Exploiting the Client Vulnerabilities in Internet E-voting Systems: Hacking Helios 2.0 as an Example

Saghar Estehghari[1] Yvo Desmedt[1,2]

[1] Department of Computer Science
University College London, UK

[2] Research Center for Information Security (RCIS)
AIST, Japan

August 9, 2010

OVERVIEW

1. Background on cryptographic e-voting
2. Background on computer security aspects of e-voting
3. Motivation to hack Helios 2.0
4. The attack against Helios 2.0
5. Generalizations, defenses and Helios 3.0
6. Future
7. Conclusions

AIST

UCL

1. BACKGROUND ON CRYPTOGRAPHIC E-VOTING

Techniques proposed in the early years to achieve anonymity (privacy) and correctness include:

MIX servers: messages are mixed to achieve anonymity. Several mix servers are used in sequence. (Credit: Chaum 1981, although NSA may have invented this independently in the context of SALT II verification, see Simmons 1996).

In the context of e-voting: encrypted votes are mixed by different servers after:

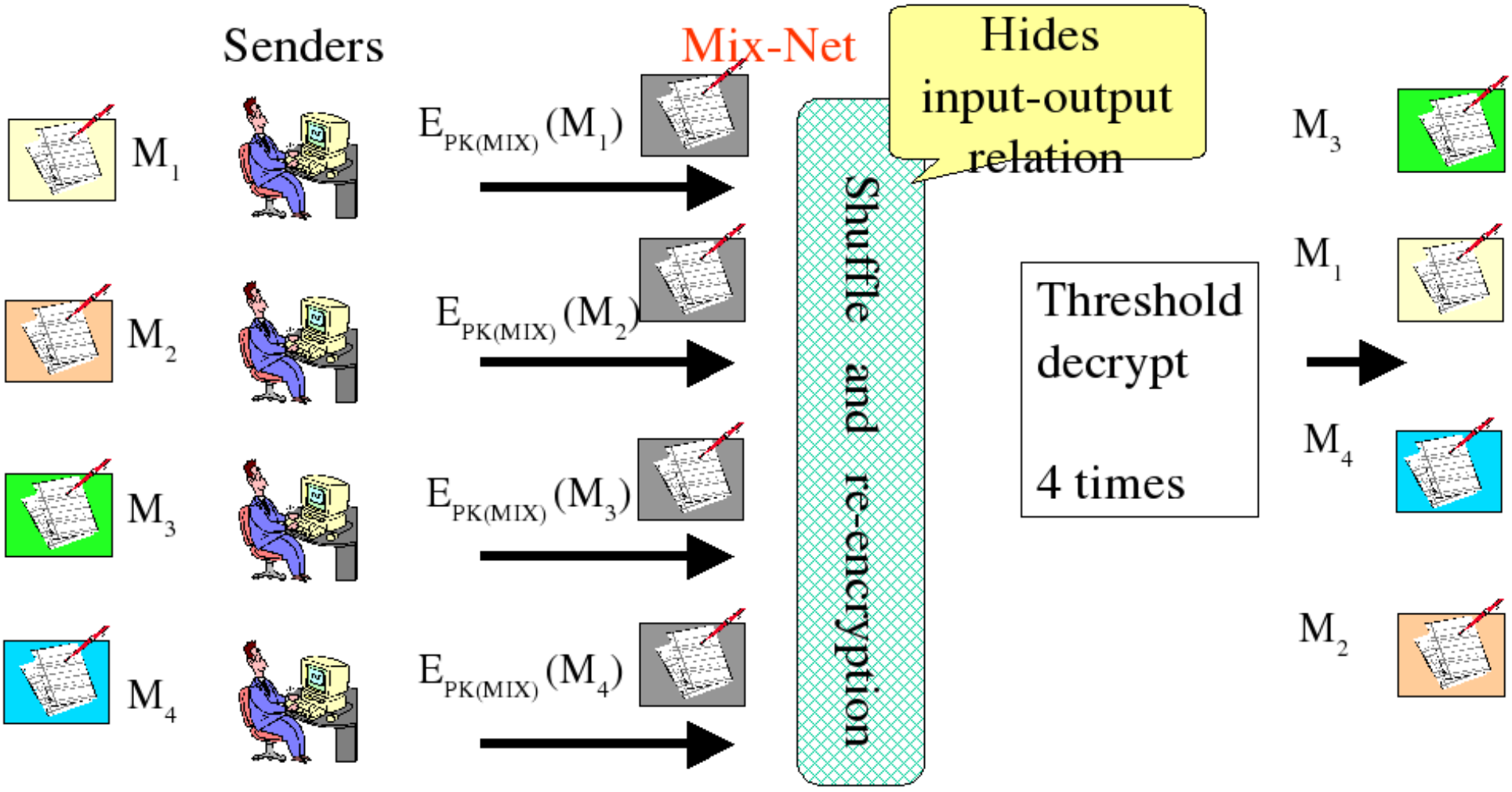
- checking the voter is registered
- removing any identification of the voter

Issues: how to guarantee that during mixing the votes remained unchanged. Solution: use zero-knowledge interactive proof (see e.g., Sako-Kilian 1995).

After the encrypted votes are mixed, the decryption is done by using threshold decryption (Abe, 1999).

Note: prior to Pfitzmann-Pfitzmann attack and Park-Itoh-Kurosawa (1993) use of ElGamal, MIX servers were RSA based.

MIX networks: survey:



Homomorphic schemes: variant solutions (see e.g., Benaloh-Yung 1986, Cramer-Gennaro-Schoenmakers 1997, Hirt-Sako 2000) use homomorphic encryption (e.g., $E(M_1 + M + 2) = E(M_1) * E(M_2)$).

As pointed out in Wagner's Crypto 2006 survey:

"The early years"

- How to prove ballots were counted correctly (using crypto)
- But: fails to address ballot preparation

Solutions: see Benaloh, Chaum, Neff, Schneier, Ryan.

Benaloh's solution:

Benaloh's Simple Verifiable Voting (2006), which uses concepts as:

- Separation of duties
- cryptographic thumbprint
- etc.

2. BACKGROUND ON COMPUTER SECURITY ASPECTS OF E-VOTING

The following statements should not be forgotten:

"Four Grand Challenges in Trustworthy Computing"p. 17 (2003) stated that:

> There are many new systems planned or currently under design that have significant societal impact, and there is a high probability that we will come to rely on these systems immediately upon their deployment. Among these systems are electronic voting systems, . . . A grand research challenge is to ensure that these systems are highly trustworthy despite being attractive targets for attackers.

. . . Despite many advances in computer and communications hardware and software, existing technology has not enabled us to build systems that resist failures and repel attacks. Decision-makers are today mandating the widespread deployment of electronic and Internet-based systems for uses that-should widespread attacks succeed- would undermine public institutions and structures to a catastrophic degree.

the 2001 Report of the (US) National Workshop on Internet Voting

p. 2 states:

Remote Internet voting systems pose significant risk to the integrity of the voting process, and should not be fielded for use in public elections until substantial technical and social science

issues are addressed.

Observe that in the same report a very different statement is made about poll site voting:

> Poll site Internet voting systems offer some benefits and could be responsibly fielded within the next several election cycles.

Electronic booth voting systems were developed after the 2000 US presidential elections. Diebold was such a system. Unfortunately, it was rather easy to attack using hacking techniques, as shown by Kohno-Stubblefield-Rubin-Wallach.

For a brief survey of other attacks see our paper in the proceedings.

3. MOTIVATION OF HACKING HELIOS 2.0

During the IACR (International Association of Cryptologic Research) BOD (Board of Directors) meeting in Istanbul on April 13, 2008, when discussing IACR's move towards Internet e-voting, Halevi stated that:

> I believe server software can be developed that is immune against attacks.

To which I replied:

> I could supervise an MSc thesis attacking client software installing a Trojan hidden in a mail to force the illusion clients believed to have voted for one candidate, but the software voted for another.

Note that, as I stated in my e-mail of Wed Apr 16 14:25:04 +0200 2008:

> It is not too difficult to find a large fraction of the e-mail addresses of our members. Just crawl the LNCS publications from our conferences and workshops to collect them!

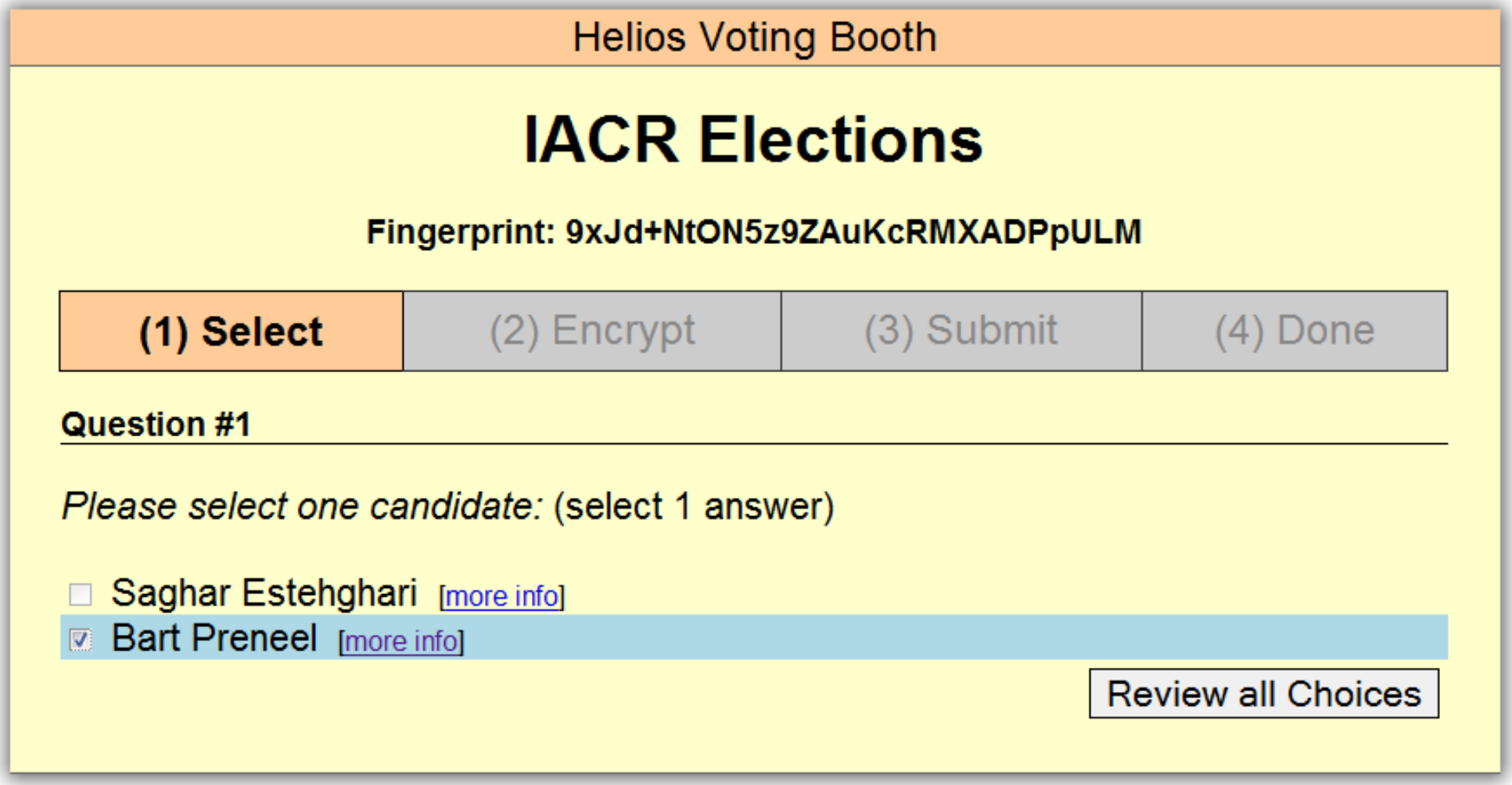
From all systems proposed during the Crypto 2008 informal session on Internet e-voting, Helios 2.0 was the one using most cryptographic techniques, so we concluded it would be a good candidate to attack. Moreover, we learned from Quisquater Helios 2.0 was being used to elect the President of the Université Catholique de Louvain, Belgium in 2009.

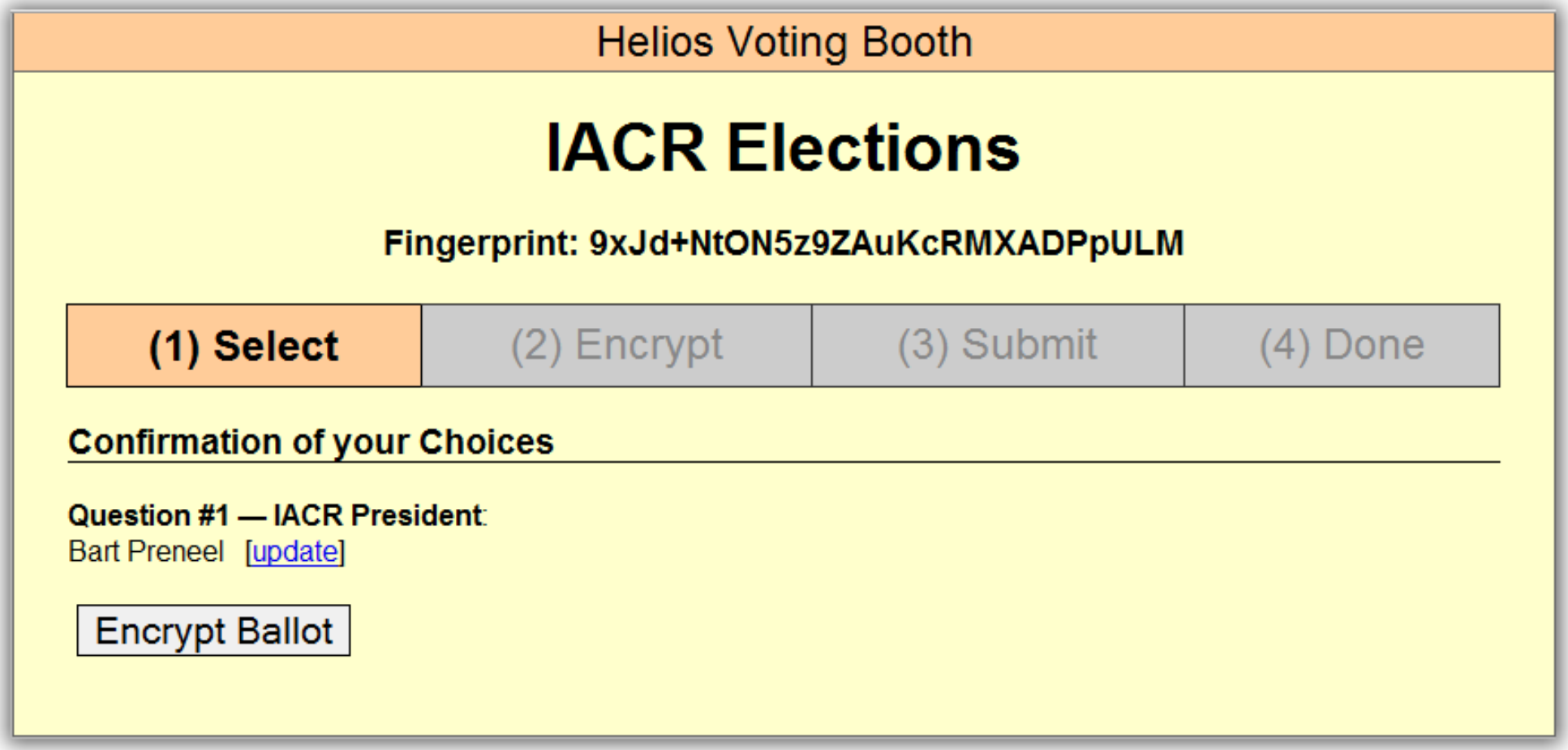
4. THE ATTACK AGAINST HELIOS 2.0

Modifications by and new ideas of my co-author Estehghari:

- Helios allows candidates to provide a URL for a candidate's statement. Using the well known vulnerabilities of Acrobat/Reader, the candidate's statement in PDF is used as the vector. This avoids the need to use e-mail, track the voter e-mail accounts, etc.
- After the client has been hacked, the Java Virtual Machine Firefox extension is modified, installing a Helios 2.0 specific browser rootkit. Using the idea of modifying an existing Firefox extension makes the attack rather stealth.
- Fool the voter to believe an incorrectly displayed audit in Helios 2.0.

Demo of a hacked Helios 2.0 mock IACR election




Helios Voting Booth
IACR Elections
Fingerprint: 9xJd+NtON5z9ZAuKcRMXADPpULM
(1) Select
(2) Encrypt
(3) Submit
(4) Done
Confirmation of your Choices
Question #1 — IACR President:
Bart Preneel [update]
Encrypt Ballot

Helios Voting Booth

IACR Elections

Fingerprint: 9xJd+NtON5z9ZAuKcRMXADPpULM

(1) Select	**(2) Encrypt**	(3) Submit	(4) Done

Your audited ballot

You have chosen to audit your encrypted ballot.

Here is the fully audited ballot information, which you can copy and paste.

"10008239478251978684575614024869231074496728980610868637334458196549326616494313795 03
{"commitment": {"A":
"16022520648352624829201851561864455303852442180911028008745928281446346561752504193 37
"B":
"40555168879896972656101153558372224495907026483694946343787711331186603547184218592 16
"challenge":
"38319662274400943022695672190797159317910832579082106157665109749645029152892429600 85
"response":
"91307819958336341609605028724404154085376684288859452058616219161223286781961506969 46
"answer": [1], "randomness":
["23600527378860879968406305388847134282129871105758042010041293401278399330366095936 4
"54864241329057359504051717597874699299902661946240911388902428110097612733448987045 27
"election_hash": "2R4LkKUBzHuu4zGmDqxHB6/tdNo", "election_id":
"agxoZWxpb3N2b3RpbmdyEAsSCEVsZWN0aW9uGILNCAw"}

Copy the content above (select it).
Visit the Helios Ballot Verifier to ensure it was properly formed.

Go Back to Choices

Helios Single-Ballot Verifier

This single-ballot verifier lets you enter an audited ballot and verify that it was prepared correctly.

Your Ballot:


```
659944150259890214423343117316453037792519403931946924964930574800361051398979961
597107165375712283139206191962331880467377703000287005114461472508702"}],
"answer": [1], "randomness":
["2360052737886087996840630538884713428212987110575804201004129340127839933036609
595364226600415406947911544469476556253219399087383664073865870501762289688433198
919201590308430005545843390302753876841185540920850414471977661827197579226807091
439778399575618966110640049409037621572995158639493173416151034926 6",
"5486424132905735950405171759787469929990266194624091138890242811009761273344898
```


Verify

election fingerprint is 9xJd+NtON5z9ZAuKcRMXADPpULM
ballot fingerprint is N/OPkgjMl/pn4DTl9XJgyMNQXpg
election fingerprint matches ballot
Ballot Contents:
Question #0 - IACR President : Bart Preneel
Encryption Verified
Proofs ok.

Helios Voting

Elections you can audit

IACR Elections

Election ID

agxoZWxpb3N2b3RpbmdyEAsSCEVsZWN0aW9uGILNCAw

Election Fingerprint

9xJd+NtON5z9ZAuKcRMXADPpULM

Vote in this election [Audit a Single Ballot] [Bulletin Board of Cast Votes]

(the tally has already been computed, but you can view the voting interface anyways.)

Administration

Election Done

- voters
- archive election

Tally

IACR President:

- Saghar Estehghari: 1
- Bart Preneel: 0

Audit the Election Tally

[Home] [My Elections] [Learn] [Blog/Updates]

Details of the hacking

Two weeks were spent on the development of the actual attack software.

Around 950 lines of code were written for this attack. Of these, roughly 50% is dedicated to the development of the malicious extension. The other 50% is related to embed JavaScript for Adobe Acrobat and the executable program. Only 10% of the codes is unique to Helios.

The software does not slow the client machine down. The only noticeable event during the attack run-time is the sudden closure of the browser, as the Firefox needs a restart for loading the changes

that have been made to the victim's extension.

5. GENERALIZATIONS, DEFENSES AND HELIOS 3.0

Generalizations

Our attack was very limited in scope: the actual attack works only on Windows XP and if the voter uses Firefox and a vulnerable version of Acrobat Reader. However, only 2 weeks were spent on the development!

Internet voting is being pushed for national elections in several countries. In such settings hackers will have enough incentives to extend our attack to:

- other platforms, which is rather easy to do. To attack Vista platforms other vectors should be used instead of exploiting Acrobat Reader's

vulnerability.

- Attack privacy (as suggested by Estehghari, and made more stealth by a referee). Not done, since we ran out of time. Since the e-mail address of the voter is known in Helios, this is very easy when the client is hacked.
- only perform the attack with a small enough probability (suggested by referee).

Defenses and their limitations

Some defenses we considered are:

- Disable JavaScript in Adobe Reader: works against this attack.
- Analyze the candidacy statement: can be bypassed when using another vector.
- Use dedicated trusted hardware to check the cryptographic thumbprint. However, Helios does not come with this.
- Avoid Helios, e.g., using Code Voting. However, Code Voting has its own disadvantages.

Helios 3.0

After our Crypto 2009 Rump-Session presentation Helios 2.0 has been modified.

In Helios 3.0 the voters are now able to post the audited ballot to the Helios server. This implies that not only the voter is able to check whether the hash was properly computed, but also the ballot data, i.e. the randomness, the vote and the hash, can be posted on some public webpage.

6. FUTURE

Our submission was about Helios 2.0 and not about Helios 3.0. We expect to write up the weaknesses of Helios 3.0 and explain the limitations of using public webpages to patch the attack against audit.

We also plan to demonstrate that attacking privacy is easy.

7. CONCLUSIONS

Most research on cryptographic e-voting was done on booth based e-voting. So, it is no surprize that when implemented for Internet e-voting, the cryptographic security can be bypassed in such systems.

Our attack focused on undermining correctness in Helios 2.0. However, privacy is a much bigger concern when using Helios. Helios 2.0 and 3.0 do not guarantee privacy when the client is hacked!

Some potential viewpoints on Internet e-voting:

- these opposing Helios and Internet e-voting are just neo-Luddites

- the attack against Helios 2.0 is very limited (many referees disagreed with such a conclusions!)
- botnets show the power of modern hackers, so one can only expect much worse attacks against Internet e-voting.

May be the worst view on internet e-voting can be expressed using the title of Bollyn's book:

Death of Democracy or May the Best Hacker Win.

A more positive viewpoint might be that:

researchers may eventually produce a proper solution for Internet e-voting, e.g., based on a redesign of Helios, or using a version of Code Voting removing some of its disadvantages. However that means one should delay deployment until such a solution is at hand.