# Passwords for Everyone: Secure *Mnemonic-based* Accessible Authentication

Umut Topkara, Mercan Topkara, Mikhail J. Atallah

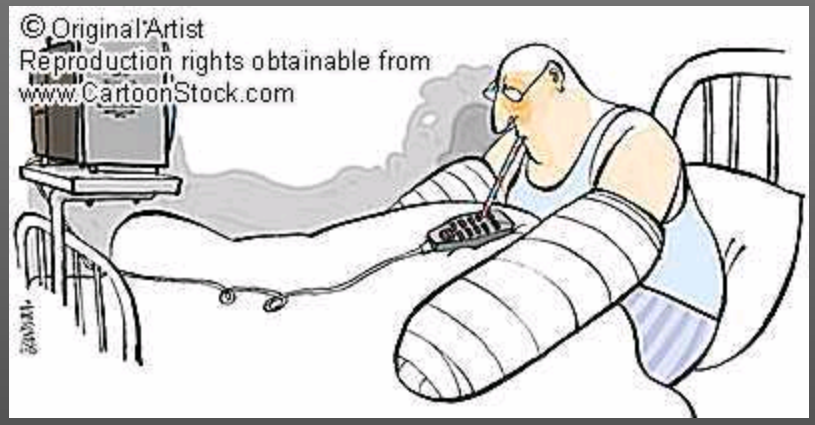
Department of Computer Science
Purdue University

PURDUE UNIVERSITY

CERIAS

# Problem

- Authentication in Input Constrained Environments



# Input Constrained Environments

- **Low bandwidth of user input**
- Motor disabilities
  - Paralyzed patients
  - Broken arm
- Input constrained devices
  - Tiny mobile devices
  - Game consoles
  - Voice sensors
  - Hands-free situations
- Non-private environments
  - Crowded areas
  - Surveillance cameras
  - Tight spaces


# Challenges

- Binary switch input
- Remember random bit string
- No paper/pen/device
- Initialization & reset with binary input
- Dictionary attack
- Replay attack
- Phishing
- Malicious software

# PassWit

- Series of yes/no questions
- Truly random passwords
- Users easily produce a long binary string
- No special device / computation
- Based on text mnemonics
- Compatible with conventional passwords

# Mnemonics

- Help for hard-to-remember information
  - e.g. unrelated sequence of objects
  - **M**y **V**ery **E**ager **M**other **J**ust **S**ewed **U**s **N**ew **P**ajamas
- [Miller 1956, Human Memory And The Storage Of Information]:
  - Semantic association: Associate a meaning
    - e.g., Manhattan, Italy Map
  - Progression of ideas: Connect as a story
    - e.g., May I have a large container of coffee? (3.1415926)
  - Syntactic Coherence: As grammatical as possible
  - Short encoding: Size of the story
    - e.g., 1101 0110 1100 0010 vs 13 6 12 2

# What's wrong with mnemonics?

- Has to be easy to remember:

  *An apple a day sends the doctor away*
- Has to be hard to guess:
  - Avoid common phrases
  - Regularity in language can be a pitfall:
    - **My (dog|cat|pet)'s name is (fido|dusty…) → M(d|c|p)ni?**
    - P(mother) ≠ P(mother | birth)
  - Need **high entropy** word sequences
- Mnemonic fatigue:
  - Hard to come up with new memorable mnemonics

# PassWit Initialization

- User is given a mnemonic sentence
- Truly random

Angry union artists simply dismissed demand to forgive the laziness of the crazy mayor.

# PassWit Initialization

| | leading | U.S. | couturiers | strongly | resist | pressure | regulate | thinness | popular | models |
|---|---|---|---|---|---|---|---|---|---|---|
| 0000 | peaceful | viking | tailor | alarmingly | welcome | attempt | modify | rent | passive | queen |
| 0001 | thoughtful | romanian | cartoonist | hardly | agree | haste | alter | wisdom | inept | leader |
| 0010 | rich | city | beekeeper | suddenly | reject | duress | cement | culture | able | senator |
| 0011 | uninterested | rural | realist | simply | embrace | pressure | manipulate | education | dull | supporter |
| 0100 | provoked | irish | firefighters | warily | resist | demand | secure | diligence | hot | king |
| 0101 | angry | suburban | artists | doubtfully | renounce | bid | fix | weakness | skilled | ally |
| 0110 | outraged | texan | architect | remarkably | submit | call | quantify | salary | adept | foe |
| 0111 | neutral | aussie | police | again | honor | ultimatum | measure | pension | dormant | manager |
| 1000 | furious | canadian | cubist | blindly | recognize | struggle | forgive | thinness | crazy | friend |
| 1001 | poor | union | farmer | suspiciously | allow | operation | change | obedience | gifted | president |
| 1010 | average | british | fantasist | delicately | accept | order | limit | laziness | bright | enemy |
| 1011 | determined | european | developer | fiercely | surrender | imperative | throttle | spirit | witless | children |
| 1100 | strong | downtown | farmer | repeatedly | tolerate | hurry | harness | tenuity | exhausted | associate |
| 1101 | calm | urban | goldsmith | reluctantly | permit | insistence | deregulate | slenderness | talented | mayor |
| 1110 | silent | italian | musician | discreetly | refuse | ban | restrict | citizenship | clumsy | chairman |
| 1111 | ordinary | french | drivers | slowly | dismiss | decree | fiddle | discipline | sharp | assistant |

angry union artists simply dismiss demand forgive laziness crazy mayor

0101 1001 0101 0011 1111 0100 1000 1010 1000 1101

# PassWit Initialization

SPORTS TRAVEL HISTORY CUISINE MUSIC

- Tables populated offline
- Different mnemonic for same password
- Random set of mnemonics shown to user
- $\log_2$(columnSize) bits per word
- Binary string stored as password
- Table ID stored in the salted hash

# PassWit Authentication

- User inputs the login name
- Answers a series of yes/no questions
- "Does your mnemonic contain one of these words?"
- Challenge list has columnSize/2 words

| |
|---|
| peaceful |
| thoughtful |
| rich |
| uninterested |
| provoked |
| angry |
| outraged |
| neutral |

# PassWit Authentication

- Get the login name
- Retrieve the tableID for the user
- For each column in the table
  - Ask $\log_2$(columnSize) questions
  - Similar to 20 Questions Game
- Determine the binary string
- Check if stored hash matches

# Adversary

- May record the responses
  - Ask a different set of questions at each session
- May infer the answer from questions
  - Determine all questions at the beginning

# Group Testing

- Find d defectives in r samples
- Non-adaptive blood test [Dorfman, 1943]

# PassWit Yes/No questions

| | |
|---|---|
| 0000 | leader |
| 0001 | children |
| 0010 | king |
| 0011 | associate |
| 0100 | enemy |
| 0101 | friend |
| 0110 | president |
| 0111 | manager |
| 1000 | Senator |
| 1001 | Mayor |
| 1010 | Queen |
| 1011 | assistant |
| 1100 | foe |
| 1101 | ally |
| 1110 | chairman |
| 1111 | supporter |

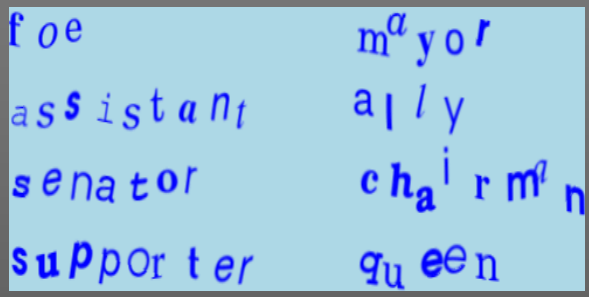
- Different at each session
- Permute the column entries
- Assign *l* bit index to each word
- For each round *i*
  - Display if $i^{th}$ bit of index is 1.

| | |
|---|---|
| senator | foe |
| mayor | ally |
| queen | chairman |
| assistant | supporter |

| | |
|---|---|
| enemy | foe |
| friend | ally |
| president | chairman |
| manager | supporter |

# Against Spyware

- Spyware may record the complete session and send back home
- Need to obfuscate the mnemonic
  - Add bogus entries to the table
  - CAPTCHA in challenges
  - CAPTCHA in answers




If your mnemonic is in the list, tell where the APPLE is, otherwise tell where the STRAWBERRY is.

YES

NO

# Against Phishing

- Mnemonic is a shared secret
- User never asked to enter mnemonic
- Adversary needs to know the tableID
- Otherwise no gain

# Related Work

- Graphical passwords
- Passthoughts [Thorpe et al. 2005]
- Pin-entry with cognitive trapdoor games [Roth et al. 2004]
- PassWit
  - Maps to ASCII passwords
  - Compatible with conventional password systems, input devices, and passwords
  - Uses text mnemonics

# Conclusions & Future Work

- Towards accessible authentication with a binary switch
- Truly random passwords
- Mnemonic-based
- Resistant to spyware, shoulder-surfing, phishing
- Near future
  - Test with brain scanner
  - Audio challenges

Thank you.

Questions?