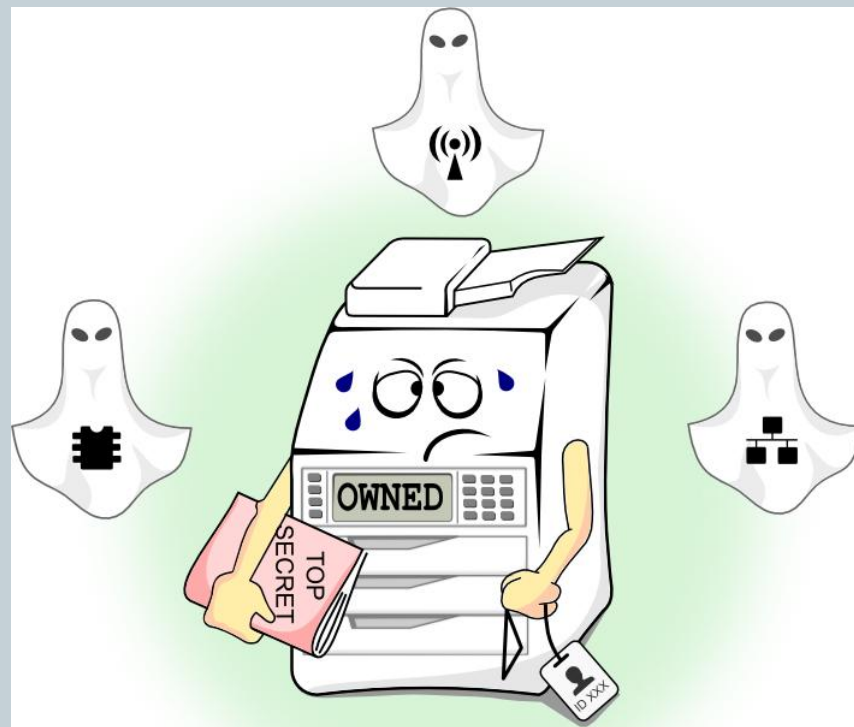


Hacking printers: for fun and profit



Impressum



- [Andrei Costin](#)
- Author of MFCUK
 - [MiFare Classic Universal toolKit](#)
- Day-time programmer (after-8pm type of hobbyist hacker)
- Generally interested in (but especially in last 2 bullets):
 - Programming/hacking: RFID, GSM, biometrics, embedded
 - Almost everything which:
 - ✦ Is connected to networks/communications lines
 - ✦ Have smart-cards (contact and contactless)
 - ✦ Have crypto involved somewhere down the line
 - ✦ Is or should be secure
 - Corporate/Enterprise IT support software & security
 - [TEMPEST](#) and [ISS](#)

Abstract



- While more and more new devices (routers, smartphones, etc.) are getting connected to our SOHO/enterprise environments, all-colour hats are getting plenty of focus on their security: defend and harden on one side; exploit and develop malware on the other.
- However, a special class of network devices (specifically network printers/scanners/MFPs), which are networked for more than 15 years, are constantly out of the modern security watchful eye.
- And even though we entrust them even the most confidential documents or the most sacred credentials (LDAP, PINs, RFID badges, etc.), we don't realize closely how weak and unsecured they are, despite the few minor security bulletins that started to pop-up here and there in the recent few months.
- In this presentation, we will try to analyze the reasons why hacking network printers/MFPs is a reasonable and accomplishable idea. Also, we will take a look at current state of (weak) affairs in the vulnerability and security research available. Then we will try to envision types of possible exploitation scenarios, backed-up with a printer remote-exploit demo. We will conclude the presentation with possible solutions and what can be done to protect ourselves as well as our network environments.

Disclaimer*



- No Warranties or Liability. Information is provided as-is, though every effort has been made to ensure the accuracy of the information presented. Author of the presentation is not legally liable under any circumstances for any damages such as but not limited to (including direct, indirect, incidental, special, consequential, exemplary or punitive damages) resulting from the use or application of the presented information.
- Unless explicitly noted in forms such as but not limited to "the XYZ Company says", etc., the opinions expressed in this presentation are solely and entirely my own. They should not be interpreted as representing the positions of any organization (past, present, future, existent, non-existent, public, private, or otherwise) with which I may or may not have been, are or are not, or will or will not be affiliated at some time in the past, present, or future.
- All trademarks and registered names are the property of their respective owners.
- This presentation: © 2010, Andrei Costin. Released under:



• *big fat one – because everybody *loves* fingerprints

\H1B%-12345X@PJL JOB “HackingPrinters”



- This presentation is about:
 - Hacking “the PC inside printers/MFPs”
 - ✦ Why would someone hack a printer/MFP
 - ✦ How would someone hack “the PC inside printers/MFPs”?
 - ✦ How easy/feasible is MFP *firm*ware creation and exploitation
 - ✦ How to protect yourself and your so-much-loved MFP?
 - Laying foundation for further community security research/development/PoC
- This presentation is NOT about:
 - Printers’ display hack (RDYMSG, OPMSG, STMSG)
 - Printers’ embedded web-server hacks
 - Printers’ SNMP configuration hacks
 - Exhaustive guide to hack every and last MFP (not yet!)