Lest We Remember: Cold-Boot Attacks on Encryption Keys

By J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten

(USENIX Security 2008, Awarded Best Student Paper)

Presented By Hyunjin Choo

Contents

Contents

Stolen Laptops

WASHINGTON

Personal Data of 26.5 Million Veterans Stolen

By DAVID STOUT MAY 22, 2006

BERKELEY / Cal issues alert about stolen laptop computer / It contains 98,000 Social Security numbers -- notifications to warn of identity-theft risk

Charles Burress, Chronicle Staff Writer Published 4:00 am PST, Tuesday, March 29, 2005

Laptop with GE employee data stolen

Computer contained social security numbers for 50,000 workers

Stolen laptop leads to breach notification for 20,000 Lifespan patients

Theft Of Gap Laptop Puts 800,000 Job Applicants At Risk

Fidelity says stolen laptop held data of customers

Fund company sends out security alerts to 196,000

By Ross Kerber
Globe Staff / March 23, 2006

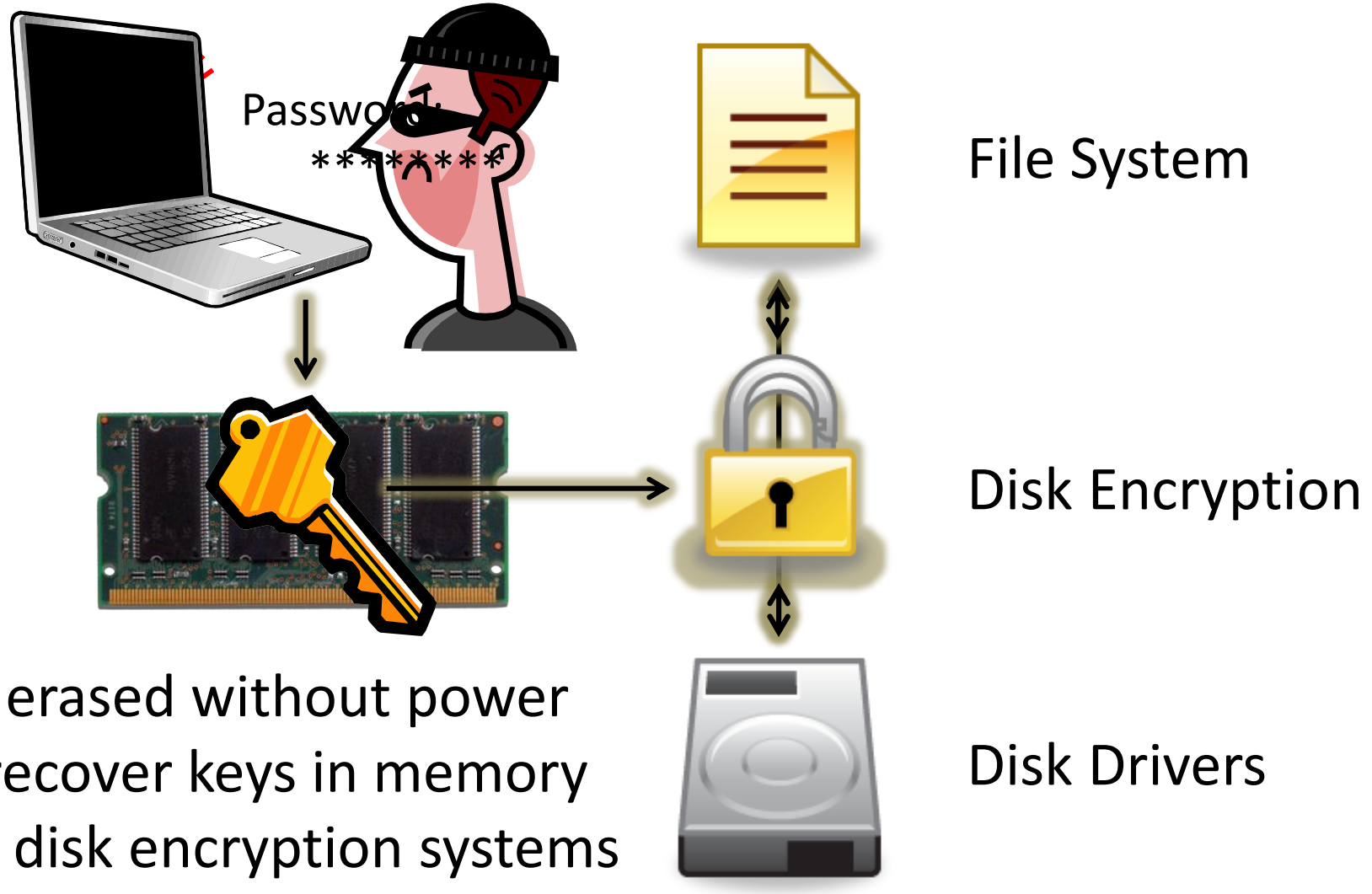
How Safe is a Stolen Laptop?

Screen	**Unlocked**	**Locked**	**Locked**
HDD	**Unencrypted**	**Unencrypted**	**Encrypted**
Protection	No protection	Minimal protection	[illegible]

Disk Encryption

- Protects access to data
- Allows read/write access while protecting via encryption
- Scrambles the contents, unreadable without an encryption key
- Encryption key needs to be kept available
  - Stored in RAM until the disk is unmounted
- BitLocker (Windows) / FileVault (Mac OS) / LoopAES (Linux)
  dm-crypt (Linux) / TrueCrypt (Win/Mac OS/Linux)

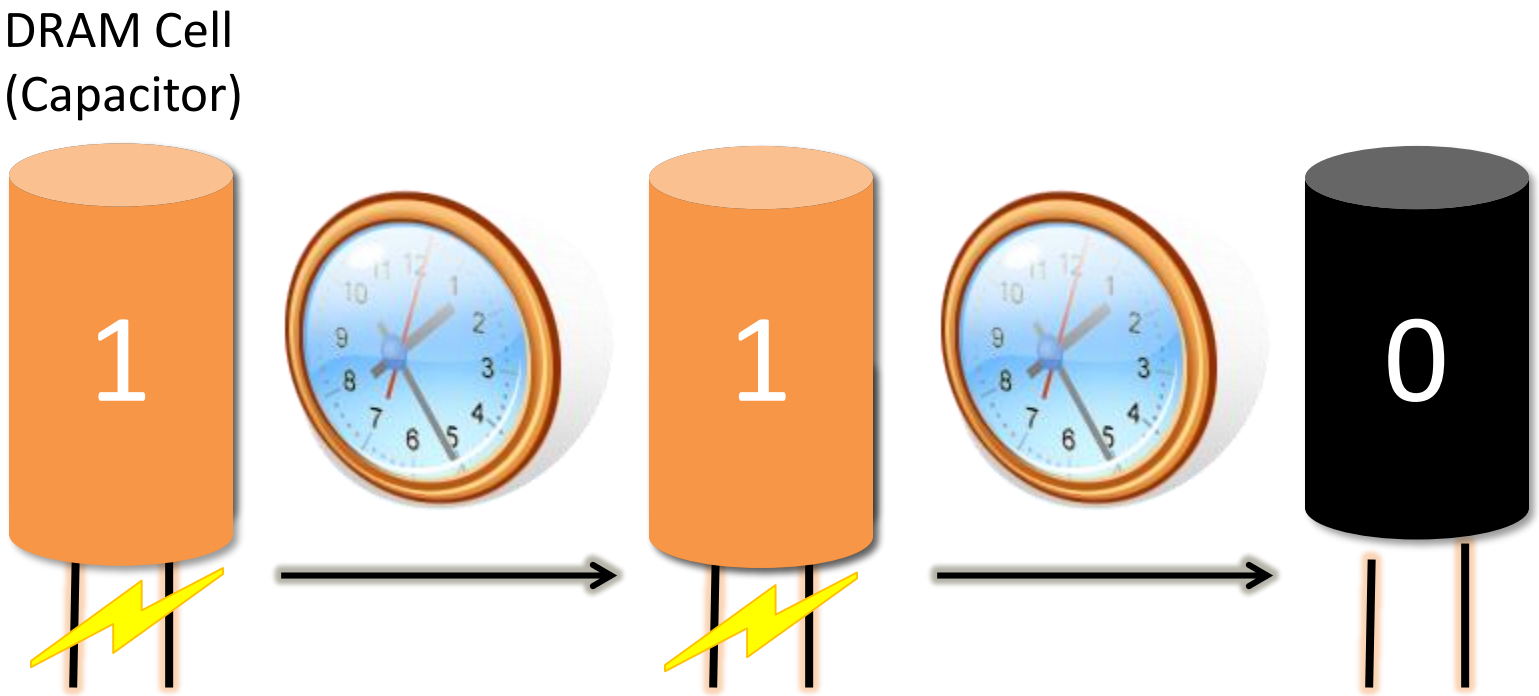
Disk Encryption (cont'd)



- Memory is not erased without power
- Exploit this to recover keys in memory
- Defeat popular disk encryption systems

Contents

DRAM Remanence

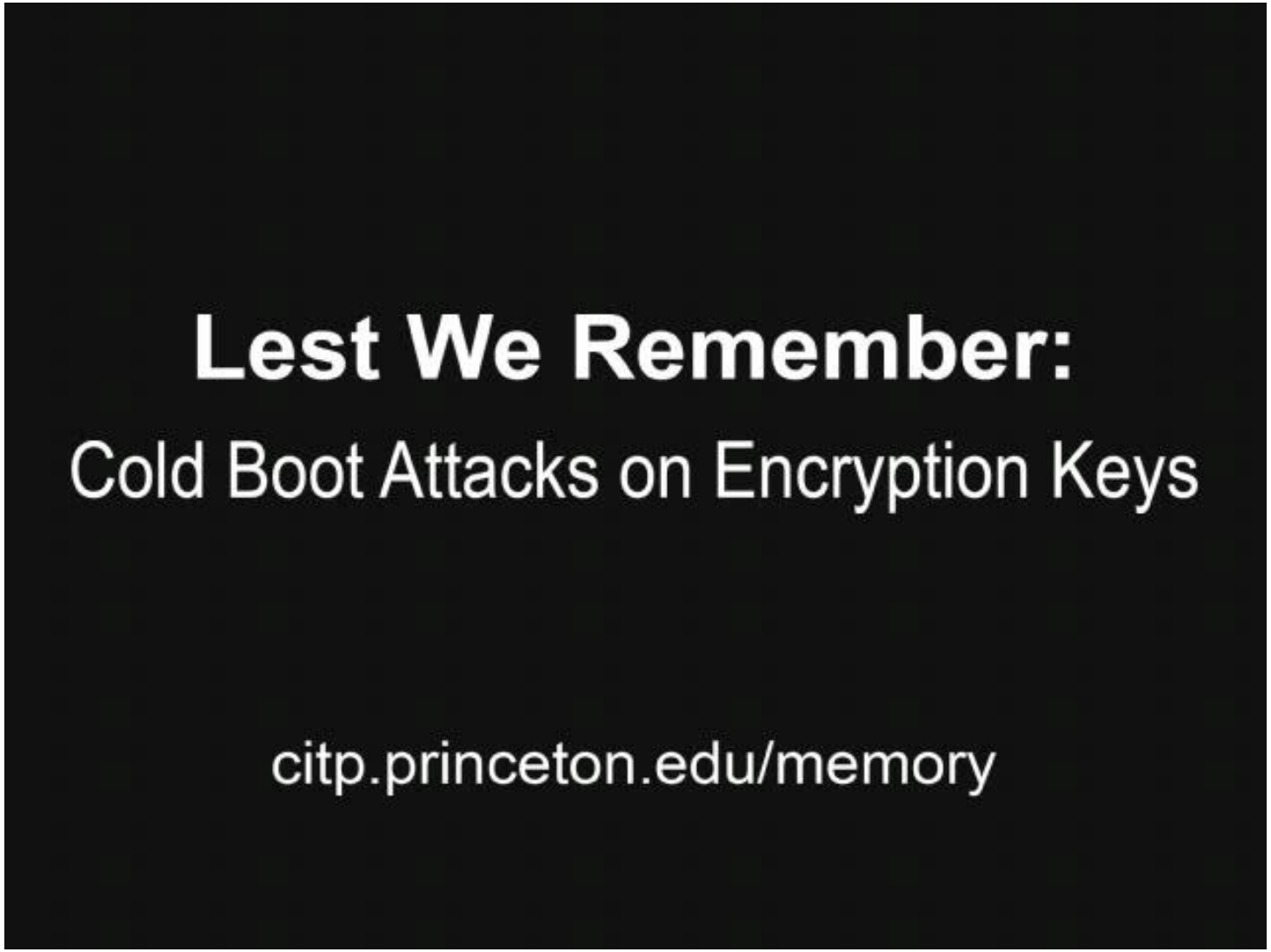


If it loses power?

Data fades almost instantaneously

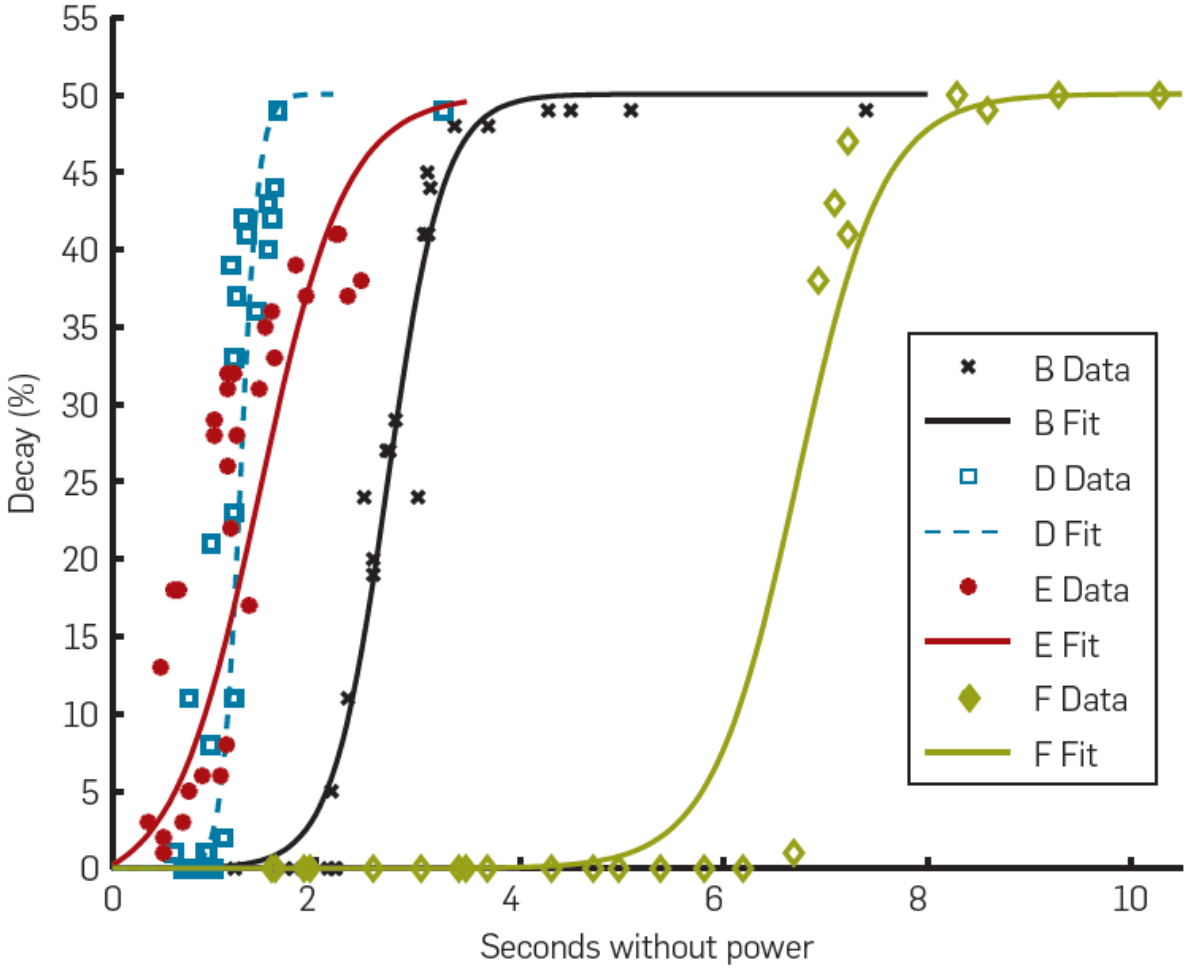
Any residual data is difficult to recover

DRAM Remanence (cont'd)

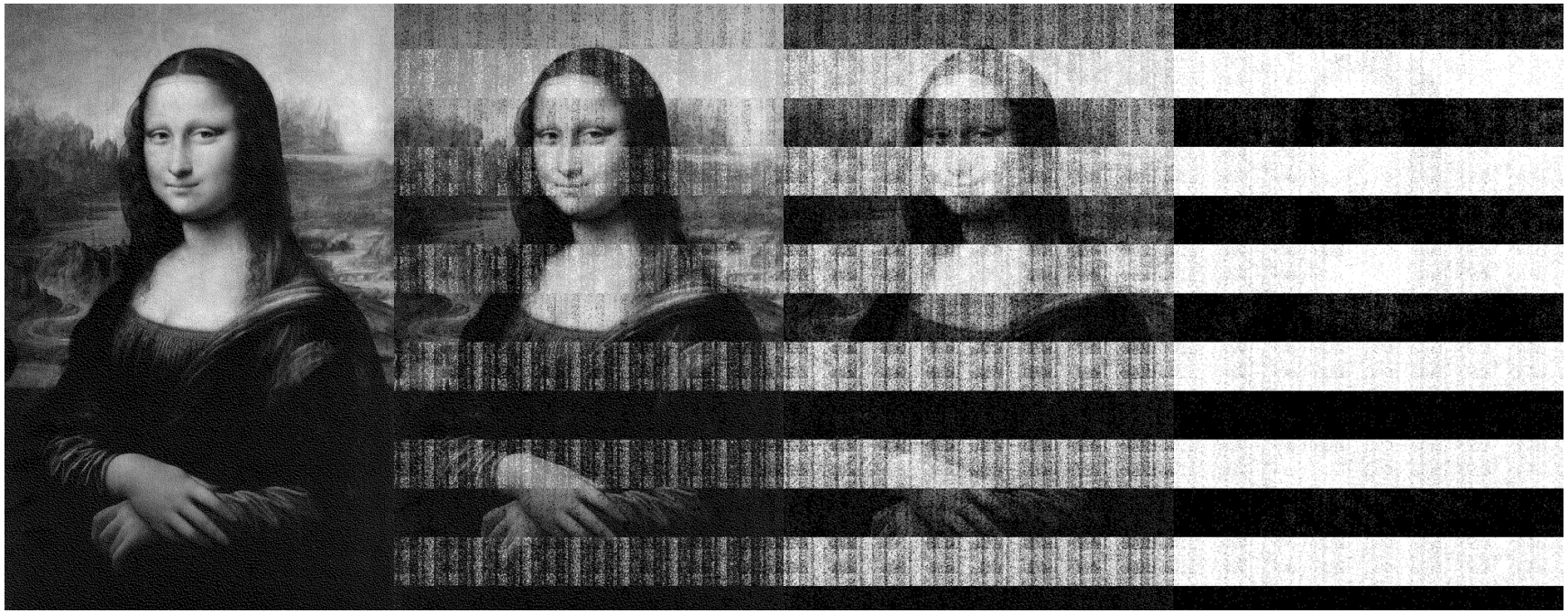


Measuring Decay

	Density	Type	System	Year
A	128MB	SDRAM	Dell Dimension 4100	1999
B	512MB	DDR	Toshiba Portégé R100	2001
C	256MB	DDR	Dell Inspiron 5100	2003
D	512MB	DDR2	IBM Thinkpad T43p	2006
E	512MB	DDR2	IBM Thinkpad x60	2007
F	512MB	DDR2	Lenovo 3000 N100	2007



Visualizing Decay



5 secs 30 secs 60 secs 300 secs

Decay at Reduced Temperature

❖ Colder temperatures slow decay

	Seconds without Power	Average Bit Errors	
		No Cooling (%)	-50 °C (%)
128MB SDRAM	60	41	No errors
	300	50	0.000095
512MB DDR	360	50	No errors
	600	50	0.000036
256MB DDR	120	41	0.00105
	360	42	0.00144
512MB DDR2	40	50	0.025
	80	50	0.18

Contents

Attack Demo Video

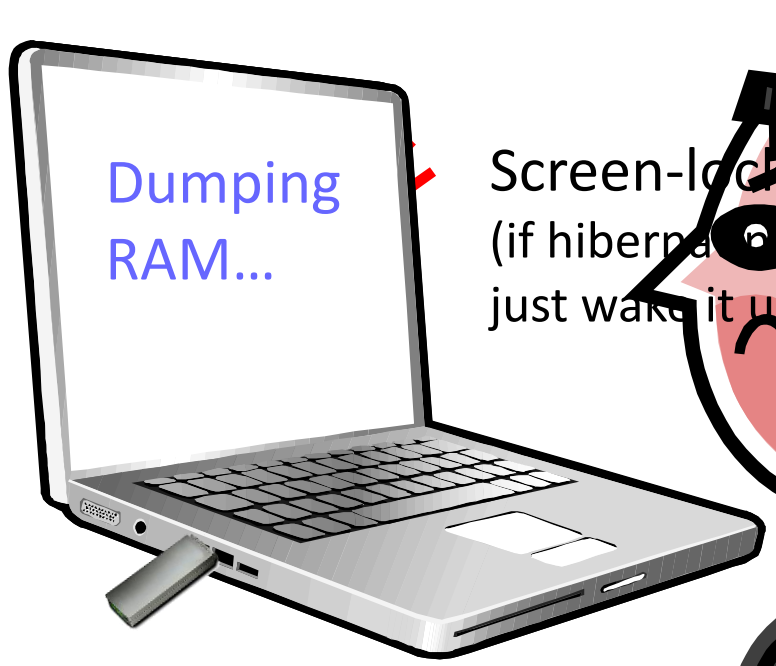
Imaging Tools

- Requires no special equipment
- Challenge: Booting will overwrite memory
  - Solution: Use program to dump contents to external medium
- Network boot
  - PXE (Intel's Preboot Execution Environment)
  - EFI (Extensible Firmware Interface)
- USB drives
- iPods

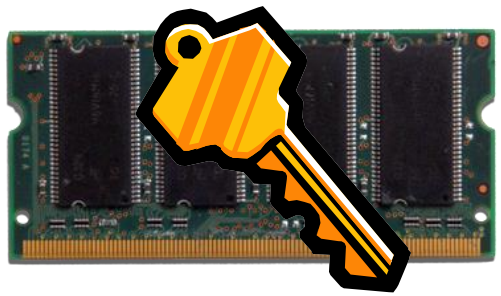
Imaging Attacks

1. Simple Reboot Attack
   - Warm-boot
     - Restarting machine while it is powered on (Ctrl + Alt + Del on Windows, kexec on Linux)
     - No memory decay, but software chance to wipe data
   - Cold-boot
     - Restarting machine from a power-less state (Disconnect and reconnect power)
     - Little to no memory decay, and no software chance to wipe data
2. Advanced Cold-Boot Attack
   - Transfer the memory to attacker's computer, if the BIOS clears RAM or prevents memory dumping
   - Cooling the memory slows decay to be transferred with minimal decay

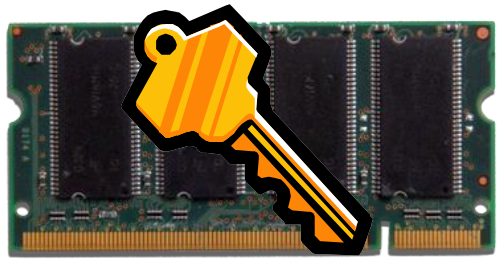
Simple Cold-Boot Attack



Screen-locked machine
(if hibernating/sleeping just wake it up!)



What if the BIOS clears RAM?

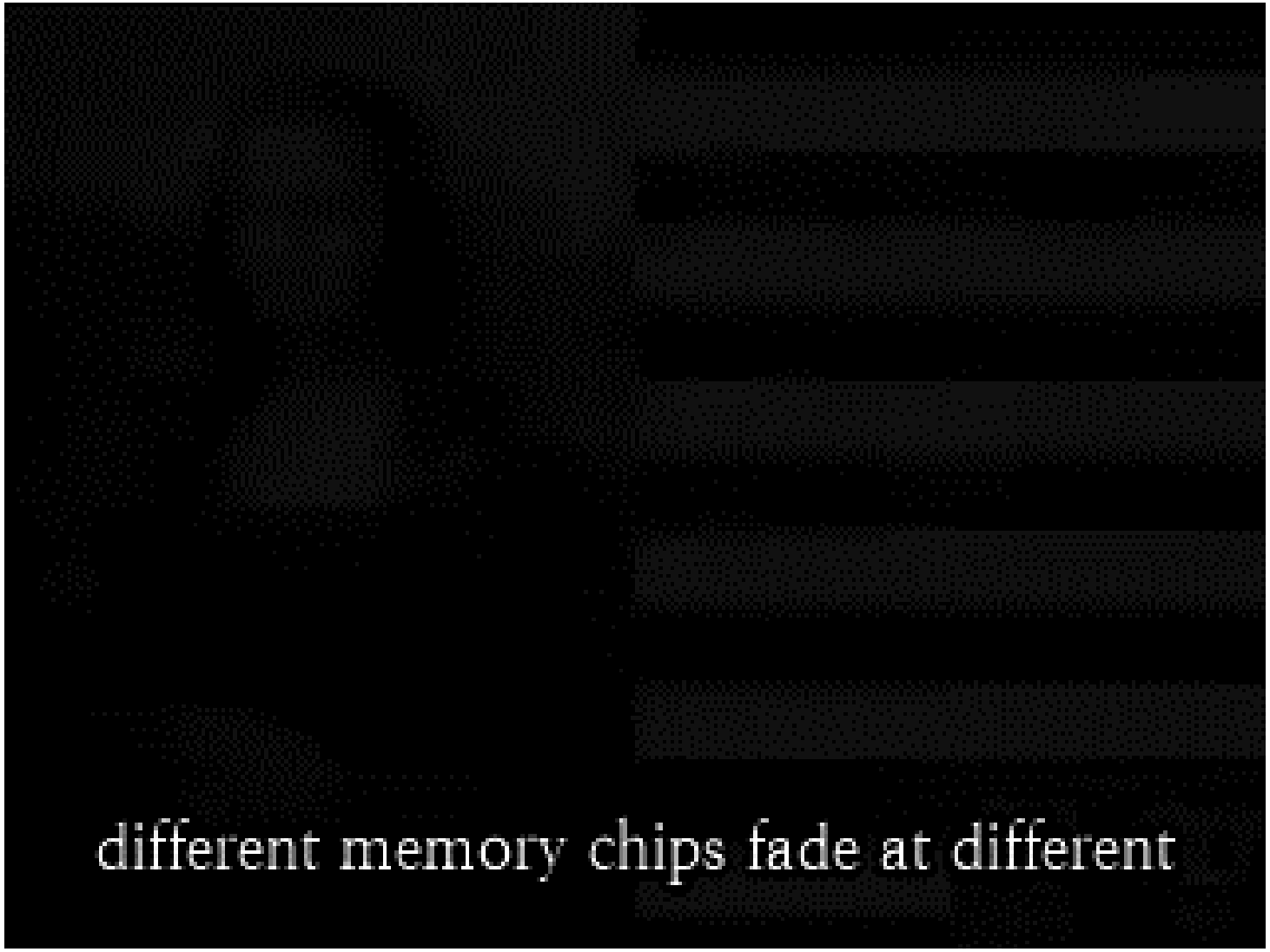


Advanced Cold-Boot Attack

Victim’s Computer

Attacker’s Computer

Advanced Cold-Boot Attack (cont'd)



Advanced Cold-Boot Attack (cont'd)

- Most powerful attack
- Reduces the temperature of the memory to −50°C while running
  - Data persists for several minutes even if the memory modules are removed
- Moves them to another machine and read them
- Cheap and practical way to move the RAM without losing data

Contents

Key Reconstruction

- Even a small error complicates extracting key
- Developed algorithms for reconstructing keys
  - Work when only 27% of the bits are known

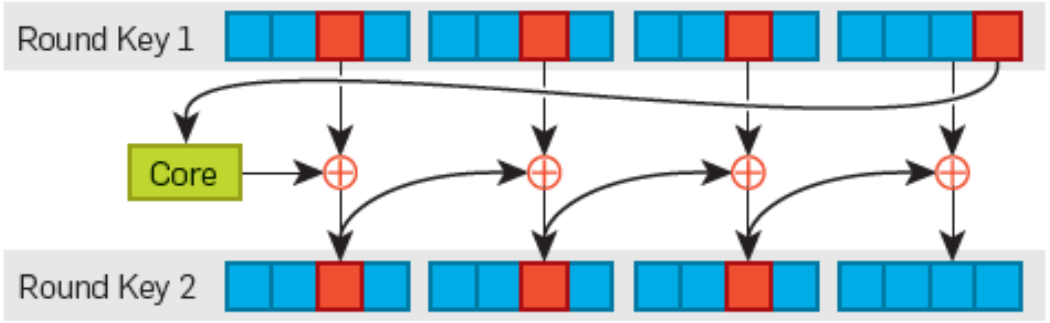
1. Trade-off between efficiency and security
   - Stores precomputed data from the encryption keys to speed up computation
   - This precomputed data contains much more structure than the key itself
2. Most decay is unidirectional
   - Bits decay to a predictable ground state
   - Decay probability is known to the attacker

DES Key Reconstruction

- DES expands the key K into key schedule
  - Cache it in memory because it takes time to compute
- Key schedule consists of 16 round keys
  - Permutation of a 48-bit subset of bits from the original 56 bit key
  - Bit from the original key is repeated in about 14 of the 16 round keys
- Consider the n bits extracted from memory as identical copies of key bit
  - Calculate whether the extracted bits were resulted from the decay of repetitions of 0 or 1
  - 5% error in key schedule: the probability of getting wrong key < 10^{-8}
  - 25% error in key schedule: the probability of getting correct key > 98%

AES Key Reconstruction

- AES uses a key schedule with a more complex structure
  - For 128-bit keys, the key schedule consists of 11 round keys, each made up of four 32-bit words.
  - Each subsequent word is generated either by XORing two earlier words, or
  - Performing a core operation on an earlier word and XORing the result with another earlier word
- Slice up the keys and use linearity in the key scheduling
  - Pick 7 bytes from the first 2 round-keys as shown in picture
- Generate the relevant 3 bytes of the next round key from first 4 bytes
  - Guess the candidate key by calculating possibilities that these 7 bytes might have decayed
  - Calculate the key schedule for each candidate key
  - Unique guess under unidirectional decay
- To reconstruct key with 7% bit error: 1 second / half of keys with 15% bit error: 30 seconds



RSA Key Reconstruction

- RSA public key consists
  - Modulus N
  - Public key exponent e
- RSA private key consists
  - Private exponent d
- Optional values
  - Prime factor p and q of N
  - $d \bmod (p-1)$
  - $d \bmod (q-1)$
  - $q^{-1} \bmod p$
- Given N and e, any of the private values is sufficient to generate the others
  - Stored to speed computation
- Key structure is the mathematical relationship between the public and private key
  - Enumerate potential RSA private keys and prune those that do not satisfy these relationships
  - Recover a RSA key in 1 second when only 27% of the bits are known

Key Identification

- Automatic techniques for locating encryption keys in memory
  - Target the key schedule instead of the key itself
- AES key identification algorithm:
  1. Iterate through each byte of memory. Treat that address as the start of an AES key schedule.
  2. Calculate the Hamming distance between each word in the potential key schedule and the value that would have been generated from the surrounding words in a real, undecayed key schedule.
  3. If the sum of the Hamming distances is sufficiently low, the region is close to a correct key schedule; output the key.
- keyfind application for 128- and 256-bit AES
  - Receive extracted memory and output a list of likely keys
  - Recovered keys from disk encryption programs successfully
- RSA key identification
  - Search for known key data or for characteristics of the standard data structure used for storing RSA private keys
  - Located the SSL private keys in memory successfully

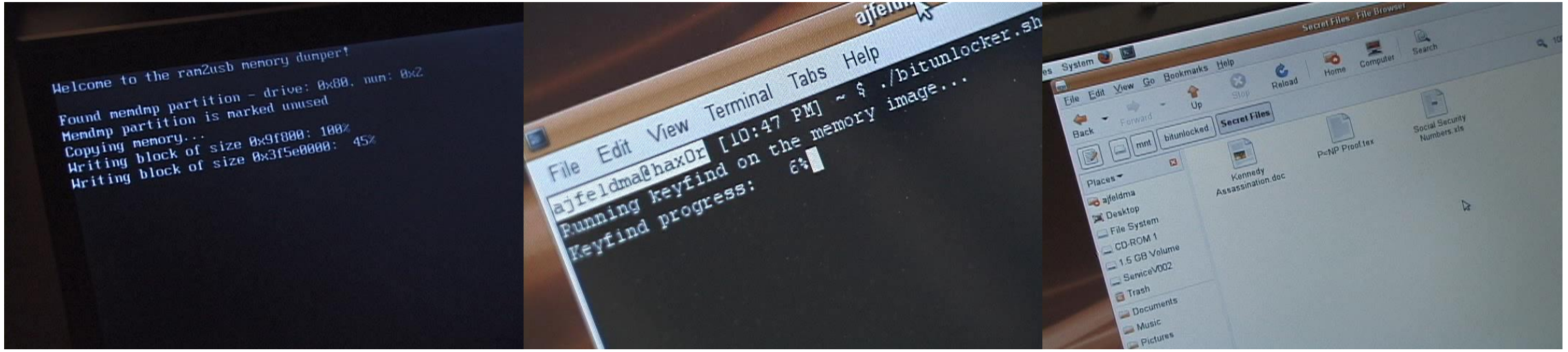
Contents

Successful Attacks Against

- Attacks work on all operating systems (Windows, Mac OS, and Linux)
- BitLocker in basic mode
  - Even fully “at rest” with computer powered off
- FileVault, dm-crypt, TrueCrypt, and Loop-AES
  - where computer was running, sleeping, or hibernating
- Disk encryption is not a sufficient defense against physical data theft

BitLocker

- Disk encryption for Windows
- BitUnlocker (fully automated demonstration attack tool)
  - External USB hard disk containing a Linux, a custom SYSLINUX based bootloader, and a custom driver that allows BitLocker volumes to be mounted under Linux
  - Reset, connect USB disk, and boot from this USB disk
  - Automatically dumps the memory, runs keyfind to locate and reconstruct candidate keys, and mounts the BitLocker encrypted volume, which can be browsed like any other volume
- Laptop with 2GB RAM as a target
- Took 25 min to recover keys and decrypt entire disk



FileVault

- Disk encryption for Mac OS
- User password for both an AES key and IVs (initialization vectors)
- EFI memory extraction program with a FileVault volume mounted
- keyfind automatically identified the FileVault AES encryption key
- IV key is present in RAM and an attacker can identify it
- Encrypts each disk block in CBC mode
  - The attacker can decrypt most disk block except the first cipher block using only the AES key
- AES and IV keys together allow full decryption using programs like vilefault

TrueCrypt, dm-crypt, and Loop-AES

- TrueCrypt is disk encryption for the Windows, Mac OS, and Linux
- dm-crypt and LoopAES are disk encryption for the Linux
- All vulnerable to attacks
  - Once a memory image extracted, to use keyfind to locate the keys and use the keys to decrypt and mount the disks were possible

Contents

Countermeasures

1. Suspending a system safely
   - Power off the machine not in use to wipe the memory
   - Encrypt the memory under a key derived from the user password
2. Storing keys differently
   - Avoiding precomputation will improve resistance but worse performance
3. Physical Defenses
   - Physically defend or detect memory from being removed
4. Architectural changes
   - DRAM could be designed to lose their state quickly
   - Store a keys securely while erasing them on power-up, reset, and shutdown
   - Encrypt the memory routinely
5. Encrypting in the disk controller
   - Store the key in the disk controller's memory
6. Trusted computing
   - Prevent a key from being loaded into memory, but cannot prevent from being captured

Contents

Previous Work

- Pettersson, T., Cryptographic key recovery from Linux memory dumps [Presentation at Chaos Communication Camp'07]
  - DRAM contents can survive cold boot and remanence could be used to acquire memory images and cryptographic keys
- Chow, J., Shredding your garbage: Reducing data lifetime through secure deallocation [USENIX Sec'05]
  - Discovered the remanence during an unrelated experiment, and remarked security implications
- MacIver, D., Penetration testing Windows Vista BitLocker drive encryption [Presentation at Hack In The Box'06]
  - Microsoft knew that memory remanence and BitLocker is vulnerable to a cold-boot attack
- Link, W., May, H., Eigenschaften von MOS-Ein-Transistorspeicherzellen bei tiefen Temperaturen [Archiv für Elektronik und Ubertragungstechnik'79]
  - Since the 1970s, DRAM remanence has been known
- Gutmann, P., Secure deletion of data from magnetic and solid-state memory / Data remanence in semiconductor devices [USENIX Sec'96 / USENIX Sec'01]
  - Attributes burn-in to physical changes, and suggests that keys be relocated periodically as a defense

Memory Scramblers

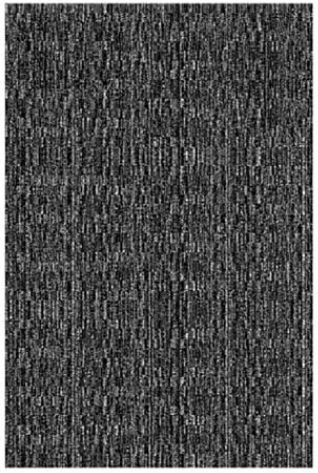
- From DDR3, *memory scramblers* are introduced as basic protection from the cold boot attack
- Memory scramblers XOR the pseudo random numbers with data to be written
  - DDR3: Number generated from pseudo random number generated from boot time and address to be written
- Gruhn, M., On the Practicability of Cold Boot Attacks [International Conference on Availability, Reliability and Security'13]
  - Could not reproduce cold boot attacks against DDR3

(a) 0 sec / 100% **(b)** 2 sec / 99.2% **(c)** 3 sec / 93.4% **(d)** 4 sec / 93.1% **(e)** 5 sec / 61.4% **(f)** 6 sec / 51.9%

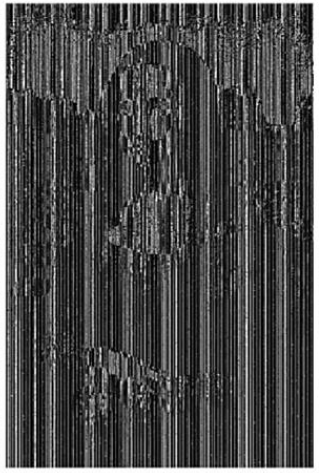
Figure 2: A picture of the Mona Lisa being recovered from system C's RAM at normal operational temperature of 20 to 25 °C after different amounts of time. Each picture's caption includes the percentage of *correct* bits that were recovered.

DDR3 was Broken

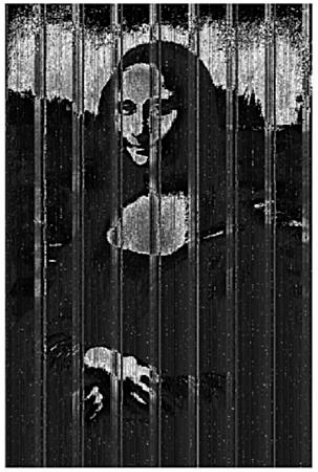
- Bauer, J., Lest we forget: Cold-boot attacks on scrambled DDR3 memory [Digital Investigation'16]
  - Demonstrated a cold boot attack that bypasses DDR3 scrambler son 2*nd* generation Intel Core (SandyBridge) CPUs
  - Requires only 64 bytes of known plaintext per memory channel and only 50 bytes if the mathematical approach is chosen to descramble the image



(a) Scrambled image captured at +30 °C



(b) Scrambled image captured at -30 °C



(c) Related-data descrambling

(d) Stencil descrambling

(a) Interleaved dual channels

(b) Deinterleaved masked image

DDR4 was also Broken

- DDR4 memory scramblers have been redesigned
- Yitbarek, SF., Cold Boot Attacks are Still Hot: Security Analysis of Memory Scramblers in Modern Processors [IEEE International Symposium on High Performance Computer Architecture'17]
  - Effective attack on DDR4
  - Scramblers do not provide confidentiality guarantees
  - Replacing memory scramblers with strong cipher engines can provide better protection

Android Smartphone

- Müller, T., Frost; Forensic Recovery of Scrambled Telephones [International Conference on Applied Cryptography and Network Security'13]
  - Broke Android smartphone with full disk encryption performing Cold-Boot Attacks
  - Recovered sensitive information from RAM

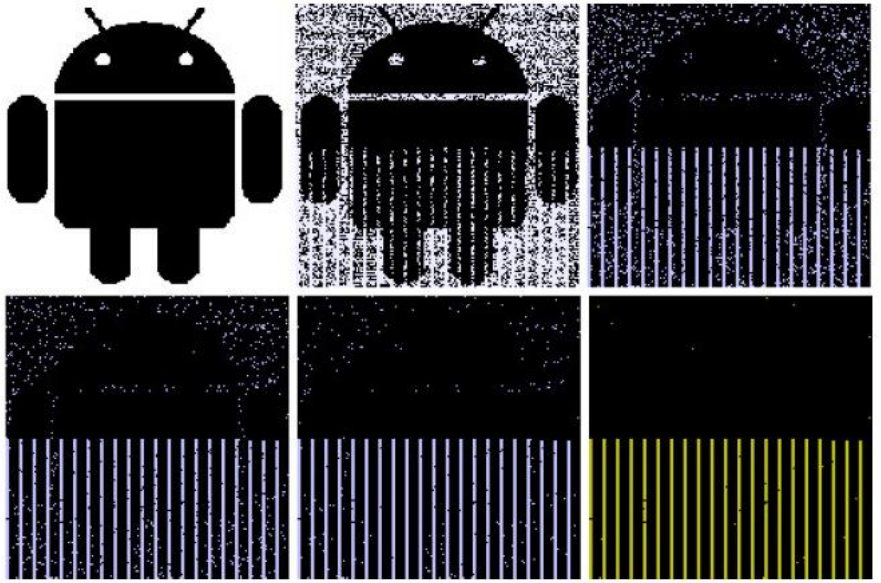


Fig. 8: An Android bitmap after $0s$, $0.5s$, $1s$, $2s$, $4s$, and $6s$ in DRAM without power. The cold boot attack has been deployed at room temperature.

Storing Keys Outside RAM

1. Register-based key storage
   - Loop-Amnesia: 2011
   - TRESOR: 2011
   - TreVisor: 2012
   - ARMORED: 2013
2. Cache-based key storage
   - Copker: 2011
   - Sentry: 2015
   - CaSE: 2016
3. GPU-based key storage
   - PixelVault: 2014

A Decade Later...

New modification of the old cold boot attack leaves most systems vulnerable

The defenses put in place to thwart the 2008 attack turn out to be very weak.

PETER BRIGHT - 9/14/2018, 5:26 AM

LILY HAY NEWMAN SECURITY 09.14.18 09:40 AM

A DECADE-OLD ATTACK CAN BREAK THE ENCRYPTION OF MOST PCS

Almost 'all modern computers' affected by cold boot attack, researchers warn

The attack would allow potential hackers to steal sensitive information stored on your RAM.

BY ALFRED NG | SEPTEMBER 13, 2018 12:02 PM PDT

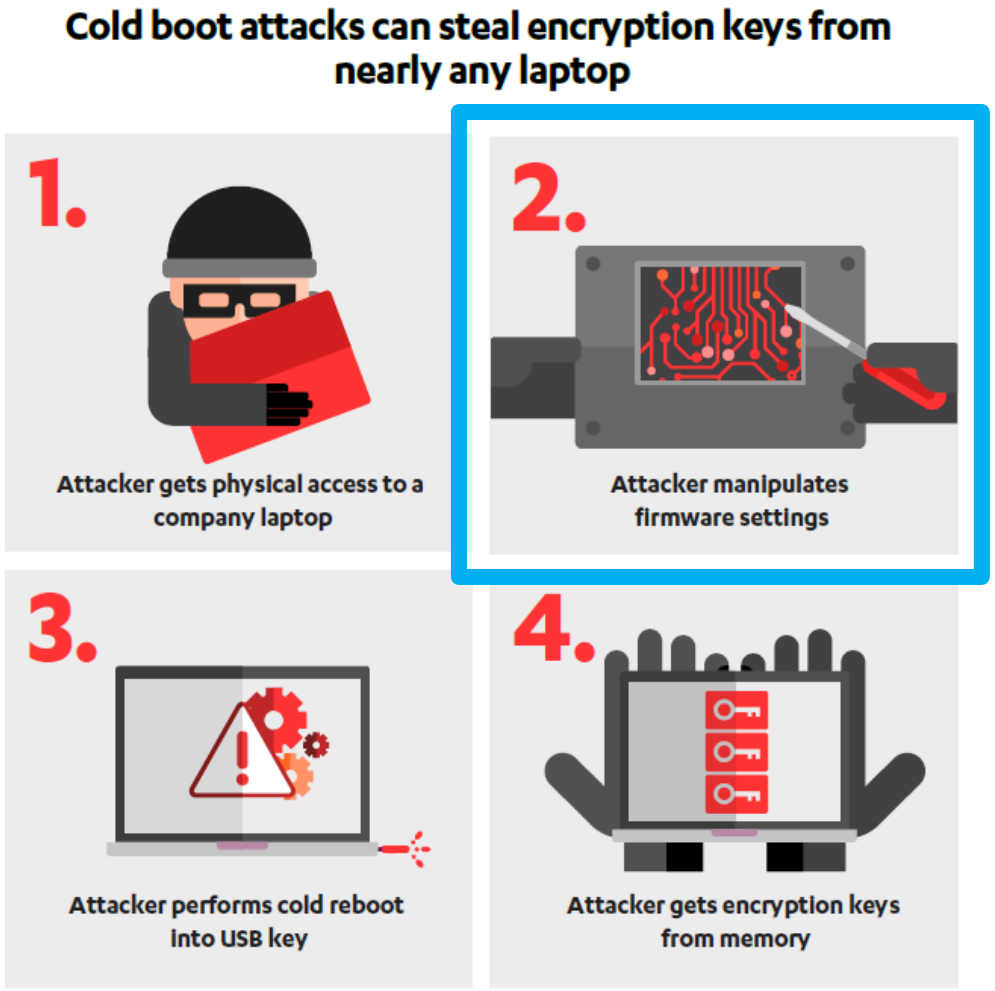
New Cold Boot Attack Unlocks Disk Encryption On Nearly All Modern PCs

September 13, 2018 Swati Khandelwal

New Cold-Boot Attack

New Cold-Boot Attack (cont'd)

- One safeguard overwrites the contents of the RAM when the power was restored
- Figured out a way to disable this overwrite feature and enable booting from external devices by physically manipulating the hardware
- Shared their research with Microsoft, Intel, and Apple and these companies are now exploring possible mitigations.



Conclusion

- DRAMs hold their values for long intervals without power or refresh
- Enables attackers to extract cryptographic keys and other sensitive information from memory
- The attacks are practical
- No perfect countermeasure so far
- Recent computers and smartphones are still vulnerable

Best Questions

- Countermeasures (Youngjin Jin): Many of you have asked. But, You ngjin was selected because of his writing.
- TEE and Secure Enclave (Kyeong Tae Kim): SGX provides such a de fense only on the enclave regions!
- Solve Ransomware Problem (Tae Hyeon Lee): They know how to e rase the key.
- Not selected but, why did this paper receive the best paper award (Minkyoo Song)?

Thank you