On designing an unaided authentication service with threat detection and leakage control for defeating opportunistic adversaries

Nilesh CHAKRABORTY, Samrat MONDAL

Frontiers of Computer Science, DOI: 10.1007/s11704-019-9134-9

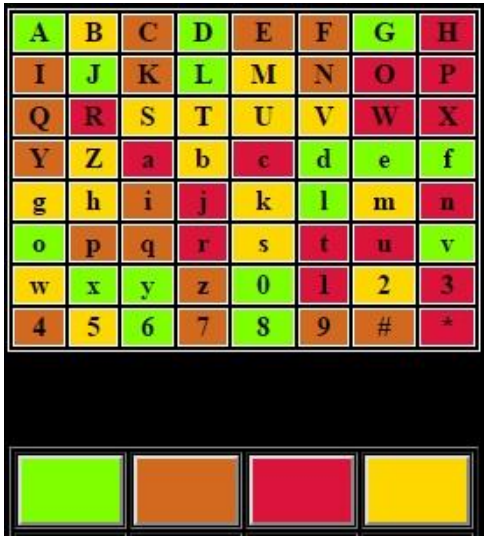
Problem & Idea

- The password of a user can often be captured under the recording attack.
- Since 1991 [Matsumoto and Imai, Eurocrypt-1991], the researchers are trying to fix this vulnerability based on the passive key entry mechanism.
- Addressing this challenge becomes particularly hard (in terms of balancing security and usability aspects) when a defense solution does not depend on any auxiliary link.
- Through this work, the authors have designed an unaided authentication protocol, which not only prevents, but also detects the activity of the recording attackers.
- The proposed work deals with opportunistic adversaries, who records the login credentials when gets an opportunity (‡).

Highlights

To the best of the authors' believe, the proposed work is the first one which detects the activity of the recording attackers.

‡ The concept of opportunistic adversary is very relevant in todays' mobile world.



User interface of the proposed framework

Outcomes

Method	LR	Avg. login time skilled user (sec)	Avg. login time (sec) all user	Error rate (%) all user	CWR (sec)	MD	HP = CWR × LR ×MD ($\times 10^2$)
CHC	5	56	65.5	17.1	9.326	16.89	7.87
PAS	4	33.44	41.52	15.2	6.837	13.51	3.69
S3PAS	4	36.56	50.8	15.7	10.597	13.51	5.55
ColorPIN	4	7.71	13.37	15.6	1.2671	27.02	1.36
var–BW	4	5.22	9.9	7.5	0.9349	13.51	0.5
TGPM ⊛	1+6	2.4 + 7.86	4.2 + 11.29	8.6	1.2329	20.27 + 27.02	0.2 + 1.99

Comparison among the methods from the usability perspectives (LR = login rounds)

Method	Secret length (ℓ)	Total elements (n)	Window size (w)	Password space	LR	Session resiliency	Pr[Threat detection]
CHC	5	112	83	1.341×10^8	5	3	0
PAS	4+2s	N/A	13	4.225×10^5	4	9+s	0
S3PAS	4	94	94	7.9×10^7	4	8	0
ColorPIN	8	N/A	3	2.4×10^5	4	3	0
var–BW	4	10	1	1×10^4	4	3	0
TGPM ⊛	6+8	64	1	1.2×10^{19}	1+6	24	0.75

Comparison among the methods from the security perspectives (LR = login rounds)

- The above results show that proposed method (TGPM) significantly improves the situation both from security and usability perspectives.
- Highest session resiliency among the existing usable authentication systems for defeating opportunistic adversary, security against password leakage from a single compromised server are the other highlights of the proposed system to eliminate the long-standing security-usability conflicts that are considered intractable in the existing literature.