In Search Of “Physical Laws” of Computer Security

Marcus J. Ranum
<mjr@ranum.com>

Who Am I?

- Early innovator in firewall market
- Early innovator in VPN market
- Early innovator in IDS market
- Currently researching system log analysis/aggregation and event management
- Sort of an “industry analyst”

What?

- What is this talk about and why?
  - I spend *way* too much time reading the writings of great scientists
  - I spend a lot of time working on internet security
  - I notice that there’s not a lot of “science” about “computer science” and even less about internet security

What is Science?

- Method, method, method!
  - – 10 Measure
  - – 20 Vary one attribute
  - – 30 Measure again
  - – 40 Learn something
  - – 50 GOTO 10

A perfect example of how “computer science” is not scientific - we accept the dogma of some old Dutch coot that GOTO is considered harmful and repeat it as if it is holy writ

What About Science in Computer Security?

- It would be nice

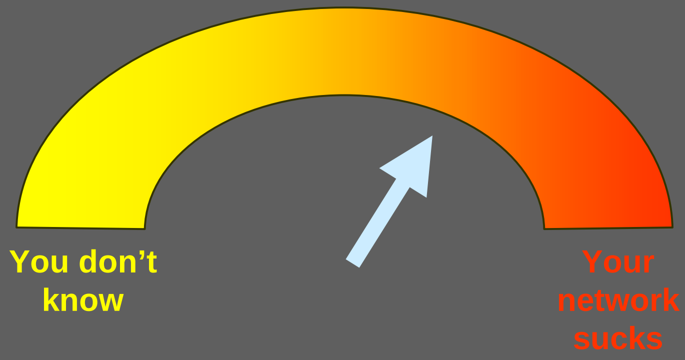
I didn’t know Ghandi, but I’m no Ghandi

The Current State of Affairs

- “Risk Management” - collect a bunch of wild guesses about probabilities of bad things happening
    - Merge those with information about known things that are wrong with our systems
        - Throw in some fudge factors and try to quantify probability that we can get hacked
            - BaH! Who cares? This is GIGO anyhow!

The Current State of Affairs

- “Penetration Testing” - Attempting to determine the quality of an unknown quantity using another unknown quantity and a constantly varying set of conditions
  - Baseline? Pshaw!
    - Regression? Ha!
      - The Badness Meter:



The Current State of Affairs

- “Security Surveys” - Largely self-selected samples (arrgh! Is there a *statistician* in the house!?)
  - Usually sponsored by vendor$
    - No connection between claim and measure (I.e.: “9 out of 10 people who *claim* they are CTOs *claim* that if they had $1m to spend they would spend it *all* on PKI thumbdrive scalable log analysis encryption!”)

The Current State of Affai

(another
self-selected
sample)

- “Statistics” - When the CSI/FBI survey reports “10% more sites report security incidents than last year”
  - – Is a virus outbreak a security incident?
    - What about theft of personal information?
      - – With no *useful* measurements it is *impossible* to assess the relative effectiveness of protections and products offering remedy
      - – We are only left with voodoo witch doctor claims - is that a coincidence?

Current Affairs: Summary

- Computer security looks more like a “cargo cult” than a scientific discipline

What to Do?

- I’d like to start trying to outline the basic physical laws of computer security
  - Obviously they are somewhat subjective but we should be able to refine them from here
  - In physics, if you claim to have a perpetual motion device you come under skeptical scrutiny
    - In security if you claim to have an “intrusion prevention system” you sell $million$

1

- Trustworthiness and Trust are not connected
  - The amount of trust that we place in a system may have nothing to do with whether or not it is worthy of that trust
  - A system can be said to be “insecure” if it is not worthy of the trust that is placed on it

The elusive definition of “secure”

2

- Transitive trust is always a property of trust
  - If A trusts B and B trusts C, A trusts C
    - And A usually doesn’t know it
  - By extension, as the number of trusted parties increases, the trustworthiness of the entire system goes down in relationship to the total amount of trusting going on

This principle has profound implications we will see again and again

3

- Security and Convenience are opposed
  - “Convenience” always means a delegation of trust, e.x:
    - Trusting my login to a .rhosts file
    - Trusting my password to an SSH client
    - Trusting my credit card # to Amazon.com
  - By extension, the more convenient the system is, the more trust I am placing in it to act automatically on my behalf

The actual explanation of WHY convenience is contrary to security!

Ergo: transitive trust

4

- Complexity and Security are opposed
  - “Complexity” is a property of implementation ***as well as*** trust relationships, e.x:
    - Subroutines in code trust eachother
    - Computer A trusts that firewall B will protect it
  - The more complex an implementation is, the less trustworthy it will be, because of trustworthiness erosion due to transitive trust

5

- Positive action is more trust-efficient than Negative action
  - “Positive action” is enumerating what you trust
  - “Negative action” is enumerating what you do not trust
  - By extension, default deny really *is* more effective than default permit *when you can do it*

I.e.: you don’t have to get as much right for it to work

Ok…

- That’s as far as I can get
- Why?
  - To go further we need to begin quantifying things!
    - We need ways to measure (demographically or otherwise!) the effectiveness of different techniques so that we can ‘fiddle the knobs’ and see if metrics have predictive power

But…

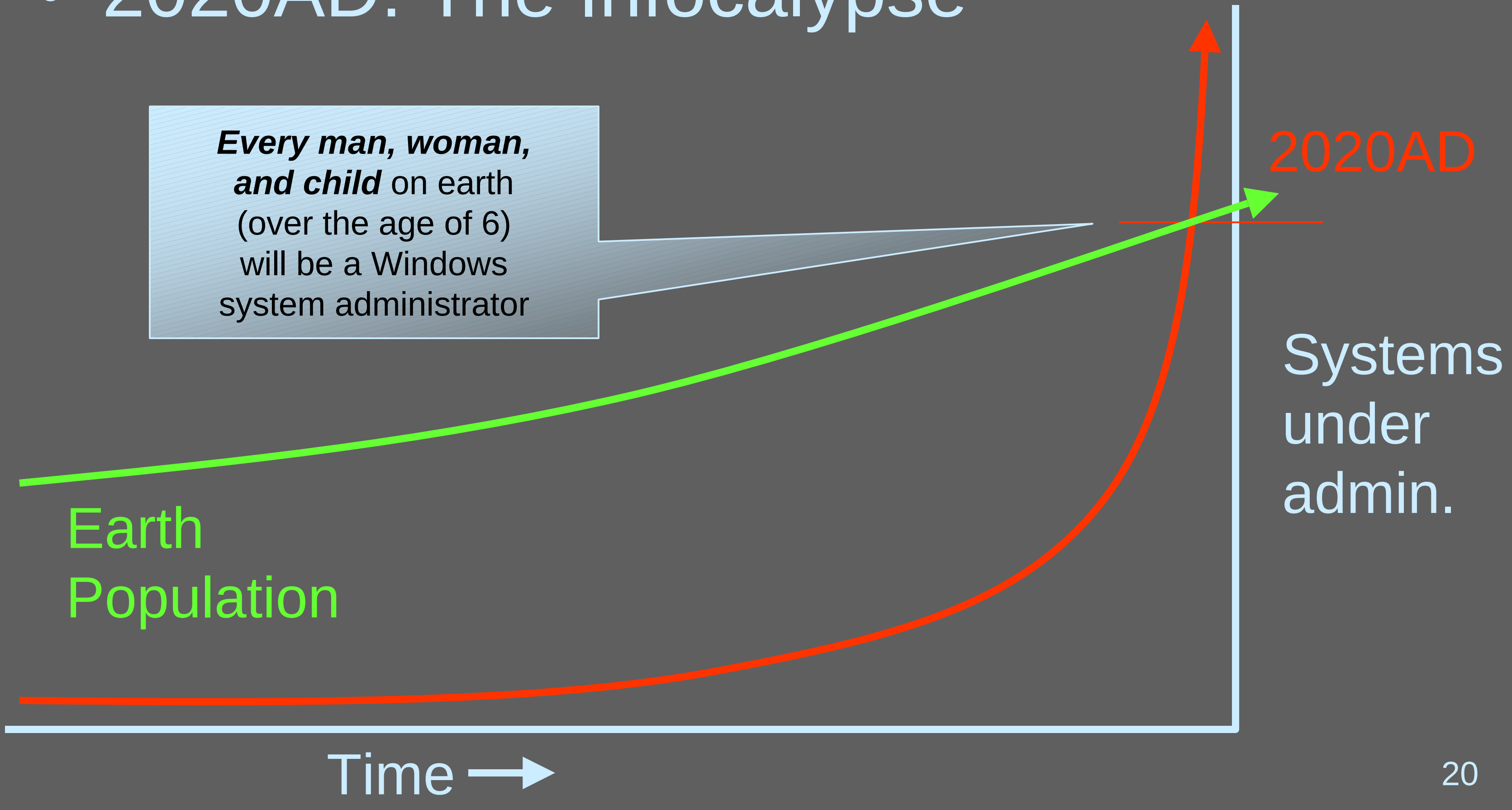
- I think you’ll find that if someone is offering you a “security solution” that appears to violate one of the first 5 laws then they are ignorant, or a charlatan, or both

It’s a start, anyway

- We have generations of smart young people coming along who are going to have to deal with the increasing complexity of computer networks and software
  - For whom trustworthiness and trust will become increasingly significant social problems!
  - Take this seriously - or else...

Windows Sys Administration

- 2020AD: The Infocalypse



Every man, woman, and child on earth (over the age of 6) will be a Windows system administrator

Summary

- We are past the early stage of computer security
  - We've graduated from being 100% B.S. to being about 50% B.S.
    - Unfortunately the dynamics of the market make it such that the B.S. is where the $$$ is
    - This does not serve the customer