Internet Voting
An Assessment & Critique

Jeremy Clark, Concordia University

English / French

Apologies 🙏

Thank you for the translation services

Where I am

- Associate Professor at the Concordia Institute for Information Systems Engineering (CIISE) in Montreal
- NSERC / Raymond Chabot Grant Thornton (RCGT) / Catallaxy Industrial Research Chair in Blockchain
- PhD from the University of Waterloo (2009)
- Team of 6+ graduate students
- Academic publications, textbooks, editorial positions on both verifiable voting & blockchain
- Part of team deploying verifiable voting (in-person/remote) for the first time in governmental elections
- Worked with various municipalities (Takoma Park, Toronto, Edmonton…) on secure voting
- Worked with government on Bitcoin/blockchain (Bank of Canada, RCMP, AMF, etc, …)
- Contributed to courses (Princeton, MIT) on bitcoin/blockchain

Online Voting

Convenient

Accessible

Environmentally-friendly

Increase turnout

Cheap

Secure

Online Voting

✅ Convenient

Accessible

Environmentally-friendly

Increase turnout

Cheap

Secure

Online Voting

✅ Convenient

✅✅✅ Accessible

Environmentally-friendly

Increase turnout

Cheap

Secure

Online Voting

✅ Convenient

✅✅✅ Accessible

✅ Environmentally-friendly

Increase turnout

Cheap

Secure

Online Voting

✅ Convenient

✅✅✅ Accessible

✅ Environmentally-friendly

🚫 Increase turnout

Cheap

Secure

Online Voting

✅ Convenient

✅✅✅ Accessible

✅ Environmentally-friendly

🚫 Increase turnout

❓ Cheap

Secure

Online Voting

✅ Convenient

✅✅✅ Accessible

✅ Environmentally-friendly

🚫 Increase turnout

❓ Cheap

🚫🚫🚫 Secure

1) Voter Authentication

When you vote in person, you show ID
When you vote online, what do you show?
PINs can be intercepted, birthdays guessed

Precedent: 2017 leadership election for United Conservative Party (UCP) in Alberta

Detectability: medium
Also affected: mail-in ballots
Unaffected: in-person voting

2) Vote Selling / Coercion

Voters can vote in front of anyone or give their passwords/PINs to anyone, for payment, social pressure, or duress.

Precedent: vote selling has been documented in Philippines (2002), Russia & Mexico (2000), Kuwait & Thailand (1996), …

Detectability:	medium
Also affected:	mail-in ballots
Unaffected:	in-person voting

3) Malware

Voters assume the responsibility of ensuring their computers are free from viruses that could modify their ballots.

Precedent: malware is rampant online and in unsolicited emails; proof of concept vote stealing malware exists; state-sponsored

Detectability:	low (medium in long term)
Also affected:	none
Unaffected:	mail-in ballots, in-person voting

3) Malware

Vote
ensu
virus

Preceder
proof of c

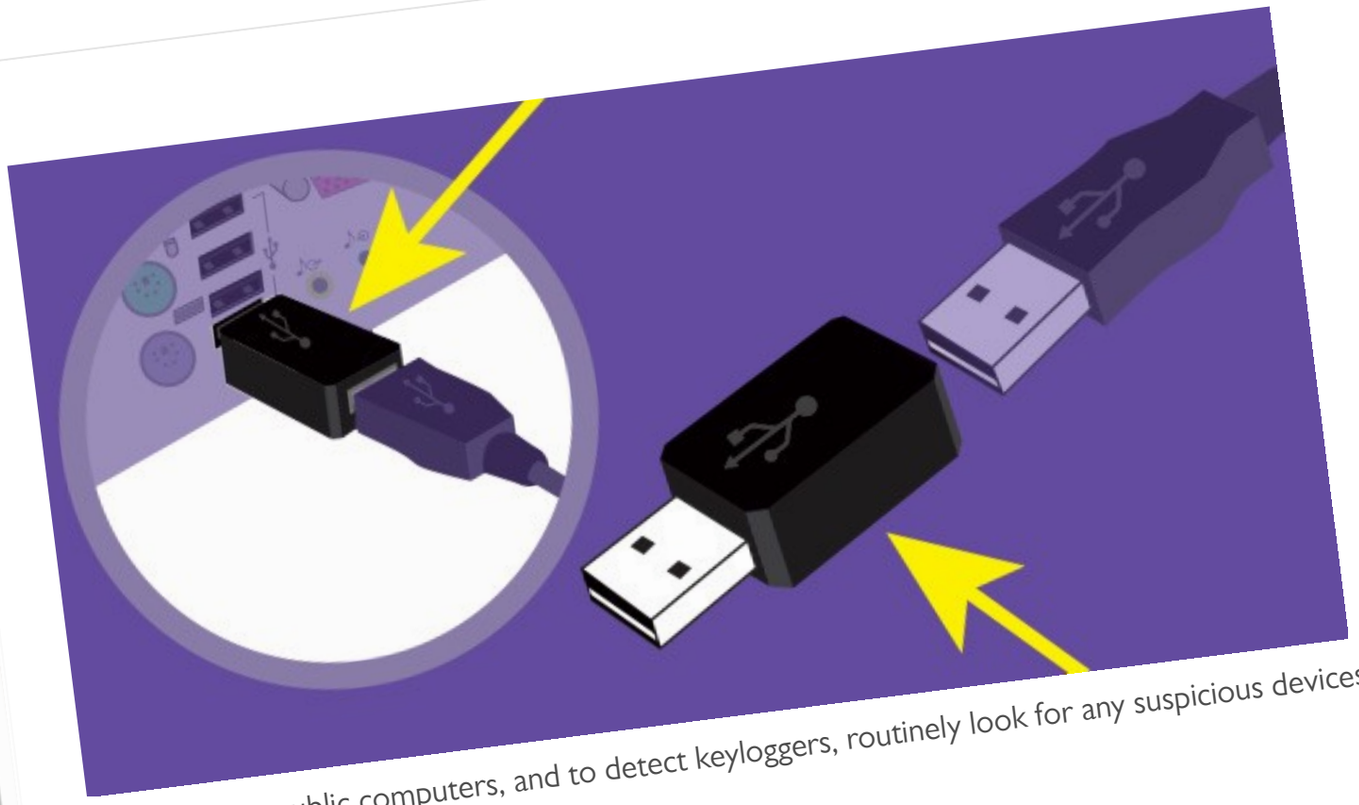
Concordia University

http://www.concordia.ca/content/shared/en/news/main/stories/2016/03/21/security-breach-involving-some-library-standing-express-workstations-keylogger.html

Security breach involving some library standing express workstations

Keylogger devices found on some standing express workstations in the libraries

March 21, 2016



When using public computers, and to detect keyloggers, routinely look for any suspicious devices or innocuous connector between the keyboard cable and the USB port.

keyloggers, which can capture computer keystrokes, were recently found on
Webster and Vanier libraries. These comput

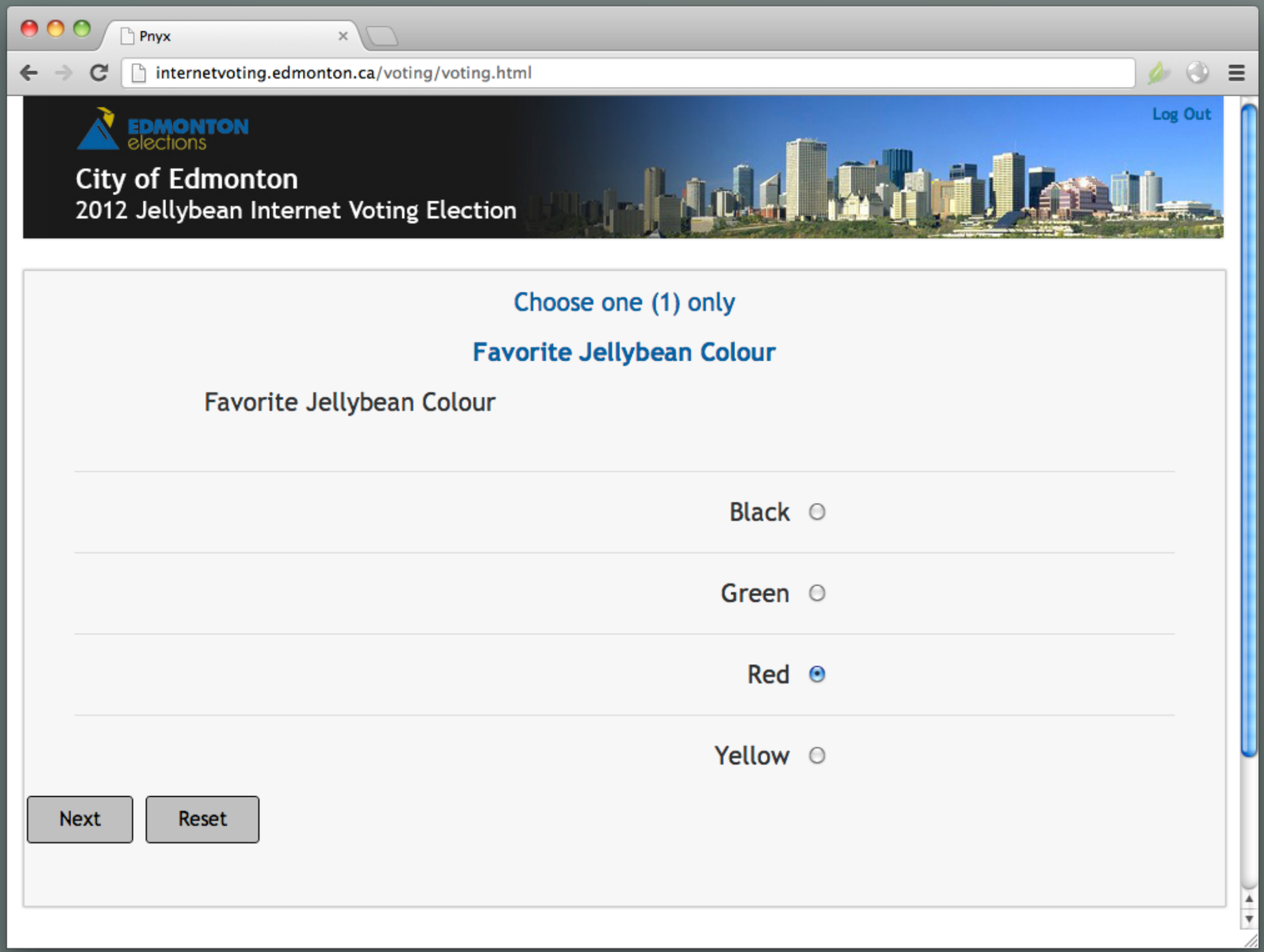
4) Insecure Transmission

To make sure ballots are transmitted securely, voters must verify the state of their connection and understand errors.

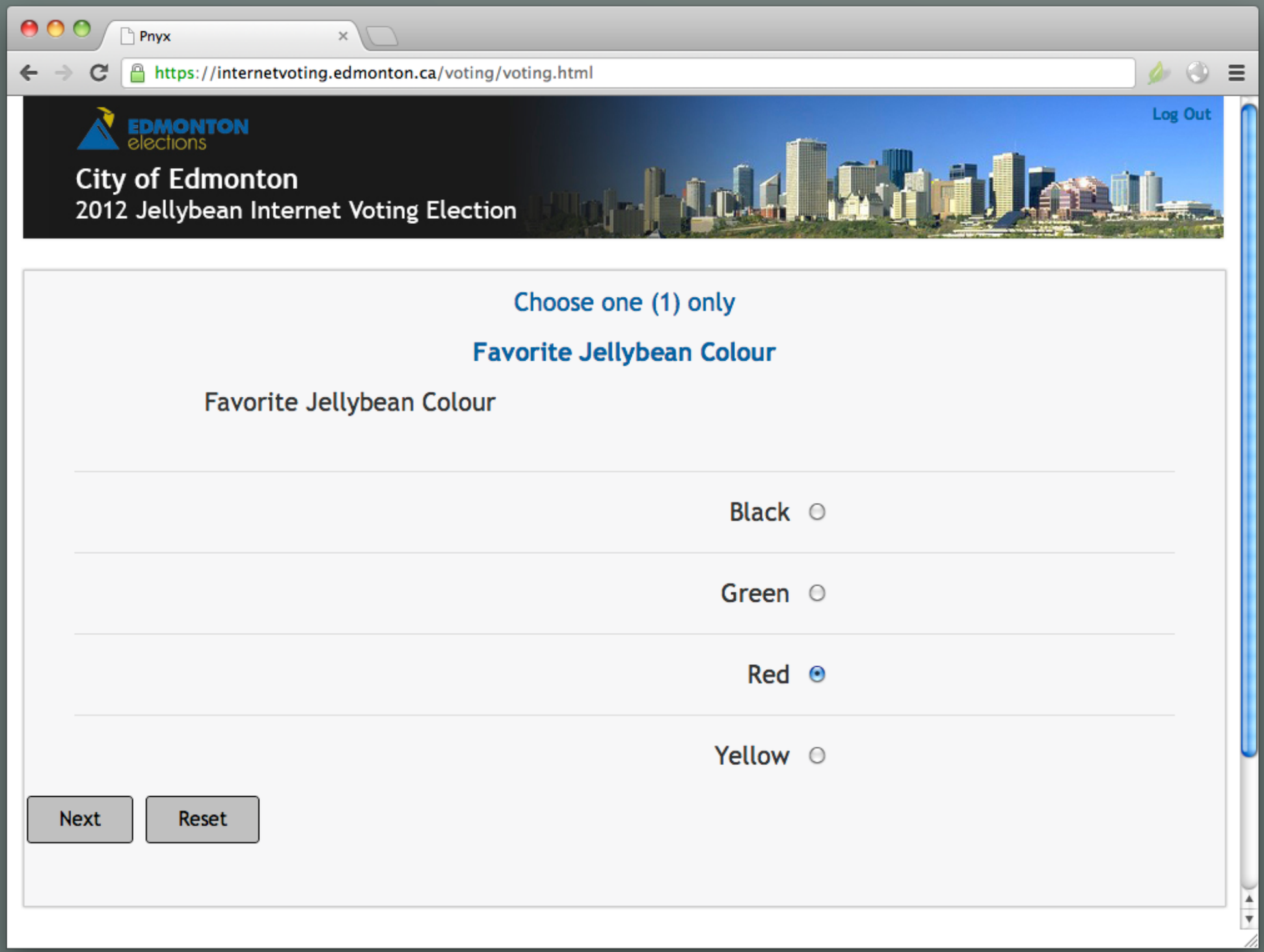
Precedent: attack on Google services in Iran, and Facebook in Syria; Comodo and DigiNotar certificate authorities compromised

Detectability:	medium
Also affected:	mail-in ballots
Unaffected:	in-person voting

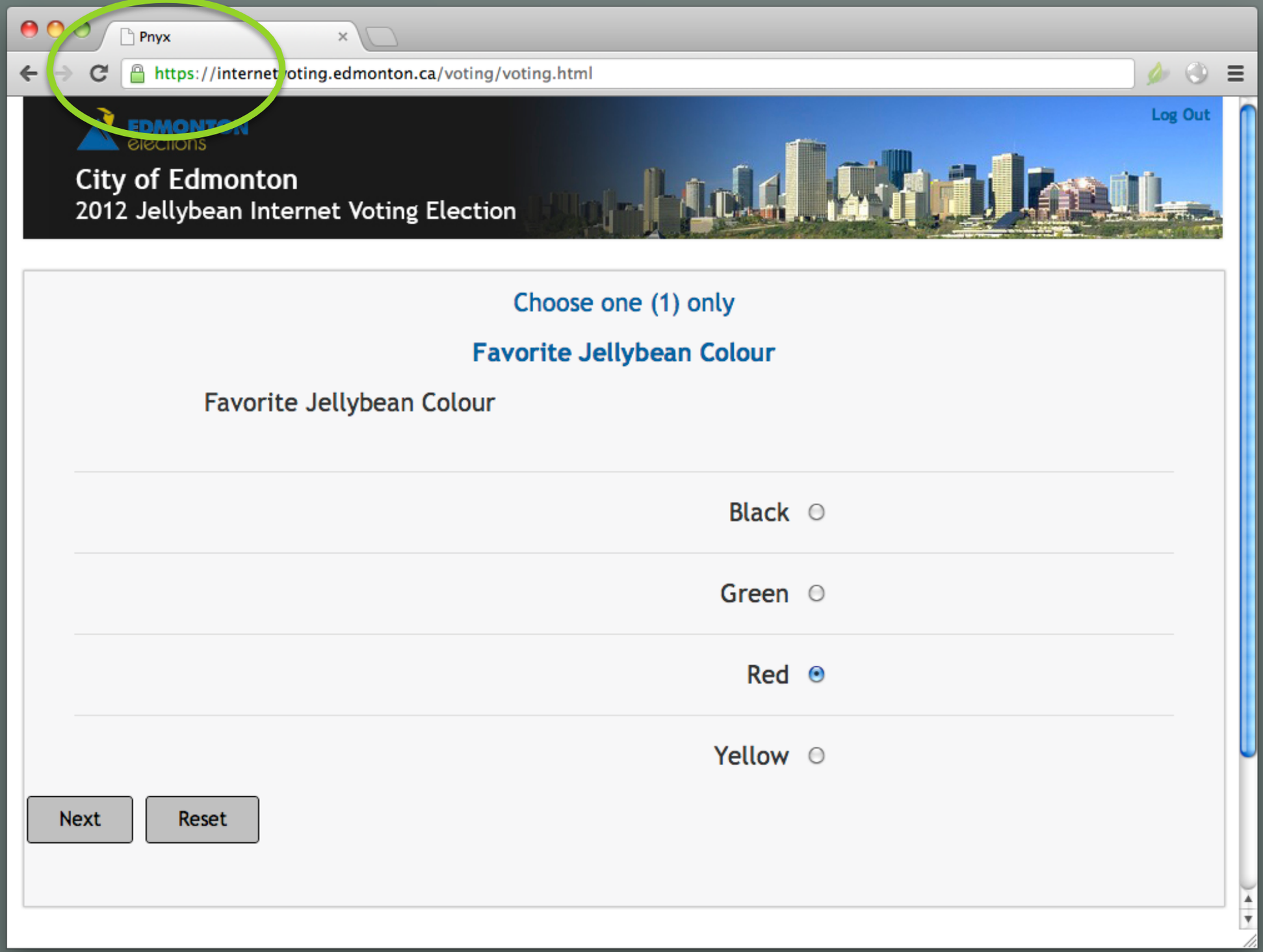
4) Insecure Transmission



4) Insecure Transmission



4) Insecure Transmission



5) Remote Intrusion

The election authority must put a computer on the public internet to collect votes.
Anyone anywhere can try to break-in.

Precedent: nearly every major website (Google, FBI, CIA,…) and Washington DC Internet Voting pilot

Detectability:	low
Also affected:	none
Unaffected:	mail-in ballots, in-person voting

6) Denial of Service

Anyone can rent a large collection of computers and flood the internet voting website with traffic, making it unresponsive

Precedent: NDP leadership internet election (2012); many elections in Ontario; power outages

Detectability:	high
Also affected:	none
Unaffected:	mail-in ballots, in-person voting

6) Denial of Service

tvo

Ontario Hubs

How e-voting's big night went wrong in Ontario

During Monday's elections, residents of 48 municipalities across the province faced service disruptions while trying to vote electronically. (iStock.com/fatido)

Municipalities have been adopting electronic voting for the past 15 years. But could a glitch that affected dozens of communities Monday night derail the experiment?

Claude Sharma - *Published on October 24, 2018*

A Few More

- Phishing (fraudulent emails/calls asking for your password or linking to an imposter website)
- Anonymity (vendor knows how you voted, even with PINs, you often also use your birthdate)
- Insider Threats (manipulation by election officials, IT staff, vendors, …)

Online Voting vs. Online Banking

- Online bank is not secure—fraud is tolerated
- Any amount of voting fraud should not be tolerated
- Bank users have zero liability for online banking
- Voters are responsible for their own security

- Banking transactions are traceable and reversible
- A credit card with $1000 limit sells for $42 on the black market
- Votes are secret, modifications cannot be noticed

Online Voting

✅ Convenient

✅✅✅ Accessible

✅ Environmentally-friendly

🚫 Increase turnout

❓ Cheap

🚫🚫🚫 Secure

Questions?

@PulpSpy http://vaddr.space