

Smolt and Web Application Privacy

Smolt is going to save the world

Smolt will protect your family

Smolt is awesome

We can all learn something from Smolt



Presentation

This presentation is available at / Diese Präsentation ist verfügbar von:

<http://ynemoy.fedorapeople.org/fosdem.pdf>

After FOSDEM, I will post it somewhere more permanent. Information will be available on my blog, at Fedora Planet. Nach FOSDEM lege ich das permanent ab. Informationen darüber werden auf meinem Blog, auf Fedora Planet verfügbar sein.

Smolt

Smolt is a basic hardware profiler. Actually it isn't; it's grown up, and collects hardware and operating system information.

Smolt ist ein einfaches Geräteinformationsfassungprogramm. Es ist ausgewachsen und sammelt Geräte- und Betriebssysteminformation.

Smolt

Smolt collects/sammelt:

- Operating System data – Betriebssystem
 - Language – Internationalisierung
 - CPU
 - Memory and Swap – Arbeitsspeicher
 - Brand – Fabrikant
 - Kernel
 - SELinux
-
-

Smolt

Smolt collects/sammelt:

- Devices and Accessories – Geräte und Zubehör
 - File system statistics – Dateisystemstatistiken
 - Anything you want it to!
 - Alles was Sie gern hätten und sonst noch!
-
-

Smolt

All of the data gathered by Smolt is available publically at <http://smolts.org/> . The rule is, any link that you have access to becomes public information. Everything we do is shared with the community

Alle Daten, die von Smolt gesammelt werden, sind öffentlich unter <http://smolts.org/> verfügbar. Die Regel ist, alle Seiten sind öffentlich. Alles was wir machen, werden mit der Open Source Gemeinde mitgeteilt.

Smolt

We have a Privacy Policy that discusses these goals further, and the level of privacy we are willing to provide. It is also the official set of rules on how you can ask us to collect more information.

Wir haben eine Privacy Policy, die diesen Zielen weiter diskutiert. Es enthält auch die offizielle Regeln, damit können Sie uns nach Information zur Sammlung befragen.

Smolt

I have made some changes to Smolt recently. The Privacy Policy is slightly out of date.

Ich habe seitdem eine paar Änderungen gemacht. Unserer Privacy Policy ist ein bisschen alt.



Smolt

Is Smolt safe?

Will it protect my privacy?

Ist Smolt sicher?

Schützt es meine Daten?

Smolt

Yes!



Smolt

No, I lied, but we try our hardest.

Nein, ich habe gelogen, aber wir versuchen uns zu verbessern.



Privacy

What is it that we actually want to protect?

Was möchten wir eigentlich schützen?

For every machine, there are a million copies. The private bit is that you own one.

Für jeder Maschine gibt es eine million Kopien.
Dass die einzigste Information, die wir haben ist:
wem gehört die Maschine.

Privacy

Your machine and the operating system make a unique 'key' of information. This is represented by your Smolt UUID.

Eine eindeutige 'Schlüssel' besteht aus Ihre Computer und Betriebssystem. Das wird durch eine Smolt-UUID dargestellt.

The UUID is stored on the server, but cannot be traced back to you.

Das UUID steht am Server aber kann nicht verwendet werden um Sie zu identifizieren.

Privacy

This works if you trust the Smoon server you use. If you don't trust it, don't use it.

Das funktioniert solange Sie dem Smoon-Server vertrauen. Sonst, benutzen Sie ihn nicht.



Privacy – Server to Server

Servers will be able to share records, for better statistics. Your UUID is meaningless to the server until you send it a message.

Servers werden in Zukunft Daten mitteilen, um besserer Statistiken zu haben. Wenn Sie keine Meldungen an uns schicken, ist Ihre UUID wertlos.

Privacy

Let's get down to code. What exactly are we protecting?

Was schützen wir genau?

- Four Functions
 - send
 - delete
 - show
 - hide
 - The bastard function
 - rate
-
-

Privacy – send and delete

In these functions, you submit information to a single server. The computer and the server need the UUID to identify you, but you don't need to see it yourself. In fact, **nobody needs to!**

In diese Funktionen geben Sie Informationen an einen Server ab. Ihr Rechner und der Server brauchen Ihre UUID um Sie zu identifizieren, aber du brauchst Sie nicht zu sehen. Eigentlich **braucht sie niemand!**

If the server doesn't save your IP address, submission is anonymous.

Wenn der Server Ihre IP-Adresse nicht speichert, ist die Abgabe anonym.

Privacy - show

I want to see my profile on the server? How can the server display this information anonymously?

Ich möchte meine Profil anschauen. Wie kann der Server es anonym darstellen?

With public UUIDs
Mit öffentlich UUIDs

Privacy - show

Public UUIDs begin with 'pub_', and are only stored on the server. In fact, they are unique to the server.

You must trust your server not to share it.

Öffentliche UUIDs fangen mit 'pub_' an und werden nur in einem Server gespeichert. Sie sind verbunden mit dem Server, und Sie müssen dem Server vertrauen, dass es nicht weitergegeben wird.

Privacy - hide

A secret between one man and himself remains a secret eternal. A secret between two men is no longer a secret. But what if you could take it back?

Tut mir leid, aber ich würde nur Ihre Sprach beschädigen würde ich diese Sätze ins Deutsch übersetzen.



Privacy – hide

You feel your 'identity' is compromised. Simply ask for a new one using hide.

Sie glauben dass Ihre geheime Identität ist kompromitiert. Bitte fragen Sie nach einer neuen, indem Sie 'hide' benutzen.



Privacy - hide

Your old identity is no longer valid, and you become perfectly anonymous. Next time, be more careful. :)

Ihre alter Identität ist nicht mehr gültig, und Sie sind wieder total anonym. Das nächste mal sei vorsichtiger. :)

Privacy - hide

Or don't. You can request a new public UUID as many times as you want.

Oder nicht. Sie können eine neue öffentliche UUID beantragen so oft wie Sie möchten.



Privacy - rate

The four functions do not require the user to interact with the private UUID. Either the computer is operating inside that function, or it isn't. Either you have a public UUID available or you don't.

Für diese vier Funktionen braucht der Benutzer nicht mit der geheimen UUID arbeiten. Entweder läuft der Computer damit oder nicht. Entweder ist eine öffentliche UUID verfügbar oder nicht.

Privacy - rate

These four functions refer only to data that exists both on the server and the sender. When a code path has access to public UUID, it can control everything. Otherwise, it can only view something.

Diese vier Funktionen verweisen nur auf Daten die im Server und auf dem Sender liegen. Wann eine Funktion Zugang zu der öffentlichen UUID hat, kann es alles steuern. Sonst kann es nur etwas sehen.

Privacy - rate

Rating a hardware profile is information that is actually only stored on the server. Other data can also be stored on the server, such as a link to a FAS or Launchpad account, or some other administrative token.

Die Abschätzungen der Daten ist nur auf dem Server gespeichert. Sonstige Daten können auch gespeichert werden, z.B eine Bindung zu eine FAS oder Launchpad Konto, oder mit anderen Daten verbunden werden.

Privacy - rate

How can we differentiate between separate classes of users? Some users might have permission to alter the ratings, other users might only have permission to view them. Some information should be hidden completely.

Wie können wir zwischen verschiedenen Benutzerrollen unterscheiden? Manche Benutzer haben Erlaubnis um Abschätzungen ändern zu können. Manche Informationen sollen komplett versteckt werden können.

Privacy - rate

To solve this problem, we use secondary tokens. A public UUID means base level access. A public UUID and a token means you receive an extra level of access.

Unsere Lösung ist Neben-Token. Eine öffentliche UUID bezeichnet den Basiszugang. Mit einem Neben-Token darf man auf erweiterbare Web-Funktionen zu greifen.

Privacy - rate

Smolt has only two levels of Web access. Our base level is to view a profile. Our secondary level is to rate it.

Smolt hat nur zwei Stufen. Basisstufe erlaubt Profil anzusehen. Zweitestufe erlaubt das Abschätzen.



Privacy - Security

The last step in our privacy system is to secure the private UUID. To be honest, I don't care how it's secured, as long as it **is secure**. Fedora will use SELinux to that end.

Schliesslich müssen wir die geheime UUID schützen. Um Ehrlich zu sein, ist mir die Methode piep egal, solange sie **geschützt wird**. In Fedora wird SELinux verwendet.

Privacy - Security

To secure the UUID, simply confine what code can access the UUID. The four functions 'submit', 'delete', 'show', and 'hide' are the only ones we have.

Um die UUID zu schützen, beschränken Sie welcher Quellcode die UUID benutzen kann. Die vier Funktionen, die wir hier haben, sind 'submit', 'delete', 'show', und 'hide'.

Smolt

Future features on the horizon / Zukünftige Sonderbeiträge

- KernelOOPS
 - Bodhi
 - Possibly inventory management with Func
 - Integration with MythTV
 - Cooperation with other similar programs
-
-

Smolt

and anything else you want!

und alles was Sie gern hätten!

