Implémentation de fonctions en éponge

Amélie Guémon
Ida Tucker
<amelie.guemon@etu.u-bordeaux.fr>

Master CSI, Université de Bordeaux, France

22 avril 2016

Plan

1. Merkle-Damgård et ses applications
2. Faiblesse de Merkle-Damgård
3. Fonctions de hachage en éponge

Plan

1. Merkle-Damgård et ses applications
2. Faiblesse de Merkle-Damgård
3. Fonctions de hachage en éponge

Internet est attaqué ! ! !

```
Newsgroups: comp.risks
Subject: Virus on the Arpanet - Milnet
<Stoll@DOCKMASTER.ARPA> Thu, 3 Nov 88 06:46 EST

Hi Gang!

It's now 3:45 AM on Wednesday 3 November 1988. I'm tired, so don't
believe everything that follows... Apparently, there is a massive
attack on Unix systems going on right now.

I have spoken to systems managers at several computers, on both the
east & west coast, and I suspect this may be a system wide problem.
Symptom: hundreds or thousands of jobs start running on a Unix system
bringing response to zero.

[...]

This virus is spreading very quickly over the Milnet. Within the past
4 hours, I have evidence that it has hit >10 sites across the country,
both Arpanet and Milnet sites. I suspect that well over 50 sites have
been hit. Most of these are "major" sites and gateways.

[...]

This is bad news.
```

Plan

1. Merkle-Damgård et ses applications

2. Faiblesse de Merkle-Damgård

3. Fonctions de hachage en éponge

On continue ! ! !

Ce slide est quasiment vide !

Plan

1. Merkle-Damgård et ses applications

2. Faiblesse de Merkle-Damgård

3. Fonctions de hachage en éponge

Livres et références I

- Chris Anley, John Heasman, Felix Linder, and Gerardo Richarte.
  The Shellcoder's Handbook : Discovering and Exploiting Security Holes.
  John Wiley & Sons, 2nd edition, 2007.

- Jon Erickson.
  Hacking : The Art of Exploitation.
  No Starch Press, 2nd edition, 2007.

- Greg Hoglund and Gary McGraw.
  Exploiting Software : How to Break Code.
  Software Security Serie. Addison Wesley, 2004.

- Jamie Hoglund, Greg et Butler.
  Rootkits : Subverting the Windows Kernel.
  Software Security Serie. Addison Wesley, 2005.

- Randall Hyde.
  The Art of Assembly Language.
  No Starch, 2003.

Livres et références II

- Joseph Kong.
  Designing BSD Rootkits : An Introduction to Kernel Hacking.
  No Starch, 2007.

- Robert Love.
  Linux Kernel Development.
  Sams, 2nd edition, 2005.

- Robert Love.
  Linux System Programming : Talking Directly to the Kernel and C Library.
  O'Reilly Media, 2007.

- Robert C. Seacord.
  Secure Coding in C and C++.
  SEI Series. Addison Wesley, 2005.

- Peter Szor.
  The Art of Computer Virus Research and Defense.
  Addison Wesley, 2005.

Questions ?