

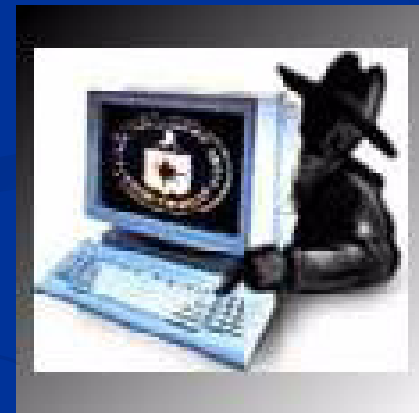


More of What Hackers Don't Want You to Know

Jeff Crume, CISSP-ISSAP
Executive IT Security Architect
IBM Corp.
crume@us.ibm.com
<http://extranet.lotus.com/crume>

Intro

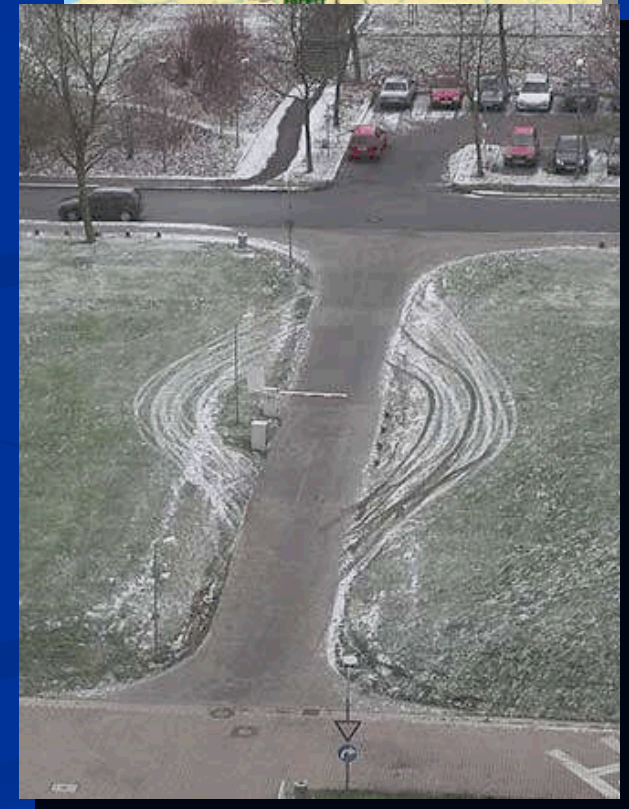
- What hackers don't want you to know ...
 - A discussion of things the bad guys know that the good guys either
 - Don't know or ignore
 - Either way, the effect is the same



- Time constraints limit this to primarily a discussion of the *problems* but *solutions* do exist

... More technology \neq more security

- Myth: My system is secure because it has _____ technology.
- Maginot Line
 - the “Great Wall of France”
 - “If you entrench yourself behind strong fortifications, you compel the enemy to seek a solution elsewhere.”
-- Carl von Clausewitz
- People are the weakest link
 - (see next slide)



... Phishing defenses aren't working

- Study by Harvard and MIT researchers found:*
- 100% ignored the absence of HTTPS
- 97% ignored the absence of site-authn image
- 53% ignored invalid cert msg from browser
- What's really broken here?
 - The technology or the user?
- Man-in-the-middle phishing compounds the problem
 - gives the illusion that everything is working



* "Study: Users ignore bank security features", *ComputerWorld*, Feb 5, 2007

... Passwords don't work

- #1 call to most help desks
- 2 out of 3 Web users use < 5 passwords for all access to electronic information*
 - 15% use a single password
- 71% of people at Victoria Station (London) station gave out passwords for an Easter egg**

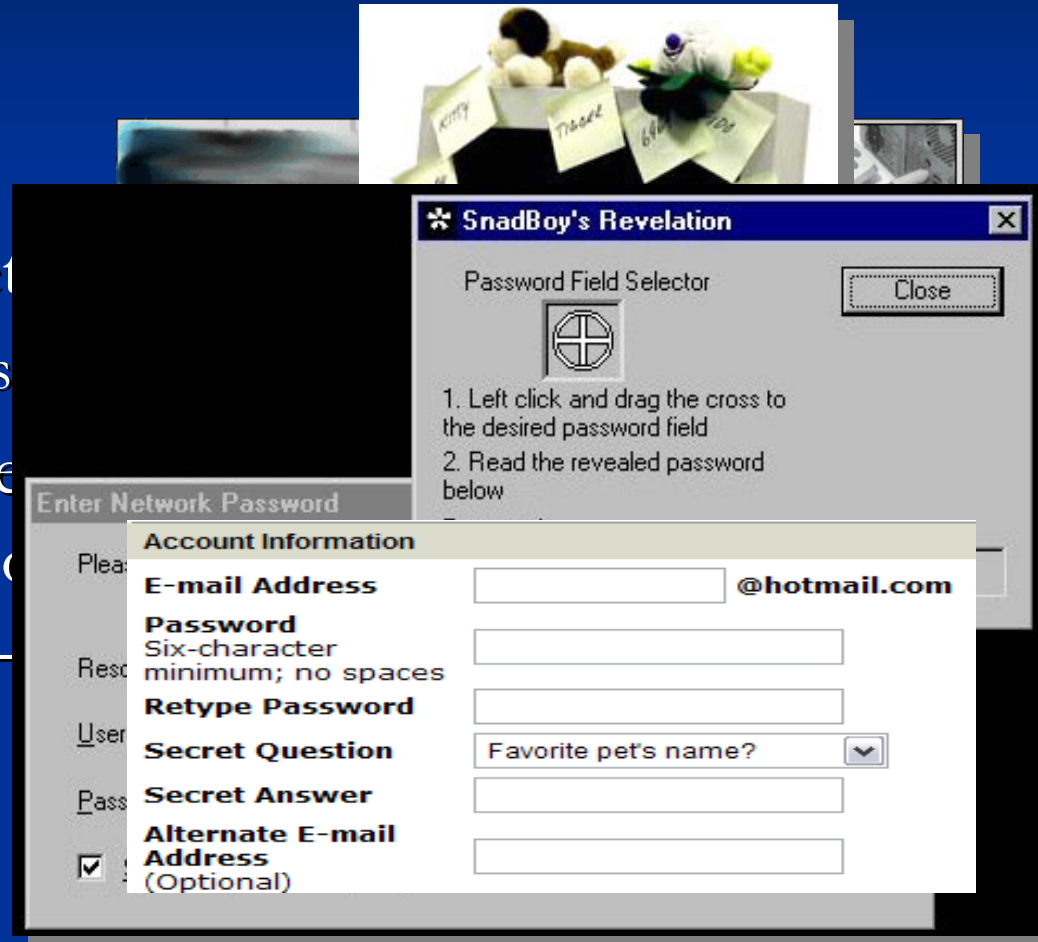


*"Security fears daunt online shoppers," Dawn Kawamoto, CNET News.com, 14 Feb 2005.

**"Password protection no match for Easter egg lovers," searchSecurity.com, 20 April 2004
© IBM Corp. 2008

... Passwords don't work

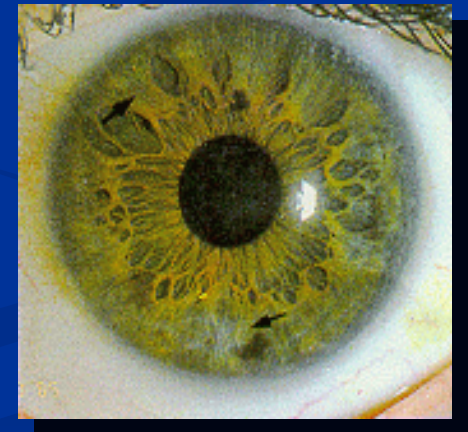
- “PC sunflower”
- Keystroke loggers
- “Hidden passwords”
- The Myth of the “secret question”
 - Typically *easier* to guess
- “Passwords have reached the end of their useful life. Today, they are obsolete for most security applications.” —



*** “The Curse of the Secret Question,” *ComputerWorld*, 9 Feb 2005

... Biometrics are broken

- Myth: Biometrics are far more secure.
 - 69% of US citizens want banks, credit cards, health care and govt to use biometrics*
- Be careful what you ask for ...
 - false positives, false negatives
 - man-in-the-middle attacks
 - replay attacks
 - expensive technology



* Ponemon Institute as reported by Information Week, Feb 6, 2007

Gummy Fingers

<http://cryptome.org/gummy.htm>

Home > OS, Software & Networking > Security >




May 23, 2002

"Gummy Fingers" Fool Fingerprint Readers

... and you can eat the evidence!

By Brett Glass

 [Discuss this now \(19 posts\)](#)

A Japanese mathematician and amateur scientist reports that he has been able to fool fingerprint recognition devices by molding a "gummy" replica of a human finger.

Tsutomu Matsumoto, who teaches mathematics at Japan's Yokohama National University, has demonstrated how to make a mold from a human finger (which can be used to store modeling compounds or with molding material to make impressions for dentures) and fills it with gelatin to make "Gummy Fingers". These gummy phony fingertip that's good enough to trigger virtually any sophisticated biometric devices. ("Gummies" are usually take the form of bears and worms in the United States, but in Japan they are usually lozenge-shaped candies -- often with uncannily accurate fingerprints.) They're commonly made either from gelatin or a soluble fiber derived from kelp.)

Solid gelatin sheet
"GELATINE LEAF"
by MARUHA CORP

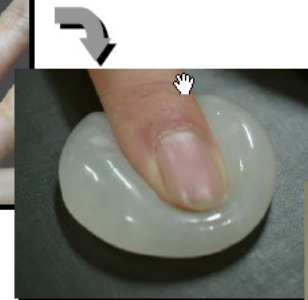


Making an Artificial Finger **directly** from a Live Finger

How to make a mold



Put the plastic into hot water to soften it.



Press a live finger against it.

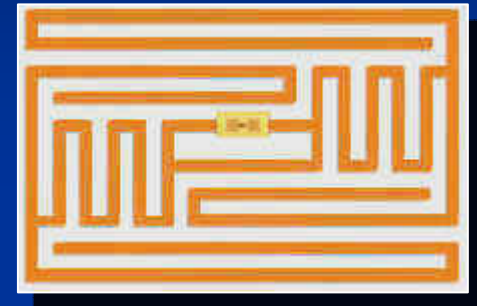


The mold

It takes around 10 minutes.

... RFID means I can see you but you can't see me

- RFID tags wireless transmit data
 - Wireless eavesdropping
 - Wireless impersonation
 - ... at a safe distance
- 1997 ExxonMobile SpeedPass
 - RFID key fob to pay for gas at the pump
 - 3 grad students impersonated the system and filled up for free
- UMass professor skimmed credit card numbers, exp. dates, names
 - Never physically possessed the card
 - Reader built for \$150 using off-the-shelf components



... Bluetooth is a hacker's best friend

- Pervasive technology
 - Mobile phones, PDAs, laptops, etc.
 - All of which hold more and more sensitive info
- Many bluetooth devices remain in discoverable mode
- “Colorful” names for various attacks:
 - Bluejacking, Bluesnarfing
 - Bluebugging, Blueprinting
- Bluesniper Rifle
 - Range > 1 mile



... Web 2.0 = Hack 2.0

- Web 2.0 called “participatory Web”
 - Wikis, Blogs, Mash-ups, Tagging, Social Networking
- Heavy reliance upon client-side scripting
 - AJAX, JavaScript, etc.
 - Long history of overlooked security vulnerabilities
 - Code is automatically downloaded and run on your system without your knowledge or permission by merely visiting a Web site
 - Mashups can lead to man-in-the-middle attacks
- Examples:
 - MySpace password stealing worm
 - Samy: MySpace worm which automatically added the author to visitor’s profiles
 - giving the illusion that he was the most popular person on the site



Other Web 2.0 risks

- Information leaks
 - Confidential information may be inferred from examining your activities
 - Even more info may be gleaned if taken for an entire dept in aggregate
 - Remember: not all the bad guys are “out there”
- Attacks on information
 - Wikiality Colbert attack
 - “A reality where, if enough of the right people agree, it becomes the truth.”
 - If trusted sources are compromised then who can you trust?
- Conclusion: Web 2.0 represents a new minefield of security vulnerabilities



Concluding Thought

"It ain't so much the things you don't know that get you in trouble. It's the things you know that just ain't so."

-- Artimus Ward, 1834-1867