

24th USENIX Security Symposium

AUGUST 12-14, 2015 • WASHINGTON, D.C.



HOME

ATTEND

PROGRAM

ACTIVITIES

PARTICIPATE

SPONSORSHIP

ABOUT

SPONSORS

Platinum Sponsor





Get more Help Promote graphics!

Facebook

POLICIES

Statement on

Environmental

Event Code of Conduct

Responsibility Policy

Conference Network Policy

GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies

Authors:

Mordechai Guri, Assaf Kachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky, and Yuval Elovici, Ben-Gurion University of the Negev

Abstract:

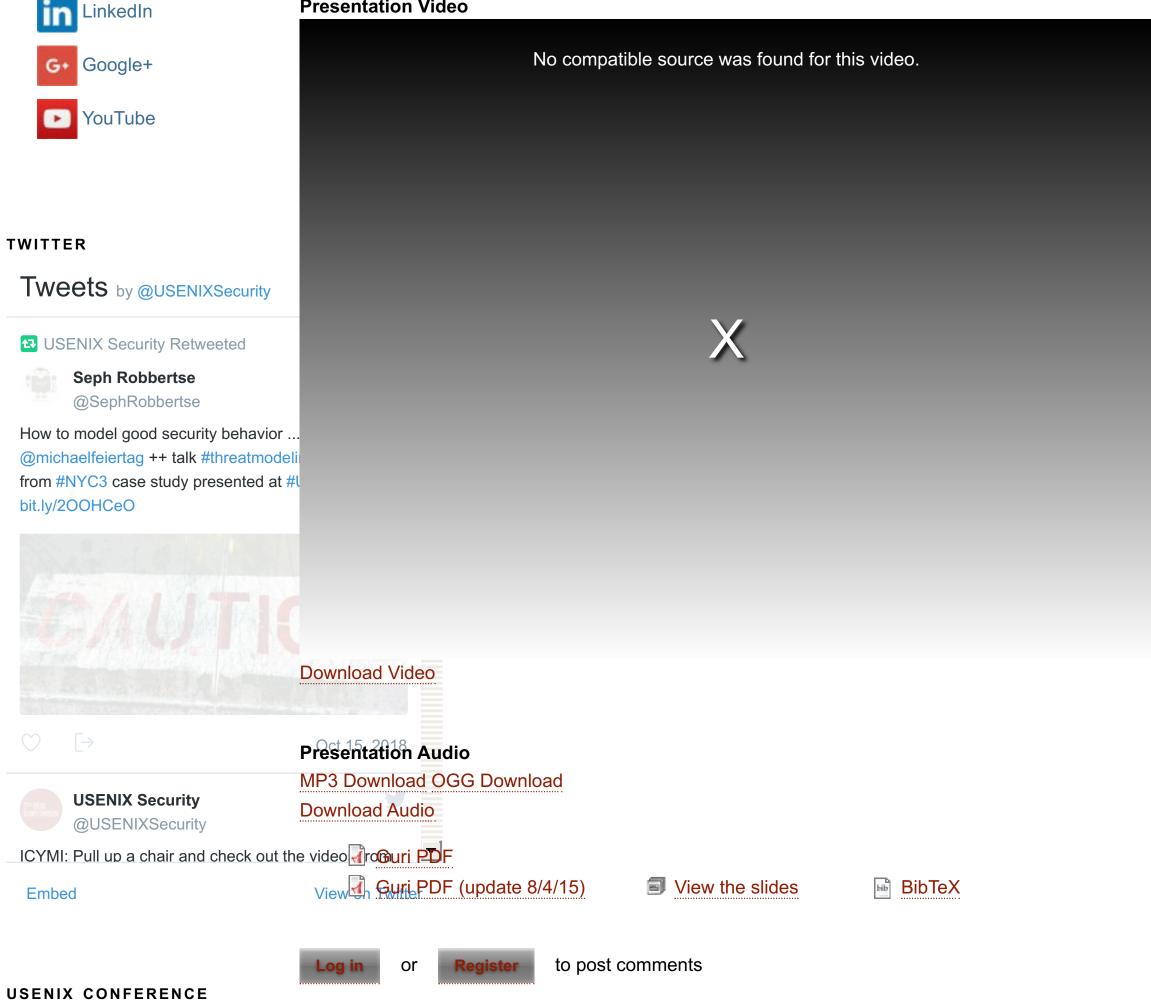
Air-gapped networks are isolated, separated both logically and physically from public networks. Although the feasibility of invading such systems has been demonstrated in recent years, exfiltration of data from air-gapped networks is still a challenging task. In this paper we present GSMem, a malware that can exfiltrate data through an air-gap over cellular frequencies. Rogue software on an infected target computer modulates and transmits electromagnetic signals at cellular frequencies by invoking specific memory-related instructions and utilizing the multichannel memory architecture to amplify the transmission. Furthermore, we show that the transmitted signals can be received and demodulated by a rootkit placed in the baseband firmware of a nearby cellular phone. We present crucial design issues such as signal generation and reception, data modulation, and transmission detection. We implement a prototype of GSMem consisting of a transmitter and a receiver and evaluate its performance and limitations. Our current results demonstrate its efficacy and feasibility, achieving an effective transmission distance of 1-5.5 meters with a standard mobile phone. When using a dedicated, yet affordable hardware receiver, the effective distance reached over 30 meters.

For more information, watch the video GSMem Breaking The Air-Gap on YouTube.

Open Access Media CONNECT WITH USENIX

USENIX is committed to Open Access to the research presented at our events. Papers and proceedings are freely available to everyone once the event begins. Any video, audio, and/or slides that are posted after the event are also free and open to everyone. Support USENIX and our commitment to Open Access.

Presentation Video



facebook

Platinum Sponsors

Gold Sponsors



Symantec.

Open access to the USENIX Security '15 videos sponsored by Symantec.

Silver Sponsors







Bronze Sponsors





General Sponsors

OXFORD

Media Sponsors & Industry Partners





























