Index

Note: Page numbers followed by f and t indicate figures and tables respectively

A
ABCD parameters, 33, 37
Access points (APs), 23
wireless, 132
Access Vector Cache (AVC), 165
ACP scan, 120
Acquisition setup, 13, 15, 16
Active fingerprinting, 119–122
Active identification, 13
Advanced Persistent Threat (APT) detection, 148
Analog VHF transmitters, 8
AND gate transitions, 42–43
Asymmetric key cryptography, 40
Authentication, 1–2, 39–40
Authentication schemes, conventional, 72
Authentication system, 57–58
receiver, 74–76
transmitter, 73–74
Automatic provenance-aware systems, 144
in applications, 145–147
in middleware, 145
in operating systems, 144

B
Background on fingerprinting, 93–94
Beacon-enabled IEEE 802.15.4 network, 56f
BEEP systems, 146, 148
Bluetooth transceivers, 8, 20
Boolean satisfiability (SAT) problem, 96, 97f
Bring Your Own Device (BYOD) policies, 117

C
Certificate of authenticity, 62f
Certified code execution, 52
Challenge-response models, 39
Challenge-response pairs, obtaining, 51–52, 51f
Channel state information (CSI), 74, 78
precoding and power-allocation with CSI, 85–86
Characteristic frequency components, 126, 129
Circuit model, 31
Classification error rate, 15, 24
Clock skew, 23, 52
definition, 52–53
estimation, 53–54
exploiting, 55–57
network authentication, 55
pitfalls, 57–58
Collusion attack, 109, 113
Communications channels, 71
Compact discs (CDs), 61
Component behaviour, 31
Component significance, determining, 36
constructing model input, 36
evaluating model output, 37–38
identity, 38
significance, 37–38
producing model output, 36–37
Conceptual fingerprint, 91f
Constraint-addition, fingerprinting with, 98–100
Constraint-based watermarking technique, 90, 94
Controlled physical unclonable functions, 49
certified code execution, 52
challenge-response pairs, obtaining, 51–52
initialization, 50
primitives, 49
secret key establishment, 50
Core Provenance Library (CPL), 145, 146
Core root of trust for measurement (CRTM), 164
Core under test (CUT), 110
CPU heat pattern, 3
Crypto-based methods and fingerprints, 39, 179
authentication, 39–40
key generation, 40
asymmetric keys, 40
symmetric keys, 40
techniques, 41
clock skew, 52–58
controlled physical unclonable functions, 49–52
physical unclonable functions (PUFs), 41–49
software control, 63–64
Trojan detection, 63
wireless devices, 58–63
tradeoffs, 64
benefits, 64
drawbacks, 65

D
Data collection, 178
setup, 132f
Data-dependency, 13
Data provenance, 142, 143, 144, 147, 148
DBNotes, 145
Delay-based implementation, 42–44
Denial, of fingerprint, 112
Device fingerprints, 2, 3, 12–13, 41, 177, 180
Device measurement and origin of variation, 31–38
ABCD parameters, 33
component significance, determining, 36
constructing model input, 36
evaluating model output, 37–38
producing model output, 36–37
measuring parameters, 34–35
proposed model, 33–34
Device under identification, 7, 8–9, 25
D-flip flop, 41–42, 110
Digital Signature Algorithm (DSA) signatures, 163
Digital versatile discs (DVDs), 61
Disclosed Provenance API (DPAPI), 145, 146
Disclosed provenance-aware systems, 143
Discrete Fourier Transform (DFT), 130
Discrete model, 31
Discrete Wavelet Transform (DWT), 11
Don’t Fragment (DF) bit, 118
Doppler effect, 179

E
Earth Science System Workbench, 143, 145
Embedded authentication, 72
framework for, 72
authentication performance, 77
receiver, 74–76
transmitter, 73–74
system diagram, 73f
Embedded fingerprint authentication, 77
metrics for, 77
authentication performance, 78
impact on data BER, 77–78
security analysis, 79
complexity, 81–82
impersonation and substitution attacks, 81
key equivocation, 79–81
Encrypted traffic, analysis of, 124
End of Option List (EOL), 118
Equal Error Rate (EER), 15
Equivocation, 79, 82–84
multiple observations, 80–81
noiseless observations, 79–80
noisy observations, 80
Error correcting syndrome values, 45–46
Error correction, 46
Error-tolerance assumption, 93, 94
Execution partitioning (EP) step, 146
Hi-Fi, completeness analysis of, 165
exfiltration, 168
persistence and stealth, 166–167
recording malicious behavior, 165–166
remote control, 167–168
spread, 168–169
High-fidelity whole systems provenance, 150, 160
design of Hi-Fi, 150–151
implementation of Hi-Fi, 154
bootstrapping filesystem provenance, 155–156
earlyboot provenance, 154–155
opaque provenance, 156
OS integration, 155
provenance logging, 154
socket provenance, 156–158
limitations of Hi-Fi, 158
system-level objects, handling of, 151–154
Host discovery, 120

I
ICBM Echo request, 120
ICBM messages, 119
ICMP timestamps, 55
Ideal fingerprint, 91
Identification signals, 7, 9
IEEE 802.11a device identification, 22
IEEE 802.11 transceivers, 8, 8f, 20
IEEE 802.11 transient signals, 20
IEEE 802.15.4 transceivers, 8
IEEE 802.15.4 wireless sensor node network, 55
Inferred features, 9, 11, 12f, 24
Inferring users’ online activities through traffic analysis, 123
In-specification characteristics, 9
Integrated circuits (ICs), 89
Integrity Measurement Architecture (IMA), 163
Intrinsic fingerprints, 69–70
IP intruder, 90
IP protection, digital fingerprinting for, 93
background on fingerprinting, 93–94
constraint-addition, fingerprinting with, 98–100
iterative fingerprinting techniques, 95–98
need and challenge of digital fingerprinting IPs, 94
requirements of digital fingerprinting, 94–95
ISO 14443 RFID transponders, 21
Iterative fingerprinting techniques, 95–98

K
K-bit fingerprints, 106
Key extraction, 60f, 61
Key generation, 40
  asymmetric keys, 40
  symmetric keys, 40

L
LineageFS, 160
Linear programming method, 53–54
Linksys CompactWireless USB adapter (WUSB54GC), 132
Linux Integrity Measurement Architecture (IMA), 163
Linux kernel’s boot-time initialization process, 154
Linux provenance modules (LPM), 159
  augmenting whole-system provenance, 159–160
deploying, 164–165
design of, 161, 161f
  netfilter hooks, 162–163
  provenance hooks, 162
  workflow provenance, 163–164
security analysis of, 169
  authenticated channel, 170
  authenticated disclosures, 170–171
  complete, 169–170
tamperproof, 170
verifiable, 170
threat model, 160–161
Linux Security Module (LSM), 150
LogGC system, 146, 148

M
Mandatory Access Control (MAC), 148, 158, 165
Marking assumption, 93
Maximum Segment Size (MSS), 118
Measurements of fingerprints, 178–179
Memory-backed “pseudo-filesystems”, 154
Message authentication code (MAC), 51–52
Messages, authenticating, 71
MIMO systems, 16, 26
MIMO transmission, 72
Modification, fingerprint, 112
Modulation-based identification techniques, 21
Multiplexer-based arbiter implementation, 41–42

N
Network analysers, 35
Network authentication, 55
Network traffic fingerprinting, 3
NI-USRP software-defined radios, 82
nmap program, 120
Noise, 45–48
Noise frequency components, 126, 129
No-Operation (NOP), 118

O
Observability Don’t Care (ODC) fingerprinting, 100
  conditions, 101
determining potential fingerprinting modifications, 102–103
finding locations for circuit modification based on, 101–102
illustrative example, 100
ODC trigger signal, 102
overhead constraints, maintaining, 103
security analysis, 103–104
Operating System (OS) fingerprinting, 115
  active fingerprinting, 119–122
detection, 120
encrypted traffic, analysis of, 124
future directions, 135
packet-content agnostic traffic analysis, 122
  hidden services, 123
  inferring users’ online activities through traffic analysis, 123
website fingerprinting, 122–123
passive fingerprinting, 117–119
smartphone OS reconnaissance, 124
  empirical evaluation, 132–135
  identifying, 128–132
  system model, 127
  threat model, 127
  smartphone traffic, analysis of, 123–124
Optical disc fingerprints, 62f
Optical media, 61–63
Oscillator implementation, 44–45
Out-specification characteristics, 9
Oven controlled crystal oscillators (OCXOs), 57
Packet-content agnostic traffic analysis, reconnaissance through, 122, see also Reconnaissance hidden services, 123
inflerring users’ online activities through traffic analysis, 123
website fingerprinting, 122–123
Passive fingerprinting, 117–119
Passive identification, 13
PERM (Provenance Extension of the Relational Model), 145
Physical-layer device identification, 5–6, 13–14, 18t–19t, 22–23
attacking, 23–24
device under identification, 8–9
tentities involved in, 7f
general view, 6–8
improving, 15–17
system performance and design issues, 14–15
uses of, 6
Physical realizations, 45
Physical unclonable functions (PUFs), 41, 63, 91
controlled PUFs, 49
certified code execution, 52
challenge-response pairs, obtaining, 51–52
initialization, 50
primitives, 49
secret key establishment, 50
delay-based implementation, 42–44
improvements, 49
multiplexer-based arbiter implementation, 41–42
noise, 45–48
oscillator implementation, 44–45
privacy, 48
Platform Configuration Registers (PCRs), 148
Platform Control Register (PCR), 163
Population sensitivity, 180–181
Port scanning, 120
POSIX shared memory, 153
Post-silicon design phase, 92, 100
Potential fingerprinting modifications, determining, 102–103
Predefined features, 9, 11, 12f, 24
Pre-silicon design phase, 92
Primitives, cryptographic, 49
Privacy, 26, 48
Probabilistic neural network (PNN), 14, 20
Propagating lineage information as datasets, 145
Provenance-aware application (PAA), 146, 148, 163
Provenance-Aware Storage System (PASS) instruments, 144, 160
Provenance-aware systems, 142
automatic provenance-aware systems, 144
in applications, 145–147
in middleware, 145
in operating systems, 144
disclosed provenance-aware systems, 143
Provenance-based access control schemes (PBAC), 147
Provenance collection, security challenges to, 147–149
Provenance monitor concept, 149–150, 158
Provenance monitors, analyzing security of, 165
Hi-Fi, completeness analysis of, 165, see also High-fidelity whole systems provenanceexfiltration, 168
persistence and stealth, 166–167
recording malicious behavior, 165–166
remote control, 167–168
spread, 168–169
Linux provenance modules (LPM), security analysis of, 169, see also Linux provenance modules (LPM) authenticated channel, 170
authenticated disclosures, 170–171
complete, 169–170
tamperproof, 170
verifiable, 170
Pseudo-filesystems, 154
Radio frequency, 58–59
Rayleigh fading, 78
Received signal strength indicator (RSSI), 60
Receiver Operating Characteristic (ROC), 15
Reconnaissance, 117, 127, see also
Smartphone OS reconnaissance, case study through packet-content agnostic traffic analysis, 122
hidden services, 123
inflerring users’ online activities through traffic analysis, 123
website fingerprinting, 122–123
Regular files, 152
Relay, defined, 154
Removal, fingerprint, 112
Request for Comments (RFC), 120
Requirements of digital fingerprinting, 94–95
Reuse-based IP business models, 90
RFID device, 8
RFID transponder, 8f, 14
Ring oscillators, 44f, 47
Robust fingerprints, 26
Robustness, 13, 25

S
Satisfiability Don’t Care (SDC) fingerprinting, 104
assumptions for, 105–106
fingerprint embedding scheme, 107–108
and illustrative example, 104–105
security analysis, 108–109
technique, 106–107
Scalar network analysers, 35
Scan chain fingerprinting, 109, 111
basics on scan chain design, 110–111
illustrative example, 109–110
security analysis, 111–113
Science of fingerprints, 179–180
SCTP scan, 120, 157
Secret key establishment, 50
Secure and trustworthy provenance
collection for digital forensics, 141
analyzing security of provenance
monitors, 165
completeness analysis of Hi-Fi,
165–169
security analysis of LPM, 169–171
ensuring trustworthiness of provenance,
147
provenance monitor concept,
149–150
security challenges to provenance
collection, 147–149
future challenges, 171–172
high-fidelity whole systems provenance,
150
design of Hi-Fi, 150–151
handling of system-level objects,
151–154
Hi-Fi implementation, 154–158
limitations of Hi-Fi, 158
Linux provenance modules, 159 see
also Linux provenance modules
(LPM) augmenting whole-system
provenance, 159–160
deploying LPM, 164–165
design of LPM, 161–164
threat model, 160–161
provenance-aware systems, 142
automatic provenance-aware
systems, 144–147
disclosed provenance-aware
systems, 143
Security and privacy of device identification,
26
Security of fingerprints, 180–181
Selective Acknowledgement (SackOk), 118
Self-timed delay, 43f
SELinux Access Vector Cache (AVC) Log,
170
Shared secret keys, 49, 51, 71
Simple modification attack, 109
Simple removal attack, 108
Smartphone OS reconnaissance, case study,
124
empirical evaluation, 132
experiment setup, 132
identification of minor versions of
smartphone OSes, 134
length of traffic traces, 133–134
performance metrics, 133
running time, 135
identifying, 128
identification algorithm, 129–132
rationale, 128–129
system model, 127
threat model, 127
Smartphone traffic, analysis of, 123–124
Socket identifiers, 154
Socket provenance, 151, 156–158
TCP sockets, 157
UDP sockets, 157–158
Software control, 63–64
SPADE, 144, 148, 159, 171
S-parameters, 34, 35
Specifications, 9
Statistical feature extraction, 16–17
Steganography, 71
Support Vector Machines (SVM), 14
SVM classifier, 21
Symmetric keys, 40
SYN-ACP packet, 118
SYN packet, 117, 118
System on a chip (SoC) paradigm, 89
**T**
TCP NULL, FIN, and Xmas scan, 120
TCP scan, 120
TCP signatures, 117
TCP SYN scan, 120
TCP timestamps, 55, 56
TCP Window scan, 120
Time domain methods, 59
Time synchronization, 57f
Time Synchronization Function, 55
Time-to-Live (TTL), 117
Timestamps, 55, 55f
Tmote Sky sensor devices, 21
Tor network, 56, 123
TPM Platform Control Register (PCR), 163
Tradeoffs, 64
  benefits, 64
drawbacks, 65
Transient-based device identification, 17, 20–21
Trojans, 93
detection, 63
Trusted Platform Module (TPM) attestations, 148, 164
Two-port model, 32
Type of Service (ToS) flags, 118

**U**
UDP scan, 120
UHF RFID tags, 22
UHF RFID transponders, 8
UHF sensor nodes, 8

*Unique identification, causes of, 25–26
USRPI devices, 82
UUIDs, 151, 153, 154*

**V**
Vector network analysers, 35
Version detection, 120
VHF FM transmitters, 17, 20
VLSI design cycle, 92, 92f

**W**
Watermarking, 3, 90
Wavelet analysis, 17
Wavelet transformations, 11
Website fingerprinting, 122–123
WiFi communication, 127
Window Scale value, 118
Wireless devices, 58
classes of, 8f
optical media, 61–63
physical-layer identification of, 7f
radio frequency, 58–59
wireless link key extraction, 59–61
Wireless link key extraction, 59–61
Write-once read-many (WORM) storage system, 151

**Z**
Zab trojan, 167