THWARTING EVIL MAID ATTACKS: PHYSICALLY UNCLONABLE FUNCTIONS FOR HARDWARE TAMPER DETECTION

HACK IN THE BOX – MALAYSIA – OCTOBER 2013

ERIC MICHAUD ERIC@RIFTRECON.COM

RYAN LACKEY RYAN@CRYPTOSEAL.COM

WHO: ERIC MICHAUD

- Co/Founder of TOOOL.US/HacDC/PS:One/Rift Recon
- Self-taught engineer/machinist/hacker/CEO
- Breaker of systems w/ a physical component and organizations
- Broke many high security locking systems and a voting machine
- Director of hardware curation @ ExploitHub.com
- Previously of Argonne National Laboratory – Vulnerability Assessment Team
- Brought Locksport to Malaysia – Hopefully Serbia?

WHO: RYAN LACKEY

- Co-Founder of HavenCo, world's first offshore datahaven, in 2000.
- Worked on several anonymous blinded ecash systems
- Security consultant in payments, HW key management, and other clients
- Founded and ran a satellite/wireless networking startup in Iraq/Afghanistan
- Operated US military medical imaging communications in Iraq/Afghanistan
- Co-founder of CryptoSeal, a Trusted computing startup in Silicon Valley

THE PROBLEM:
PHYSICAL ATTACKS SUBVERT HIGHER LAYERS

RIFT RECON

THE PROBLEM:
PHYSICAL ATTACKS SUBVERT HIGHER LAYERS

RIFT RECON

HOW IT WORKED BEFORE PERVASIVE COMPUTING

RIFT RECON

HOW IT WORKED BEFORE PERVASIVE COMPUTING

RIFT RECON

HOW IT WORKED BEFORE PERVASIVE COMPUTING

RIFT RECON

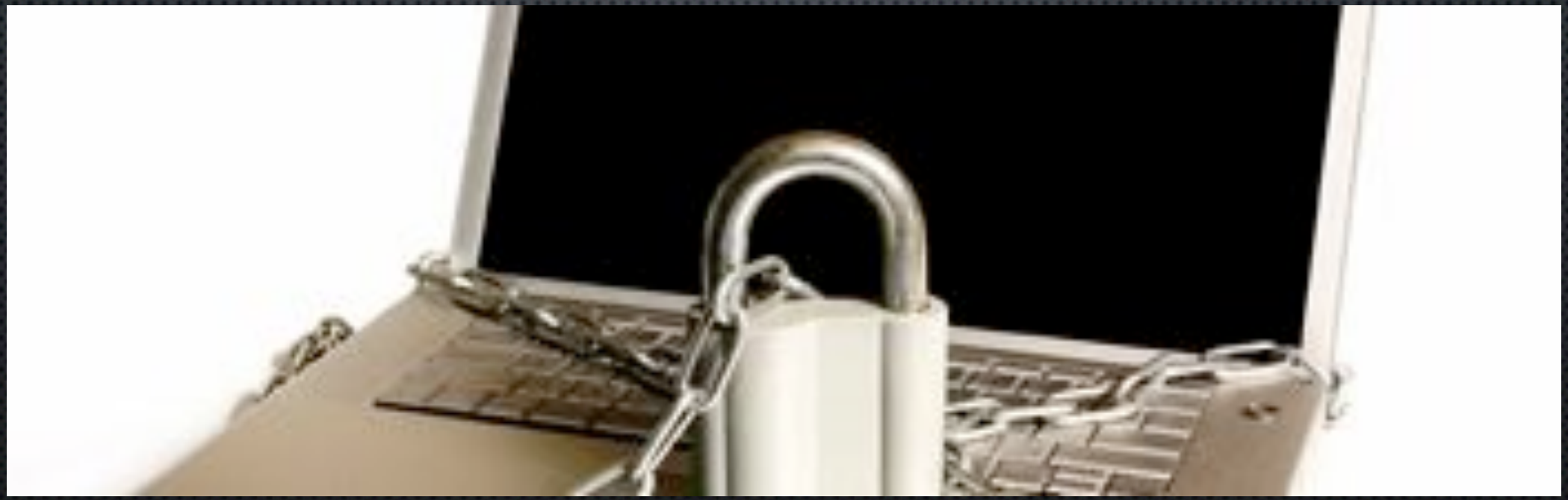
WHAT CHANGED?

RIFT RECON

THREAT MODEL

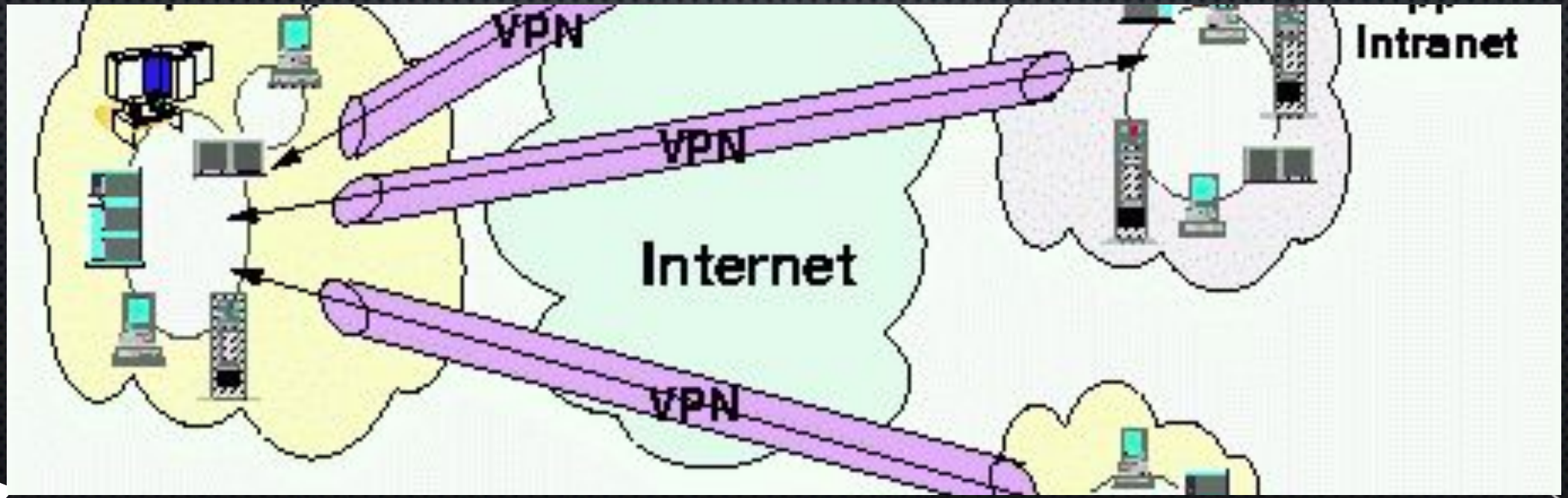
RIFT RECON

BEST PRACTICE: FULL DISK ENCRYPTION



RIFT RECON

BEST PRACTICE: VPN AND MDM



BEST PRACTICE: TRAVEL CLEAN

RIFT RECON

BEST PRACTICE: DEDICATED TRAVEL POOL

RIFT RECON

BEST PRACTICE: SEALS

RIFT RECON

BEST PRACTICE: FORENSIC TEARDOWN

RIFT RECON

A STATIC SOLUTION:
USE-TIME REMOTE-VERIFIED PHYSICAL SEALS

RIFT
RECON

RIFT
RECON
RIFT
RECON

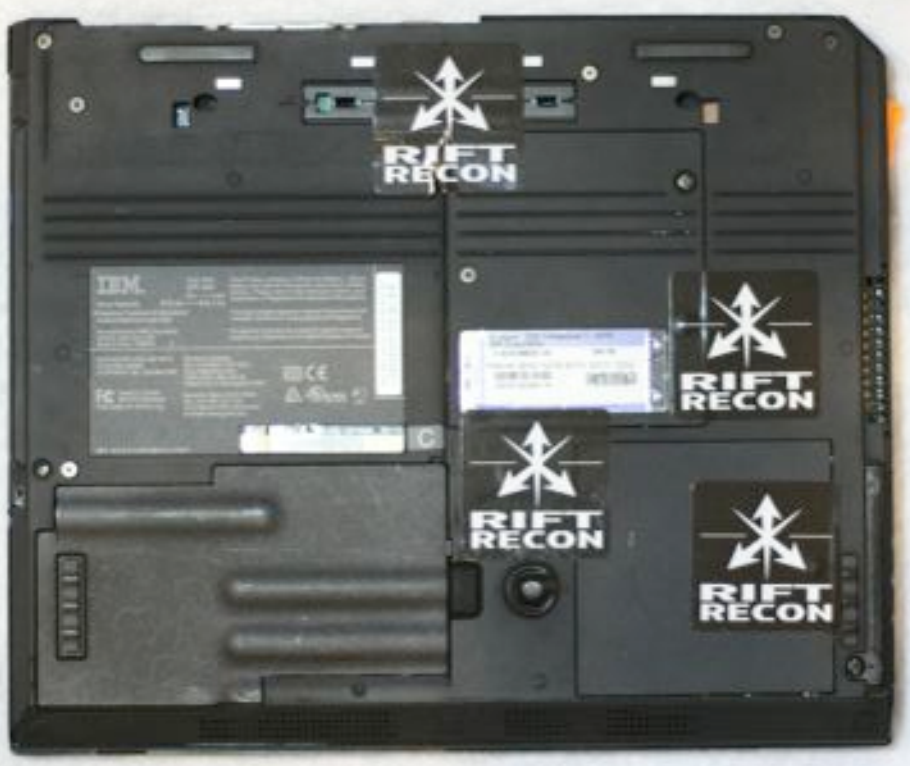
RIFT
RECON
RIFT
RECON

RIFT
RECON

RIFT RECON

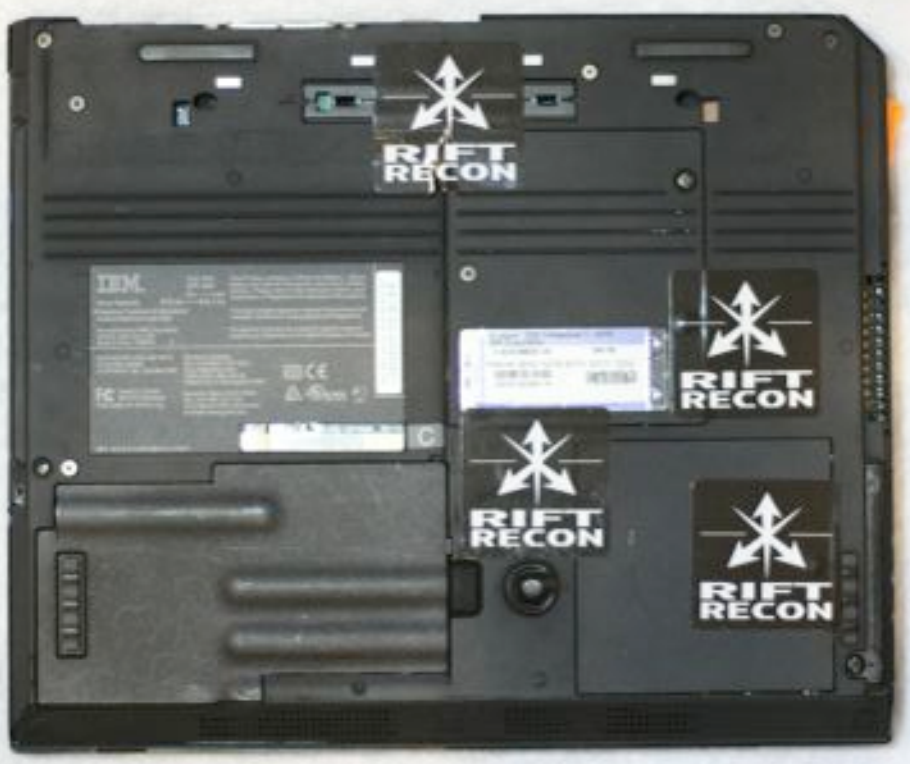
RIFT RECON


RIFT
RECON
RIFT
RECON
RIFT
RECON
RIFT
RECON


RIFT
RECON
RIFT
RECON
RIFT
RECON
RIFT
RECON

RIFT RECON

RIFT RECON



RIFT RECON

THREATS TO USE-TIME STATIC SEALS

RIFT RECON

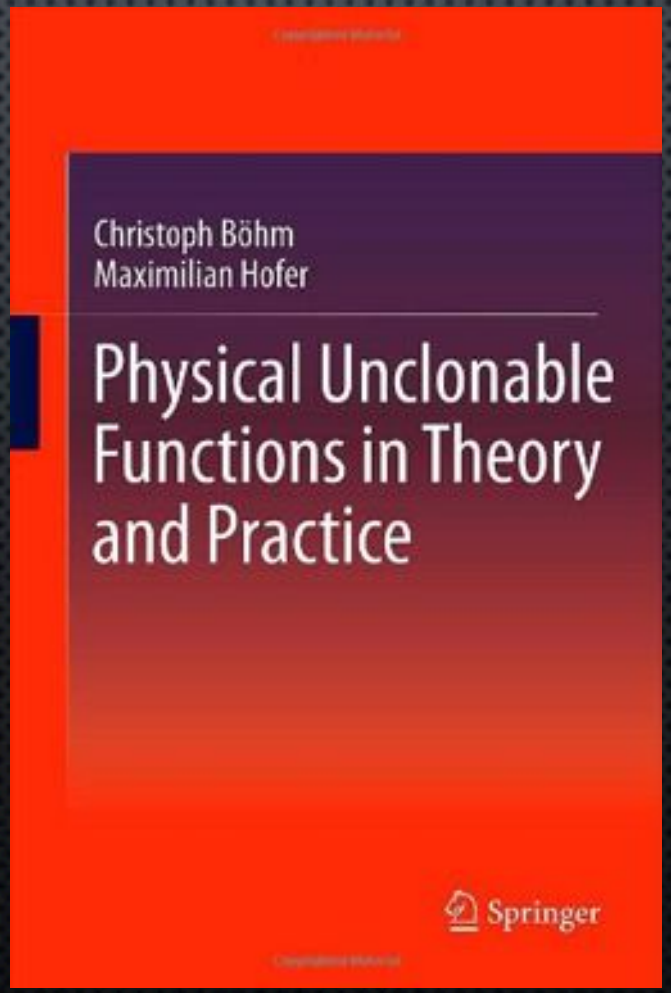
THREATS TO USE-TIME STATIC SEALS

RIFT RECON

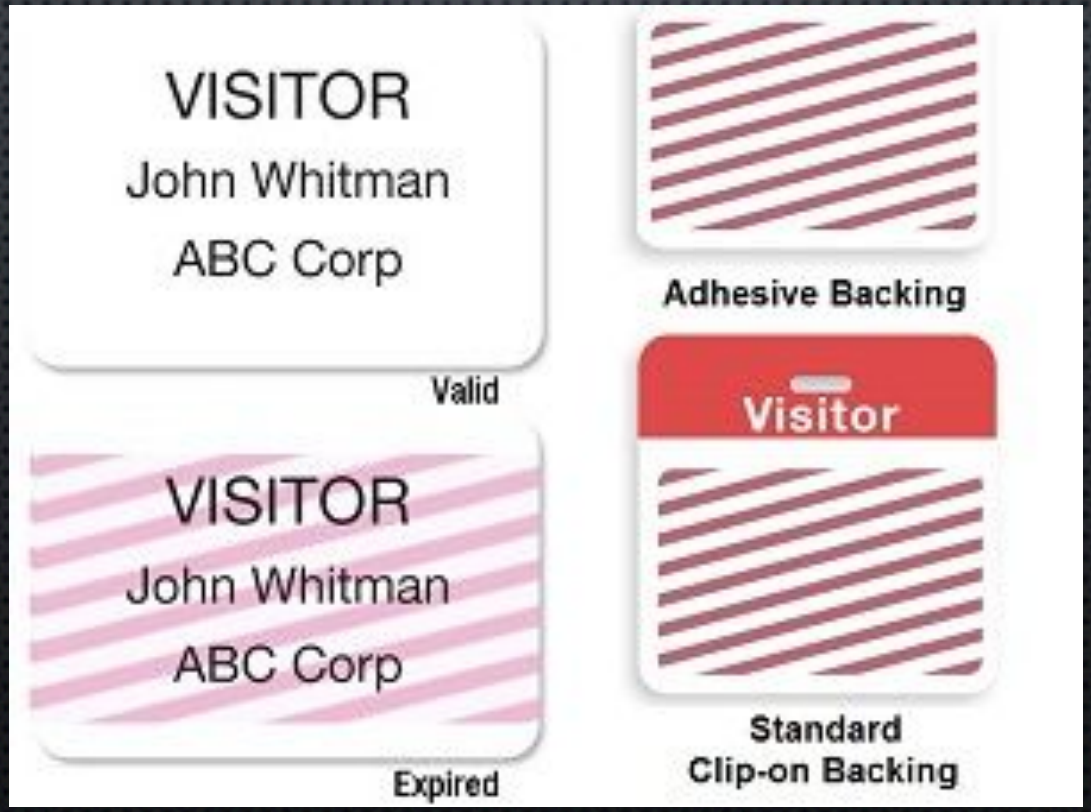
NEWEST IMPROVEMENT: DYNAMIC SEALS

RIFT RECON

PHYSICALLY UNCLONABLE FUNCTIONS



DYNAMIC SEALS: TIME

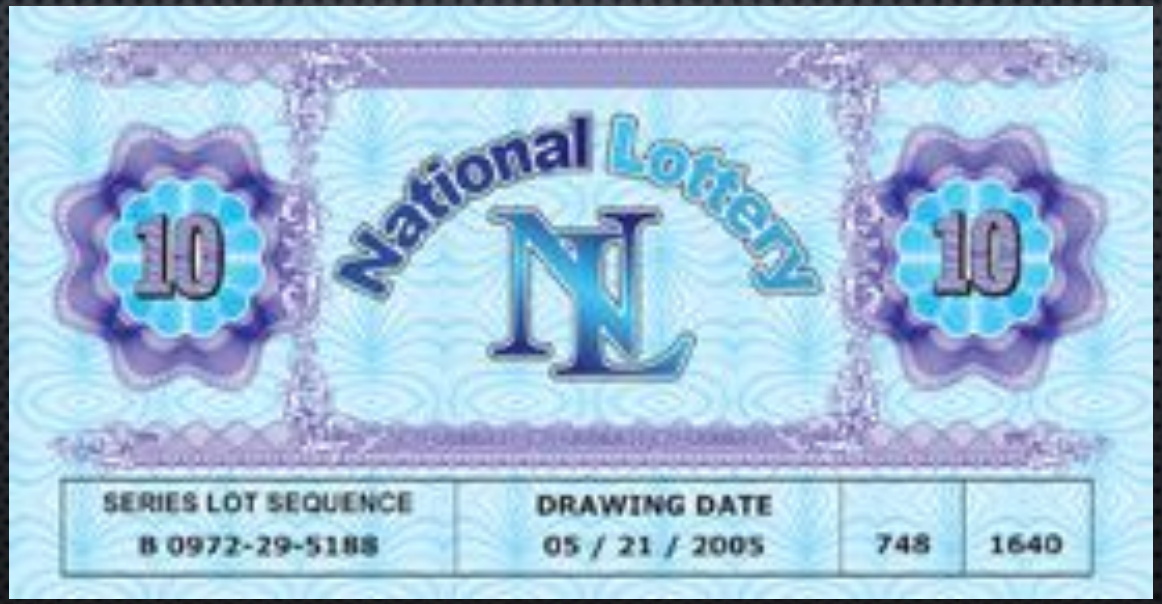


RIFT RECON

DYNAMIC SEALS: POSITION

RIFT RECON

DYNAMIC SEALS: LAYERS



RIFT RECON

DYNAMIC SEALS: VERIFIER APPLICATION

Work in progress:
https://github.com/cryptoseal/verifier

RIFT RECON

OPEN QUESTIONS

CONCLUSION/SUMMARY

- INCREASING NEED
- COOL NEW TECHNOLOGY
- OPEN SOURCE IS THE BEST MODEL

CONTACT US

- ERIC MICHAUD ERIC@RIFTRECON.COM WWW.RIFTRECON.COM @ERICMICHAUD
- RYAN LACKEY RYAN@CRYPTOSEAL.COM WWW.CRYPTOSEAL.COM @OCTAL