




Usage of Theoretical Computer Science in IT Security

Dominik Breitenbacher

Faculty of Information Technology, BUT

xbreit00@stud.fit.vutbr.cz



Authentication Protocols making use of Context- Free Grammar Guessing Strings

Authentication Protocol – Reusable passwords

- Reusable passwords are heavily used
- Weakest link of security
- Passwords are usually poorly chosen
- If chosen correctly – still can be sniffed
- Solution – One-time passwords
- One-time passwords are used only once and cannot be used again

Worst Passwords of 2014

Rank	Password
1	123456
2	password
3	12345
4	12345678
5	qwerty

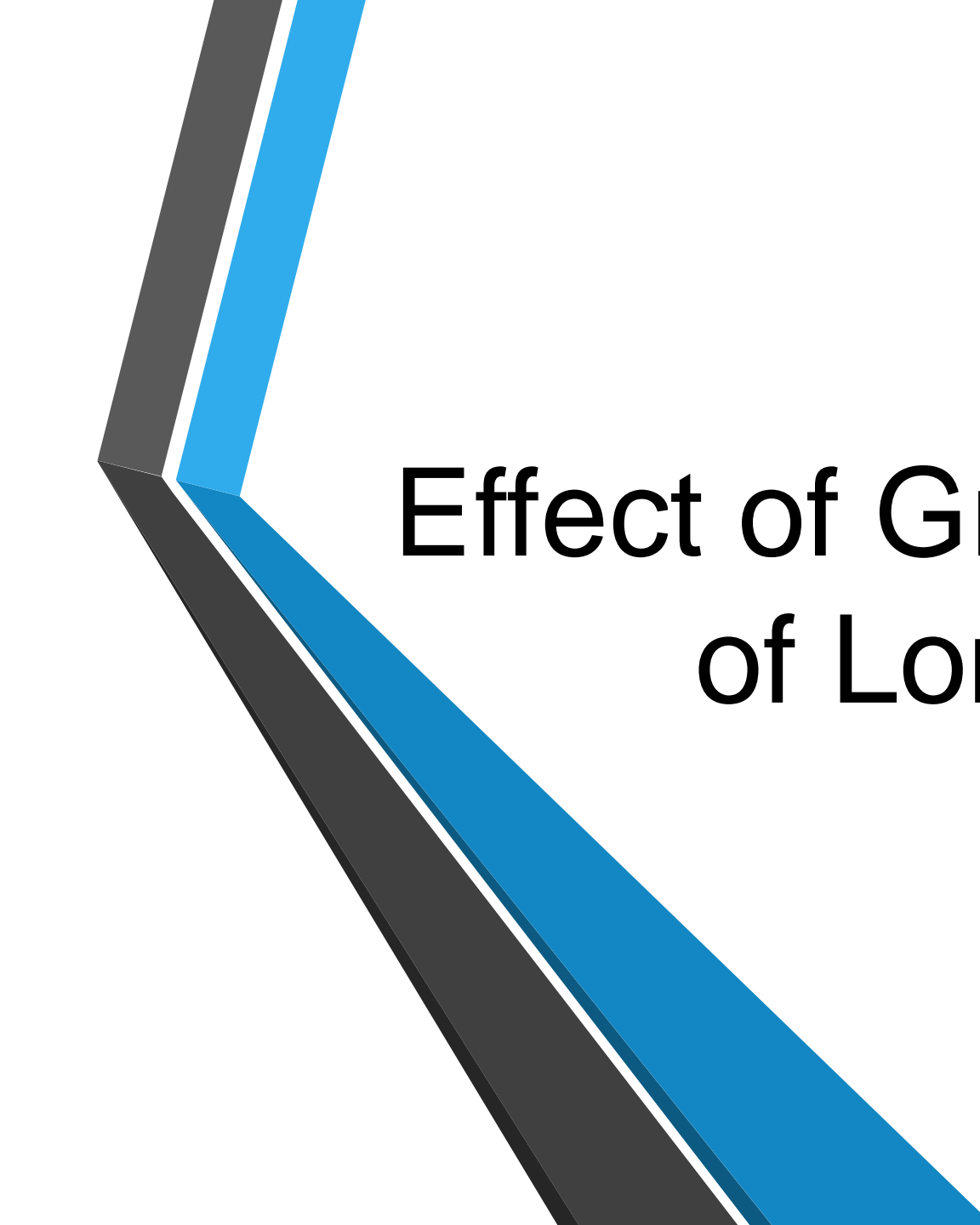
Source: <https://www.teamsid.com/worst-passwords-of-2014/>

Authentication Protocol – Password Generation and Verification

- Generator and Verifier have k independent CFGs that they can use
- CFGs are same on the both sides
- Generator randomly selects n grammars and generates n strings
- One-time password is concatenation of those n strings
- On the verifier side, the one-time password is split into n substrings
- Substrings are parsed by CFGs
- If substrings are successfully parsed, user is authenticated

Authentication Protocol – Provided Security and its limitations

- Using one grammar is insecure
- Attacker can use learning algorithms for password guessing
- The more grammars are used, the more the protocol is secure
- Weak against replay attack



Effect of Grammar on Security of Long Passwords

Password Cracking – Long Passwords

- Passwords are usually easy to guess
- To make the passwords more secure, user has to follow restrictions
- This form of password is not comfortable for user
- Alternative – long text-based passwords
- Long passwords usually contain some phrase or sentence
- This may make them vulnerable to grammar aware password crackers

Password Cracker – Implementation Details

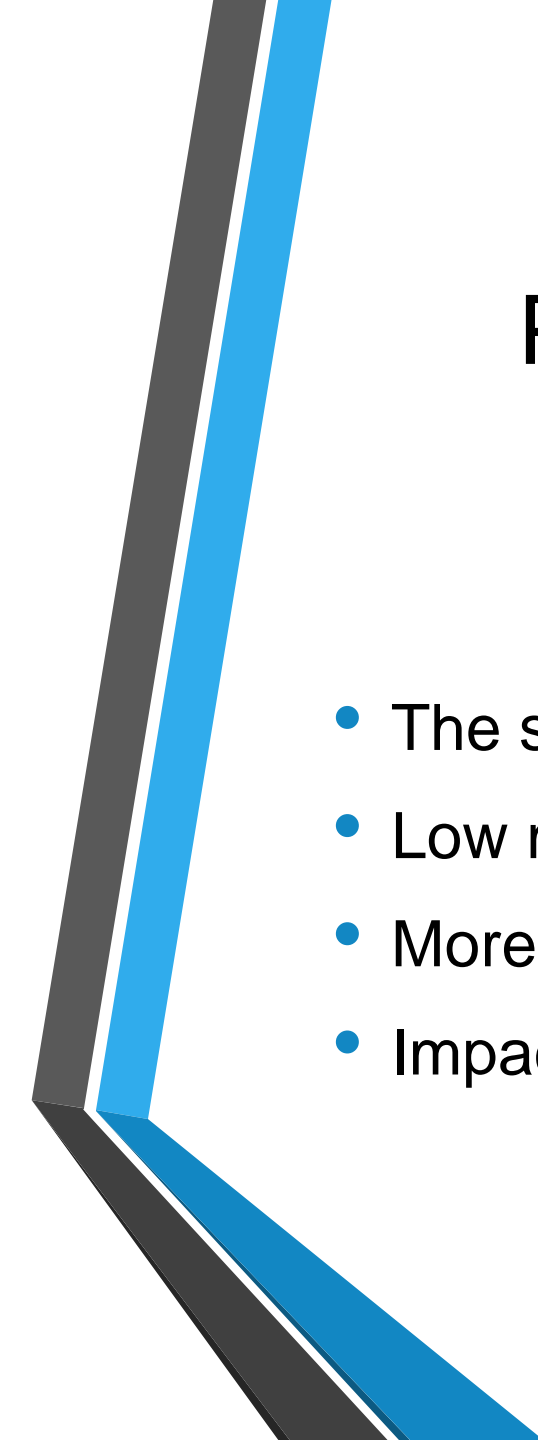
- At first the authors decided to use Regular Grammars
- Part-of-Speech tagging technique for grammatical rules modeling
- Only proper grammatical rules will be used (Determiner Adjective Noun)
- For this purpose the Brown Corpus is used
- This helps to dramatically reduce the search space
- Based on this the grammar aware password cracker has been developed

Password Cracking – Efficiency of Current Traditional Password Crackers

Experiment	P16 %Cracked	P16S %Cracked	Total Guesses	Session Completed
JTR L-8	13.60	6.90	2.31E10	YES
JTR GW25-8	20.50	34.70	2.48E12	YES
Weir LASCII	12.00	4.80	1.07E12	NO
JTR Incremental	0.00	0.00	2.48E12	NO


Password Cracking – Efficiency of Implemented Grammar Aware Password Cracker

Guesses	P16S %Cracked with BWeb	P16S %Cracked with BWeb90	%Exclusive
5.0E10	9.7	18.7	4.8
1.0E12	14.5	25.0	9.0
2.5E12	15.2	27.0	10.4
10E12	20.1	29.1	11.8
40E12	25.6	35.4	13.8



Password Cracking – Paper Conclusion

- The second most efficient cracker for long password cracking
- Low memory consumption
- More than 10% passwords exclusively cracked
- Impact on security policy



Revolver: An Automated Approach to the Detection of Evasive Web-based Malware

Malware Detection – Data Collection and Abstract Syntax Tree Extraction

- External tool for malware detection is used
- Not dependent on any specific external tool
- After data collection the Abstract Syntax Trees (AST) are extracted
- Each AST is stored to the dataset with its classification result
- Also for each node of the AST its position in the statement execution order is stored

Malware Detection – Similarity detection

- For each AST up to k its malicious neighbors are found.
- The similarity is measured between the given AST and its neighbors
- Output is a list of similar pairs
- Each pair is classified to one of five possible groups

Malware Detection – Classification Classes

- Evolution group
 - Two malicious scripts
 - Not much interesting for Revolver
- Data-dependency group
 - Packers
 - Also not much interesting for Revolver
- General Evolution group
 - Both scripts are changed
 - Due to the changes one of them is no longer detectable by the external detection tool

Malware detection – Classification groups II

- JavaScript injection group
 - Malware code injected to the benign script
- Evasion group
 - Script is improved by evasion techniques
 - The most interesting group for Revolver

Malware Detection – Collected data

- External detection tool was able to process **591 543** scripts in a single day
- External detection tool collected and analyzed **20 732 766** benign and **186 032** malicious scripts
- **705 472** unique benign and **5 701** unique malicious ASTs were extracted.

Malware Detection – Results

Category	Similar Scripts	Number of groups by malicious AST
Data-dependencies	101 039	701
JavaScript Injections	6 996	475
Evasions	4 147	155
General Evolutions	2 490	275
Total	114 672	1 604

- 5 out of 4 147 classified evasions are false positives.
- 4 of them classified as evasion, because they stop due to errors like missing dependencies etc.

Summary

- 3 articles closely described
- 3 IT security topics discussed
- 3 different subjects of theoretical computer science utilized in presented works



Thanks for the attention!

References

- [1] SINGH, Abhishek; DAGON, David; DOS SANTOS, Andre Luiz Moura. Authentication Protocols making use of Context free Grammar: Guessing Strings. 2004.
- [2] RAO, Ashwini; JHA, Birendra; KINI, Gananand. Effect of grammar on security of long passwords. In: *Proceedings of the third ACM conference on Data and application security and privacy*. ACM, 2013. p. 317-324.
- [3] KAPRAVELOS, Alexandros, et al. Revolver: An Automated Approach to the Detection of Evasive Web-based Malware. In: *USENIX Security*. 2013. p. 637-652.