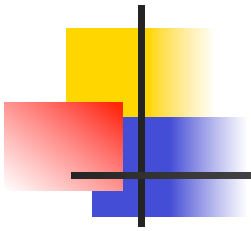
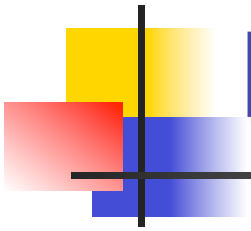


My Password is: #FullOfFail!

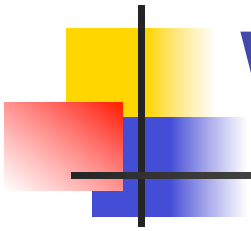
The core problem with authentication and how we can overcome it

Jason M. Pittman



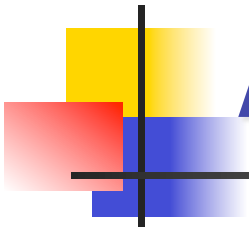
Parental Advisory

- We’re goin’ deep, son!
- Deep philosophically that is…
- Tools, who needs ‘em
- 8.75 of 10 zombies do recommend brains anyway…



What are we talking about?

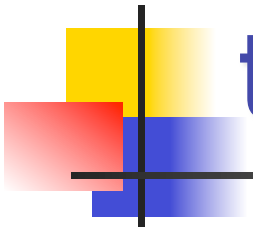
- Modern (current) authentication
  - Passwords specifically
    - Extends to all types however
  - Current authentication research
  - The theoretical flaws
  - Examples



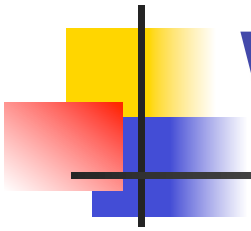
And we'll talk some more…

- Future Authentication
  - One authentication to rule them all
  - Theoretical implementation
  - Examples
- Possible security threats in this future

Why are we talking about this?



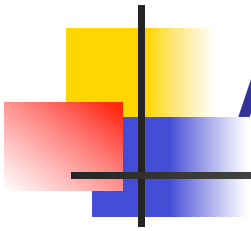
- Research questions:
  - Why is modern authentication full of fail?
  - Why aren't researchers addressing this?
- Research purpose & goals
  - Develop a theoretical approach for future authentication



Why is this important?

- Authentication is ubiquitous
- Authentication is integrated into modern, digital life
- The Singularity may be near…
  - Or it might not and we still need to address the core problem

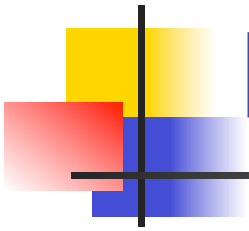
Authentication Today



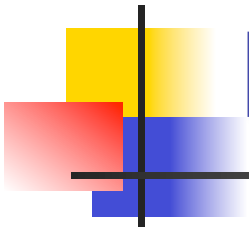
Authentication Primer

- Authentication is:
  - Something you know
  - Something you have
  - Something you are
  - Something + Something
    - And maybe + another Something
- Ask yourself, is there a (a priori) difference between all these?

Password Poster Boy Disclaimer

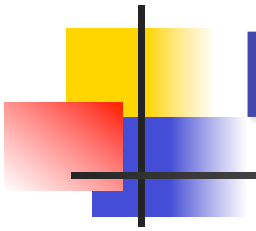


- Passwords are the best example
  - High Usage (user base)
  - High Penetration (most common form of authentication)
  - Easy to conceptualize
- Keep in mind – what we're going to talk about applies to ALL forms of authentication!



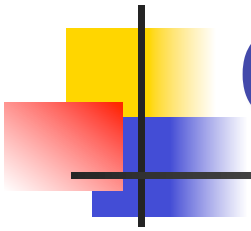
History of passwords

- How long have computing systems relied on authentication, specifically passwords?
  - 1961 – MIT CTSS
  - 1978 – Morris invents crypt(3)



Password Trends

- Two trend defining moments:
  - Transition from single user systems to networked operating systems
  - Explosion of authentication as a consequence of the Web 2.0/Digital era.



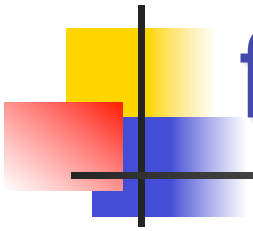
Question for the group…

- How many of us have more than 1 password?
  - More than 3 passwords? Hands?
  - More than 5 passwords? Hands?
  - More than 9 passwords? Hands?

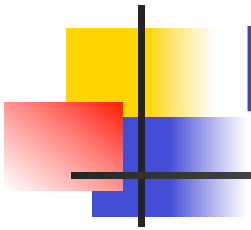
Modern passwords – facts

- SafeNet/Rainbow Technologies Survey (2003) says:
  - 1 -2 passwords 17.7%
  - 3-4 passwords 34.4%
  - 5-6 passwords 18.4%
  - 7-8 passwords 5.6%
  - 8 or more 23.9%

Modern passwords – more facts

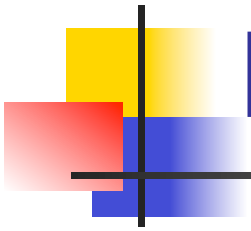


- Florencio & Herley (2007) demonstrated that users type a password ~8 times a day
- The same users retain ~6.5 passwords.
- Each password is shared between 3-4 accounts.



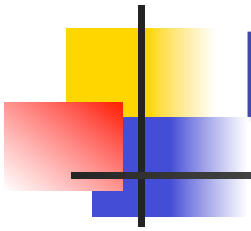
Did you catch that?

- 2003 – 3.5 passwords
- 2007 – 6.5 passwords
- 2011 – ?
- Pittman's Law of Passwords
  - The number of passwords per user will roughly double every four years.



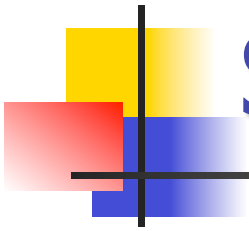
Failtistics 101

- 80% of users want something other than passwords (Infosecurity Europe Survey, April 2004)
- Largest perceived threats are (TriCipher Survey, 27 July 2005):
  - Keyloggers (35%), Password Sharing (26%), and Phishing (12%)



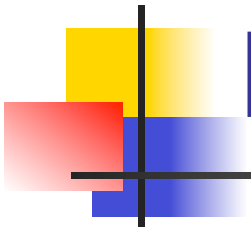
More Failtistics 101

- Over 43% of security breaches related to authentication (Camelot Network Security & Privacy Study, 25 June 2001)
- Approx 60% of attacks related to authentication (The State of IT Security, July 2003)
- Etc…



Signs of the times

- The majority of recent compromises either started from authentication or resulted in disclosure of authentication data
  - HBGary
  - RSA
  - InfraGard
  - Etc.

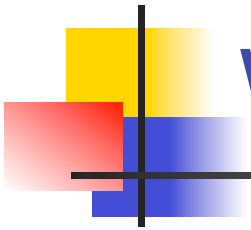


Let's get this straight…

- Passwords are the most prevalent form of authentication
- Passwords are responsible for or related to a majority of security breaches
- Users hate them
- We (researchers and professionals) keep telling users and ourselves to make even more passwords!

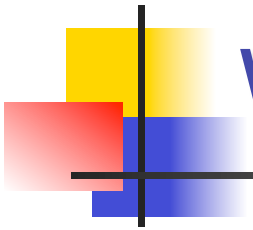
Welcome aboard the…

The Problem



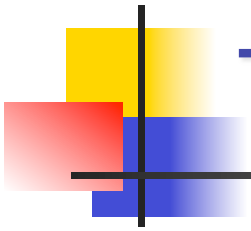
Why is authentication full of fail?

- Current authentication (passwords) are indirect forms of identify assertion
- Software is making the identity assertion on behalf of the user
- The system or application authenticating the user has indirect knowledge of the user's true identity



Worth repeating…

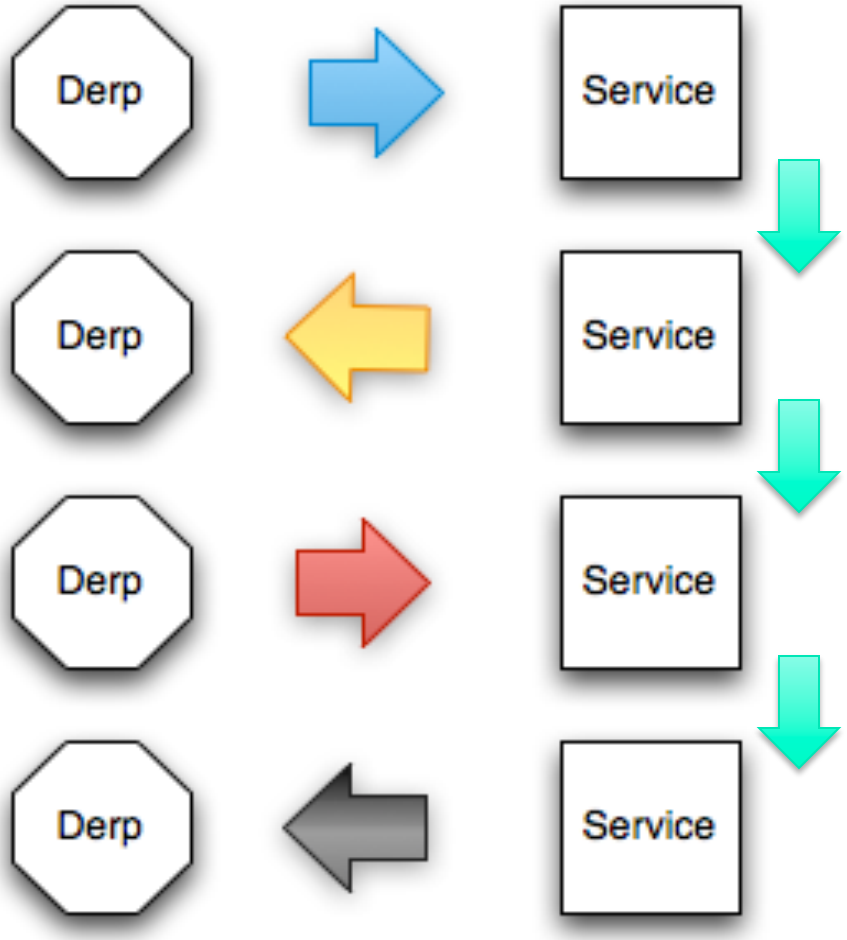
- Modern authentication uses or relies on an indirection assertion of identity



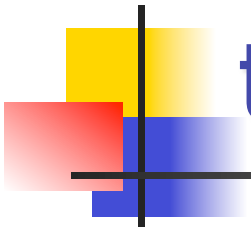
Thought Experiment

- You need to confirm the identity of your partner/friend/parent when:
  - You cannot see them
  - Voice harmonics are normalized
  - You cannot touch them
- What if you're in the middle of two people that need to assert identity?

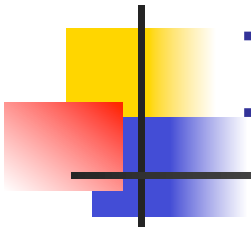
The Current Paradigm – Indirect Assertion Authentication



Are we doing anything about this?



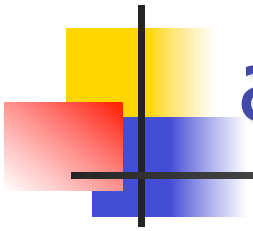
- Cognitive passwords (Allendoerfer &Pai, 2005)
- Proactive passwords (Vu, et al, 2007)
- Visual/Graphical passwords (Renaud& De Angeli, 2009).



Is new research effective?

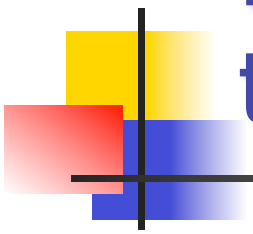
- Just new ways of doing the same thing
- Most/All ease the cognitive burden of authentication
- None address the fundamental flaw in authentication design

Wow – what about other forms of authentication?

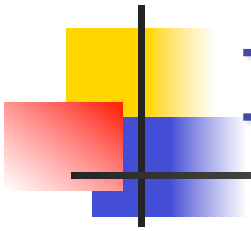


- Pittman's Rule of Authentication:
  - Any authentication that abstracts (biological) identity is full of fail.
- Tokens, PKI, Multifactor, Federated, etc.
  - Yep…
- What about biometrics? Surely I can't be serious?

Biometrics – why I'm not 100% totally wrong…probably

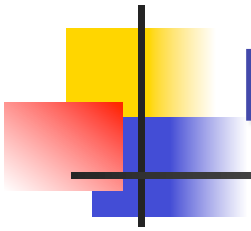


- Fingerprints as an example
  - Is software telling a system *about* your print?
  - Or is your *print* telling a system?



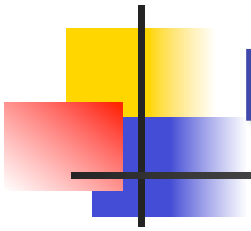
Indirect Assertion Threats

- Threats focus on the software middleman
  - E.g., Keyloggers
- Threats exploit the bad philosophy
  - The software middleman has no capability to control



How did we get here?

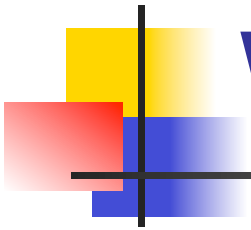
- Authentication was an afterthought
  - The systems came first, then we had authentication
- The essential model has sprawled
  - We keep changing the paint but we haven't thought about a better house
- We blame users, not our philosophy



Do we need to run for the hills?

- The point is to understand the core philosophical flaw
- We don’t want to:
  - Perpetuate authentication sprawl
  - Repeat the mistake when we have a chance to avoid repetition

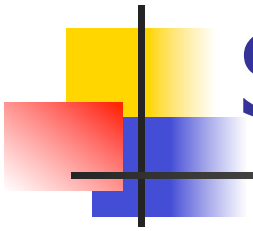
The Future of Authentication



Where do we need to go?

- Start thinking 20, 30, 40 years out, right now.
- Kurzweil (and Vinge!) might be wrong but they're definitely right.
  - That is, we might not have uploaded consciousness
  - We definitely have exponential growth in technology

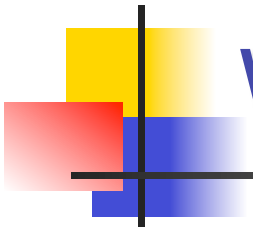
Consequences of the Singularity



- Full Transhumanism
  - How are we going to authenticate (bi-directionally):
    - Immersive Nanotech
    - Our machine “housing”
    - Other’s nanotech & “housing”
    - Sentient machines

Consequences of the Singularity

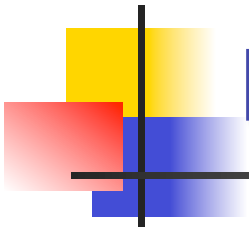
- Partial Transhumanism
  - How are we going to authenticate (bi-directionally):
    - Semi-sentient machines (e.g., the digital analogue for protists or bacteria)
    - Genetically engineered material?
    - Non-immersive nanotech



We need to be Direct

- Direct assertion authentication
  - Remove the middleware
  - Requires direct interface between humans and computing systems/applications

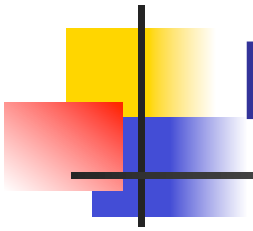
The New Paradigm – Direct Assertion Authentication



How will this work exactly?

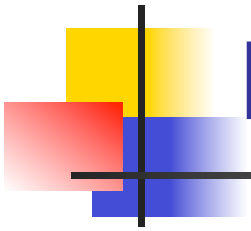
- Let's take a classic shibboleth example
  - WWII – lollapalooza (Stimpson, 1985)
  - Also WWII – "thunder", "lightning"
- Mash-up with biological or bio-physiological "signature"

Direct Assertion Authentication - Examples



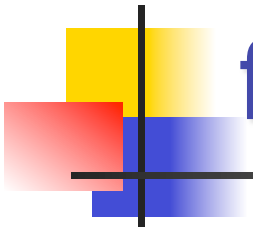
- The Matrix – two forms of direct assertion are observed:
  - Machines authenticated users via direct neural interfacing
    - Key point: access to the Matrix is direct; there is no middleman software
  - Humans (Zion) authenticated the Matrix "visually" across their broadcast uplinks
    - The déjà vu scene

Direct Assertion Authentication - Examples

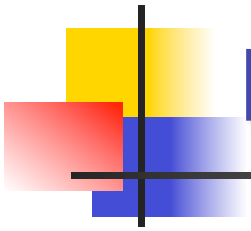


- Surrogates – again, two forms of direct assertion authentication
  - The bio-physiological interface between user and robotic avatar
    - We infer there is no authentication between user and the interface sleds
  - The “visual” authentication between avatars
    - Robots are simulacra of the human operators

Isn't Direct Assertion just science fiction?

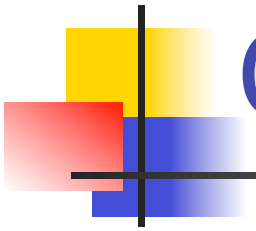


- Short answer: no
- We know how to create the technology
  - Intendix, Emotiv, etc.
- Future research needs to focus on creating systems & applications that accept Direct Assertion



Direct Assertion Threats

- Threats will focus on the point of interface
  - Imagine a type of keylogger that capture bioinformation
- Threats will exploit biological vulnerabilities
  - Art that imitates life (e.g., malware today) will come back to imitate art.



Questions?

- Don’t be shy!
- Email me:
  - jmpittman@capitol-college.edu

References

All surveys available: www.passwordresearch.com/stats/statindex.html

Allendoerfer, K., & Pai, S. (2006). *Human factors considerations for passwords and other user identification techniques part 2: Field study, results and analysis* (DOT/FAA/CT-06/09). Atlantic City International Airport, NJ: Federal Aviation Administration William J. Hughes Technical Center.

Florencio, D., & Herley, C. (2007) *A large-scale study of web password habits*. In *Proceedings of the 16th international conference on the World Wide Web*. 657-666.

Karen, R., & De Angeli, D. (2009). Visual passwords: cure-all or snake-oil? *Commun. ACM 52* (12): 135-140.

Stimpson, G. (1985). *Book about a thousand things.* Century Bookbindery.

Vu, K., Proctor, R., Bhargav-Spantzel, A., Tai, B., Cook, J., & Schultz, E. E. (2007). Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies,* 65. 744–757.