THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

A Science of Security? An Empirical Perspective

Mike Reiter

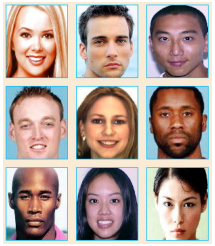
Empiricism in Computer Security

- A substantial — and growing — amount of research in computer security is empirical in nature
  - This is the "natural" part of the science, as opposed to the "formal" side of it
- Certainly this applies to systems-building, but I'm willing ***for the purposes of this panel*** to relegate that to "engineering"
- Still, several areas of research fall into this category
  - Usability (and anything else involving a human)
  - Internet "sociology"
- A "science of security" that ignores this part of the field is incomplete at best, and risks doing a disservice for the field

Example:

Graphical Passwords

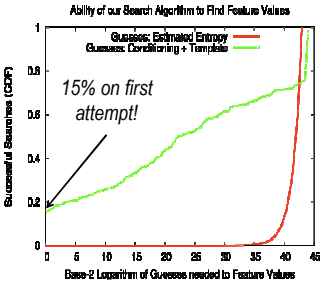
- Graphical passwords enable a user to authenticate to a system by interacting with a graphical interface
  - Intended to overcome shortcomings of text passwords
- Davis et al. [USENIX 2004] showed that passwords like this one suffer from enrollment bias based on attractiveness and race
  - 10% of male's passwords guessed in two attempts
  - 10% of Asian's passwords guessed in six tries if gender is known
- Thorpe et al. [USENIX 2004, 2007] have shown weaknesses in graphical passwords of our own design



Example:

Biometric Key Generators

- Biometric key generators enable the recovery of a strong cryptographic key from user's biometric measurements
  - Must defend against compromise even of the biometric template
- Ballard et al. [USENIX 2008] analyzed a proposal of Vielhauer and Steinmetz using real biometric data
- Results: huge disconnect between projected and actual security
  - Projections didn't account for public data
  - Projections artificially inflated by methodology

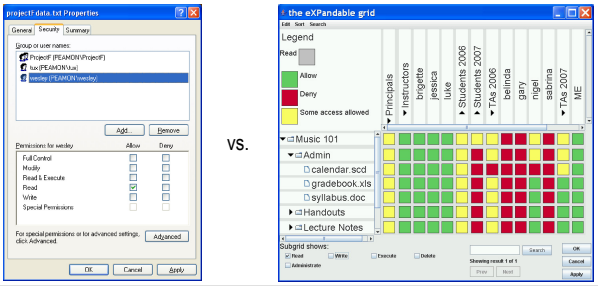


Copyright © 2008 by Michael Reiter
All rights reserved.

Example:

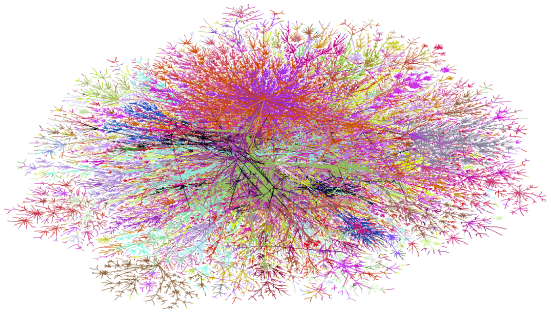
Access-Control Policy Authoring

- Policy authors create, edit and view rules that determine the conditions under which access is allowed to a resource
- Reeder et al. [CHI 2008] have shown that existing list-of-rules interfaces can be improved by showing *effective* policy



Internet "Sociology"

- Just because we built computers doesn't mean that we understand them



Example:

Attacker and Victim Behavior on the Internet

- **Cheating or free-riding in peer-to-peer systems**
  - Aber & Huberman. Free riding on Gnutella. *First Monday*, 2000.
  - Lian et al. An empirical study of collusion behavior in the Maze P2P file-sharing system. *ICDCS* 2007.
- **Behavior of spammers and spammees (i.e., the rest of us)**
  - Ramachandran and Feamster. Understanding the network-level behavior of spammers. *SIGCOMM* 2006.
  - Kanich et al. Spamalytics: An empirical analysis of spam marketing conversion. *CCS* 2008.

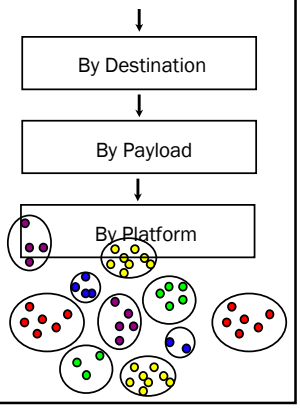
Example:

Traffic Aggregation for Malware Detection

Filter traffic to find hosts that …

- **… contact sites uncommon to benign hosts …**
- **… use similar payloads …**
- **… and that share similar platforms.**

What is left warrants further investigation as likely malware traffic [DIMVA 2008].



Copyright © 2008 by Michael Reiter
All rights reserved.

A "Science of Security"?

- **Is there *A* science of …**
  - … war? … law enforcement? …
  - … biology? … psychology? …
- **Why might we think that there is no such overarching science?**

1. **Security is not an isolated property …**
   - We don't have systems so they will be secure, but rather we build systems so they DO something
   - What it's doing often changes what "security" means
2. **Such a science would necessarily (?) presume a knowledge of all possible classes of attacks**
   - Attackers have proven remarkably agile

My First Wish for a "Science of Security"

- **Provide a way of proving that a specific change to a system makes it …**
  - More secure in some sense
  - No less secure in every other sense
- **Why is this hard?**
  - We haven't figured out how to anticipate all the attacks that can be brought against a system
  - Paying attention only to the attack we think we're fixing doesn't suffice
  - Humans mess things up

Copyright © 2008 by Michael Reiter
All rights reserved.