Observer-Resistant Password Systems (ORPSs): Usability vs. Security

Dr Shujun Li
Senior Lecturer, Department of Computer Science
Deputy Director, Surrey Centre for Cyber Security (SCCS)
University of Surrey, UK

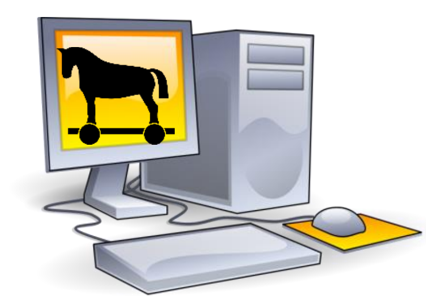
Outline

- What is it all about?
- Threat Model
- System and Attack Modelling
- Selected Work (1991-2015)
- Road Ahead?

- Acknowledgments
- Questions and Answers

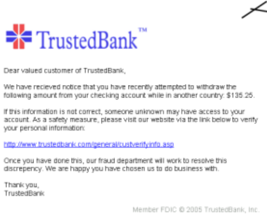
What is it all about?
Users, passwords and observers!

- 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/phone.
  - …



What is it all about?
Different kinds of observers/attacks

- Shoulder-surfers
- Hidden cameras
- Keyloggers and other password recording devices
- Password stealing software tools
- Attacks based on electromagnetic / optical / acoustic emanations
- Phishers
- Malware
- Man-in-the-middle/browser/computer/phone
- Public terminals (@ cafés, airports, hotels, …)
- …


TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

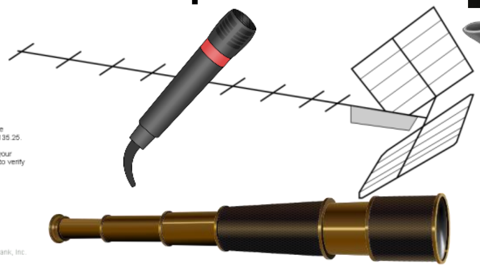
If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

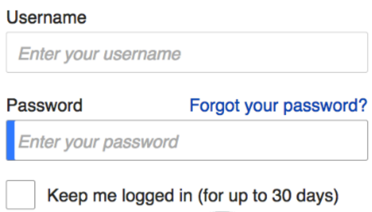
Thank you,
TrustedBank

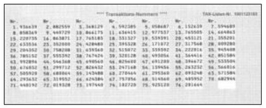
Member FDIC © 2005 TrustedBank, Inc.



What is it all about?
Existing “solutions” against observers

- “What you know”
  - Static passwords: not secure at all
- “What you have”
  - One-time passwords (OTP) generators, cards + card readers, security tokens, …
  - Problems: not always secure, prone to theft and loss, higher implementation costs, less usable / portable, …
- “Who you are”
  - Problems: not always secure, you can’t change your secret (easily), privacy concerns, higher implementation costs, …
- Multi-factor authentication?





What is it all about? Name(s) of the game

- Observer-resistant/Observation-resistant password system (ORPS) (Li 2015)
- Leakage-resilient password system (LRPS) (Yan et al. NDSS 2012)
- Virtual passwords [Lei et al. ICC 2008 + CompComm 2008]
- Cognitive authentication (Weinshall IEEE S&P 2006)
- Secure Human-Computer Interface/Identification (SecHCI) (Li & Shum 2002-2005)
- Human-computer cryptography (Matsumoto CCS ’96)
- Human authentication/identification (protocol / system / scheme) (many researchers 1991-2015)
- …

Threat Model

Threat Model: Two basic requirements

1. The password should **remain secret after a number of (ideally infinite) authentication sessions are observed** by an untrusted party (= observer).
2. Any computation in the authentication process must be conducted by the **human user alone**. = The process should be **human-executable**. = **Any computing devices** beyond the human user's brain are **untrusted**.

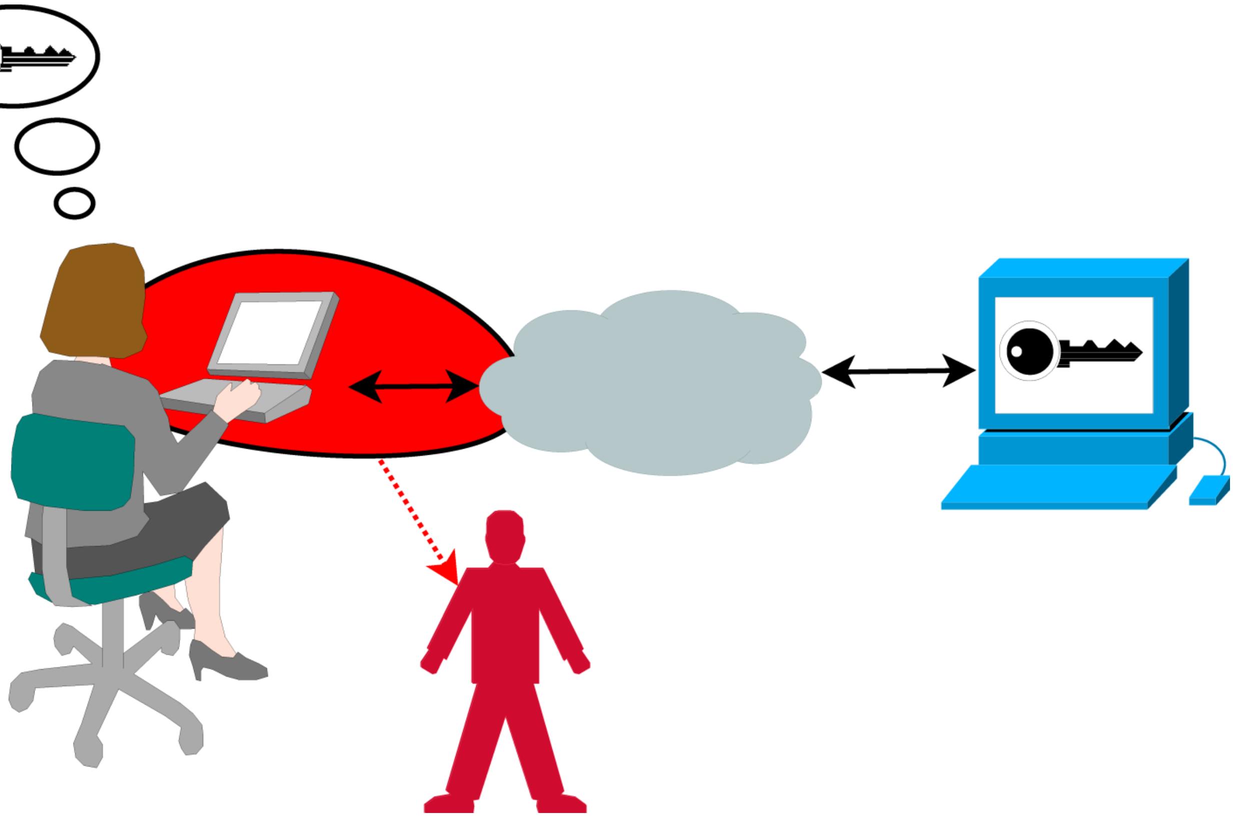
Here, the word "password" is a loose term referring to a secret shared between a human user (client) and a computer verifier (server).

Threat Model: Manuel Blum's words

- HUMANOIDs is a protocol that allows a **naked human inside a glass house** to authenticate securely to a non-trusted terminal. "Naked" means that the human carries nothing: no smart cards, no laptops, no pencil or paper. "Glass house" means that anybody can see what the human is doing, including everything that the human is typing.
- PhoneOIDs: HUMANOIDs over phone

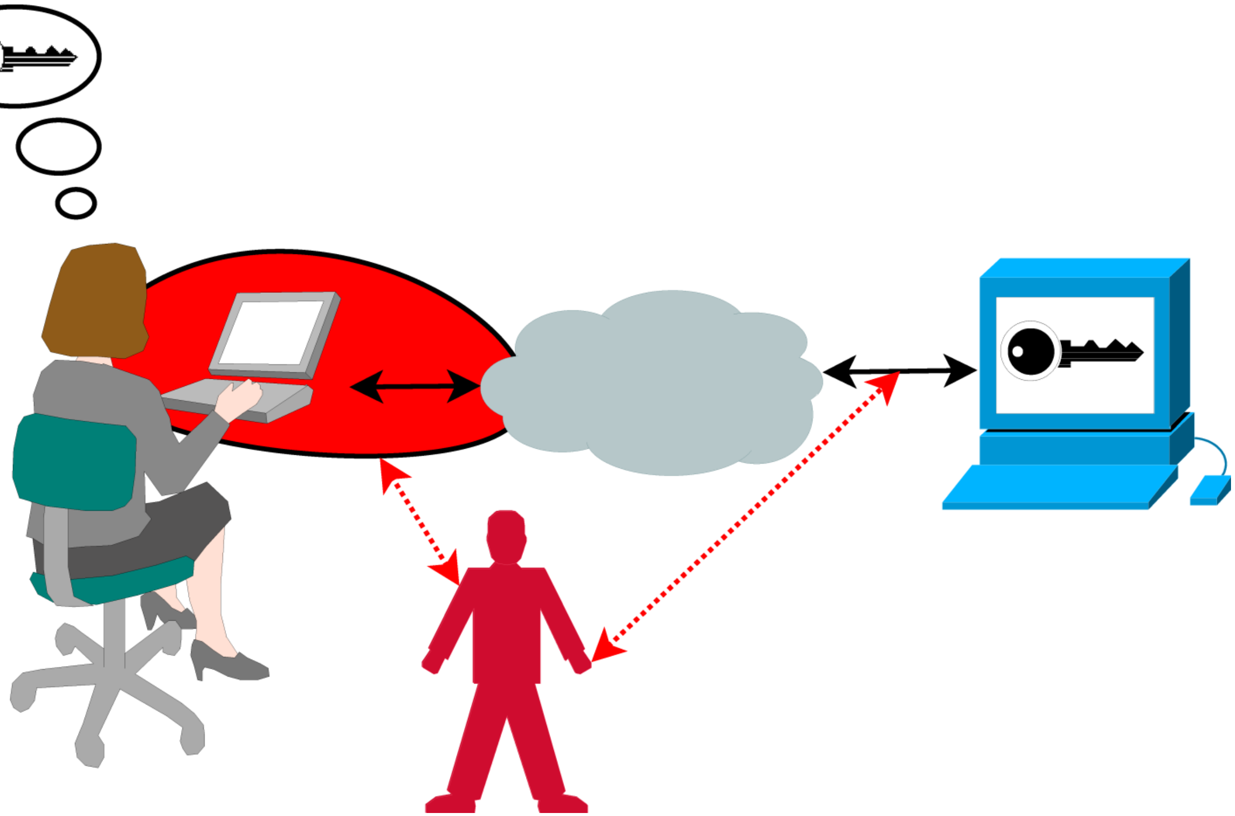
Threat Model:
Passive observers vs. Active observers

- Passive observers = Observers who only observe all authentication sessions passively (without manipulating any communications).



Threat Model:
Passive observers vs. <u>Active observers</u>

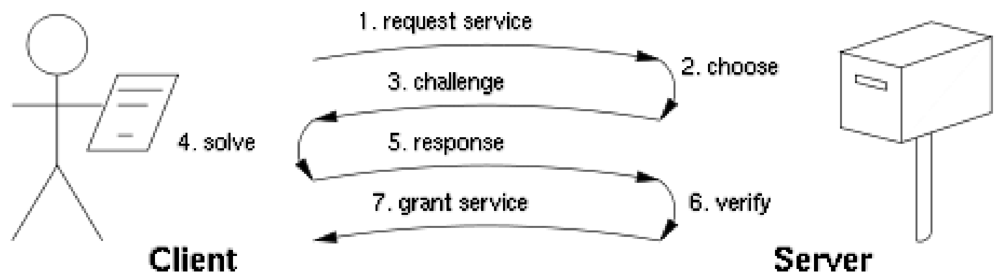
- Active observers = Observers who also try to manipulate the communications (e.g. to choose part of the authentication sessions).



System and Attack Modelling

System and Attack Modelling: Interactive challenge-response protocol

- A secret *S* shared between prover/human (H) and verifier/computer (C)



- Authentication is a challenge-response protocol
  - C $\Rightarrow$ H: t challenges $C_1(S)$, …, $C_t(S)$
  - H $\Rightarrow$ C: t responses $R_1=f_1(C_1(S),S)$, …, $R_t=f_t(C_t(S),S)$
  - C: Accept H if all the t responses are correct; otherwise reject H.
  - NB: For some designs, less than t (and/or more than $t'<t$) correct responses may still be acceptable.

System and Attack Modelling: Security and usability requirements

UNIVERSITY OF SURREY

- **The authentication process**: $\langle H(x), C(y)\rangle$ = accept, reject or attack detected
- ***p*-completeness**: $\forall z$, $\Pr[\langle H(z), C(z)\rangle = \text{accept}] \geq 1-p$
- **p-soundness**: $\forall x \neq y$, $\Pr[\langle H(x), C(y)\rangle = \text{accept}] \leq p$
- **(α,β,τ)-Human Executability**: $\forall H(x)$, $(1-\alpha)$ portion of the human population can execute $H(x)$ with the error probability β and within τ seconds
- **(p,k)-Security against Passive Observers**: $\forall z$, $\Pr[\langle \mathfrak{A}(T^k(H(z),C(z))), C(z)\rangle = \text{accept}] \leq p$
- **(p,k)-Security against Active Observers**: $\forall z$, $\Pr[\langle \mathfrak{A}(T^k(\mathfrak{A},H(z),C(z))), C(z)\rangle = \text{accept}] \leq p$
- **(q,k)-Detecting against Active Observers**: $\forall z$, $\Pr[\langle \mathfrak{A}(T^k(\mathfrak{A},H(z),C(z))), C(z)\rangle = \text{attack detected}] \geq 1-q$

System and Attack Modelling: Modelling observers

- The aim: Given n observed / chosen successful authentication sessions (= nt challenge-response pairs), try to solve the secret S with a computational complexity smaller than brute force (of S).
- $$\left.\begin{array}{l} R_1^{(1)}=f_1(C_1^{(1)}(S),S) \\ \ldots \\ R_t^{(1)}=f_t(C_t^{(1)}(S),S) \\ \ldots \\ R_1^{(n)}=f_1(C_1^{(n)}(S),S) \\ \ldots \\ R_t^{(n)}=f_t(C_t^{(n)}(S),S) \end{array}\right\} \Rightarrow \begin{array}{l} S=? \\ \text{Complexity} < \#(S) \end{array}$$

System and Attack Modelling: Information-theoretic perspective

- Assume 1) there are r>1 possible responses; 2) each possible response is equally possible for any challenge and any password; 3) all responses are independent of each other.
- Each challenge-response pair leaks $\log_2(r)$-bit information about S.
- $\Rightarrow$ After $\#(S)/\log_2(r)$ observed challenge-response pairs (= $\#(S)/\log_2(r)/t$ observed authentication sessions), S is revealed.
- **The design goal of ORPS**: the leaked information cannot be handled more effectively than a simple brute-force attack of S.

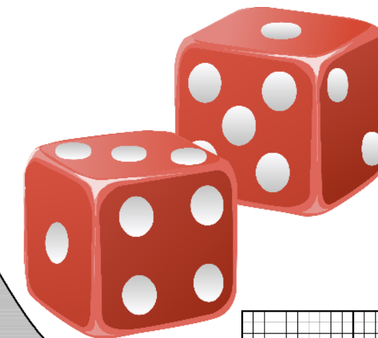
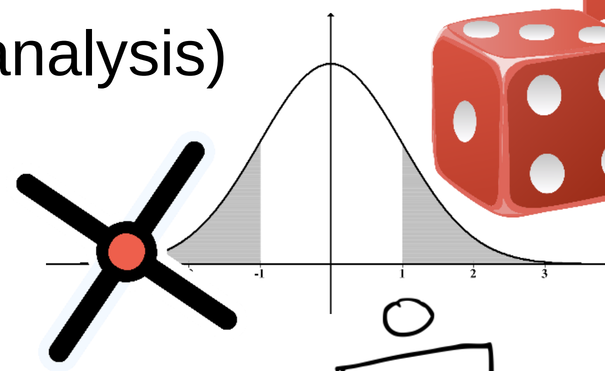
System and Attack Modelling: An *asymmetric* war

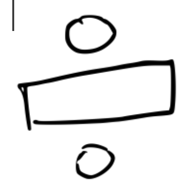
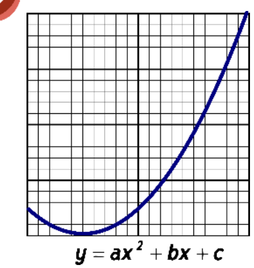
- **Security** requires $f_i(C_i(S),S)$ to be **sufficiently complicated** for **observers** to calculate S out of a number of ($C_i(S)$, R_i) pairs.
- **Usability** requires $f_i(C_i(S),S)$ to be **sufficiently simple** for **humans** to understand and execute.

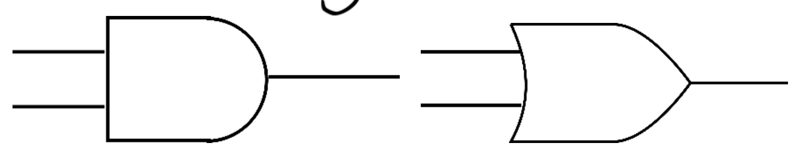
- **Observers** are computationally bounded adversaries, but they have access to **computers** as **auxiliary computing resources**.
- **Human users** have **only their brains** as the **computing resources**.
  - The only advantage human users have is knowledge of S.
  - $\Rightarrow$ We need a **human-executable trapdoor function**.

System and Attack Modelling: A large number of attacking strategies

- Random guess (base line “attack”)
- Statistical attacks (frequency analysis)
- Algebraic attacks
- Intersection attacks
- Divide and conquer attacks
- SAT solver based attacks
- Meet-in-the-middle attacks
- Side channel attacks
- Human behavior related attacks
- “Smarter” brute force attacks
- Partially-known-password attacks
- …

Selected Work: Where are we now?

- Some general principles have been identified.
- Some general design strategies have been proposed.
- A number of generic attacks have been known.
- Many ORPS schemes have been proposed.
- None of existing ORPS schemes have an acceptable balance between security (for a sufficiently large *k*) and usability.
- Clues have been found about theoretical impossibility of sufficiently secure and usable ORPS.
- Active observers are harder to handle.

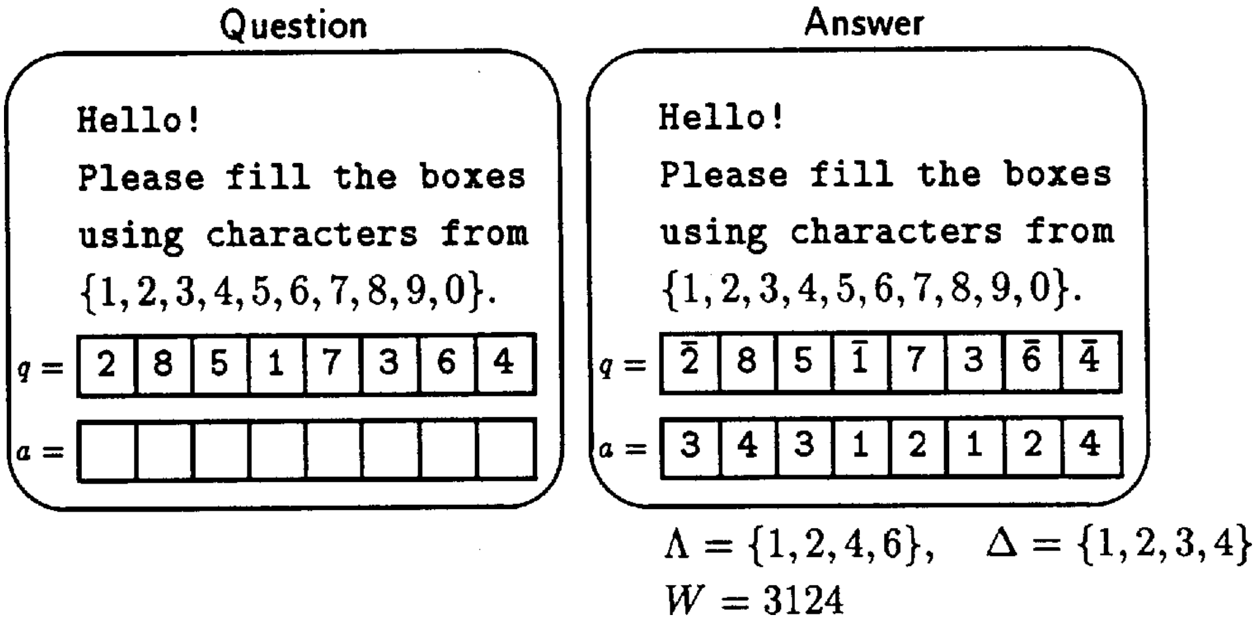
Selected Work: Security vs. Usability

- 7 example ORPS schemes compared [Yan et al. NDSS 2012] (a smaller usability score is better)

ORPS Scheme	Usability Score	Security Level
HB protocol (LPN)	33,874	No major attacks
APW protocol	18,787	No major attacks
CAS high	8,594	Best known attack: *O*(10) observed authentication sessions
CAS low	7,818	
Foxtail	3,513	Best known attack: *O*(100) observed authentication sessions
CHC	1,575	Best known attack: *O*(10) observed authentication sessions
PAS	924	Best known attack: *O*(10) observed authentication sessions

Selected Work: Matsumoto-Imai scheme (EuroCrypt'91)

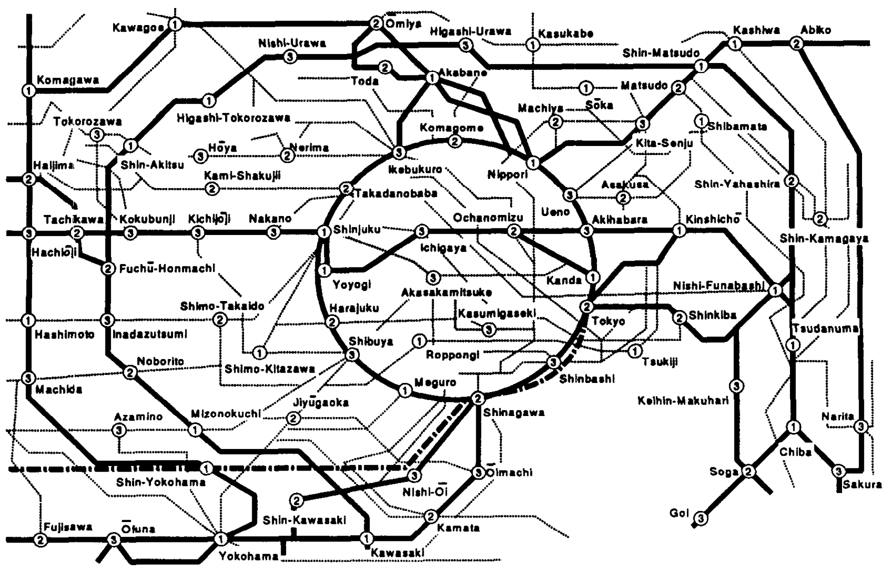
- Matsumoto-Imai scheme (EuroCrypt'91)
  -

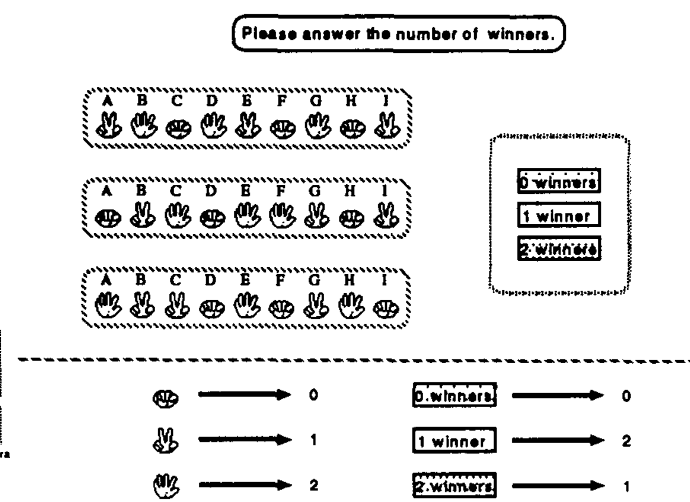


  - Too complicated for users $\Rightarrow$ Usability problem
  - Cryptanalyzed by Wang et al. (EuroCrypt'95)
- Enhanced MI scheme (Wang et al. EuroCrypt'95)
  - Too complicated for users $\Rightarrow$ Usability problem

Selected Work:
Matsumoto protocols (CCS'96)

- Dot-product based: $R_i = C_i \cdot K_i$, where K_i is a sub-password.
- The password can be derived with $O(v)$ authentication sessions, where v is the dimensionality of K_i.





Selected Work: Hopper-Blum protocols (AsiaCrypt'2001)

- A general strategy: designing ORPSs based on known (NP-)hard problems.
  - HB Protocol 1: Based on Learning Parity with Noise (LPN) problem
  - HB Protocol 2: Based on Sum of *k* Mins problem
- Plausible security vs. Usability problem
  - 166 seconds for login for an implementation of Protocol 1
- Find applications in light-weight cryptography (RFID chips replacing human users)

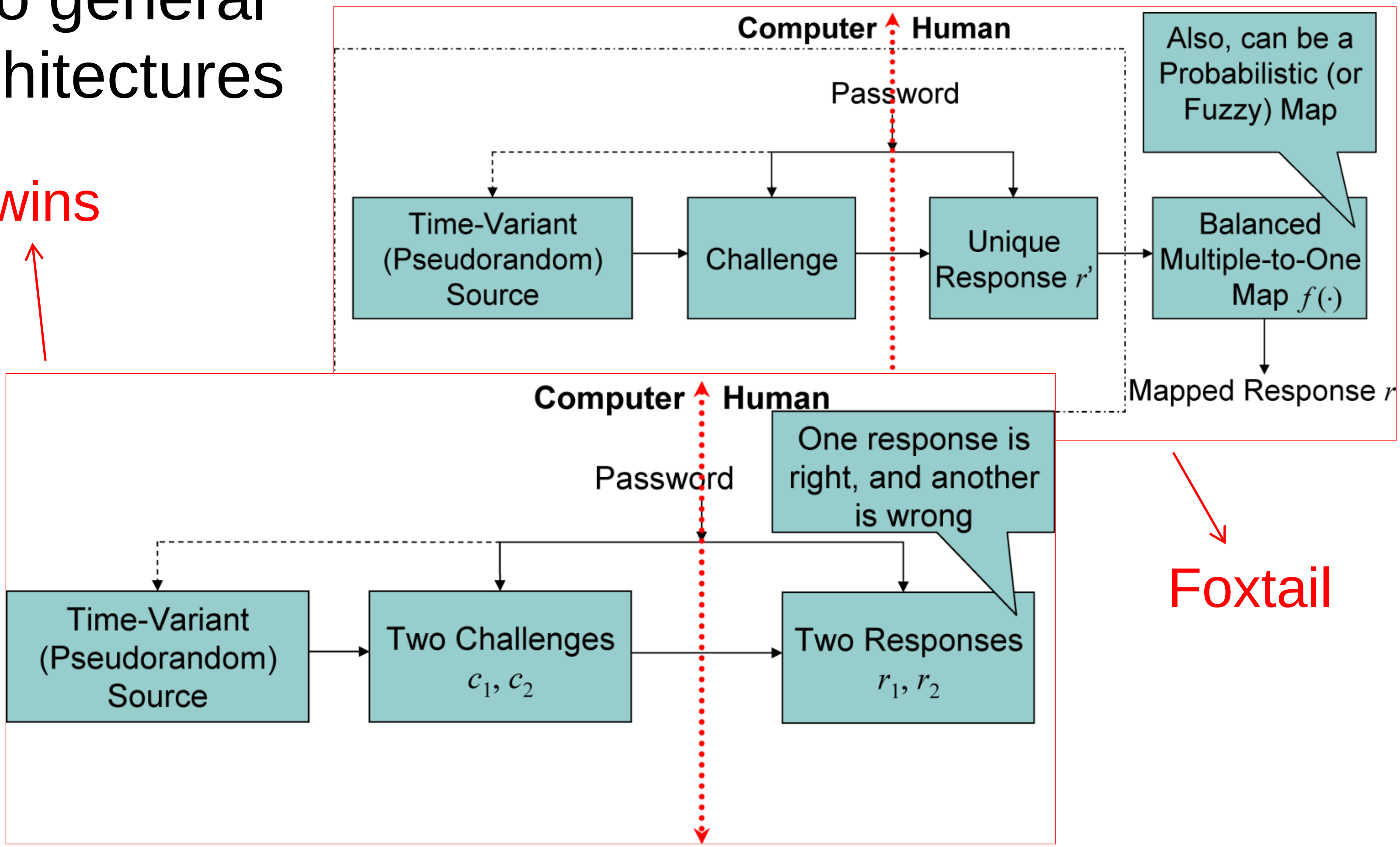
Selected Work:
Convex Hull Click protocols (2002-2006)

- First proposed by Sobrado and Birget in 2002 and further extended by Wiedenbeck et al. in 2006
- A number of variants proposed
- Usability: Better for small parameters
- Two statistical attacks: Insecure against *O*(10) observed authentication sessions (my work @ ISC 2010 and IJIS 2013)

Selected Work:
Twins and Foxtail (my work 2004-2005)

Two general architectures

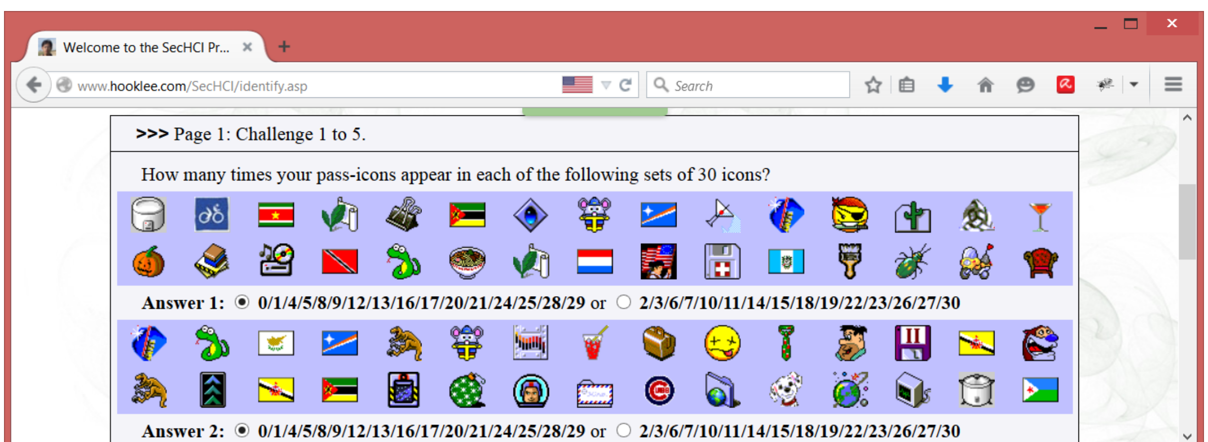
Twins



Foxtail

Selected Work:
A Foxtail protocol (my work 2004-2005)

- Password: *k* pass-icons out of a pool of *n* icons
- Challenge: *m* randomly selected icons + *m* icons in which the number of pass-icons is 0-3 with equal probability
- Response: floor((#(pass-icons) mod 4) / 2) = 0 or 1
- Usability: 2-3 mins for login for 20 challenges (not usable)
- Statistical attacks: insecure against *O*(100) observed authentication sessions (Yan et al. NDSS 2012)

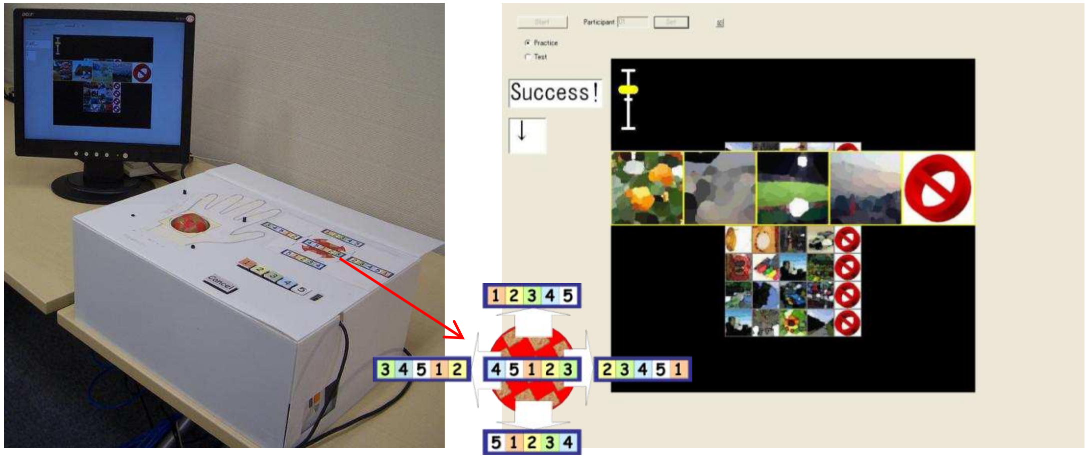


Selected Work:
Weinshall's CAS (IEEE S&P 2006)

- CAS = Cognitive Authentication Scheme
  - Usability problem (30/60 secret pictures to recall, 1-3 minutes for login)
  - SAT solver based attack: Insecure against *O*(10) observed authentication sessions (IEEE S&P 2007)

Selected Work: Undercover (ACM CHI 2008)

- A general strategy: Hiding part of challenges via a trusted channel (a tracking ball covered by hand)
- A trusted channel is not always available.
- Intersection attacks and human behavior based timing attacks reported (my work @ SOUPS 2011)
- The timing attack has its root in an improper GUI design.



Selected Work: Bai et al.'s PAS (ACSAC 2008)

- PAS = Predicate-based Authentication Service
- A very involved system with a number of tables for each challenge and a list of tuples as password
- CAPTCHAs are used to disable automated attacks
- Security and usability: PAS ≈ Less secure and less usable OTP (my work @ ACSAC 2009)

(1,1) D F G H K R T U V W X Y Z	(1,2) A B D F G L M O R S U W Y	(1,3) A B F G J K L N S U W X Z	(1,4) D G H L M N P R U V W X Z	(1,5) C D E F K M O P S T U X Z
(2,1) D E F H J K O P S T U V W	(2,2) C H K L N O P Q R V X Y Z	(2,3) C E H L N O R S U W X Y Z	(2,4) D E F G J K O Q S T V Y Z	(2,5) A B C D E F G K L M O R X
(3,1) A F G H J K M O Q R S T V	(3,2) A E F H K Q R S U W X Y Z	(3,3) B C E F H J L O P Q U W Z	(3,4) A E G H J L M O Q T U V W	(3,5) D F G H K M N O Q T W X Y
(4,1) A B E F G J K N P S T X Z	(4,2) B C D E F H M Q S T U X Y	(4,3) A G H J K M N P Q T U W Y	(4,4) A B C D G H L M N O P V X	(4,5) A C E G L M N P R S T X Z
(5,1) A C E G K M N O R T W X Y	(5,2) C D E F G H J M O Q S T U	(5,3) B C H K M N R T V W X Y Z	(5,4) C D E F H J L M Q R S T V	(5,5) E F G H L N O Q R S T X Z

(1,1) C E H K L M N P Q R U V W	(1,2) C E K L N O P Q R S V Y Z	(1,3) A B E G K L O Q S T V W Y	(1,4) A C F L M O P Q R S U V Z	(1,5) A B C D H K O R S T U W Z
(2,1) B C E F M O P Q S T V W Y	(2,2) A C D E F J N O P Q S T X	(2,3) A C E H J M N P Q T U Y Z	(2,4) A C D G H J K L N Q S T X	(2,5) A C E F K M N Q R T X Y Z
(3,1) B C D F H J M N Q R S V Y	(3,2) A D E F G H L M P Q R U Y	(3,3) A B E J L N Q R S V W X Y	(3,4) A D E G K M N O P Q R T U	(3,5) A C D F H J M O Q R S U Z
(4,1) B D E K O P Q S T U V X Z	(4,2) A C E F K M N P R S T V W	(4,3) A B F G K O Q S T V W X Z	(4,4) A B D E J K L P S T U V X	(4,5) B G H J K N O Q R S V W X
(5,1) B C D E F L N P Q R U V X	(5,2) C D J K N O P Q S U X Y Z	(5,3) A B C H K O P R S T V Y Z	(5,4) A C F G J L N Q R T U V W	(5,5) A D F H J K N P R V W X Z

	2: No No	2: No Yes	2: Yes No	2: Yes Yes
1: No No				
1: No Yes				
1: Yes No				
1: Yes Yes				

Selected Work: Yan et al.'s NDSS 2012 work

- The most comprehensive review of ORPS schemes
  - Yan et al. a different "Leakage-Resilient Password Systems" (LRPSs)
- One of two outstanding papers of NDSS 2012
- A number of security-oriented principles for ORPS design
- **<u>A quantitative usability evaluation framework</u>** based on cognitive workload and memory demand models
- A new 2-D statistical attack showing insecurity of my Foxtail protocol (against *O*(100) observed authentication sessions)

Selected Work: My NDSS 2013 work

- A rigorous theoretical treatment of the 2-D statistical attacks discovered by Yan et al. at NDSS 2012.
- Discovery of two families of the statistical attacks on some ORPSs: "**response-independent frequency analysis**" and "**response-dependent frequency analysis**".
  - Why they work? – Statistical asymmetry between pass- and non-pass-objects in the password.
  - Yan et al.'s 2-D attack is just a special case.
  - A less effective 1-D attack exists ($O(1000)$ sessions required).
- Each family contains **infinite** number of attacks $\Rightarrow$ Implies theoretical impossibility of security against all those attacks for ORPSs with **finite** number of parameters?
- Two new principles and fixed Foxtail protocols proposed

Selected Work: New timing attacks (IEEETIFS 2015)

- Further development based on my SOUPS 2011 work on Underwork by my collaborators Perković and Čagalj.
- Generalized human behavior based timing attacks to two new ORPS schemes: HB protocol 1 and a patented Mod10 method
  - Why do they work? – **Cognitive asymmetry**: Different cognitive loads required for different challenges
- Level of success: for HB protocol 1 (default parameters) with $O(100)$ observed sessions the password can be derived fully with high probability.
- New ORPS design principle proposed on asymmetry related to cognitive load and user interface

Selected Work:
My latest work (IEEETIFS 2015)

- Two ORPS schemes modelled as linear systems of congruences linked to the learning with (structured) noise (LwE) problem.
  - A fixed Foxtail protocol (my work @ NDSS 2013)
  - A Twins protocol (Catuogno and Galdi WISTP 2008)
- Various attacking strategies studied
  - Linear algebra, lattice and coding theory based attacks
- Results
  - The fixed Foxtail protocol: insecure against $O(n^2)$ observed authentication sessions where n is the number of objects
  - CG protocol: insecure against $O(n)$ observed sessions
- Results generalizable to other ORPS schemes
- Open question: ORPSs secure against $\geq O(n^2)$ sessions?

Road Ahead?

Road Ahead?
General design strategies and principles

- Designing ORPSs based on more candidate (NP-)hard problems.
  - Fixed-parameter intractable problems and paraNP-hard problems are of particular interests.
  - Three key parameters: n – number of objects, k – size of password (number of pass-objects), m – size of challenge (number of objects in a challenge, may be equal to n)
- Pay attention to ALL known attacks.
  - Pay special attention to details in user interface and how human users interact with the interface.
- Twins and Foxtail protocols still stand as good ORPS architectures.

Road Ahead?
Automating security/usability evaluation

- Current practice does not allow a large number of potential ORPS designs and implementations to be checked quickly.
- First quantitative usability evaluation framework has appeared (Yan et al. NDSS 2012) but not complete nor computable.
- Use of cognitive models has proved useful.
  - CPM-GOMS was used in two recent papers on ORPSs against shoulder surfers for modelling shoulder surfers' cognitive powers.
- Security evaluation automation is possible (mathematical models + Monte Carlo methods)
- Software tools are still missing.
  - Some cognitive modelling tools exist, but cannot be used directly.

Road Ahead?
Studies on impossibility

- Humans' cognitive limitations are largely known.
  - Miller's law: The magic number of 7±2 in human's working memory (*Psychological Review* 1956)
  - Cowan's law: The magic number of 4 in human's short-term memory (Behavioral and Brain Sciences 2001)
  - …
- Requirements on security and usability are largely known if application context is given.
- ORPSs have a general mathematical model.
- Some clues have been seen (e.g. my work @ NDSS 2013)
- $\Rightarrow$ Can impossibility be proved at least for some applications?

Back Matter

Acknowledgments: Research institutes + Funders

- Microsoft Research Asia (2002)
  - Student Intern
- Xi’an Jiaotong University (2002-2003)
  - PhD Student
- Universität Konstanz and German Research Foundation (DFG), Germany (2009-2011)
  - 5-Year Zukunftskolleg Fellow
- University of Surrey, UK (2011-present)
  - Senior Lecturer

Acknowledgments:
Main collaborators

- Dr. Hassan Jameel Asghar
  - NICTA, Australia (2014-)
  - Macquarie University, Australia (2009-2013)
- Dr. Toni Perković and Dr. Mario Čagalj
  - FESB, University of Split, Croatia (2010-)
- Prof. Josef Pieprzyk
  - Queensland University of Technology (2014-)
  - Macquarie University, Australia (2009-2013)
- Prof. Dr.-Ing. Ahmad-Reza Sadeghi
  - Technische Universität Darmstadt, Germany (2012-)
  - Ruhr-Universität Bochum, Germany (2009-2011)
- Dr. Heung-Yeung (Harry) Shum
  - Microsoft Research Asia, China (2002)






Thanks for your attention!

Questions?