Authentication: Cautionary Tales



Rick Smith, Ph.D., CISSP rick@cryptosmith.com http://www.cryptosmith.com/ July 2003

R. Smith - Authentication

July 2003



The Authentication factors

- Something you Know, Have, Are
- Passwords, Tokens, Biometrics

Attacking Today's Passwords

- Especially credit cards, SSNs, etc.
- Attacking Today's Tokens
 - Especially satellite TV cards
- Attacking Today's Biometrics
 - Especially at the airport



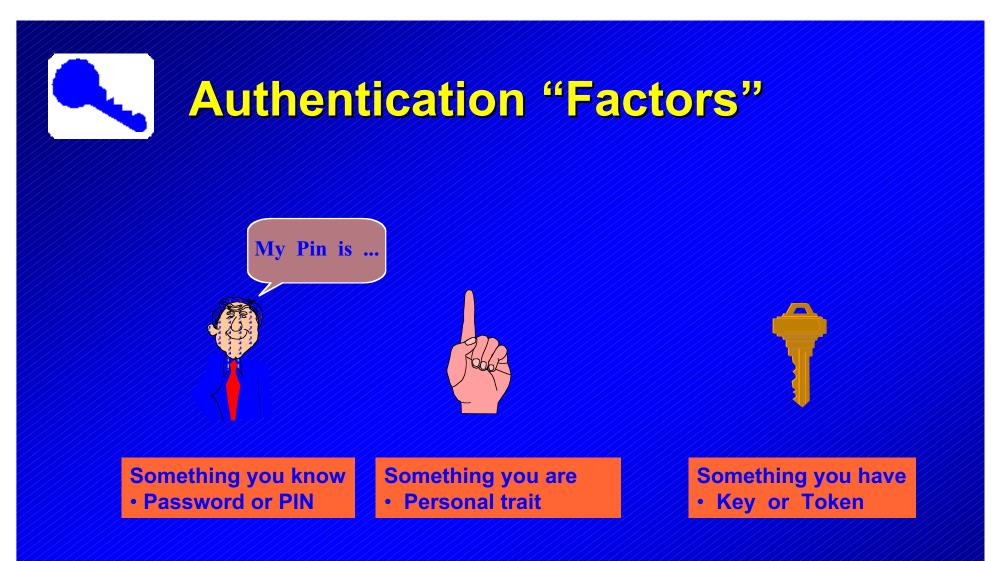
Authentication



Cover art from *Authentication: From Passwords to Public Keys* by Richard E. Smith © 2002, Addison Wesley. Illustration by Peter Steiner, The Cartoon Bank. Used by permission.

"On the Internet, no one knows you're a dog."

July 2003



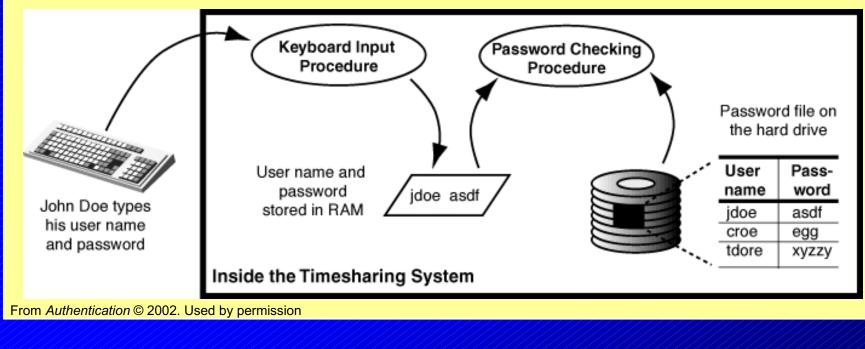
Traditional parallel terms: Something you know, are, have

July 2003

The Password Tradition

Passwords: the essence of computer authentication:

Verifies the ownership of a personal secret



July 2003

Today's Passwords

- Sometimes they're really a personally chosen secret
 - The perfect password:
 Impossible to Remember and Never Written Down

Today we often just use personal information

- Name, or contraction of your name
- Phone number or extension
- Social security number
- Credit card number
- Mother's maiden name
- Birth date

Attacking Today's Passwords

- Database Theft
- Phishing: Intercepting through Trickery
- Sniffing
- Making it Too Easy
 - Passwords in Plaintext
 - Obvious Passwords
 - Tax ID as Password

Database Intrusion and Theft

59,000 records at the University of Texas

- SSNs of current and former students and employees
- Reported in Austin American-Statesman, March 6, 2003

5,000,000 Visa card accounts accessed

- Reported by Reuters, February 18, 2003
- 500,000 medical records for military personnel
 - Hard drives physically stolen from health care organization
 - Reported by Associated Press, January 2, 2003
- 30,000 entries from Experian credit bureau
- 52,000 passwords at University of Oslo
 - Snuck through unpatched MS SQL software
 - Reported in RISKS, December 1, 2002

July 2003

Phishing: Web Site Trickery

Typical Scenario

 Person receives an e-mail directing them to check their account and giving them a link to a bogus, but plausible-looking, web site

Discover Card – bogus account status message

- "Your account is inactive. To reactivate it, visit this site"
- Site collects SSN, mother's maiden name, account numbers...
- Reported in Computerworld, April '03

Network Solutions – domain name renewals

 Reported to customers that bogus renewal e-mails have been sent that direct payment to a bogus Web site

Reported in RISKS, April 23, 2003

BestBuy.com – a "fraud alert"

 Pretending concern about a BestBuy on-line purchase and possible fraud, the e-mail directs users to a bogus Web site to enter account numbers and SSN

Reported in NY Times, June 21, 2003

July 2003

eBay and PayPal Phishing

- "Paypal Alert" classic Web site trickery
 - E-mail exhorts "Visit this site to update update your billing information"
 - Reported in RISKS, Dec 13, 2002 and June 25, 2003
- eBayupdates.com more of the same
 - Attempts to collect credit card information from victims
 - Reported by Reuters, December 11, 2002
- Stolen credit card used to set up another bogus eBay web site
 - Woman's stolen card number buys "change-ebay.com"
 - Site prompts for Ebay user name and password
 - Reported in CNET News, November 22, 2002

July 2003



OnlineNIC.com – proxy redirection

- "Our web site is being attacked. Redirect your browser to one of the following proxy servers..."
- Reported in RISKS, March 31, 2003

UK Bank

- Scammers buy a domain containing the bank's name
- Set up a variant of the Nigerian scam with the legitimate-seeming bank web site as a front
- Reported in BBC News, October 8, 2002

Monster.com – bogus employer's background check

- The "background check" is really an identity theft scam
- Bogus companies can look the same as real ones on Monster's site
- Reported by MSNBC, November 4, 2002

Fraud via Creative Synthesis

Consider the following:

- Last year, two men hacked a race track betting system
- Mix this with Web site phishing

The combination yields this e-mail message:

- "I used to write software for NetGaming Casino. They won't pay me what I earned. To get even, I installed a back door. Here's how you can screw them while making lots of money yourself. Just follow this link to NetGaming Casino and play..."
- Reported in RISKS, February 24, 2003
- Include a bit of the Nigerian Scam if the guy offers you money he's already making on it

Recent Password Sniffing

Intercept passwords inside computers

No network sniffing – too much SSL usage

Tokyo Internet Kiosks

- Two men loaded keystroke logging software onto public kiosks
- Transferred ¥16 million (\$141K) from 5 victims' accounts
- Associated Press, March 7, 2003

• Birmingham, England, Internet cafes

- Apparent use of keystroke logging
- Reported in The Register, January 27, 2003

Passwords in Plaintext

Microsoft Passport Registration

- During registration, Passport sends sensitive personal data in the clear, like name, birthday, password, secret question/answer
- Reported in RISKS, March 19, 2003

First USA/Bank One: web site login

- Reported in RISKS, March 6, 2003
- Equifax: User name, password in e-mail
 - Reported in RISKS, January 18, 2003
- eBay: Passwords usually sent in the clear
- Cordless Keyboard input received by neighbor
 - Not really a password incident, but...
 - Reported in Aftenposten, Norway, October 2002

Obvious Passwords

Patriot Media broadband: "rcnrcn" for all users

- Changed all user passwords to "rcnrcn"
- Reported in RISKS, May 23, 2003

Unnamed company: user initials + phone extension

- Originally used complicated passwords for external access
 - Enforced complexity requirements, periodic changes
- Outsourced network administrator changed them to unchangeable, easy-to-guess passwords

Reported in Computerworld, April '03

Sprint DSL Modems: "1234" configuration password

- Reported in Wired News, February '03
- New York Times (last summer)
 - Reassigned Web site passwords to match internal user names



T-Mobile Wireless Hotspots

- Use SSN as passphrase to register at a hotspot
- Reported in RISKS, May 8, 2003

PNC Bank

- All Princeton University on-line accounts use the same identifier – the university's tax ID
- Students managing funds for student organizations use the same ID and thus have access to <u>all</u> University accounts
- Reported in RISKS, March 6, 2003



Something you have that's hard to copy

- Attacker needs to steal it to log on
- I can't tell if someone has sniffed my password, but I can tell immediately if someone has stolen my token

Cracking Today's Tokens

Magnetic Stripes

- Too easy to copy hardware is widely available
- Boston College student copied other students' stripes onto his, charging his campus purchases to their accounts
 - Reported in Boston Globe, February 7, 2003

USB Tokens

- Read internal secrets by probing unprotected pins
 - iKey: unpopulated memory slot gives bus access (retrieve MKEY)
 - eToken: separate EEPROM leads are uncovered (reset internal PIN)
 - see Kingpin, Attacks on and Countermeasures for USB Hardware Token Devices, @Stake research report

Smart Cards – challenging, but the lure of "free" premium TV appeals to many people

Cracking Smart Cards

Examples from the Satellite TV world

- Interception attacks
- Card rewriting
- Reverse engineering
- Insider theft

Some players:

- Satellite programming vendors: DirecTV (DSS), Dish, Sky, Canal Plus, etc
- Satellite TV/smart card developer: NDS
- Gray Market vendors: huproloader.com, dssstuff.ca, [use your search engine]
 - Gray market has withered as law enforcement has clamped down both in Canada and the USA

Countermeasures

"Ping pong" between industry and hackers

Hacker Attacks

- Man-in-middle attack between receiver and card
- Card rewriting/reprogramming through experimentation
- Reverse engineering
- Insider theft of information

Industry defenses

- Anti-reverse-engineering
- Internal secrets and encryption
- Command protocols
- "ECM" messages that cause bogus cards to "loop"

Interception Attacks

 "Interception Boards" insert into the card slot and intercept commands traveling between the satellite receiver and the card. The board modifies commands and responses so that the receiver believes that the card's owner has paid for lots of channels



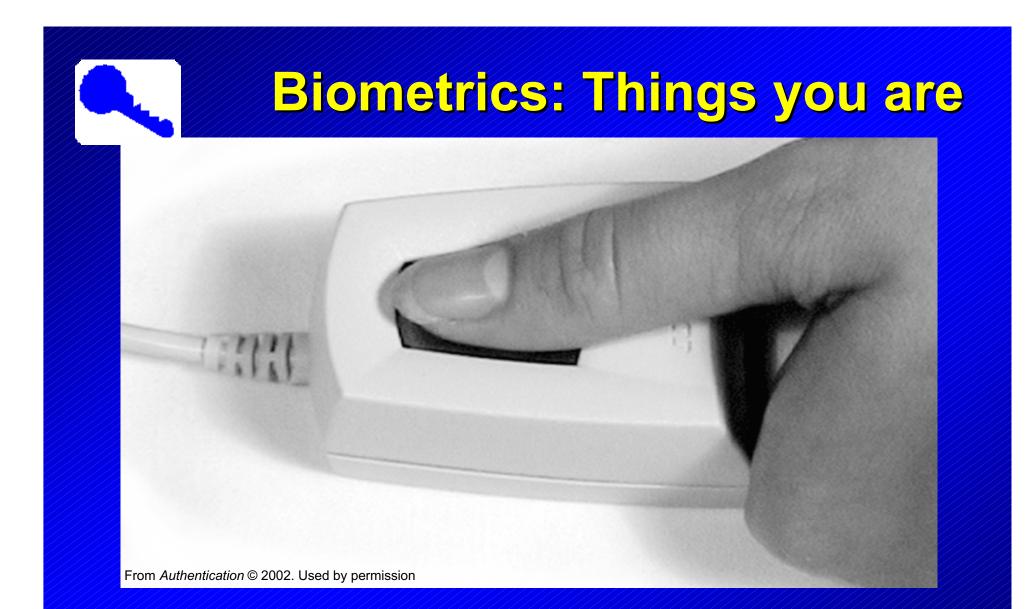
- Card readers/programmers are used to probe the card to retrieve its contents.
- New contents are written to the card so the receiver believes that the card's owner has paid for lots of channels
- Series "H" cards: on-board encryption, plaintext commands
- Series "HU" cards: on-board encryption, encrypted commands
 - Attacks succeed without breaking the encryption

Reverse Engineering

- Use IC reverse engineering technology to reverse engineer a smart card chip
- NDS (satellite TV/smart card security developer) legal problems
 - Sued by Canal Plus, who accused it of reverse-engineering the Canal Plus smart card technology and of posting the results on the Internet
 - DSS joined the suit last year



- Technical details for "P4" the latest DSS card technology - was captured and distributed to the satellite cracking community in late 2002
- Allegedly provided by temporary help at a law firm
- The law firm was representing DSS in its lawsuit against NDS



Measure physical trait: finger, hand, eye, face, ...

July 2003

Cracking Modern Biometrics

The cloning problem

- Face cloning
- Fingerprint cloning
- Iris cloning

Screening Problems

– Can biometrics really identify terrorists in airports?



- Show the camera a photograph or video clip instead of the real face
- Photo and video were taken without the victim's assistance
- Face recognition was fooled

Source: C'T (Germany) "Body Check" by Thalheim, Krissler, and Ziegler http://www.heise.de/ct/english/02/11/114/



 Willis and Lee could trick 4 of 6 sensors tested in 1998 with cloned fingers

• Willis and Lee, "Six Biometric Devices Point The Finger At Security" in Network Computing, 1 June 1998

- Thalheim et al could trick both "capacitive" and "optical" sensors with cloned fingers
 - Products from Siemens, Cherry, Eutron, Verdicom
 - Latent image reactivation only worked on capacitive sensors, not on optical ones

Thalheim, Krissler, and Ziegler, "Body Check," C'T (Germany)
 http://www.heise.de/ct/english/02/11/114/

Matsumoto tested 11 capacitive and optical sensors

- Cloned fingers tricked all of them
- Compaq, Mitsubishi, NEC, Omron, Sony, Fujitsu, Siemens, Secugen, Ethentica

 Tsutomu Matsumoto, ITU-T Workshop on Security, Seoul, May 2002; http://www.itu.int/itudoc/itut/workshop/security/present/s5p4.pdf

July 2003



- Thalheim et al have also successfully spoofed iris authentication using a Panasonic Authenticam
- Placed a printed copy of a human iris in front of an eyeball, with a hole punched out for the pupil.

 Thalheim, Krissler, and Ziegler, "Body Check," C'T (Germany) http://www.heise.de/ct/english/02/11/114/

July 2003



- How effective is face recognition?
- How big is the watch list?
- Given those, is there a prayer of success?

Face Recognition Testing

- Government testing by NIST/DOD team
- Primarily an "off-line" test against a precompiled database of digitized faces
 - 121,589 images of 37,437 people
 - Compute performance and reliability estimates
 - Tested established, "mature" face recognition products
- With "reasonable controlled indoor lighting"...
 - Recognizes a user 90% of the time
 - With a false acceptance rate of 1%
 - As database size increases, recognition rate falls
 - Size 800 = rate 85%; 1600=83%, 37,437 = 73%



The Whole Terrorist List = 13 million names

- Names only, not faces
- Reported in NY Daily News, April 8, 2003

US Government "No Fly" Lists

- Again, Names only
- Actually, there are two lists with over a thousand names
- Name collision problem: innocent "David Nelsons"

640 Million people a year use US airports



- A database of 1,600 "No Fly" faces
 Misses a "No Fly" person on 1 out of 6 visits
- A database of 35,000 "No Fly" faces
 Misses a "No Fly" person on 1 out of 4 visits
- With a 1% False Positive Rate
 6.4 <u>Million</u> people/year incorrectly detained at US airports



- All is not hopeless. Really.
- Just recognize the limits of full automation
- Critical systems have always and will always require multiple layers and cross checks
 - Think nuclear missile launches
 - Think two-signature bank check
 - Think "trust, but verify"

Thank You!



Questions? Comments? My e-mail: rick@cryptosmith.com http://www.cryptosmith.com

July 2003