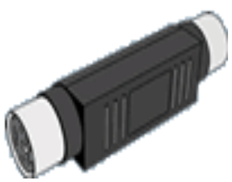
On Limitations of Designing Leakage-Resilient Password Systems: Attacks, Principles and Usability

Qiang Yan, Jin Han, Yingjiu Li, Robert H. Deng
School of Information Systems
Singapore Management University

Leakage-Resilient Password Systems (LRPS)

- Malware, e. g. software keylogger, MITM-at-the-browser

- Untrusted input device
  e.g. hardware keylogger

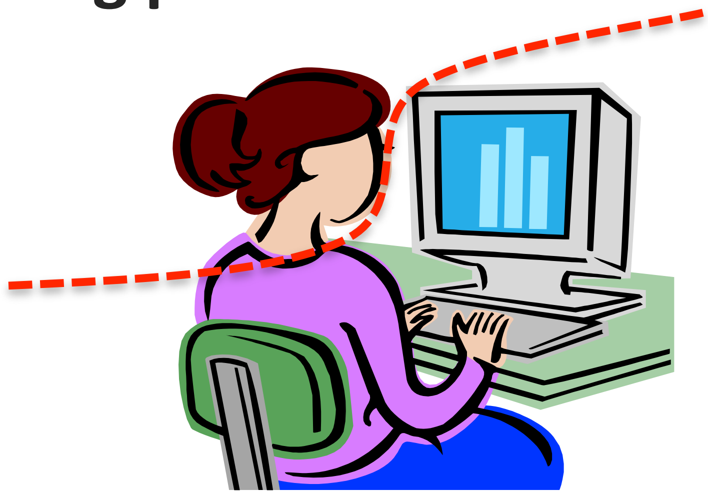


- Shoulder surfing
  e. g. hidden camera recording

SMU
SINGAPORE MANAGEMENT UNIVERSITY

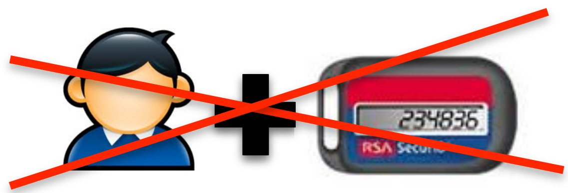
<u>L</u>eakage-<u>R</u>esilient <u>P</u>assword <u>S</u>ystems (LRPS)

- **Assumption**
  - **strong passive attacker**



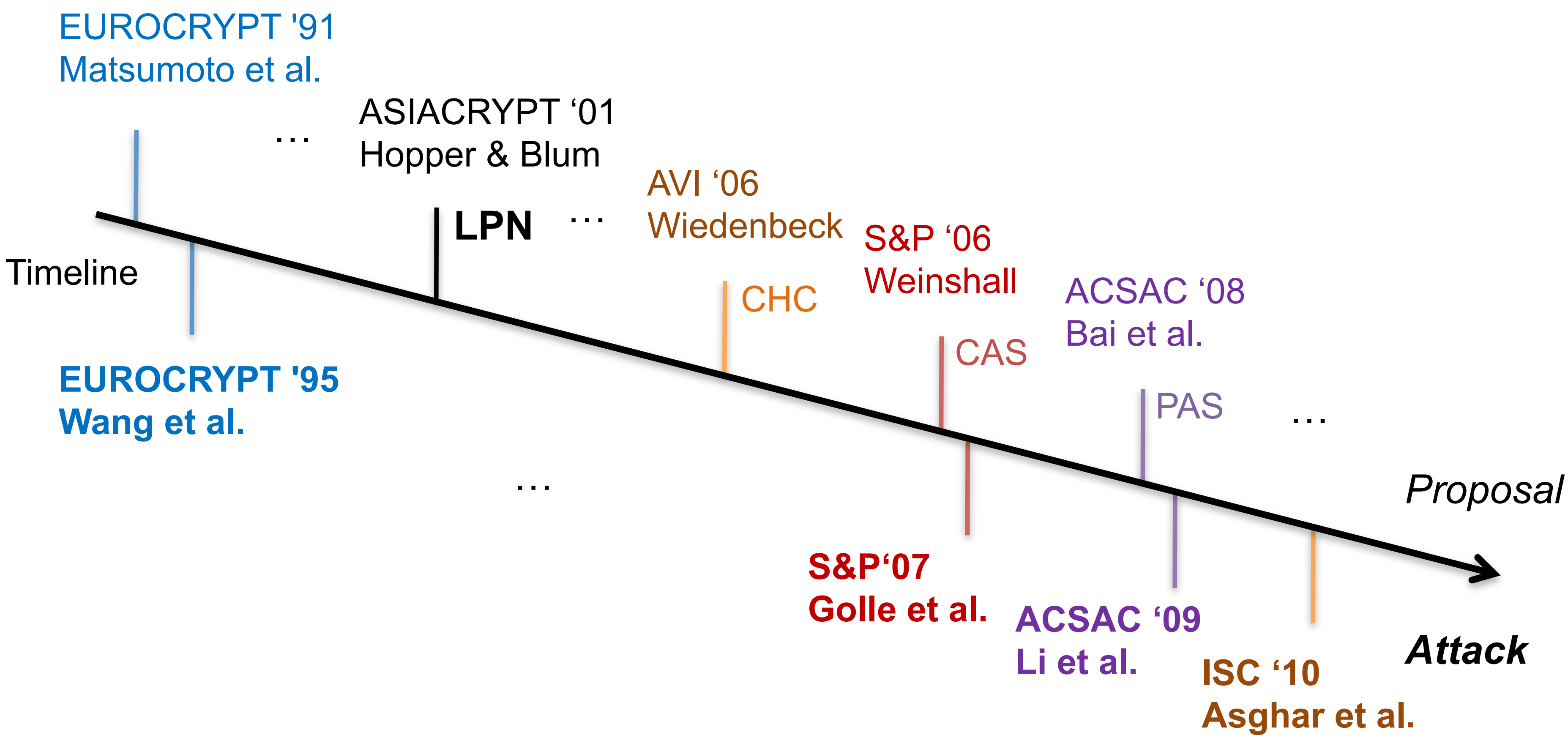
*Adversary sees **everything** below the red line.*

  - **Unaided user**



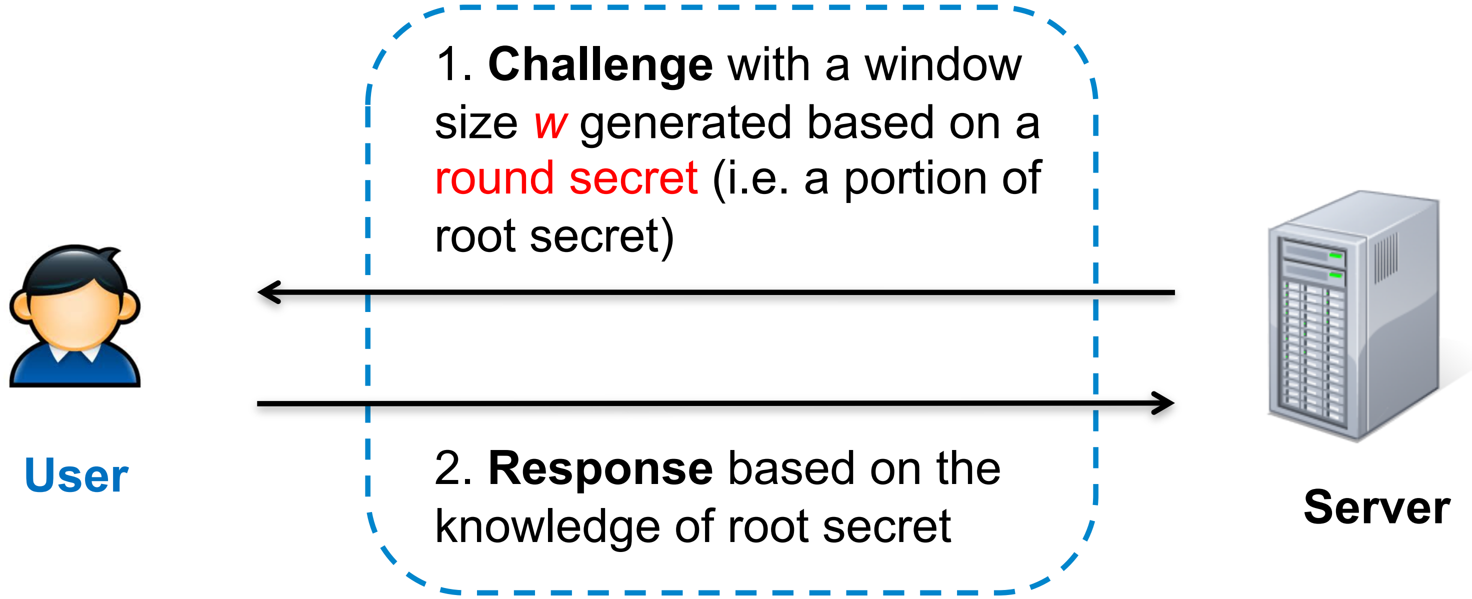
Aided User

Prior efforts on LRPS for unaided humans



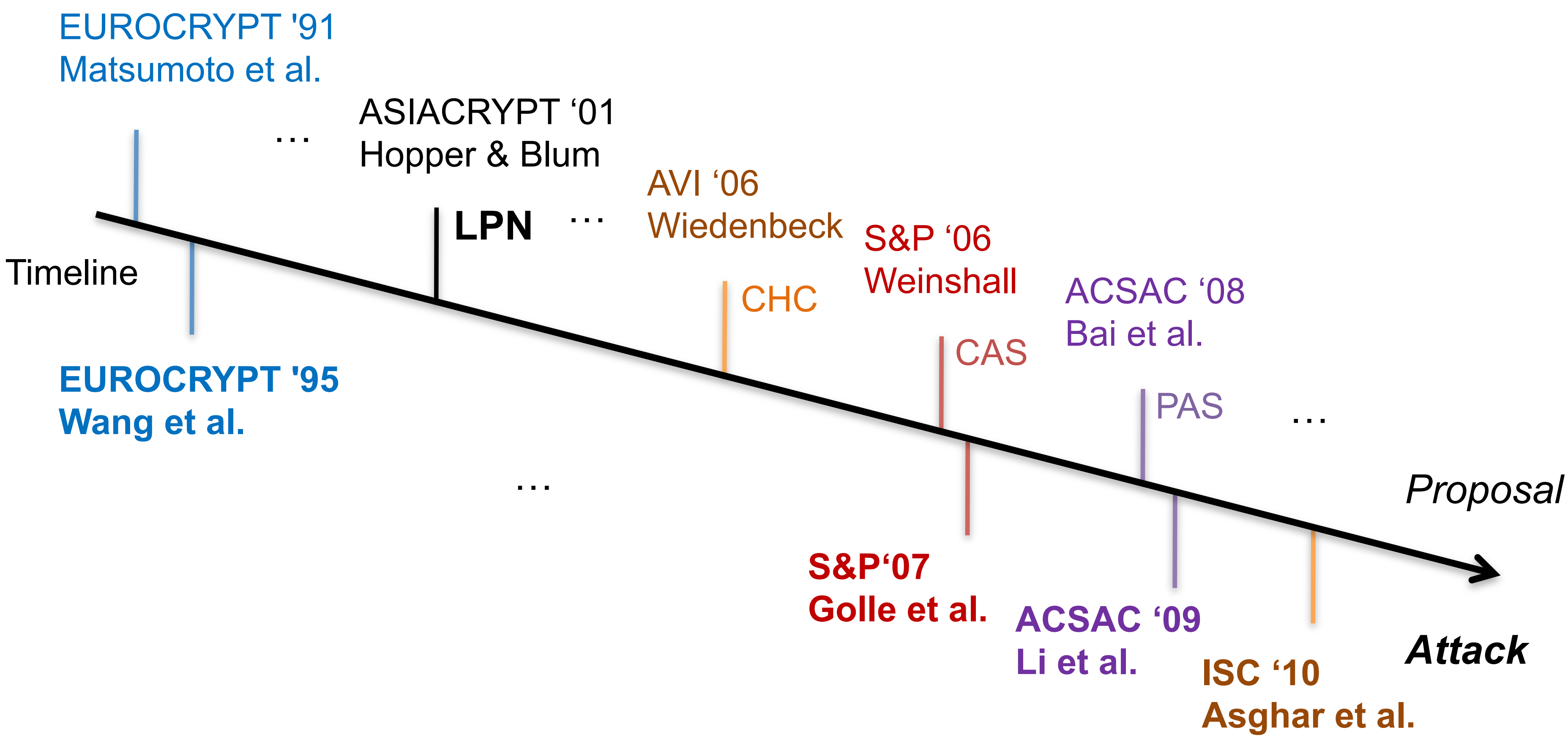
The *k*-out-of-*n* LRPS Paradigm

User's root secret (i.e. password) consists of *k* secret elements out of *n*.



Repeat steps 1 and 2, until the number of correct user responses reaches a ***threshold****.*

Prior efforts on LRPS for unaided humans



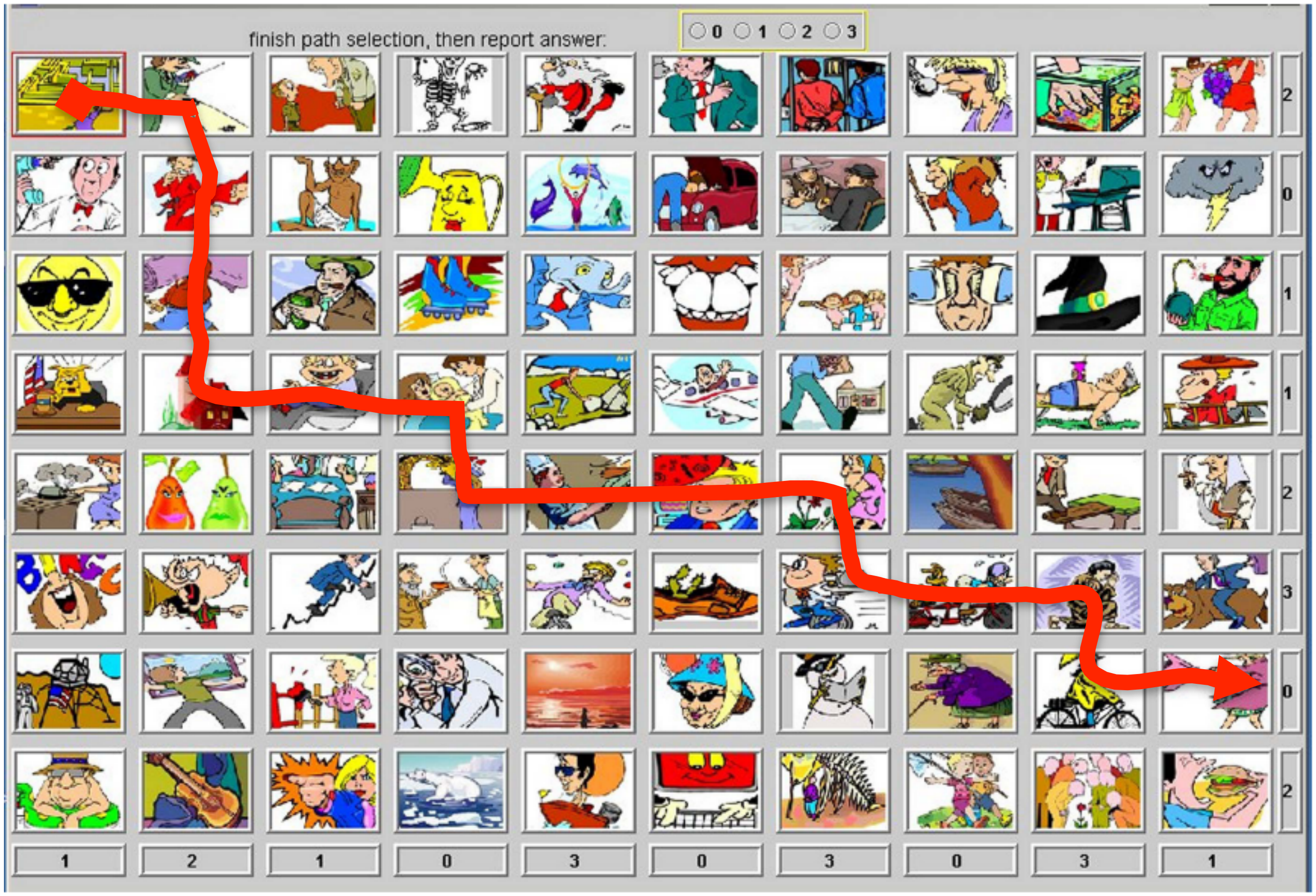
Two generic attacks

- **Brute force**
  - Eliminate password candidates that do not lead to correct responses.
  - Effectiveness is *design-independent*.
    - Applicable to any LRPS with small password space
- **Statistical analysis**
  - Find out the most likely passwords.
  - Effectiveness is *design-dependent*.
    - Applicable to many LRPSs even with large password space
- They are common knowledge but are **underestimated**.

SMU SINGAPORE MANAGEMENT UNIVERSITY

Statistical bias in decision paths (1/2)

CAS High [S&P06, Weinshall]: *Root secret consists of* ***k*** *= 30 images out of 80*

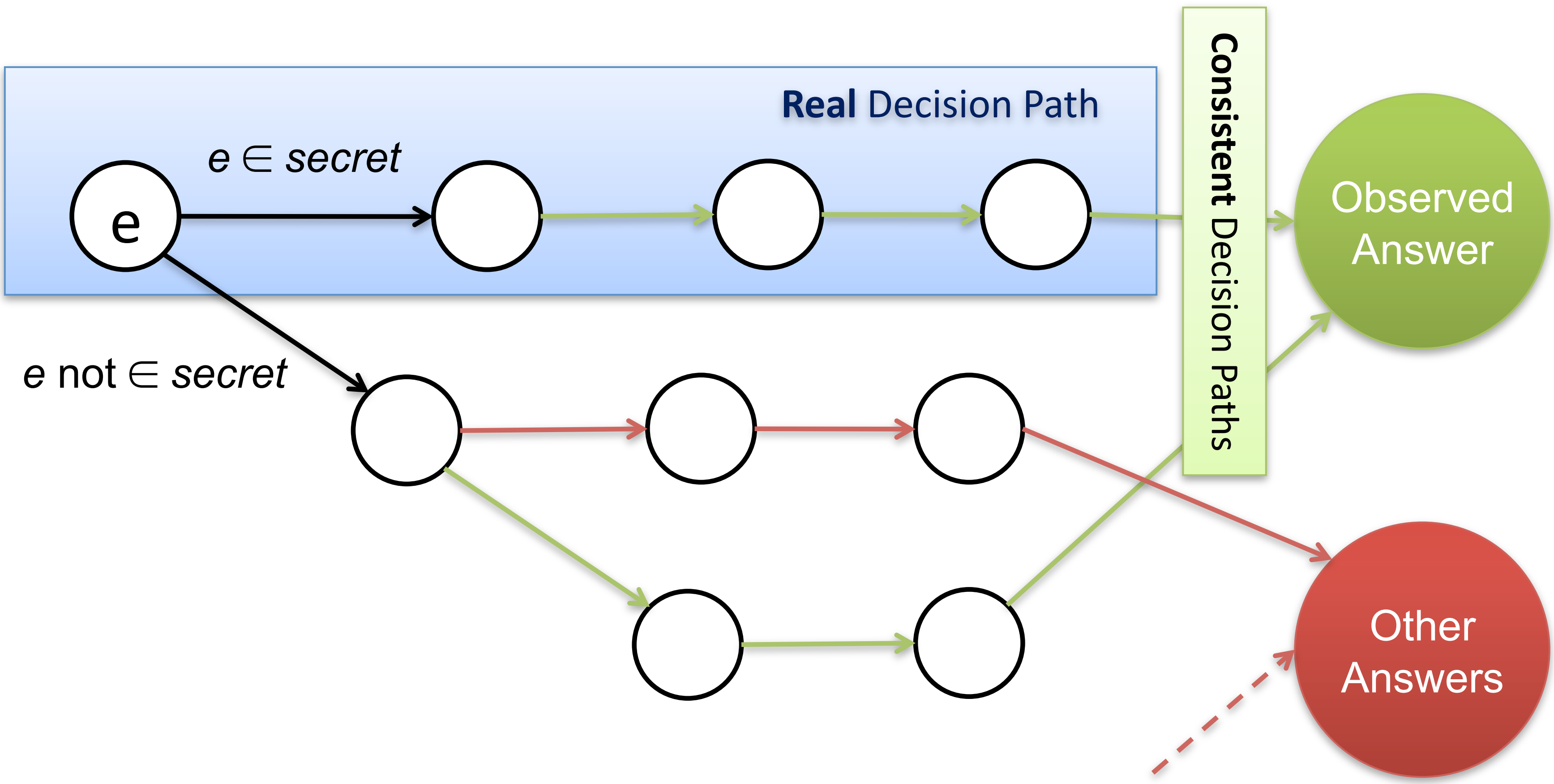


1. Start from upper-left corner.

2. Move down if the current image is a secret image; Otherwise move right.

3. ***Answer*** *= the number associated with the exit.*

Probabilistic decision tree



Score mechanism of probabilistic decision tree

- Rationale:
  - At least one of the consistent decision paths is the **correct** path.
  - Other consistent decision paths are "**noises**" whose effects will cancel out over multiple rounds.
- Basic probabilities:
  - P_1: $P(e \in secret) = k/n$
  - P_0: $P(e \text{ not} \in secret) = 1 - P_1$
- Create a *1-element score table*; in each round, compute
  - $P(X) = P(<S_1, D_1, D_2, S_2>) = P_1 * P_0 * P_0 * P_1$
  - P_C = sum of probabilities of all consistent paths
  - $Score(S_1)$ += $P(X)/P_C$
  - $Score(D_1)$ -= $P(X)/P_C$

Statistical bias in decision paths (2/2)

CAS High [S&P06, Weinshall]

43758 possible decision paths in total, with average path length of 14.55.

Secret images score significantly higher than decoy images after a sufficient number of observations.

Recover the exact root secret after observing 65 sessions.

Usability costs of preventing the two generic attacks

1. **Large** root secret space	Memory
2. **Large** round secret space	Memory; Computation
3. **Uniformly** distributed challenges	Round Number; Window Size
4. **Complex** challenges	Computation
or **counting-based** challenges	Round Number

Quantitative evidences from psychology

- Human beings have limitations on **cognitive capability** and **memory**.
  - These limitations will NOT be significantly improved even after repetitive rehearsal.
- Atomic Cognitive Operations
  - (Single/Parallel) **Recognition**
  - (Free/Cued) **Recall**
  - (Single-target/Multi-target) **Visual Search**
  - Simple **Cognitive Arithmetic**

High security at cost of heavy cognitive demand

More secure

	k	n	Win size	Password space	Reported Time /round(sec)	HP (C) /round (sec)	HP (C) /login (sec)	HP (M)	HP Total =M×C ($\times 10^2$)
LPN[15]	15	200	200	1.463×10^{22}	**23.71**	**33.423**	668.45	50.68	**338.74**
APW[2]	16	200	200	8.369×10^{24}	**35.50**	**57.928**	347.57	54.05	**187.87**
CAS Low[31]	60	240	20	2.433×10^{57}	**5.00**	**6.073**	121.46	70.75	**85.94**
CAS High[31]	30	80	80	8.871×10^{21}	**20.00**	**22.099**	220.99	35.38	**78.18**
SecHCI[20]	14	140	30	6.510×10^{18}	**9.00**	**10.638**	212.76	16.51	**35.13**
CHC[32]	5	112	83	1.341×10^{8}	**10.97**	**9.326**	93.26	16.89	**15.75**
PAS[4]	4	N/A	13	4.225×10^{5}	**8.37**	**6.837**	68.37	13.51	**9.24**

More usable

The **strict** tradeoff relation may not holds, but the **low bound** does.

SMU SINGAPORE MANAGEMENT UNIVERSITY

Why so hard? – capability asymmetry

The adversary

Advantage:
Computation Power
Storage

Disadvantage:
Don't know the password

The user

Advantage:
Knowledge of the password

Disadvantage:
Limited cognitive computation
impossible to do CPA secure encryption
***E*(*secret*, *challenge*)**
Limited memory

Conclusion

- Our work analyzed the **inherent** limitations of designing Leakage-Resilient Password Systems.
  - Analyze the impact of two generic attacks that are usually overlooked.
  - Propose the design principles that are necessary to mitigate these generic attacks.
  - Establish the first quantitative analysis framework on usability costs of the existing LRPS systems.
- *Our results imply that:*
  - *An LRPS has to incorporate certain **trusted** devices in order to be both secure and usable.*

SMU
SINGAPORE MANAGEMENT UNIVERSITY

Thank You!

Q & A

SMU
SINGAPORE MANAGEMENT UNIVERSITY

Brute force for biased challenges

Undercover [CHI08, Sasamoto et al.]: *User selects **k** = 5 pictures out of **n** = 28; # of candidate root secrets is* $C_{28}^{5} = 98280$

At most one secret image will appear in each challenge.

P = 1 (0-indexed)

Brute force recovers the exact root secret after observing 6 sessions.

Answer *= (P + **r**) mod 5, where **r** is a random integer delivered via a secure channel. Without knowing **r**, the answer tells nothing.*

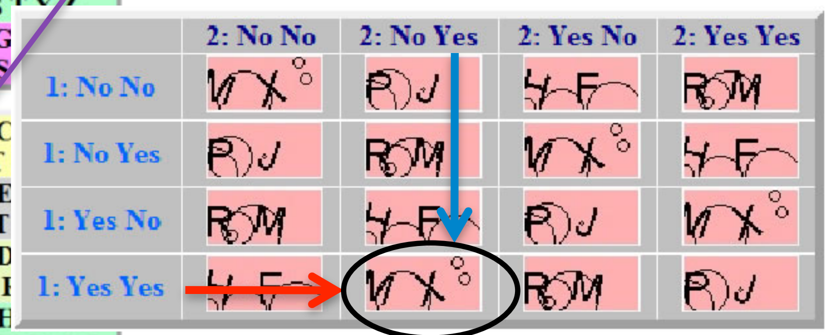
Brute force for round secrets

PAS [ACSAC08, Bai et al.]

Password = (<3, 2>, hello), (<1, 3>, world)

Challenge index = 2

Predicate = (<3, 2>, e),(<1, 3>, o)



Answer = *MX*

= *table[YES, YES][NO, YES]*

The SAME index is used for the same authentication session.
Brute force recover the round secret after observing 1 session.

Implications: *A challenge that can be solved by a small number secret elements is not secure, cognitive workload has to be increased.*

Statistical bias in challenges

Undercover [CHI08, Sasamoto et al.]

At most one secret image will appear in each challenge.

P = 1 (0-indexed)

Build a 2-element counting table. A secret image will NOT appear together with another secret image. Recover root secret in 20 sessions.

Answer = *(P + r) mod 5, where r is a random integer delivered via a secure channel. Without knowing r, the answer tells nothing.*

Implications: *A challenge that uniformly draws the candidate elements will be secure, but it will increase the round number or impose a larger window size.*

SMU SINGAPORE MANAGEMENT UNIVERSITY

Statistical bias in responses (1/2)

SecHCI [Cryptology ePrint 05, Li et al.]: *Root secret consists of **k**=14 icons, **n**=140*

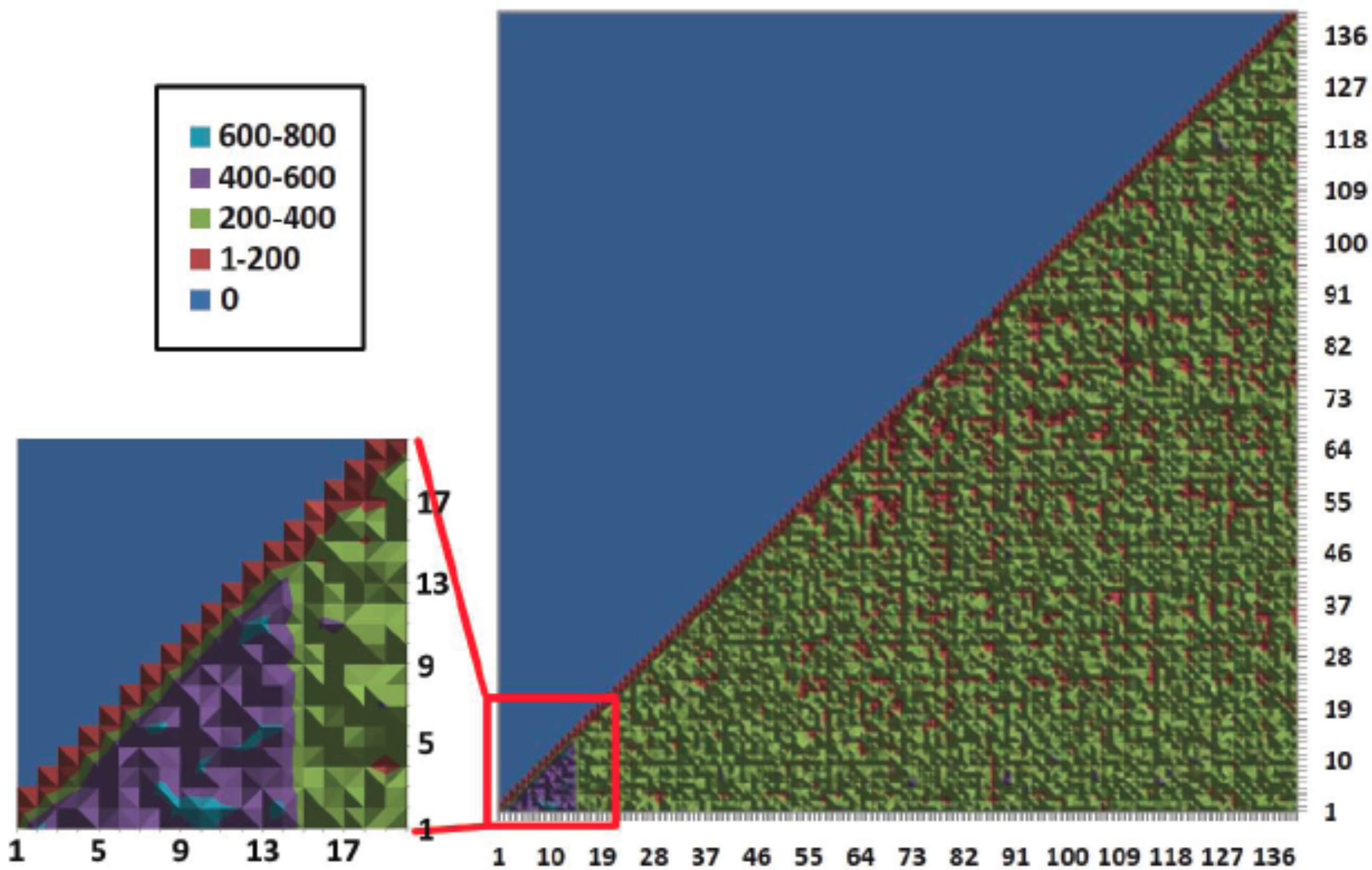
5 secret icons appear (**duplications** allowed).

Answer *= 5 mod 4 = 1, choose '0/1'*

Challenges are designed such that *0/1 and 2/3 appear with the same probability*, which is different from of the uniform distribution of secret pictures appearing in a challenge.

SMU SINGAPORE MANAGEMENT UNIVERSITY

Statistical bias in responses (2/2)



Expected # of secret pairs for response *'0/1'* is *2.416.*

Expected # of secret pairs for response *'2/3'* is *1.816.*

Fig shows pair-based scores after 20000 rounds.

Implications: *A challenge based on counting problem must use the form r = x mod 2; otherwise the pair-wise bias appears. This is true for all counting based challenges.*

SMU SINGAPORE MANAGEMENT UNIVERSITY

Usability score in the quantitative analysis framework

- Cognitive workload: HP(C)
  - Measured by sum of the **reaction time** of each atomic operations (e. g., counting, mod, simple arithmetic)
  - How fast can an **average** human solve the challenge?
    - The time limit is implementation-independent
- Memory demand: HP(M)
  - Measured by # of elements memorized X difficulty factor of the specific memory retrieval operation
    - **Recall** is much more difficult than **recognition**
- HP = HP(C) X HP(M)

SMU
SINGAPORE MANAGEMENT UNIVERSITY