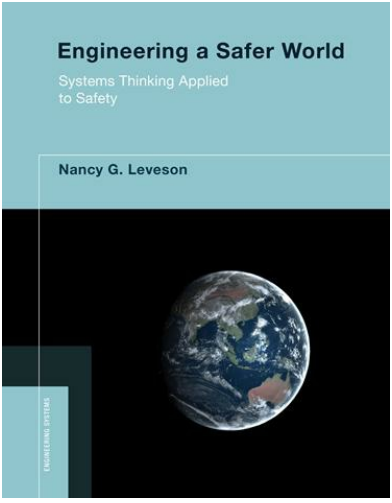
Q: Why InfoSec? A: Storytime...

2007-2009:

2009-present:

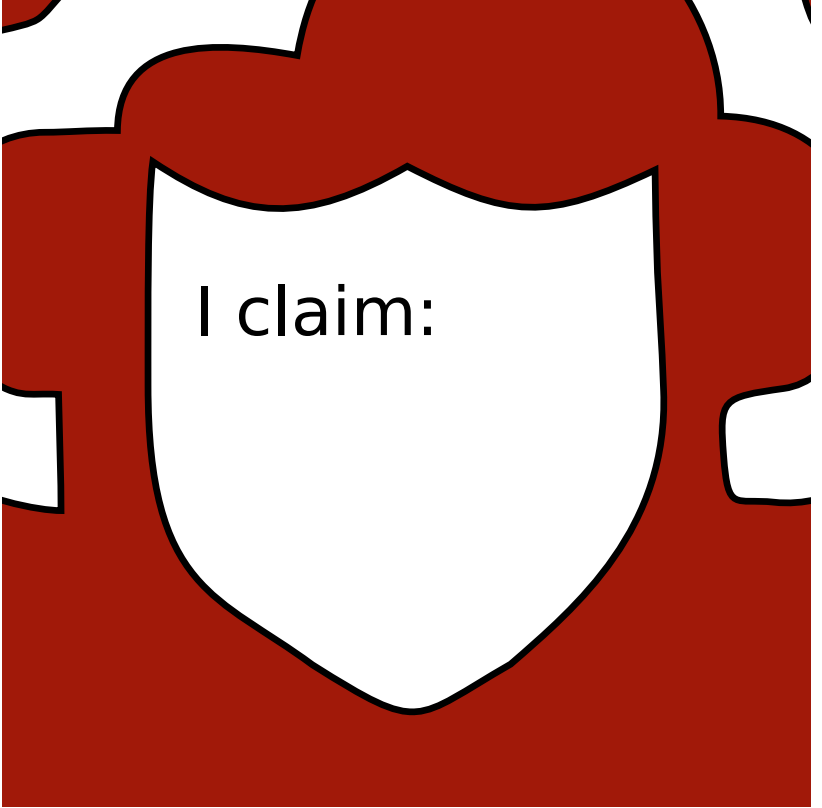
search: "nortel espionage", "stuxnet", "aurora"

Q: Can system safety improve web security?



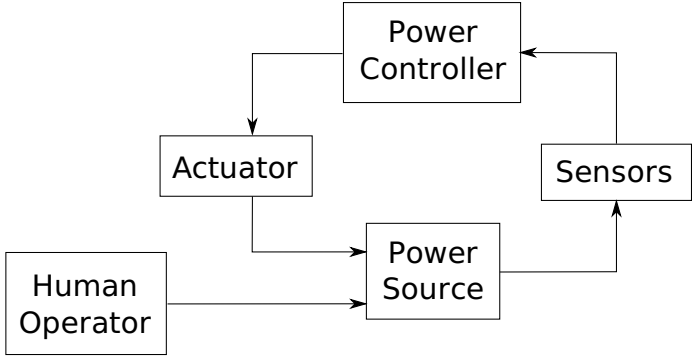
?

Q: ...or vice versa?

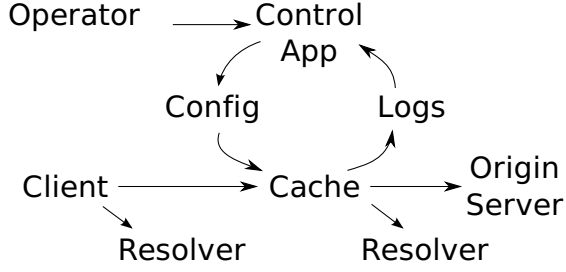

I claim:

Motivation 1: Diagrams sure look similar...

EaSW,
Ch. 8



Akamai:



Motivation 2: Definitions seem to align...

safety:
absence of accidents

accident:
unplanned + unacceptable loss event

"accident":
an unplanned + unacceptable loss event...
...potentially triggered by malicious activity.

∴ "Accidents" ⊆ Accidents
∴ Safety ⇒ no "accidents"

Problems:

1. No credible documentation of legacy safety constraints.

2. Control is non-hierarchical.

3. The system changes *fast*.

Solution:

rubric + ***examples*** *(+ research)*.

Motivation:

People need digestable training materials.

Rubric

context	At the coffee shop where Alice is browsing Bob's e-commerce site...
principals	we are relying on Alice and Bob *and **every** SSL CA*...
goals	to keep Alice's credit card number secret...
adversary powers	despite Mallory's snooping...
controls	by correctly using HTTPS and X509.

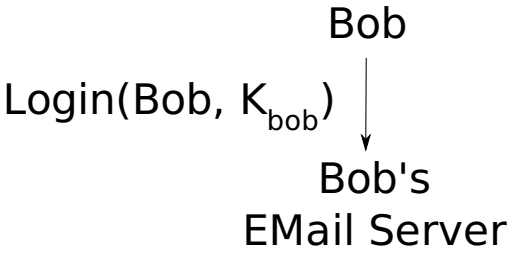
Key Observation

To get security by way of safety, incorporate your **Adversary** into the **environment** and build a control system to suit.

Typical **goals**:
secrecy, authentication, availability, access control, ...

Typical **adversary powers**:
reading, writing, spamming, spoofing, parsing, unparsing, ...

Example



Goals

availability
authentication
secrecy
access control

Q: Is this "safe"?

A: Depends on the Adversary's powers!

Power	Affected Goal(s)	Notes
provide	secrecy	impersonate Bob
withhold	availability	DoS Bob
delay	...	...
...	...	...
read	secrecy	**steal passwd**
write	authentication	**guess passwd**
	availability	**lock Bob's acct**
spam	availability	**DoS Server**

Zooming out...

Principals are (smaller) systems:

(i.e., "Alice" = Alice + desktop + browser + ...)

Protocols make untenable assumptions.

Conflicts of interest abound.

Finally, there are systemic risks...

Questions?

Michael Stone
<mistone@akamai.com>

http://mstone.info

(Thanks!)