LogPicker

Strengthening Certificate Transparency Against Covert Adversaries

Alexandra Dirksen[*], David Klein[*], Robert Michael[†], Konrad Rieck[†], Martin Johns[*]

[*]Institute of Application Security
[†]Institute of System Security

a.dirksen@tu-braunschweig.de
@z4lem

INSTITUTE FOR APPLICATION SECURITY

Technische Universität Braunschweig

(In)Secure Web Communication

https://

Secure Communication on the Web

- HTTPS $\rightarrow$ default nowadays [4]

Secure Communication on the Web

- HTTPS $\rightarrow$ default nowadays [4]
- CAs as trust anchors of Web PKI

Secure Communication on the Web

- HTTPS $\rightarrow$ default nowadays [4]
- CAs as trust anchors of Web PKI
- Guidelines by CA/Browser Forum [7]

Secure Communication on the Web

- HTTPS $\rightarrow$ default nowadays [4]
- CAs as trust anchors of Web PKI
- Guidelines by CA/Browser Forum [7]
- Increasing number of illicit certificate creations [10]

A Tale of Illicit Certificate Creations

[14]

[12]

[12]

[15]

[9]

HTTPS Interception Attempts by Governments

[1]

EFF DONATE

EFF TURNS 30! LEARN MORE.

Kazakhstan Considers a Plan to Snoop on all Internet Traffic

DEEPLINKS BLOG

NEWS UPDATE BY BILL BUDINGTON AND EVA GALPERIN
DECEMBER 10, 2015

In an unusually direct attack on online privacy and free speech, the ruling regime of Kazakhstan appears to have mandated the country's telecommunications operators to intercept citizens' Internet traffic using a government-issued certificate starting on January 1, 2016. The press release announcing the new measure was published last week by Kazakhtelecom JSC, the nation's largest telecommunications company, but appears to

EFF DONATE

EFF TURNS 30! LEARN MORE.

Proposed New Internet Law in Mauritius Raises Serious Human Rights Concerns

DEEPLINKS BLOG

BY JILLIAN C. YORK AND DAVID GREENE
APRIL 30, 2021

As debate continues in the U.S. and Europe over how to regulate social media, a number of countries—such as India and Turkey—have imposed stringent rules that threaten free speech, while others, such as Indonesia, are considering them. Now, a new proposal to amend Mauritius' Information and Communications Technologies Act (ICTA)

EFF

EFF TURNS 30! LEARN MORE.

A Syrian Man-In-The-Middle Attack against Facebook

DEEPLINKS BLOG

TECHNICAL ANALYSIS BY PETER ECKERSLEY
MAY 5, 2011

Yesterday we learned of reports that the Syrian Telecom Ministry had launched a man-in-the-middle attack against the HTTPS version of the Facebook site. The attack is ongoing and has been seen by users of multiple Syrian ISPs. We cannot confirm the identity of the perpetrators.

The attack is not extremely sophisticated: the certificate is invalid in user's browsers, and

EFF

EFF TURNS 30! LEARN MORE.

Iranian Man-in-the-Middle Attack Against Google Demonstrates Dangerous Weakness of Certificate Authorities

DEEPLINKS BLOG

AUGUST 29, 2011

What's worse than finding a worm in your apple? Finding half a worm.

What's worse than discovering that someone has launched a man-in-the-middle attack against Iranian Google users, silently intercepting everything from email to search

[1] Kazakhstan: [16], Mauritius: [3], Syria: [8], Iran: [17]

HTTPS Interception Attempts by Governments

[1]

DONATE

EFF TURNS 30! LEARN MORE.

Kazakhstan Considers a Plan to Snoop on all Internet Traffic

DEEPLINKS BLOG

NEWS UPDATE BY BILL BUDINGTON AND EVA GALPERIN
DECEMBER 10, 2015

In an unusually direct attack on online privacy and free speech, the ruling regime of Kazakhstan appears to have mandated the country's telecommunications operators to intercept citizens' Internet traffic using a government-issued certificate starting on January 1, 2016. The press release announcing the new measure was published last week by Kazakhtelecom JSC, the nation's largest telecommunications company, but appears to

DONATE

EFF TURNS 30! LEARN MORE.

Proposed New Internet Law in Mauritius Raises Serious Human Rights Concerns

DEEPLINKS BLOG

BY JILLIAN C. YORK AND DAVID GREENE
APRIL 30, 2021

As debate continues in the U.S. and Europe over how to regulate social media, a number of countries—such as India and Turkey—have imposed stringent rules that threaten free speech, while others, such as Indonesia, are considering them. Now, a new proposal to amend Mauritius' Information and Communications Technologies Act (ICTA)

EFF TURNS 30! LEARN MORE.

A Syrian Man-In-The-Middle Attack against Facebook

DEEPLINKS BLOG

TECHNICAL ANALYSIS BY PETER ECKERSLEY
MAY 5, 2011

Yesterday we learned of reports that the Syrian Telecom Ministry had launched a man-in-the-middle attack against the HTTPS version of the Facebook site. The attack is ongoing and has been seen by users of multiple Syrian ISPs. We cannot confirm the identity of the perpetrators.

The attack is not extremely sophisticated: the certificate is invalid in user's browsers, and

EFF TURNS 30! LEARN MORE.

Iranian Man-in-the-Middle Attack Against Google Demonstrates Dangerous Weakness of Certificate Authorities

DEEPLINKS BLOG

AUGUST 29, 2011

What's worse than finding a worm in your apple? Finding half a worm.

What's worse than discovering that someone has launched a man-in-the-middle attack against Iranian Google users, silently intercepting everything from email to search

Why should attacker stop here?

[1] Kazakhstan: [16], Mauritius: [3], Syria: [8], Iran: [17]

A Strong Attack Scenario

Covert Adversary [5][2]

[2]Aumann & Lindell, 2007
[3]Soghoian & Stamm, 2010

A Strong Attack Scenario

Covert Adversary [5][2]

Compelled Certificate Creation [18][3]

[2] Aumann & Lindell, 2007
[3] Soghoian & Stamm, 2010

A Strong Attack Scenario

Covert Adversary [5][2]

Compelled Certificate Creation [18][3]

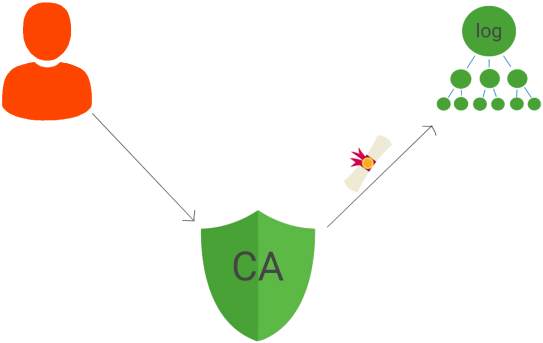
Attacker succeeds if he can create a rogue certificate that remains unnoticed by domain owner!

[2] Aumann & Lindell, 2007
[3] Soghoian & Stamm, 2010

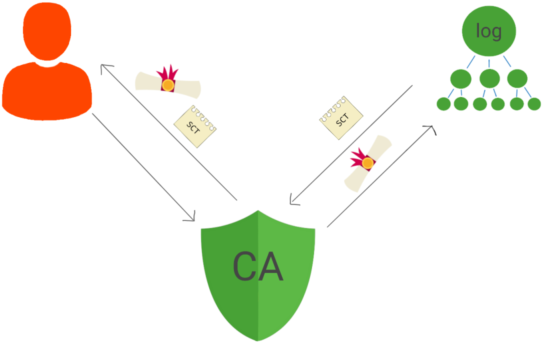
Public Certificate Creation[4]

[4] Laurie, 2012

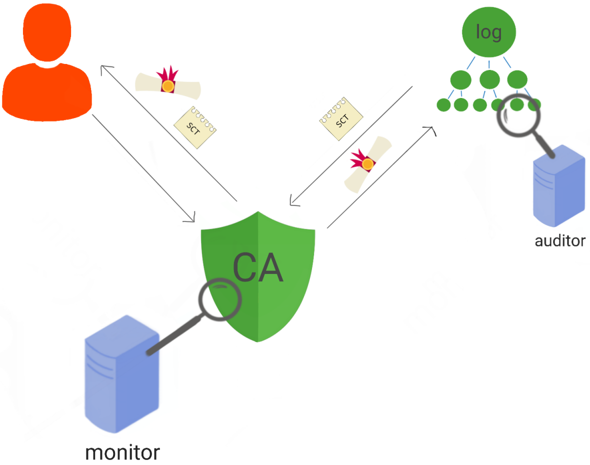
Certificate Transparency



Certificate Transparency



Certificate Transparency



Certificate Transparency is still vulnerable

[5] June, 2021
[6] Bussiere, 2008

Certificate Transparency is still vulnerable

- All logs belong to CA vendors[1][5]

[5] June, 2021
[6] Bussiere, 2008

Certificate Transparency is still vulnerable

- All logs belong to CA vendors[1][5]
- First compromise of a CT log in 2020[2]

[5] June, 2021
[6] Bussiere, 2008

Certificate Transparency is still vulnerable

- All logs belong to CA vendors[1][5]
- First compromise of a CT log in 2020[2]
- CT is vulnerable to collaboration attacks[11]

[5] June, 2021
[6] Bussiere, 2008

Certificate Transparency is still vulnerable

- All logs belong to CA vendors[1][5]
- First compromise of a CT log in 2020[2]
- CT is vulnerable to collaboration attacks[11]
  - Low probability, but high impact [6][6]

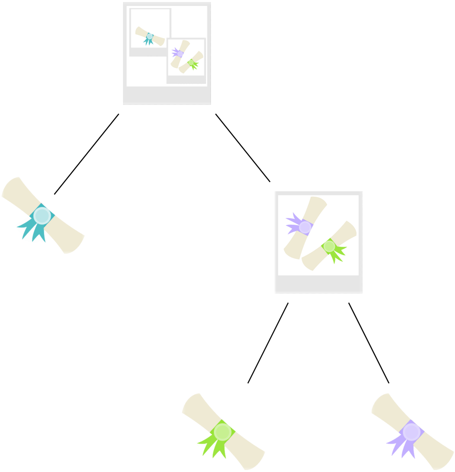
[5] June, 2021
[6] Bussiere, 2008

Certificate Transparency is still vulnerable

- All logs belong to CA vendors[1][5]
- First compromise of a CT log in 2020[2]
- CT is vulnerable to collaboration attacks[11]
  - Low probability, but high impact [6][6]
  - Split View attacks possible

[5] June, 2021
[6] Bussiere, 2008

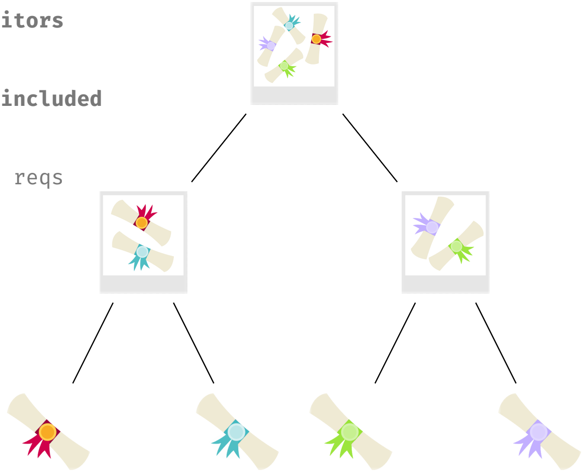
Split View Attack



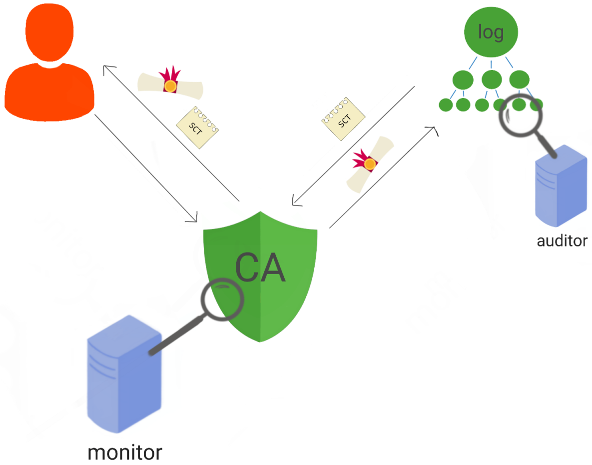
- View served to **monitors**
- Rogue certificate **excluded**
- Attack remains undetected

Split View Attack

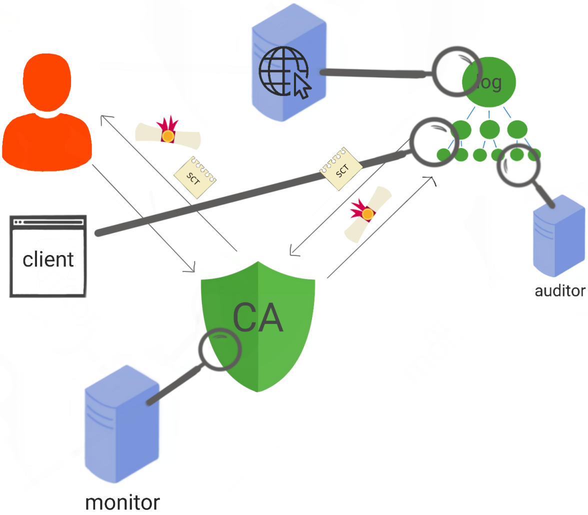
- View served to **auditors**
- Rogue certificate **included**
- Violations of CA/B reqs remain undetected



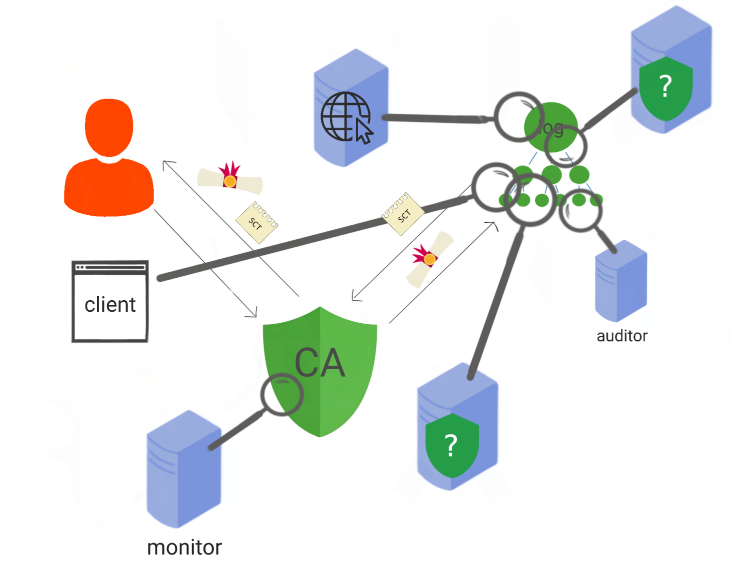
Certificate Transparency - Reminder on CT



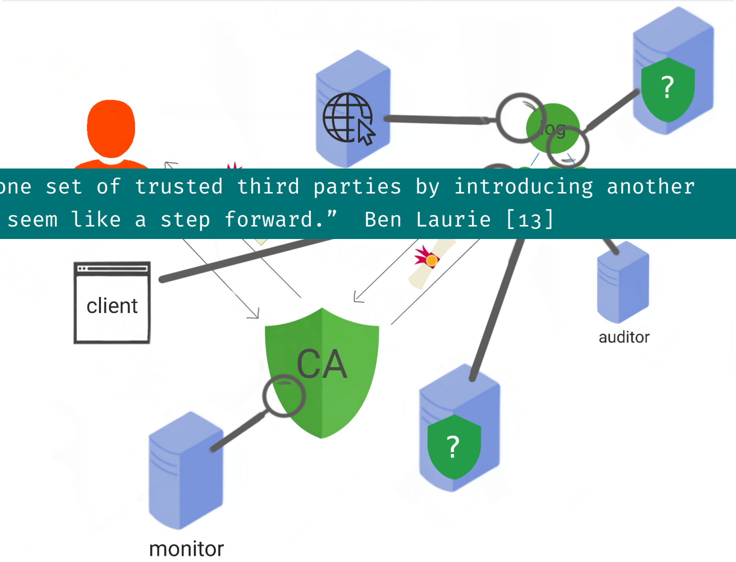
Certificate Transparency - Gossip



Further Trusted Parties?

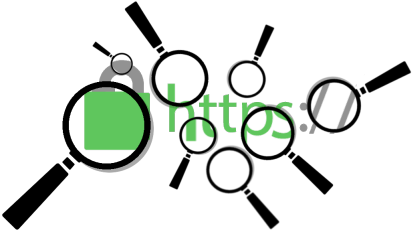


Further Trusted Parties?



"fixing one set of trusted third parties by introducing another "doesn't seem like a step forward." Ben Laurie [13]

LogPicker: A Decentralized Approach



Desiderata

- Security Goals

Desiderata

- Security Goals
  - Thwarts collaboration of malicious CA/CT logs

Desiderata

- Security Goals
  - Thwarts collaboration of malicious CA/CT logs
  - More witnesses to the certificate issuance

Desiderata

- Security Goals
  - Thwarts collaboration of malicious CA/CT logs
  - More witnesses to the certificate issuance
  - Proof of the certificate issuance

Desiderata

- Security Goals
  - Thwarts collaboration of malicious CA/CT logs
  - More witnesses to the certificate issuance
  - Proof of the certificate issuance
  - Earlier involvement of monitors

Desiderata

- Security Goals
  - Thwarts collaboration of malicious CA/CT logs
  - More witnesses to the certificate issuance
  - Proof of the certificate issuance
  - Earlier involvement of monitors
- Design Goals

Desiderata

- Security Goals
  - Thwarts collaboration of malicious CA/CT logs
  - More witnesses to the certificate issuance
  - Proof of the certificate issuance
  - Earlier involvement of monitors
- Design Goals
  - No involvement of user data

Desiderata

- Security Goals
  - Thwarts collaboration of malicious CA/CT logs
  - More witnesses to the certificate issuance
  - Proof of the certificate issuance
  - Earlier involvement of monitors
- Design Goals
  - No involvement of user data
  - No change on webservers [19]

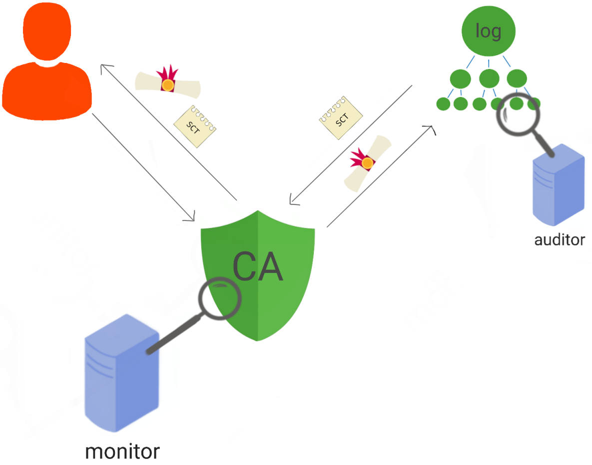
Desiderata

- Security Goals
  - Thwarts collaboration of malicious CA/CT logs
  - More witnesses to the certificate issuance
  - Proof of the certificate issuance
  - Earlier involvement of monitors
- Design Goals
  - No involvement of user data
  - No change on webservers [19]
  - Incremental deployability

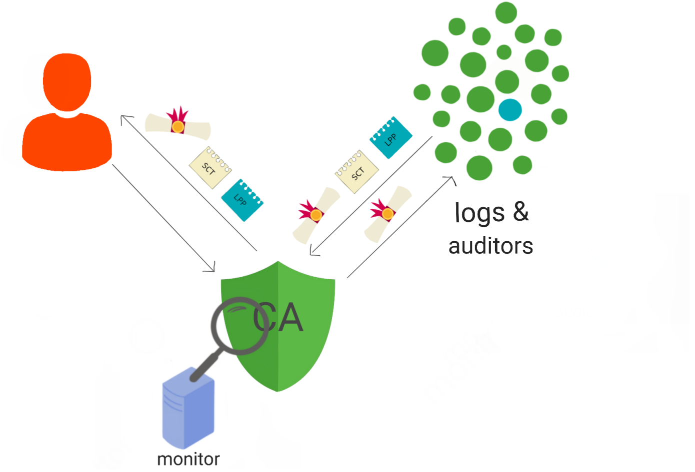
Desiderata

- Security Goals
  - Thwarts collaboration of malicious CA/CT logs
  - More witnesses to the certificate issuance
  - Proof of the certificate issuance
  - Earlier involvement of monitors
- Design Goals
  - No involvement of user data
  - No change on webservers [19]
  - Incremental deployability
  - No new trusted entities

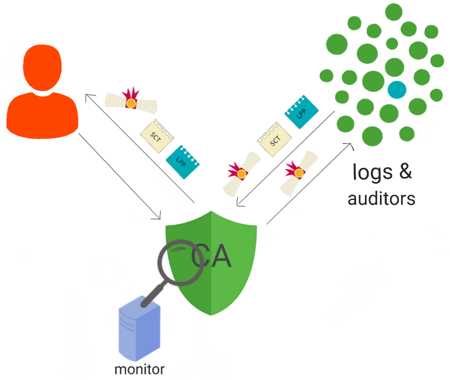
LogPicker - Reminder on CT



LogPicker - High Level Overview

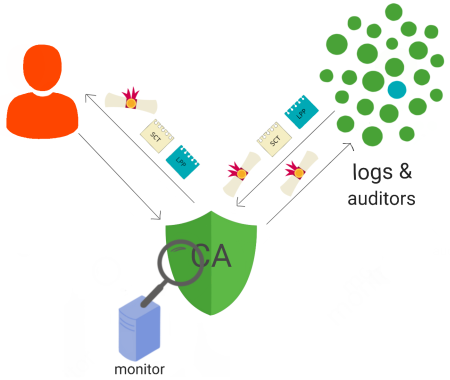


LogPicker - High Level Overview



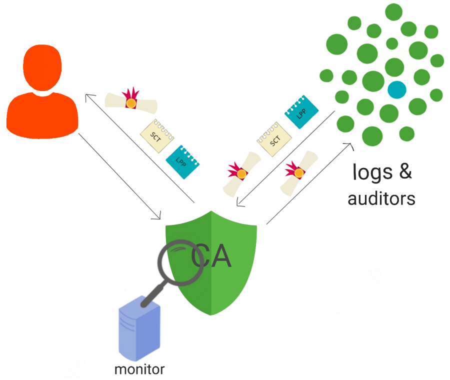
1. CA chooses leader

LogPicker - High Level Overview



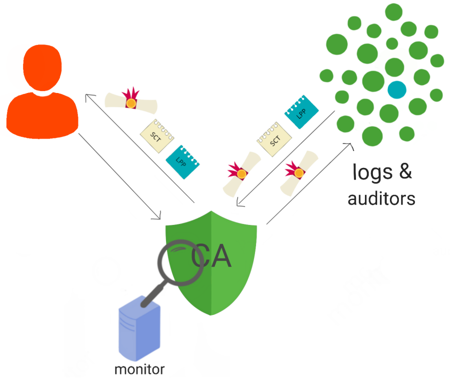
1. CA chooses leader
2. Leader contacts log pool

LogPicker - High Level Overview



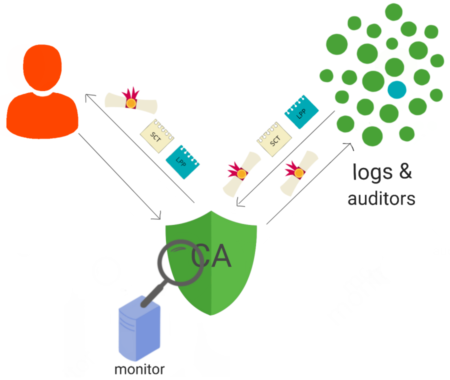
1. CA chooses leader
2. Leader contacts log pool
3. Pool select one log

LogPicker - High Level Overview



1. CA chooses leader
2. Leader contacts log pool
3. Pool select one log
4. Each log signs the proof

LogPicker - High Level Overview



1. CA chooses leader
2. Leader contacts log pool
3. Pool select one log
4. Each log signs the proof
5. Proof is aggregated & attached to cert

LogPicker's Achievements

- Security Goals
  - ✓ Thwarts collaboration of malicious CA/CT logs
  - – More witnesses to the certificate issuance
  - – Proof of the certificate issuance
  - – Earlier involvement of monitors
- Design Goals
  - – No involvement of user data
  - – No change on webservers
  - – Incremental deployability
  - – No new or trusted entities

LogPicker's Achievements

- Security Goals
  - ✓ Thwarts collaboration of malicious CA/CT logs
  - ✓ More witnesses to the certificate issuance
  - – Proof of the certificate issuance
  - – Earlier involvement of monitors
- Design Goals
  - – No involvement of user data
  - – No change on webservers
  - – Incremental deployability
  - – No new or trusted entities

LogPicker's Achievements

- Security Goals
  - ✓ Thwarts collaboration of malicious CA/CT logs
  - ✓ More witnesses to the certificate issuance
  - ✓ Proof of the certificate issuance
  - – Earlier involvement of monitors
- Design Goals
  - – No involvement of user data
  - – No change on webservers
  - – Incremental deployability
  - – No new or trusted entities

LogPicker's Achievements

- Security Goals
  - ✓ Thwarts collaboration of malicious CA/CT logs
  - ✓ More witnesses to the certificate issuance
  - ✓ Proof of the certificate issuance
  - ✓ Earlier involvement of monitors
- Design Goals
  - – No involvement of user data
  - – No change on webservers
  - – Incremental deployability
  - – No new or trusted entities

LogPicker's Achievements

- Security Goals
  - ✓ Thwarts collaboration of malicious CA/CT logs
  - ✓ More witnesses to the certificate issuance
  - ✓ Proof of the certificate issuance
  - ✓ Earlier involvement of monitors
- Design Goals
  - ✓ No involvement of user data
  - – No change on webservers
  - – Incremental deployability
  - – No new or trusted entities

LogPicker's Achievements

- Security Goals
  - ✓ Thwarts collaboration of malicious CA/CT logs
  - ✓ More witnesses to the certificate issuance
  - ✓ Proof of the certificate issuance
  - ✓ Earlier involvement of monitors
- Design Goals
  - ✓ No involvement of user data
  - ✓ No change on webservers
  - – Incremental deployability
  - – No new or trusted entities

LogPicker's Achievements

- Security Goals
  - ✓ Thwarts collaboration of malicious CA/CT logs
  - ✓ More witnesses to the certificate issuance
  - ✓ Proof of the certificate issuance
  - ✓ Earlier involvement of monitors
- Design Goals
  - ✓ No involvement of user data
  - ✓ No change on webservers
  - ✓ Incremental deployability
  - – No new or trusted entities

LogPicker's Achievements

- Security Goals
  - ✓ Thwarts collaboration of malicious CA/CT logs
  - ✓ More witnesses to the certificate issuance
  - ✓ Proof of the certificate issuance
  - ✓ Earlier involvement of monitors
- Design Goals
  - ✓ No involvement of user data
  - ✓ No change on webservers
  - ✓ Incremental deployability
  - ✓ No new or trusted entities

Additional paper contribution

[7] https://logpicker.github.io/

Additional paper contribution

- Protocol goals and crypto primitives

[7] https://logpicker.github.io/

Additional paper contribution

- Protocol goals and crypto primitives
- Analysis of LogPicker's achievements

[7] https://logpicker.github.io/

Additional paper contribution

- Protocol goals and crypto primitives
- Analysis of LogPicker's achievements
- Probabilistic analysis of correctness

[7] https://logpicker.github.io/

Additional paper contribution

- Protocol goals and crypto primitives
- Analysis of LogPicker's achievements
- Probabilistic analysis of correctness
- Discussion on the policies of CT and LP based PKI

[7] https://logpicker.github.io/

Additional paper contribution

- Protocol goals and crypto primitives
- Analysis of LogPicker's achievements
- Probabilistic analysis of correctness
- Discussion on the policies of CT and LP based PKI
- Prototyped simulation of LogPicker protocol [7]

[7] https://logpicker.github.io/

Outlook

- ? Inclusion of monitors
- ? Interlog auditing
- ? Handling protocol aborts
- ? Revocation's still a nightmare

References

[1] Certificate transparency - known logs.
https://www.gstatic.com/ct/log_list/v3/log_list.json.

[2] Ct2 log compromised via salt vulnerability, 2020.
https://groups.google.com/a/chromium.org/forum/#!topic/ct-policy/aKNbZuJzwfM.

[3] Consultation paper on proposed amendments to the ict act for regulating the use and addressing the abuse and misuse of social media in mauritius.
Information & Communication Technologies Authority, Apr 2021.

[4] Transparency report: Https encryption on the web (2023-24-03), 2023.
https://transparencyreport.google.com/https/overview?hl=en.

[5] Y. Aumann and Y. Lindell.
Security against covert adversaries: Efficient protocols for realistic adversaries.
Journal of Cryptology, 2007.

[6] M. Bussiere and M. Fratzscher.
Low probability, high impact: Policy making and extreme events.
Journal of Policy Modeling, 30(1):111–121, 2008.

[7] CA/Browser Forum.
Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, Mar. 2020.
https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.6.8.pdf.

[8] P. Eckersley.
A syrian man-in-the-middle attack against facebook, May 2011.

[9] E. Galperin, S. Schoen, and P. Eckersley.
A post mortem on the iranian diginotar attack, Sep 2011.
https://www.eff.org/de/deeplinks/2011/09/post-mortem-iranian-diginotar-attack.

[10] R. Housley and K. O'Donoghue.
Problems with the Public Key Infrastructure (PKI) for the World Wide Web.
IETF Draft, 2017.

[11] S. Kent.
Attack and threat model for certificate transparency.
Internet Engineering Task Force, 2018.

[12] A. Langley.
Fraudulent digital certificates could allow spoofing, Jan 2013.
https://security.googleblog.com/2013/01/enhancing-digital-certificate-security.html.

[13] B. Laurie.
Certificate Transparency.
ACM Queue, (8), 2014.

[14] G. Markham.
Incidents involving the ca wosign, Aug 2016.
https://groups.google.com/forum/#!topic/mozilla.dev.security.policy/k9PBmyLCi8I%5B1-25%5D.

[15] J. Nightingale.
Revoking trust in digicert sdn. bhd intermediate certificate authority, Mar 2011.
.

[16] R. S. Raman, L. Evdokimov, E. Wurstrow, J. A. Halderman, and R. Ensafi.
Investigating large scale https interception in kazakhstan.
In Proceedings of the ACM Internet Measurement Conference, pages 125–132, 2020.

[17] E. G. Seth Schoen.
Iranian man-in-the-middle attack against google demonstrates dangerous weakness of certificate authorities, Aug 2011.

[18] C. Soghoian and S. Stamm.
Certified lies: Detecting and defeating government interception attacks against ssl.
In Proceedings of ACM Symposium on Operating Systems Principles, pages 1–18, 2010.

[19] T. Zimmermann, J. Ruth, B. Wolters, and O. Hohlfeld.
How HTTP/2 pushes the web: An empirical study of HTTP/2 server push.
In 2017 IFIP Networking Conference, IFIP Networking 2017 and Workshops, 2017.

@z4lem

a.dirksen@tu-braunschweig.de

www.tu-bs.de/ias