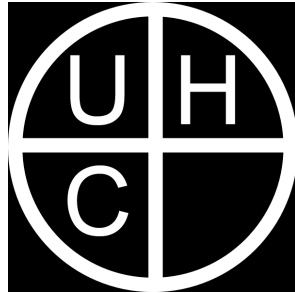


The Underhanded Crypto Contest



Who we are and what we are doing.

Adam Caudill

Twitter: @AdamCaudill

Web: <https://adamcaudill.com/>

Email: adam@adamcaudill.com

Taylor Hornby

Twitter: @DefuseSec

Web: <https://defuse.ca/>

Email: th@defuse.ca

New Organizer: Tony Arcieri

Twitter: @bascule

Web: <http://tonyarcieri.com/>

Welcome to the team!

Why study backdoors?

- Better Software
- Faster Detection
- ...oh, and it's fun!

Underhanded Crypto Contest

- We're interested in backdoored cryptography **design** and **implementation**.
- The UHC is a platform for discovering new backdoor techniques and defenses.
- Like the Underhanded C contest, but with a specific focus on cryptography.

Crypto Village Mini-Contest

DEADLINE: Tomorrow at 8am!

Two categories:

1. GnuPG key leaking.
2. Password hashing (or auth.) backdoor.

submit@underhandedcrypto.com

<http://tinyurl.com/CryptoVillageUHC>

Category: Backdoor GnuPG

“Patch the GPG source code, to leak the user’s private key in a subtle way. The leak should be performed in such a way that the average user would not notice it.”

Category: Password Auth.

“Design and optionally implement a password hashing system or password-based authentication protocol that, when a secret value is supplied, will allow an attacker to authenticate to any account. The system should appear secure under a typical peer review. Bonus points for a working implementation.”

Crypto Village Mini-Contest

DEADLINE: Tomorrow at 8am!

Two categories:

1. GnuPG key leaking.
2. Password hashing (or auth.) backdoor.

submit@underhandedcrypto.com

<http://tinyurl.com/CryptoVillageUHC>

2014 Contest Recap

16 entries. 2 winners.

Announced: September 2014.

Deadline: December 2014.

Winners announced: March 2015.

2014 Winner: John Meacham

- Bug in tiny AES implementation targeting IoT.
 - Buffer re-used for key (pre-expansion) and IV.
 - Using ‘unsigned char’ as a boolean type causes the key expansion to get run on the IV.

```
typedef unsigned char boolean;
uint8 buf[KLEN];
void aes_ctr_crypt(uint8 data[], int len, unsigned mode) {
    if (excess) {
        // ...
        aes_setup(mode & MODE_KEEPKEY, mode & MODE_GENIV, mode & MODE_RESETIV);
    }
    // ...

    static void aes_setup(boolean key_expanded, boolean generate_iv, boolean reset_iv) {
        if (!key_expanded) {
            KeyExpansion(); // Runs key expansion on 'buf'. But 'buf' contains the IV!
        }
        // ...
    }
}
```

2014 Runner-up: Gaëtan Leurent

- Stern's zero-knowledge authentication protocol.
- "Improves" the hamming weight calculation.
- But returns 0 on weight-63 integers.
- Still works fine with high probability.
- But... can be broken if you know the backdoor.

2014 “Finalists”

Round 3:

- Ryan Castellucci
- Solar Designer

Round 2:

- Aleksander Essex
- Alfonso De Gregorio
- anonymous
- Dr. Gavekort
- George Kadianakis
- Jacob Thompson
- Rogdham
- Simon Nicolussi

Thanks to our Judges!

Jean-Philippe Aumasson

Frank Denis

Oxabad1dea (Melissa Elliott)

Daira Hopwood

Juliano Rizzo

Tomás Touceda

Justin Troutman

Florian Mendel

Thanks to our Sponsors!



Prize: \$600 CPU (or cash)



Prize: Free S4 service and a T-shirt.

Lessons Learned from 2014

We learned a lot from the 2014 contest...

- Must automate collection and judging.
- Simpler process, fewer judges.
- Write/speak about the entries.
- Draw conclusions.

←You can help.

The Future of UHC

- Details Announced in February
- Judging Starts in June
- Challenges Announced in July
- Winners Announced at Crypto & Privacy Village

Crypto Village Mini-Contest

DEADLINE: Tomorrow at 8am!

Two categories:

1. GnuPG key leaking.
2. Password hashing (or auth.) backdoor.

submit@underhandedcrypto.com

<http://tinyurl.com/CryptoVillageUHC>