Zcash Ceremony and Audit

Zerocoin Electric Coin Company (ZECC)

May 10, 2017 – Version 1.0

Prepared for

Nathan Wilcox

Prepared by

Derek Hinch

While precautions have been taken in the preparation of this document, NCC Group the publisher, and the author(s) assume no responsibility for errors, omissions, or for damages resulting from the use of the information contained herein. Use of NCC Group's services does not guarantee the security of a system, or that computer intrusions will not occur.

Executive Summary

Zerocoin Electric Coin Company (ZECC) contracted NCC Group to participate in the Zcash cryptographic key generation ceremony, which was held on October 22 and October 23, 2016. The purpose of the engagement was to act as a threat actor and perform adversarial tests against copies of the production nodes used in the ceremony as well as to act as a forensically verifiable 'honest' member of the ceremony. The intent of the adversarial tests was to attempt to circumvent the Zcash security controls and extract data from a running 'test compute' node that would violate the integrity of the cryptographic key generation ceremony.

In an effort to simulate adversarial tests, NCC Group and Zcash developed a scenario to model targeted threats centered around the potential for the user of the compute node acting with malicious intent. During the ceremony, the entire operating system and cryptographic operations were performed in memory on the compute node and as such extraction of the compute node's memory would be the primary attack vector. Using this premise, NCC Group and Zcash developed the following attack scenarios:

- With root-level access, attempt to compromise the memory via forensic memory acquisition (software-based imaging of the physical memory device).
- With root-level access, and with the correct credentials to disable RBAC in grsecurity, attempt to compromise the memory via forensic memory acquisition.
- With physical access to the machine, attempt a Direct Memory Access attack on the physical memory via FireWire.

To perform such attacks, NCC Group and Zcash architected an attack test bed that modeled the ceremony, and NCC Group would operate under the name 'Moses Spears.' NCC Group would (and did) remain in audio/visual contact with the other ceremony members throughout the ceremony. NCC Group performed the tests by setting up a third node that was a copy of the compute node being used in the ceremony. This system was air gapped and used an exact copy of the DVD-R that was used in ceremony.

Each attack was performed by NCC Group and only the DMA attack was successful at extracting memory from the 'test' compute node. The DMA attack was only able to perform a partial extraction of memory. Based on this finding, it is our recommendation that the computation process perform a pre-compute validation step that audits any detected DMA surface areas, namely FireWire, for being present on the device.

After the ceremony was completed, an audit was performed on all of the ceremony media used to boot the live environment. Throughout the audit, no malicious processes were identified and no network listeners, or network transmissions, were attempted by the compute node on boot. Video of the ceremony, when in action, was taken. The facility's closed-circuit video, alarms, and access control systems were operable throughout the ceremony and no anomalous activity was detected during the ceremony.

Based upon the evidence examined by NCC Group, it is our expert opinion that the NCC Group compute node was not compromised throughout the duration of the event.

Procedures

Per the Zcash procedures, all equipment used during the ceremony was randomly sourced and purchased from the area local to NCC Group. Once purchased, NCC Group staff removed the WiFi/Bluetooth radio cards from the motherboards of the two computer systems. All internal disk drives were disconnected from the systems prior to the launch of the ceremony. These actions were performed in a secured area within the NCC Group Austin Lab environment, and were documented via video and photographic evidence.

To transfer data between the network node and the compute node, randomly sourced and locally purchased blank DVD-R media was used. These discs were later logically imaged with FTK imager and are available for download/inspection. Please contact Zcash for more information on obtaining these items by emailing info@z.cash.

Multiple physical measures (audio/video surveillance, access control, motion alarms) were in place during the ceremony at the NCC Group location. Network telemetry logging (firewalls/network sensors) were in place during the ceremony at the facility. During the times of computation, the compute and network nodes were also directly video recorded. The recorded videos were reviewed and there was no access to the systems during the ceremony, except for when NCC Group staff was involved in the ceremony.

Network traffic flow data during the period was logged from the network node and showed only traffic to the Zcash coordination server during the expected times of the ceremony.

All artifacts available to NCC Group analysts with regards to the physical and communication security of these systems resulted in no unauthorized access to the area being detected.

A third node was set up as a copy of the compute node being used in the ceremony. The third node used an exact copy of the DVD-R that was being used by the ceremony to boot up the operating system for the compute node. The purpose of this system was to become a test bed of attacks that NCC Group and Zcash had modeled against the ceremony.

Dashboard

Target Metadata

Name	ZCash Ceremony
Type	Live Media Local Instance
Platforms	Alpine Linux with grsecurity enabled
Environment	Live Media Local Test Instance

Engagement Data

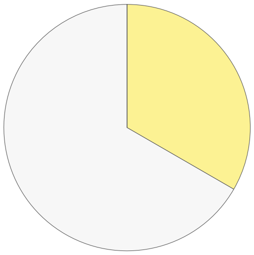
Type	Ceremony Performance and Compute Node Audit
Method	Architecture Review, Functional Testing, Memory Imaging, DMA Attacks
Dates	2016-10-22 to 2016-10-23
Consultants	2
Level of effort	7 Person-Days

Targets

Production Compute Node	After-action live media audit, production compute ceremony setup and execution/documentation
Test Compute Node	Software-based memory attacks with the highest level of system access, hardware (FireWire/DMA) based memory attacks with professional forensic FireWire memory imaging suite.

Finding Breakdown

Critical Risk issues	0
High Risk issues	0
Medium Risk issues	0
Low Risk issues	1
Informational issues	2
Total issues	3



Category Breakdown

Access Controls	1	⬜
Cryptography	1	⬜
Data Exposure	1	🟨

Component Breakdown

Test Compute Node	2	🟨 ⬜
Ceremony Hashing	1	⬜

Key

Critical 🟥 High 🟥 Medium 🟧 Low 🟨 Informational ⬜

Document Control

Document Version Control

Data Classification	Public
Client Name	Zerocoin Electric Coin Company (ZECC)
Project Reference	N/A
Proposal Reference	N/A
Document Title	Zcash Ceremony and Audit
Author	Derek Hinch

Document History

Issue No.	Issue Date	Issued By	Change Description
0.1	2016-11-03	Derek Hinch	Initial Draft
0.2	2016-11-16	Derek Hinch	Initial Review
0.3	2016-12-06	Derek Hinch	Initial QA
0.4	2016-12-22	Derek Hinch	Client Review
0.5	2017-01-03	Derek Hinch	Client Edits Applied
0.6-1.0	2017-02-15	Derek Hinch	Internal Public Facing Document Review

Table of Findings

For each finding, NCC Group uses a composite risk score that takes into account the severity of the risk, application's exposure and user population, technical difficulty of exploitation, and other factors. For an explanation of NCC Group's risk rating and finding categorization, see Appendix A on page 10.

Title	ID	Risk
Hardware (DMA) Memory Extraction Partially Successful	002	Low
Software-Based Memory Imaging Attempts Failed on Test Compute Node	001	Informational
Commitment and Disc Hashing	003	Informational

Finding	**Hardware (DMA) Memory Extraction Partially Successful**
Risk	Low Impact: Medium, Exploitability: Low
Identifier	NCC-2016-002
Category	Data Exposure
Component	Test Compute Node
Location	NCC Security Defense Operations Facility Austin, TX
Impact	Partial memory extraction possible.
Description	Using the Passware Firewire Memory Extraction bootable media (included in Passware Forensics edition), NCC Group was able to extract 2.2 gigabytes of the full 8 gigabytes of system memory from a modified ‘test compute’ node. This was accomplished by modifying ‘test compute’ node hardware to include a powered Firewire 1394 PCI Express card and extracting memory via a forensics utility. Due to this attack’s limitations, a maximum of 4 gigabytes of memory could potentially be extracted. The resulting memory sample was examined and running processes could be identified; however, portions of the process memory could not be recovered. The ‘test compute’ node was not performing shard operations at the time, but theoretically whatever exists in memory below the addressable 4-gigabyte barrier could be recovered.
Recommendation	The procedure documentation should be updated to remove any and all Firewire devices if equipped. NCC Group had to add this capability (since Firewire is deprecated) in order to perform this attack.

Finding Software-Based Memory Imaging Attempts Failed on Test Compute Node

Risk **Informational** Impact: None, Exploitability: None

Identifier NCC-2016-001

Category Access Controls

Component Test Compute Node

Location NCC Security Defense Operations Facility
Austin, TX

Impact Local access to the 'compute node', with proper root credentials (including the RBAC admin password), did not result in successful imaging of the physical memory. The grsecurity enhanced kernel prevented /proc/kcore from being exposed. Multiple methods of software-based memory extraction were attempted, and all failed due to the grsecurity memory protections.

Description The 'compute' operating system (Alpine Linux grsec enhanced kernel) included a bash shell. Zcash provided NCC Group with root credentials, as well as credentials to disable/change/re-enable RBAC (role based access control) in grsec.

Aside from directly disabling RBAC with gradm, NCC Group also attempted to modify the policy configuration for grsecurity to expose /proc/kcore and other process specific memory segments. While attempting to restart RBAC, grsecurity detected our purposeful misconfiguration of policy and refused to load the RBAC system.[1] This effectively prevented our software-based 'on host' attacks.

Recommendation Continue to implement kernels enhanced with grsecurity in any future ceremony.

[1] The RBAC System, "The RBAC System, grsecurity"

Finding Commitment and Disc Hashing

Risk Informational Impact: None, Exploitability: None

Identifier NCC-2016-003

Category Cryptography

Component Ceremony Hashing

Location NCC Security Defense Operations Facility
Austin, TX

Impact During the Zcash ceremony, several hashes were created and recorded as part of the process. These images were logically imaged with FTK Imager, and constitute the only data transferred between the network and compute nodes.

Description NCC Group confirmed the hashes obtained locally were the ones that were consumed during the ceremony.

Commitment Hash:	`2YrFsjMadFukhdkQpn8oFgET2EQd9WnDW3AzYqNc3kELU45p7t`
Disc A Hash:	`2oQgZxPLAL2f8xkvm71RqwKK6dCFQSrazESXci32M2LZeG7nxe`
Disc B Hash:	`UBjr6UU8oJ4ZzpsTU3vRHmzZmuN7TjX3eLsmdRhw4dW6dEbvH`
Disc C Hash:	`2RvKUp94tXE5b1qhyLpGPTXeWpS7FdNDvCG5MJPmZiccNuRYcw`
Disc D Hash:	`ApPFWMqGBMemE3sTAuMRnwbmGonsPoXYC4r45HBMdmiRWLXqH`
Disc E Hash:	`CFEWpN9STr4iVM8NLGcSUyoaEDr94FEp7VWR9HhQQYhuwUu7f`
Disc F Hash:	`2vohW4tyybTEZyf3ZarX5R1CgsUehQfwASExZQ86EWNd8ByC6a`

Appendix A: Finding Field Definitions

The following sections describe the risk rating and category assigned to issues NCC Group identified.

Risk Scale

NCC Group uses a composite risk score that takes into account the severity of the risk, application's exposure and user population, technical difficulty of exploitation, and other factors. The risk rating is NCC Group's recommended prioritization for addressing findings. Every organization has a different risk sensitivity, so to some extent these recommendations are more relative than absolute guidelines.

Overall Risk

Overall risk reflects NCC Group's estimation of the risk that a finding poses to the target system or systems. It takes into account the impact of the finding, the difficulty of exploitation, and any other relevant factors.

Critical Implies an immediate, easily accessible threat of total compromise.

High Implies an immediate threat of system compromise, or an easily accessible threat of large-scale breach.

Medium A difficult to exploit threat of large-scale breach, or easy compromise of a small portion of the application.

Low Implies a relatively minor threat to the application.

Informational No immediate threat to the application. May provide suggestions for application improvement, functional issues with the application, or conditions that could later lead to an exploitable finding.

Impact

Impact reflects the effects that successful exploitation upon the target system or systems. It takes into account potential losses of confidentiality, integrity and availability, as well as potential reputational losses.

High Attackers can read or modify all data in a system, execute arbitrary code on the system, or escalate their privileges to superuser level.

Medium Attackers can read or modify some unauthorized data on a system, deny access to that system, or gain significant internal technical information.

Low Attackers can gain small amounts of unauthorized information or slightly degrade system performance. May have a negative public perception of security.

Exploitability

Exploitability reflects the ease with which attackers may exploit a finding. It takes into account the level of access required, availability of exploitation information, requirements relating to social engineering, race conditions, brute forcing, etc, and other impediments to exploitation.

High Attackers can unilaterally exploit the finding without special permissions or significant roadblocks.

Medium Attackers would need to leverage a third party, gain non-public information, exploit a race condition, already have privileged access, or otherwise overcome moderate hurdles in order to exploit the finding.

Low Exploitation requires implausible social engineering, a difficult race condition, guessing difficult-to-guess data, or is otherwise unlikely.

Category

NCC Group categorizes findings based on the security area to which those findings belong. This can help organizations identify gaps in secure development, deployment, patching, etc.

Access Controls Related to authorization of users, and assessment of rights.

Auditing and Logging Related to auditing of actions, or logging of problems.

Authentication Related to the identification of users.

Configuration Related to security configurations of servers, devices, or software.

Cryptography Related to mathematical protections for data.

Data Exposure Related to unintended exposure of sensitive information.

Data Validation Related to improper reliance on the structure or values of data.

Denial of Service Related to causing system failure.

Error Reporting Related to the reporting of error conditions in a secure fashion.

Patching Related to keeping software up to date.

Session Management Related to the identification of authenticated users.

Timing Related to race conditions, locking, or order of operations.