The Attackers' Principles

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

Alexandre Dulaunoy

alexandre.dulaunoy@circl.lu

January 8, 2016

Introduction or Disclaimer

- We operated honeynets and honeypots the past 6 years and we collected "some" data
- Based on the analysis of "some" data, 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

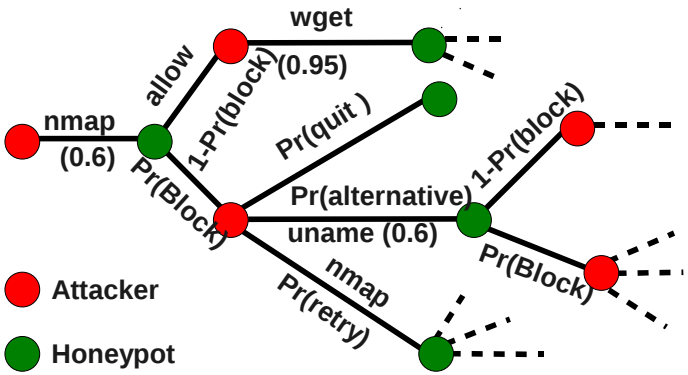
Principles are based on the recurring patterns discovered in the various attacks.

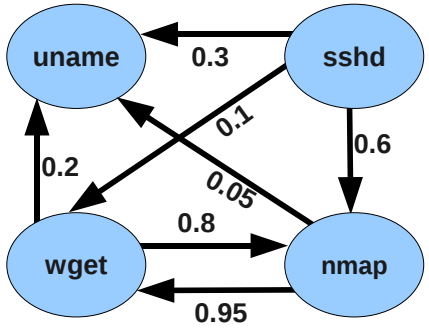
The ssh password brute-force case

- 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

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 Honeypots 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

Scanning Internet

- Scanning networks is an old but effective technique to find vulnerable systems.
  - Scanning NoSQL databases[1] was a source of recent leak of information (December 2015).
  - Finding vulnerable and/or backdoored routers [2], Juniper ScreenOS case is a critical example (December 2015).
  - Attackers find vulnerable devices to relay their traffic (e.g. Dridex malware using SSL/TLS relay over misconfigured routers).
  - Finding vulnerable administration panels of CMS (e.g. WordPress, Joomla!, ...).

[1] https://www.circl.lu/pub/tr-32/
[2] https://www.circl.lu/pub/tr-42/

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

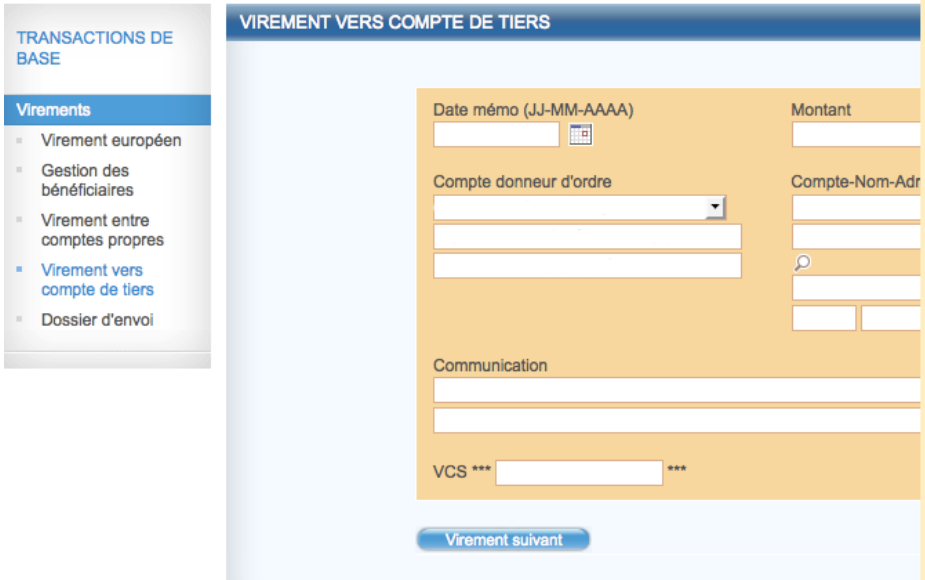
- Internet browsers try to improve the situation for SSL website
- Is it really an improvement? or even more confusion?
- If confusion is still there, the attacker is still able to collect passwords...

image from bitofprevention.com

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



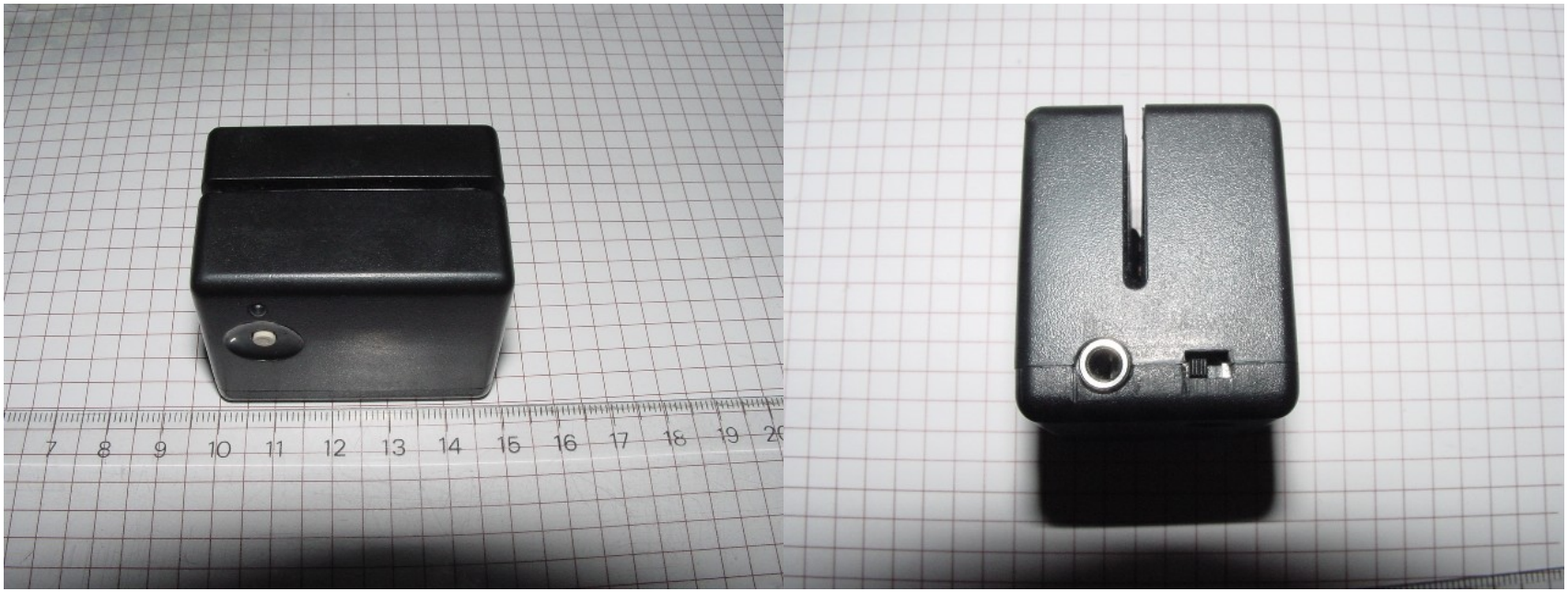
Torpig or Silentbanker are well-known trojan and they know the different bank forms.

- Avoid the OTP by compromising directly the browser
- Even with the help of the user. Have you ever installed a toolbar 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

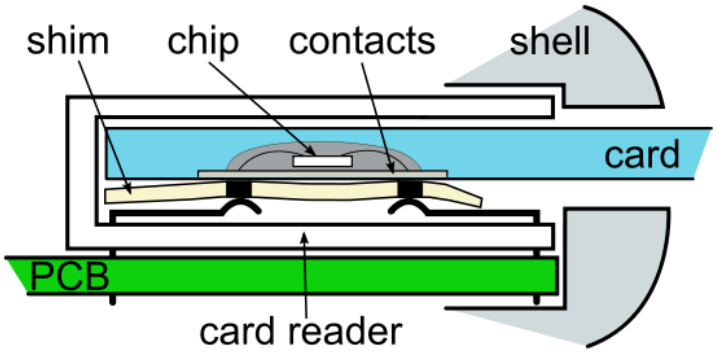
- Use the principle of the weakest link
  - Today, bank users have an OTP token to use online banking
  - Attackers won't defeat the OTP scheme, they just hook on the DOM of the Internet browser (e.g. Torpig or SilentBanker)
  - Users don't even need a vulnerable browser, they just install extension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

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 compability

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

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
- 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

Q and A

- Thanks for listening.
- alexandre.dulaunoy@circl.lu
- a small quiz : how can you defeat a "Gas Protection Unit" in an ATM?