DieHarder:
Securing the Heap

Gene Novark & Emery Berger
University of Massachusetts, Amherst

[originally presented at CCS 2011]
DieHard: Probabilistic Memory Safety for C/C++ Programs [PLDI 2005]

Direct inspiration for Windows 7’s Fault-Tolerant Heap (2009)
DieHard: Probabilistic Memory Safety for C/C++ Programs [PLDI 2005]
Buried deep beneath hills are the impregnable forts shown in the above drawing. Even railways are provided for.

INVISIBLE and sunk beneath the rolling and wooded terrain in Lorraine is a great underground fortification system, 300 miles...
World’s Greatest Underground Fortifications Guard

Buried deep beneath hills are the impregnable forts shown in the above drawing. Even railways are provided for.

INVISIBLE and sunk beneath the rolling and wooded terrain in Lorraine is a great underground fortification system—200 miles...
Solid black line shows location of 200 mile system of French underground forts, opposite disputed Saar basin.
THE HEAP IS NEITHER ANIMAL NOR MAN—BUT A HALF-WORLD CREATURE THAT IS A BAD PRODUCT OF WORLD WAR #1, WHEN THE BODY OF A HALF-DEAD GERMAN FLYER, BARON VON EMMELMAN, UNITED ITSELF WITH SWAMP VEGETATION.... AND IN THE PROCESS HAS CREATED THIS PLANT-LIKE THING THAT HAS THE POWER TO REMEMBER—IF NOT TO THINK VERY EFFICIENTLY.... AND NOW....
sensitive data / metadata
All data / metadata sensitive
guard / unmapped page
Microsoft Office PowerPoint has encountered a problem and needs to close. We are sorry for the inconvenience.

The information you were working on might be lost. Microsoft Office PowerPoint can try to recover it for you.

- Recover my work and restart Microsoft Office PowerPoint

Please tell Microsoft about this problem.
We have created an error report that you can send to help us improve Microsoft Office PowerPoint. We will treat this report as confidential and anonymous.

What data does this error report contain?
Why should I report to Microsoft?

Send Error Report  Don't Send
Address-space layout randomization
char * f = new char[10];
char * f = new char[10];
char * f = new char[10];

heap metadata

object free space
char * f = new char[10];

object

[object]

free space

[free space]

heap metadata

(heap metadata)
≈ 4-5 bits of entropy
Maximal entropy: 
\[ \log N \text{ bits (e.g., } \approx 25-30) \]
Allocation space (randomly placed pages)
Die HARDER:
Securing the Heap

Gene Novark & Emery Berger
University of Massachusetts, Amherst