Towards Evidence-Based Security

Adam Shostack
ShmooCon '05

Slides at
http://www.homeport.org/~adam/shmoocon/

Speakers

- Crispin Cowan
- Al Potter
- Ed Reed
- Adam Shostack

Outline

- Adam's 10 minutes
  - What is Evidence Based Security
    - Why we need it
  - What EB Security is Not
  - What We Need to Make EB a reality
- Crispin, Ed, Al
- You All

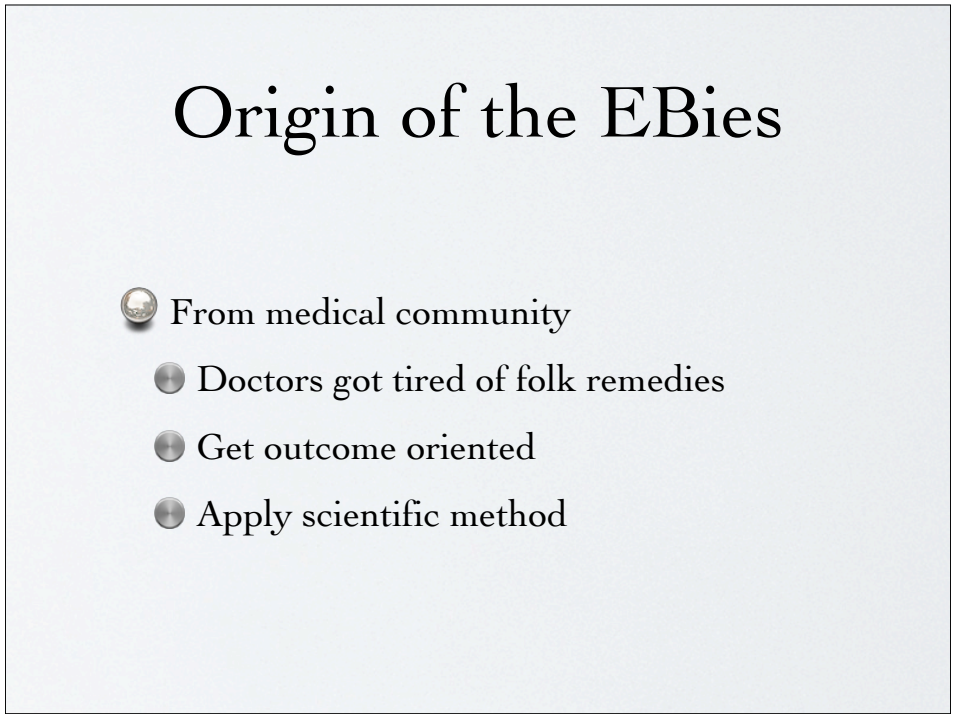
Are We Successful?

- Morris Worm used buffer overflows, bad passwords, and sendmail to spread in 1989
  - 16 years later, sendmail is fixed
- Worms, phishing, spyware
- Social engineering
- Litany of problems gets no shorter

Linux not a panacea
More types of attacks
Attacks that 0wn systems growing faster than clue
Attacks always get better
No rational security expert is optimistic

Origin of EB

- A desire to do better
- Question why we're not
- Apply scientific method:
  - Testable hypotheses
  - Occam's Razor



Rescorla origin of term
Microsoft use in .NET

Some doctors wanted proof and evidence; todays methods don't work. Use large meta-studies and look at huge populations

Scientific method here means Popperism: Good hypothesis withstand tests

What Is EB?

- Hypothesize, **test**, repeat
- Look to real world
  - Normalize for deployment?
- Smaller and larger tests
  - Deployed systems survivability time?
  - Does this system survive this attack?

Analogy to safes, TL-15, TL-60, F-30

We explicitly blame the designer: systems are deployed in the real world, not a lab. Ease of administration matters. Why Johnny can't encrypt. Your grandmother has to remove spyware.

Why do we hypothesize, test and repeat?

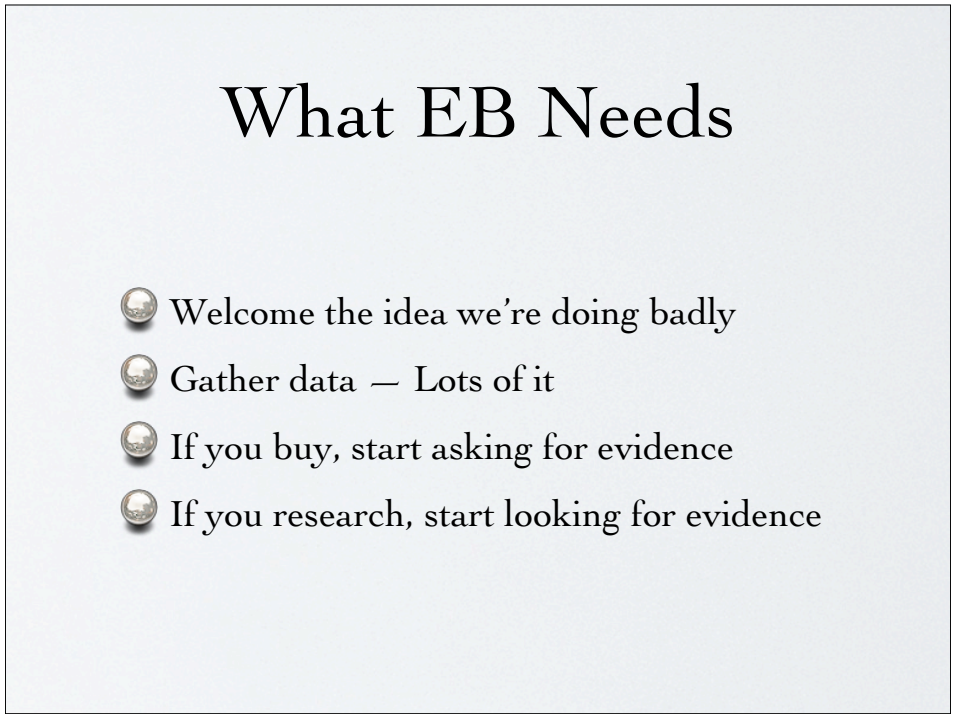
Survivability time, not survivability average: Variance matters. Mean & median matter

What EB Is Not

- Process Oriented
  - Stacks of paper don't defend systems
  - Al & Crispin to cover?
- Proof Oriented
  - Computers are **not** mathematical systems
  - Proofs rarely relate to real world security

OpenBSD vs X
Evaluating stacks of paper too hard. CC & such standards require bizzare language

Turing's halting problem.
Mathematicians like proofs, but "provably secure" cryptosystems get attacked through some other angle.
Cryptographers in fact rely on experiment, from Deep Crack to the sha1 demos last summer at crypto



9

Welcome the idea of making mistakes, because otherwise we can't expect to embrace what we need to do better
"Hello, my name is Adam, and I'm a security practitioner, this is my first meeting, and some friends suggested that I should come here."

We all agree know that defense is harder than offense. Naturally, people get broken into. It's common. Let's stop trying to hide it, and talk about it.

if you research, sit on a program comittee, organize workshops, etc.