Asignment Week 1

Nathan A. Nordby

1 Process learning

This by far was worse than the first week. In learning there was a steep curve figuring out Overleaf, management sources for references (Zot..Mend..) and others, and even tried a web-crawler to try to save time. Long story short: the longest time taker was learning the tools. Thanks to the class notes I was able to reasonably adapt to reading effectively and efficiently a significant number of papers. It is hard to tell how well each of them got an objective look because I found after about 20 minutes of 1-2 minute reads I had to take a break or else I began skipping over key facts due to disinterest. In the end I was able to find a method going between the abstract-conclusion and key figures to do a search in about 30 seconds. This quick search allowed me to determine if it was a paper "worth reading" meaning: it was applicable to my current topic and may have useful direct/indirect contributing research toward that topic. GitHUB by far is the easiest and cleanest user interface with simple control flowt without hickup. I had zotero and many other programs crash numerous times when I tried to do control paths that likely were not considered in there design.

2 Scan 8+ papers

2.1 Fast, Lean, and Accurate: Modeling Password Guessability Using Neural Networks [1]

(Category: vulnerability of human generated passwords (Context: usenix, multiple papers on password guessing (Contributions: created neural network to guess human passwords, created counter java code to help check passwords being created (Credible: moderatly, lots of questionable repositoriery references (Care: NA (Cost: 2 hours

2.2 Post-quantum key exchange – a new hope* [2]

(Category: crypto vulnerability due to quantum computing (Context: usenix, significant other authors and history (Contributions: Create a lattice solution cipher to protect against quantum computing (Credible: Very credible, significant horizonontal work and research (Care: published and open on GIT (Cost: 2-4 hours

2.3 FlowFence: Practical Data Protection for Emerging IoT Application Frameworks [3]

(Category: expose vulnerability in the data flow of IoT devices through the internet (Context: usenix, information flow security (Contributions: create a softare design to help keep flow information secure between devices, and keep them arbitary and prevent direct connection through a third party connection (Credible: Very credible, significant horizonontal work and research (Care: published and signficant references, already a lot of work done in this area (Cost: 2-4 hours

2.4 DROWN: Breaking TLS using SSLv2 [4]

(Category: expose vulnerability in known and extinct sslv2 (Context: usenix, information flow security (Contributions: create an attack to use known vulnerabilities in SSLv2 to break TLS (Credible: very credible based on known vulnerabilities (Care: Pretty good demonstration of what any remaining servers need to dump sslv2 now! (Cost: 2 hours

2.5 fTPM: A Software-only Implementation of a TPM Chip [5]

(Category: Cryptography replace TPM with software (Context: usenix, information flow security (Contributions: create a software version of TPM based on fuses on board processors, Device Key, and UUID (Credible: credible (Care: keep much of the work confidential but appear accomplish the same effect as TPM (Cost: 4 hours

2.6 Sanctum: Minimal Hardware Extensions for Strong Software Isolation [6]

(Category: Cryptography replace TPM with software (Context: usenix, information flow security (Contributions: Physically modify an existing chip to introdue TPM (Credible: Hard to tell not my area of expertise they physically modify an existing chip (Care: Unknown (Cost: 2 hours

2.7 The Million-Key Question – Investigating the Origins of RSA Public Keys [7]

(Category: Crypotgraphy finding out if RSA key pair generation is trully uniform primes distributed with different vendors/libraries (Context: usenix, information flow security (Contributions: They demosnstrate that some specicially one card vendor does not proerply unifomrly distribute their findings of primes (Credible: Credible based on exsiting crypto and signifcant search space (Care: Out to get some attention since they kind of invalidate one of the card companies random key pair generation (Cost: 2 hours

2.8 Fingerprinting Electronic Control Units for Vehicle Intrusion Detection [8]

(Category: ECU protection of new vulnerabilities in automotive vehicles (Context: usenix, information flow security (Contributions: The created a custom intrusion detection system based on timing and clocks of the vehicle (Credible: yes (Care: Yes, will provide another possible solution to prevent hijacking of an ecu. (Cost: 2 hours

2.9 Lock It and Still Lose It – On the (In)Security of Automotive Remote Keyless Entry Systems [9]

(Category: Vulnerability analysis of RKE and vehicular entry systems (Context: Jam Intercept and Replay Attack against Rolling Code Key Fob Entry Systems using RTL-SDR Comprehensive experimental analyses of automotive attack aces,Breaking the security of physical devices, Vulnerabilities of Crypotography in RKEs for vehicles (Contributions: Provide several methods for automotive industry to move forward with new measures (Credible: Very Crecidble Usenix conference, responsible disclosure worked with manufactures and specific parts (Care: Responsible Dislosure, and automakers already acting on the data (Cost: 1-2 hours

3 Critical/Creative Read

3.1 Lock It and Still Lose It – On the (In)Security of Automotive Remote Keyless Entry Systems [9]

3 Types of remote systems RKE button press Imobolizer may or may not be linked with RKE PKES Passive Remote Keyless Entry, within certain range automatically challenge and response ?-2005 2006-2012 2013 2016 RKE TXI-DTS-40 NXP HITAG-2 Megamos Crypto trans Immobilizer PKES

TXI DTS-40 40 bit key broken by exhaustive key search space of 40 bit key nto the 40 key search NXP HITAG-2 48 bit key broken in 5 minutes with Megamos Crypto trans 96 bit key broken in days to seconds using Time-Memory Tradeoff (TMTO) using crypto analytics brings key size down to 57 bits

RKE PKES 315 433 868 MHz Immobilizers 125 MHz Some using infrared instead of RF

All attacks require some initial interaction with user key. PKES more vulnerable because pasively initiated conversation can occur at any time vs. RKE needing button press. Once attacker has key examples can use to crypto analyze and break and create key for entry Black market devices available for sale to break PKES lock and unlock commands require different rolling code Used HackRF, USRP, RTL-sdr DVB-T USB sticks and RF modules all costing 40 dollars. Most use ASK or FSK with Machestor or Pulse-width encoding 1-20 kbits/s Authenticates using UID and countor or Message Authentication Code (MAC) Did not validate or determine exactly what vehcles the

vulnerability applies to Hard to reverse engineer microcontrolers in RKEs, but possible to reverse engineer RKE system based on ECUs Using widely available, standard programming tools for automotive processors, we were able to ob tain firmware dumps for all studied ECUs. We then located and recovered the cryptographic algorithms by performing static analysis of the firmware im age, searching amongst others for constants used in common symmetric ciphers and common patterns of such ciphers (e.g., table lookups, sequences of bit wise operations). The results of this process are de

VW rolling code only permutates and XORs the ID and uses a LFSR to determine the rolling code (easitly rellicatable and basically little to no crypto) BLUF: VW uses a few master keys for all their cars world wide so all vehicles are susceptiable to easy teheft by electronic means

3.2 Fingerprinting Electronic Control Units for Vehicle Intrusion Detection [8]

Reasonable introduction give good explanation for need of the problem First large assumption is scalling adversaries as week and strong, but seems reasonable for purposes of discussion Clock offset calculations is sofisticated but seems reasonable Clock offset for some vehicles has verly little or similar drift but still drift Paper addreses simliar clock offsets but from different ECUS in Paper does a good job evaluating false positive scenario since it could cause unecesary loss of use of vehicle Paper does not run many tests for false positives Test set of vehicles is very limited to Honda, Toyota, Dodge Ram There maybe many other ways to false positive CIDS and discussion on how to protect CIDS is very limited

3.3 fTPM: A Software-only Implementation of a TPM Chip [5]

Section 13 in related work is very helpfuland gives a great baseline on some industry standards that are even being looked at adopted globally for trusted runtime execution Somewhat of a survey paper the researchers appear not to provide an actuall tested solution Only discuss two chip TPM implementations ARM and Intell, but seems reasonable since these are the main producers. Does not give background or info on how much these two chips with on-board tpm are in production or currently used. Thesres is a limited test set of 4 devices and they are kept confidential Authors do an extensive job discussing the reasons behind the basis rules for their fTPM and upcomign TPM 2.0 Authors do a good job comparing their performance to that of platform based TPMs. Authors do not bound how many primes are usually searched for when conducting crypto search for primes

References

[1] W. Melicher, B. Ur, S. M. Segreti, S. Komanduri, L. Bauer, N. Christin, and L. F. Cranor, "Fast, lean, and accurate: Modeling password guessability using neural networks," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 175–191, may be worth learning about better options for password crackign using neaural network techniques that are faster than brute force. minute 56.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/melicher

[2] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, "Post-quantum key exchange{$\backslash$backslash$textemdash}a new hope," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 327–343, discusses crypto work in quantam computing and how to keep systems secure 1.00 minute 15.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/alkim

[3] E. Fernandes, J. Paupore, A. Rahmati, D. Simionato, M. Conti, and A. Prakash, "FlowFence: Practical data protection for emerging IoT application frameworks," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 531–548, a useful scan paper considering flow of data between hand held IoT devices and the larger scheme of information sharing and security minute 30.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/fernandes

[4] N. Aviram, S. Schinzel, J. Somorovsky, N. Heninger, M. Dankel, J. Steube, L. Valenta, D. Adrian, J. A. Halderman, V. Dukhovni, E. Käsper, S. Cohney, S. Engels, C. Paar, and Y. Shavitt, "{DROWN}: Breaking {TLS} using SSLv2," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 689–706, a possibly and very quick method for breaking TLS minute 39.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/aviram

[5] H. Raj, S. Saroiu, A. Wolman, R. Aigner, J. Cox, P. England, C. Fenner, K. Kinshumann, J. Loeser, D. Mattoon, M. Nystrom, D. Robinson, R. Spiger, S. Thom, and D. Wooten, "fTPM: A software-only implementation of a {TPM} chip," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 841–856, created a software system to provide like results as TPM in hardware minute 32.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/raj

[6] V. Costan, I. Lebedev, and S. Devadas, "Sanctum: Minimal hardware extensions for strong software isolation," in *25th {USENIX} Security*

Symposium ({USENIX} Security 16). {USENIX} Association, pp. 857–874, interesting for another project where they added blocks without changing a chip architecture to bypass built in functionality of a chipset minute 41.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/costan

[7] P. Svenda, M. Nemec, P. Sekan, R. Kvasnovsky, D. Formanek, D. Komarek, and V. Matyas, "The million-key question{$\backslash$textemdash}investigating the origins of {RSA} public keys," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 893–910, very interesting may reveal other crypto techniques for crypto analysis minute 38.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/svenda

[8] K.-T. Cho and K. G. Shin, "Fingerprinting electronic control units for vehicle intrusion detection," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 911–927, finally, this is a usefull paper minute 37.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/cho

[9] F. D. Garcia, D. Oswald, T. Kasper, and P. Pavlidès, "Lock it and still lose it {$\backslash$textemdash}on the (in)security of automotive remote keyless entry systems," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, AWESOME! This is what I have been looking for vulnerability analysis in crypto codes of RKEs for vehicles minute 21.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/garcia

[10] J. B. Almeida, M. Barbosa, G. Barthe, F. Dupressoir, and M. Emmi, "Verifying constant-time implementations," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 53–70, may be worth learning about timeleaks for crypto analysis 2.00 minute 50.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/almeida

[11] D. Andriesse, X. Chen, V. van der Veen, A. Slowinska, and H. Bos, "An in-depth analysis of disassembly on full-scale x86/x64 binaries," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 583–600, scan for other research project, demonstrates disasembly capability modernly as a survey paper minute 47.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/andriesse

[12] S. Angel, R. S. Wahby, M. Howald, J. B. Leners, M. Spilo, Z. Sun, A. J. Blumberg, and M. Walfish, "Defending against malicious peripherals with cinch," in *25th {USENIX} Security Symposium ({USENIX} Security*

16). {USENIX} Association, pp. 397–414, a physical solution to provide a untrusted computer conection to trusted computer to protect from perphrials I think like USB periphrials minute 37.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/angel

[13] K. Bartos, M. Sofka, and V. Franc, "Optimized invariant representation of network traffic for detecting unseen malware variants," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 807–822, creating a processing system to detect known and new mutated advanced persistent threats minute 46.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/bartos

[14] M. A. Bashir, S. Arshad, W. Robertson, and C. Wilson, "Tracing information flows between ad exchanges using retargeted ads," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 481–496, how to detect and limit information flow between ad exchanges and ad targeting of user information 1.00 minute 8.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/bashir

[15] A. Biryukov and D. Khovratovich, "Egalitarian computing," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 315–326, proposes using FPGAs and GPUs to do conterdefensive computing measure to make equal dificulty for attackers minute 54.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/biryukov

[16] Y. Cao, Z. Qian, Z. Wang, T. Dao, S. V. Krishnamurthy, and L. M. Marvel, "Off-path {TCP} exploits: Global rate limit considered dangerous," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 209–225, discuses vulnerability CVE-2016-5696 published in TCP and how to mitigate it 1.00 minute 4.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/cao

[17] N. Carlini, P. Mishra, T. Vaidya, Y. Zhang, M. Sherr, C. Shields, D. Wagner, and W. Zhou, "Hidden voice commands," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 513–530, voice interaction for devices is common, authors create commands to attack these systems minute 33.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/carlini

[18] M. Caselli, E. Zambon, J. Amann, R. Sommer, and F. Kargl, "Specification mining for intrusion detection in networked control systems," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX}

Association, pp. 791–806, create an automated rule generation for IDS minute 20.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/caselli

[19] S. Cristalli, M. Pagnozzi, M. Graziano, A. Lanzi, and D. Balzarotti, "Micro-virtualization memory tracing to detect and prevent spraying attacks," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 431–446, stop the pain. . . .this paper talks about creating a hypervisor that protects from spraying attacks against hidden memory minute 25.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/stefano

[20] S. Dechand, D. Schürmann, K. Busse, Y. Acar, S. Fahl, and M. Smith, "An empirical study of textual key-fingerprint representations," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 193–208, focused on vulnerabilities in fingerprenting using hexadecimal strings and provides a proposed solution 1.00 minute 20.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/dechand

[21] B. Dowling, D. Stebila, and G. Zaverucha, "Authenticated network time synchronization," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 823–840, created an authenticated ntp in order to protect systems from a timing attack minute 35.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/dowling

[22] K. Du, H. Yang, Z. Li, H. Duan, and K. Zhang, "The ever-changing labyrinth: A large-scale analysis of wildcard {DNS} powered blackhat {SEO}," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 245–262, interesting but focused on SEO and crawler DNS wildcard malicious activity 1.00 minute 0.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/du

[23] E. Elnikety, A. Mehta, A. Vahldiek-Oberwagner, D. Garg, and P. Druschel, "Thoth: Comprehensive policy compliance in data retrieval systems," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 637–654, a confidential preservering data capture solutino for large and complex systems minute 30.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/elnikety

[24] C. Garman, M. Green, G. Kaptchuk, I. Miers, and M. Rushanan, "Dancing on the lip of the volcano: Chosen ciphertext attacks on apple iMessage," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 655–672, a possible way to decrypt a ciphertext conversation after it occurred on a iphone minute 37.00 seconds.

[Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/garman

[25] T. V. Goethem, M. Vanhoef, F. Piessens, and W. Joosen, "Request and conquer: Exposing cross-origin resource size," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 447–462, vulnerabilities in TLS based on packet size that allow an attacker to get PII minute 37.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/goethem

[26] E. Gökta\${\textbackslash}backslash\$c s, R. Gawlik, B. Kollenda, E. Athanasopoulos, G. Portokalidis, C. Giuffrida, and H. Bos, "Undermining information hiding (and what to do about it)," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 105–119, focused on how to break information hiding with stack spraying 1.00 minute 47.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/goktas

[27] S. Jana, Y. J. Kang, S. Roth, and B. Ray, "Automatically detecting error handling bugs using error specifications," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 345–362, research into error finding in primitive languages like C that do not provide error handeling automatically minute 51.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/jana

[28] A. Kharaz, S. Arshad, C. Mulliner, W. Robertson, and E. Kirda, "{UNVEIL}: A large-scale, automated approach to detecting ransomware," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 757–772, usefull for another study because it detects when ransomware interacts with user data, kind of like a hypervisor but kind of not minute 47.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/kharaz

[29] E. K. Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, and B. Ford, "Enhancing bitcoin security and performance with strong consistency via collective signing," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 279–296, BitCoin processing through a better method minute 50.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/kogias

[30] D. Kohlbrenner and H. Shacham, "Trusted browsers for uncertain times," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 463–480, how to protect against fuzzing time in java timing reference codes minute 39.00 seconds.

[Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/kohlbrenner

[31] P. Kotzias, L. Bilge, and J. Caballero, "Measuring {PUP} prevalence and {PUP} distribution through pay-per-install services," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 739–756, study of unwanted sofware and analyzing it minute 27.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/kotzias

[32] M. Lipp, D. Gruss, R. Spreitzer, C. Maurice, and S. Mangard, "ARMageddon: Cache attacks on mobile devices," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 549–564, how to do side channell attacks on andriod multi ARM processor architecture minute 28.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/lipp

[33] G. Maisuradze, M. Backes, and C. Rossow, "What cannot be read, cannot be leveraged? revisiting assumptions of JIT-ROP defenses," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 139–156, focused on executable run time compile on demand schemes called JIT-ROP 1.00 minute 50.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/maisuradze

[34] G. Nakibly, J. Schcolnik, and Y. Rubin, "Website-targeted false content injection by network operators," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 227–244, interesting but focused on injection of material for web sites from operators 1.00 minute 42.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/nakibly

[35] T. Nelms, R. Perdisci, M. Antonakakis, and M. Ahamad, "Towards measuring and mitigating social engineering software download attacks," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 773–789, study of sucesfull social engineering tactics to lure users to download malware minute 24.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/nelms

[36] O. Ohrimenko, F. Schuster, C. Fournet, A. Mehta, S. Nowozin, K. Vaswani, and M. Costa, "Oblivious multi-party machine learning on trusted processors," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 619–636, machine learning using multiple data sets but keeping privacy of the data sets minute 36.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/ohrimenko

[37] A. Oikonomopoulos, E. Athanasopoulos, H. Bos, and C. Giuffrida, "Poking holes in information hiding," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 121–138, focused on how to break information hiding with large memory addressing 1.00 minute 32.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/oikonomopoulos

[38] P. Pessl, D. Gruss, C. Maurice, M. Schwarz, and S. Mangard, "{DRAMA}: Exploiting {DRAM} addressing for cross-CPU attacks," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 565–581, how to maliciously gain access to data on hypervised machine like server to gain access to other cloud users minute 30.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/pessl

[39] D. Plohmann, K. Yakdan, M. Klatt, J. Bader, and E. Gerhards-Padilla, "A comprehensive measurement study of domain generating malware," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 263–278, focused on botnets command and control through Domain Generation Algorithms (DGAs) 1.00 minute 48.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/plohmann

[40] A. Rane, C. Lin, and M. Tiwari, "Secure, precise, and fast floating-point operations on x86 processors," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 71–86, memory floating point and side channells 1.00 minute 18.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/rane

[41] K. Razavi, B. Gras, E. Bosman, B. Preneel, C. Giuffrida, and H. Bos, "Flip feng shui: Hammering a needle in the software stack," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 1–18, focused on memory management manipulation to gain values such as secret key 4.00 minute 30.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/razavi

[42] P. Rindal and M. Rosulek, "Faster malicious 2-party secure computation with online/offline dual execution," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 297–314, proposes a more secure protocol for P2P 1.00 minute 10.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/rindal

[43] W. Song, H. Choi, J. Kim, E. Kim, Y. Kim, and J. Kim, "PIkit: A new kernel-independent processor-interconnect rootkit," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association,

pp. 37–51, focused on memory management row hammer of DRAM 1.00 minute 45.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/song

[44] R. Strackx and F. Piessens, "Ariadne: A minimal approach to state continuity," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 875–892, a solution to isolated processing that has caused inconsistent states minute 31.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/strackx

[45] K. Thomas, J. A. E. Crespo, R. Rasti, J.-M. Picod, C. Phillips, M.-A. Decoste, C. Sharp, F. Tirelo, A. Tofigh, M.-A. Courteau, L. Ballard, R. Shield, N. Jagpal, M. A. Rajab, P. Mavrommatis, N. Provos, E. Bursztein, and D. McCoy, "Investigating commercial pay-per-install and the distribution of unwanted software," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 721–739, analysis of pay-per install as bundled comodatee minute 21.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/thomas

[46] D. J. Tian, N. Scaife, A. Bates, K. Butler, and P. Traynor, "Making {USB} great again with {USBFILTER}," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 415–430, packet level accesss control for USB devices minute 38.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/tian

[47] S. Torres-Arias, A. K. Ammula, R. Curtmola, and J. Cappos, "On omitting commits and committing omissions: Preventing git metadata tampering that (re)introduces software vulnerabilities," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 379–395, a metadata attack on repositories like GIT that provide malicious options to inject unsafe code minute 41.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/torres-arias

[48] F. Tramèr, F. Zhang, A. Juels, M. K. Reiter, and T. Ristenpart, "Stealing machine learning models via prediction APIs," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 601–618, a black box test is built that can steal a confidential Machine learning model minute 42.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/tramer

[49] A. Vasudevan, S. Chaki, P. Maniatis, L. Jia, and A. Datta, "überSpark: Enforcing verifiable object abstractions for automated compositional security analysis of a hypervisor," in *25th {USENIX}*

Security Symposium ({USENIX} Security 16). {USENIX} Association, pp. 87–104, focused on hypervisors 1.00 minute 2.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/vasudevan

[50] D. L. Wheeler, "zxcvbn: Low-budget password strength estimation," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 157–173, replacement code for Lower Upercase and Digits and Symbols password strength estimator (LUDS) 1.00 minute 15.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/wheeler

[51] Y. Xu, T. Price, J.-M. Frahm, and F. Monrose, "Virtual u: Defeating face liveness detection by building virtual models from your public photos," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 497–512, how to defeat facial recongnition software by 3D rendering of 2d social pictures of target minute 33.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/xu

[52] I. Yun, C. Min, X. Si, Y. Jang, T. Kim, and M. Naik, "APISan: Sanitizing {API} usages through semantic cross-checking," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 363–378, tool to quality check code for secure API ussage minute 36.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/yun

[53] Y. Zhang, J. Katz, and C. Papamanthou, "All your queries are belong to us: The power of file-injection attacks on searchable encryption," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association, pp. 707–720, query and injection methods for breakign encryption on systems minute 28.00 seconds. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/zhang

[54] *25th {USENIX} Security Symposium ({USENIX} Security 16)*. {USENIX} Association. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16