



Efficient Data Structures for Tamper-Evident Logging

Scott A. Crosby

Dan S. Wallach

Rice University

Presented at USENIX Security 2009

Reliance on logs

Assume the adversary doesn't tamper with the logs.

<p>Towards Scalable Cluster Auditing through Grammatical Inference over Provenance Graphs</p> <p>Wajih Ul Hassan, Mark Lemay,¹ Nuruln Agase, Adam Bates, Thomas Moyer*</p> <p>University of Illinois at Urbana-Champaign {whassan3, aguse2, bates}@illinois.edu</p> <p>¹ Boston University lemay@bu.edu</p> <p>* UNC Charlotte tom.moyer@unc.edu</p> <p>Abstract—Investigating the nature of system intrusions in large distributed systems remains a notoriously difficult challenge. While monitoring tools (e.g., Firewalk, IDS) provide preliminary alerts through easy-to-use administrative interfaces, attack reconstruction still requires that administrators sift through gigabytes of system audit logs stored locally on hundreds of machines. At present, two fundamental obstacles prevent synergy between system-layer auditing and modern cluster monitoring tools: 1) the sheer volume of audit data generated in a data center is prohibitively costly to transmit to a central node, and 2) system-layer auditing poses a “needle-in-a-haystack” problem, such that hundreds of employee hours may be required to diagnose a single intrusion.</p> <p>This paper presents Winmover, a scalable system for audit-based cluster monitoring that addresses these challenges. Our key insight is that, for tasks that are replicated across nodes in a distributed application, a model can be defined over audit logs to succinctly summarize the behavior of many nodes, thus eliminating the need to transmit redundant audit records to a central monitoring node. Specifically, Winmover parses audit records into provenance graphs that describe the actions of individual nodes, then performs grammatical inference over individual graphs using a novel adaptation of Deterministic Finite Automata (DFA) Learning to produce a behavioral model of many nodes at once. This provenance model can be efficiently transmitted to a central node and used to identify anomalous events in the cluster. We have implemented Winmover for Docker Swarm container clusters and evaluate our system against real-world applications and attacks. We show that Winmover dramatically reduces storage and network overhead associated with aggregating system audit logs by as much as 98%, without sacrificing the important information needed for attack investigation. Winmover thus represents a significant step forward for security monitoring in distributed systems.</p>	<p>Session F2: Insights from Logins</p> <p>DeepLog: Anomaly Detection and Diagnosis from System Logs through Deep Learning</p> <p>Min Du, Feifei Li, Guineng Zheng, Vivek Srikumar</p> <p>School of Computing, University of Utah {mind, lifefei, guineng, srivek}@cs.utah.edu</p> <p>ABSTRACT</p> <p>Anomaly detection is a critical step towards building a secure and trustworthy system. The primary purpose of a system log is to record system state and significant events at various critical points to help debug performance issues and failures, and perform root cause analysis. Such log data is universally available in nearly all computer systems and is a valuable resource for understanding system status. Furthermore, since system logs record</p> <p>challenging and many traditional anomaly detection methods based on standard mining methodologies are no longer effective. System logs record system state and significant events at various critical points to help debug performance issues and failures, and perform root cause analysis. Such log data is universally available in nearly all computer systems and is a valuable resource for understanding system status. Furthermore, since system logs record</p>	<p>RAIN: Refinable Attack Investigation with On-demand Inter-Process Information Flow Tracking</p> <p>Yang Ji, Sangho Lee, Evan Downing, Weiren Wang, Mattia Fazzini, Tassos Kim, Alessandro Orso, and Wenke Lee</p> <p>Georgia Institute of Technology</p> <p>ABSTRACT</p> <p>As modern attacks become more stealthy and persistent, detecting or preventing them at their early stages becomes virtually impossible. Instead, an attack investigation or provenance system aims to continuously monitor and log interesting system events with minimal overhead. Later, if the system observes any anomalous behavior, it analyzes the logs to identify which processes initiated the attack and</p>	<p>Intrusion Recovery Using Selective Re-execution</p> <p>Tassos Kim, Xi Wang, Nikolai Zeldovich, and M. Frans Kaashoek</p> <p>MIT CSAIL</p> <p>ABSTRACT</p> <p>Recovery requires a desktop or server after an adversary compromises it, by undoing the adversary's changes while preserving legitimate user actions, with minimal user involvement. During normal operation, RECOVER records an activity history graph, which is a detailed dependency graph describing the system's execution. RECOVER uses its knowledge to describe each system state and its actions as a single</p> <p>ing actions from the past, such as a TCP connection or an HTTP request from an adversary, that they want to undo. RECOVER then queries the system's state to find the history by selectively undoing the offending actions—but is, essentially, a new system state, as if the offending actions never took place, but all legitimate actions remained. Thus, by selectively undoing the adversary's changes while preserving user actions, RECOVER makes intrusion recovery more precise.</p> <p>In these initial stages during RECOVER, consider the following attack, which we will use as a running example in this paper. For an on-demand computer system, a Linux machine and client is a node. To make her fail, the adversary has had her nodes crash the system log. She then creates a new node on the system, including a new account for user, and a PHP script that allows her to execute arbitrary commands via HTTP. For her success, she has to download and install a binary client. To ensure control of the machine, the adversary adds a line to the <code>/usr/bin/crontab</code> shell script to trigger for PHP to restart her bot. In the meantime, legitimate users log in, install their own PHP scripts, use text editors, and use other legitimate users.</p> <p>To make attacks, RECOVER provides a system-wide, real-time view of existing actions, changes, and effects in order to identify all downstream effects of a compromise. The key challenge is that a compromise in the past may have effects on subsequent legitimate actions, especially if the administrator discovers an attack long after it occurred. RECOVER must verify that this undoing is not malicious and is necessary. In our running example, the changes to the <code>crontab</code> file and to <code>crontab</code> are not part with legitimate users that modified or created the <code>crontab</code> file, or used <code>crontab</code>. If legitimate users can</p>
<p>ProTracer: Towards Practical Provenance Tracing by Alternating Between Logging and Tainting</p> <p>Shiqing Ma, Purdue University shiqingma@purdue.edu</p> <p>Xiangyu Zhang, Purdue University xyzhong@purdue.edu</p> <p>Dongyan Xu, Purdue University xdyanxu@purdue.edu</p> <p>Abstract—Provenance tracing is a very important approach to Advanced Persistent Threat (APT) attack detection and investigation. Existing techniques either suffer from the dependence on logging or tainting, which is not practical in large-scale systems. We propose ProTracer, a hybrid provenance tracing system that alternates between system event logging and unit level tainting. The technique is built on an on-the-fly system event processing infrastructure that features a very lightweight kernel module and a sophisticated user space daemon that performs on-demand and just-in-time event processing. The evaluation</p>	<p>Transparent Web Service Auditing via Network Provenance Functions*</p> <p>Adam Bates, Wajih Ul Hassan, University of Illinois at Urbana-Champaign {abates, whassan3}@illinois.edu</p> <p>Kevin Butler, Bradley Heavies, University of Florida {butler, daddio, heavies}@uf.edu</p> <p>Patrick Cable, Thomas Moyer, Nabil Schohar, MIT Lincoln Laboratory {poc, n.schohar, rzh}@mit.edu</p> <p>ABSTRACT</p> <p>Logging and capturing the nature of attacks in distributed web services is often difficult—examining the nature of suspicious activity requires following the trail of an attacker through a chain of heterogeneous systems comprising load balancers, proxies, web servers, and other services. Unfortunately, existing forensic solutions cannot provide the necessary context to link across these complex workflows, particularly in instances where the forensic data is distributed across multiple systems.</p>	<p>Backtracking Intrusions</p> <p>Samuel T. King, University of Michigan kingst@umich.edu</p> <p>Department of Electrical Engineering and Computer Science, University of Michigan Ann Arbor, MI 48109-2122</p> <p>Peter M. Chen, University of Michigan pmchen@umich.edu</p> <p>ABSTRACT</p> <p>Analysing intrusions today is an arduous, largely manual task because system administrators lack the information and tools needed to understand easily the sequence of events that occurred in an attack. The goal of BackTracker is to facilitate automatically generated sequences of steps that occurred in an intrusion, starting with a single execution point (e.g., a specific file). BackTracker identifies key steps of an intrusion that could have affected the system and displays a chain of events in a dependency graph. We use</p>	<p>LogGC: Garbage Collecting Audit Log</p> <p>Kyu Hyung Lee, Xiangyu Zhang, Dongyan Xu</p> <p>Department of Computer Science and CERAS, Purdue University West Lafayette, IN 47907, USA {kyuhlee, xyzhong, dxu}@cs.purdue.edu</p> <p>ABSTRACT</p> <p>System-level audit logs capture the interaction between applications and the system environment. They are highly valuable for forensic analysis of the system. However, they are also highly sensitive to tampering. In this paper, we propose LogGC, an on-the-fly logging system with garbage collection (GC) capability. We identify and overcome the unique challenges of garbage collection in the context of computer forensic analysis, which makes LogGC different from traditional memory GC techniques. We also develop techniques that increment our application state and handle the stateful data in our additional system events so that we can substantially reduce the false positives between system events to GC effectiveness. Our results show that LogGC can reduce audit log size by 3.5 times for regular user systems and 37 times for server systems, without affecting the accuracy or processing analysis.</p> <p>Categories and Subject Descriptors</p> <p>D.4.5 Management of Computing and Information Systems; D.4.6 Operating Systems; D.4.7 Operating Systems; D.4.8 Operating Systems; D.4.9 Operating Systems; D.4.10 Operating Systems; D.4.11 Operating Systems; D.4.12 Operating Systems; D.4.13 Operating Systems; D.4.14 Operating Systems; D.4.15 Operating Systems; D.4.16 Operating Systems; D.4.17 Operating Systems; D.4.18 Operating Systems; D.4.19 Operating Systems; D.4.20 Operating Systems; D.4.21 Operating Systems; D.4.22 Operating Systems; D.4.23 Operating Systems; D.4.24 Operating Systems; D.4.25 Operating Systems; D.4.26 Operating Systems; D.4.27 Operating Systems; D.4.28 Operating Systems; D.4.29 Operating Systems; D.4.30 Operating Systems; D.4.31 Operating Systems; D.4.32 Operating Systems; D.4.33 Operating Systems; D.4.34 Operating Systems; D.4.35 Operating Systems; D.4.36 Operating Systems; D.4.37 Operating Systems; D.4.38 Operating Systems; D.4.39 Operating Systems; D.4.40 Operating Systems; D.4.41 Operating Systems; D.4.42 Operating Systems; D.4.43 Operating Systems; D.4.44 Operating Systems; D.4.45 Operating Systems; D.4.46 Operating Systems; D.4.47 Operating Systems; D.4.48 Operating Systems; D.4.49 Operating Systems; D.4.50 Operating Systems; D.4.51 Operating Systems; D.4.52 Operating Systems; D.4.53 Operating Systems; D.4.54 Operating Systems; D.4.55 Operating Systems; D.4.56 Operating Systems; D.4.57 Operating Systems; D.4.58 Operating Systems; D.4.59 Operating Systems; D.4.60 Operating Systems; D.4.61 Operating Systems; D.4.62 Operating Systems; D.4.63 Operating Systems; D.4.64 Operating Systems; D.4.65 Operating Systems; D.4.66 Operating Systems; D.4.67 Operating Systems; D.4.68 Operating Systems; D.4.69 Operating Systems; D.4.70 Operating Systems; D.4.71 Operating Systems; D.4.72 Operating Systems; D.4.73 Operating Systems; D.4.74 Operating Systems; D.4.75 Operating Systems; D.4.76 Operating Systems; D.4.77 Operating Systems; D.4.78 Operating Systems; D.4.79 Operating Systems; D.4.80 Operating Systems; D.4.81 Operating Systems; D.4.82 Operating Systems; D.4.83 Operating Systems; D.4.84 Operating Systems; D.4.85 Operating Systems; D.4.86 Operating Systems; D.4.87 Operating Systems; D.4.88 Operating Systems; D.4.89 Operating Systems; D.4.90 Operating Systems; D.4.91 Operating Systems; D.4.92 Operating Systems; D.4.93 Operating Systems; D.4.94 Operating Systems; D.4.95 Operating Systems; D.4.96 Operating Systems; D.4.97 Operating Systems; D.4.98 Operating Systems; D.4.99 Operating Systems; D.4.100 Operating Systems; D.4.101 Operating Systems; D.4.102 Operating Systems; D.4.103 Operating Systems; D.4.104 Operating Systems; D.4.105 Operating Systems; D.4.106 Operating Systems; D.4.107 Operating Systems; D.4.108 Operating Systems; D.4.109 Operating Systems; D.4.110 Operating Systems; D.4.111 Operating Systems; D.4.112 Operating Systems; D.4.113 Operating Systems; D.4.114 Operating Systems; D.4.115 Operating Systems; D.4.116 Operating Systems; D.4.117 Operating Systems; D.4.118 Operating Systems; D.4.119 Operating Systems; D.4.120 Operating Systems; D.4.121 Operating Systems; D.4.122 Operating Systems; D.4.123 Operating Systems; D.4.124 Operating Systems; D.4.125 Operating Systems; D.4.126 Operating Systems; D.4.127 Operating Systems; D.4.128 Operating Systems; D.4.129 Operating Systems; D.4.130 Operating Systems; D.4.131 Operating Systems; D.4.132 Operating Systems; D.4.133 Operating Systems; D.4.134 Operating Systems; D.4.135 Operating Systems; D.4.136 Operating Systems; D.4.137 Operating Systems; D.4.138 Operating Systems; D.4.139 Operating Systems; D.4.140 Operating Systems; D.4.141 Operating Systems; D.4.142 Operating Systems; D.4.143 Operating Systems; D.4.144 Operating Systems; D.4.145 Operating Systems; D.4.146 Operating Systems; D.4.147 Operating Systems; D.4.148 Operating Systems; D.4.149 Operating Systems; D.4.150 Operating Systems; D.4.151 Operating Systems; D.4.152 Operating Systems; D.4.153 Operating Systems; D.4.154 Operating Systems; D.4.155 Operating Systems; D.4.156 Operating Systems; D.4.157 Operating Systems; D.4.158 Operating Systems; D.4.159 Operating Systems; D.4.160 Operating Systems; D.4.161 Operating Systems; D.4.162 Operating Systems; D.4.163 Operating Systems; D.4.164 Operating Systems; D.4.165 Operating Systems; D.4.166 Operating Systems; D.4.167 Operating Systems; D.4.168 Operating Systems; D.4.169 Operating Systems; D.4.170 Operating Systems; D.4.171 Operating Systems; D.4.172 Operating Systems; D.4.173 Operating Systems; D.4.174 Operating Systems; D.4.175 Operating Systems; D.4.176 Operating Systems; D.4.177 Operating Systems; D.4.178 Operating Systems; D.4.179 Operating Systems; D.4.180 Operating Systems; D.4.181 Operating Systems; D.4.182 Operating Systems; D.4.183 Operating Systems; D.4.184 Operating Systems; D.4.185 Operating Systems; D.4.186 Operating Systems; D.4.187 Operating Systems; D.4.188 Operating Systems; D.4.189 Operating Systems; D.4.190 Operating Systems; D.4.191 Operating Systems; D.4.192 Operating Systems; D.4.193 Operating Systems; D.4.194 Operating Systems; D.4.195 Operating Systems; D.4.196 Operating Systems; D.4.197 Operating Systems; D.4.198 Operating Systems; D.4.199 Operating Systems; D.4.200 Operating Systems; D.4.201 Operating Systems; D.4.202 Operating Systems; D.4.203 Operating Systems; D.4.204 Operating Systems; D.4.205 Operating Systems; D.4.206 Operating Systems; D.4.207 Operating Systems; D.4.208 Operating Systems; D.4.209 Operating Systems; D.4.210 Operating Systems; D.4.211 Operating Systems; D.4.212 Operating Systems; D.4.213 Operating Systems; D.4.214 Operating Systems; D.4.215 Operating Systems; D.4.216 Operating Systems; D.4.217 Operating Systems; D.4.218 Operating Systems; D.4.219 Operating Systems; D.4.220 Operating Systems; D.4.221 Operating Systems; D.4.222 Operating Systems; D.4.223 Operating Systems; D.4.224 Operating Systems; D.4.225 Operating Systems; D.4.226 Operating Systems; D.4.227 Operating Systems; D.4.228 Operating Systems; D.4.229 Operating Systems; D.4.230 Operating Systems; D.4.231 Operating Systems; D.4.232 Operating Systems; D.4.233 Operating Systems; D.4.234 Operating Systems; D.4.235 Operating Systems; D.4.236 Operating Systems; D.4.237 Operating Systems; D.4.238 Operating Systems; D.4.239 Operating Systems; D.4.240 Operating Systems; D.4.241 Operating Systems; D.4.242 Operating Systems; D.4.243 Operating Systems; D.4.244 Operating Systems; D.4.245 Operating Systems; D.4.246 Operating Systems; D.4.247 Operating Systems; D.4.248 Operating Systems; D.4.249 Operating Systems; D.4.250 Operating Systems; D.4.251 Operating Systems; D.4.252 Operating Systems; D.4.253 Operating Systems; D.4.254 Operating Systems; D.4.255 Operating Systems; D.4.256 Operating Systems; D.4.257 Operating Systems; D.4.258 Operating Systems; D.4.259 Operating Systems; D.4.260 Operating Systems; D.4.261 Operating Systems; D.4.262 Operating Systems; D.4.263 Operating Systems; D.4.264 Operating Systems; D.4.265 Operating Systems; D.4.266 Operating Systems; D.4.267 Operating Systems; D.4.268 Operating Systems; D.4.269 Operating Systems; D.4.270 Operating Systems; D.4.271 Operating Systems; D.4.272 Operating Systems; D.4.273 Operating Systems; D.4.274 Operating Systems; D.4.275 Operating Systems; D.4.276 Operating Systems; D.4.277 Operating Systems; D.4.278 Operating Systems; D.4.279 Operating Systems; D.4.280 Operating Systems; D.4.281 Operating Systems; D.4.282 Operating Systems; D.4.283 Operating Systems; D.4.284 Operating Systems; D.4.285 Operating Systems; D.4.286 Operating Systems; D.4.287 Operating Systems; D.4.288 Operating Systems; D.4.289 Operating Systems; D.4.290 Operating Systems; D.4.291 Operating Systems; D.4.292 Operating Systems; D.4.293 Operating Systems; D.4.294 Operating Systems; D.4.295 Operating Systems; D.4.296 Operating Systems; D.4.297 Operating Systems; D.4.298 Operating Systems; D.4.299 Operating Systems; D.4.300 Operating Systems; D.4.301 Operating Systems; D.4.302 Operating Systems; D.4.303 Operating Systems; D.4.304 Operating Systems; D.4.305 Operating Systems; D.4.306 Operating Systems; D.4.307 Operating Systems; D.4.308 Operating Systems; D.4.309 Operating Systems; D.4.310 Operating Systems; D.4.311 Operating Systems; D.4.312 Operating Systems; D.4.313 Operating Systems; D.4.314 Operating Systems; D.4.315 Operating Systems; D.4.316 Operating Systems; D.4.317 Operating Systems; D.4.318 Operating Systems; D.4.319 Operating Systems; D.4.320 Operating Systems; D.4.321 Operating Systems; D.4.322 Operating Systems; D.4.323 Operating Systems; D.4.324 Operating Systems; D.4.325 Operating Systems; D.4.326 Operating Systems; D.4.327 Operating Systems; D.4.328 Operating Systems; D.4.329 Operating Systems; D.4.330 Operating Systems; D.4.331 Operating Systems; D.4.332 Operating Systems; D.4.333 Operating Systems; D.4.334 Operating Systems; D.4.335 Operating Systems; D.4.336 Operating Systems; D.4.337 Operating Systems; D.4.338 Operating Systems; D.4.339 Operating Systems; D.4.340 Operating Systems; D.4.341 Operating Systems; D.4.342 Operating Systems; D.4.343 Operating Systems; D.4.344 Operating Systems; D.4.345 Operating Systems; D.4.346 Operating Systems; D.4.347 Operating Systems; D.4.348 Operating Systems; D.4.349 Operating Systems; D.4.350 Operating Systems; D.4.351 Operating Systems; D.4.352 Operating Systems; D.4.353 Operating Systems; D.4.354 Operating Systems; D.4.355 Operating Systems; D.4.356 Operating Systems; D.4.357 Operating Systems; D.4.358 Operating Systems; D.4.359 Operating Systems; D.4.360 Operating Systems; D.4.361 Operating Systems; D.4.362 Operating Systems; D.4.363 Operating Systems; D.4.364 Operating Systems; D.4.365 Operating Systems; D.4.366 Operating Systems; D.4.367 Operating Systems; D.4.368 Operating Systems; D.4.369 Operating Systems; D.4.370 Operating Systems; D.4.371 Operating Systems; D.4.372 Operating Systems; D.4.373 Operating Systems; D.4.374 Operating Systems; D.4.375 Operating Systems; D.4.376 Operating Systems; D.4.377 Operating Systems; D.4.378 Operating Systems; D.4.379 Operating Systems; D.4.380 Operating Systems; D.4.381 Operating Systems; D.4.382 Operating Systems; D.4.383 Operating Systems; D.4.384 Operating Systems; D.4.385 Operating Systems; D.4.386 Operating Systems; D.4.387 Operating Systems; D.4.388 Operating Systems; D.4.389 Operating Systems; D.4.390 Operating Systems; D.4.391 Operating Systems; D.4.392 Operating Systems; D.4.393 Operating Systems; D.4.394 Operating Systems; D.4.395 Operating Systems; D.4.396 Operating Systems; D.4.397 Operating Systems; D.4.398 Operating Systems; D.4.399 Operating Systems; D.4.400 Operating Systems; D.4.401 Operating Systems; D.4.402 Operating Systems; D.4.403 Operating Systems; D.4.404 Operating Systems; D.4.405 Operating Systems; D.4.406 Operating Systems; D.4.407 Operating Systems; D.4.408 Operating Systems; D.4.409 Operating Systems; D.4.410 Operating Systems; D.4.411 Operating Systems; D.4.412 Operating Systems; D.4.413 Operating Systems; D.4.414 Operating Systems; D.4.415 Operating Systems; D.4.416 Operating Systems; D.4.417 Operating Systems; D.4.418 Operating Systems; D.4.419 Operating Systems; D.4.420 Operating Systems; D.4.421 Operating Systems; D.4.422 Operating Systems; D.4.423 Operating Systems; D.4.424 Operating Systems; D.4.425 Operating Systems; D.4.426 Operating Systems; D.4.427 Operating Systems; D.4.428 Operating Systems; D.4.429 Operating Systems; D.4.430 Operating Systems; D.4.431 Operating Systems; D.4.432 Operating Systems; D.4.433 Operating Systems; D.4.434 Operating Systems; D.4.435 Operating Systems; D.4.436 Operating Systems; D.4.437 Operating Systems; D.4.438 Operating Systems; D.4.439 Operating Systems; D.4.440 Operating Systems; D.4.441 Operating Systems; D.4.442 Operating Systems; D.4.443 Operating Systems; D.4.444 Operating Systems; D.4.445 Operating Systems; D.4.446 Operating Systems; D.4.447 Operating Systems; D.4.448 Operating Systems; D.4.449 Operating Systems; D.4.450 Operating Systems; D.4.451 Operating Systems; D.4.452 Operating Systems; D.4.453 Operating Systems; D.4.454 Operating Systems; D.4.455 Operating Systems; D.4.456 Operating Systems; D.4.457 Operating Systems; D.4.458 Operating Systems; D.4.459 Operating Systems; D.4.460 Operating Systems; D.4.461 Operating Systems; D.4.462 Operating Systems; D.4.463 Operating Systems; D.4.464 Operating Systems; D.4.465 Operating Systems; D.4.466 Operating Systems; D.4.467 Operating Systems; D.4.468 Operating Systems; D.4.469 Operating Systems; D.4.470 Operating Systems; D.4.471 Operating Systems; D.4.472 Operating Systems; D.4.473 Operating Systems; D.4.474 Operating Systems; D.4.475 Operating Systems; D.4.476 Operating Systems; D.4.477 Operating Systems; D.4.478 Operating Systems; D.4.479 Operating Systems; D.4.480 Operating Systems; D.4.481 Operating Systems; D.4.482 Operating Systems; D.4.483 Operating Systems; D.4.484 Operating Systems; D.4.485 Operating Systems; D.4.486 Operating Systems; D.4.487 Operating Systems; D.4.488 Operating Systems; D.4.489 Operating Systems; D.4.490 Operating Systems; D.4.491 Operating Systems; D.4.492 Operating Systems; D.4.493 Operating Systems; D.4.494 Operating Systems; D.4.495 Operating Systems; D.4.496 Operating Systems; D.4.497 Operating Systems; D.4.498 Operating Systems; D.4.499 Operating Systems; D.4.500 Operating Systems; D.4.501 Operating Systems; D.4.502 Operating Systems; D.4.503 Operating Systems; D.4.504 Operating Systems; D.4.505 Operating Systems; D.4.506 Operating Systems; D.4.507 Operating Systems; D.4.508 Operating Systems; D.4.509 Operating Systems; D.4.510 Operating Systems; D.4.511 Operating Systems; D.4.512 Operating Systems; D.4.513 Operating Systems; D.4.514 Operating Systems; D.4.515 Operating Systems; D.4.516 Operating Systems; D.4.517 Operating Systems; D.4.518 Operating Systems; D.4.519 Operating Systems; D.4.520 Operating Systems; D.4.521 Operating Systems; D.4.522 Operating Systems; D.4.523 Operating Systems; D.4.524 Operating Systems; D.4.525 Operating Systems; D.4.526 Operating Systems; D.4.527 Operating Systems; D.4.528 Operating Systems; D.4.529 Operating Systems; D.4.530 Operating Systems; D.4.531 Operating Systems; D.4.532 Operating Systems; D.4.533 Operating Systems; D.4.534 Operating Systems; D.4.535 Operating Systems; D.4.536 Operating Systems; D.4.537 Operating Systems; D.4.538 Operating Systems; D.4.539 Operating Systems; D.4.540 Operating Systems; D.4.541 Operating Systems; D.4.542 Operating Systems; D.4.543 Operating Systems; D.4.544 Operating Systems; D.4.545 Operating Systems; D.4.546 Operating Systems; D.4.547 Operating Systems; D.4.548 Operating Systems; D.4.549 Operating Systems; D.4.550 Operating Systems; D.4.551 Operating Systems; D.4.552 Operating Systems; D.4.553 Operating Systems; D.4.554 Operating Systems; D.4.555 Operating Systems; D.4.556 Operating Systems; D.4.557 Operating Systems; D.4.558 Operating Systems; D.4.559 Operating Systems; D.4.560 Operating Systems; D.4.561 Operating Systems; D.4.562 Operating Systems; D.4.563 Operating Systems; D.4.564 Operating Systems; D.4.565 Operating Systems; D.4.566 Operating Systems; D.4.567 Operating Systems; D.4.568 Operating Systems; D.4.569 Operating Systems; D.4.570 Operating Systems; D.4.571 Operating Systems; D.4.572 Operating Systems; D.4.573 Operating Systems; D.4.574 Operating Systems; D.4.575 Operating Systems; D.4.576 Operating Systems; D.4.577 Operating Systems; D.4.578 Operating Systems; D.4.579 Operating Systems; D.4.580 Operating Systems; D.4.581 Operating Systems; D.4.582 Operating Systems; D.4.583 Operating Systems; D.4.584 Operating Systems; D.4.585 Operating Systems; D.4.586 Operating Systems; D.4.587 Operating Systems; D.4.588 Operating Systems; D.4.589 Operating Systems; D.4.590 Operating Systems; D.4.591 Operating Systems; D.4.592 Operating Systems; D.4.593 Operating Systems; D.4.594 Operating Systems; D.4.595 Operating Systems; D.4.596 Operating Systems; D.4.597 Operating Systems; D.4.598 Operating Systems; D.4.599 Operating Systems; D.4.600 Operating Systems; D.4.601 Operating Systems; D.4.602 Operating Systems; D.4.603 Operating Systems; D.4.604 Operating Systems; D.4.605 Operating Systems; D.4.606 Operating Systems; D.4.607 Operating Systems; D.4.608 Operating Systems; D.4.609 Operating Systems; D.4.610 Operating Systems; D.4.611 Operating Systems; D.4.612 Operating Systems; D.4.613 Operating Systems; D.4.614 Operating Systems; D.4.615 Operating Systems; D.4.616 Operating Systems; D.4.617 Operating Systems; D.4.618 Operating Systems; D.4.619 Operating Systems; D.4.620 Operating Systems; D.4.621 Operating Systems; D.4.622 Operating Systems; D.4.623 Operating Systems; D.4.624 Operating Systems; D.4.625 Operating Systems; D.4.626 Operating Systems; D.4.627 Operating Systems; D.4.628 Operating Systems; D.4.629 Operating Systems; D.4.630 Operating Systems; D.4.631 Operating Systems; D.4.632 Operating Systems; D.4.633 Operating Systems; D.4.634 Operating Systems; D.4.635 Operating Systems; D.4.636 Operating Systems; D.4.637 Operating Systems; D.4.638 Operating Systems; D.4.639 Operating Systems; D.4.640 Operating Systems; D.4.641 Operating Systems; D.4.642 Operating Systems; D.4.643 Operating Systems; D.4.644 Operating Systems; D.4.645 Operating Systems; D.4.646 Operating Systems; D.4.647 Operating Systems; D.4.648 Operating Systems; D.4.649 Operating Systems; D.4.650 Operating Systems; D.4.651 Operating Systems; D.4.652 Operating Systems; D.4.653 Operating Systems; D.4.654 Operating Systems; D.4.655 Operating Systems; D.4.656 Operating Systems; D.4.657 Operating Systems; D.4.658 Operating Systems; D.4.659 Operating Systems; D.4.660 Operating Systems; D.4.661 Operating Systems; D.4.662 Operating Systems; D.4.663 Operating Systems; D.4.664 Operating Systems; D.4.665 Operating Systems; D.4.666 Operating Systems; D.4.667 Operating Systems; D.4.668 Operating Systems; D.4.669 Operating Systems; D.4.670 Operating Systems; D.4.671 Operating Systems; D.4.672 Operating Systems; D.4.673 Operating Systems; D.4.674 Operating Systems; D.4.675 Operating Systems; D.4.676 Operating Systems; D.4.677 Operating Systems; D.4.678 Operating Systems; D.4.679 Operating Systems; D.4.680 Operating Systems; D.4.681 Operating Systems; D.4.682 Operating Systems; D.4.683 Operating Systems; D.4.684 Operating Systems; D.4.685 Operating Systems; D.4.686 Operating Systems; D.4.687 Operating Systems; D.4.688 Operating Systems; D.4.689 Operating Systems; D.4.690 Operating Systems; D.4.691 Operating Systems; D.4.692 Operating Systems; D.4.693 Operating Systems; D.4.694 Operating Systems; D.4.695 Operating Systems; D.4.696 Operating Systems; D.4.697 Operating Systems; D.4.698 Operating Systems; D.4.699 Operating Systems; D.4.700 Operating Systems; D.4.701 Operating Systems; D.4.702 Operating Systems; D.4.703 Operating Systems; D.4.704 Operating Systems; D.4.705 Operating Systems; D.4.706 Operating Systems; D.4.707 Operating Systems; D.4.708 Operating Systems; D.4.709 Operating Systems; D.4.710 Operating Systems; D.4.711 Operating Systems; D.4.712 Operating Systems; D.4.713 Operating Systems; D.4.714 Operating Systems; D.4.715 Operating Systems; D.4.716 Operating Systems; D.4.717 Operating Systems; D.4.718 Operating Systems; D.4.719 Operating Systems; D.4.720 Operating Systems; D.4.721 Operating Systems; D.4.722 Operating Systems; D.4.723 Operating Systems; D.4.724 Operating Systems; D.4.725 Operating Systems; D.4.726 Operating Systems; D.4.727 Operating Systems; D.4.728 Operating Systems; D.4.729 Operating Systems; D.4.730 Operating Systems; D.4.731 Operating Systems; D.4.732 Operating Systems; D.4.733 Operating Systems; D.4.734 Operating Systems; D.4.735 Operating Systems; D.4.736 Operating Systems; D.4.737 Operating Systems; D.4.738 Operating Systems; D.4.739 Operating Systems; D.4.740 Operating Systems; D.4.741 Operating Systems; D.4.742 Operating Systems; D.4.743 Operating Systems; D.4.744 Operating Systems; D.4.745 Operating Systems; D.4.746 Operating Systems; D.4.747 Operating Systems; D.4.748 Operating Systems; D.4.749 Operating Systems; D.4.750 Operating Systems; D.4.751 Operating Systems; D.4.752 Operating Systems; D.4.753 Operating Systems; D.4.754 Operating Systems; D.4.755 Operating Systems; D.4.756 Operating Systems; D.4.757 Operating Systems; D.4.758 Operating Systems; D.4.759 Operating Systems; D.4.760 Operating Systems; D.4.761 Operating Systems; D.4.762 Operating Systems; D.4.763 Operating Systems; D.4.764 Operating Systems; D.4.765 Operating Systems; D.4.766 Operating Systems; D.4.767 Operating Systems; D.4.768 Operating Systems; D.4.769 Operating Systems; D.4.770 Operating Systems; D.4.771 Operating Systems; D.4.772 Operating Systems; D.4.773 Operating Systems; D.4.774 Operating Systems; D.4.775 Operating Systems; D.4.776 Operating Systems; D.4.777 Operating Systems; D.4.778 Operating Systems; D.4.779 Operating Systems; D.4.780 Operating Systems; D.4.781 Operating Systems; D.4.782 Operating Systems; D.4.783 Operating Systems; D.4.784 Operating Systems; D.4.785 Operating Systems; D.4.786 Operating Systems; D.4.787 Operating Systems; D.4.788 Operating Systems; D.4.789 Operating Systems; D.4.790 Operating Systems; D.4.791 Operating Systems; D.4.792 Operating Systems; D.4.793 Operating Systems; D.4.794 Operating Systems; D.4.795 Operating Systems; D.4.796 Operating Systems; D.4.797 Operating Systems; D.4.798 Operating Systems; D.4.799 Operating Systems; D.4.800 Operating Systems; D.4.801 Operating Systems; D.4.802 Operating Systems; D.4.803 Operating Systems; D.4.804 Operating Systems; D.4.805 Operating Systems; D.4.806 Operating Systems; D.4.807 Operating Systems; D.4.808 Operating Systems; D.4.809 Operating Systems; D.4.810 Operating Systems; D.4.811 Operating Systems; D.4.812 Operating Systems; D.4.813 Operating Systems; D.4.814 Operating Systems; D.4.815 Operating Systems; D.4.816 Operating Systems; D.4.817 Operating Systems; D.4.818 Operating Systems; D.4.819 Operating Systems; D.4.820 Operating Systems; D.4.821 Operating Systems; D.4.822 Operating Systems; D.4.823 Operating Systems; D.4.824 Operating Systems; D.4.825 Operating Systems; D.4.826 Operating Systems; D.4.827 Operating Systems; D.4.828 Operating Systems; D.4.829 Operating Systems; D.4.830 Operating Systems; D.4.831 Operating Systems; D.4.832 Operating Systems; D.4.833 Operating Systems; D.4.834 Operating Systems; D.4.835 Operating Systems; D.4.836 Operating Systems; D.4.837 Operating Systems; D.4.838 Operating Systems; D.4.839 Operating Systems; D.4.840 Operating Systems; D.4.841 Operating Systems; D.4.842 Operating Systems; D.4.843 Operating Systems; D.4.844 Operating Systems; D.4.845 Operating Systems; D.4.846 Operating Systems; D.4.847 Operating Systems; D.4.848 Operating Systems; D.4.849 Operating Systems; D.4.850 Operating Systems; D.4.851 Operating Systems; D.4.852 Operating Systems; D.4.853 Operating Systems; D.4.854 Operating Systems; D.4.855 Operating Systems; D.4.856 Operating Systems; D.4.857 Operating Systems; D.4.858 Operating Systems; D.4.859 Operating Systems; D.4.860 Operating Systems; D.4.861 Operating Systems; D.4.862 Operating Systems; D.4.863 Operating Systems; D.4.864 Operating Systems; D.4.865 Operating Systems; D.4.866 Operating Systems; D.4.867 Operating Systems; D.4.868 Operating Systems; D.4.869 Operating Systems; D.4.870 Operating Systems; D.4.871 Operating Systems; D.4.872 Operating Systems; D.4.873 Operating Systems; D.4.874 Operating Systems; D.4.875 Operating Systems; D.4.876 Operating Systems; D.4.877 Operating Systems; D.4.878 Operating Systems; D.4.879 Operating Systems; D.4.880 Operating Systems; D.4.881 Operating Systems; D.4.882 Operating Systems; D.4.883 Operating Systems; D.4.884 Operating Systems; D.4.885 Operating Systems; D.4.886 Operating Systems; D.4.887 Operating Systems; D.4.888 Operating Systems; D.4.889 Operating Systems; D.4.890 Operating Systems; D.4.891 Operating Systems; D.4.892 Operating Systems; D.4.893 Operating Systems; D.4.894 Operating Systems; D.4.895 Operating Systems; D.4.896 Operating Systems; D.4.897 Operating Systems; D.4.898 Operating Systems; D.4.899 Operating Systems; D.4.900 Operating Systems; D.4.901 Operating Systems; D.4.902 Operating Systems; D.4.903 Operating Systems; D.4.904 Operating Systems; D.4.905 Operating Systems; D.4.906 Operating Systems; D.4.907 Operating Systems; D.4.908 Operating Systems; D.4.909 Operating Systems; D.4.910 Operating Systems; D.4.911 Operating Systems; D.4.912 Operating Systems; D.4.913 Operating Systems; D.4.914 Operating Systems; D.4.915 Operating Systems; D.4.916 Operating Systems; D.4.917 Operating Systems; D.4.918 Operating Systems; D.4.919 Operating Systems; D.4.920 Operating Systems; D.4.921 Operating Systems; D.4.922 Operating Systems; D.4.923 Operating Systems; D.4.924 Operating Systems; D.4.925 Operating Systems; D.4.926 Operating Systems; D.4.927 Operating Systems; D.4.928 Operating Systems; D.4.929 Operating Systems; D.4.930 Operating Systems; D.4.931 Operating Systems; D.4.932 Operating Systems; D.4.933 Operating Systems; D.4.934 Operating Systems; D.4.935 Operating Systems; D.4.936 Operating Systems; D.4.937 Operating Systems; D.4.938 Operating Systems; D.4.939 Operating Systems; D.4.940 Operating Systems; D.4.941 Operating Systems; D.4.942 Operating Systems; D.4.943 Operating Systems; D.4.944 Operating Systems; D.4.945 Operating Systems; D.4.946 Operating Systems; D.4.947 Operating Systems; D.4.948 Operating Systems; D.4.949 Operating Systems; D.4.950 Operating Systems; D.4.951 Operating Systems; D.4.952 Operating Systems; D.4.953 Operating Systems; D.4.954 Operating Systems; D.4.955 Operating Systems; D.4.956 Operating Systems; D.4.957 Operating Systems; D.4.958 Operating Systems; D.4.959 Operating Systems; D.4.960 Operating Systems; D.4.961 Operating Systems; D.4.962 Operating Systems; D.4.963 Operating Systems; D.4.964 Operating Systems; D.4.965 Operating Systems; D.4.966 Operating Systems; D.4.967 Operating Systems; D.4.968 Operating Systems; D.4.969 Operating Systems; D.4.970 Operating Systems; D.4.971 Operating Systems; D.4.972 Operating Systems; D.4.973 Operating Systems; D.4.974 Operating Systems; D.4.975 Operating Systems; D.4.976 Operating Systems; D.4.977 Operating Systems; D.4.978 Operating Systems; D.4.979 Operating Systems; D.4.980 Operating Systems; D.4.981 Operating Systems; D.4.982 Operating Systems; D.4.983 Operating Systems; D.4.984 Operating Systems; D.4.985 Operating Systems; D.4.986 Operating Systems; D.4.987 Operating Systems; D.4.988 Operating Systems; D.4.989 Operating Systems; D.4.990 Operating Systems; D.4.991 Operating Systems; D.4.992 Operating Systems; D.4.993 Operating Systems; D.4.994 Operating Systems; D.4.995 Operating Systems; D.4.996 Operating Systems; D.4.997 Operating Systems; D.4.998 Operating Systems; D.4.999 Operating Systems; D.5.00</p>

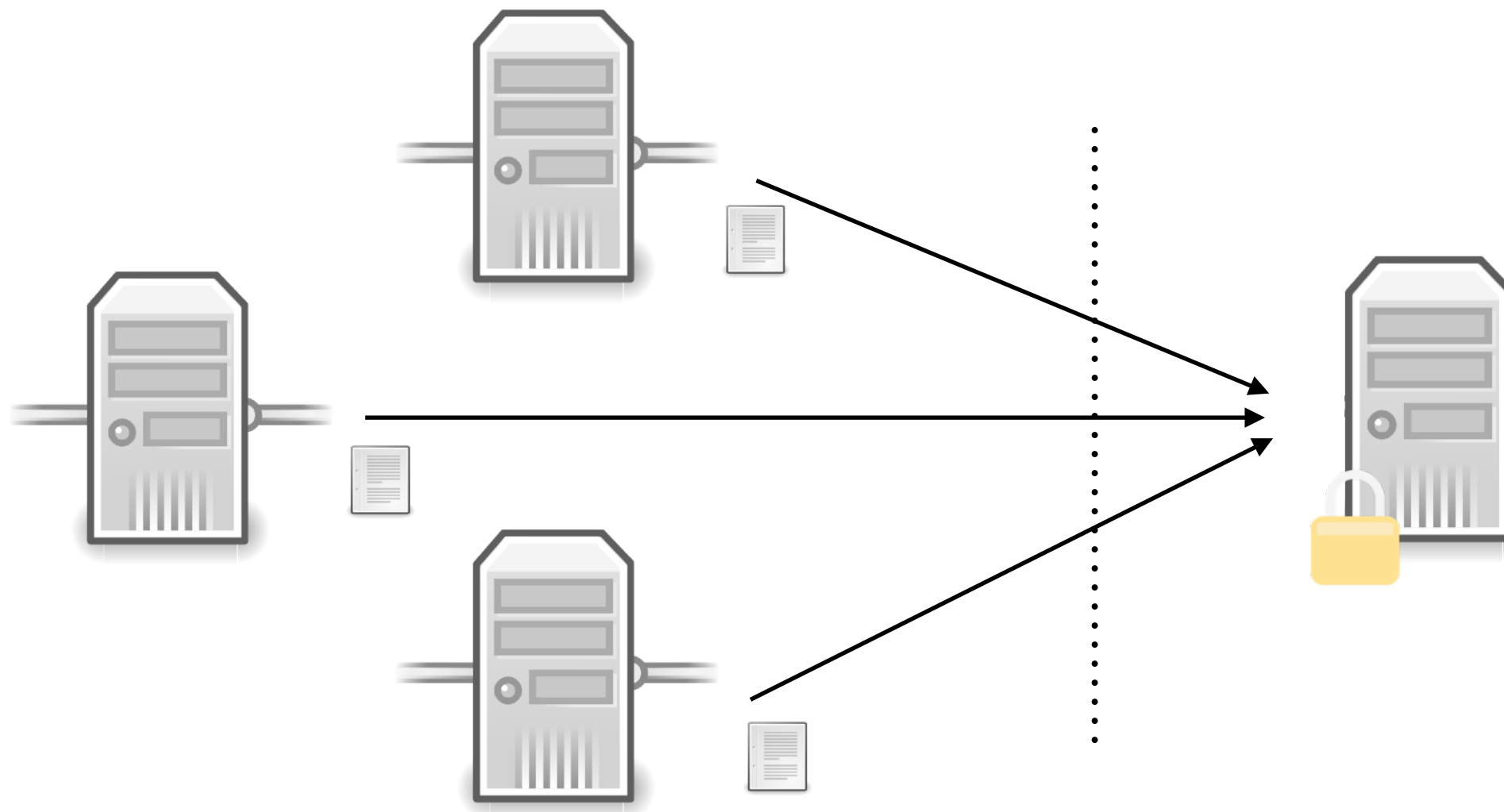
Can we trust the logs?



The attacker may modify the log file to cover their traces!

Goal: An event, once correctly logged, cannot be *undetectably* hidden or modified.

Send logs to a **trusted** central server



This paper



Allow the central server to be **untrusted**.

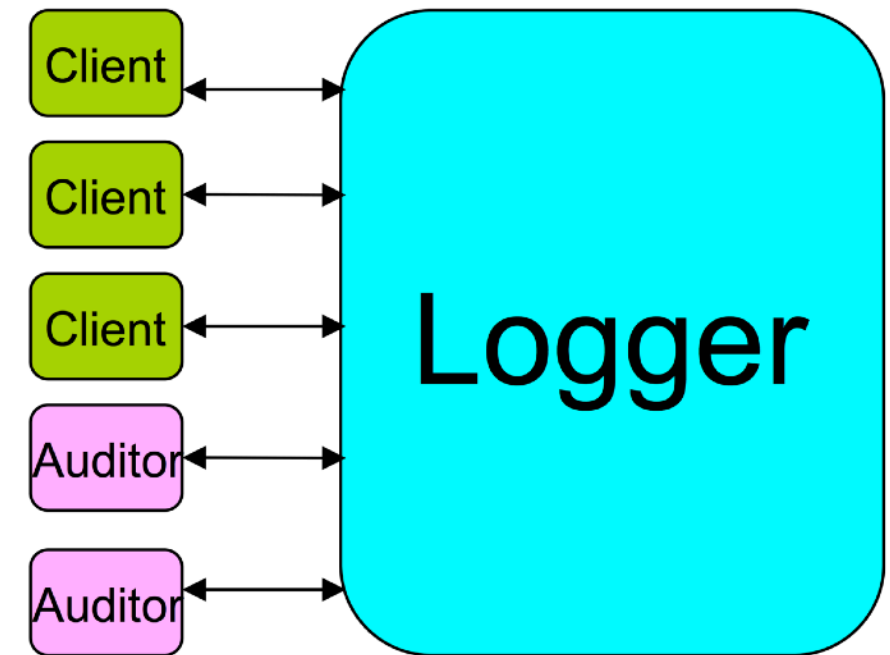
Ingredients:

1. Auditing
2. History Tree

High-level design



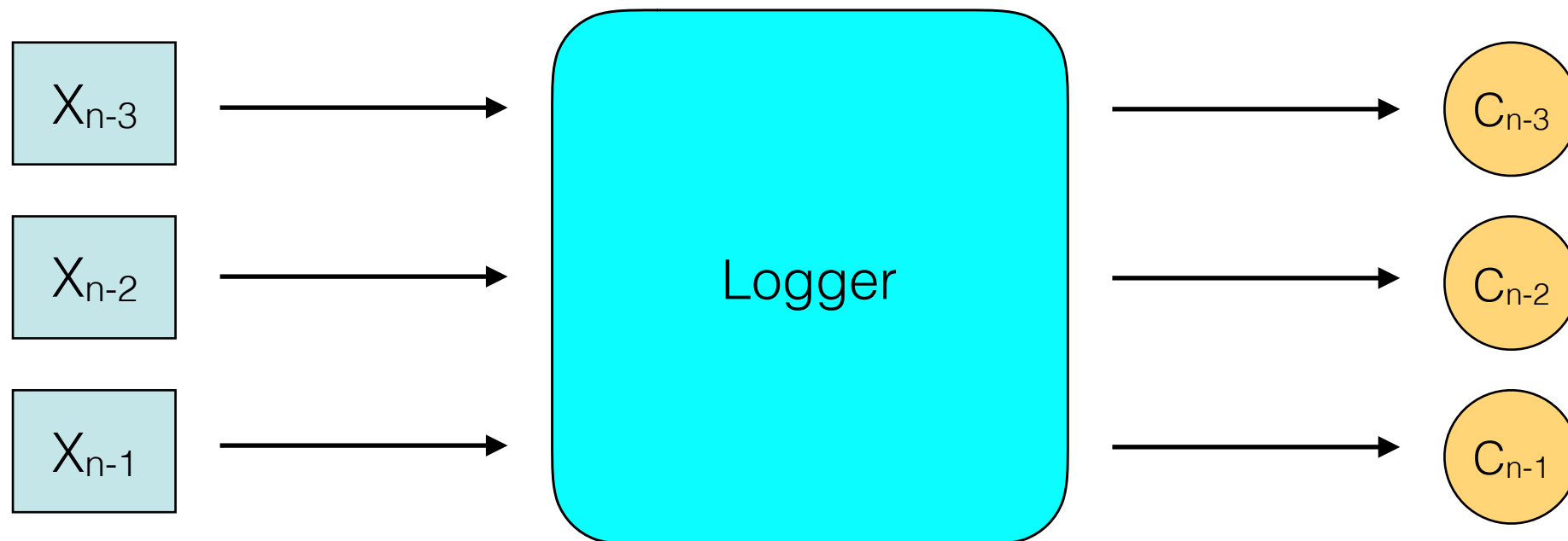
- Logger (central server)
 - Stores logs
- Clients
 - Generate logs
- Auditors
 - Verify the correct operation of the logger



Logger



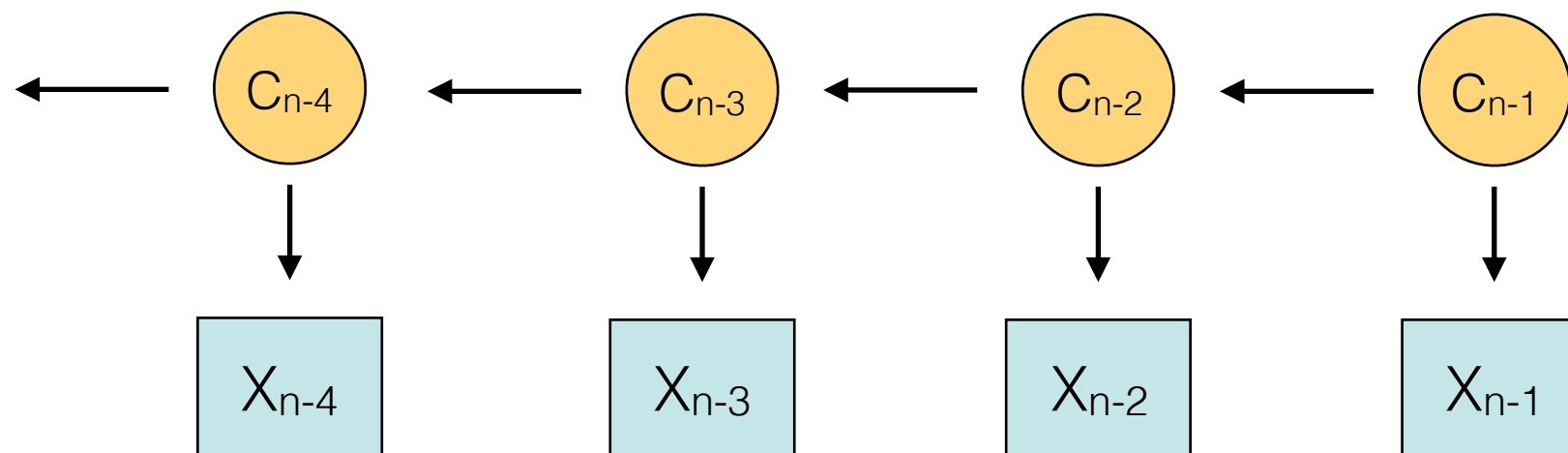
- Logs come in
- Commitments go out



Commitments



- Each commits to the entire past. Example construction [Kelsey, Schneier]:
 - $C_n = H(C_{n-1} \parallel X_n)$
- They are signed by the logger



We don't trust the logger!

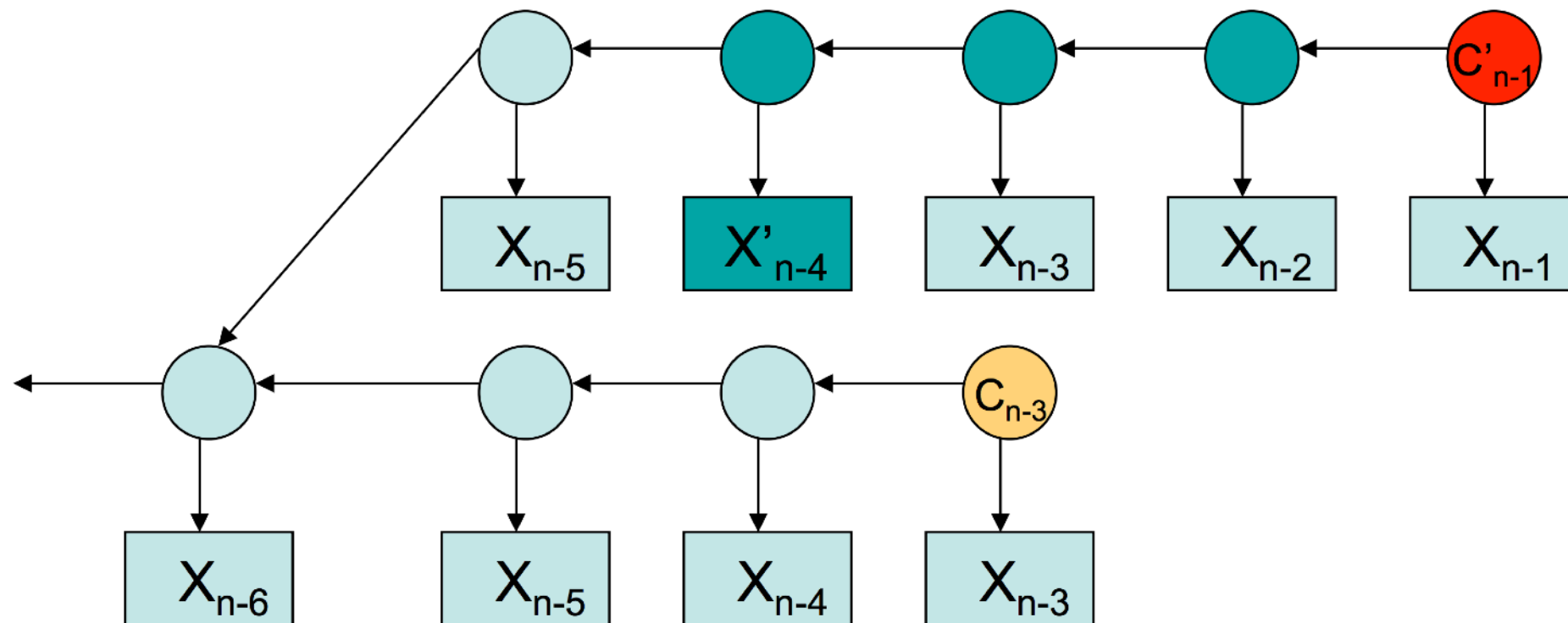


- Does C_{n-3} really contain X_{n-3} ?
- Do C_{n-2} and C_{n-1} commit the same historical events?
- Is the event at index i in the log defined by C_n really X_i ?

Example: log forks



- What if the logger rolls back the log and adds on different events?



Solution: Auditing

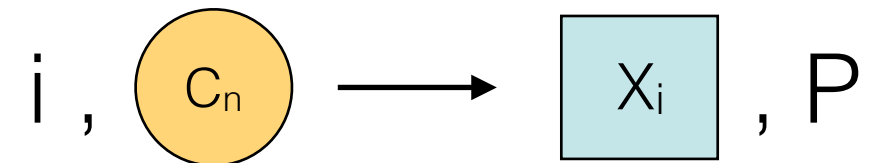


- Check the returned commitments
 - For correct event lookup
 - For consistency

Two kinds of audits

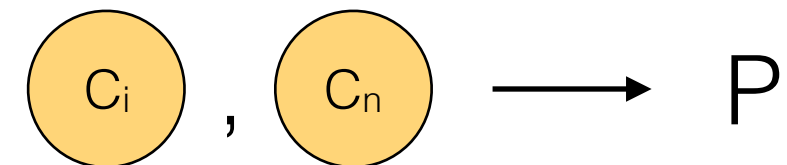


- Membership auditing



- Verify proper insertion
- Lookup historical events

- Incremental auditing



- Prove consistency
between two commitments

Who does what?

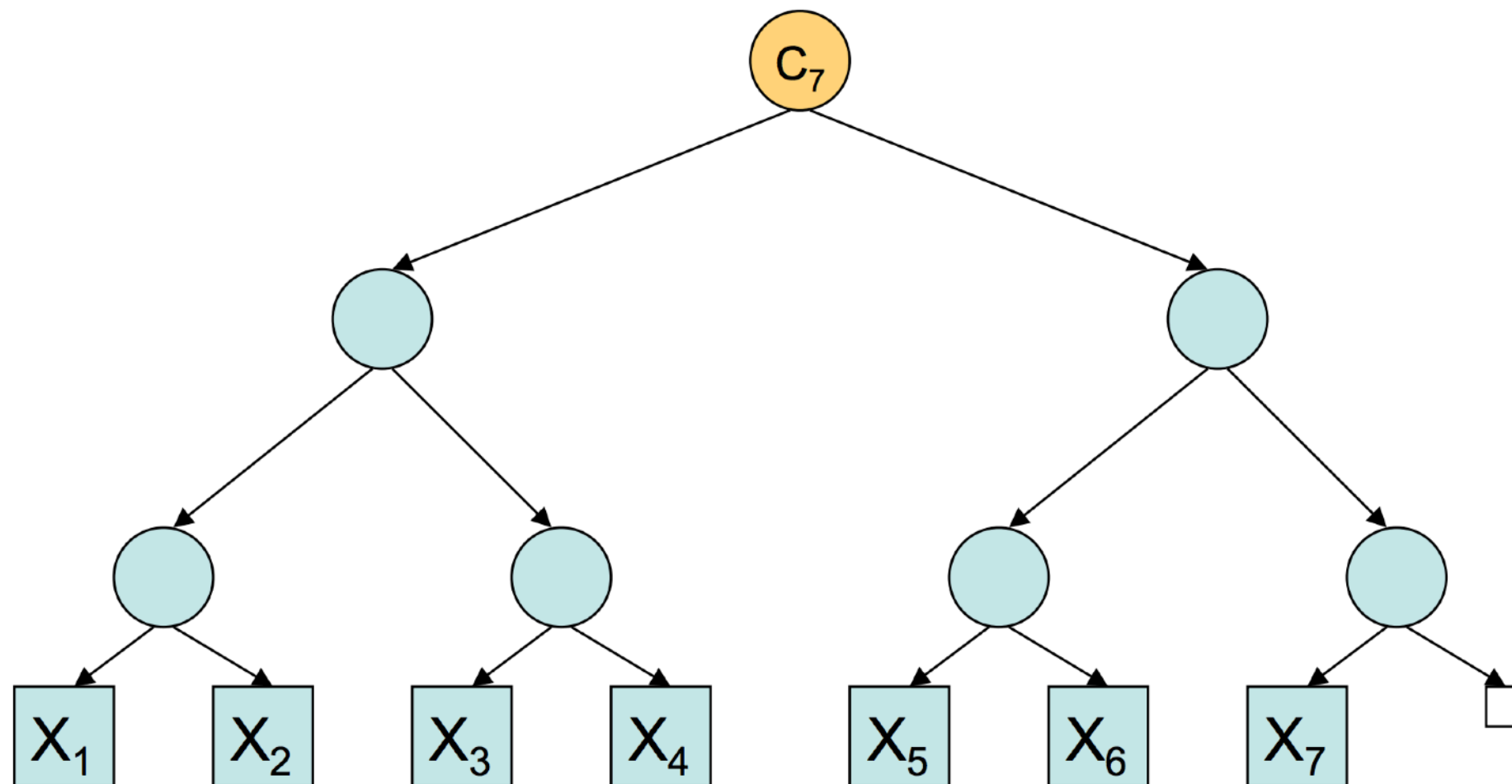


- **Clients must redistribute their received commitments from the logger to auditors.**
- A host can be both client and auditor at the same time.
- Auditing strategies are not discussed in detail.

Making audits cheap



- Logs are stored in a **history tree**

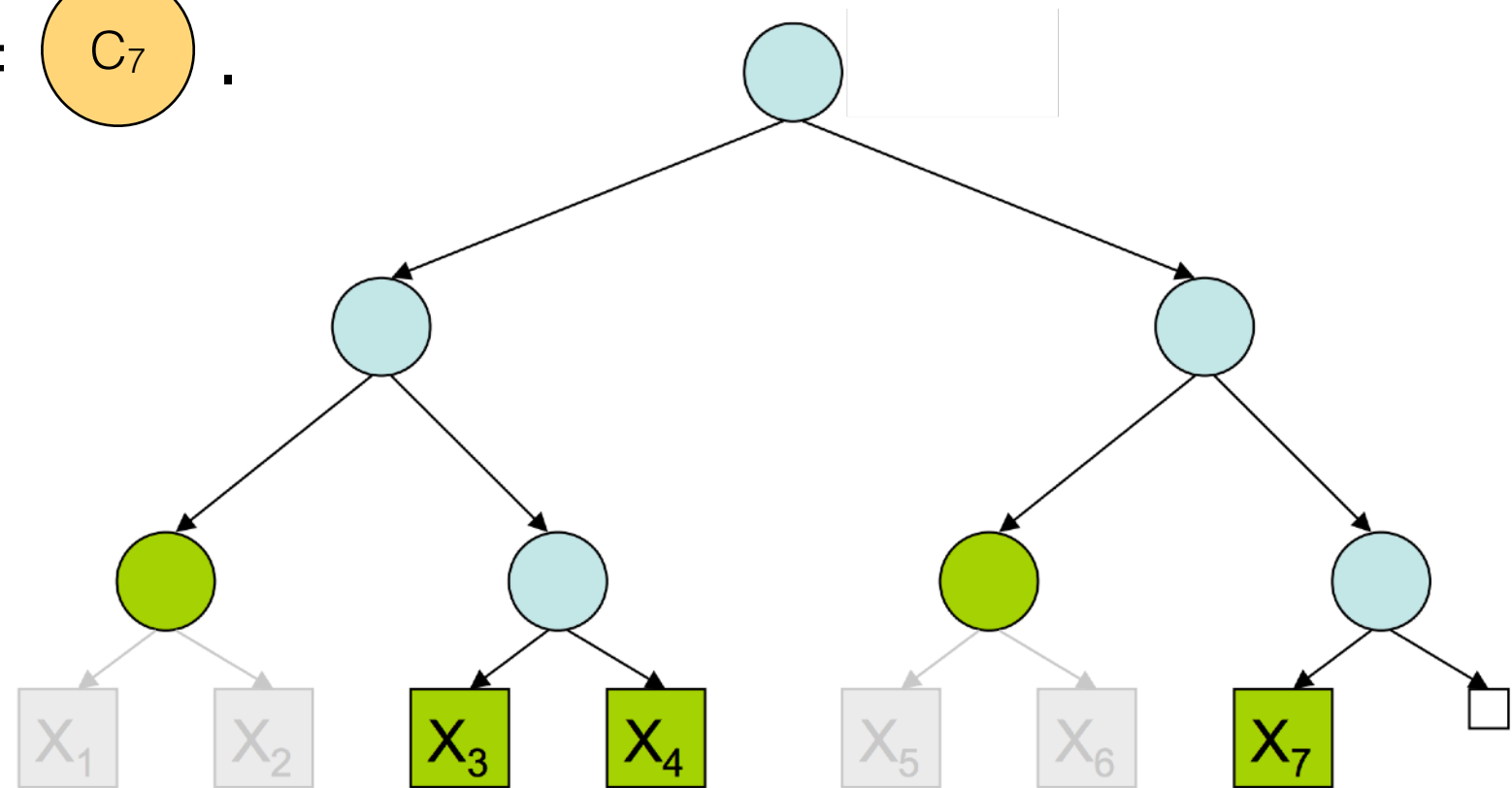


Membership Auditing



Given $(3, \textcircled{C_7})$ return $(\boxed{X_3}, P)$, where P is:

Valid if $\text{root} == \textcircled{C_7}$.



P takes $O(\log n)$ to build

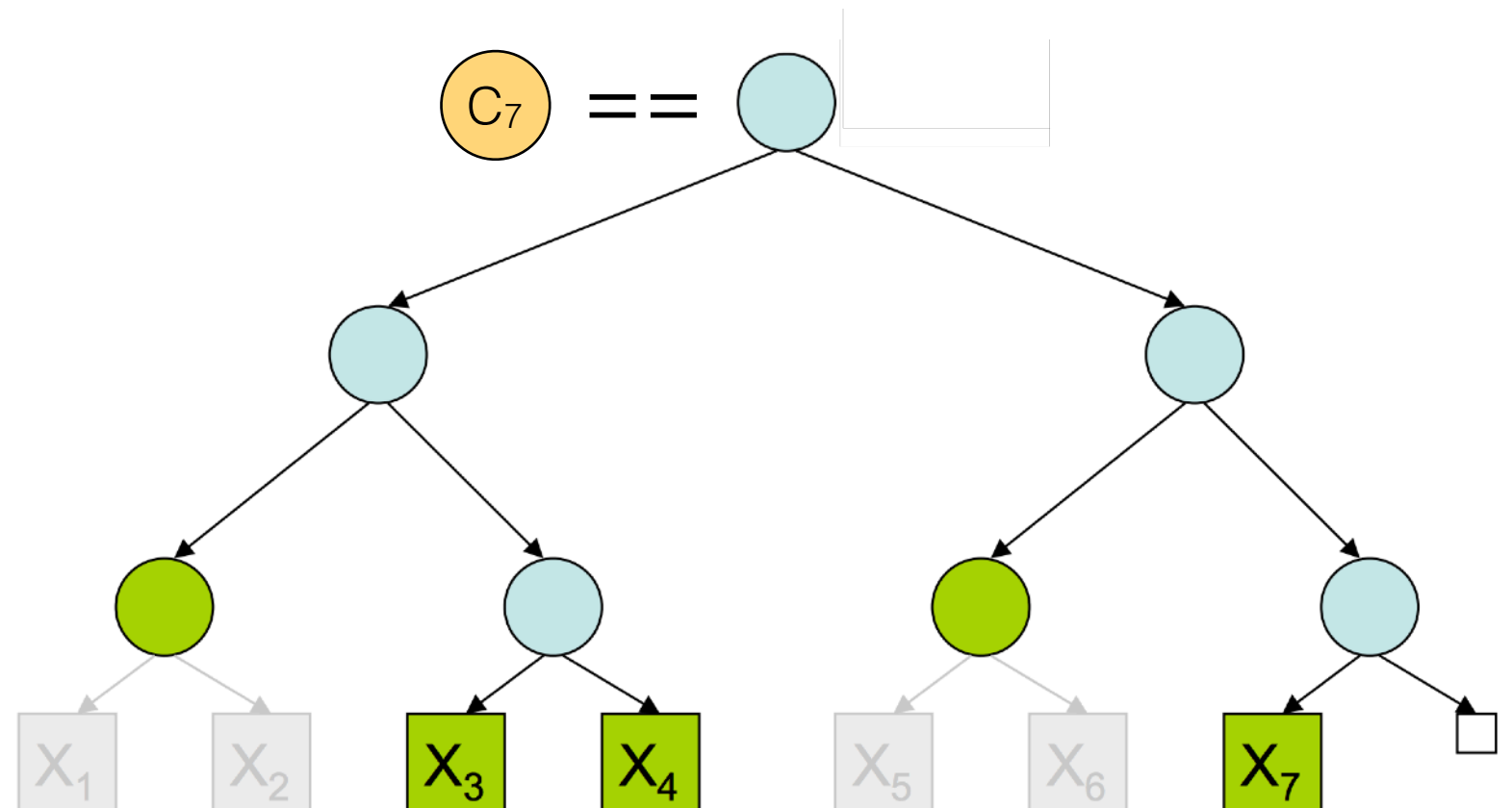
Incremental Auditing



Given (C_3, C_7) return (P) , where P is:

Valid if:

- P is consistent with C_7
- P is consistent with C_3



P takes $O(\log n)$ to build

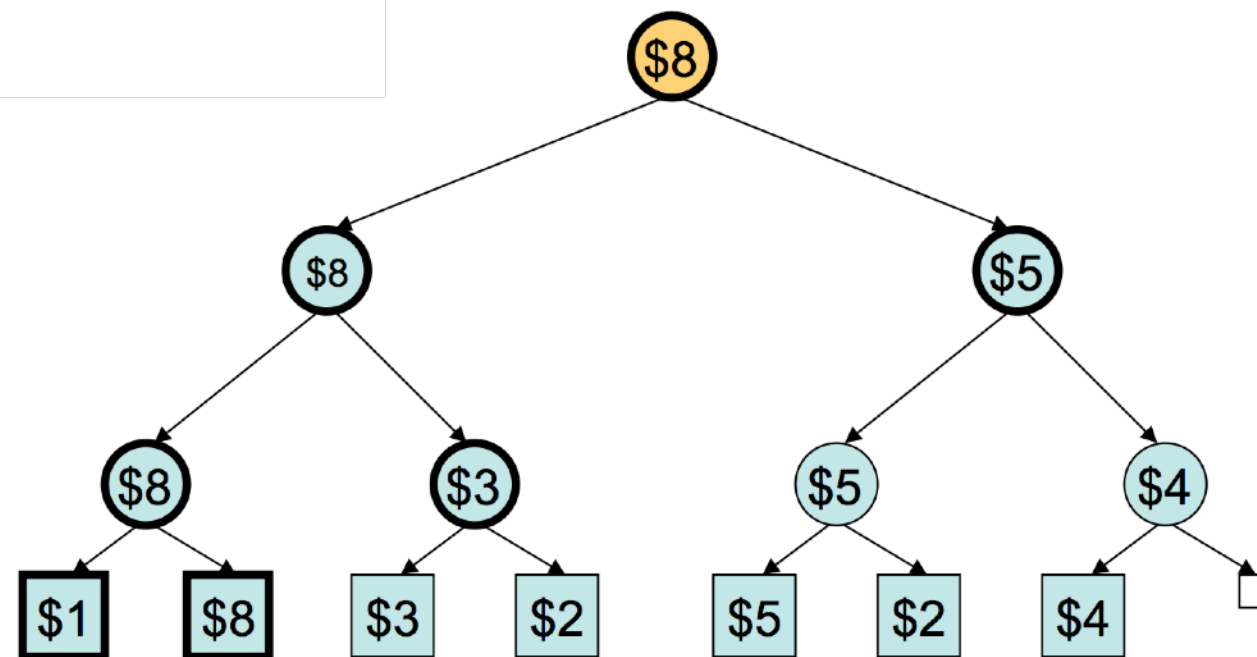
Merkle Aggregation



History trees can be extended to annotate events with attributes.

Application: support content searches.

- Max()



Find all transactions over \$6



- Insert performance: 1,750 events/sec
 - 2.4%: Parse the log event
 - 2.6%: Insert the event to the tree
 - 11.8%: Get root commitment
 - 83.3%: Sign commitment
- Proof generation:
 - With locality (all events in RAM):
 - 10,000-18,000 incremental proofs/sec
 - 8,600 membership proofs/sec
 - Without locality
 - 30 membership proofs/sec



- History trees allow the logger to store log events and generate integrity proofs efficiently.
- Other hosts (auditors) need to demand those proofs to ensure the logs are not tampered.
- Result: the logger can be untrusted (but at least one auditor needs to be honest).



- No security analysis: what happens if a client colludes with the logger? What if the secret key of the logger is compromised?
- No full-system evaluation with multiple hosts. Network overhead? Overhead of redistributing commitments with gossip? Scalability?
- No auditing strategies are presented. What kind of audits, from whom and how often should be asked to the logger? What happens when tampering is detected? Lying auditors?