IEEE INTERNATIONAL CONFERENCE ON COMMUNICATIONS 2010

Universität Konstanz

HOCHSCHULE DER MEDIEN

Breaking Randomized Linear Generation Functions based Virtual Password System

Shujun Li[1], Syed Ali Khayam[2], Ahmad-Reza Sadeghi[3], Roland Schmitz[4]

[1]University of Konstanz, Germany

[2]National University of Science & Technology, Pakistan

[3]Ruhr-University of Bochum, Germany

[4]Stuttgart Media University, Germany

26 May, 2010

Outlines

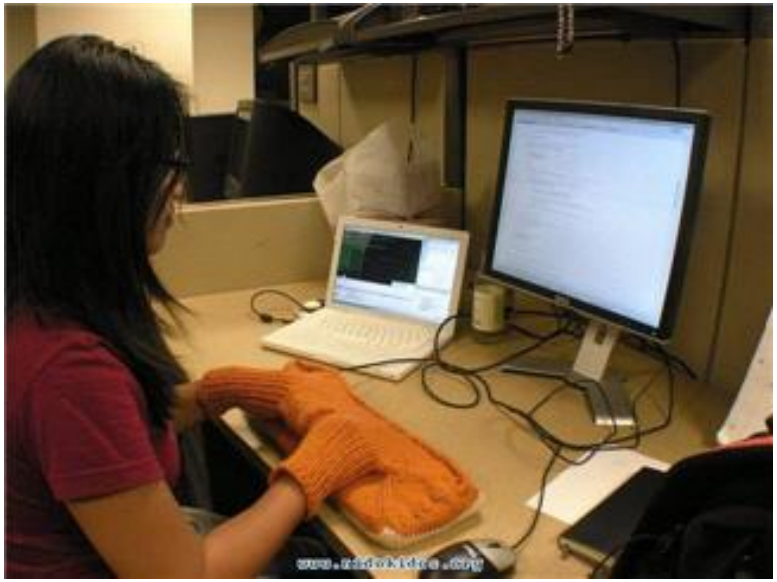
- The problem/system under study
  - The threat model
  - Virtual password system based on randomized linear generation function
  - A reported brute force attack
- Our proposed attack
  - Getting an equivalent password
  - Recovering the original password
  - A simple example
  - Simulation results
- Take-home message (with related work)

The problem/system under study

The threat model

- Who?
  - Alice and Eve
- What?
  - Alice is typing her password.
  - Eve is looking at Alice's fingers.
- How?
  - Eve is behind/beside Alice.
  - Eve installed a hidden camera.
  - Eve's malware in Alice's PC.
  - …
- So, we need a solution!

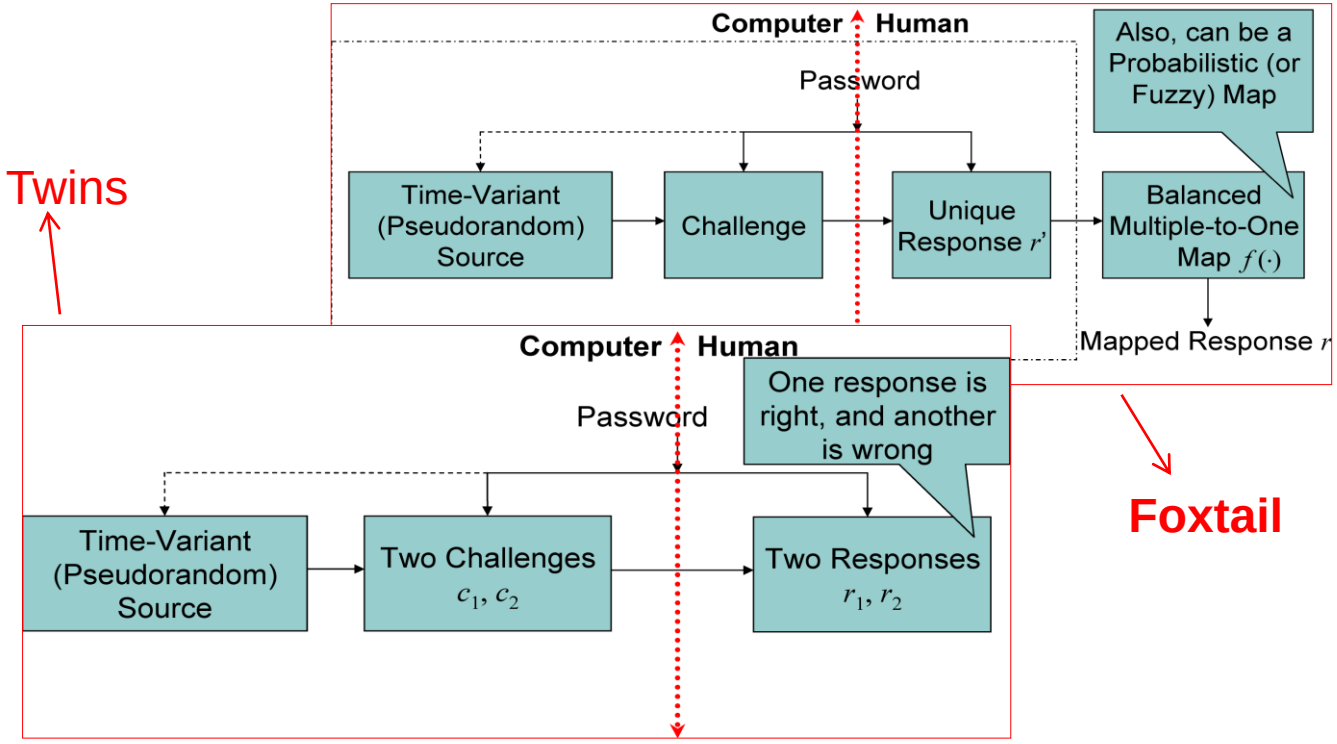
Maybe something like these?



http://www.isgafrica.org/blog/?p=138

Two basic structures

- Proposed by Li & Shum in 2002



The virtual password system (VPS)

- Who and where?
  - Proposed by Lei et al. at ICC 2008 (two papers)
  - A journal edition was published later in *Computer Communications* (also in 2008)

- What and how?
  - "Virtual password"

    - A static password $X=x_1x_2\ldots x_n$ in $\mathbb{Z}^n$, where $\mathbb{Z}=\{0,\ldots,Z\text{-}1\}$
    - A virtual function $\mathfrak{B}$: $\mathbb{Z}^{2n} \rightarrow \mathbb{Z}^n$
  - Login = A challenge-response (Foxtail) protocol

    - The challenge: A "random salt" $Y=y_1y_2\ldots y_n$ in $\mathbb{Z}^n$
    - The response: A "dynamical password" $K=k_1k_2\ldots k_n = \mathfrak{B}(X,Y)$

VPS based on randomized linear generation function

- The virtual function
  - A randomized linear function modulus an integer Z
- The static password
  - The password string $X=x_1x_2\ldots x_n$ in $\mathbb{Z}^n$
  - A secret integer α in $\mathbb{Z}$
- The login process
  - Server $\Rightarrow$ User: $Y=y_1y_2\ldots y_n$
  - User: A random integer c in $\mathbb{Z}$
    - $k_1=\mathfrak{B}_1(X,\mathrm{a},Y,\mathrm{c})=(\alpha x_1+y_1+x_2+c) \bmod Z$
    - $k_i=\mathfrak{B}_i(X,\alpha,k_{i-1},Y,\mathrm{c})=(\alpha k_{i-1}+y_i+x_i+c+x_{i+1}) \bmod Z$, for $i=2,\ldots,n-1$
    - $k_n=\mathfrak{B}_n(X,\alpha,k_{n-1},Y,\mathrm{c})=(\alpha k_{n-1}+y_n+x_n+c+x_1) \bmod Z$
  - User $\Rightarrow$ Server: $K=k_1\ldots k_n$

A reported brute-force attack

- Who and where?
  - Coskun & Herley at ISC 2008 INFORMATION SECURITY CONFERENCE
- How?
  - For n login sessions, exhaustive search X,α,Y,c and intersect the result to get the password
    - $O(nZ^4) \Rightarrow O(nZ^3) \Rightarrow O(nZ^2) \Rightarrow O(nZ) \Rightarrow O(n)$
- What's the problem?
  - c is session-varying so simple intersection does not work.
  - It can be fixed, but the attack will become more complicated.

Our proposed attack

Getting an equivalent password (1)

- The idea
  - We can turn to break an equivalent password X^*, α
- Observed login sessions
  - Login session 1: c, $Y=y_1 \ldots y_n \Rightarrow K=k_1 \ldots k_n$
  - Login session 2: c', $Y'=y'_1 \ldots y'_n \Rightarrow K'=k'_1 \ldots k'_n$

- Breaking the secret integer α
  - $\alpha(k'_{i-1}-k_{i-1}) \equiv (k'_i-k_i)-(y'_i-y_i)-(k'_1-k_1)+(y'_1-y_1) \pmod{Z}$
  - If $\gcd(k'_{i-1}-k_{i-1}, Z)=1$, then
    $\alpha = (k'_{i-1}-k_{i-1})^{-1}((k'_i-k_i)-(y'_i-y_i)-(k'_1-k_1)+(y'_1-y_1)) \bmod Z$
  - Probability = $\varphi(Z)/Z = \Pi_{p|Z}(1-p^{-1})$
  - Complexity $\leq O((\log Z)^2)$

Getting an equivalent password (2)

- Deriving an equivalent password string $X^*=x^*_1 \ldots x^*_n$
  - $x^*_1 \equiv (\alpha x_1 + x_2 + c) \equiv (k_1 - y_1) \pmod{Z}$
  - $x^*_i \equiv (x_i + x_{i+1} + c) \equiv (k_i - \alpha k_{i-1} - y_i) \pmod{Z}$, for $i=2,\ldots,n-1$
  - $x^*_n \equiv (x_n + x_1 + c) \equiv (k_i - \alpha k_{i-1} - y_i) \pmod{Z}$

- To impersonate the legitimate user
  - Pick a random integer c^* in $\mathbb{Z}$
  - Send a response $K^* = k^*_1 \ldots k^*_n$ to the server
    - $k^*_1 = (x^*_1 + y_1 + c^*) \bmod Z$
    - $k^*_i = (\alpha k^*_{i-1} + y_i + x^*_i + c^*) \bmod Z$, for $i=2,\ldots,n$

Getting an equivalent password (2)

- Deriving an equivalent password string $X^*=x^*_1 \ldots x^*_n$
  - $x^*_1 \equiv (\alpha x_1 + x_2 + c) \equiv (k_1 - y_1) \pmod{Z}$
  - $x^*_i \equiv (x_i + x_{i+1} + c) \equiv (k_i - \alpha k_{i-1} - y_i) \pmod{Z}$, for $i=2,\ldots,n-1$
  - $x^*_n \equiv (x_n + x_1 + c) \equiv (k_i - \alpha k_{i-1} - y_i) \pmod{Z}$

- To impersonate the legitimate user
  - Pick a random integer c^* in $\mathbb{Z}$
  - Send a response $K^*= k^*_1 \ldots k^*_n$ to the server
    - $k^*_1 = (x^*_1 + y_1 + c^*) \bmod Z$
    - $k^*_i = (\alpha k^*_{i-1} + y_i + x^*_i + c^*) \bmod Z$, for $i=2,\ldots,n$

Breaking the original password?

- It is possible to break X in most cases!
- How?
  - $\mathbf{X^*} \equiv \mathbf{A}\mathbf{X}+c \pmod{Z}$, where $\mathbf{A} = \begin{bmatrix} a & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}$
  - $|\mathbf{A}| = a$-1 (when n is odd) or a+1 (when n is even)
  - If $g=\gcd(|\mathbf{A}|,Z)=1$: $\mathbf{X} = (\mathbf{A}^{-1}(\mathbf{X^*}-c)) \bmod Z$
  - If $g=\gcd(|\mathbf{A}|,Z)>1$: $\mathbf{X} \equiv (|\mathbf{A}|/g)^{-1}\mathrm{adj}(\mathbf{A})(\mathbf{X^*}-c) \pmod{Z/g}$
    - If $g^n<Z^{n-1}$: The password space can be narrowed down to reveal X with $m>1$ observed login sessions.

A simple example

- Parameters: Z=10, n=4
- Password: α=7, X=1234
- Two observed login sessions
  - Login session 1: Y=1674 $\Rightarrow$ K=3526
  - Login session 2: Y'=6837 $\Rightarrow$ K'=4094
- Getting the equivalent password (α,$X^*=x^*_1x^*_2x^*_3x^*_4$)
  - α = gcd(4-3,10)$^{-1}$((0-5)-(8-6)-(4-3)+(6-1)) mod 10 = 7 ✓
  - x^*_1 = (3-1) mod 10 = 2
  - x^*_2 = (5-7*3-6) mod 10 = 8
  - x^*_3 = (2-7*5-7) mod 10 = 0
  - x^*_4 = (6-7*2-4) mod 10 = 8

Simulation results

- Success rate of 1000 random attacks (n=4)

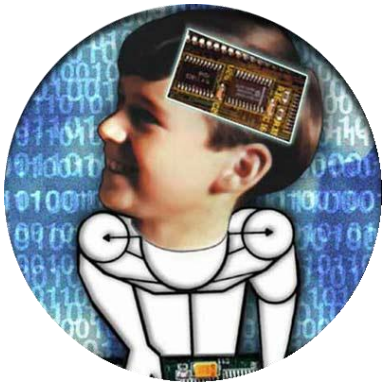
	m=2	m=3	m=4	m=5	m≥6
Z = 10	0.791	0.984	0.998	1	1
Z = 26	0.838	0.988	0.999	1	1
Z = 36	0.699	0.960	0.995	0.998	1
Z = 52	0.839	0.985	1	1	1
Z = 62	0.865	0.981	0.998	1	1
Z = 95	0.985	1	1	1	1

- Try our MATLAB code yourself
  - http://www.hooklee.com/Papers/Data/VPS.zip
  - Run `RandomAttack` to simulate an attack
  - Run `SuccessRates` to estimate the success rate of a number of random attacks

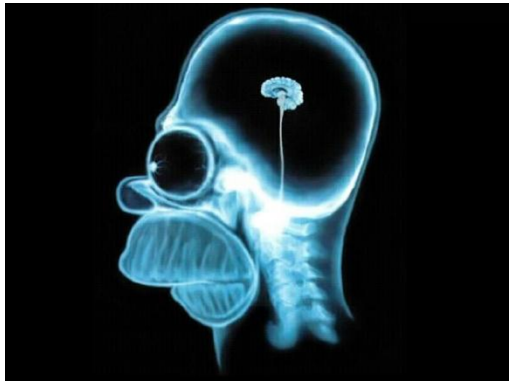
Take-home message (with related work)

This is an unsolved open problem for nearly 20 years!

- Security vs. Usability

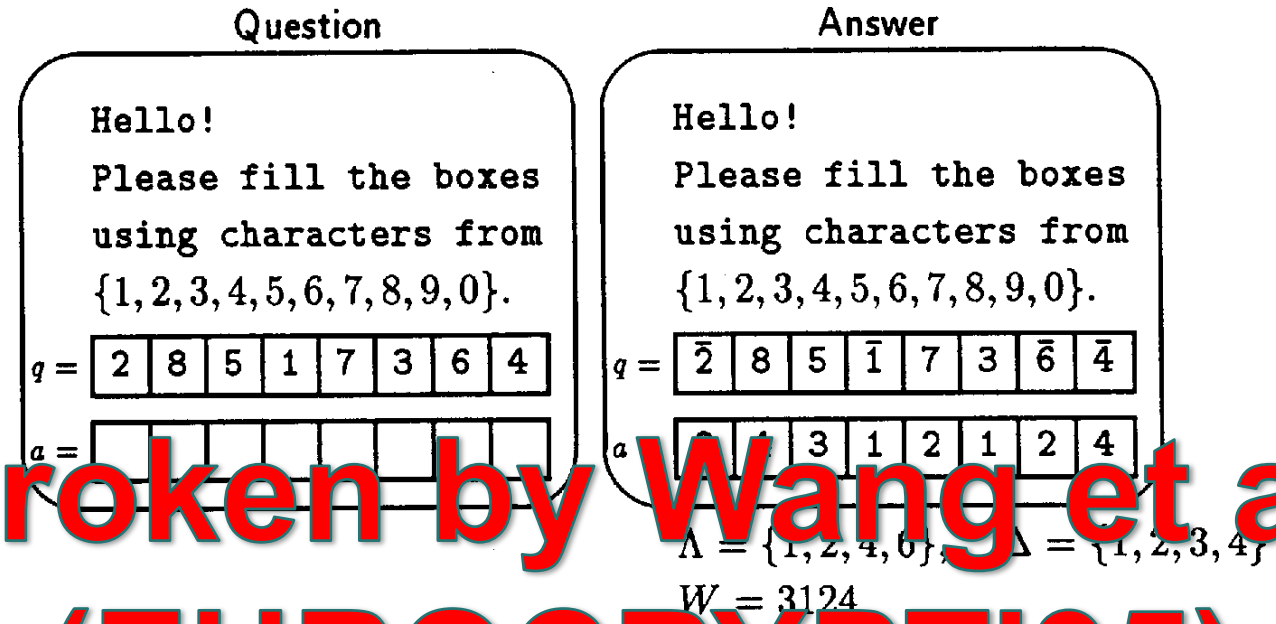


- Rich and smart attackers vs. Poor and “stupid” users



Related work: Is it indeed that difficult?

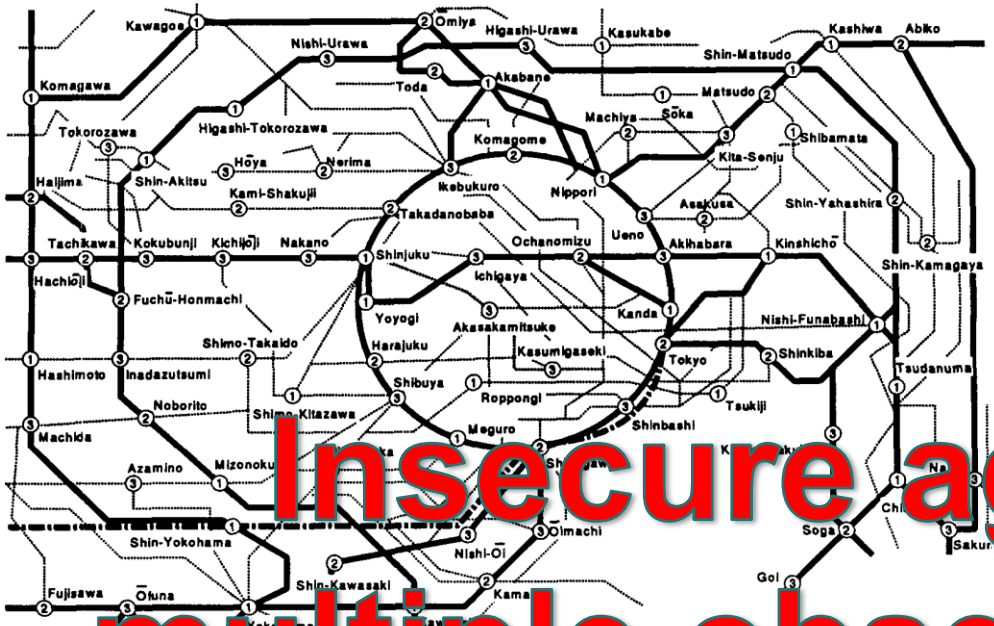
- T. Matsumoto and H. Imai, “Human identification through insecure channel,” EUROCRYPT’91



Broken by Wang et al. (EUROCRYPT’95)

Related work: Is it indeed that difficult?

- T. Matsumoto, “Human-computer cryptography: An attempt,” CCS’96



Insecure against multiple observations

Related work: Is it indeed that difficult?

- N. J. Hopper and M. Blum, “Secure human identification protocols,” ASIACRYPT’2001
  - Two protocols based on mathematical hard problems
  - $\Rightarrow$ Security may be ensured (if the underlying problem is indeed hard)

  - Require the user to make deliberate errors and/or perform nontrivial computations
  - $\Rightarrow$ Usability is problematic (166 seconds for login for an implementation reported in HB paper)

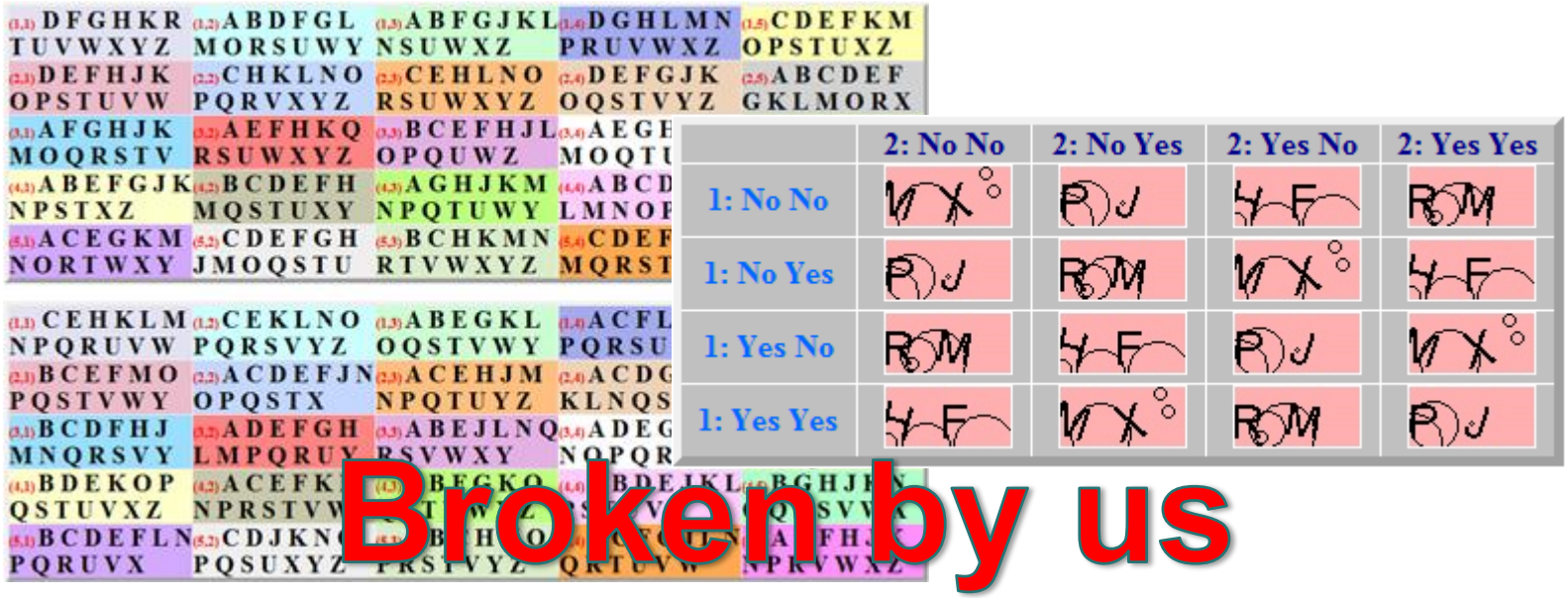
Related work: Is it indeed that difficult?

- D. Weinshall, “Cognitive authentication schemes safe against spyware,” Oakland’2006

Broken by Golle & Wagner (Oakland’2007)

Related work: Is it indeed that difficult?

- Xiaole Bai et al., “PAS: Predicate-based Authentication Services Against Powerful Passive Adversaries,” ACSAC’2008



Related work: Is it indeed that difficult?

- Hirokazu Sasamoto, Nicolas Christin and Eiji Hayashi, “Undercover: Authentication Usable in Front of Prying Eyes,” CHI’2008

To be broken by us (CHI’2011?)

Thanks for your attention!

It’s time for questions and answers ☺