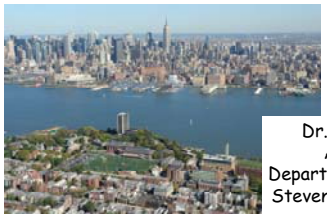
STEVENS Institute of Technology

Privacy and Security
Why should I care?

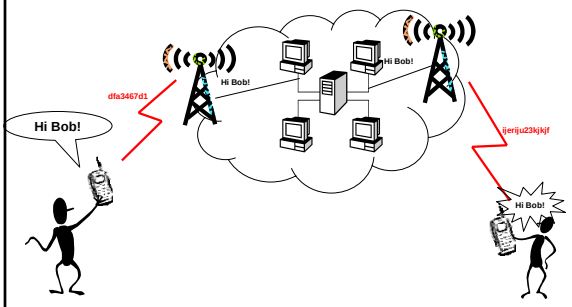


Dr. -Ing. Susanne Wetzel
Associate Professor
Department of Computer Science
Stevens Institute of Technology
Hoboken, NJ, USA

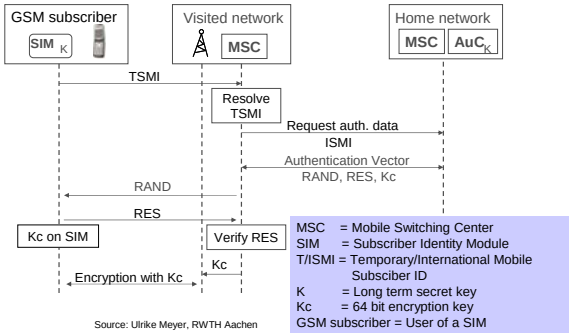
Security as Part of Day-To-Day Activities

- Internet
- Passwords
- Wireless Communication
  - WLAN
  - Bluetooth
  - Cell Phones
- RFID
- Biometrics
  - Passports
- Etc.

Cell Phones

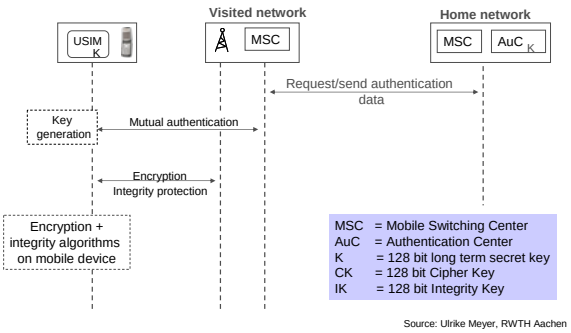


GSM Security



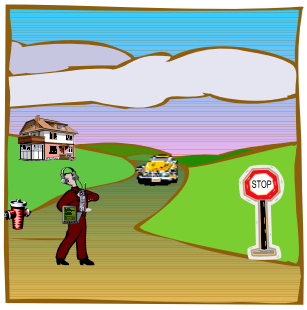
Source: Ulrike Meyer, RWTH Aachen

UMTS Security



Source: Ulrike Meyer, RWTH Aachen

Bluetooth/WLAN



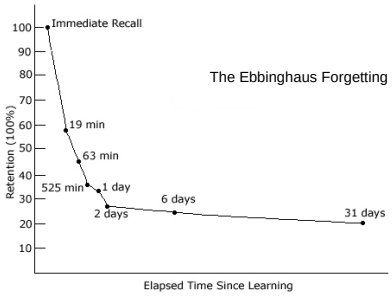
Status

- Bluetooth:
  - Eavesdropping
  - Impersonation
  - Location Privacy
  - Weak Encryption
  - Bluebugging, bluesnarfing, etc.
- WLAN:
  - WEP (Wired Equivalent Privacy)
    - Weak Key Management
    - Problem with Integrity Protection, etc.
  - State-of-the-Art: WPA2 (Wi-Fi Protected Access)

Authentication

- Something you know (e.g., password)
- Something you have (e.g., hardware token)
- Something you are (e.g., biometrics)

Why Password Reset?



Passwords

Hacker impersonated Palin, stole e-mail password

Sep 18 03:25 PM US Eastern
By TED BRIDIS
Associated Press Writer

231 Comments

WASHINGTON (AP) - Details emerged Thursday behind the break-in of Republican vice presidential candidate Sarah Palin's e-mail account, including a first-hand account suggesting it was vulnerable because a hacker was able to impersonate her online to obtain her password.

The hacker guessed that Alaska's governor had met her husband in high school, and knew Palin's date of birth and home Zip code. Using those details, the hacker tricked Yahoo Inc.'s service into assigning a new password, "popcorn," for Palin's e-mail account, according to a chronology of the crime published on the Web site where the hacking was first revealed.

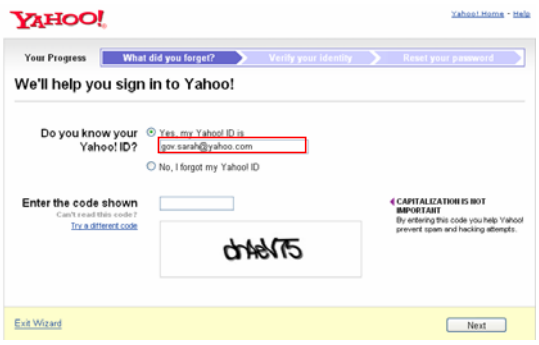
The FBI and Secret Service launched a formal investigation Wednesday. Yahoo declined to comment Thursday on details of the investigation, citing Palin's privacy and the sensitivity of such investigations.

BREITBART TV RELATED VIDEO

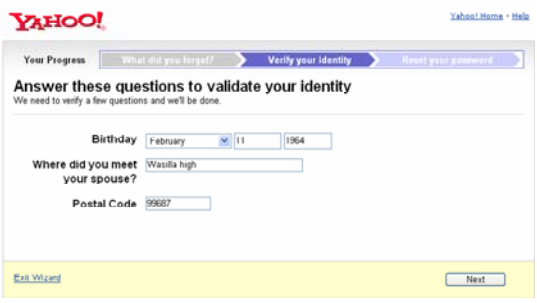
Hackers Break Into Palin's E-Mail Account & Post Messages

http://news.yahoo.com/s/ap/20080918/ap_on_hi_te/palin_hacked

Passwords cont'd



Passwords cont'd



Typical Security Questions

- Make of your first car
- Mother's maiden name
- City of your birth
- Date of birth
- High school you graduated from
- First name of your best friend
- Name of your pet

Some Data Mining…

- Make of your first car?
  - Until 1998, Ford has >25% market share (US market)
- First name of your best friend?
  - 10% of males named James (Jim), John, or Robert (Bob or Rob)
- Name of your first / favorite pet?
  - Top pets names are listed online

Another Problem: Users Forget Answers

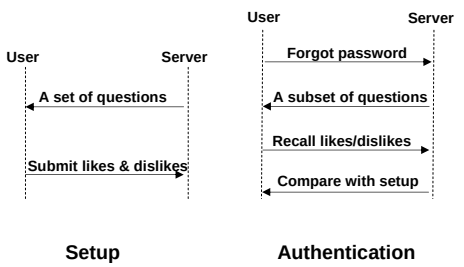
- Name of the street you grew up on?
  - There may have been more than one
- First name of your best friend?
  - Friends change
- City in which you were born?
  - NYC? New York? New York City? Manhattan? The Big Apple?

Intuition

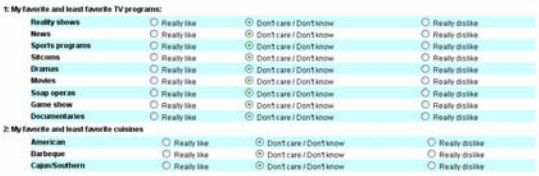
Preference-based Authentication:

- Preferences are more stable than long-term memory (confirmed by psychology research)
- Preferences are rarely documented (in contrast to city of birth, brand of first car, etc.)

Our Approach



Questions and User Interface



Questions chosen from dating websites relating to TV programs, Food, Music, Hobbies, etc.

New Interface: Setup

http://blue-moon-authentication.com/

New Interface: Authentication

Under the Hood

- Small reward for each correct answer
- Large penalty for each incorrect answer
- Comparison to a suitable threshold
- Amounts for reward and penalty depend on the uncertainty of the answers

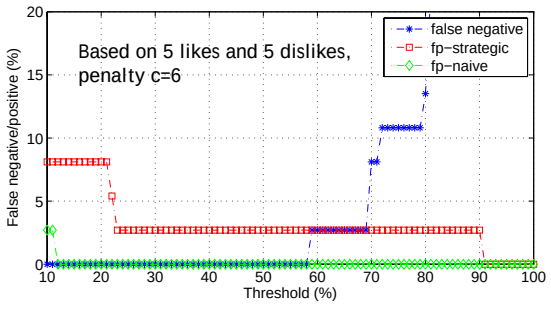
Adversary Model

- Naïve attack
  - The adversary randomly selects likes and dislikes during the authentication
- Strategic attack
  - The adversary knows the distribution of answers (like-rates and dislike-rates)
  - The adversary selects a combination to maximize his success rate

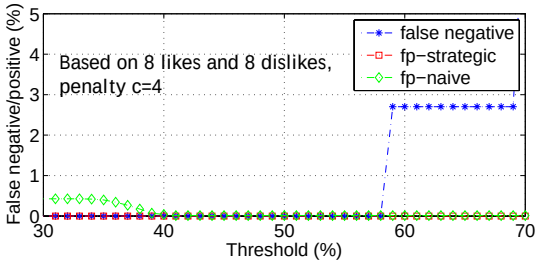
Security / Usability

- False negative / positive error rates
- Requires finding of suitable parameters to balance and minimize error rates
  - Amount of penalty for incorrect answers/amount of reward for correct answer
  - Threshold to pass the authentication

Security: User Study



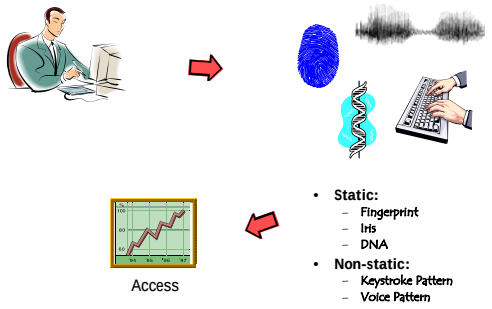
Security: Simulation



Next Steps?

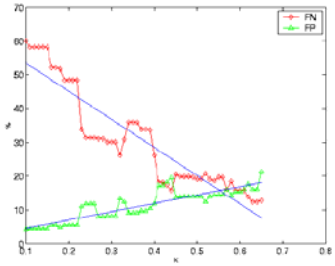
- Additional user studies
- Other attacker models
- Social networks

Biometrics

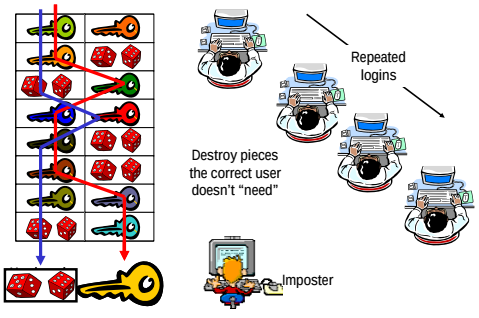


Biometrics: Problem

- "False positive" und "false negative"

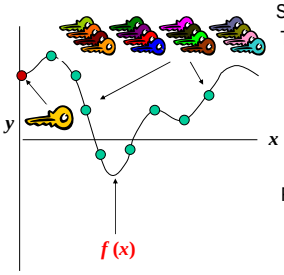


Multi-Factor Authentication



Work by Monrose, Reiter, Wetzel

Shamir's Secret Sharing Scheme



Setup:

To distribute a secret S to m users

- choose random polynomial f of degree $m-1$, such that $f(0) = S$.
- compute shares $S_i = (i, f(i))$ for $i=1,..,m$

Reconstruction:

Any group of m or more users can reconstruct the secret S by Lagrange interpolation.

Initialization

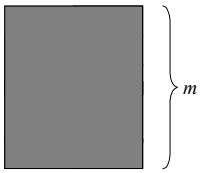
1) User chooses her password pwd

2) Login program chooses random secret hpwd from, e.g., $\mathbf{Z}_q$, where q is a 160-bit prime

3) Generate shares $f(2i\text{-}1)$ and $f(2i)$ for i=1,..., m of hpwd

4) Arrange shares in a m x 2 table

5) Encrypt table with pwd



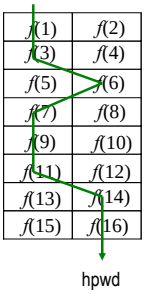
Logging In

1) User enters pwd
   - decrypt instruction table

2) For each φ_i
   - if φ_i measured $< t_i$, use point in left column of i-th row
   - if φ_i measured $> t_i$, use point in right column of i-th row

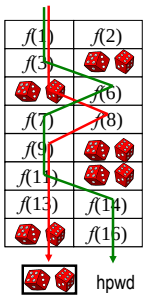
3) Use values to reconstruct hpwd

4) Verify hpwd



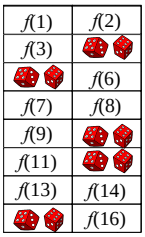
Hardening the Password

- If user reliably repeats φ_i
  - if φ_i usually measures $< t_i$, then perturb right column of i-th row
  - if φ_i usually measures $> t_i$, then perturb left column of i-th row
- Other typing yields wrong reconstruction; online attacker can't log in!
- Correct user still logs in easily



Dictionary Attacks

- Attacker guesses passwords, decrypts table with each
- For each incorrect guess, the resulting table is random
- For the correct guess, the resulting table is the correct one
- Key question: How efficiently can an attacker distinguish these cases?



Alternative Construction: Vector Spaces

Choose $\{\mathbf{v}_i^0, \mathbf{v}_i^1\}_{1\le i\le m} \subset \mathbf{Z}_q^m$ such that

- $\det(\mathbf{v}_1^0, ..., \mathbf{v}_m^0) \bmod q = \text{hpwd}$
- Choose unimodular matrix $U=\Pi U'\Pi^{-1}$ where U' is upper triangular matrix with diagonal entries 1, Π permutation matrix.
- Determine second set of vectors as:

$$(\mathbf{v}_1^1, ..., \mathbf{v}_m^1) = (\mathbf{v}_1^0, ..., \mathbf{v}_m^0) * U \bmod q$$

Approach to Security Analysis

- Represent the choice for value of feature i as function of a Boolean variable:

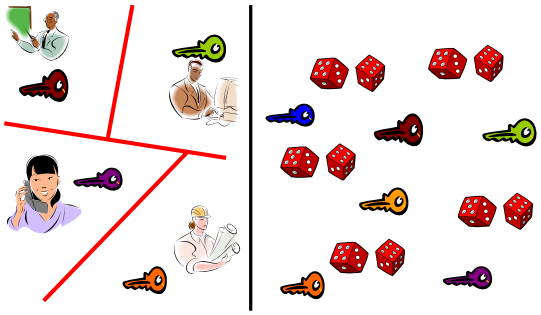
  $\varphi_i(x_i)$ = if x_i then $\mathbf{v}_i^0$ else $\mathbf{v}_i^1$

  Expand determinant computation as Boolean formula.
- Finding zeros of polynomial representing the determinant

$$\det(\mathbf{v}_1^0 - \mathbf{v}_1^1, (1\text{-}x_2)\,\mathbf{v}_2^0 + x_2\,\mathbf{v}_2^1, ..., (1\text{-}x_m)\,\mathbf{v}_m^0 + x_m\,\mathbf{v}_m^1)$$

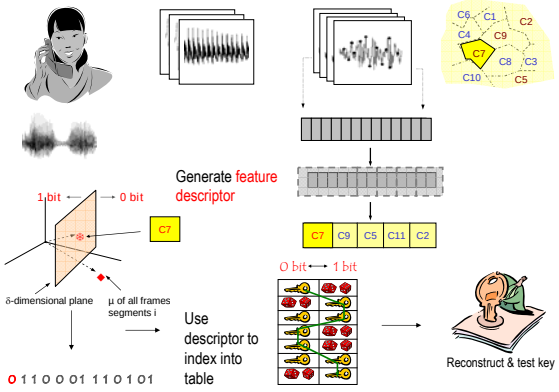
- Connection to quadratic cryptanalysis (security evaluation of AES)

Secret Sharing vs. Secret Locking



Using Other Biometrics: Voice Signal

Work by Monrose, Li, Reiter, Wetzel



RFID I

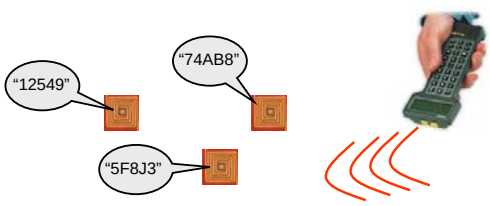
- RFID = **R**adio **F**requency **ID**entification **T**ag
  - → Modern Barcode:

Unique Identification of Product Type

Unique Identification of a Specific Product

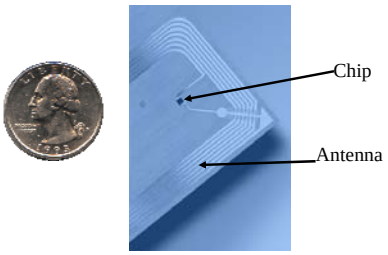
- Can be read "silently" (range of few inches to a few meters)

RFID II



Source:: RSA Security

RFID III



Source: RSA Security

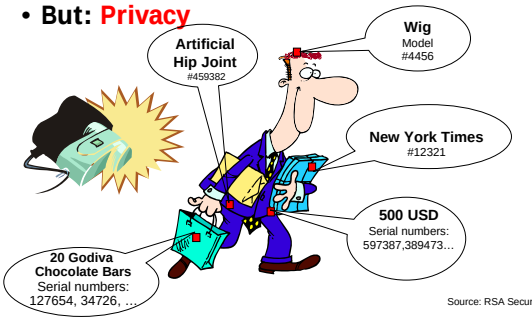
RFID IV

- Applications:
  - WalMart, Metro
  - E-ZPass
  - ExxonMobil Speedpass
  - Etc.
- Advantages:
  - Logistics
  - Unique identification
  - Etc.

Source: RSA Security

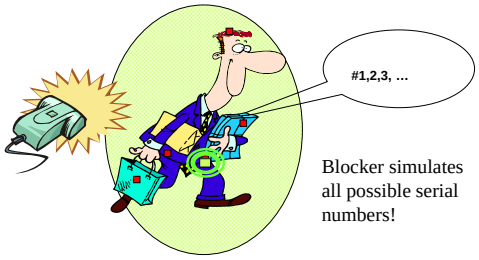
RFID V

- **But: Privacy**



Source: RSA Security

RFID VI: Privacy



Blocker simulates all possible serial numbers!

Source: RSA Security

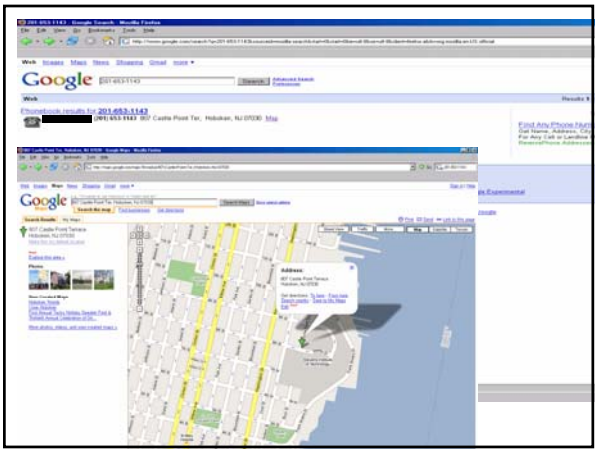
Privacy: Some Food for Thought

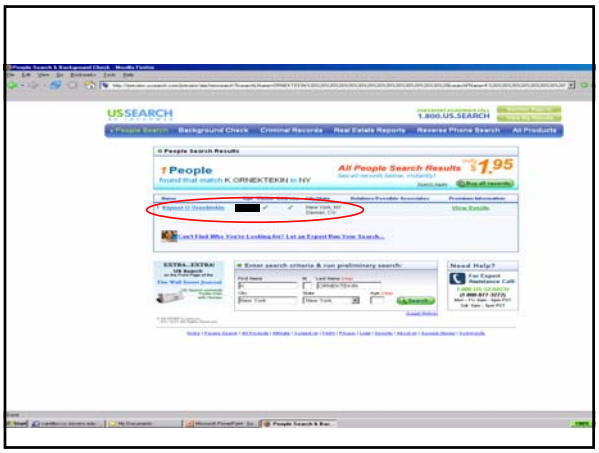
- If asked, do you provide the cashier with your phone number?
- Do you use consumer cards?
- Do you put long lists of email addresses in the to/cc fields?
- Do you use Google services?
- Is your phone number listed?
- Do you do customer surveys and provide personal information?
- What information do you provide on your webpage/on your blog?
- What information do you provide as part of social networks?
- …

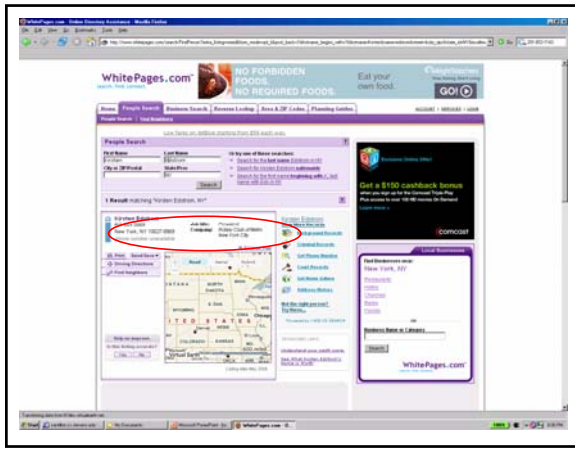
Privacy: Some Food for Thought

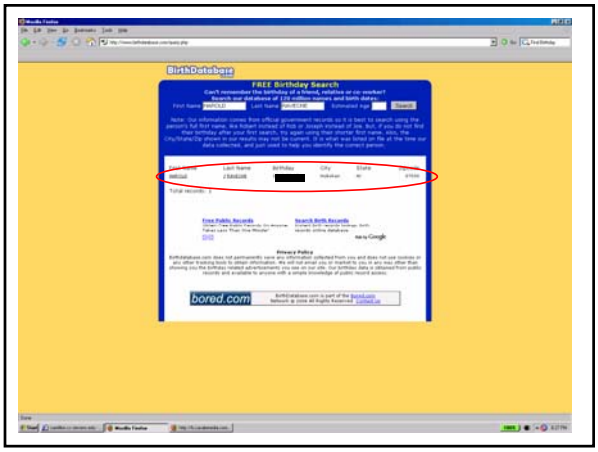
- If asked, do you provide the cashier with your phone number?
- Do you use consumer cards?
- Do you put long lists of email [illegible]he to/cc fields?
- Do you use Goo[illegible]
- Is your p[illegible]
- Do you do[illegible]veys and provide personal informatio[illegible]
- **What information do you provide on your webpage/on your blog??**
- **What information do you provide as part of social networks?**
- …

Data Mining









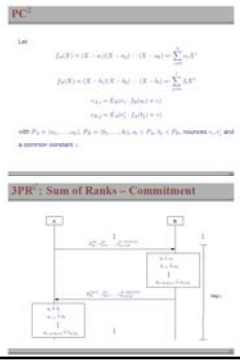
Remember…

- Don't put in an email what you would not put on a postcard!
- Assume that what you post on the Web will be out there once and forever! The Web does NOT forget!
- Think about PRIVACY every time someone requests some personal information from you!

The Fascination of Cybersecurity

Manifold aspects:

- Technology
  - Hardware
  - Software
  - (Mathematical) foundations
- Economy
- Law
- Society
- Politics
- …



Thanks for your Attention!

Questions?