Man-At-The-End Attacks and Defenses

Internet 2 Global Summit

Christian Collberg Saumya Debray

Department of Computer Science
University of Arizona

http://collberg.cs.arizona.edu

collberg@gmail.com

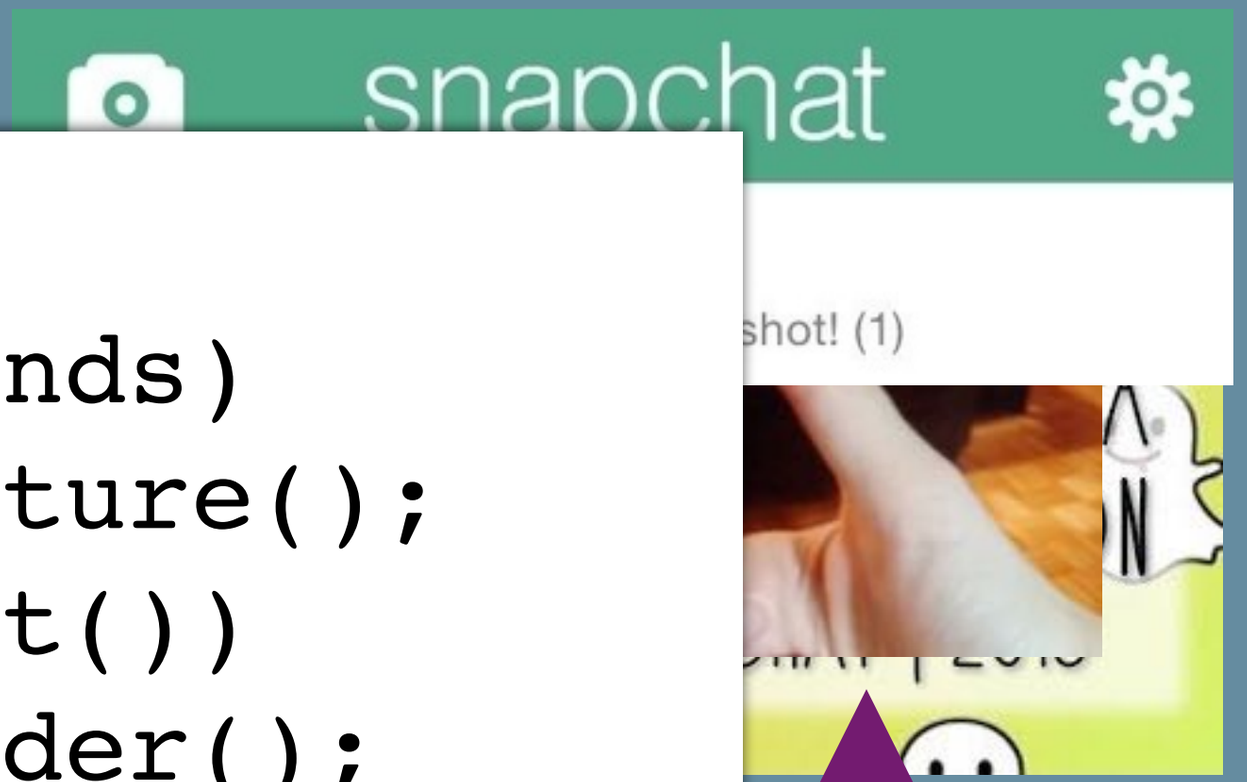
Supported by NSF grants 1525820 and 1318955 and
Israel Binational Science Foundation grant 2008362

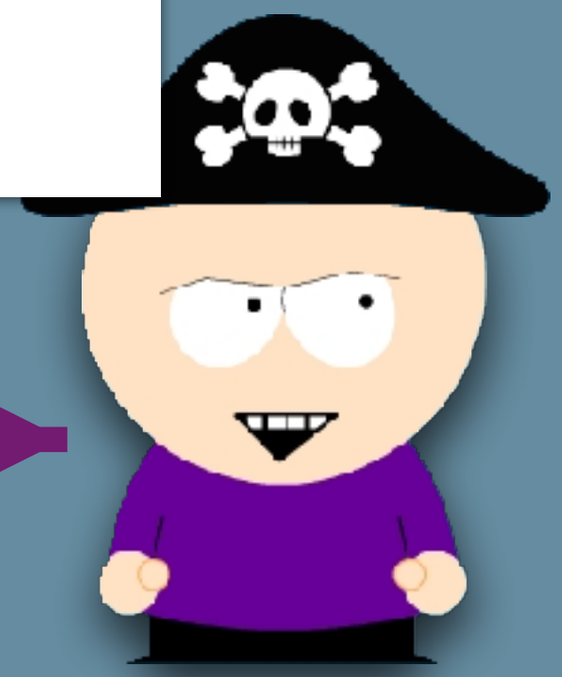
Man-At-The-End Scenarios

Protection Tools vs Analysis Tools

Application: Secure Provenance

```
snapchat() {
    after (8 seconds)
        remove_picture();
    if (screenshot())
        notify_sender();
    if (app_is_tampered())
        punish_bob();
}
```

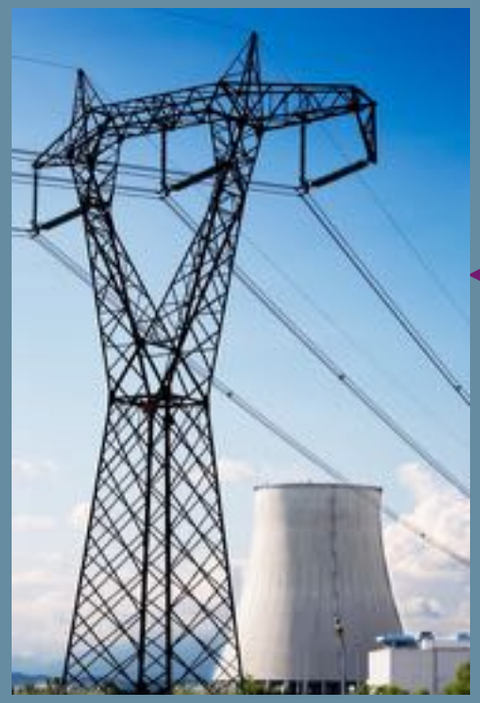




```
set_top_box() {
    if (bob_paid("ESPN"))
        allow_access();

    if (is_tampered())
        punish_bob();
}
```

Tamper Clone Keys Code & Content



kWh

On/Off

Off!

Man-At-The-End (MATE) attacks occur in any setting where an adversary has physical access to a device and compromises it by inspecting, reverse engineering, or tampering with its hardware or software.

Assets

- Source
- Algorithms
- Keys
- Media

Protection Tools vs. Analysis Tools

Prog(){

Assets

- Source
- Algorithms
- Keys
- Media

}

Code Transformations

Tigress

Prog'(){

Assets

- Source
- Algorithms
- Keys
- Media

}

Lynx

Assets

- Source
- Algorithms
- Keys
- Media

Code Analyses

Research Program

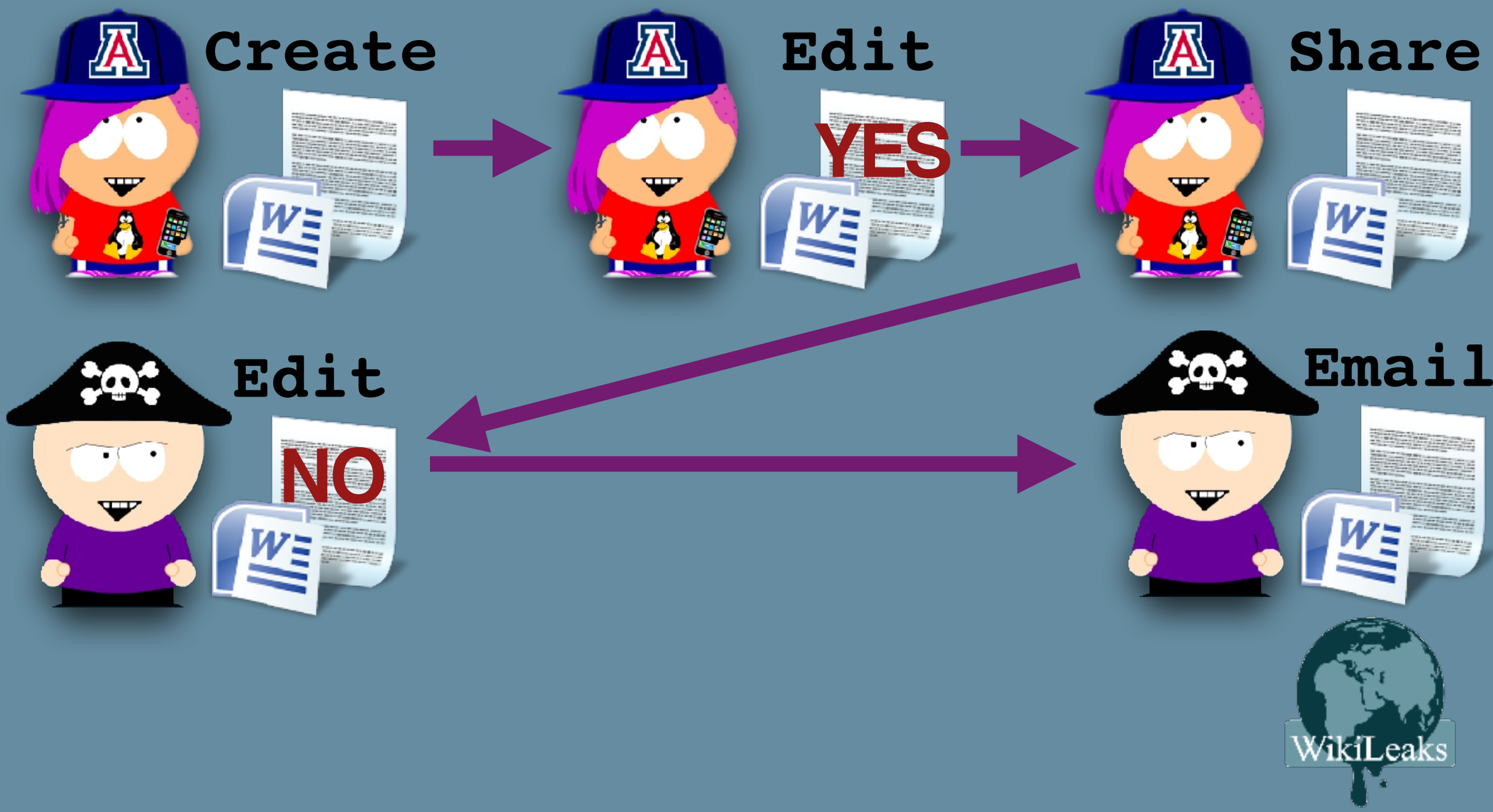
Overhead vs Protection

Precision vs Performance

- Protection techniques with better protection and performance
- Analysis techniques with better precision and performance
- Better methods of evaluation
- Novel application domains

Secure Provenance for Office Documents

Document Provenance

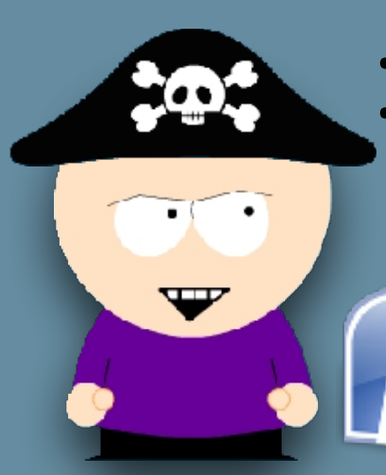


Document Provenance

Create

Edit

Share



Edit

Email

Provenance

When	Who	What
April 23	Alice	Create document
April 24	Alice	Add text “YES”
April 25	Alice	Share with Bob
April 26	Bob	Change “YES” to “NO”
April 27	Bob	Email to WikiLeaks

Digital Provenance

The provenance of a digital object gives a history of its creation, update, and access. It provides meta-level information of the sequence of events that lead up to the current version of the object, as well as its chain of custody.

Attacks on Provenance

Create

Edit

Share

Edit

Email

Provenance

When	Who	What
April 23	Alice	Create document
April 24	Alice	Add text “YES”
April 25	Alice	Share with Bob
April 26	Alice	Change “YES” to “NO”
April 27	Bob	Email to Charles

Who Needs Secure Document Provenance?

Everything!

Raytheon

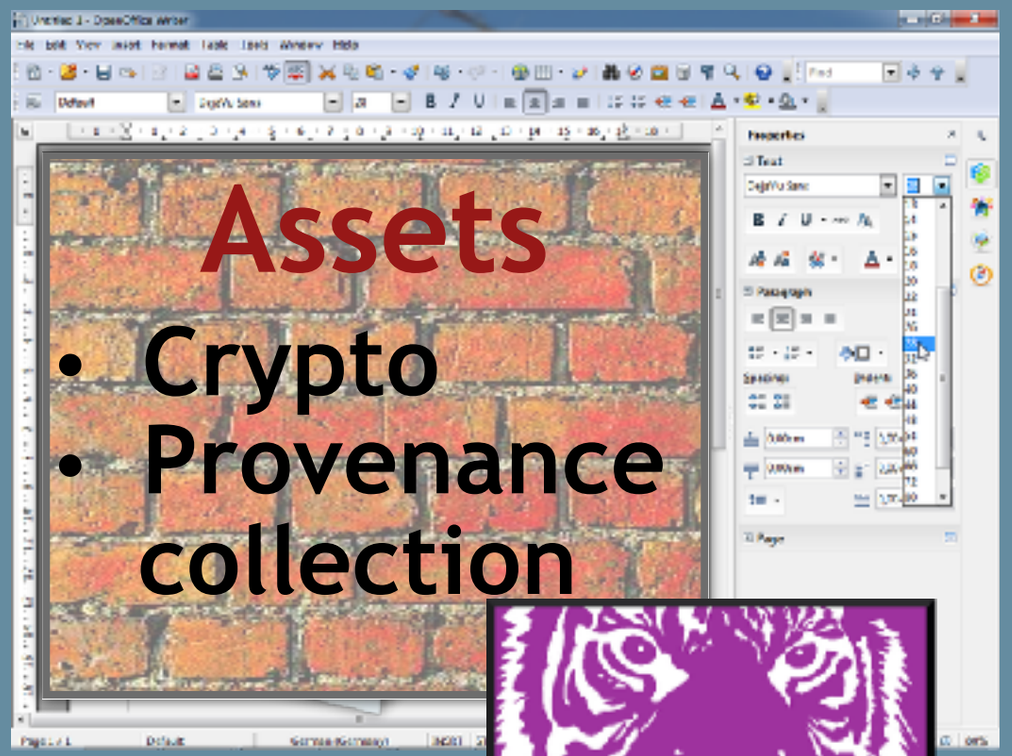
Missile sales

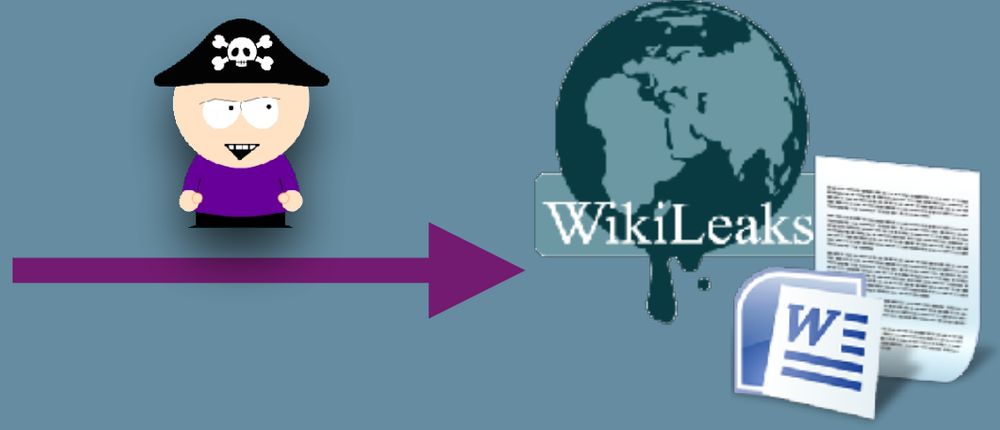
Malicious Insider

Visitor Logs

iPhone 8 Design

Secure Provenance System





- Trace leaked document back to insider
- Ensure integrity of provenance
- Collect fine-grained provenance
- Extension of OpenOffice Writer

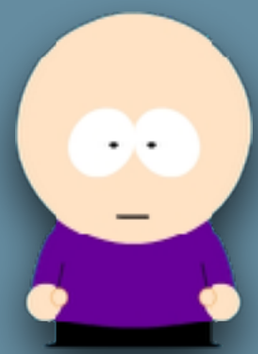
haathi

- End-point security is essential to ensure overall system integrity and confidentiality

- Our group builds freely available
  - protection tools
  - analysis tools
  - real-world use cases

- Tigress is used both in industry and academia

- We seek collaboration to guide further
  - tool development
  - evaluation
  - use cases



Questions?

collberg@gmail.com

tigress.cs.arizona.edu
collberg.github.io/provenance
www2.cs.arizona.edu/projects/lynx-project