The UMBC Center for Information Security and Assurance

Finding privacy leaks and stolen data with bulk data analysis and optimistic decoding

Dr. Simson Garfinkel, Naval Postgraduate School

12-1pm Friday December 6, 2013, 229 ITE Building

Modern digital forensics tools are largely based on the recovery and analysis of files. This talk explores how identity information such as email addresses, credit card numbers, and other of information can be more efficiently found using bulk data analysis, and how results are significantly improved through the use of optimistic decompression. Together, these techniques can find important information on computer media that are ignored by the majority of today's digital forensics tools. This talk presents the results of a study of roughly 5000 hard drives purchased on the secondary market and shows how different kinds of data formats can be traced to different kinds of privacy leaks and coding errors. It shows how the results were generated using bulk_extractor, an easy-to-use open source digital forensics tool. Finally, it shows how bulk_extractor was extended to detect data obscured with a simple steganographic technique (XOR 255), and how a subsequence re-analysis of the research corpus found significant use of the technique in commercial software, malware, and by at least one computer criminal.

Simson L. Garfinkel is an Associate Professor at the Naval Postgraduate School. Based in Arlington VA, Garfinkel's research interests include digital forensics, usable security, data fusion, information policy and terrorism. He holds six US patents for his computer-related research and has published dozens of research articles on security and digital forensics. Garfinkel is the author or co-author of fourteen books on computing. He is perhaps best known for his book Database Nation: The Death of Privacy in the 21st Century. Garfinkel's most successful book, Practical UNIX and Internet Security (co-authored with Gene Spafford), has sold more than 250,000 copies and been translated into more than a dozen languages since the first edition was published in 1991. Garfinkel received three Bachelor of Science degrees from MIT in 1987, a Master's of Science in Journalism from Columbia University in 1988, and a Ph.D. in Computer Science from MIT in 2005.

Host: Dr. Alan T. Sherman (sherman@umbc.edu)

http://bit.ly/UMBCtalks